



Cyber Protect User Guide

Version 21.06

Project/Customer	Version / Date / Classification	Autors
Green	1.0	Acronis
Industriestrasse 33	03.06.2021	
5242 Lupfig	Public	

Table of contents

1 Cyber Protection service editions and sub-editions	15
1.0.1 Cyber Protect edition	15
1.0.2 Cyber Backup edition	15
1.0.3 Comparison of editions	15
1.0.4 Disaster Recovery add-on	15
2 Advanced protection	17
3 Supported Cyber Protect features by operating system	18
4 Software requirements	24
4.1 Supported web browsers	24
4.2 Supported operating systems and environments	24
4.2.1 Agent for Windows	24
4.2.2 Agent for SQL, Agent for Active Directory, Agent for Exchange (for database backup and application-aware backup)	25
4.2.3 Agent for Data Loss Prevention	25
4.2.4 Agent for Exchange (for mailbox backup)	25
4.2.5 Agent for Microsoft 365	26
4.2.6 Agent for Oracle	26
4.2.7 Agent for Linux	26
4.2.8 Agent for Mac	27
4.2.9 Agent for VMware (Virtual Appliance)	27
4.2.10 Agent for VMware (Windows)	27
4.2.11 Agent for Hyper-V	27
4.2.12 Agent for Virtuozzo	28
4.2.13 Agent for Virtuozzo Hybrid Infrastructure	28
4.2.14 Agent for Scale Computing HC3	28
4.2.15 Agent for oVirt	28
4.3 Supported Microsoft SQL Server versions	28
4.4 Supported Microsoft Exchange Server versions	28
4.5 Supported Microsoft SharePoint versions	29
4.6 Supported Oracle Database versions	29
4.7 Supported SAP HANA versions	29
4.8 Supported virtualization platforms	29
4.8.1 Limitations	33
4.9 Compatibility with encryption software	35
4.9.1 Common installation rule	35

4.9.2 The way of using Secure Zone	35
4.9.3 Common backup rule	35
4.9.4 Software-specific recovery procedures	35
5 Supported file systems	37
5.0.1 Data Deduplication	38
6 Activating the account	39
6.1 Two-factor authentication	39
6.1.1 What if...	40
7 Accessing the Cyber Protection service	41
8 Installing the software	42
8.1 Which agent do I need?	42
8.2 System requirements for agents	44
8.3 Preparation	45
8.3.1 Step 1	45
8.3.2 Step 2	45
8.3.3 Step 3	45
8.3.4 Step 4	46
8.3.5 Step 5	46
8.3.6 Step 6	47
8.4 Linux packages	47
8.4.1 Are the required packages already installed?	48
8.4.2 Installing the packages from the repository	49
8.4.3 Installing the packages manually	50
8.5 Proxy server settings	51
8.5.1 In Windows	51
8.5.2 In Linux	52
8.5.3 In macOS	53
8.5.4 In bootable media	54
8.6 Installing Cyber Protection agents	54
8.6.1 Downloading Cyber Protection agents	54
8.6.2 Installing Cyber Protection agents in Windows	55
8.6.3 Installing Cyber Protection agents in Linux	56
8.6.4 Installing Cyber Protection agents in macOS	58
8.6.5 Changing the logon account on Windows machines	59
8.6.6 Dynamic installation and uninstallation of components	60
8.7 Unattended installation or uninstallation	61
8.7.1 Unattended installation or uninstallation in Windows	61

8.7.2 Unattended installation or uninstallation in Linux	67
8.7.3 Unattended installation and uninstallation in macOS	72
8.8 Registering machines manually	75
8.8.1 Passwords with special characters or blank spaces	78
8.9 Autodiscovery of machines	78
8.9.1 How it works	79
8.9.2 Prerequisites	79
8.9.3 Machine discovery process	80
8.9.4 Autodiscovery and manual discovery	81
8.9.5 Managing discovered machines	86
8.9.6 Troubleshooting	87
8.10 Deploying Agent for VMware (Virtual Appliance)	88
8.10.1 Before you start	88
8.10.2 Deploying the OVF template	89
8.10.3 Configuring the virtual appliance	89
8.11 Deploying Agent for Scale Computing HC3 (Virtual Appliance)	91
8.11.1 Before you start	91
8.11.2 Deploying the QCOW2 template	92
8.11.3 Configuring the virtual appliance	93
8.11.4 Agent for Scale Computing HC3 – required roles	94
8.12 Deploying Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance)	94
8.12.1 Before you start	94
8.12.2 Configuring networks in Virtuozzo Hybrid Infrastructure	95
8.12.3 Configuring user accounts in Virtuozzo Hybrid Infrastructure	96
8.12.4 Deploying the QCOW2 template	98
8.12.5 Configuring the virtual appliance	99
8.13 Deploying Agent for oVirt (Virtual Appliance)	102
8.13.1 Before you start	102
8.13.2 Deploying the OVA template	103
8.13.3 Configuring the virtual appliance	104
8.13.4 Agent for oVirt – required roles and ports	105
8.14 Deploying agents through Group Policy	106
8.14.1 Prerequisites	106
8.14.2 Step 1: Generating a registration token	106
8.14.3 Step 2: Creating the .mst transform and extracting the installation package	108
8.14.4 Step 3: Setting up the Group Policy objects	108
8.15 Updating agents	109

8.15.1 Updating agents manually	109
8.15.2 Updating agents automatically	111
8.16 Preventing unauthorized uninstallation or modification of agents	113
8.17 Uninstalling agents	114
8.17.1 In Windows	114
8.17.2 In Linux	114
8.17.3 In macOS	114
8.17.4 Removing Agent for VMware (Virtual Appliance)	115
8.17.5 Removing machines from the service console	115
8.18 Security settings	115
8.18.1 Automatic updates for components	115
8.18.2 Updating the Cyber Protection definitions by schedule	116
8.18.3 Updating the Cyber Protection definitions on-demand	117
8.18.4 Cache storage	117
8.18.5 Remote connection	117
8.19 Changing the service quota of machines	118
8.20 Cyber Protection services installed in your environment	118
8.20.1 Services installed in Windows	118
8.20.2 Services installed in macOS	119
9 Service console	120
10 Device groups	123
10.1 Built-in groups	123
10.2 Custom groups	123
10.3 Creating a static group	124
10.4 Adding devices to static groups	124
10.5 Creating a dynamic group	124
10.5.1 Search criteria	125
10.5.2 Operators	129
10.6 Applying a protection plan to a group	130
11 Multitenancy support	131
12 Protection plan and modules	132
12.1 Creating a protection plan	133
12.2 Default protection plans	133
12.2.1 Default plan options	134
12.3 Resolving plan conflicts	137
12.3.1 Applying several plans to a device	137
12.3.2 Resolving plan conflicts	137

12.4 Operations with protection plans	138
13 #CyberFit Score for machines	140
13.1 How it works	140
13.1.1 #CyberFit scoring mechanism	140
13.2 Running a #CyberFit Score scan	144
14 Backup and recovery	146
14.1 Backup	146
14.2 Protection plan cheat sheet	148
14.3 Selecting data to back up	150
14.3.1 Selecting disks/volumes	150
14.3.2 Selecting files/folders	153
14.3.3 Selecting system state	155
14.3.4 Selecting ESXi configuration	155
14.4 Continuous data protection (CDP)	156
14.5 Selecting a destination	162
14.5.1 Advanced storage option	163
14.5.2 About Secure Zone	163
14.6 Schedule	166
14.6.1 Backup schemes	166
14.6.2 Additional scheduling options	167
14.6.3 Schedule by events	169
14.6.4 Start conditions	172
14.7 Retention rules	178
14.7.1 What else you need to know	179
14.8 Replication	179
14.8.1 Usage examples	179
14.8.2 Supported locations	179
14.9 Encryption	180
14.9.1 Encryption in a protection plan	180
14.9.2 Encryption as a machine property	181
14.9.3 How the encryption works	182
14.10 Notarization	182
14.10.1 How to use notarization	183
14.10.2 How it works	183
14.11 Starting a backup manually	183
14.12 Default backup options	183
14.13 Backup options	184

14.13.1 Availability of the backup options	184
14.13.2 Alerts	187
14.13.3 Backup consolidation	187
14.13.4 Backup file name	188
14.13.5 Backup format	191
14.13.6 Backup validation	193
14.13.7 Changed block tracking (CBT)	193
14.13.8 Cluster backup mode	194
14.13.9 Compression level	195
14.13.10 Error handling	195
14.13.11 Fast incremental/differential backup	197
14.13.12 File filters	197
14.13.13 File-level backup snapshot	199
14.13.14 Forensic data	199
14.13.15 Log truncation	208
14.13.16 LVM snapshotting	208
14.13.17 Mount points	209
14.13.18 Multi-volume snapshot	209
14.13.19 Performance and backup window	210
14.13.20 Physical Data Shipping	214
14.13.21 Pre/Post commands	215
14.13.22 Pre/Post data capture commands	216
14.13.23 Scheduling	219
14.13.24 Sector-by-sector backup	219
14.13.25 Splitting	220
14.13.26 Task failure handling	220
14.13.27 Task start conditions	220
14.13.28 Volume Shadow Copy Service (VSS)	221
14.13.29 Volume Shadow Copy Service (VSS) for virtual machines	222
14.13.30 Weekly backup	223
14.13.31 Windows event log	223
14.14 Recovery	223
14.14.1 Recovery cheat sheet	223
14.14.2 Safe recovery	225
14.14.3 Recovering a machine	226
14.14.4 Prepare drivers	234
14.14.5 Check access to the drivers in bootable environment	234

14.14.6 Automatic driver search	235
14.14.7 Mass storage drivers to install anyway	235
14.14.8 Recovering files	237
14.14.9 Recovering system state	242
14.14.10 Recovering ESXi configuration	242
14.14.11 Recovery options	243
14.15 Operations with backups	251
14.15.1 The Backup storage tab	251
14.15.2 Mounting volumes from a backup	252
14.15.3 Deleting backups	253
14.16 Protecting Microsoft applications	255
14.16.1 Protecting Microsoft SQL Server and Microsoft Exchange Server	255
14.16.2 Protecting Microsoft SharePoint	255
14.16.3 Protecting a domain controller	255
14.16.4 Recovering applications	255
14.16.5 Prerequisites	256
14.16.6 Database backup	258
14.16.7 Application-aware backup	263
14.16.8 Mailbox backup	265
14.16.9 Recovering SQL databases	266
14.16.10 Recovering Exchange databases	270
14.16.11 Recovering Exchange mailboxes and mailbox items	272
14.16.12 Changing the SQL Server or Exchange Server access credentials	278
14.17 Protecting mobile devices	279
14.17.1 Supported mobile devices	279
14.17.2 What you can back up	279
14.17.3 What you need to know	279
14.17.4 Where to get the Cyber Protect app	280
14.17.5 How to start backing up your data	280
14.17.6 How to recover data to a mobile device	281
14.17.7 How to review data via the service console	281
14.18 Protecting Hosted Exchange data	282
14.18.1 What items can be backed up?	282
14.18.2 What items can be recovered?	282
14.18.3 Selecting mailboxes	283
14.18.4 Recovering mailboxes and mailbox items	283
14.19 Protecting Microsoft 365 data	285

14.19.1 Why back up Microsoft 365 data?	285
14.19.2 Agent for Microsoft 365	286
14.19.3 Limitations	287
14.19.4 Required user rights	288
14.19.5 Using the locally installed Agent for Office 365	288
14.19.6 Using the cloud Agent for Microsoft 365	291
14.20 Protecting Google Workspace data	313
14.20.1 What does Google Workspace protection mean?	313
14.20.2 Required user rights	314
14.20.3 About the backup schedule	314
14.20.4 Limitations	314
14.20.5 Adding a Google Workspace organization	315
14.20.6 Creating a personal Google Cloud project	316
14.20.7 Protecting Gmail data	319
14.20.8 Protecting Google Drive files	323
14.20.9 Protecting Shared drive files	327
14.20.10 Notarization	330
14.21 Protecting Oracle Database	331
14.22 Protecting SAP HANA	331
14.23 Protecting websites and hosting servers	331
14.23.1 Protecting websites	331
14.23.2 Protecting web hosting servers	335
14.24 Special operations with virtual machines	335
14.24.1 Running a virtual machine from a backup (Instant Restore)	335
14.24.2 Working in VMware vSphere	339
14.24.3 Backing up clustered Hyper-V machines	356
14.24.4 Limiting the total number of simultaneously backed-up virtual machines	356
14.24.5 Machine migration	357
14.24.6 Windows Azure and Amazon EC2 virtual machines	359
15 Disaster recovery	360
15.1 About Cyber Disaster Recovery Cloud	360
15.1.1 The key functionality	360
15.2 Software requirements	361
15.2.1 Supported operating systems	361
15.2.2 Supported virtualization platforms	361
15.2.3 Limitations	362
15.3 Setting up the disaster recovery functionality	362

15.4 Create a disaster recovery protection plan	363
15.4.1 Editing the Recovery server default parameters	364
15.4.2 Cloud network infrastructure	366
15.5 Setting up connectivity	366
15.5.1 Networking concepts	367
15.5.2 Initial connectivity configuration	377
15.5.3 Prerequisites	379
15.5.4 Network management	385
15.5.5 Prerequisites	397
15.6 Setting up recovery servers	398
15.6.1 Creating a recovery server	398
15.6.2 How failover works	400
15.6.3 How failback works	404
15.6.4 Working with encrypted backups	410
15.7 Setting up primary servers	411
15.7.1 Creating a primary server	411
15.7.2 Operations with a primary server	412
15.8 Managing the cloud servers	412
15.9 Firewall rules for cloud servers	413
15.9.1 Setting firewall rules for cloud servers	414
15.9.2 Checking the cloud firewall activities	417
15.10 Backing up the cloud servers	417
15.11 Orchestration (runbooks)	418
15.11.1 Why use runbooks?	418
15.11.2 Creating a runbook	418
15.11.3 Operations with runbooks	420
16 Antimalware and web protection	422
16.1 Antivirus and antimalware protection	422
16.1.1 Antimalware features	422
16.1.2 Scanning types	422
16.1.3 Antivirus and antimalware protection settings	424
16.2 Active Protection in the Cyber Backup Standard edition	433
16.2.1 Active protection settings in Cyber Backup Standard	434
16.3 URL filtering	438
16.3.1 How it works	438
16.3.2 URL filtering configuration workflow	440
16.3.3 URL filtering settings	440

16.4 Microsoft Defender Antivirus and Microsoft Security Essentials	446
16.4.1 Schedule scan	446
16.4.2 Default actions	447
16.4.3 Real-time protection	447
16.4.4 Advanced	448
16.4.5 Exclusions	448
16.5 Quarantine	449
16.5.1 How do files get into the quarantine folder?	449
16.5.2 Managing quarantined files	449
16.5.3 Quarantine location on machines	450
16.6 Corporate whitelist	450
16.6.1 Automatic adding to the whitelist	450
16.6.2 Manual adding to the whitelist	451
16.6.3 Adding quarantined files to the whitelist	451
16.6.4 Whitelist settings	451
16.7 Antimalware scan of backups	451
16.7.1 How to configure backup scanning in the cloud	452
17 Protection of collaboration and communication applications	453
18 Vulnerability assessment and patch management	454
18.1 Vulnerability assessment	454
18.1.1 Supported Microsoft and third-party products	455
18.1.2 Supported Apple and third-party products	456
18.1.3 Supported Linux products	457
18.1.4 Vulnerability assessment settings	457
18.1.5 Vulnerability assessment for Windows machines	459
18.1.6 Vulnerability assessment for Linux machines	459
18.1.7 Vulnerability assessment for macOS devices	459
18.1.8 Managing found vulnerabilities	460
18.2 Patch management	461
18.2.1 How it works	462
18.2.2 Patch management settings	463
18.2.3 Managing list of patches	466
18.2.4 Automatic patch approval	467
18.2.5 Manual patch approval	470
18.2.6 On-demand patch installation	470
18.2.7 Patch lifetime in the list	471
19 Software inventory	472

19.1	Enabling the software inventory scanning	472
19.2	Running a software inventory scan manually	473
19.3	Browsing the software inventory	473
19.4	Viewing the software inventory of a single device	475
20	Hardware inventory	477
20.1	Enabling the hardware inventory scanning	477
20.2	Running a hardware inventory scan manually	478
20.3	Browsing the hardware inventory	478
20.4	Viewing the hardware of a single device	481
21	Remote desktop access	483
21.1	Remote access (RDP and HTML5 clients)	483
21.1.1	How it works	484
21.1.2	How to connect to a remote machine	484
21.1.3	How to run a remote assistance session	485
21.2	Share a remote connection with users	485
22	Remote wipe	487
23	Smart protection	488
23.1	Threat feed	488
23.1.1	How it works	488
23.1.2	Deleting all alerts	490
23.2	Data protection map	491
23.2.1	How it works	491
23.2.2	Managing the detected unprotected files	491
23.2.3	Data protection map settings	492
24	Enhanced security mode	494
24.1	Limitations	494
24.2	Setting the encryption password	494
24.3	Changing the encryption password	495
24.4	Recovering backups	495
25	Device control	496
25.0.1	Limitation on the use of the agent for Data Loss Prevention with Hyper-V	497
25.1	Using device control	498
25.1.1	Enable or disable device control	498
25.1.2	View or change access settings	499
25.1.3	Exclude device subclasses from access control	500
25.1.4	Exclude individual USB devices from access control	500
25.1.5	View device control alerts	502

25.2 Access settings	502
25.2.1 OS notification and service alerts	506
25.3 Device types allowlist	507
25.4 USB devices allowlist	508
25.4.1 USB devices database	510
25.5 Excluding processes from access control	512
25.6 Device control alerts	514
25.6.1 Action field values	515
26 The Plans tab	518
26.1 Protection plan	518
26.2 Backup scanning plan	518
26.3 Backup plans for cloud applications	519
27 Bootable media	521
27.1 Custom or ready-made bootable media?	521
27.2 Linux-based or WinPE/WinRE-based bootable media?	521
27.2.1 Linux-based	521
27.2.2 WinPE/WinRE-based	521
27.3 Creating physical bootable media	522
27.4 Bootable Media Builder	523
27.4.1 Why use Bootable Media Builder?	523
27.4.2 32-bit or 64-bit?	523
27.4.3 Linux-based bootable media	523
27.4.4 Top-level object	528
27.4.5 Variable object	528
27.4.6 Control type	529
27.4.7 WinPE-based and WinRE-based bootable media	531
27.4.8 Registering the bootable media	534
27.4.9 Network settings	535
27.5 Connecting to a machine booted from bootable media	536
27.5.1 Local connection	536
27.5.2 Configuring network settings	536
27.6 Operations with bootable media	537
27.6.1 Setting up a display mode	537
27.6.2 Recovery	538
27.7 Startup Recovery Manager	538
28 Monitoring	540
28.1 Cyber Protection	541

28.2 Protection status	541
28.2.1 Protection status	541
28.2.2 Discovered machines	542
28.3 #CyberFit Score by machine	543
28.4 Disk health monitoring	543
28.4.1 How it works	544
28.4.2 Disk health widgets	544
28.4.3 Disk health status alerts	547
28.5 Data protection map	547
28.6 Vulnerability assessment widgets	548
28.6.1 Vulnerable machines	548
28.6.2 Existing vulnerabilities	549
28.7 Patch installation widgets	549
28.7.1 Patch installation status	549
28.7.2 Patch installation summary	550
28.7.3 Patch installation history	550
28.7.4 Missing updates by categories	550
28.8 Backup scanning details	551
28.9 Recently affected	551
28.10 Cloud applications	552
28.11 Software inventory widgets	553
28.12 Hardware inventory widgets	554
29 Reports	555
29.0.1 Adding a report	556
29.0.2 Editing a report	556
29.0.3 Scheduling a report	557
29.0.4 Exporting and importing the report structure	558
29.0.5 Downloading a report	558
29.0.6 Dumping the report data	558
30 Troubleshooting	559
Glossary	560
Index	564

1 Cyber Protection service editions and sub-editions

This section contains information about working with services, editions, and offering items that were available as part of the licensing model in Acronis Cyber Cloud 21.02 and earlier. These offering items and editions are still supported and can be configured for tenants as needed, but not recommended, and are considered legacy now. For information about the new offering items, see "Advanced protection" (p. 17).

The following editions are available:

- Cyber Protect
- Cyber Backup

1.0.1 Cyber Protect edition

This edition is licensed per workload—that is, according to the number of protected machines, regardless of the size of backed-up data.

Within the Cyber Protect edition, the following sub-editions are available:

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

1.0.2 Cyber Backup edition

This edition is licensed per GB—that is, according to the size of backed-up data, regardless of the number of protected machines.

In the Cyber Backup edition, there are no sub-editions—only Cyber Backup Standard offering items are available.

1.0.3 Comparison of editions

The number and scope of the available features depend on the edition of Cyber Protection service. For a detailed comparison between the features in each edition and sub-edition, refer to [Compare Acronis Cyber Protection Editions](#).

1.0.4 Disaster Recovery add-on


The Disaster Recovery add-on provides recovery functionality designed for companies that have high requirements for the Recovery Time Objective (RTO). This add-on is available only with the Cyber Protect edition.


Note

The Disaster recovery add-on cannot be used with the Cyber Protect Essentials sub-edition.

2 Advanced protection

By default, Cyber Protect includes features that cover most of the cyber security threats. You can use these features without an additional fee. In addition, you can enable advanced features to boost the protection of your workloads.

If an Advanced protection feature is enabled for you to use, it appears in the protection plan marked with the Advanced feature icon . When you try to enable the feature, you will be prompted that additional billing applies.

If an Advanced protection feature is not enabled for you, the following icon appears next to the feature name in the protection plan . A message will prompt you to contact your administrator to enable the required advanced pack for you.

3 Supported Cyber Protect features by operating system

Note

This topic contains information about all Cyber Protect features and the operating systems on which they are supported. Some features might require additional licensing, depending on the applied licensing model.

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

- Windows: Windows 7 Service Pack 1 and later, Windows Server 2008 R2 Service Pack 1 and later. Windows Defender Antivirus management is supported on Windows 8.1 and later.
- Linux: CentOS 6.10, 7.8+, CloudLinux 6.10, 7.8+, Ubuntu 16.04.7+, where plus refers to minor versions of these distributions.

Other Linux distributions and versions might be supported, but have not been tested.

- macOS: 10.13.x and later (only Antivirus and Antimalware protection, and Device control are supported). Device control functionality is supported on macOS 10.15 and later or macOS 11.2.3 and later.

Agent for Data Loss Prevention might be installed on unsupported macOS systems because it is an integral part of Agent for Mac. In this case, the Cyber Protect console will display that Agent for Data Loss Prevention is installed on the computer, but the device control functionality will not work. Device control functionality will only work on [macOS systems that are supported by Agent for Data Loss Prevention](#).

Note

Antimalware protection for Linux and macOS is supported only when Advanced antimalware protection is enabled.

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, Agent for Virtuozzo Hybrid Infrastructure, Agent for Scale Computing, or Agent for oVirt only backup is supported.

Cyber Protect features	Windows	Linux	macOS
Default protection plans			
Remote Workers	Yes	No	No
Office Workers (third-party antivirus)	Yes	No	No
Office Workers (Cyber Protect antivirus)	Yes	No	No

Cyber Protect Essentials (only for Cyber Protect Essentials edition)	Yes	No	No
Forensic backup			
Collecting memory dump	Yes	No	No
Snapshot of running processes	Yes	No	No
Forensic backup for machines with one drive without reboot	Yes	No	No
Notarization of local image forensic backup	Yes	No	No
Notarization of cloud image 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
Active Protection			
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 Anti-malware components)
Trusted/blocked process management	Yes	No	Yes
Processes/folders exclusions	Yes	Yes	Yes
Ransomware detection based on a process behavior (AI-based)	Yes	No	No

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	Yes	Yes
Server-side protection	Yes	No	No
Zoom, Cisco Webex, Citrix Workspace, and Microsoft Teams protection	Yes	No	No
Antivirus and Antimalware protection			
Fully-integrated Active Protection functionality	Yes	No	No
Real-time antimalware protection	Yes	Yes, when Advanced antimalware is enabled	Yes, when Advanced antimalware is enabled
Advanced real-time antimalware protection with local signature-based detection	Yes	Yes	Yes
Static analysis for portable executable files	Yes	No	Yes*
On-demand antimalware scanning	Yes	Yes**	Yes
Network folder protection	Yes	Yes	No
Server-side protection	Yes	No	No
Scan of archive files	Yes	No	Yes
Scan of removable drives	Yes	No	Yes
Scan of only new and changed files	Yes	No	Yes
File/folder exclusions	Yes	Yes	Yes***
Processes exclusions	Yes	No	No
Behavioral analysis engine	Yes	No	No
Exploit prevention	Yes	No	No
Quarantine	Yes	Yes	Yes
Quarantine auto clean-up	Yes	No	Yes
URL filtering (http/https)	Yes	No	No
Corporate-wide whitelist	Yes	No	Yes

Microsoft Defender Antivirus management	Yes	No	No
Microsoft Security Essentials management	Yes	No	No
Registering and managing Antivirus and Antimalware protection via Windows Security Center	Yes	No	No
Vulnerability assessment			
Vulnerability assessment of operating system and its native applications	Yes	Yes****	Yes
Vulnerability assessment for 3rd-party applications	Yes	No	Yes
Patch management			
Patch auto-approval	Yes	No	No
Patch auto-installation	Yes	No	No
Patch testing	Yes	No	No
Manual patch installation	Yes	No	No
Patch scheduling	Yes	No	No
Fail-safe patching: backup of machine before installing patches as part of protection plan	Yes	No	No
Cancellation of a machine reboot if a backup is running	Yes	No	No
Data protection map			
Adjustable definition of important files	Yes	No	No
Scanning machines to find unprotected files	Yes	No	No
Unprotected locations overview	Yes	No	No
Ability to start the protection action from the Data protection map widget (Protect all files action)	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			
Antimalware scan of image backups as part of backup plan	Yes	No	No
Scanning of image backups for malware in cloud	Yes	No	No
Malware scan of encrypted backups	Yes	No	No
Safe recovery			
Antimalware scanning with Antivirus and Antimalware protection during the recovery process	Yes	No	No
Safe recovery for encrypted backups	Yes	No	No
Remote desktop connection			
Connection via HTML5-based client	Yes	No	No
Connection via native Windows RDP client	Yes	No	No
Remote assistance	Yes	No	No
#CyberFit Score			
#CyberFit Score status	Yes	No	No
#CyberFit Score standalone tool	Yes	No	No
#CyberFit Score recommendations	Yes	No	No
Data loss prevention			
Device control	Yes	No	Yes
Management options			
Upsell scenarios to promote Cyber Protect editions	Yes	Yes	Yes
Web-based centralized and remote management console	Yes	Yes	Yes
Protection options			
Remote wipe (Windows 10 only)	Yes	No	No
Cyber Protect Monitor			
Cyber Protect Monitor app	Yes	No	Yes

Protection status for Zoom	Yes	No	No
Protection status for Cisco Webex	Yes	No	No
Protection status for Citrix Workspace	Yes	No	No
Protection status for Microsoft Teams	Yes	No	No
Software inventory			
Software inventory scanning	Yes	No	Yes
Software inventory monitoring	Yes	No	Yes
Hardware inventory			
Hardware inventory scanning	Yes	No	Yes
Hardware inventory monitoring	Yes	No	Yes

* Static analysis for portable executable files is supported only for scheduled scans on macOS.

** Start conditions are not supported for on-demand scanning on Linux.

*** 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.

**** 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.

4 Software requirements

4.1 Supported web browsers

The web interface supports the following web browsers:

- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later
- Windows Internet Explorer 11 or later
- Microsoft Edge 25 or later
- Safari 8 or later running in the macOS and iOS operating systems

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

4.2 Supported operating systems and environments

4.2.1 Agent for Windows

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 and later – Standard and Enterprise editions (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Vista – all editions
- 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 Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server

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

Each of these agents can be installed on a machine running any operating system listed above and a supported version of the respective application.

4.2.3 Agent for Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 and later
- Microsoft Windows Server 2008 R2 and later
- macOS 10.15 (Catalina) and later
- macOS 11.2.3 (Big Sur) and later

Note

Agent for Data Loss Prevention for macOS supports only x64 processors (ARM64 is not supported).

Note

Agent for Data Loss Prevention might be installed on unsupported macOS systems because it is an integral part of Agent for Mac. In this case, the Cyber Protect console will display that Agent for Data Loss Prevention is installed on the computer, but the device control functionality will not work. Device control functionality will only work on [macOS systems that are supported by Agent for Data Loss Prevention](#).

4.2.4 Agent for Exchange (for mailbox backup)

- 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

4.2.5 Agent for Microsoft 365

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

4.2.6 Agent for Oracle

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

4.2.7 Agent for Linux

Linux with kernel from 2.6.9 to 5.7 and glibc 2.3.4 or later, including the following x86 and x86_64 distributions:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0*, 8.1*, 8.2*, 8.3*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10 and 11
- SUSE Linux Enterprise Server 12 – supported on file systems, except for Btrfs
- Debian 4, 5, 6, 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
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.8, 8.0, 8.1, 8.2, 8.3– both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.2, 8.3
- ClearOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7
- 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`

* Configurations with Stratis are not supported.

4.2.8 Agent for Mac

Both x64 and ARM64* processors are supported.

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

* Antimalware Protection, Hardware inventory, and Software inventory require Rosetta 2 on Apple Silicon Macs.

4.2.9 Agent for VMware (Virtual Appliance)

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

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

4.2.10 Agent for VMware (Windows)

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

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

4.2.11 Agent for Hyper-V

- Windows Server 2008 (x64 only) with Hyper-V role, including Server Core installation mode
- Windows Server 2008 R2 with Hyper-V role, including Server Core installation mode
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 with Hyper-V role, including Server Core installation mode
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (x64 only) with Hyper-V
- Windows 10 – Pro, Education, and Enterprise editions with Hyper-V

- Windows Server 2016 with Hyper-V role – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 with Hyper-V role – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2019

4.2.12 Agent for Virtuozzo

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

4.2.13 Agent for Virtuozzo Hybrid Infrastructure

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5

4.2.14 Agent for Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0

4.2.15 Agent for oVirt

Red Hat Virtualization 4.2, 4.3, 4.4

4.3 Supported Microsoft SQL Server versions

- 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 SQL Server 2008
- Microsoft SQL Server 2005

4.4 Supported Microsoft Exchange Server versions

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

4.5 Supported Microsoft SharePoint versions

Cyber Protection supports the following Microsoft SharePoint versions:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

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

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

4.6 Supported Oracle Database versions

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

Only single-instance configurations are supported.

4.7 Supported SAP HANA versions

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

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

4.8 Supported virtualization platforms

The following table summarizes how various virtualization platforms are supported.

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

VMware vSphere Essentials*		
VMware vSphere Essentials Plus*		
VMware vSphere Standard*		
VMware vSphere Advanced		
VMware vSphere Enterprise		
VMware vSphere Enterprise Plus		
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual server)		
VMware Workstation		+
VMware ACE		
VMware Player		
Microsoft		
Windows Server 2008 (x64) with Hyper-V		
Windows Server 2008 R2 with Hyper-V		
Microsoft Hyper-V Server 2008/2008 R2	+	+
Windows Server 2012/2012 R2 with Hyper-V		
Microsoft Hyper-V Server 2012/2012 R2		

Windows 8, 8.1 (x64) with Hyper-V		
Windows 10 with Hyper-V		
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		
Microsoft Virtual PC 2004 and 2007		+
Windows Virtual PC		
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5		Only fully virtualized (aka HVM) guests. Paravirtualized (aka PV) guests are not supported.
Red Hat and Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0,		+

3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		
Red Hat Virtualization (managed by oVirt) 4.2, 4.3, 4.4	+	+
Kernel-based Virtual Machines (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Only fully virtualized (aka HVM) guests. Paravirtualized (aka PV) guests are not supported.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x through 20180425.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Virtual machines only. Containers are not supported.
Virtuozzo 7.0.13, 7.0.14	Ploop containers only. Virtual machines are not supported.	Virtual machines only. Containers are not

		supported.
Virtuozzo Hybrid Server 7.5	+	Virtual machines only. Containers are not supported.
Virtuozzo Hybrid Infrastructure		
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+
Amazon		
Amazon EC2 instances		+
Microsoft Azure		
Azure virtual machines		+

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

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

4.8.1 Limitations

- **Fault tolerant machines**

Agent for VMware backs up a fault tolerant machine only if fault tolerance was enabled in VMware vSphere 6.0 and later. If you upgraded from an earlier vSphere version, it is enough to disable and enable fault tolerance for each machine. If you are using an earlier vSphere version, install an agent in the guest operating system.

- **Independent disks and RDM**

Agent for VMware does not back up Raw Device Mapping (RDM) disks in physical compatibility mode or independent disks. The agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding independent disks and RDMs in physical compatibility mode from the protection plan. If you want to back up these disks or data on these disks, install an agent in the guest operating system.

- **Pass-through disks**

Agent for Hyper-V does not back up pass-through disks. During backup, the agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding pass-through disks

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

- **Linux machines containing logical volumes (LVM)**

Agent for VMware and Agent for Hyper-V do not support the following operations for Linux machines with LVM:

- P2V migration, V2P migration, and V2V migration from Virtuozzo. Use Agent for Linux to create the backup and bootable media to recover.
- Running a virtual machine from a backup created by Agent for Linux.

- **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 GEN2 VMs, Secure Boot is disabled after the virtual machine is recovered to both new virtual machine or an existing virtual machine.

- **ESXi configuration backup** is not supported for VMware vSphere 7.0.

4.9 Compatibility with encryption software

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

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

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

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

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

4.9.1 Common installation rule

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

4.9.2 The way of using Secure Zone

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

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

4.9.3 Common backup rule

You can do a disk-level backup in the operating system.

4.9.4 Software-specific recovery procedures

Microsoft BitLocker Drive Encryption

To recover a system that was encrypted by BitLocker:

1. Boot from the bootable media.
2. Recover the system. The recovered data will be unencrypted.

3. Reboot the recovered system.
4. Turn on BitLocker.

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

McAfee Endpoint Encryption and PGP Whole Disk Encryption

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

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

5 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 (bootable media supports only recovery). The limitations apply to both the agents and bootable media.

File system	Supported by			Limitations
	Agents	Bootable media for Windows and Linux	Bootable media for Mac	
FAT16/32	All agents	+	+	No limitations
NTFS		+	+	
ext2/ext3/ext4		+	-	
HFS+	Agent for Mac	-	+	<ul style="list-style-type: none"> Supported starting with macOS High Sierra 10.13 Disk configuration should be re-created manually when recovering to a non-original machine or bare metal.
APFS		-	+	
JFS	Agent for Linux	+	-	<ul style="list-style-type: none"> Files cannot be excluded from a disk backup Fast incremental/differential backup cannot be enabled
ReiserFS3		+	-	
ReiserFS4		+	-	
ReFS	All agents	+	+	<ul style="list-style-type: none"> Files cannot be excluded from a disk backup Fast incremental/differential backup cannot be enabled Volumes cannot be resized during a recovery
XFS		+	+	
Linux swap	Agent for Linux	+	-	No limitations
exFAT	All agents	+	+	<ul style="list-style-type: none"> Only disk/volume backup

		Bootable media cannot be used for recovery if the backup <i>is stored on</i> exFAT		is supported <ul style="list-style-type: none"> Files cannot be excluded from a backup Individual files cannot be recovered from a backup
--	--	--	--	---

The software automatically switches to the sector-by-sector mode when backing up drives with unrecognized or unsupported file systems (for example, Btrfs). 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.

5.0.1 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.

6 Activating the account

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

- **Your login.** This is the user name that you use to log in. Your login is also shown on the account activation page.
- **Account activation button.** Click the button and set the password for the account. Ensure that your password is at least nine characters long.
If your administrator has enabled two-factor authentication, you will be prompted to [set up two-factor authentication for your account](#).

6.1 Two-factor authentication

Two-factor authentication provides extra protection from unauthorized access to your account. When two-factor authentication is set up, you are required to enter your password (the first factor) and a one-time code (the second factor) to log in to the service console. The one-time code is generated by a special application that must be installed on your mobile phone or another device that belongs to you. Even if someone finds out your login and password, they still will not be able to login without access to your second-factor device.

The one-time code is generated based on the device's current time and the secret provided by the Cyber Protection service as the QR code or alphanumeric code. During the first login, you need to enter this secret to the authentication application.

To set up two-factor authentication for your account

1. Choose the second-factor device.
Most commonly it is a mobile phone, but you can also use a tablet, laptop, or desktop.
2. Ensure that the device time settings are correct and reflect the actual current time. Ensure that the device locks itself after a period of inactivity.
3. Install the authentication application on the device. The recommended applications are Google Authenticator or Microsoft Authenticator.
4. Go to the service console login page and set your password.
The service console shows the QR code and the alphanumeric code.
5. Save the QR code and the alphanumeric code in any convenient way (such as, print out the screen, write down the code, or save the screenshot in cloud storage). If you lose the second-factor device, you will be able to reset the two-factor authentication by using these codes.
6. Open the authentication application, and then do one of the following:
 - Scan the QR code
 - Manually enter the alphanumeric code to the applicationThe authentication application generates a one-time code. A new code will be generated every 30 seconds.
7. Return to the service console login page and enter the generated code.

A one-time code is valid for 30 seconds. If you wait longer than 30 seconds, use the next generated code.

When logging in the next time, you can select the checkbox **Trust this browser....** If you do this, the one-time code will not be required when you log in by using this browser on this machine.

6.1.1 What if...

...I lost the second-factor device?

If you have a trusted browser, you will be able to log in by using this browser. Nevertheless, when you have a new device, repeat steps 1-3 and 6-7 of the above procedure by using the new device and the saved QR code or alphanumeric code.

If you have not saved the code, ask the administrator or service provider to reset the two-factor authentication for your account, and then repeat steps 1-3 and 6-7 of the above procedure by using the new device.

...I want to change the second-factor device?

When logging in, click the **Reset two-factor authentication settings** link, confirm the operation by entering the one-time code, and then repeat the above procedure by using the new device.

7 Accessing the Cyber Protection service

You can log in to the Cyber Protection service if you activated your account.

To log in to the Cyber Protection service

1. Go to the Cyber Protection service login page. The login page address was included in the activation email message.
2. Type the login, and then click **Next**.
3. Type the password, and then click **Next**.
4. If you have the administrator role in the Cyber Protection service, click **Cyber Protection**.

Users who do not have the administrator role log in directly to the service console.


The timeout period for the service console is 24 hours for active sessions and 1 hour for idle sessions.

To reset your password

1. Go to the Cyber Protection service login page.
2. Type your login, and then click **Next**.
3. Click **Forgot password?**
4. Confirm that you want further instructions by clicking **Send**.
5. Follow the instructions in the email that you have received.
6. Set up your new password. Ensure that your password is at least eight characters long.

You can change the language of the web interface by clicking the account icon in the top-right corner.

If **Cyber Protection** is not the only service you are subscribed to, you can switch between the

services by using the  icon in the top-right corner. Administrators can also use this icon for switching to the management portal.

If you are subscribed to any of the Cyber Protection editions, you can send feedback about the product from the service console. In the left navigation menu, click **Send feedback**, fill in the fields, attach files (if any) and click **Send**.

8 Installing the software

8.1 Which agent do I need?

Selecting an agent depends on what you are going to back up. The table below summarizes the information, to help you decide.

In Windows, Agent for Exchange, Agent for SQL, Agent for Active Directory, and Agent for Oracle require that Agent for Windows is also installed. Thus, if you install, for example, Agent for SQL, you also will be able to back up the entire machine where the agent is installed.

It is recommended to install Agent for Windows when you install also Agent for VMware (Windows) and Agent for Hyper-V.

In Linux, Agent for Oracle and Agent for Virtuozzo require that Agent for Linux (64-bit) is also installed. These three agents share one installer.

What are you going to back up?	Which agent to install?	Where to install it?
Physical machines		
Physical machines running Windows	Agent for Windows	On the machine that will be backed up.
Physical machines running Linux	Agent for Linux	
Physical machines running macOS	Agent for Mac	
Applications		
SQL databases	Agent for SQL	On the machine running Microsoft SQL Server.
Exchange databases	Agent for Exchange	On the machine running the Mailbox role of Microsoft Exchange Server.*
Microsoft 365 mailboxes	Agent for Microsoft 365	On a Windows machine that is connected to the Internet. Depending on the desired functionality, you may or may not need to install Agent for Microsoft 365. For more information, refer to "Protecting Microsoft 365 data".
Microsoft 365 OneDrive files and SharePoint Online sites	—	This data can be backed up only by an agent that is installed in the cloud. For more information, refer to "Protecting Microsoft 365 data".
Google Workspace Gmail mailboxes, Google Drive	—	This data can be backed up only by an agent that is installed in the cloud. For more information, refer to

files, and Shared drive files		"Protecting Google Workspace" .
Machines running Active Directory Domain Services	Agent for Active Directory	On the domain controller.
Machines running Oracle Database	Agent for Oracle	On the machine running Oracle Database.
Virtual machines		
VMware ESXi virtual machines	Agent for VMware (Windows)	On a Windows machine that has network access to vCenter Server and to the virtual machine storage.**
	Agent for VMware (Virtual Appliance)	On the ESXi host.
Hyper-V virtual machines	Agent for Hyper-V	On the Hyper-V host.
Scale Computing HC3 virtual machines	Agent for Scale Computing HC3 (Virtual Appliance)	On the Scale Computing HC3 host.
Red Hat Virtualization virtual machines (managed by oVirt)	Agent for oVirt (Virtual Appliance)	On the Red Hat Virtualization host.
Virtuozzo virtual machines and containers***	Agent for Virtuozzo	On the Virtuozzo host.
Virtuozzo Hybrid Infrastructure virtual machines	Agent for Virtuozzo Hybrid Infrastructure	On the Virtuozzo Hybrid Infrastructure host.
Virtual machines hosted on Amazon EC2	The same as for physical machines****	On the machine that will be backed up.
Virtual machines hosted on Windows Azure		
Citrix XenServer virtual machines		
Red Hat Virtualization (RHV/RHEV)		
Kernel-based Virtual Machines (KVM)		

Oracle virtual machines		
Nutanix AHV virtual machines		
Mobile devices		
Mobile devices running Android	Mobile app for Android	On the mobile device that will be backed up.
Mobile devices running iOS	Mobile app for iOS	

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

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

***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.

8.2 System requirements for agents

Agent	Disk space required for installation
Agent for Windows	1.2 GB
Agent for Linux	2 GB
Agent for Mac	1 GB
Agent for SQL and Agent for Windows	1.2 GB
Agent for Exchange and Agent for Windows	1.3 GB
Agent for Data Loss Prevention	500 MB
Agent for Microsoft 365	500 MB
Agent for Active Directory and Agent for Windows	2 GB
Agent for VMware and Agent for Windows	1.5 GB

Agent for Hyper-V and Agent for Windows	1.5 GB
Agent for Virtuozzo and Agent for Linux	1 GB
Agent for Virtuozzo Hybrid Infrastructure	700 MB
Agent for Oracle and Agent for Windows	2.2 GB
Agent for Oracle and Agent for Linux	2 GB

Backup operations 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.

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

8.3 Preparation

8.3.1 Step 1

Choose an agent, depending on what you are going to back up. For more information on the possible choices, refer to [Which agent do I need?](#)

8.3.2 Step 2

Ensure that there is enough free space on your hard drive to install an agent. For detailed information about the required space, refer to "System requirements for agents" (p. 44).

8.3.3 Step 3

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

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

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

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

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

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

8.3.4 Step 4

Cyber Protect features require Microsoft Visual C++ 2017 Redistributable. Please ensure that it is already installed on your machine or install it before installing the agent. After the installation of Microsoft Visual C++, a restart may be required. You can find the Microsoft Visual C++ Redistributable package here <https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows>.

8.3.5 Step 5

Verify that your firewalls and other components of your network security system (such as a proxy sever) allow both inbound and outbound connections through the following TCP ports.

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

If a proxy server is enabled in your network, refer to the "[Proxy server settings](#)" section to understand whether you need to configure these settings on each machine that runs a protection agent.

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

TCP ports required for backup and replication of VMware virtual machines

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

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

The service that is responsible for accepting VM replication data on the target Agent for VMware (Virtual Appliance) is called "Replica disk server." This service is responsible for the WAN optimization techniques, such as traffic compression and deduplication during VM replication, including replica seeding (see [Seeding an initial replica](#)). When no Agent for VMware (Virtual

Appliance) is running on the target ESXi host, this service is not available, and therefore the replica seeding scenario is not supported.

Ports required by the Downloader component

The Downloader component is responsible for delivering updates to a computer and distributing them to other Downloader instances. It can run in agent mode which turns its computer into Downloader agent. The Downloader agent downloads updates from the internet and servers as the source of updates distribution to other computers. The Downloader requires the following ports to operate.

- **6888** Used by BitTorrent protocol for torrent peer to peer updates.
- **6771** Used as the local peer discovery port. Also takes part in peer to peer updates.
- **18018** Used for communication between updaters working in different modes: Updater and UpdaterAgent.
- **18019** Local port, used for communication between the Updater and the <BRAND> Cyber Protection agent.

8.3.6 Step 6

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

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

Note

You do not have to open them in the Firewall.

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

Changing the ports used by the Cyber Protection agent

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

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

8.4 Linux packages

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

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

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

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

8.4.1 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.

8.4.2 Installing the packages from the repository

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

Linux distribution	Package names	How to install
Red Hat Enterprise Linux	kernel-devel gcc make elfutils-libelf-devel	The setup program will download and install the packages automatically by using your Red Hat subscription.
	perl	Run the following command: <pre>yum install perl</pre>
CentOS Fedora	kernel-devel gcc make elfutils-libelf-devel	The setup program will download and install the packages automatically.
	perl	Run the following command: <pre>yum install perl</pre>
Ubuntu Debian	linux-headers linux-image gcc make perl	Run the following commands: <pre>sudo apt-get update sudo apt-get install linux-headers-\$(uname -r) sudo apt-get install linux-image-\$(uname -r) sudo apt-get install gcc-<package version> sudo apt-get install make sudo apt-get install perl</pre>
SUSE Linux OpenSUSE	kernel-source gcc make perl	<pre>sudo zypper install kernel-source sudo zypper install gcc sudo zypper install make sudo zypper install perl</pre>

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

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

8.4.3 Installing the packages manually

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

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

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

- In Red Hat Enterprise Linux, CentOS, or Fedora, run the following command as the root user:

```
rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

- In Ubuntu, run the following command:

```
sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

Example: Installing the packages manually in Fedora 14

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

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

```
cat /proc/version
```

The output of this command includes the following:

```
Linux version 2.6.35.6-45.fc14.i686  
gcc version 4.5.1
```

2. Obtain the **kernel-devel** and **gcc** packages that correspond to this kernel version:

```
kernel-devel-2.6.35.6-45.fc14.i686.rpm  
gcc-4.5.1-4.fc14.i686.rpm
```

3. Obtain the **make** package for Fedora 14:

```
make-3.82-3.fc14.i686
```

4. Install the packages by running the following commands as the root user:

```
rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
rpm -ivh gcc-4.5.1.fc14.i686.rpm
rpm -ivh make-3.82-3.fc14.i686
```

You can specify all these packages in a single `rpm` command. Installing any of these packages may require installing additional packages to resolve dependencies.

8.5 Proxy server settings

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

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

8.5.1 In Windows

If a proxy server is configured in Windows (**Control panel > Internet Options > Connections**), the setup program reads the proxy server settings from the registry and uses them automatically. Also, you can enter the proxy settings during the installation, or specify them in advance by using the procedure described below. To change the proxy settings after the installation, use the same procedure.

To specify the proxy settings in Windows

1. Create a new text document and open it in a text editor, such as Notepad.
2. Copy and paste the following lines into the file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Replace `proxy.company.com` with your proxy server host name/IP address, and `000001bb` with the hexadecimal value of the port number. For example, `000001bb` is port 443.
4. If your proxy server requires authentication, replace `proxy_login` and `proxy_password` with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the document as **proxy.reg**.
6. Run the file as an administrator.
7. Confirm that you want to edit the Windows registry.
8. If the protection agent is not installed yet, you can install it now.
9. Open file **%programdata%\Acronis\Agent\etc\aaokore.yaml** in a text editor.

10. 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
```

11. Replace proxy_login and proxy_password with the proxy server credentials, and proxy_address:port with the address and port number of the proxy server.
12. In the **Start** menu, click **Run**, type: **cmd**, and click **OK**.
13. Restart the aakore service by using the following commands:

```
net stop aakore  
net start aakore
```

14. Restart the agent by using the following commands:

```
net stop mms  
net start mms
```

8.5.2 In Linux

Run the installation file with the parameters `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD`. To change the proxy settings after the installation, use the procedure described below.

To change the proxy settings in Linux

1. Open the file **/etc/Acronis/Global.config** in a text editor.
2. 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.
3. Replace ADDRESS with the new proxy server host name/IP address, and PORT with the decimal value of the port number.
 4. If your proxy server requires authentication, replace LOGIN and PASSWORD with the proxy server credentials. Otherwise, delete these lines from the file.
 5. Save the file.
 6. Open file **/opt/acronis/etc/aakore.yaml** in a text editor.

7. Locate the **env** section or create it and add the following lines:

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

8. Replace proxy_login and proxy_password with the proxy server credentials, and proxy_address:port with the address and port number of the proxy server.
9. Restart the aakore service by using the following command:

```
sudo service aakore restart
```

10. Restart the agent by executing the following command in any directory:

```
sudo service acronis_mms restart
```

8.5.3 In macOS

You can enter the proxy settings during the installation, or specify them in advance by using the procedure described below. To change the proxy settings after the installation, use the same procedure.

To specify the proxy settings in macOS

1. Create the file **/Library/Application Support/Acronis/Registry/Global.config** and open it in a text editor, such as Text Edit.
2. Copy and paste the following lines into the file

```
<?xml version="1.0" ?>
<registry name="Global">
  <key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"proxy.company.com"</value>
    <value name="Port" type="Tdword">"443"</value>
    <value name="Login" type="TString">"proxy_login"</value>
    <value name="Password" type="TString">"proxy_password"</value>
  </key>
</registry>
```

3. Replace proxy.company.com with your proxy server host name/IP address, and 443 with the decimal value of the port number.
4. If your proxy server requires authentication, replace proxy_login and proxy_password with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the file.
6. If the protection agent is not installed yet, you can install it now.
7. Open file **/Library/Application Support/Acronis/Agent/etc/aakore.yaml** in a text editor.
8. 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
```

9. Replace proxy_login and proxy_password with the proxy server credentials, and proxy_address:port with the address and port number of the proxy server.
10. Go to **Applications > Utilities > Terminal**
11. Restart the aakore service by using the following commands:

```
sudo launchctl stop aakore  
sudo launchctl start aakore
```

12. Restart the agent by using the following commands:

```
sudo launchctl stop acronis_mms  
sudo launchctl start acronis_mms
```

8.5.4 In bootable media

When working under bootable media, you may need to access the cloud storage via a proxy server. To specify the proxy server settings, click **Tools > Proxy server**, and then specify the proxy server host name/IP address, port, and credentials.

8.6 Installing Cyber Protection agents

You can install agents on machines running any of the operating systems listed in ["Supported operating systems and environments"](#). The operating systems that support the Cyber Protect features are listed in ["Supported Cyber Protect features by operating system"](#).

8.6.1 Downloading Cyber Protection agents

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

To download an agent while adding a workload to protect

1. In the Cyber Protection console, navigate to **Devices > All devices**.
2. In the upper right, click **Add device**.
3. In the **Add devices** panel, from the **Release channel** drop-down menu, select an agent version.
 - **Previous** - download the agent version from the previous release.
 - **Current** - download the latest available agent version.
4. Select the agent that corresponds to the operating system of the workload that you are adding. The **Save As** dialog opens.
5. [Only for Agent for mac OS (ARM)] Click **Cancel**. In the Add Mac panel that opens, click the **Download ARM installer** link.
6. 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 Protection console, click the **User** icon.
2. Click **Downloads**.
3. In the **Downloads** dialog, from the **Release channel** drop-down menu, select an agent version.
 - **Previous** - download the agent version from the previous release.
 - **Current** - download the latest available agent version.
4. 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.
5. Select a location to save the agent installation file and click **Save**.

8.6.2 Installing Cyber Protection agents in Windows

Prerequisites

Download the agent that you need on the machine that you plan to protect. See "Downloading Cyber Protection agents" (p. 54).

To install Agent for Windows

1. Ensure that the machine is connected to the Internet.
2. Log on as an administrator and start the installer.
3. [Optional] Click **Customize installation settings** and make the appropriate changes if you want:
 - To change the components to install (for example, to disable the installation of Cyber Protection Monitor or the Command-Line Tool, or to install the Agent for Antimalware protection and URL filtering).

Note

On Windows machines, the antimalware protection and URL filtering features require the installation of Agent for Antimalware protection and URL filtering. It will be installed automatically for protected workloads if the **Antivirus & Antimalware protection** or the **URL filtering module** is enabled in their protection plans.

- To change the method of registering the machine in the Cyber Protection service. You can switch from **Use service console** (default) to **Use credentials** or **Use registration token**.
 - To change the installation path.
 - To change the user account under which the agent service will run. For details, refer to ["Changing the logon account on Windows machines"](#).
 - To verify or change the proxy server host name/IP address, port, and credentials. If a proxy server is enabled in Windows, it is detected and used automatically.
4. Click **Install**.
 5. [Only when installing Agent for VMware] Specify the address and access credentials for the vCenter Server or stand-alone ESXi host whose virtual machines the agent will back up, and then click **Done**. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the [necessary privileges](#) on the vCenter Server or ESXi.

6. [Only when installing on a domain controller] Specify the user account under which the agent service will run, and then click **Done**. For security reasons, the setup program does not automatically create new accounts on a domain controller.
7. If you kept the default registration method **Use service console** in step 3, wait until the registration screen appears, and then proceed to the next step. Otherwise, no more actions are required.
8. Do one of the following:
 - Click **Register the machine**. In the opened browser window, sign in to the service console, review the registration details, and then click **Confirm registration**.
 - Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The registration code is valid for one hour.Alternatively, you can access the registration form by clicking **All devices > Add**, scrolling down to **Registration via code**, and then clicking **Register**.

Note

Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program and repeat the installation procedure.

As a result, the machine will be assigned to the account that was used to log in to the service console.

- Register the machine manually by using the command line. For more information on how to do this, refer to ["Registering machines manually"](#).
9. [If the agent is registered under an account whose tenant is in the Enhanced security mode] Set the encryption password.

8.6.3 Installing Cyber Protection agents in Linux

Prerequisites

- Download the agent that you need on the machine that you plan to protect. See "Downloading Cyber Protection agents" (p. 54).
- To install Agent for Linux, you need at least 2 GB of free disk space.

To install Agent for Linux

1. Ensure that the machine is connected to the Internet.
2. As the root user, run the installation file.

If a proxy server is enabled in your network, when running the file, specify the server host name/IP address and port in the following format: `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`.

If you want to change the default method of registering the machine in the Cyber Protection service, run the installation file with one of the following parameters:

- `--register-with-credentials` – to ask for a user name and password during the installation
 - `--token=STRING` – to use a registration token
 - `--skip-registration` – to skip the registration
3. Select the check boxes for the agents that you want to install. The following agents are available:
- **Agent for Linux**
 - **Agent for Virtuozzo**
 - **Agent for Oracle**
- Agent for Virtuozzo and Agent for Oracle require that Agent for Linux (64-bit) is also installed.
4. If you kept the default registration method in step 2, proceed to the next step. Otherwise, enter the user name and password for the Cyber Protection service, or wait until the machine will be registered by using the token.
5. Do one of the following:

- Click **Register the machine**. In the opened browser window, sign in to the service console, review the registration details, and then click **Confirm registration**.
- Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The registration code is valid for one hour.

Alternatively, you can access the registration form by clicking **All devices > Add**, scrolling down to **Registration via code**, and then clicking **Register**.

Note

Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program and repeat the installation procedure.

As a result, the machine will be assigned to the account that was used to log in to the service console.

- Register the machine manually by using the command line. For more information on how to do this, refer to "[Registering machines manually](#)".
6. [If the agent is registered under an account whose tenant is in the Enhanced security mode] Set the encryption password.
7. If the 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.

8. After the installation completes, do one of the following:

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

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

8.6.4 Installing Cyber Protection agents in macOS

Prerequisites

Download the agent that you need on the machine that you plan to protect. See "Downloading Cyber Protection agents" (p. 54).

To install Agent for Mac OS or Agent for Mac OS (ARM)

1. Ensure that the machine is connected to the Internet.
2. Double-click the installation file (.dmg).
3. Wait while the operating system mounts the installation disk image.
4. Double-click **Install**.
5. If a proxy server is enabled in your network, click **Protection Agent** in the menu bar, click **Proxy server settings**, and then specify the proxy server host name/IP address, port, and credentials.
6. If prompted, provide administrator credentials.
7. Click **Continue**.
8. Wait until the registration screen appears.
9. Do one of the following:
 - Click **Register the machine**. In the opened browser window, sign in to the service console, review the registration details, and then click **Confirm registration**.
 - Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The registration code is valid for one hour.

Alternatively, you can access the registration form by clicking **All devices > Add**, scrolling down to **Registration via code**, and then clicking **Register**.

Note

Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program and repeat the installation procedure.

As a result, the machine will be assigned to the account that was used to log in to the service console.

- Register the machine manually by using the command line. For more information on how to do this, refer to ["Registering machines manually"](#).

10. [If the agent is registered under an account whose tenant is in the Enhanced security mode] Set the encryption password.
11. If your macOS version is Mojave 10.14.x or later, grant full disk access to the protection agent to enable backup operations.
See <https://kb.acronis.com/content/62133> for instructions.

8.6.5 Changing the logon account on Windows machines

On the **Select components** screen, define the account under which the services will run by specifying **Logon account for the agent service**. You can select one of the following:

- **Use Service User Accounts** (default for the agent service)
Service User Accounts are Windows system accounts that are used to run services. The advantage of this setting is that the domain security policies do not affect these accounts' user rights. By default, the agent runs under the **Local System** account.
- **Create a new account**
The account name will be Agent User for the agent.
- **Use the following account**
If you install the agent on a domain controller, the system prompts you to specify existing accounts (or the same account) for the agent. For security reasons, the system does not automatically create new accounts on a domain controller.

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

Privileges required for the logon account

A protection agent is run as a Managed Machine Service (MMS) on a Windows machine. The account under which the agent will run must have specific rights for the agent to work correctly. Thus, the MMS user should be assigned the following privileges:

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

How to assign the user rights

Follow the instructions below to assign the user rights (this example uses the **Log on as service** user right, the steps are the same for other user rights):

1. Log on to the computer by using an account with administrative privileges.
2. Open **Administrative Tools** from **Control Panel** (or click Win+R, type **control admintools**, and press Enter) and open **Local Security Policy**.
3. Expand **Local Policies** and click on **User Rights Assignment**.
4. In the right pane, right-click **Log on as a service** and select **Properties**.
5. Click on the **Add User or Group...** button to add a new user.
6. In the **Select Users, Computers, Service Accounts, or Groups** window, find the user you wish to enter and click **OK**.
7. Click **OK** in the **Log on as a service Properties** to save the changes.

Important

Ensure that the user which you have added to the **Log on as service** user right is not listed in the **Deny log on as a service** policy in **Local Security Policy**.

Note that it is not recommended to change logon accounts manually after the installation is completed.

8.6.6 Dynamic installation and uninstallation of components

For Windows workloads protected by agent version 15.0.26986 (released in May 2021) or later, the following components are installed dynamically – that is, only when required by a protection plan:

- Agent for Antimalware protection and URL filtering – required for the operation of the antimalware protection and URL filtering features.
- Agent for Data Loss Prevention – required for the operation of the device control features.

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
- Device control

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

Dynamic installation or uninstallation of components takes up to 10 minutes after you change the protection plan. However, if any of the following operations are running, dynamic installation or uninstallation will start after this operation finishes:

- Backup
- Recovery

- Backup replication
- Virtual machine replication
- Testing a replica
- Running a virtual machine from backup (including finalization)
- Disaster recovery failover
- Disaster recovery failback
- Running a script (for Cyber Scripting functionality)
- Patch installation
- ESXi configuration backup

8.7 Unattended installation or uninstallation

8.7.1 Unattended installation or uninstallation in Windows

This section describes how to install or uninstall protection agents in the unattended mode on a machine running Windows, by using Windows Installer (the `msiexec` program). In an Active Directory domain, another way of performing unattended installation is through Group Policy—see ["Deploying agents through Group Policy"](#).

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

Creating the `.mst` transform and extracting the installation packages

1. Log on as an administrator and start the setup program.
2. Click **Create .mst and .msi files for unattended installation**.
3. In **What to install**, select the components that you want to install. The installation packages for these components will be extracted from the setup program.
4. In **Registration settings**, select **Use credentials** or **Use registration token**. For more information on how to generate a registration token, refer to ["Deploying agents through Group Policy"](#).
5. Review or modify other installation settings that will be added to the `.mst` file.
6. Click **Proceed**, and then select the folder where the `.mst` transform will be generated and the `.msi` and `.cab` installation packages will be extracted.
7. Click **Generate**.

Installing the product by using the `.mst` transform

On the command line, run the following command.

Command template:

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

Here:

- <package name> is the name of the .msi file.
- <transform name> is the name of the transform.

Command example:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

Installing or uninstalling the product by specifying parameters manually

On the command line, run the following command.

Command template (installing):

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

Here, <package name> is the name of the .msi file. All available parameters and their values are described in "[Unattended installation or uninstallation parameters](#)".

Command template (uninstalling):

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

The .msi package must be of the same version as the product that you want to uninstall.

Unattended installation or uninstallation parameters

This section describes parameters that are used during unattended installation or uninstallation in Windows. In addition to these parameters, you can use other parameters of msiexec, as described at [https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx).

Installation parameters

Basic parameters

ADDLOCAL=<list of components>

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

The full list of the components is as follows:

Component	Must be installed together with	Bitness	Component name / description
MmsMspComponents		32-bit/64-bit	Core components

			for agents
BackupAndRecoveryAgent	MmsMspComponents	32-bit/64-bit	Agent for Windows
AmpAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Antimalware and URL filtering
DlpAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Data Loss Prevention
ArxAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32-bit/64-bit	Agent for Microsoft 365
OracleAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Oracle
AcronisESXSupport	MmsMspComponents	64-bit	Agent for VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32-bit/64-bit	Agent for Hyper-V
CommandLineTool		32-bit/64-bit	Command-Line Tool
TrayMonitor	BackupAndRecoveryAgent	32-bit/64-bit	Cyber Protection Monitor
BackupAndRecoveryBootableComponents		32-bit/64-bit	Bootable Media Builder

TARGETDIR=<path>

The folder where the product will be installed. By default, this folder is: C:\Program Files\BackupClient.

REBOOT=ReallySuppress

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

/l*v <log file>

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

CURRENT_LANGUAGE=<language ID>

The product language. Available values are as follows: en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW.

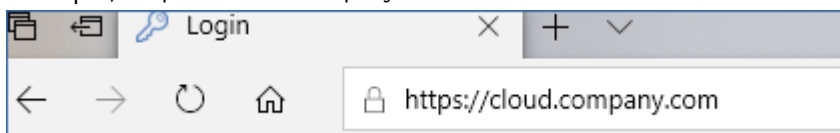
If this parameter is not specified, the product language will be defined by your system language on the condition that it is in the list above. Otherwise, the product language will set to English (en).

Registration parameters

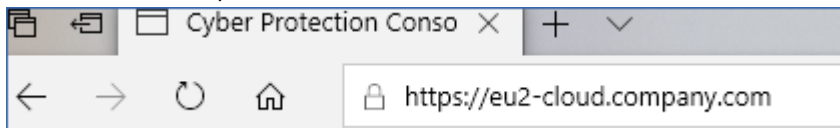
REGISTRATION_ADDRESS

This is the URL for the Cyber Protection service. You can use this parameter either with the REGISTRATION_LOGIN and REGISTRATION_PASSWORD parameters, or with the REGISTRATION_TOKEN one.

- When you use REGISTRATION_ADDRESS with REGISTRATION_LOGIN and REGISTRATION_PASSWORD parameters, specify the address that you use **to log in** to the Cyber Protection service. For example, <https://cloud.company.com>:



- When you use REGISTRATION_ADDRESS with the REGISTRATION_TOKEN parameter, specify the exact datacenter address. This is the URL that you see **once you are logged in** to the Cyber Protection service. For example, <https://eu2-ccloud.company.com>.



Do not use <https://cloud.company.com> here.

REGISTRATION_LOGIN and REGISTRATION_PASSWORD

Credentials for the account under which the agent will be registered in the Cyber Protection service. This cannot be a partner administrator account.

REGISTRATION_PASSWORD_ENCODED

Password for the account under which the agent will be registered in the Cyber Protection service, encoded in base64. For more information on how to encode your password, refer to ["Registering machines manually"](#).

REGISTRATION_TOKEN

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

REGISTRATION_REQUIRED={0,1}

Defines how the installation will finish if the registration fails. If the value is 1, the installation also fails. The default value is 0, so if you don't specify this parameter, the installation completes successfully even though the agent is not registered.

Additional parameters

To define the logon account for the agent service in Windows, use one of the following parameters:

- MMS_USE_SYSTEM_ACCOUNT={0,1}

If the value is 1, the agent will run under the **Local System** account.

- MMS_CREATE_NEW_ACCOUNT={0,1}

If the value is 1, the agent will run under a newly created account named **Acronis Agent User**.

- MMS_SERVICE_USERNAME=<user name> and MMS_SERVICE_PASSWORD=<password>

Use these parameters to specify an existing account under which the agent will run.

For more information on logon accounts, refer to ["Changing the logon account on Windows machines"](#).

SET_ESX_SERVER={0,1}

- If the value is 0, Agent for VMware being installed will not be connected to a vCenter Server or an ESXi host. If the value is 1, specify the following parameters:

- ESX_HOST=<host name>

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

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

Credentials to access the vCenter Server or ESXi host.

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

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

HTTP_PROXY_LOGIN=<login> and HTTP_PROXY_PASSWORD=<password>

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

HTTP_PROXY_ONLINE_BACKUP={0,1}

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

Uninstallation parameters

REMOVE={<list of components>|ALL}

The components to be removed, separated by commas and without space characters. If the value is ALL, all of the product components will be uninstalled.

Additionally, you can specify the following parameter:

DELETE_ALL_SETTINGS={0, 1}

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

ANTI_TAMPER_PASSWORD=<password>

The password required for uninstalling a password-protected Agent for Windows or modifying its components.

Examples

- Installing Agent for Windows, Agent for Antimalware and URL filtering, Command-Line Tool, and Cyber Protection Monitor. Registering the machine in the Cyber Protection service by using a user name and password.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
Monitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_
LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
```

- Installing Agent for Windows, Command-Line Tool, and Cyber Protection Monitor. Creating a new logon account for the agent service in Windows. Registering the machine in the Cyber Protection service by using a token.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Installing Agent for Windows, Command-Line Tool, Agent for Oracle and Cyber Protection Monitor. Registering the machine in the Cyber Protection service by using a user name and encoded in base64 password.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Installing Agent for Windows, Command-Line Tool, and Cyber Protection Monitor. Registering the machine in the Cyber Protection service by using a token. Setting an HTTP proxy.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
```

```
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com  
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

- Uninstalling all the agents and deleting their logs, tasks, and configuration settings.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_  
SETTINGS=1 REBOOT=ReallySuppress
```

8.7.2 Unattended installation or uninstallation in Linux

This section describes how to install or uninstall protection agents in the unattended mode on a machine running Linux, by using the command line.

To install or uninstall a protection agent

1. Open Terminal.
2. Do one of the following:
 - To start the installation by specifying the parameters on the command line, run the following command:

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

Here, <package name> is the name of the installation package (an .i686 or an .x86_64 file). All available parameters and their values are described in "[Unattended installation or uninstallation parameters](#)".

- To start the installation with parameters that are specified in a separate text file, run the following command:

```
<package name> -a --options-file=<path to the file>
```

This approach might be useful if you don't want to enter sensitive information on the command line. In this case, you can specify the configuration settings in a separate text file and ensure that only you can access it. Put each parameter on a new line, followed by the desired value, for example:

```
--rain=https://cloud.company.com  
--login=johndoe  
--password=johnspassword  
--auto
```

or

```
-C  
https://cloud.company.com  
-g  
johndoe  
-w  
johnspassword
```

```
-a
--language
en
```

If the same parameter is specified both on the command line and in the text file, the command line value precedes.

3. If UEFI Secure Boot is enabled on the machine, you are informed that you need to restart the system after the installation. Be sure to remember what password (that of the root user or "acronis") should be used. During the system restart, opt for MOK (Machine Owner Key) management, choose **Enroll MOK**, and then enroll the key by using the recommended password.

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

Unattended installation or uninstallation parameters

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

The minimal configuration for unattended installation includes -a and registration parameters (for example, --login and --password parameters; --rain and --token parameters). You can use more parameters to customize you installation.

Installation parameters

Basic parameters

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

The components to be installed, separated by commas and without space characters. The following components are available in the .x86_64 installation package:

Component	Component description
BackupAndRecoveryAgent	Agent for Linux
AgentForPCS	Agent for Virtuozzo
OracleAgentFeature	Agent for Oracle

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

Both Agent for Virtuozzo and Agent for Oracle require that Agent for Linux is also installed.

The .i686 installation package contains only BackupAndRecoveryAgent.

```
{-a|--auto}
```

The installation and registration process will complete without any further user interaction. When using this parameter, you must specify the account under which the agent will be registered

in the Cyber Protection service, either by using the `--token` parameter, or by using the `--login` and `--password` parameters.

`{-t|--strict}`

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

`{-n|--nodeps}`

The absence of required Linux packages will be ignored during the installation.

`{-d|--debug}`

Writes the installation log in the verbose mode.

`--options-file=<location>`

The installation parameters will be read from a text file instead of the command line.

`--language=<language ID>`

The product language. Available values are as follows: en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW.

If this parameter is not specified, the product language will be defined by your system language on the condition that it is in the list above. Otherwise, the product language will set to English (en).

Registration parameters

Specify one of the following parameters:

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

Credentials for the account under which the agent will be registered in the Cyber Protection service. This cannot be a partner administrator account.

- `--token=<token>`

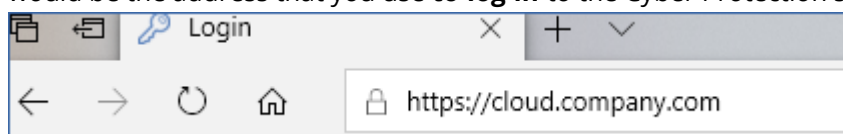
The registration token is a series of 12 characters, separated by hyphens in three segments. You can generate one in the service console, as described in ["Deploying agents through Group Policy"](#).

You cannot use the `--token` parameter along with `--login`, `--password`, and `--register-with-credentials` parameters.

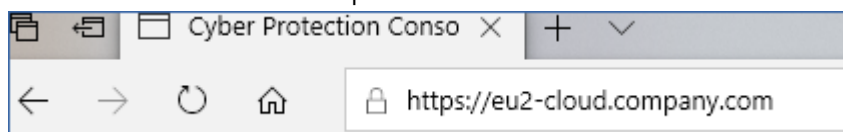
- `{-C|--rain=}<service address>`

The URL of the Cyber Protection service.

You don't need to include this parameter explicitly when you use `--login` and `--password` parameters for registration, because the installer uses the correct address by default – this would be the address that you use **to log in** to the Cyber Protection service. For example:



However, when you use `{-C|--rain=}` with the `--token` parameter, you must specify the exact datacenter address. This is the URL that you see **once you are logged in** to the Cyber Protection service. For example:



- `--register-with-credentials`

If this parameter is specified, the installer's graphical interface will start. To finish the registration, enter the user name and password for the account under which the agent will be registered in the Cyber Protection service. This cannot be a partner administrator account.

- `--skip-registration`

Use this parameter if you need to install the agent but you plan to register it in the Cyber Protection service later. For more information on how to do this, refer to "[Registering machines manually](#)".

Additional parameters

`--http-proxy-host=<IP address>` and `--http-proxy-port=<port>`

The HTTP proxy server that the agent will use for backup and recovery from the cloud, and for connection to the management server. Without these parameters, no proxy server will be used.

`--http-proxy-login=<login>` and `--http-proxy-password=<password>`

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

`--tmp-dir=<location>`

Specifies the folder where the temporary files are stored during the installation. The default folder is **`/var/tmp`**.

`{-s|--disable-native-shared}`

Redistributable libraries will be used during the installation, even though they might have already been present on your system.

`--skip-prereq-check`

There will be no check of whether the packages required for compiling the snapapi module are already installed.

`--force-weak-snapapi`

The installer will not compile a snapapi module. Instead, it will use a ready-made module that might not match the Linux kernel exactly. Using this option is not recommended.

`--skip-svc-start`

The services will not start automatically after the installation. Most often, this parameter is used with the `--skip-registration` one.

Information parameters

`{-?|--help}`

Shows the description of parameters.

`--usage`

Shows a brief description of the command usage.

`{-v|--version}`

Shows the installation package version.

`--product-info`

Shows the product name and the installation package version.

`--snapapi-list`

Shows the available ready-made snapapi modules.

`--components-list`

Shows the installer components.

Parameters for legacy features

These parameters relate to a legacy component, `agent.exe`.

`{-e|--ssl=}<path>`

Specifies the path to a custom certificate file for SSL communication.

`{-p|--port=}<port>`

Specifies the port on which `agent.exe` listens for connections. The default port is 9876.

Uninstallation parameters

`{-u|--uninstall}`

Uninstalls the product.

`--purge`

Uninstalls the product and removes its logs, tasks, and configuration settings. You don't need to specify the `--uninstall` parameter explicitly when you use the `--purge` one.

Examples

- Installing Agent for Linux without registering it.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- Installing Agent for Linux, Agent for Virtuozzo, and Agent for Oracle, and registering them by using credentials.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnpassword
```

- Installing Agent for Oracle and Agent for Linux, and registering them by using a registration token.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- Installing Agent for Linux, Agent for Virtuozzo, and Agent for Oracle with configuration settings in a separate text file.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- Uninstalling Agent for Linux, Agent for Virtuozzo, and Agent for Oracle, and removing all its logs, tasks, and configuration settings.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

8.7.3 Unattended installation and uninstallation in macOS

This section describes how to install, register, and uninstall the Cyber Protection agent in the unattended mode on a machine running macOS, by using the command line.

To download the installation file (.dmg)

- In the service console, go to **Devices > All devices**.
- Click **Add**, and then click **Mac**.

To install Agent for Mac

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

```
mkdir <dmg_root>
```

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

- Mount the .dmg file.

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

Here, <dmg_file> is the name of the installation file. For example, **Cyber_Protection_Agent_for_MAC_x64.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/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint  
mydirectory
```

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

```
hdiutil detach mydirectory
```

To register Agent for Mac

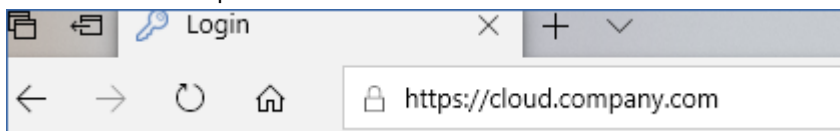
Do one of the following:

- Register the agent under a specific account, by using a user name and password.

```
sudo /Library/Application\  
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a <Cyber Protection  
service address> -t cloud -u <user name> -p <password> -o register
```

Here:

<Cyber Protection service address> is the address that you use **to log in** to the Cyber Protection service. For example:

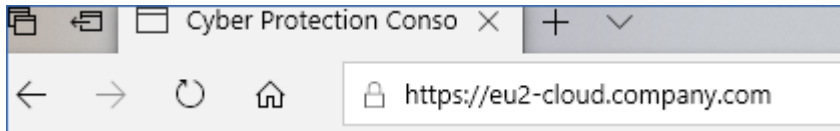


<user name> and <password> are the credentials for the account under which the agent will be registered. This cannot be a partner administrator account.

- Register the agent by using a registration token.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a <Cyber Protection
service address> -t cloud -o register --token <token>
```

The registration token is a series of 12 characters, separated by hyphens in three segments. You can generate one in the service console, as described in "[Deploying agents through Group Policy](#)". When you use a registration token, you must specify the exact datacenter address. This is the URL that you see **once you are logged in** to the Cyber Protection service. For example:



Examples

Registration with a user name and password.

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

Registration with a token.

- ```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a https://eu2-cloud
company.com -t cloud o -register --token D91D-DC46-4F0B
```

Important

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

To uninstall Agent for Mac

Run the following command:

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

To remove all logs, tasks and configuration settings during the uninstallation, run the following command:

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

8.8 Registering machines manually

In addition to registering a machine in the Cyber Protection service during the agent installation, you can also register it by using the command line interface. You might need to do so if you have installed the agent but the automatic registration failed, for example, or if you want to register an existing machine under a new account.

To register a machine

To register a machine by using a user name and password, run the following command.

In Windows

Command for registering a machine under the current account:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms -t cloud --update
```

Command template for registering a machine under another account:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a <service address> -u <user name> -p <password>
```

Command example:

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

In Linux

Command for registering a machine under the current account:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --update
```

Command template for registering a machine under another account:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service address> -u <user name> -p <password>
```

Command example:

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

In macOS

Command for registering a machine under the current account:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -s mms -t cloud --update
```

Command template for registering a machine under another account:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> -u <user name> -p <password>
```

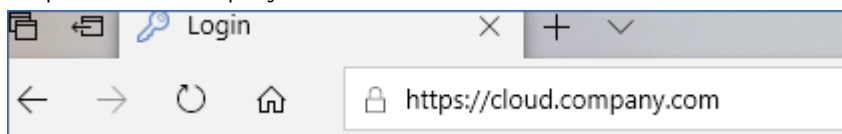
Command example:

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

Note

Use the user name and password for the specific account under which the agent will be registered. This cannot be a partner administrator account.

The service address is the URL that you use **to log in** to the Cyber Protection service. For example, <https://cloud.company.com>:



Alternatively, you can register a machine by using a registration token. To do so, run the following command.

In Windows

Command template:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> --token <token>
```

Command example:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

In Linux

Command template:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> --token <token>
```

Command example:


```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

In macOS

Command template:

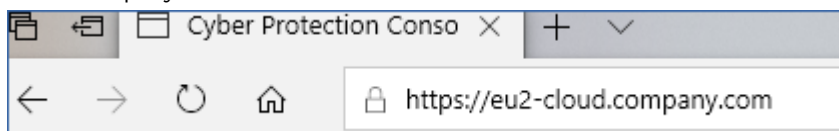
```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service address> --token <token>
```

Command example:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

Note

When you use a registration token, you must specify the exact datacenter address. This is the URL that you see **once you are logged in** to the Cyber Protection service. For example, https://eu2-cloud.company.com.



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

The registration token is a series of 12 characters, separated by hyphens in three segments. For more information on how to generate one, refer to ["Deploying agents through Group Policy"](#).

To unregister a machine

Run the following command:

In Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

In Linux

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

In macOS

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

8.8.1 Passwords with special characters or blank spaces

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

For example, in Windows, run this command.

Command template:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud  
-a <service address> -u <user name> -p "<password>"
```

Command example:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud  
-a https://cloud.company.com -u johndoe -p "johns password"
```

If you still receive an error:

- Encode your password into base64 format at <https://www.base64encode.org/>.
- On the command line, specify the encoded password by using the `-b` or `--base64` parameter.

For example, in Windows, run this command.

Command template:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud  
-a <service address> -u <user name> -b -p <encoded password>
```

Command example:

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

8.9 Autodiscovery of machines

The discovery of machines functionality allows you to do the following:

- Automate the process of protection agent installation and machine registration, by automatically detecting machines in your Active Directory (AD) domain or local network.
- Install and update the protection agent on a batch of machines.
- Use synchronization with Active Directory, to lower the efforts and overhead for resource provisioning and machine management in a large AD environment.

Important

Machine discovery can be performed only by the agents installed on Windows machines. Currently, not only Windows machines can be detected by the discovery agent but remote software installation is possible only on Windows machines.

If there is no machine with the installed agent, then the autodiscovery functionality will be hidden - the **Multiple devices** section will be hidden in the Add new device wizard.

After adding machines to the service console, they are categorized as follows:

- **Discovered** – machines that were discovered, but the protection agent is not installed on them.
- **Managed** – machines on which the protection agent is installed.
- **Unprotected** – machines to which the protection plan is not applied. Unprotected machines include both discovered and managed machines with no protection plan applied.
- **Protected** – machines to which the protection plan is applied.

8.9.1 How it works

During the local network scanning, the discovery agent uses the following technologies: NetBIOS discovery, Web Service Discovery (WSD), and the Address Resolution Protocol (ARP) table. The agent tries to get the following parameters of each machine:

- Name (short/NetBIOS hostname)
- FQDN
- Domain/workgroup
- IPv4/IPv6 addresses
- MAC addresses
- Operating system (name/version/family)
- Machine category (workstation/server/domain controller)

When AD scanning is performed, the agent tries to get almost the same parameters of each machines as listed above. The difference is that it will additionally get the Organizational Unit (OU) parameter, more full information about the name and operating system, and it won't get IP address and MAC address information.

8.9.2 Prerequisites

Before discovering machines, you must install the protection agent on at least one machine in your local network to use it as a discovery agent.

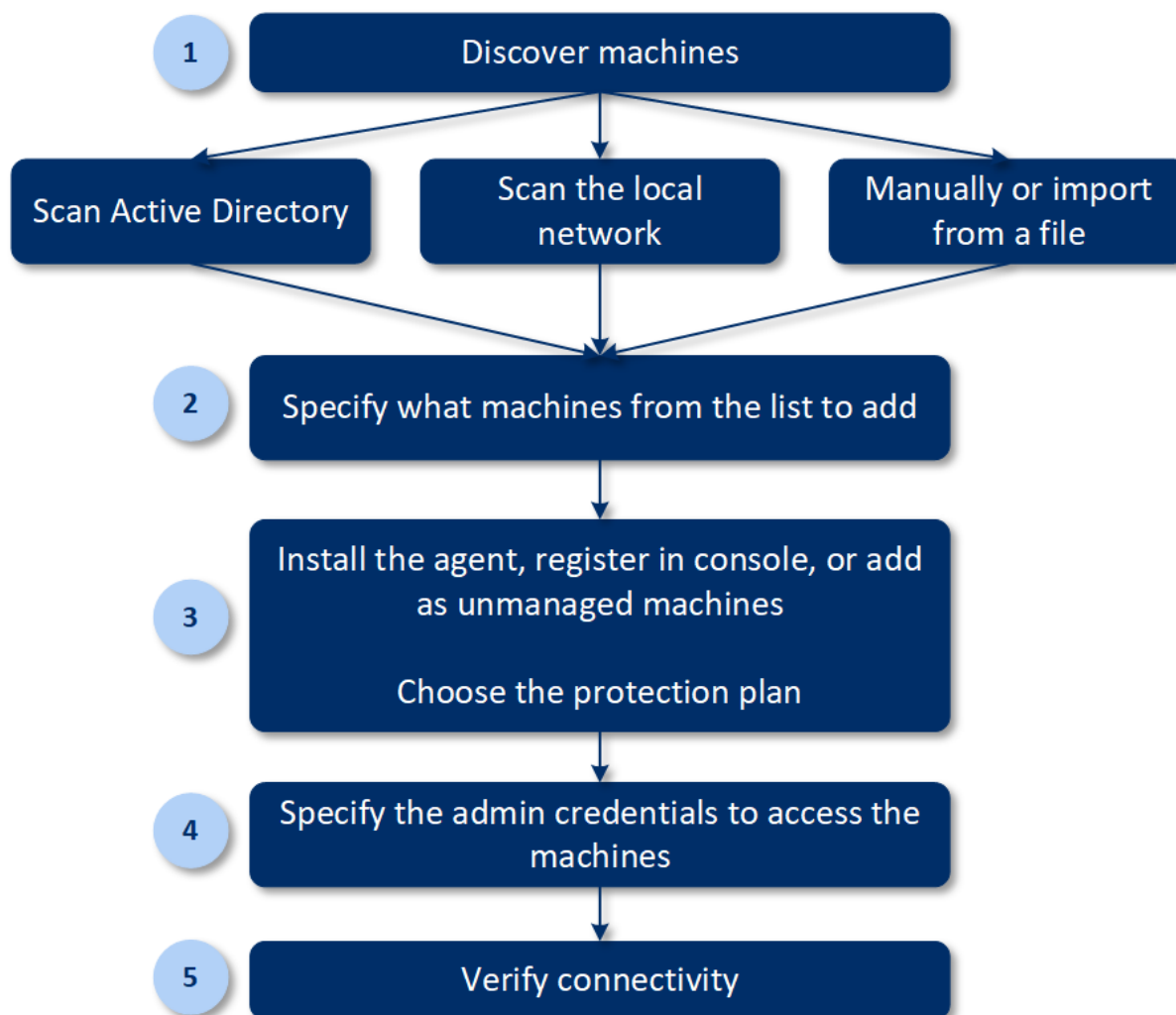
If you are planning to discover machines in the Active Directory domain, you must install the agent on at least one machine in the AD domain. This agent will be used as a discovery agent during scanning of AD.

Note

Agent for Windows cannot be installed on a remote machine running Windows XP.
To install Agent for Windows on a machine running Windows Server 2012 R2, you must have Windows update [KB2999226](#) installed on this machine.

8.9.3 Machine discovery process

In the following scheme, you can see the main steps of the machine discovery process:



Generally, the whole autodiscovery process consists of the following steps:

1. Select the method of machine discovery:
 - By scanning Active Directory
 - By scanning the local network
 - Manual – adding a machine by IP address or hostname, or importing a list of machines from a file

The first two methods filter results automatically to exclude machines that have agents installed.

The manual method performs upgrade and re-registration for the existing agents. When you run autodiscovery by using the same account, it means that the agent will just be updated to the latest version if necessary. If you use another account, the agent will be updated and re-registered under the tenant to which the account belongs.

2. Select machines to be added from the list received as a result of the previous step.
3. Select how the machines will be added:
 - The protection agent and additional components will be installed on the machines, and they will also be registered in the service console.
 - The machines will be registered in the service console (if they already have the installed agent).
 - The machines will be added as **Unmanaged machines** to the service console, without any agent or component installation.

If you selected one of the first two methods to add a machine, you can also select the protection plan from the existing ones and apply to machines.

4. Provide the credentials of the user who has the administrator rights for managing the machines.
5. Verify connectivity to machines by using the provided credentials.

In the next topics, you will get more detailed information about the discovery procedure.

8.9.4 Autodiscovery and manual discovery

Before starting the discovery, ensure that the [prerequisites](#) are met.

To discover machines

1. In the service console, go to **Devices > All devices**.
2. Click **Add**.
3. In **Multiple devices**, click **Windows-only**. The discovery wizard opens.
4. [If there are units in your organization] Select a unit. Then, in **Discovery agent** you will be able to select the agents associated with the selected unit and its child units.
5. Select the discovery agent that will perform the scan to detect machines.
6. Select the discovery method:
 - **Search Active Directory**. Ensure that the machine with the discovery agent is the Active Directory domain member.
 - **Scan local network**. If the selected discovery agent could not find any machines, select another discovery agent.
 - **Specify manually or import from file**. Manually define the machines to be added or import them from a text file.
7. [If the Active Directory discovery method is selected] Select how to search for machines:
 - **In organizational unit list**. Select the group of machines to be added.
 - **By LDAP dialect query**. Use the [LDAP dialect](#) query to select the machines. **Search base** defines where to search, while **Filter** allows you to specify the criteria for machine selection.

8. [If the Active Directory or local network discovery method is selected] Use a list to select the machines that you want to add.

[If the Manual discovery method is selected] Specify the machine IP addresses or hostnames, or import the machine list from a text file. The file must contain IP addresses/hostnames, one per line. Here is an example of a file:

```
156.85.34.10
156.85.53.32
156.85.53.12
EN-L00000100
EN-L00000101
```

After adding machine addresses manually or importing from a file, the agent tries to ping the added machines and define their availability.

9. Select what actions must be performed after the discovery:

- **Install agents and register machines.** You can select which components to install on the machines by clicking **Select components**. For more details, refer to "Selecting components for installation" (p. 85).

On the **Select components** screen, define the account under which the services will run by specifying **Logon account for the agent service**. You can select one of the following:

- **Use Service User Accounts** (default for the agent service)

Service User Accounts are Windows system accounts that are used to run services. The advantage of this setting is that the domain security policies do not affect these accounts' user rights. By default, the agent runs under the **Local System** account.

- **Create a new account**

The account name will be Agent User for the agent.

- **Use the following account**

If you install the agent on a domain controller, the system prompts you to specify existing accounts (or the same account) for the agent. For security reasons, the system does not automatically create new accounts on a domain controller.

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

- **Register machines with installed agents.** This option is used if the agent is already installed on machines and you need only to register them in Cyber Protection. If no agent is found inside the machines, then they will be added as **Unmanaged** machines.
- **Add as unmanaged machines.** The agent will not be installed on the machines. You will be able to view them in the console and install or register the agent later.

[If the **Install agents and register machines** post-discovery action is selected] **Restart the machine if required** – if the option is enabled, the machine will be restarted as many times as required to complete the installation.

Restart of the machine may be required in one of the following cases:

- Installation of prerequisites is completed and restart is required to continue the installation
- Installation is completed but restart is required as some files are locked during installation
- Installation is completed but restart is required for other previously installed software

[If **Restart the machine if required** is selected] **Do not restart if the user logged in** – if the option is enabled, the machine will not be automatically restarted if the user is logged in to the system. For example, if a user is working while installation requires restart, the system will not be restarted.

If the prerequisites were installed and then the reboot was not done because a user was logged in, then to complete the agent installation you need to reboot the machine and start the installation again.

If the agent was installed but then the reboot was not done, then you need to reboot the machine.

[If there are units in your organization] **User for whom to register the machines** – select the user of your unit or subordinate units for whom the machines will be registered.

If you have selected one of the first two post-discovery actions, then there is also an option to apply the protection plan to the machines. If you have several protection plans, you can select which one to use.

10. Specify the credentials of the user with administrator rights for all of the machines.

Important

Note that remote installation of agent works without any preparations only if you specify the credentials of the built-in administrator account (the first account created when the operating system is installed). If you want to define some custom administrator credentials, then you should do additional manual preparations as described in "Enabling remote installation of an agent for a custom administrator" below.

11. The system checks connectivity to all of the machines. If the connection to some of the machines fails, you can change the credentials for these machines.

When the discovery of machines is initiated, you will find the corresponding task in **Dashboard > Activities > Discovering machines** activity.

Preparing a machine for remote installation

1. For successful installation on a remote machine running Windows Vista or later, the option **Control panel > Folder options > View > Use Sharing Wizard** must be *disabled* on that machine.
2. For successful installation on a remote machine that is *not* a member of an Active Directory domain, User Account Control (UAC) must be *disabled* on that machine. For more information on how to disable it, refer to "[Requirements on User Account Control \(UAC\)](#)" > To disable UAC.
3. By default, the credentials of the built-in administrator account are required for remote installation on any Windows machine. To perform remote installation by using the credentials of another administrator account, User Account Control (UAC) remote restrictions must be *disabled*.

For more information on how to disable them, refer to "[Requirements on User Account Control \(UAC\)](#)" > To disable UAC remote restrictions.

4. 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 Vista, Windows Server 2008, Windows 7, or later: go to **Control panel > Windows Firewall > Network and Sharing Center > Change advanced sharing settings**.
5. Cyber Protection uses TCP ports 445, 25001, and 43234 for remote installation.

Port 445 is automatically opened when you enable File and Printer Sharing. Ports 43234 and 25001 are automatically opened through Windows Firewall. If you use a different firewall, make sure that these three ports are open (added to exceptions) for both incoming and outgoing requests.

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

Requirements on User Account Control (UAC)

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

To disable UAC

Do one of the following depending on the operating system:

- **In a Windows operating system prior to Windows 8:**

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

To disable UAC remote restrictions

1. Open Registry Editor.
2. Locate the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. For **LocalAccountTokenFilterPolicy** value, change the setting to **1**.

If the **LocalAccountTokenFilterPolicy** value does not exist, create it as DWORD (32-bit). For more information about this value, refer to the Microsoft documentation:

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

Note

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

Selecting components for installation

You can find the description of mandatory and additional components in the following table:

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	
Agent for Data Loss Prevention	This agent enables you to limit the user access to local and redirected peripheral devices, ports, and clipboard on machines under protection plans. It will be installed if selected.
Antimalware and URL filtering	This component enables the Antivirus & Antimalware protection module 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 and will be installed on Hyper-V hosts. It will be installed if selected and detected Hyper-V role on a machine.
Agent for SQL	This agent backs up SQL Server databases and will be installed on machines running Microsoft SQL Server. It will be installed if selected and application detected on a machine.
Agent for Exchange	This agent backs up Exchange databases and mailboxes and will be installed on machines running the Mailbox role of Microsoft Exchange Server. I will be installed if selected and application detected on a machine.
Agent for Active Directory	This agent backs up the data of Active Directory Domain Services and will be installed on domain controllers. It will be installed if selected and application detected on a machine.
Agent for VMware (Windows)	This agent backs up VMware virtual machines and will be installed on Windows machines that have network access to vCenter Server. It will be installed if selected.

Agent for Microsoft 365	This agent backs up Microsoft 365 mailboxes to a local destination and will be installed on Windows machines. It will be installed if selected.
Agent for Oracle	This agent backs up Oracle databases and will be installed on machines running Oracle Database. It will be installed if selected.
Cyber Protection Monitor	This component enables a user to monitor execution of running tasks in the notification area and will be installed on Windows machines. It will be installed if selected. Supported on Windows 7 Service Pack 1 and later, and Windows Server 2008 R2 Service Pack 1 and later.
Command-line tool	Cyber Protection 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 Protection components - agents and the management server. It will be installed if selected.

8.9.5 Managing discovered machines

After the discovery process is performed, you can find all of the discovered machines in **Devices > Unmanaged machines**.

This section is divided into subsections by the discovery method used. The full list of machine parameters is shown below (it may vary depending on the discovery method):

Name	Description
Name	The name of the machine. The IP address will be shown if the name of the machine could not be discovered.
IP address	The IP address of the machine.
Discovery type	The discovery method that was used to detect the machine.
Organizational unit	The organizational unit in Active Directory that the machine belongs to. This column is shown if you view the list of machines in Unmanaged machines > Active Directory .
Operating system	The operating system installed in the machine.

There is an **Exceptions** section, where you can add the machines that must be skipped during the discovery process. For example, if you do not need the exact machines to be discovered, you can add them to this list.

To add a machine to **Exceptions**, select it in the list and click **Add to exceptions**. To remove a machine from **Exceptions**, go to **Unmanaged machines > Exceptions**, select the machine, and click **Remove from exceptions**.

You can install the protection agent and register a batch of discovered machines in Cyber Protection by selecting them in the list and clicking **Install and register**. The opened wizard also allows you to assign the protection plan to a batch of machines.

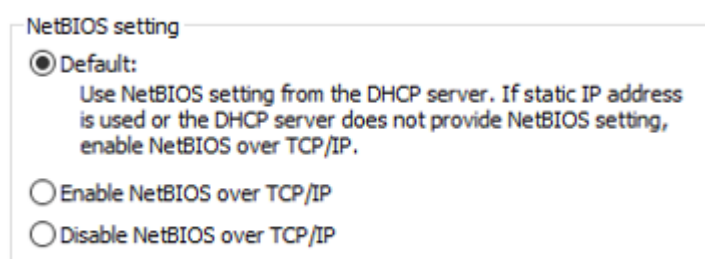
After the protection agent is installed on machines, those machines will be shown in the **Devices > Machines with agents** section.

To check your protection status, go to **Dashboard > Overview** and add the **Protection status** widget or the **Discovered machine** widget.

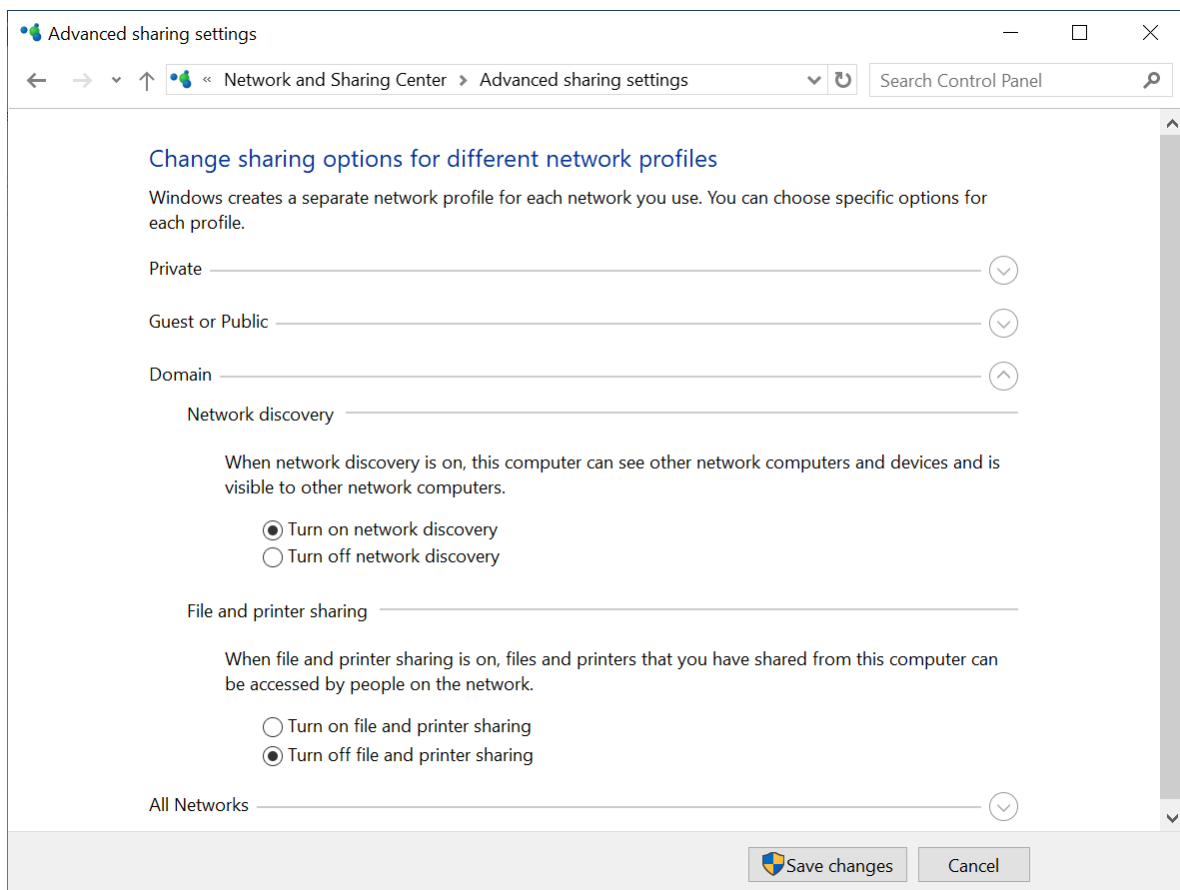
8.9.6 Troubleshooting

If you have any issues with the autodiscovery functionality, try to check the following:

- Check that 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 that the Function Discovery Provider Host service is running on the machine that does discovery and on the machines to be discovered.
- Check that the Function Discovery Resource Publication service is running on the machines to be discovered.

8.10 Deploying Agent for VMware (Virtual Appliance)

8.10.1 Before you start

System requirements for the agent

By default, the virtual appliance is assigned 4 GB of RAM and 2 vCPUs, which is optimal and sufficient for most operations. We recommend increasing these resources to 8 GB of RAM and 4 vCPUs if the backup traffic bandwidth is expected to exceed 100 MB per second (for example, in 10-Gbit networks), in order to improve backup performance.

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

How many agents do I need?

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

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

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

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**.

8.10.2 Deploying the OVF template

1. Click **All devices > Add > VMware ESXi > Virtual Appliance (OVF)**.
The .zip archive is downloaded to your machine.
2. Unpack the .zip archive. The folder contains one .ovf file and two .vmdk files.
3. Ensure that these files can be accessed from the machine running the vSphere Client.
4. Start the vSphere Client and log on to the vCenter Server.
5. 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, be sure to select a network that allows an Internet connection, so that the agent can properly register itself in the cloud.

8.10.3 Configuring the virtual appliance

1. Starting the virtual appliance

In the vSphere Client, display the **Inventory**, right-click the virtual appliance's name, and then select **Power > Power On**. Select the **Console** tab.

2. Proxy server

If a proxy server is enabled in your network:

- a. To start the command shell, press CTRL+SHIFT+F2 while in the virtual appliance UI.
- b. Open the file **/etc/Acronis/Global.config** in a text editor.

c. Do one of the following:

- If the proxy settings were specified during the agent installation, find the following section:

```
<key name="HttpProxy">
  <value name="Enabled" type="Tdwor" >"1"</value>
  <value name="Host" type="TString">"ADDRESS"</value>
  <value name="Port" type="Tdwor" >"PORT"</value>
  <value name="Login" type="TString">"LOGIN"</value>
  <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Otherwise, copy the above lines and paste them into the file between the <registry name="Global">...</registry> tags.

- d. Replace ADDRESS with the new proxy server host name/IP address, and PORT with the decimal value of the port number.
- e. If your proxy server requires authentication, replace LOGIN and PASSWORD with the proxy server credentials. Otherwise, delete these lines from the file.
- f. Save the file.
- g. Open the file **/opt/acronis/etc/aakore.yaml** in a text editor.
- h. Locate the **env** section or create it and add the following lines:

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

- i. Replace proxy_login and proxy_password with the proxy server credentials, and proxy_address:port with the address and port number of the proxy server.

j. Run the reboot command.

Otherwise, skip this step.

3. Network settings

The agent's network connection is configured automatically by using Dynamic Host Configuration Protocol (DHCP). To change the default configuration, under **Agent options**, in **eth0**, click **Change** and specify the desired network settings.

4. vCenter/ESX(i)

Under **Agent options**, in **vCenter/ESX(i)**, click **Change** and specify the vCenter Server name or IP address. The agent will be able to back up and recover any virtual machine managed by the vCenter Server.

If you do not use a vCenter Server, specify the name or IP address of the ESXi host whose virtual machines you want to back up and recover. Normally, backups run faster when the agent backs up virtual machines hosted on its own host.

Specify the credentials that the agent will use to connect to the vCenter Server or ESXi. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the [necessary privileges](#) on the vCenter Server or ESXi.

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

5. Management server

- a. Under **Agent options**, in **Management Server**, click **Change**.
- b. In **Server name/IP**, select **Cloud**. The software displays the Cyber Protection service address. Do not change this address unless instructed otherwise.
- c. In **User name** and **Password**, specify the user name and password for the Cyber Protection service. The agent and the virtual machines managed by the agent will be registered under this account.

6. Time zone

Under **Virtual machine**, in **Time zone**, click **Change**. Select the time zone of your location to ensure that the scheduled operations run at the appropriate time.

7. [Optional] Local storages

You can attach an additional disk to the virtual appliance so the Agent for VMware can back up to this locally attached storage.

Add the disk by editing the settings of the virtual machine and click **Refresh**. The **Create storage** link becomes available. Click this link, select the disk, and then specify a label for it.

8.11 Deploying Agent for Scale Computing HC3 (Virtual Appliance)

8.11.1 Before you start

This appliance is a pre-configured virtual machine that you deploy in a Scale Computing HC3 cluster. It contains a protection agent that enables you to administer cyber protection for all virtual machines in the cluster.

System requirements for the agent

By default, the virtual machine with the agent uses 2 vCPUs and 4 GiB of RAM. These settings are sufficient for most operations but you can change them by editing the virtual machine in the Scale Computing HC3 web interface. 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 size of the appliance virtual disk is about 9 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 a similar number of machines.

Automatic redistribution occurs when the load imbalance among the agents reaches 20 percent. This may happen after you add or remove a machine or an agent. 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 redistributed 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 Protection service console.

To check which agent manages a specific machine

1. In the Cyber Protection service console, click **Devices**, and then select **Scale Computing**.
2. Click the gear icon in the upper right corner of the table, and under **System**, select the **Agent** check box.
3. Check the name of the agent in the column that appears.

8.11.2 Deploying the QCOW2 template

1. Log in to your Cyber Protection account.
2. Click **Devices > All devices > Add > Scale Computing HC3**.
The .zip archive is downloaded to your machine.
3. Unpack the .zip archive, and then save the .qcow2 file and the .xml file to a folder named **ScaleAppliance**.
4. Upload the **ScaleAppliance** folder to a network share and ensure that the Scale Computing HC3 cluster can access it.
5. Log in to the Scale Computing HC3 cluster as an administrator who has the **VM Create/Edit** role assigned. For more information about the roles required for operations with Scale Computing HC3 virtual machines, refer to "Agent for Scale Computing HC3 – required roles" (p. 94).
6. In the Scale Computing HC3 web interface, import the virtual machine template from the **ScaleAppliance** folder.
 - a. Click the **Import HC3 VM** icon.
 - b. In the **Import HC3 VM** window, specify the following:
 - A name for the new virtual machine.
 - The network share on which the **ScaleAppliance** folder is located.
 - The user name and password required for accessing this network share.
 - [Optional] A domain tag for the new virtual machine.
 - The path to the **ScaleAppliance** folder on the network share.
 - c. Click **Import**.

After the deployment completes, you must configure the virtual appliance. For more information on how to configure it, refer to "Configuring the virtual appliance" (p. 93).

Note

If you need more than one virtual appliance in your cluster, repeat the steps above and deploy additional virtual appliances. Do not clone an existing virtual appliance by using the **Clone VM** option in the Scale Computing HC3 web interface.

8.11.3 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 Protection service.

To configure the virtual appliance

1. Log in to your Scale Computing HC3 account.
2. Select the appliance virtual machine that you need 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 **Scale Computing** field, click **Change** to specify the Scale Computing HC3 cluster address and credentials for accessing it:
 - a. In the **Server name/IP** field, enter the DNS name or IP address of the cluster.
 - b. In the **User name** and **Password** fields, enter the credentials for the Scale Computing HC3 administrator account.
Ensure that this account has the roles required for operations with Scale Computing HC3 virtual machines. For more information about these roles, refer to "Agent for Scale Computing HC3 – required roles" (p. 94).
 - c. [Optional] Click **Check connection** to ensure that the provided credentials are correct.
 - d. Click **OK**.
5. In the **Management Server** field, click **Change** to specify the Cyber Protection service address and credentials for accessing it.
 - a. In the **Server name/IP** field, select **Cloud**, and then specify the Cyber Protection service address.
 - b. In the **User name** and **Password** fields, enter the credentials for your account in the Cyber Protection service.
 - c. Click **OK**.
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 Protection service 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.

To protect virtual machines in the Scale Computing HC3 cluster

1. Log in to your Cyber Protection 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.

8.11.4 Agent for Scale Computing HC3 – required roles

This section describes the roles required for operations with Scale Computing HC3 virtual machines.

Operation	Role
Back up a virtual machine	Backup VM Create/Edit
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

8.12 Deploying Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance)

8.12.1 Before you start

This appliance is a pre-configured virtual machine that you deploy in Virtuozzo Hybrid Infrastructure. It contains a protection agent that enables you to administer cyber protection for all virtual machines in a Virtuozzo Hybrid Infrastructure cluster.

Note

To ensure that backups with enabled **Volume Shadow Copy Service (VSS) for virtual machines** backup option run properly and capture data in application-consistent state, verify that Virtuozzo Guest Tools are installed and up-to-date on the protected virtual machines.

System requirements for the agent

When deploying the virtual appliance, you can choose between different predefined combinations of vCPUs and RAM (flavors). You can also create your own flavors.

2 vCPUs and 4 GB of RAM (medium flavor) are optimal and sufficient for most operations. We recommend increasing these resources to 4 vCPUs and 8 GB 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.

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 a similar number of machines.

Automatic redistribution occurs when the load imbalance among the agents reaches 20 percent. This may happen after you add or remove a machine or an agent. 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 redistributed among the remaining agents. However, this will not happen if an agent gets corrupted or is deleted manually from the Virtuozzo Hybrid Infrastructure node. Redistribution will start only after you remove such an agent from the Cyber Protection web interface.

To check which agent manages a specific machine

1. In the Cyber Protection service console, click **Devices**, and then select **Virtuozzo Hybrid Infrastructure**.
2. Click the gear icon in the upper right corner of the table, and under **System**, select the **Agent** check box.
3. Check the name of the agent in the column that appears.

Limitations

- Virtuozzo Hybrid Infrastructure appliance cannot be deployed remotely.
- Application-aware backup of virtual machines is not supported.

8.12.2 Configuring networks in Virtuozzo Hybrid Infrastructure

Before deploying and configuring the virtual appliance, you need to have your networks in Virtuozzo Hybrid Infrastructure configured.

Network requirements for the Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance)

- The virtual appliance requires 2 network adapters.
- The virtual appliance must be connected to Virtuozzo networks with the following network traffic types:
 - Compute API
 - VM Backup
 - ABGW Public
 - VM Public

For more information about configuring the networks, see [Requirements for the compute cluster](#) in the Virtuozzo documentation.

8.12.3 Configuring user accounts in Virtuozzo Hybrid Infrastructure

To configure the virtual appliance, you need a Virtuozzo Hybrid Infrastructure user account. This account must have the **Administrator** role in the **Default** domain. For more information about users, refer to [Managing domain users](#) in the Virtuozzo Hybrid Infrastructure documentation. Ensure that you granted this account access to all projects in the **Default** domain.

To grant access to all projects in the Default domain

1. Create an environment file for the system administrator. To do this, run the following script in the Virtuozzo Hybrid Infrastructure cluster via the OpenStack Command-Line Interface. For more information on how to connect to this interface, refer to [Connecting to OpenStack command-line interface](#) in the Virtuozzo Hybrid Infrastructure documentation.

```
su - vstoradmin
kolla-ansible post-deploy
exit
```

2. Use the environment file to authorize further OpenStack commands:

```
. /etc/kolla/admin-openrc.sh
```

3. Run the following commands:

```
openstack --insecure user set --project admin --project-domain Default --domain Default <username>
openstack --insecure role add --domain Default --user <username> --user-domain Default compute --inherited
```

Here, <username> is the Virtuozzo Hybrid Infrastructure account with the **Administrator** role in the **Default** domain. The virtual appliance will use this account in order to back up and restore the virtual machines in any child project under the **Default** domain.

Example

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

To manage backups for virtual machines in a domain that is different from the **Default** domain, run the following command as well.

To grant access to all projects in a different domain

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

Here, <domain name> is the domain to the projects in which the <username> account will have access.

Example

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

After granting access to projects, check what roles are assigned to the account.

To check assigned roles

```
openstack --insecure role assignment list --user <username> --names
```

Here, <username> is the Virtuozzo Hybrid Infrastructure account.

Example

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+-----+-----+-----+-----+
| Role      | User              | Project | Domain    |
+-----+-----+-----+-----+
| admin     | johndoe@Default  |         | MyNewDomain |
| compute   | johndoe@Default  |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+-----+-----+-----+-----+
```

In this example, the options `-c Role`, `-c User`, `-c Project`, and `-c Domain` are used to abridge the command output to fit the page.

To check what effective roles are assigned to the account in all projects, run the following command as well.

To check effective roles in all projects

```
openstack --insecure role assignment list --user <username> --names --effective
```

Here, `<username>` is the Virtuozzo Hybrid Infrastructure account.

Example

```
openstack --insecure role assignment list --user johndoe --names --effective -c Role -c
User -c Project -c Domain
```

Role	User	Project	Domain
domain_admin	johndoe@Default		Default
compute	johndoe@Default	admin@Default	
compute	johndoe@Default	service@Default	
domain_admin	johndoe@Default	admin@Default	
domain_admin	johndoe@Default	service@Default	
project_user	johndoe@Default	service@Default	
member	johndoe@Default	service@Default	
reader	johndoe@Default	service@Default	
project_user	johndoe@Default	admin@Default	
member	johndoe@Default	admin@Default	
reader	johndoe@Default	admin@Default	
project_user	johndoe@Default		Default
member	johndoe@Default		Default
reader	johndoe@Default		Default

In this example, the options `-c Role`, `-c User`, `-c Project`, and `-c Domain` are used to abridge the command output to fit the page.

8.12.4 Deploying the QCOW2 template

1. Log in to your Cyber Protection account.
2. Click **Devices > All devices > Add > Virtuozzo Hybrid Infrastructure**.
The .zip archive is downloaded to your machine.
3. Unpack the .zip archive. It contains a .qcow2 image file.
4. Log in to your Virtuozzo Hybrid Infrastructure account.
5. Add the .qcow2 image file to the Virtuozzo Hybrid Infrastructure compute cluster as follows:
 - On the **Compute > Virtual machines > Images** tab, click **Add image**.
 - In the **Add image** window, click **Browse**, and then select the .qcow2 file.

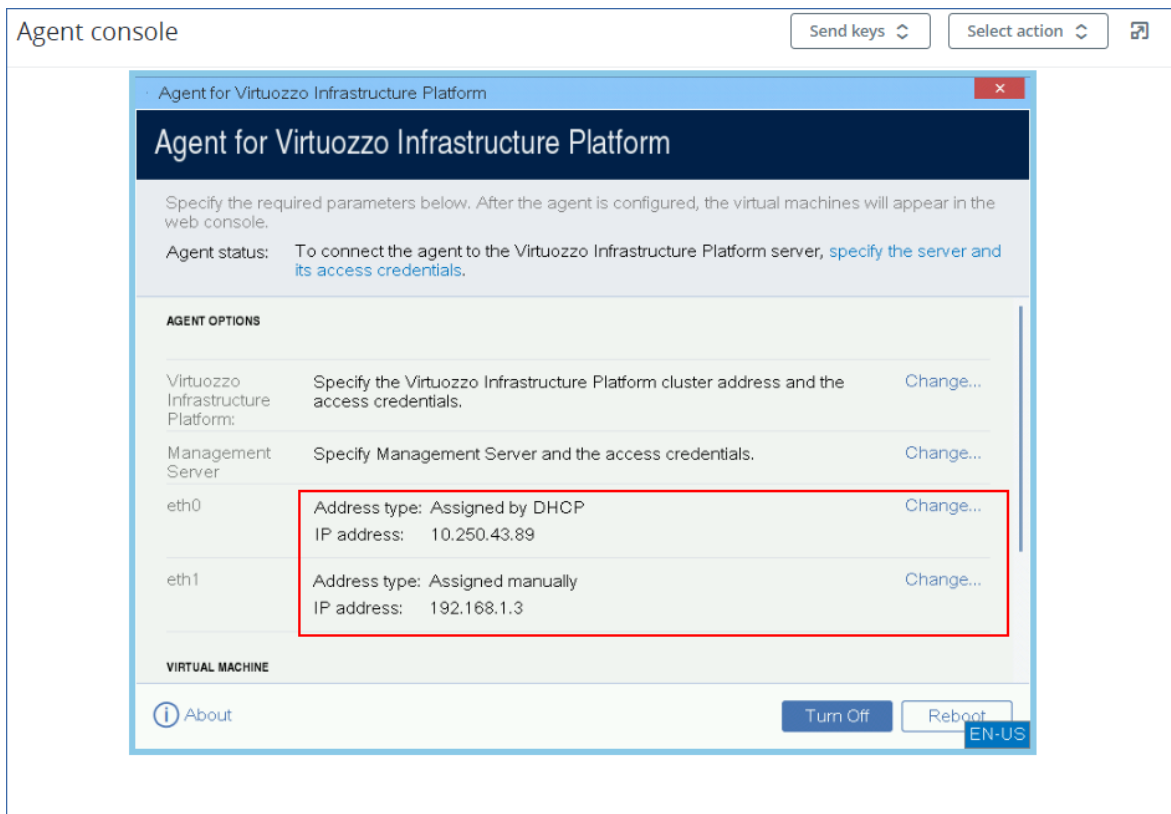
- Specify the image name, select the **Generic Linux OS** type, and then click **Add**.
6. In the **Compute > Virtual machines > Virtual machines** tab, click **Create virtual machine**. A window will open where you need to specify the following parameters:
 - A name for the new virtual machine.
 - In **Deploy from**, choose **Image**.
 - In the **Images** window, select the .qcow2 image file of the appliance, and then click **Done**.
 - In the **Volumes** window, you don't need to add any volumes. The volume that is added automatically for the system disk is sufficient.
 - In the **Flavor** window, choose your desired combination of vCPUs and RAM, and then click **Done**. Usually, 2 vCPUs and 4 GiB of RAM are enough.
 - In the **Network interfaces** window, click **Add**, select the virtual network of type *public*, and then click **Add**. It will appear in the **Network interfaces** list.
If you use a setup with more than one physical network (and thus, with more than one virtual network of type public), repeat this step and select the virtual networks that you need.
 7. Click **Done**.
 8. Back in the **Create virtual machine** window, click **Deploy** to create and boot the virtual machine.

8.12.5 Configuring the virtual appliance

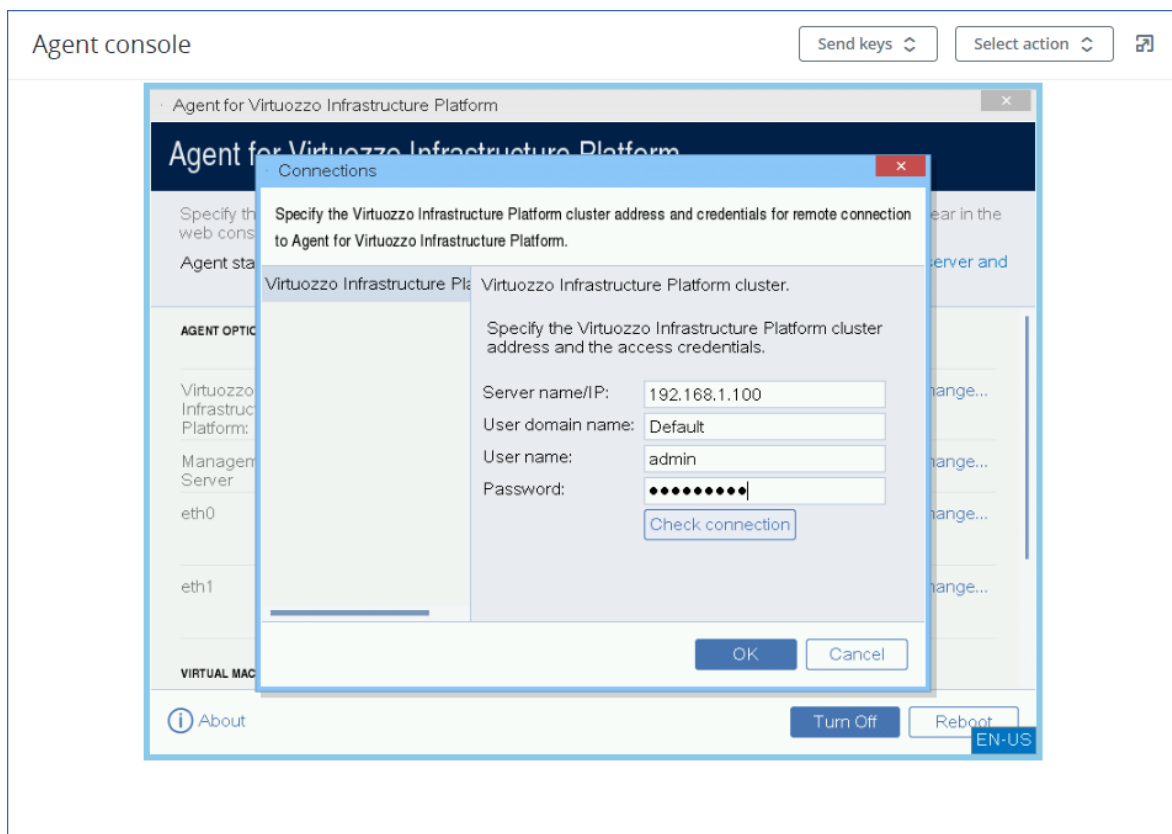
After deploying the virtual appliance, you need to configure it so that it can reach both the Virtuozzo Hybrid Infrastructure cluster that it will protect and the Cyber Protection cloud service.

To configure the virtual appliance

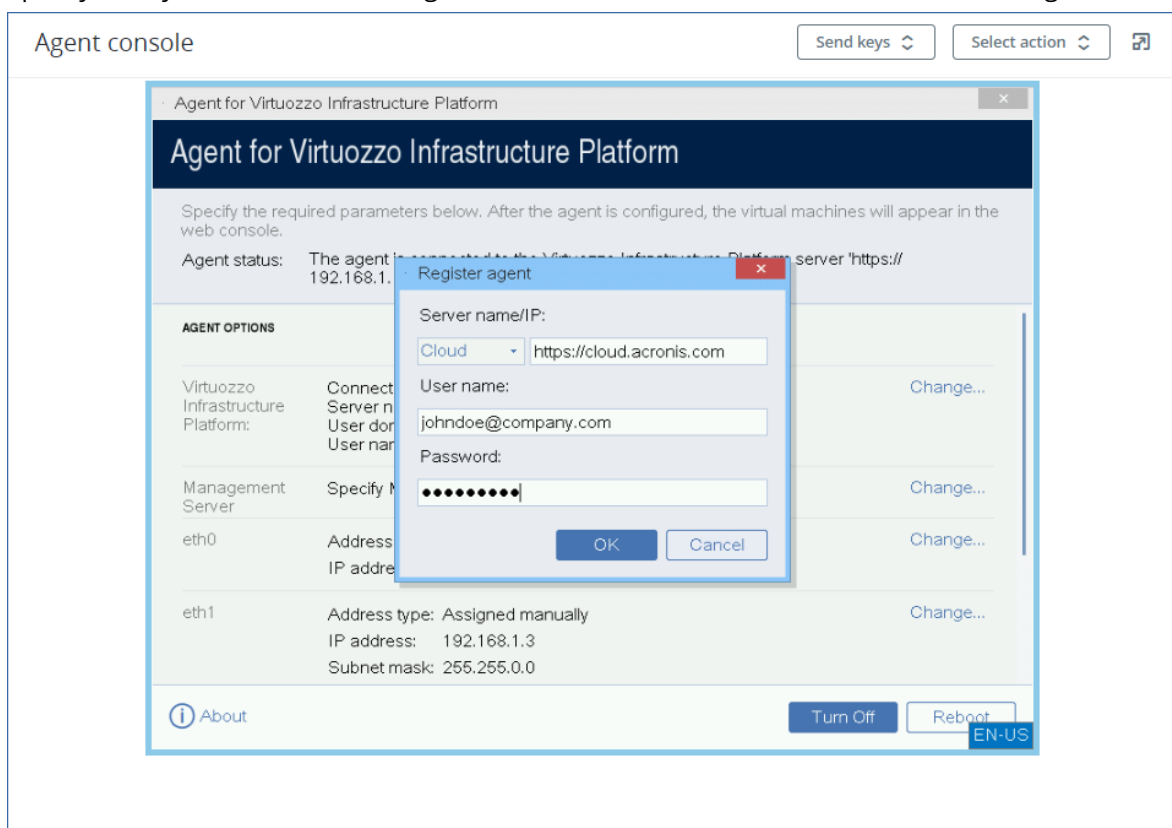
1. Log in to your Virtuozzo Hybrid Infrastructure account.
2. On the **Compute > Virtual machines > Virtual Machines** tab, select the virtual machine that you created. Then, click **Console**.
3. Configure the network interfaces of the appliance. There may be one or more interfaces to configure – it depends on the number of virtual 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 Virtuozzo cluster address and credentials:
 - DNS name or IP address of the Virtuozzo Hybrid Infrastructure cluster – this is the address of the management node of the cluster. The default port 5000 will be automatically set. If you use a different port, you need to specify it manually.
 - In the **User domain name** field, specify your domain in Virtuozzo Hybrid Infrastructure. For example, **Default**.
The domain name is case-sensitive.
 - In the **User name** and **Password** fields, enter the credentials for Virtuozzo Hybrid Infrastructure user account with **Administrator** role in the specified domain. For more information about users, roles, and domains, refer to [Configuring user accounts in Virtuozzo Hybrid Infrastructure](#).

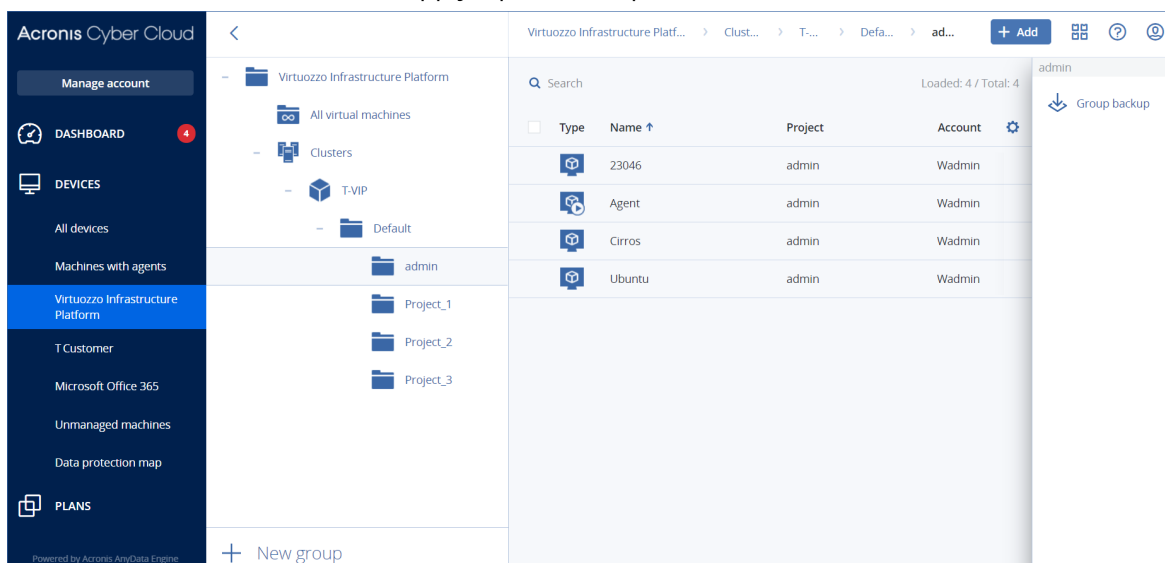


- Specify the Cyber Protection management server address and credentials for accessing it.



To protect the virtual machines in the Virtuozzo Hybrid Infrastructure cluster

1. Log in to your Cyber Protection account.
2. Navigate to **Devices** > **Virtuozzo Hybrid Infrastructure** > <your cluster> > **Default project** > **admin** or find your machines in **Devices** > **All devices**.
3. Select the desired machines and apply a protection plan for them.



8.13 Deploying Agent for oVirt (Virtual Appliance)

8.13.1 Before you start

This appliance is a pre-configured virtual machine that you deploy in a Red Hat Virtualization/oVirt data center. The appliance contains a protection agent that enables you to administer cyber protection for all virtual machines in the data center.

System requirements for the agent

By default, the virtual machine with the agent uses 2 vCPUs and 4 GiB of RAM. These settings are sufficient for most operations but you can edit them in Red Hat Virtualization/oVirt Administration Portal. 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 size of the appliance virtual disk is 8 GiB.

How many agents do I need?

One agent can protect the entire data center. However, you can have more than one agent in the data center if you need to distribute the backup traffic bandwidth load.

If you have more than one agent in the data center, the virtual machines are automatically distributed between the agents, so that each agent manages a similar number of machines.

Automatic redistribution occurs when the load imbalance among the agents reaches 20 percent. This may happen after you add or remove a machine or an agent. For example, you realize that you need more agents to help with throughput and you deploy an additional virtual appliance to the data center. The management server will assign the most appropriate machines to the new agent. The old agents' load will reduce. When you remove an agent, the machines assigned to the agent are redistributed among the remaining agents. However, this will not happen if an agent gets corrupted or is deleted manually from Red Hat Virtualization/oVirt Administration Portal. Redistribution will start only after you remove such an agent from the Cyber Protection service console.

To check which agent manages a specific machine


1. In the Cyber Protection service 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** check box.
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:

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

8.13.2 Deploying the OVA template

1. Log in to your Cyber Protection account.
2. Click **Devices > All devices > Add > Red Hat Virtualization (oVirt)**.
The .zip archive is downloaded to your machine.
3. Unpack the .zip archive. It contains one .ova file.
4. Upload the .ova file to a host in the Red Hat Virtualization/oVirt data center 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, refer to "Agent for oVirt – required roles and ports" (p. 105).
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:

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

The deployment is now complete. Next, you have to configure the virtual appliance. For more information on how to configure it, refer to "Configuring the virtual appliance" (p. 104).

Note

If you need more than one virtual appliance in your data center, repeat the steps above and 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 exclude the virtual appliance from dynamic group backups, you must also exclude it from the list of virtual machines in the Cyber Protection service console. To exclude it, in Red Hat Virtualization/oVirt Administration Portal, select the virtual machine with the agent, and then assign the tag `acronis_virtual_appliance` to it.

8.13.3 Configuring the virtual appliance

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

To configure the virtual appliance

1. Log in to Red Hat Virtualization/oVirt Administration Portal.
2. Select the virtual machine with the agent that you need 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 – required roles and ports" (p. 105).

- c. [Optional] Click **Check connection** to ensure that the provided credentials are correct.
- d. Click **OK**.
5. In the **Management Server** field, click **Change** to specify the Cyber Protection service address and credentials for accessing it.
 - a. In the **Server name/IP** field, select **Cloud**, and then specify the Cyber Protection service address.
 - b. In the **User name** and **Password** fields, enter the credentials for your account in the Cyber Protection service.
 - c. Click **OK**.
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 Protection service 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.

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

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

8.13.4 Agent for oVirt – 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

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4

- 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
<code>https://ovirt.company.com/</code>	443	HTTPS
<code>http://ovirt.company.com/</code>	80	HTTP
<code>https://ovirt.company.com:1234/</code>	1234	HTTPS

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

8.14 Deploying agents through Group Policy

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

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

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

8.14.1 Prerequisites

Before proceeding with agent deployment, ensure that:

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

8.14.2 Step 1: Generating a registration token

A registration token passes the identity of an user to the agent setup program without storing the user credentials for the service console. This enables users to register any number of machines under their account without having to log in. For security reasons, tokens have limited lifetime that you can adjust. The default period is 3 days.

To generate a registration token for your account

1. Sign in to the service console.
2. Click **Devices > All devices > Add**.
3. Scroll down to **Registration token**, and then click **Generate**.
4. Specify the token lifetime.
5. [Optional] To enable the user of the token to apply and revoke a protection plan on the added machines, select the plan from the drop-down list.
6. Click **Generate token**.
7. Copy the token or write it down.
Be sure to save the token if you need it for further use.

You can click **Manage active tokens** to view and delete the tokens that are generated for your account.

Note

For security reasons, the Active Tokens table does not display full token values.

To generate a registration token on behalf of a user in the tenants that you can manage

1. Sign in to the service console as a Partner or Customer administrator.
If you are already signed in to the management console, on the **Cyber Protection** tab, click **Manage service** to navigate to the service console.
2. From the drop-down list in the upper left, select the tenant that contains the user on whose behalf you want to create a token.
3. Under **Devices**, click **All devices > Add**.
The Add devices dialog opens on the right.
4. Scroll down to **Registration token**, and then click **Generate**.
5. Specify the token lifetime.
6. Select the user for whom you want to generate a token.
7. [Optional] To enable the user of the token to apply and revoke a protection plan on the added machines, select the plan from the drop-down list.
8. Click **Generate token**.
9. Copy the token or write it down.
Be sure to save the token if you need it for further use.

You can click **Manage active tokens** to view and delete the tokens that are generated for users that you can manage.

Note

For security reasons, the Active Tokens table does not display full token values.

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

1. Log on as an administrator on any machine in the domain.
2. Create a shared folder that will contain the installation packages. Ensure that domain users can access the shared folder—for example, by leaving the default sharing settings for **Everyone**.
3. Start the setup program.
4. Click **Create .mst and .msi files for unattended installation**.
5. Click **Specify** next to **Registration settings**, and then enter the token you generated.
You can change the method of registering the machine in the Cyber Protection service from **Use registration token** (default) to **Use credentials** or **Skip registration**. The **Skip registration** option presumes that you will register the machine at a later time.
6. Review or modify the installation settings that will be added to the .mst file, and then click **Proceed**.
7. In **Save the files to**, specify the path to the folder you created.
8. Click **Generate**.

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

8.14.4 Step 3: Setting up the Group Policy objects

1. Log on to the domain controller as a domain administrator; if the domain has more than one domain controller, log on to any of them as a domain administrator.
2. If you are planning to deploy the agent in an organizational unit, ensure that the organizational unit exists in the domain. Otherwise, skip this step.
3. In the **Start** menu, point to **Administrative Tools**, and then click **Active Directory Users and Computers** (in Windows Server 2003) or **Group Policy Management** (in Windows Server 2008 or later).
4. In Windows Server 2003:
 - Right-click the name of the domain or organizational unit, and then click **Properties**. In the dialog box, click the **Group Policy** tab, and then click **New**.In Windows Server 2008 or later:
 - Right-click the name of the domain or organizational unit, and then click **Create a GPO in this domain, and Link it here**.
5. Name the new Group Policy object **Agent for Windows**.
6. Open the **Agent for Windows** Group Policy object for editing, as follows:
 - In Windows Server 2003, click the Group Policy object, and then click **Edit**.
 - In Windows Server 2008 or later, under **Group Policy Objects**, right-click the Group Policy object, and then click **Edit**.
7. In the Group Policy object editor snap-in, expand **Computer Configuration**.

8. In Windows Server 2003 and Windows Server 2008:
 - Expand **Software Settings**.In Windows Server 2012 or later:
 - Expand **Policies > Software Settings**.
9. Right-click **Software installation**, then point to **New**, and then click **Package**.
10. Select the agent's .msi installation package in the shared folder that you previously created, and then click **Open**.
11. In the **Deploy Software** dialog box, click **Advanced**, and then click **OK**.
12. On the **Modifications** tab, click **Add**, and then select the .mst transform that you previously created.
13. Click **OK** to close the **Deploy Software** dialog box.

8.15 Updating agents

You can update all agents manually.

You can configure automatic updates for the following agents:

- Agent for Windows
- Agent for Linux
- Agent for Mac

8.15.1 Updating agents manually

You can update agents either by using the service console or by downloading and running the installation file.

Virtual appliances with the following versions must be updated only by using the service console:

- Agent for VMware (Virtual Appliance): version 12.5.23094 and later.
- Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance): version 12.5.23094 and later.

Agents with the following versions can also be updated by using the service console:

- Agent for Windows, Agent for VMware (Windows), Agent for Hyper-V: version 11.9.191 and later.
- Agent for Linux: version 11.9.179 and later.
- Other agents: any version can be updated.

To find the agent version, in the service console, select the machine, and then click **Details**.

To update earlier agent versions of those agents, download and install the newest version manually.

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

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>.

To update an agent by using the service console

1. Click **Settings > Agents**.
The software displays the list of machines. The machines with outdated agent versions are marked with an orange exclamation mark.
2. Select the machines that you want to update the agents on. The machines must be online.
3. Click **Update agent**.

Note

During the update, any backups that are in progress will fail.

To update Agent for VMware (Virtual Appliance) whose version is below 12.5.23094

1. Click **Settings > Agents > the agent that you want to update > Details**, and then examine the **Assigned virtual machines** section. You will need to re-enter these settings after the update.
 - a. Make note of the position of the **Automatic assignment** switch.
 - b. To find out what virtual machines are manually assigned to the agent, click the **Assigned:** link.
The software displays the list of assigned virtual machines. Make note of the machines that have (M) after the agent name in the **Agent** column.
2. Remove Agent for VMware (Virtual Appliance), as described in "[Uninstalling agents](#)". In step 5, delete the agent from **Settings > Agents**, even though you are planning to install the agent again.
3. Deploy Agent for VMware (Virtual Appliance), as described in "[Deploying the OVF template](#)".
4. Configure Agent for VMware (Virtual Appliance), as described in "[Configuring the virtual appliance](#)".
If you want to reconstruct the locally attached storage, in step 7 do the following:
 - a. Add the disk containing the local storage to the virtual appliance.
 - b. Click **Refresh > Create storage > Mount**.
 - c. The software displays the original **Letter** and **Label** of the disk. Do not change them.
 - d. Click **OK**.
5. Click **Settings > Agents > the agent that you want to update > Details**, and then reconstruct the settings that you made note of in step 1. If some virtual machines were manually assigned to the agent, assign them again as described in "[Virtual machine binding](#)".
Once the agent configuration is completed, the protection plans that were applied to the old agent are re-applied automatically to the new agent.
6. The plans with application-aware backup enabled require the guest OS credentials to be re-entered. Edit these plans and re-enter the credentials.
7. The plans that back up ESXi configuration require the "root" password to be re-entered. Edit these plans and re-enter the password.

To update the Cyber Protection definitions on a machine

1. Click **Settings > Agents**.
2. Select the machine on which you want to update the Cyber Protection definitions and click **Update definitions**. The machine must be online.

To assign the Updater role to an agent

1. Click **Settings > Agents**.
2. Select the machine to which you want to assign the [Updater role](#), click **Details**, then in the **Cyber Protection definitions** section, enable **Use this agent to download and distribute patches and updates**.

To clear cached data on an agent

1. Click **Settings > Agents**.
2. Select the machine on which you want to clear the cached data (outdated update files and patch management data) and click **Clear cache**.

8.15.2 Updating agents automatically

To facilitate management of multiple workloads, you can configure automatic updates for Agent for Windows, Agent for Linux, and Agent for Mac. Automatic updates are available for agents version 15.0.26986 (released in May 2021) or later. Older agents must be updated manually to the latest version, first.

Automatic updates are supported on machines running any of the following operating systems:

- Windows XP SP 3 and later
- Red Hat Enterprise Linux 6 and later, CentOS 6 and later
- OS X 10.9 Mavericks and later

The settings for automatic updates are preconfigured on a data center level. A company administrator can customize these settings – for all machines in a company or a unit, or for individual machines. If no custom settings are applied, then the settings from the upper level are used, in this order:

1. Cyber Protection data center
2. Company (customer tenant)
3. Unit
4. Machine

For example, a unit administrator can configure custom auto-update settings for all machines in the unit, which might differ from the setting applied to the machines on the company level. The administrator can also configure different settings for one or more individual machines in the unit, to which neither the unit settings nor the company settings will be applied.

After enabling the automatic updates, you can configure the following options:

- **Update channel**

The update channel defines which version of the agents will be used – the most up-to-date one or the latest version from the previous release.

- **Maintenance window**

The maintenance window defines when updates can be installed. If the maintenance window is disabled, updates can run anytime.

Even within the enabled maintenance window, updates will not be installed while the agent is running any of the following operations:

- Backup
- Recovery
- Backup replication
- Virtual machine replication
- Testing a replica
- Running a virtual machine from backup (including finalization)
- Disaster recovery failover
- Disaster recovery failback
- Running a script (for Cyber Scripting functionality)
- Patch installation
- ESXi configuration backup

To customize auto-update settings

1. In the service console, go to **Settings > Agents**.
2. Select the scope for the settings:
 - To change the settings for all machines, click **Edit default agent update settings**.
 - To change the settings for specific machines, select the desired machines, and then click **Agent update settings**.
3. Configure the settings according to your needs, and then click **Apply**.

To remove the custom auto-update settings

1. In the service console, go to **Settings > Agents**.
2. Select the scope for the settings:
 - To remove the custom settings for all machines, click **Edit default agent update settings**.
 - To remove the custom settings for specific machines, select the desired machines, and then click **Agent update settings**.
3. Click **Reset to default settings**, and then click **Apply**.

To check the auto-update status

1. In the service console, go to **Settings > Agents**.
2. Click the gear icon in the upper right corner of the table, and then ensure that **Auto-update** check box is selected.
3. Check the status that is shown in the **Auto-update** column.

8.16 Preventing unauthorized uninstallation or modification of agents

You can protect Agent for Windows against unauthorized uninstallation or modification, by enabling the **Password protection** setting in a protection plan. This setting is available only when the **Self-protection** setting is enabled.

To enable Password protection

1. In a protection plan, expand the **Antivirus & Antimalware protection** module (**Active Protection** module for Cyber Backup editions).
2. Click **Self-protection** and ensure that the **Self-protection** switch is enabled.
3. Enable the **Password protection** switch.
4. In the window that opens, copy the password that you need to uninstall or modify the components of a protected Agent for Windows.
This password is unique and you will not be able to recover it once you close this window. If you lose or forget this password, you can edit the protection plan and create a new password.
5. Click **Close**.
6. In the **Self-protection** pane, click **Done**.
7. Save the protection plan.

Password protection will be enabled for the machines to which this protection plan is applied.

Password protection is only available for Agent for Windows version <VERSION 20.11> or newer. The machines must be online.

You can apply a protection plan with Password protection enabled to a machine running macOS, but no protection will be provided. You cannot apply such a plan to a machine running Linux.

Also, you cannot apply more than one protection plan with Password protection enabled to the same Windows machine. To learn how to resolve a possible conflict, refer to [Resolving plan conflicts](#).

To change the password in an existing protection plan

1. In the protection plan, expand the **Antivirus & Antimalware protection** module (**Active Protection** module for Cyber Backup edition).
2. Click **Self-protection**.
3. Click **Create new password**.
4. In the window that opens, copy the password that you need to uninstall or modify the components of a protected Agent for Windows.
This password is unique and you will not be able to recover it once you close this window. If you lose or forget this password, you can edit the protection plan and create a new password.
5. Click **Close**.

6. In the **Self-protection** pane, click **Done**.
7. Save the protection plan.

8.17 Uninstalling agents

8.17.1 In Windows

If you want to remove individual product components (for example, one of the agents or Cyber Protection Monitor), run the **All agents for Windows** setup program, choose to modify the product, and clear the selection of the components that you want to remove. The link to the setup program is 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.

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 Protection Agent > Uninstall**.
3. [For password-protected agent] Specify the password that you need to uninstall the agent, and then click **Next**.
4. [Optional] Select the **Remove the logs and configuration settings** check box.
If you are planning to install the agent again, keep this check box cleared. If you select the check box, the machine may be duplicated in the service console and the backups of the old machine may not be associated with the new machine.
5. Click **Uninstall**.

8.17.2 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.
If you are planning to install the agent again, keep this check box cleared. If you select the check box, the machine may be duplicated in the service console and the backups of the old machine may not be associated with the new machine.
3. Confirm your decision.

8.17.3 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.

8.17.4 Removing Agent for VMware (Virtual Appliance)

1. Start the vSphere Client and log on to the vCenter Server.
2. If the virtual appliance (VA) is powered on, right-click it, and then click **Power > Power Off**. Confirm your decision.
3. If the 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.
5. [Optional] If you are planning to install the agent again, skip this step. Otherwise, in the service console, click **Backup storage > Locations**, and then delete the location corresponding to the locally attached storage.

8.17.5 Removing machines from the service console

After uninstalling an agent, it will be unregistered from the Cyber Protection service, and the machine where the agent was installed will be automatically removed from the service console.

However, if during this operation the connection to the service is lost – due to a network problem, for example – the agent might be uninstalled but its machine might still be shown in the service console. In this case, you need to remove the machine from the service console manually.

To remove a machine from the service console manually

1. Log in to the Cyber Protection service as an administrator.
2. In the service console, go to **Settings > Agents**.
3. Select the machine where the agent was installed.
4. Click **Delete**.

8.18 Security settings

To configure the general protection settings for Cyber Protection, go to **Settings > Protection** in the service console.

8.18.1 Automatic updates for components

By default, all agents can connect to the Internet and download updates.

An administrator can minimize the network bandwidth traffic by selecting one or several 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.

To prepare a machine for the Updater role

1. On agent machine where you plan to enable the Updater role, 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 a protection agent

1. In the service console, go to **Settings > Agents**.
2. Select the machine 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.

The peer-to-peer update works as follows.

1. The agent with the Updater role checks by schedule the index file provided by the service provider to update the core components.
2. The agent with the Updater role starts to download and distribute updates to all agents.

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 the source for definition updates.

8.18.2 Updating the Cyber Protection definitions by schedule

On the **Schedule** tab, you can set up the schedule for automatic update of the Cyber Protection definitions for each of the following components:

- Antimalware
- Vulnerability assessment
- Patch management

To change the definition updates setting, navigate to **Settings > Protection > Protection definitions update > Schedule**.

Schedule type:

- **Daily** – define on which days of a week to update definitions.
Start at – you can select at what time to update definitions.
- **Hourly** – define more granular hourly schedule for definition updates.
Run every – define the periodicity for running definition updates.
From ... To – define a specific time range within which the automatic definition updates will be performed.

8.18.3 Updating the Cyber Protection definitions on-demand

To update Cyber Protection Definitions for a particular machine on-demand

1. In the service console, go to **Settings > Agents**.
2. Select the machines on which you want to update the Cyber Protection definitions and click **Update definitions**.

8.18.4 Cache storage

Location of cached data:

- On Windows machines: C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache
- On Linux machines: /opt/acronis/var/atp-downloader/Cache
- On MacOS machines: /Library/Application Support/Acronis/Agent/var/atp-downloader/Cache

To change the cache storage setting, navigate to **Settings > Protection > Protection definitions update > Cache Storage**

In **Outdated update files and patch management data**, specify after what period to remove cached data.

Maximum cache storage size (GB) for agents:

- **Updater role** – define storage size for cache on the machines with the Updater role.
- **Other roles** – define storage size for cache on other machines.

8.18.5 Remote connection

Click **Remote desktop connection**, to enable the remote connection to machines via RDP client or HTML5 client. If it is disabled, then the **Connect via RDP client / Connect via HTML5 client** options will be hidden in the service console, and users will not be able to connect to machines remotely. This option affects all users of your organization.

Click **Share remote desktop connection**, to enable sharing the remote connection with users. As a result, the new option **Share remote connection** will appear in the right menu when you select a machine, and you will be able to generate a link to be shared with users for accessing the remote machine.

8.19 Changing the service quota of machines

The service quota is automatically assigned when a protection plan is applied to a machine for the first time.

You can manually change the original assignment later. For example, to apply a more advanced protection plan to the same machine, you might need to upgrade the machine's service quota. If the features required by this protection plan are not supported by the currently assigned service quota, the protection plan will fail. Alternatively, you can change the service quota if you purchase more appropriate quotas after the original one is assigned. For example, a **Workstations** quota is assigned to a virtual machine. After you purchase a **Virtual machines** quota, you can manually assign it to this machine. You can also release the currently assigned service quota, and then assign it to another machine.

You can change the service quota of an individual machine or for a group of machines.

To change the service quota of an individual machine

1. In the Cyber Protection service console, go to **Devices**.
2. Select the desired machine, and then click **Details**.
3. In the **Service quota** section, click **Change**.
4. In the **Change license** window, select the desired service quota or **No quota**, and then click **Change**.

To change the service quota for a group of machines

1. In the Cyber Protection service console, go to **Devices**.
2. Select more than one machine, and then click **Assign quota**.
3. In the **Change license** window, select the desired service quota or **No quota**, and then click **Change**.

8.20 Cyber Protection services installed in your environment

Cyber Protection installs some or all of the following services, depending on the Cyber Protection options that you use.

8.20.1 Services installed in Windows

Service name	Purpose
Acronis Managed Machine Service	Provides backup, recovery, replication, retention, validation functionality
Acronis Scheduler2 Service	Executes scheduled tasks on certain events

Acronis Active Protection Service	Provides protection against ransomware
Acronis Cyber Protection Service	Provides antimalware protection

8.20.2 Services installed in macOS

Service name and location	Purpose
/Library/LaunchDaemons/com.acronis.aakore.plist	Serves for communication between the agent and management components
/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist	Provides detection of malware
/Library/LaunchDaemons/com.acronis.mms.plist	Provides backup and recovery functionality
/Library/LaunchDaemons/com.acronis.schedule.plist	Executes scheduled tasks

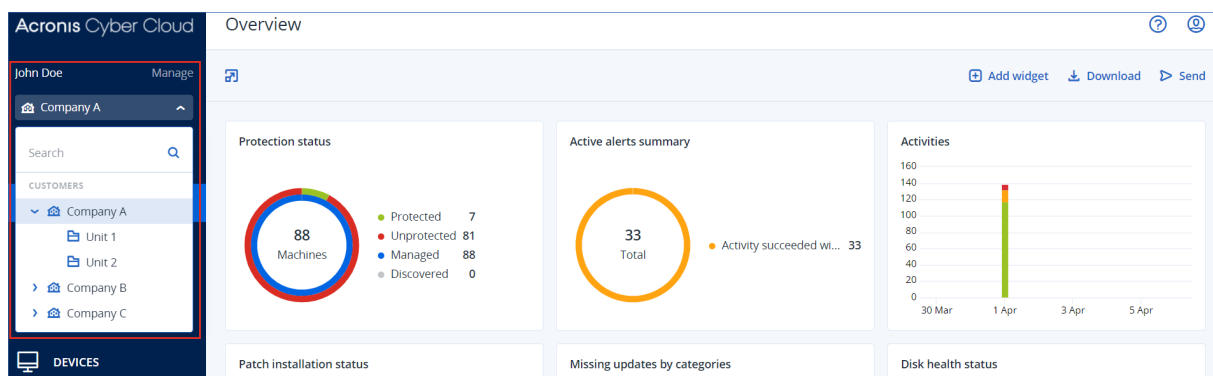
9 Service console

In the service console, you can manage devices and protection plans, change the protection settings, configure reports, or check the backup storage.

You can find the most important information about your protection on the dashboard.

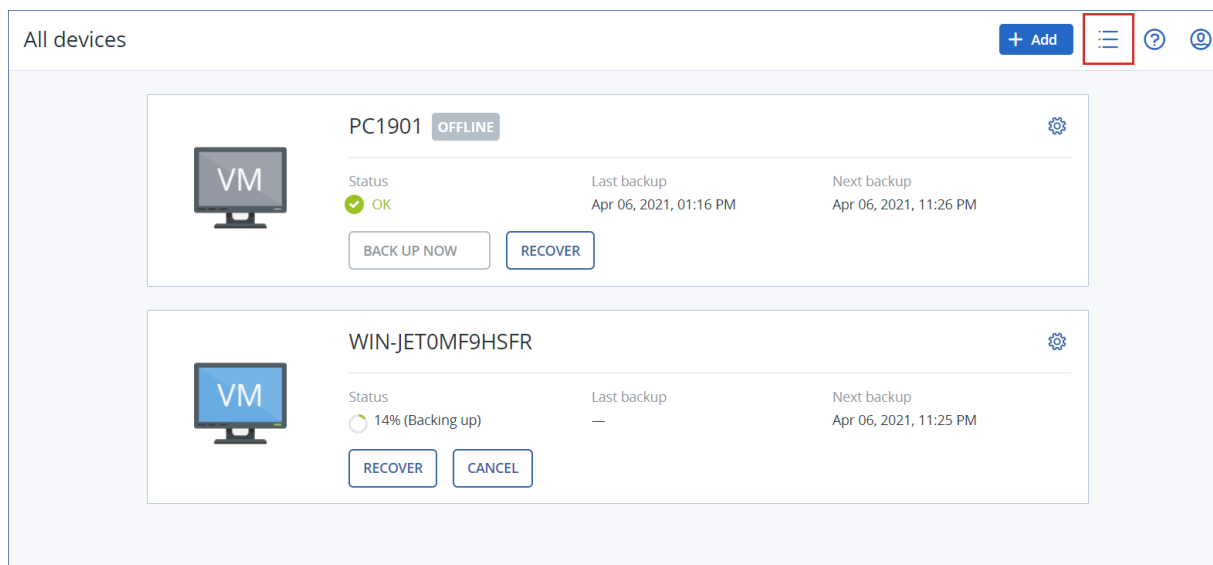
The service console gives you access to additional Cyber Protection services or features, such as File Sync & Share or Antivirus and Antimalware protection, Patch management, Device control, and Vulnerability assessment. Their type and number vary according to your Cyber Protection license.

Depending on your access permissions, you can manage the protection for one or multiple customer tenants or units in a tenant. To switch the hierarchy level, use the drop-down list in the navigation menu. Only the levels to which you have access are shown. To go to the Management Portal, click **Manage**.



The **Devices** section is available in simple and table view. To switch between them, click the corresponding icon in the top right corner.

The simple view shows only a few machines.



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

All devices							
<div> <div>+ Add</div> <div></div> <div>?</div> <div></div> </div>							
<div> <div>Q Search</div> <div>Loaded: 2 / Total: 2 View: Standard</div> </div>							
<input type="checkbox"/>	Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup
	PC1901	CompanyA	625/850	OK	Apr 06 01:16:14 PM	Apr 06 11:26:28 PM	
	WIN-JET0MF9HSFR	CompanyA	625/850	14% (Backing up)	Never	Apr 06 11:25:23 PM	

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

To delete a machine from the service console

1. Select the check box next to the desired machine.
2. Click **Delete**, and then confirm your choice.

Important

Deleting a machine from the service console does not uninstall the protection agent on it and does not delete the protection plans applied to this machine. The backups of the deleted machine will also be kept.

ESXi hosts and virtual machines on the following virtualization platforms can be backed up by an agent that is not installed on them—that is, in the agentless mode:

- Hyper-V
- VMware
- Virtuozzo Hybrid Infrastructure
- Scale Computing
- Red Hat Virtualization/oVirt

You cannot delete such machines individually. To delete them, you need to find and delete the machine on which the respective agent (Agent for Hyper-V, Agent for VMware, Agent for Virtuozzo Hybrid Infrastructure, Agent for Scale Computing, or Agent for oVirt) is installed.

To delete a virtual machine or ESXi host without an agent

1. Under **Devices**, select **All devices**.
2. Click the gear icon in the upper right corner and enable the **Agent** column.

All devices

+ Add

?

Q Search

Loaded: 2 / Total: 2 View: Last used

<input type="checkbox"/>	Type	Name ↑	Account	#CyberFit Score ?	Status	Last backup	Next backup	
<input type="checkbox"/>	VM	PC1901	CompanyA	625/850	OK	Apr 06 01:16:14		
<input type="checkbox"/>	VM	WIN-JETOMF9HSFR	CompanyA	625/850	16% (Backing up)	Never		

General

Hardware

System

Motherboard

Motherboard serial num

BIOS version

Organization

Owner

Domain

Agent

Operating system

Operating system build

Plans

3. In the **Agent** column, check the name of the machine where the respective agent is installed.
4. Delete this machine from the service console. This will also delete all of the machines that are backed up by its agent.
5. Uninstall the agent from the deleted machine as described in "Uninstalling agents" (p. 114).

10 Device groups

Note

The availability of this feature depends on the service quotas that are enabled for your account.

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.

10.1 Built-in groups

Once a device is registered, it appears in one of the built-in root groups on the **Devices** tab.

Root groups cannot be edited or deleted. You cannot apply plans to root groups.

Some of the root groups contain built-in sub-root groups. These groups cannot be edited or deleted. However, you can apply plans to sub-root built-in groups.

10.2 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.

10.3 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.

10.4 Adding devices to static groups

1. Click **Devices**, and then select one or more devices that you want to add to a group.
2. Click **Add to group**.
The software displays a tree of groups to which the selected device can be added.
3. If you want to create a new group, do the following. Otherwise, skip this step.
 - a. Select the group in which you want to create a group.
 - b. Click **New group**.
 - c. Specify the group name, and then click **OK**.
4. Select the group to which you want to add the device, and then click **Done**.

Another way to add devices to a static group is to select the group and click **Add devices**.

10.5 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.

Note

You cannot create dynamic groups for the All devices group.

2. Search for devices by using the search field. You can use multiple search criteria and operators described below.
3. Click **Save as** next to the search field.

Note

Some search criteria are not supported for group creation. See the table in section Search criteria below.

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

10.5.1 Search criteria

The following table summarizes the available search criteria.

Criterion	Meaning	Search query examples	Supported for group creation
name	<ul style="list-style-type: none"> • Host name for physical machines • Name for virtual machines • Database name • Email address for mailboxes 	name = 'en-00'	Yes
comment	<p>Comment for a device.</p> <p>Default value:</p> <ul style="list-style-type: none"> • For physical machines running Windows, the computer description taken from the computer properties in Windows. This value is updated automatically every 15 minutes. • Empty for other devices. <p>To view the comment, under Devices, select the device, click Details, and then locate the Comment section.</p> <p>To add or change the comment manually, click Add or Edit. In this case, automatic update will stop working. To allow automatic</p>	<p>comment = 'important machine'</p> <p>comment = '' (all machines without a comment)</p>	Yes

	<p>updates again, clear the comment that you have added.</p> <p>To refresh the comment field for your devices, restart the Managed Machine Service in Windows Services or run the following commands at the command prompt:</p> <pre>net stop mms</pre> <pre>net start mms</pre>		
ip	IP address (only for physical machines).	ip RANGE ('10.250.176.1', '10.250.176.50')	Yes
memorySize	RAM size in megabytes (MiB).	memorySize < 1024	Yes
diskSize	Hard drive size in gigabytes or megabytes (only for physical machines).	diskSize < 300GB diskSize >= 3000000MB	No
insideVm	<p>Virtual machine with an agent inside.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • true • false 	insideVm = true	Yes
osName	Operating system name.	osName LIKE '%Windows XP%'	Yes
osType	<p>Operating system type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 'windows' • 'linux' • 'macosx' 	osType IN ('linux', 'macosx')	Yes
osProductType	<p>The operating system product type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 'dc' <p>Stands for Domain Controller.</p> <p>Note When the domain</p>	osProductType = 'server'	Yes

	<p>controller role is assigned on a Windows server, the osProductType changes from "server" to "dc". Such machines will be not included in search results for filter "osProductType='server'.</p> <ul style="list-style-type: none"> • 'server' • 'workstation' 		
tenant	The name of the unit to which the device belongs.	tenant = 'Unit 1'	Yes
tenantId	<p>The identifier of the unit to which device belongs.</p> <p>To get the unit ID, under Devices, select the device, click Details > All properties. The ID is shown in the ownerId field.</p>	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	Yes
state	<p>Device state.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz' 	state = 'backup'	No
protectedByPlan	Devices that are protected by a protection plan with a given ID.	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No

	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. To get the device ID, under Devices , select the device, click Details > All properties . The ID is shown in the id field.	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Yes
lastBackupTime*	The date and time of the last successful backup. The format is 'YYYY-MM-DD HH:MM'.	lastBackupTime > '2020-03-11' lastBackupTime <= '2019-03-11 00:15' lastBackupTime is null	No
lastBackupTryTime*	The time of the last backup attempt.	lastBackupTryTime >= '2020-03-11'	No

	The format is 'YYYY-MM-DD HH:MM'.		
nextBackupTime*	The time of the next backup. The format is 'YYYY-MM-DD HH:MM'.	nextBackupTime >= '2021-03-11'	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: <ul style="list-style-type: none"> 'machine' 'virtual_machine.vmwesx' 'virtual_machine.mshyperv' 'virtual_machine.rhev' 'virtual_machine.kvm' 'virtual_machine.xen' 	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	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

10.5.2 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'

NOT	Logical negation operator.	NOT(osProductType = 'workstation')
LIKE 'wildcard pattern'	<p>This operator is used to test if an expression matches the wildcard pattern. This operator is case-insensitive.</p> <p>The following wildcard operators can be used:</p> <ul style="list-style-type: none"> • * 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_'
IN (<value1>, ... <valueN>)	This operator is used to test if an expression matches any value in a list of values. This operator is case-sensitive.	osType IN ('windows', 'linux')
RANGE(<starting_value>, <ending_value>)	This operator is used to test if an expression is within a range of values (inclusive).	ip RANGE ('10.250.176.1', '10.250.176.50')
<	Less than operator.	memorySize < 1024
>	Greater than operator.	diskSize > 300GB
<=	Less than or equal to operator.	lastBackupTime <= '2019-03-11 00:15'
>=	Greater than or equal to operator.	nextBackupTime >= '2021-03-11'
= or ==	Equal to operator.	osProductType = 'server'
!= or <>	Not equal to operator.	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'

10.6 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 "[Protection plan](#)".

11 Multitenancy support

Cyber Protection supports multitenancy. This means that a tenant administrator/user can manage objects that are related to their tenant or its sub-tenants (units). An administrator/user from a unit cannot manage objects of the parent tenant.

For example, a customer administrator created a protection plan and applied it to a machine. A customer administrator can also manage protection plans created by a unit administrator. However, a unit administrator cannot manage the protection plan created by the customer administrator. A unit administrator can create its own protection plan that does not conflict with the plan of the customer administrator.

Multitenancy also implies that a tenant administrator/user can see all objects that are related to this tenant or its sub-tenants (units). An administrator/user from a unit cannot see objects of the parent tenant.

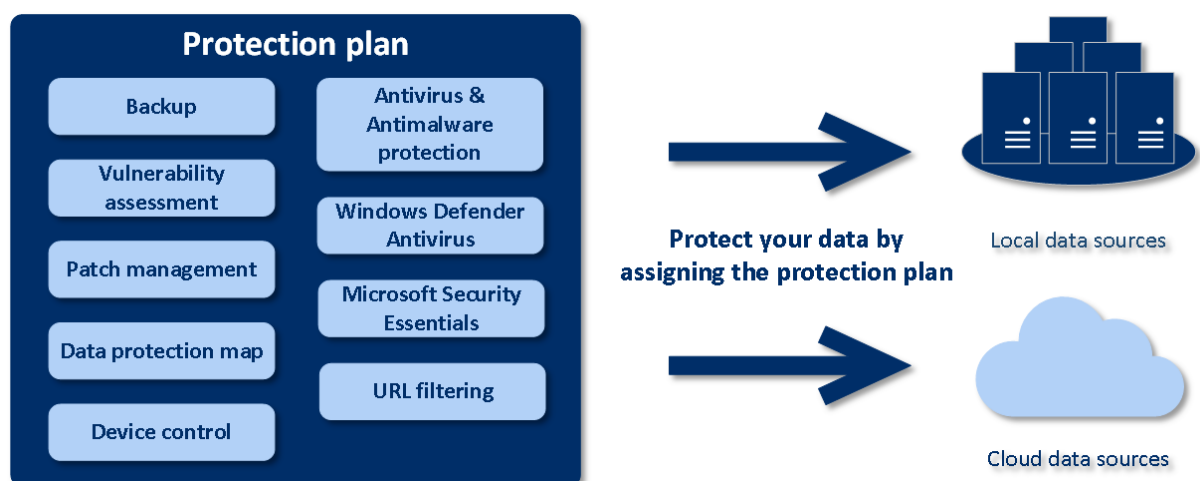
For example, the data shown in the patch list, quarantine, threat feed, alerts, and activities will be shown only for the current tenant and its sub-tenants. The data related to the parent tenant is not shown.

12 Protection plan and modules

The protection plan is a plan that combines several data protection modules including

- **Backup** – allows you to back up your data sources to local or cloud storage.
- "Disaster recovery" (p. 360) - allows you to launch exact copies of your machines in the cloud site and switch the workload from the corrupted original machines to the recovery servers in the cloud.
- **Antivirus and Antimalware protection** – allows you to check your machines with the built-in antimalware solution.
- **URL filtering** – allows you to protect your machines from threats coming from the Internet by blocking access to malicious URLs and content to be downloaded.
- **Windows Defender Antivirus** – allows you to manage the settings of Windows Defender Antivirus to protect your environment.
- Microsoft Security Essentials – allows you to manage the settings of Microsoft Security Essentials to protect your environment.
- **Vulnerability assessment** – automatically checks the Microsoft, Linux, macOS, Microsoft third-party products, and macOS third-party products installed on your machines for vulnerabilities and notifies you about them.
- **Patch management** – enables you to install patches and updates for the Microsoft, Linux, macOS, Microsoft third-party products, and macOS third-party products on your machines to close the discovered vulnerabilities.
- **Data protection map** – allows you to discover the data in order to monitor the protection status of important files.
- **Device control** - allows you to specify devices that users are allowed or restricted to use on your machines.

Use the protection plan to protect your data sources completely from external and internal threats. By enabling and disabling different modules and setting up the module settings, you can build flexible plans satisfying various business needs.



12.1 Creating a protection plan

A protection plan can be applied to multiple machines at the time of its creation, or later. When you create a plan, the system checks the operating system and the device type (for example, workstation, virtual machine, etc.) and shows only those plan modules that are applicable to your devices.

A protection plan can be created in the following ways.

- In the **Devices** section – when you select the device or devices to be protected and then create a plan for them.
- In the **Plans** section – [when you create a plan and then select the machines to be applied to](#).

To create the first protection plan in the Devices section

1. In the service console, go to **Devices > All devices**.
2. Select the machines that you want to protect.
3. Click **Protect**, and then click **Create plan**.
The protection plan default settings open.
4. [Optional] To modify the protection plan name, click on the pencil icon next to the name.
5. [Optional] To enable or disable the plan module, click the switch next to the module name.
6. [Optional] To configure the module parameters, click the corresponding section of the protection plan.
7. When ready, click **Create**.

The Backup, Antivirus and Antimalware protection, Vulnerability assessment, Patch management, and Data protection map modules can be performed on demand by clicking **Run now**.

For more information on the Disaster recovery module, see "Create a disaster recovery protection plan" (p. 363).

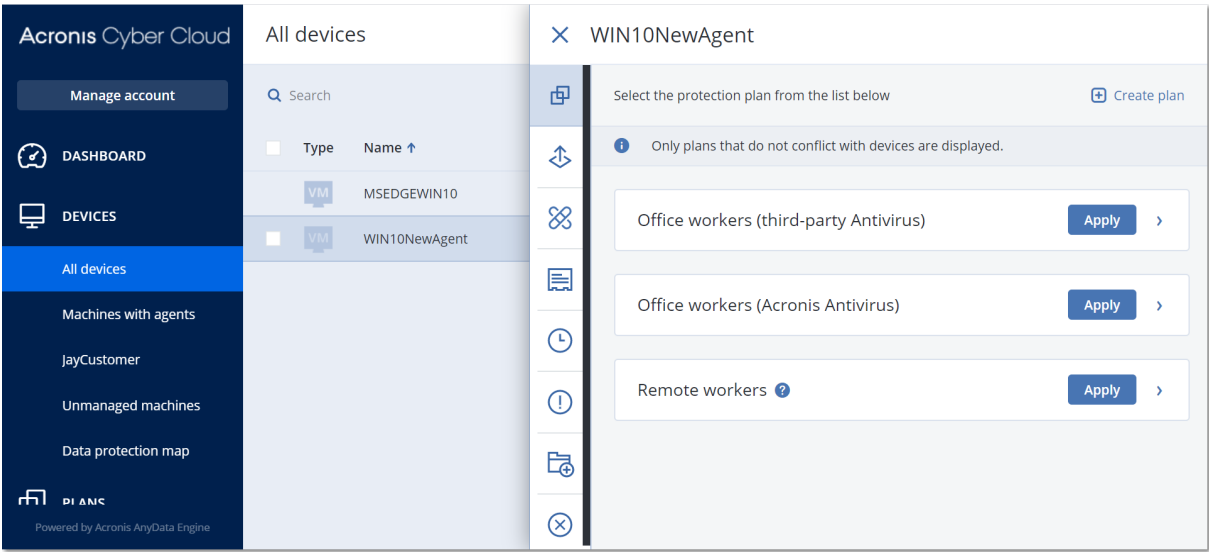
For more information on the Device control module, see "Device control" (p. 496).

12.2 Default protection plans

Three preconfigured plans, available by default, ensure quick protection for specific workloads:

- Office workers (Acronis Antivirus)
This plan is optimized for users working in the office and having a preference to use the Acronis antivirus software.
- Office workers (third-party Antivirus)
This plan is optimized for users working in the office and having a preference to use a third-party antivirus software. The main difference is that this plan has the **Antivirus and Antimalware protection** module and **Active Protection** disabled.
- Remote workers

This plan is optimized specifically for users working remotely. It has more frequent tasks (such as backup, antimalware protection, vulnerability assessment), stricter protection actions, and optimized performance and power options.



To apply a default protection plan

- 1. In the service console, go to **Devices > All devices**.
- 2. Select the machines that you want to protect.
- 3. Click **Protect**.
- 4. Select one of the default plans, and then click **Apply**.

Note

You can also configure [your own protection plan](#) by clicking **Create plan**.

To modify an applied default protection plan

- 1. In the service console, go to **Plans > Protection**.
- 2. Select the plan that you want to modify, and then click **Edit**.
- 3. Modify the modules that are included in this plan, or their options, and then click **Save**.

Important

Some settings cannot be changed for an existing protection plan.

12.2.1 Default plan options

The preconfigured plans use the default options for each module*, with the following modifications:

Modules and options/Plan	Office workers (Acronis Antivirus)	Office workers (third-party Antivirus)	Remote workers
"Backup" (p. 146)			

What to back up	Entire machine	Entire machine	Entire machine
Continuous data protection (CDP)	Disabled	Disabled	Enabled
Where to back up	Cloud storage	Cloud storage	Cloud storage
Backup scheme	Always incremental (single-file)	Always incremental (single-file)	Always incremental (single-file)
Schedule	Default daily schedule	Default daily schedule	<p>Daily: Monday to Friday at 12:00 PM</p> <p>Additionally enabled options and start conditions:</p> <ul style="list-style-type: none"> • If the machine is turned off, run missed tasks at the machine startup • Wake up from the sleep or hibernate mode to start a scheduled backup • Save battery power: Do not start when on battery • Do not start when on metered connection
How long to keep	<p>Monthly: 12 months</p> <p>Weekly: 4 weeks</p> <p>Daily: 7 days</p>	<p>Monthly: 12 months</p> <p>Weekly: 4 weeks</p> <p>Daily: 7 days</p>	<p>Monthly: 12 months</p> <p>Weekly: 4 weeks</p> <p>Daily: 7 days</p>
Backup options	Default options	Default options	<p>Default options, plus:</p> <p>Performance and backup window (the green set):</p> <ul style="list-style-type: none"> • CPU priority: Low • Output speed: 50%
"Antivirus and antimalware protection" (p. 422)			
Schedule scan	Scan type: Quick	n/a	<p>Scan type: Full</p> <p>Additionally enabled options and start conditions:</p> <ul style="list-style-type: none"> • If the machine is turned off, run missed tasks at the machine startup • Wake up from the sleep or hibernate mode to start a scheduled backup • Save battery power: Do not start

			when on battery
"URL filtering" (p. 438)			
Malicious websites access	Always ask user	Always ask user	Block
"Vulnerability assessment" (p. 454)			
	Default	Default	Default
"Patch management" (p. 461)			
Schedule	Default	Default	Daily: Monday to Friday at 02:20PM
Pre-update backup	Off	Off	On
"Data protection map" (p. 491)			
Extensions	Default options	Default options	Default options, plus: Images: <ul style="list-style-type: none"> • .bmp • .png • .ico • .wbmp • .gif • .bmp • .xcf • .psd • .tiff • .jpeg, .jpg • .dwg Audio: <ul style="list-style-type: none"> • .wav • .aif, .aifc, .aiff • .au, .snd • .mid, .midi • .mid • .mpga, .mp3 • .oga • .flac • .oga • .oga • .opus • .oga

			<ul style="list-style-type: none"> • .spx • .oga • .ogg • .ogx • .ogx • .mp4
"Device control" (p. 496)			
Device control	Disabled	Disabled	Disabled

* The number of modules in the default protection plan may vary between editions of the Cyber Protection service.

12.3 Resolving plan conflicts

A protection plan can be in the following statuses:

- **Active** - a plan that is assigned to devices and executed on them.
- **Inactive** - a plan that is assigned to devices but disabled and not executed on them.

12.3.1 Applying several plans to a device

You can apply several protection plans to a single device. As a result, you will get a combination of different protection plans assigned on a single device. For example, you may apply a plan that has only the Antivirus and Antimalware protection module enabled in the plan and another plan that contains only the backup module. The protection plans can be combined only if they do not have intersecting modules. If there are similar enabled modules in the applied protection plans, you must resolve conflicts between such modules.

12.3.2 Resolving plan conflicts

Plan conflicts with already applied plans

When you create a new plan on a device or devices with already applied plans that conflict with the new plan, you can resolve a conflict with one of the following ways:

- Create a new plan, apply it, and disable all already applied conflicting plans.
- Create a new plan and disable it.

When you edit a plan on a device or devices with already applied plans that conflict with the changes made, you can resolve a conflict with one of the following ways:

- Save changes to the plan and disable all already applied conflicting plans.
- Save changes to the plan and disable it.

A device plan conflicts with a group plan

If a device is included in a group of devices with an assigned group plan, and you try to assign a new plan to a device, then the system will ask you to resolve the conflict by doing one of the following:

- Remove a device from the group and apply a new plan to the device.
- Apply a new plan to the whole group or edit the current group plan.

License issue

The assigned quota on a device must be appropriate for the protection plan to be performed, updated, or applied. To resolve the license issue, do one of the following:

- Disable the modules that are unsupported by the assigned quota and continue using the protection plan.
- Change the assigned quota manually: go to **Devices** > **<particular_device>** > **Details** > **Service quota**, then revoke the existing quota and assign a new one.

12.4 Operations with protection plans

Available actions with a protection plan

You can perform the following actions with a protection plan:

- Rename a plan.
- Enable/disable modules and edit each module setting.
- Enable/disable a plan.

A disabled plan will not be carried out on the device to which it is applied.

This action is convenient for administrators who intend to protect the same device with the same plan later. The plan is not revoked from the device and to restore the protection, you must only re-enable the plan.

- Apply a plan to a device or a group of devices.
- Revoke a plan from a device.

A revoked plan is not applied to a device anymore.

This action is convenient for administrators who do not need to protect quickly the same device with the same plan again. To restore the protection of a revoked plan, you must know the name of this plan, select it from the list of available plans, and then re-apply it to the desired device.

- Import/export a plan.

Note

You can import protection plans created in Cyber Protection 9.0 (released in March 2020) and later. Plans created in earlier product versions are incompatible with versions 9.0 and later.

- Delete a plan.

To apply an existing protection plan

1. Select the machines that you want to protect.
2. Click **Protect**. If a protection plan is already applied to the selected machines, click **Add plan**.
3. The software displays previously created protection plans.
4. Select a protection plan to apply and click **Apply**.

To edit a protection plan

1. If you want to edit the protection plan for all machines to which it is applied, select one of these machines. Otherwise, select the machines for which you want to edit the protection plan.
2. Click **Protect**.
3. Select the protection plan that you want to edit.
4. Click the Ellipsis icon next to the protection plan name, and then click **Edit**.
5. To modify the plan parameters, click the corresponding section of the protection plan panel.
6. Click **Save changes**.
7. To change the protection plan for all machines to which it is applied, click **Apply the changes to this protection plan**. Otherwise, click **Create a new protection plan only for the selected devices**.

To revoke a protection plan from machines

1. Select the machines that you want to revoke the protection plan from.
2. Click **Protect**.
3. If several protection plans are applied to the machines, select the protection plan that you want to revoke.
4. Click the ellipsis icon next to the protection plan name, and then click **Revoke**.

To delete a protection plan

1. Select any machine to which the protection plan that you want to delete is applied.
2. Click **Protect**.
3. If several protection plans are applied to the machine, select the protection plan that you want to delete.
4. Click the ellipsis icon next to the protection plan name, and then click **Delete**.
As a result, the protection plan is revoked from all of the machines and completely removed from the web interface.

13 #CyberFit Score for machines

#CyberFit Score provides you with a security assessment and scoring mechanism that evaluates the security posture of your machine. It identifies security gaps in the IT environment and open attack vectors to endpoints and provides recommended actions for improvements in the form of a report. This feature is available in all Cyber Protect editions.

The #CyberFit Score functionality is supported on:

- Windows 7 (first version) and later versions
- Windows Server 2008 R2 and later versions

13.1 How it works

The protection agent that is installed on a machine performs a security assessment and calculates the #CyberFit Score for the machine. The #CyberFit Score of a machine is automatically periodically recalculated.

13.1.1 #CyberFit scoring mechanism

The #CyberFit Score for a machine is calculated, based on the following metrics:

- Antimalware protection 0-275
- Backup protection 0-175
- Firewall 0-175
- Virtual private network (VPN) 0-75
- Full disk encryption 0-125
- Network security 0-25

The maximum #CyberFit Score for a machine is 850.

Metric	What is assessed?	Recommendations to users	Scoring
Antimalware	The agent checks whether antimalware software is installed on a machine.	<p>Findings:</p> <ul style="list-style-type: none">• You have antimalware protection enabled (+275 points)• You don't have antimalware protection, your system may be at risk (0 points) <p>Recommendations provided by #CyberFit Score:</p> <p>You should have an antimalware solution installed and enabled on your machine to stay protected from security risks.</p> <p>You should refer to websites such as AV-Test or AV-Comparatives for a list of recommended</p>	<p>275 - antimalware software is installed on a machine</p> <p>0 - no antimalware software is installed on a machine</p>

		antimalware solutions.	
Backup	The agent checks if a backup solution is installed on a machine.	<p>Findings:</p> <ul style="list-style-type: none"> You have a backup solution protecting your data (+175 points) No backup solution was found, your data may be at risk (0 points) <p>Recommendations provided by #CyberFit Score:</p> <p>We recommend that you back up your data regularly to prevent data loss or ransomware attacks. Below are some backup solutions that you should consider using:</p> <ul style="list-style-type: none"> Acronis Cyber Protect / Cyber Backup / True Image Windows Server Backup (Windows Server 2008 R2 and later) 	<p>175 - a backup solution is installed on a machine</p> <p>0 - no backup solution is installed on a machine</p>
Firewall	<p>The agent checks whether a firewall is available and enabled in your environment.</p> <p>The agent does the following:</p> <ol style="list-style-type: none"> Checks Windows Firewall and Network Protection whether a public firewall is turned on. Checks Windows Firewall and Network Protection whether a private firewall is turned on. Checks for a 3-rd party firewall solution/agent if Windows public 	<p>Findings:</p> <ul style="list-style-type: none"> You have a firewall enabled for public and private networks, or a 3-rd party firewall solution is found (+175 points) You have a firewall enabled only for public networks (+100 points) You have a firewall enabled only for private networks (+75 points) You have no firewall enabled, your network connection is not secure (0 points) <p>Recommendations provided by #CyberFit Score:</p> <p>It is recommended to enable firewall for your public and private networks to improve your security protection against malicious attacks on your system. Below are provided detailed guides on setting-up your Windows firewall, depending on your security needs and network architecture:</p> <p>Guides for end-users/employees:</p> <p>How to set up Windows Defender Firewall on your PC</p> <p>How to set up Windows Firewall on your PC</p> <p>Guides for system administrators and engineers:</p> <p>How to deploy Windows Defender Firewall with Advanced Security</p>	<p>100 - Windows public firewall is enabled</p> <p>75 - Windows private firewall is enabled</p> <p>175 - Windows public and private firewall are enabled</p> <p>OR</p> <p>a third-party firewall solution is enabled</p> <p>0 - neither a Windows firewall, nor a third-party firewall solution are enabled</p>

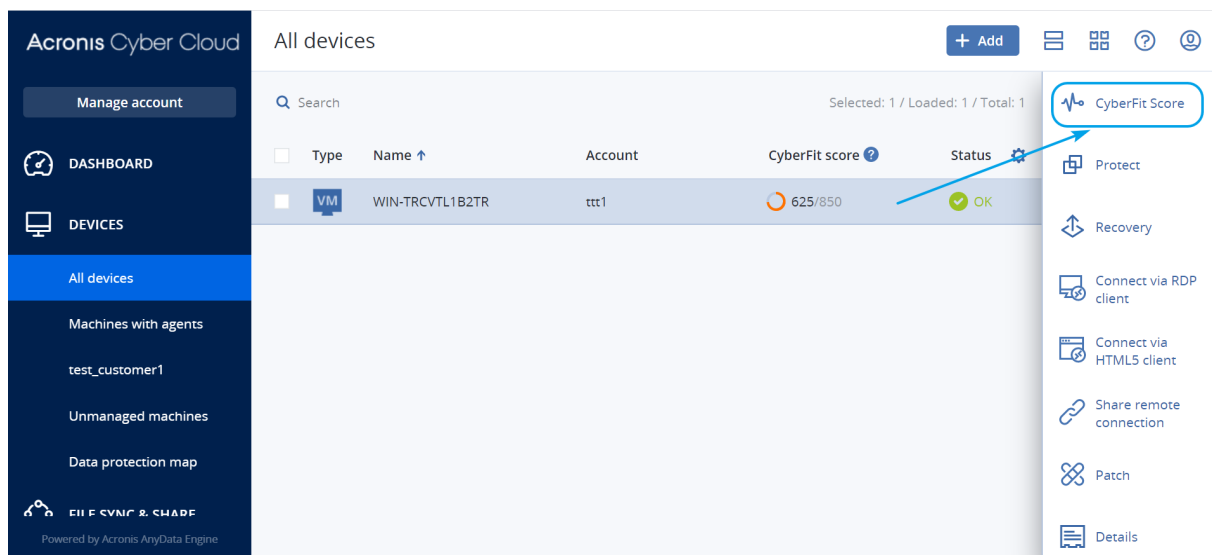
	and private firewalls are disabled.	How to create Advanced Rules in Windows Firewall	
Virtual Private Network (VPN)	The agent checks whether a VPN solution is installed on a machine and whether the VPN is enabled and running.	<p>Findings:</p> <ul style="list-style-type: none"> You have a VPN solution and can safely receive and send data across public and shared networks (+75 points) No VPN solution was found, your connection to public and shared networks is not secure (0 points) <p>Recommendations provided by #CyberFit Score:</p> <p>It is recommended to use VPN to access your corporate network and confidential data. It is critical to use a VPN to keep your communications safe and private, especially if you use complimentary Internet access from a cafe, library, airport, or elsewhere. Below are some VPN solutions that you should consider using:</p> <ul style="list-style-type: none"> Acronis Business VPN OpenVPN Cisco AnyConnect NordVPN TunnelBear ExpressVPN PureVPN CyberGhost VPN Perimeter 81 VyprVPN IPVanish VPN Hotspot Shield VPN Fortigate VPN ZYXEL VPN SonicWall GVPN LANCOM VPN 	<p>75 - VPN is enabled and running</p> <p>0 - VPN is not enabled</p>
Disk encryption	<p>The agent checks whether a machine has disk encryption enabled.</p> <p>The agent checks whether</p>	<p>Findings:</p> <ul style="list-style-type: none"> You have full disk encryption enabled, your machine is protected against physical tampering (+125 points) Only some hard drives are encrypted, your machine may be at risk from physical tampering (+75 points) 	<p>125 - all disks are encrypted</p> <p>75 - at least one of your disks is encrypted but there are also</p>

	Windows BitLocker is turned on.	<ul style="list-style-type: none"> No disk encryption was found, your machine is at risk from physical tampering (0 points) <p>Recommendations provided by #CyberFit Score:</p> <p>It is recommended to turn on Windows BitLocker to improve protection of your data and files.</p> <p>Guide: How to turn on device encryption on Windows</p>	<p>unencrypted disks</p> <p>0 - no disks are encrypted</p>
Network security (outgoing NTLM traffic to remote servers)	The agent checks whether a machine has restricted outgoing NTLM traffic to remote servers.	<p>Findings:</p> <ul style="list-style-type: none"> Outgoing NTLM traffic to remote servers is denied, your credentials are protected (+25 points) Outgoing NTLM traffic to remote servers is not denied, your credentials may be vulnerable to exposure (0 points) <p>Recommendations provided by #CyberFit Score:</p> <p>It is recommended to deny all outgoing NTLM traffic to remote servers for better security protection. You can find information on how to change the NTLM settings and add exceptions by following the link below.</p> <p>Guide: Restrict outgoing NTLM traffic to remote servers</p>	<p>25 - outgoing NTLM traffic is set to DenyAll</p> <p>0 - outgoing NTLM traffic is set to another value</p>

Based on the summed points awarded to each metric, the total #CyberFit Score of a machine can fit one of the following ratings that reflect the endpoint's level of protection:

- 0 - 579 - Poor
- 580 - 669 - Fair
- 670 - 739 - Good
- 740 - 799 - Very good
- 800 - 850 - Excellent

You can see the #CyberFit Score for your machines in the service console: go to **Devices > All devices**. In the list of devices, you can see the **#CyberFit Score** column. You can also [run the #CyberFit Score scan](#) for a machine to check its security posture.

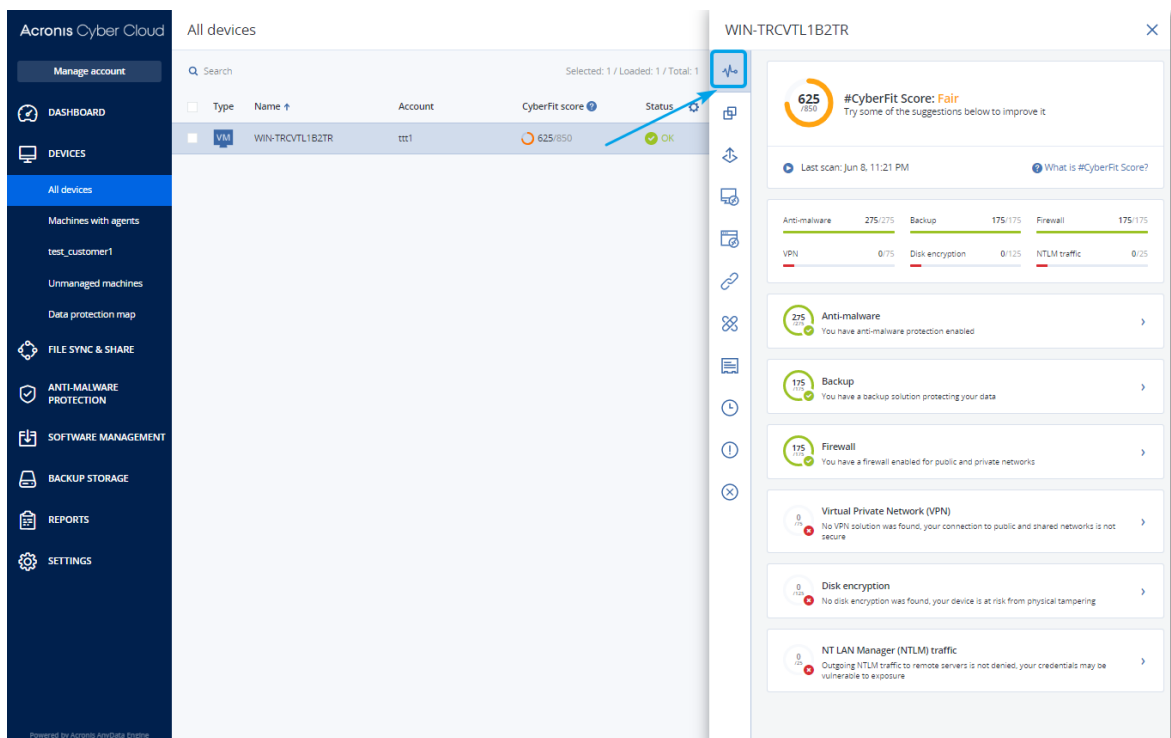


You can also get information about the #CyberFit Score in the corresponding [widget](#) and [report](#) pages.

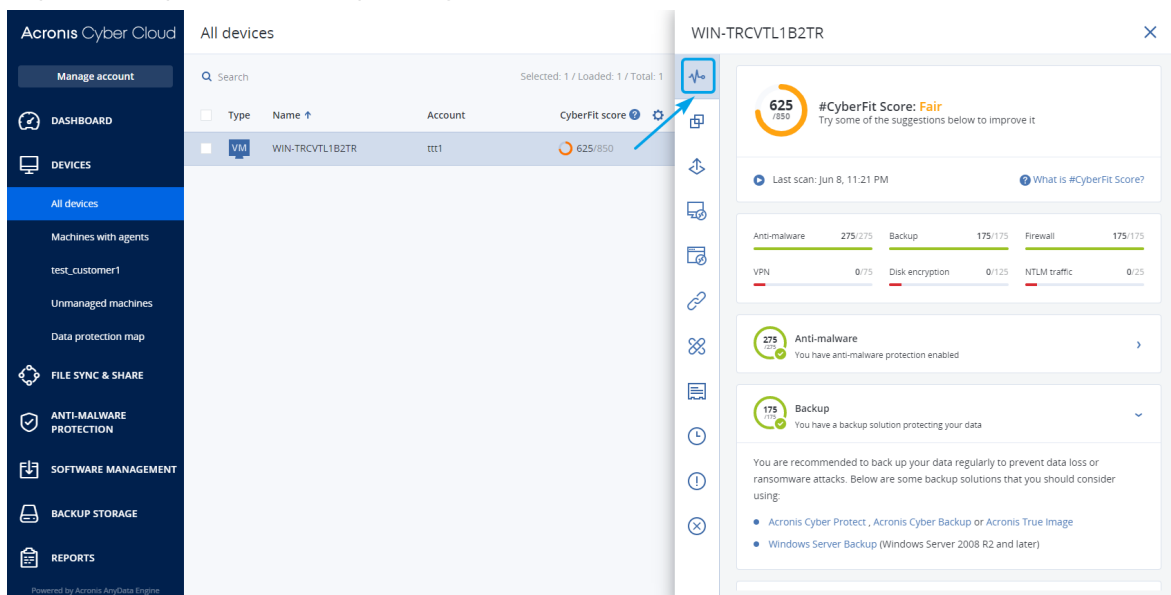
13.2 Running a #CyberFit Score scan

To run a #CyberFit Score scan

1. In the service console, go to **Devices**.
2. Select the machine and click **#CyberFit Score**.
3. If the machine has never been scanned before, then click **Run a first scan**.
4. After the scan is completed, you will see the total #CyberFit Score for the machine along with the scores of each of the six assessed metrics - Antimalware, Backup, Firewall, Virtual Private Network (VPN), Disk encryption, and NT LAN Manager (NTLM) traffic.



- To check how to increase the score of each metric for which the security configurations could be improved, expand the corresponding section and read the recommendations.



- After addressing the recommendations, you can always recalculate the #CyberFit Score of the machine by clicking on the arrow button right under the total #CyberFit Score.

14 Backup and recovery

The backup module enables backup and recovery of physical and virtual machines, files, and databases to local or cloud storage.

14.1 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.

To create the first protection plan with the Backup module enabled

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

The software displays protection plans that are applied to the machine. If the machine does not have any plans already assigned to it, then you will see the default protection plan that can be applied. You can adjust the settings as needed and apply this plan or create a new one.

3. To create a new plan, click **Create plan**. Enable the **Backup** module and unroll the settings.

New protection plan (2)

Cancel

Create

Backup

Entire machine to Cloud storage, Monday to Friday at 05:45 PM

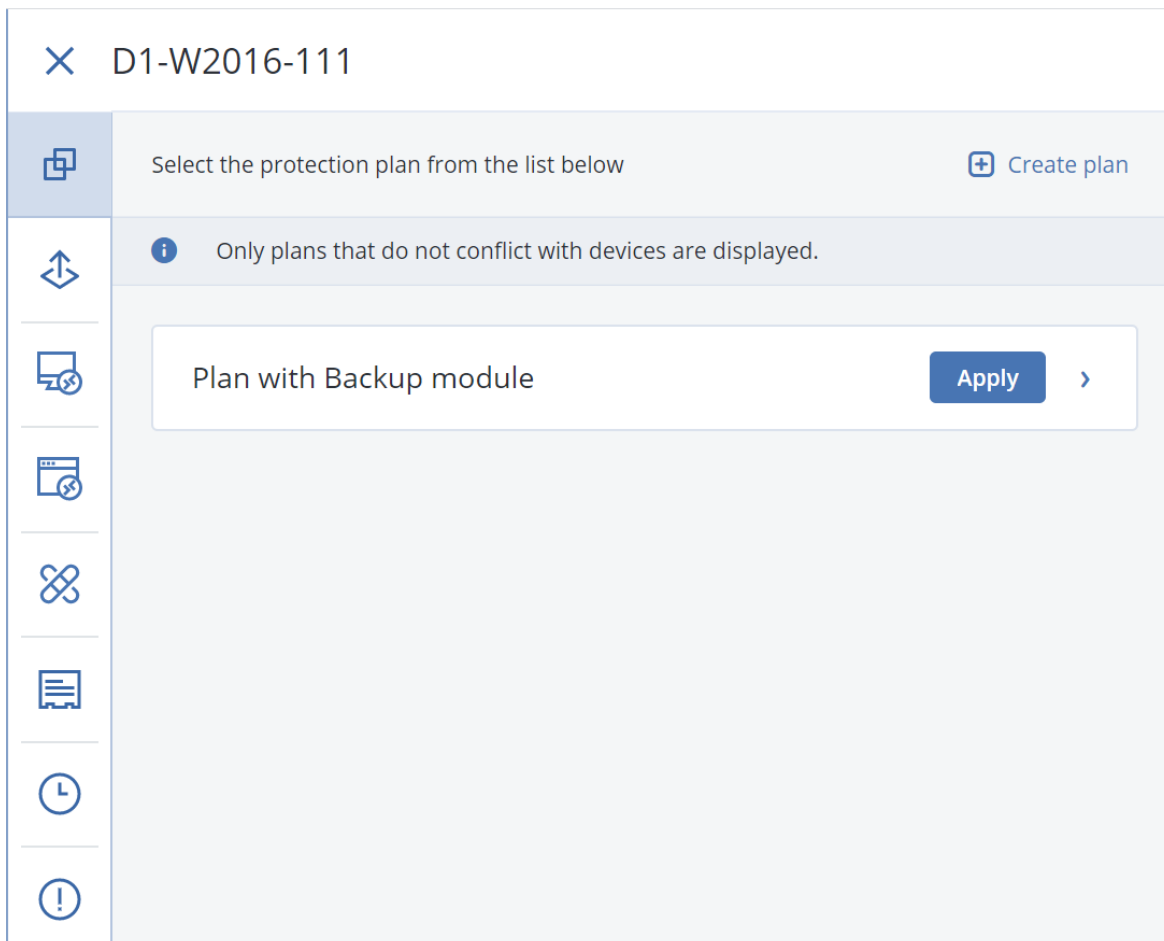
What to back up	Entire machine	
Continuous data protection (CDP)		
Where to back up	Cloud storage	
Schedule	Monday to Friday at 05:45 PM	
How long to keep	Monthly: 6 months Weekly: 4 weeks Daily: 7 days	
Encryption		
Application backup	Disabled	
Backup options	Change	

- [Optional] To modify the protection plan name, click the default name.
- [Optional] To modify the Backup module parameters, click the corresponding setting of the protection plan panel.
- [Optional] To modify the backup options, click **Change** next to **Backup options**.
- Click **Create**.

To apply an existing protection plan

- Select the machines that you want to back up.
- 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**.

14.2 Protection plan cheat sheet

The following table summarizes the available protection plan 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 machines ¹)	Direct selection Policy rules File filters	Cloud Local folder Network folder	Always incremental (Single-file) Always full Weekly full, Daily incremental	By backup age (single rule/per backup set) By number of backups

¹A machine that is backed up by an agent installed in the operating system.

			NFS*		
			Secure Zone**		
Disks/volumes (virtual machines ¹)	Policy rules File filters	Cloud Local folder Network folder NFS*	Monthly full, Weekly differential, Daily incremental (GFS) Custom (F-D-I)		
Files (physical machines only ²)	Direct selection Policy rules File filters	Cloud Local folder Network folder NFS* Secure Zone**	Always incremental (Single-file)*** Always full Weekly full, Daily incremental Monthly full, Weekly differential, Daily incremental (GFS)		
ESXi configuration	Direct selection	Local folder Network folder NFS*	Custom (F-D-I)		
Websites (files and MySQL databases)	Direct selection	Cloud	—		
System state		Cloud	Always full		
SQL databases	Direct selection	Local folder	Weekly full, daily incremental		
Exchange databases		Network folder	Custom (F-I)		
Microsoft 365	Mailboxes (local Agent for Microsoft 365) Direct selection	Cloud Local folder	Always incremental (Single-file)		

By total size of backups****
Keep indefinitely

¹A virtual machine that is backed up at a hypervisor level by an external agent such as Agent for VMware or Agent for Hyper-V. A virtual machine with an agent inside is treated as physical from the backup standpoint.

²A machine that is backed up by an agent installed in the operating system.

			Network folder		
	Mailboxes (cloud Agent for Microsoft 365)	Direct selection	Cloud	—	
	Public folders				
	Teams				
	OneDrive files	Direct selection			
	SharePoint Online data				
Google Workspace	Gmail mailboxes	Direct selection			Cloud
	Google Drive files	Direct selection			
	Shared drive files	Policy rules			

* Backup to NFS shares is not available in Windows.

** Secure Zone cannot be created on a Mac.

*** The option Always incremental (Single-file) is available only if the primary backup destination is Cloud.

**** The **By total size of backups** retention rule is not available with the **Always incremental (single-file)** backup scheme or when backing up to the cloud storage.

14.3 Selecting data to back up

14.3.1 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.

Disks connected via the iSCSI protocol to a physical machine can also be backed up though there are [limitations](#) if you use Agent for VMware or Agent for Hyper-V for backing up the iSCSI-connected disks.

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

Direct selection

Direct selection is available only for physical machines.

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

Using policy rules

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

Rules for Windows, Linux, and macOS

- [All Volumes] selects all volumes on machines running Windows and all mounted volumes on machines running Linux or macOS.

Rules for Windows

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

Rules for Linux

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

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

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

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

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

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

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

Rules for macOS

- [Disk 1] Selects the first disk of the machine, including all volumes on that disk. To select another disk, type the corresponding number.

What does a disk or volume backup store?

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

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

Windows

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

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

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

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

MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup. This means that in operating systems starting with Windows Vista, 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.

14.3.2 Selecting files/folders

File-level backup is available for physical machines and virtual machines backed up by an agent installed in the guest system. Files and folders located on disks connected via the iSCSI protocol to a physical machine can also be backed up though there are [limitations](#) if you use Agent for VMware or Agent for Hyper-V for backing up data on the iSCSI-connected disks.

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

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

Direct selection

1. In **What to back up**, select **Files/folders**.
2. Specify **Items to back up**.
3. In **Select items for backup**, select **Directly**.

4. For each of the machines included in the protection plan:
 - a. Click **Select files and folders**.
 - b. Click **Local folder** or **Network folder**.

The share must be accessible from the selected machine.
 - c. Browse to the required files/folders or enter the path and click the arrow button. If prompted, specify the user name and password for the shared folder.

Backing up a folder with anonymous access is not supported.
 - d. Select the required files/folders.
 - e. Click **Done**.

Using policy rules

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

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

Selection rules for Windows

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

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

Selection rules for Linux

- Full path to a file or directory. For example, to back up **file.txt** on the volume **/dev/hda3** mounted on **/home/usr/docs**, specify **/dev/hda3/file.txt** or **/home/usr/docs/file.txt**.
 - **/home** selects the home directory of the common users.
 - **/root** selects the root user's home directory.

- /usr selects the directory for all user-related programs.
- /etc selects the directory for system configuration files.
- Templates:
 - [All Profiles Folder] selects **/home**. This is the folder where all user profiles are located by default.

Selection rules for macOS

- Full path to a file or directory.
- Templates:
 - [All Profiles Folder] selects **/Users**. This is the folder where all user profiles are located by default.

Examples:

- To back up **file.txt** on your desktop, specify **/Users/<username>/Desktop/file.txt**, where <username> is your user name.
- To back up all users' home directories, specify **/Users**.
- To back up the directory where the applications are installed, specify **/Applications**.

14.3.3 Selecting system state

System state backup is available for machines running Windows Vista and later.

To back up system state, in **What to back up**, select **System state**.

A system state backup is comprised of the following files:

- Task scheduler configuration
- VSS Metadata Store
- Performance counter configuration information
- MSSearch Service
- Background Intelligent Transfer Service (BITS)
- The registry
- Windows Management Instrumentation (WMI)
- Component Services Class registration database

14.3.4 Selecting ESXi configuration

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

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

A backup of an ESXi host configuration includes:

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

Prerequisites

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

Limitations

- ESXi configuration backup is not supported for VMware vSphere 7.0.
- 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 **Protect**.
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.

14.4 Continuous data protection (CDP)

Backups are usually performed with the regular but quite long time intervals due to performance reasons. If the system is suddenly damaged, the data changes between the last backup and the system failure will be lost.

The **Continuous data protection** functionality allows you to back up changes of the selected data between the scheduled backups on the continuous basis:

- By tracking changes in the specified files/folders
- By tracking changes of the files modified by the specified applications

You can select particular files for continuous data protection from the data selected for a backup. The system will back up every change of these files. You can recover these files to the last change time.

Currently, the **Continuous data protection** functionality is supported for the following operating systems:

- Windows 7 and later
- Windows Server 2008 R2 and later

The supported file system: NTFS only, local folders only (shared folders are not supported).

The **Continuous data protection** option is not compatible with the **Application backup** option.

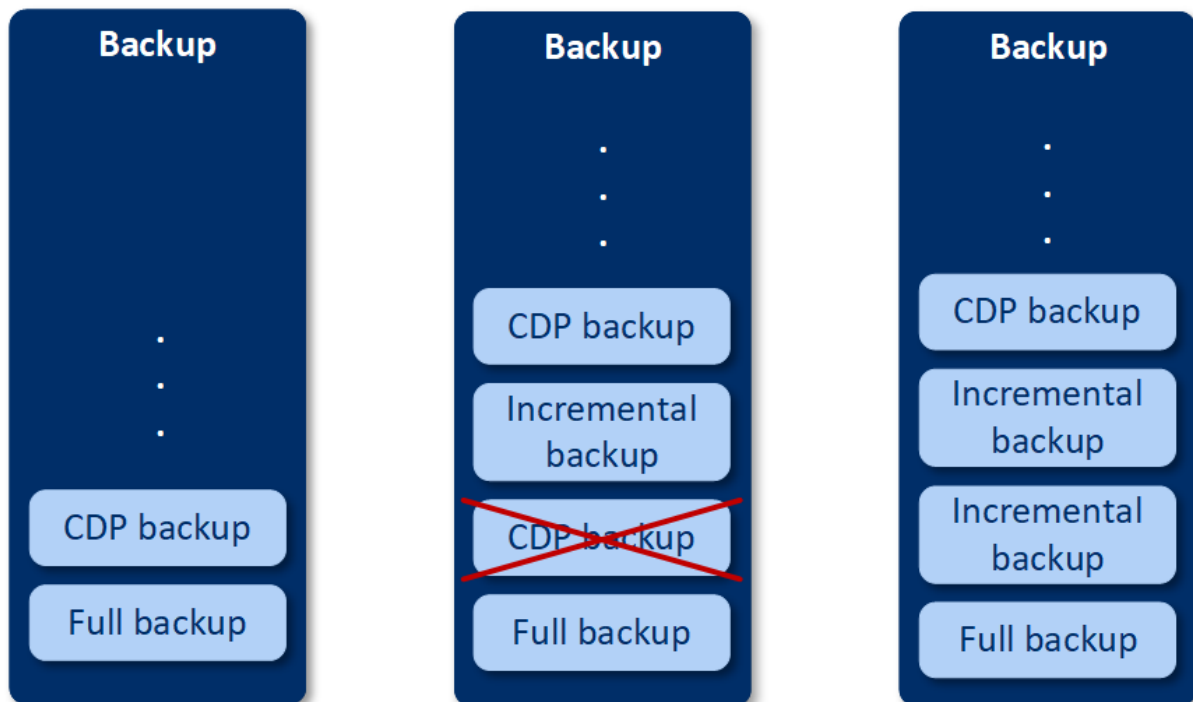
How it works

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 have to be created preliminarily.

When you first run the protection plan with the backup module and **Continuous data protection** enabled, a full backup is created first. Right after that the CDP backup for the selected or changed files/folders will be created. The CDP backup always contains data selected by you in the latest state. When you make changes to the selected files/folders, no new CDP backup is created, all changes are recorded to the same CDP backup.

When the time comes for a scheduled incremental backup, the CDP backup is dropped, and a new CDP backup is created after the incremental backup is done.

Thus, the CDP backup always stays as the latest backup in the backup chain having the latest actual state of the protected files/folders.



If you already have a protection plan with the backup module enabled and you decided to enable **Continuous data protection**, then the CDP backup will be created right after enabling the option as the backup chain already has full backups.

Supported data sources and destinations for continuous data protection

For continuous data protection proper work, you need to specify the following items for the following data sources:

What to back up	Items to back up
-----------------	------------------

Entire machine	Either files/folders or applications must be specified
Disks/volumes	Disks/volumes and either files/folders or applications must be specified
Files/folders	Files/folders must be specified Applications can be specified (not mandatory)

The following backup destinations are supported for continuous data protection:

- Local folder
- Network folder
- Location defined by a script
- Cloud storage
- Acronis Cyber Infrastructure

To protect the devices with continuous data protection

1. In the service console, [create a protection plan](#) with the **Backup** module enabled.
2. Enable the **Continuous data protection (CDP)** option.
3. Specify **Items to protect continuously**:
 - **Applications** (any file modified by the selected applications will be backed up). We recommend to use this option to protect your Office documents with the CDP backup.

Items to protect continuously

Choose files for continuous protection out of the data selected for backup. The software will back up every change of these files. You will be able to revert these files to the last change time.

Applications

Files/folders

Every file modified by the selected applications will be backed-up

Predefined application categories

☒ Office documents



☒ Engineering



☒ Imaging and video



Other applications

To add more applications, specify their paths in the format: C:\Program Files\Microsoft Office\Office16\WINWORD.EXE or *:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Add applications

OK

Cancel

- You can select the applications from the predefined categories or specify other applications by defining the path to the application executable file. Use one of the following formats:
C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
OR

*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

- **Files/folders** (any file modified in the specified location(s) will be backed up). We recommend to use this option to protect those files and folders that are constantly changing.

×

Items to protect continuously

Choose files for continuous protection out of the data selected for backup. The software will back up every change of these files. You will be able to revert these files to the last change time.

Applications

Files/folders

Every change of the selected files, and of files in the selected folders, will be backed up. ?

Machine to browse from: NIKITATIKHOB524 ▼ ⊕ Select files and folders

Add files/folders

OK

Cancel

1. **Machine to browse from** – specify the machine whose files/folders you want to select for continuous data protection.

Click **Select files and folders** to select files/folders on the specified machine.

Important

If you manually specify a whole folder whose files will be continuously backed up, use the mask, for example:

Correct path: D:\Data*

Incorrect path: D:\Data\

In the text field, you can also specify rules for selecting files/folders that will be backed up. For more details how to define rules, refer to "Selecting files/folders". When ready, click **Done**.

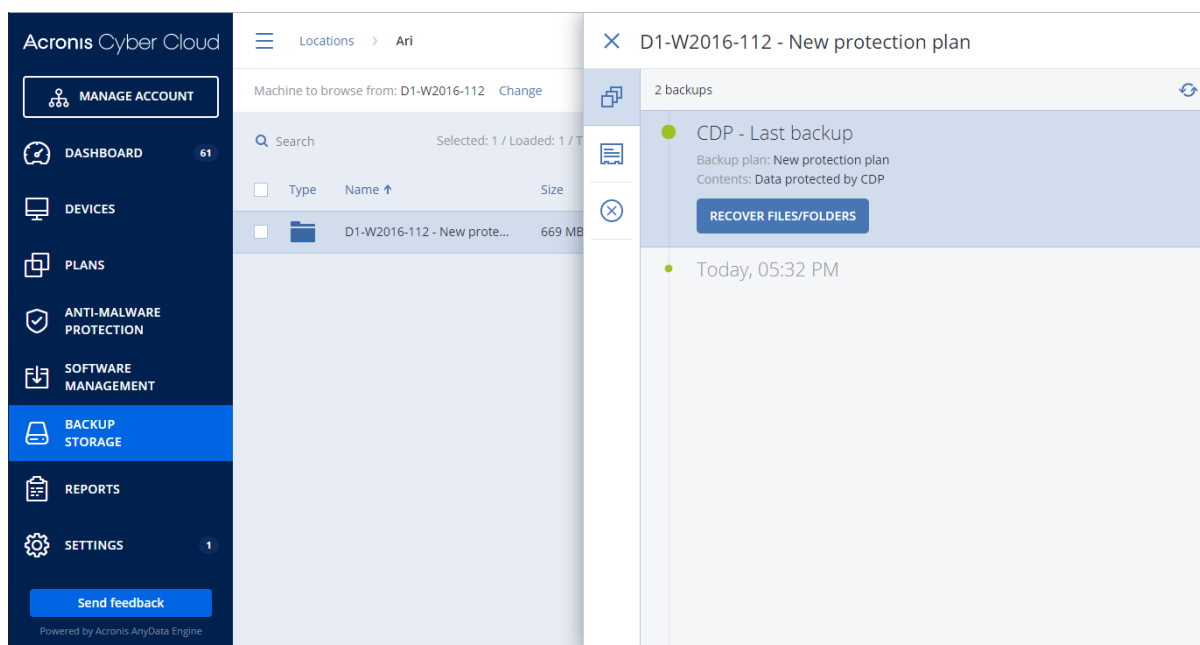
2. Click **Create**.

As a result, the protection plan with continuous data protection enabled will be assigned to the selected machine. After the first regular backup, the backups with the latest copy of the protected by CDP data will be created on the continuous basis. Both, the data defined via Applications and Files/folders, will be backed up.

Continuously backed-up data are retained according to the retention policy defined for the backup module.

How to distinguish backups that are protected on continuous basis

The backups that are backed up on continuous basis have the CDP prefix.



How to recover your entire machine to the latest state

If you want to be able to recover an entire machine to the latest state, you can use the **Continuous data protection (CDP)** option in the backup module of a protection plan.

You can recover either an entire machine or files/folders from a CDP backup. In first case, you will get an entire machine in the latest state, in the second case – files/folders in the latest state.

14.5 Selecting a destination

Click **Where to back up**, and then select one of the following:

- **Cloud storage**

Backups will be stored in the cloud data center.

- **Local folders**

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.

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

Verify that the nfs-utils package is installed on the Linux server where the 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.

Note

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

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

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

14.5.1 Advanced storage option

Note

This functionality is available only in the Advanced edition of the Cyber Protection service.

Defined by a script (available for machines running Windows)

You can store each machine's backups in a folder defined by a script. The software supports scripts written in JScript, VBScript, or Python 3.5. When deploying the protection plan, the software runs the script on each machine. The script output for each machine should be a local or network folder path. If a folder does not exist, it will be created (limitation: scripts written in Python cannot create folders on network shares). On the **Backup storage** tab, each folder is shown as a separate backup location.

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

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

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

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

14.5.2 About Secure Zone

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

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

Why use Secure Zone?

Secure Zone:

- Enables recovery of a disk to the same disk where the disk's backup resides.
- Offers a cost-effective and handy method for protecting data from software malfunction, virus attack, human error.

- Eliminates the need for a separate media or network connection to back up or recover the data. This is especially useful for roaming users.
- Can serve as a primary destination when using replication of backups.

Limitations

- Secure Zone cannot be organized on a Mac.
- Secure Zone is a partition on a basic disk. It cannot be organized on a dynamic disk or created as a logical volume (managed by LVM).
- Secure Zone is formatted with the FAT32 file system. Because FAT32 has a 4-GB file size limit, larger backups are split when saved to Secure Zone. This does not affect the recovery procedure and speed.
- Secure Zone does not support the single-file backup format¹. When you change the destination to Secure Zone in a protection plan that has the **Always incremental (Single-file)** backup scheme, the scheme is changed to **Weekly full, daily incremental**.

How creating Secure Zone transforms the disk

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

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

Important

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

¹A backup format, in which the initial full and subsequent incremental backups are saved to a single .tibx file. 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.

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.

Create Secure Zone

Secure Zone disk

Disk 1, 60.0 GB

Maximum possible size of Secure Zone: 35.9 GB

Secure Zone size:

20 GB

There is not enough unallocated space. Free space will be taken from all volumes where it is present.

[Select volumes](#)

Password protection

☐ Off

6. [Optional] Enable the **Password protection** switch and specify a password.
The password will be required to access the backups located in Secure Zone. Backing up to Secure Zone does not require a password, unless the backup is performed under bootable media.
7. Click **Create**.

The software displays the expected partition layout. Click **OK**.

8. Wait while the software creates Secure Zone.

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

How to delete Secure Zone

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

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

Resizing the volume from which the system is booted requires a reboot.

5. Click **Delete**.

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

14.6 Schedule

The schedule employs the time settings (including the time zone) of the operating system where the agent is installed. The time zone of Agent for VMware (Virtual Appliance) can be configured [in the agent's interface](#).

For example, if a protection plan is scheduled to run at 21:00 and applied to several machines located in different time zones, the backup will start on each machine at 21:00 local time.

14.6.1 Backup schemes

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

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

- **Always incremental (single-file)**

By default, backups are performed on a daily basis, Monday to Friday. You can select the time to run the backup.

If you want to change the backup frequency, move the slider, and then specify the backup schedule.

The backups use the single-file backup format¹.

¹A backup format, in which the initial full and subsequent incremental backups are saved to a single .tibx file. 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.

The first backup is full, which means that it is the most time-consuming. All subsequent backups are incremental and take significantly less time.

This scheme is highly recommended if the backup location is cloud storage. Other backup schemes may include multiple full backups that consume much time and network traffic.

This scheme is not available when backing up to Secure Zone.

- **Always full**

By default, backups are performed on a daily basis, Monday to Friday. You can select the time to run the backup.

If you want to change the backup frequency, move the slider, and then specify the backup schedule.

All backups are full.

- **Weekly full, Daily incremental**

By default, backups are performed on a daily basis, Monday to Friday. You can modify the days of the week and the time to run the backup.

A full backup is created once a week. All other backups are incremental. The day on which the full backup is created depends on the **Weekly backup** option (click the gear icon, then **Backup options > Weekly backup**).

- **Monthly full, Weekly differential, Daily incremental (GFS)**

By default, incremental backups are performed on a daily basis, Monday to Friday; differential backups are performed every Saturday; full backups are performed on the first day of each month. You can modify these schedules and the time to run the backup.

This backup scheme is displayed as a **Custom** scheme on the protection plan panel.

- **Custom**

Specify schedules for full, differential, and incremental backups.

Differential backup is not available when backing up SQL data, Exchange data, or system state.

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

14.6.2 Additional scheduling options

With any destination, you can do the following:

- Specify the backup start conditions, so that a scheduled backup is performed only if the conditions are met. For more information, refer to "Start conditions".
- Set a date range for when the schedule is effective. Select the **Run the plan within a date range** check box, and then specify the date range.
- Disable the schedule. While the schedule is disabled, the retention rules are not applied unless a backup is started manually.
- Introduce a delay from the scheduled time. The delay value for each machine is selected randomly and ranges from zero to the maximum value you specify. You may want to use this setting when backing up multiple machines to a network location, to avoid excessive network

load.

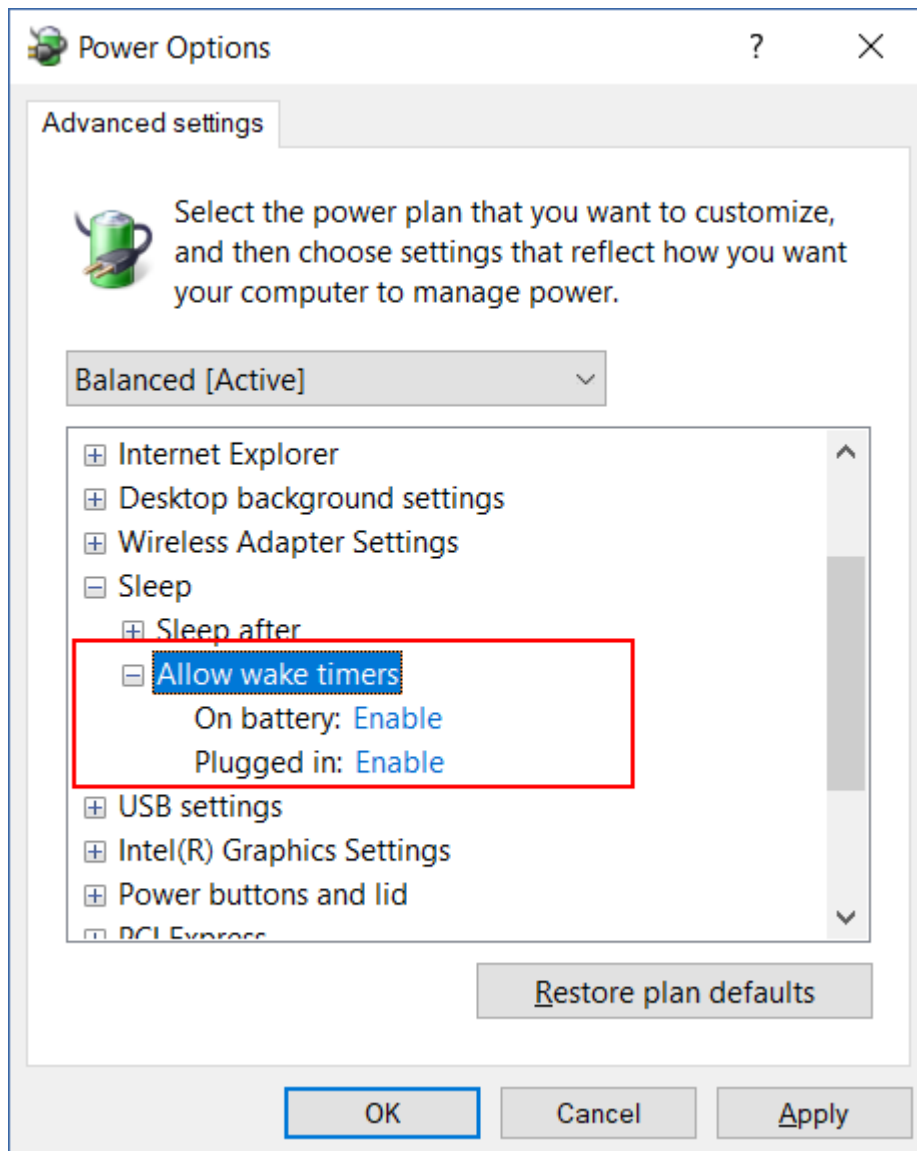
In the protection plan in the Backup module settings, go to **Backup options > Scheduling**. Select **Distribute backup start times within a time window**, and then specify the maximum delay.

The delay value for each machine is determined when the protection plan is applied to the machine and remains the same until you edit the protection plan and change the maximum delay value.

Note

This option is enabled by default, with the maximum delay set to 30 minutes.

- Click **Show more** to access the following options:
 - **If the machine is turned off, run missed tasks at the machine startup** (disabled by default)
 - **Prevent the sleep or hibernate mode during backup** (enabled by default)
This option is effective only for machines running Windows.
 - **Wake up from the sleep or hibernate mode to start a scheduled backup** (disabled by default)
This option is effective only for machines running Windows whose power plan has the **Allow wake timers** setting enabled.



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

14.6.3 Schedule by events

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

You can choose one of the following events:

- **Upon time since last backup**

This is the time since the completion of the last successful backup within the same protection plan. You can specify the length of time.

Note

Because the schedule is based on a successful backup event, if a backup fails, the scheduler will not run the job again until an operator runs the plan manually and the run completes successfully.

- **When a user logs on to the system**

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

- **When a user logs off the system**

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

Note

The backup will not run at a system shutdown because shutting down is not the same as logging off.

- **On the system startup**

- **On the system shutdown**

- **On Windows Event Log event**

You must specify the event properties.

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

WHAT TO BACK UP	Upon time since last backup	When a user logs on to the system	When a user logs off the system	On the system startup	On the system shutdown	On Windows Event Log event
Disks/volumes or files (physical machines)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Disks/volumes (virtual machines)	Windows, Linux	–	–	–	–	–
ESXi configuration	Windows, Linux	–	–	–	–	–
Microsoft 365 mailboxes	Windows	–	–	–	–	Windows
Exchange databases and mailboxes	Windows	–	–	–	–	Windows
SQL databases	Windows	–	–	–	–	Windows

On Windows Event Log event

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

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

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

Event properties

Log name

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

Event source

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

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

Event type

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

Event ID

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

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

Example: "Bad block" emergency backup

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

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

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

- **Log name:** System
- **Event source:** disk
- **Event type:** Error
- **Event ID:** 7

Important

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

14.6.4 Start conditions

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

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

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

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

WHAT TO BACK UP	Disks/volumes or files (physical machines)	Disks/volumes (virtual machines)	ESXi configuration	Microsoft 365 mailboxes	Exchange databases and mailboxes	SQL databases
User is idle	Windows	–	–	–	–	–
The backup location's host is available	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Users logged off	Windows	–	–	–	–	–
Fits the time interval	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Save battery power	Windows	–	–	–	–	–

Do not start when on metered connection	Windows	-	-	-	-	-
Do not start when connected to the following Wi-Fi networks	Windows	-	-	-	-	-
Check device IP address	Windows	-	-	-	-	-

User is idle

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

Example

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

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

As a result,

- (1) If the user becomes idle before 21:00, the backup will start at 21:00.
- (2) If the user becomes idle between 21:00 and 23:00, the backup will start immediately after the user becomes idle.
- (3) If the user is still active at 23:00, the backup will start at 23:00.

The backup location's host is available

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

This condition is effective for network folders, the cloud storage, and locations managed by a storage node.

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

Example

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

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

As a result:

- (1) If 21:00 comes and the host is available, the backup will start immediately.
- (2) If 21:00 comes but the host is unavailable, the backup will start on the next workday if the host is available.
- (3) If the host is never available on workdays at 21:00, the backup will never start.

Users logged off

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

Example

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

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

As a result:

- (1) If all users are logged off at 20:00, the backup will start at 20:00.
- (2) If the last user logs off between 20:00 and 23:00, the backup will start immediately after the user logs off.
- (3) If any user is still logged on at 23:00, the backup will start at 23:00.

Fits the time interval

Restricts a backup start time to a specified interval.

Example

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

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

As a result:

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

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

Save battery power

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

- **Do not start when on battery**
A backup will start only if the device is connected to a power source.
- **Start when on battery if the battery level is higher than**
A backup will start if the device is connected to a power source or if the battery level is higher than the specified value.

Example

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

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

As a result:

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

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

Do not start when on metered connection

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

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

Example

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

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

As a result:

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

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

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

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

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

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

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

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

Example

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

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

As a result:

- (1) If 21:00 comes and the machine is not connected to the specified network, the backup will start immediately.
- (2) If 21:00 comes and the machine is connected to the specified network, the backup will start on the next workday.
- (3) If the machine is always connected to the specified network on workdays at 21:00, the backup will never start.

Check device IP address

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

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

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

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

Example

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

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Check device IP address, Start if outside IP range, From:** <beginning of the VPN IP address range>, **To:** <end of the VPN IP address range>.
- Backup start conditions: **Wait until the conditions are met.**

As a result:

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

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

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

14.7 Retention rules

1. Click **How long to keep**.
2. In **Cleanup**, choose one of the following:
 - **By backup age** (default)
Specify how long to keep backups created by the protection plan. By default, the retention rules are specified for each backup set¹ separately. If you want to use a single rule for all backups, click **Switch to single rule for all backup sets**.
 - **By number of backups**
Specify the maximum number of backups to keep.
 - **By total size of backups**
Specify the maximum total size of backups to keep.
This setting is not available with the **Always incremental (single-file)** backup scheme or when backing up to the cloud storage.
 - **Keep backups indefinitely**
3. Select when to start the cleanup:
 - **After backup** (default)
The retention rules will be applied after a new backup is created.
 - **Before backup**
The retention rules will be applied before a new backup is created.

¹A 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.

This setting is not available when backing up Microsoft SQL Server clusters or Microsoft Exchange Server clusters.

14.7.1 What else you need to know

- The last backup created by the protection plan always will be kept, even if a retention rule violation is detected. Do not try to delete the only backup that you have by applying the retention rules before backup.
- If, according to the backup scheme and backup format, each backup is stored as a separate file, this file cannot be deleted until the lifetime of all its dependent (incremental and differential) backups expires. This requires extra space for storing backups whose deletion is postponed. Also, the backup age, number, or size of backups may exceed the values you specify. This behavior can be changed by using the "[Backup consolidation](#)" backup option.
- Retention rules are a part of a protection plan. They stop working for a machine's backups as soon as the protection plan is revoked from the machine, or deleted, or the machine itself is deleted from the Cyber Protection service. If you no longer need the backups created by the plan, delete them as described in "[Deleting backups](#)".

14.8 Replication

If you enable backup replication, each backup will be copied to another location immediately after creation. If earlier backups were not replicated (for example, the network connection was lost), the software also replicates all of the backups that appeared after the last successful replication. If backup replication is interrupted in the middle of a process, then on the next replication start the already replicated data will not be replicated again which allows reducing time loss.

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

14.8.1 Usage examples

- **Reliable disaster recovery**
Store your backups both on-site (for immediate recovery) and off-site (to secure the backups from local storage failure or a natural disaster).
- **Using the cloud storage to protect data from a natural disaster**
Replicate the backups to the cloud storage by transferring only the data changes.
- **Keeping only the latest recovery points**
Delete older backups from a fast storage according to retention rules, in order to not overuse expensive storage space.

14.8.2 Supported locations

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

- A local folder
- A network folder
- Secure Zone

You can replicate a backup to any of these locations:

- A local folder
- A network folder
- The cloud storage

To enable replication of backups

1. On the protection plan panel, click **Add location**.
The **Add location** control is shown only if replication is supported *from* the last selected location.
2. Specify the location where the backups will be replicated.
3. [Optional] In **How long to keep**, change the retention rules for the chosen location, as described in "[Retention rules](#)".
4. [Optional] Click the gear icon > **Performance and backup window**, and then set the backup window for the chosen location, as described in "[Performance and backup window](#)". These settings will define the replication performance.
5. [Optional] Repeat steps 1-4 for all locations where you want to replicate the backups. Up to five consecutive locations are supported, including the primary one.

14.9 Encryption

We recommend that you encrypt all backups that are stored in the cloud storage, especially if your company is subject to regulatory compliance.

Warning!

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

14.9.1 Encryption in a protection plan

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

For accounts in the Enhanced security mode, you cannot set the encryption password in a protection plan. You must set this password locally, on the protected device.

To specify the encryption settings in a protection plan

1. On the protection plan panel in the Backup module settings, enable the **Encryption** switch.
2. Specify and confirm the encryption password.
3. Select one of the following encryption algorithms:

- **AES 128** – the backups will be encrypted by using the Advanced Encryption Standard (AES) algorithm with a 128-bit key.
- **AES 192** – the backups will be encrypted by using the AES algorithm with a 192-bit key.
- **AES 256** – the backups will be encrypted by using the AES algorithm with a 256-bit key.

4. Click **OK**.

14.9.2 Encryption as a machine property

You can enforce encryption of backups or set a unique encryption password for a machine, regardless of the settings in its protection plan. The backups will be encrypted using the AES algorithm with a 256-bit key.

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

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

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

Important

Change the encryption settings on a machine only before its protection plan creates any backups. If you change the encryption settings later, the protection plan will fail and you will need a new protection plan to continue backing up this machine.

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

To save the encryption settings on a machine

1. Log on as an administrator (in Windows) or the root user (in Linux).
2. Run the following script:
 - In Windows: `<installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password <encryption_password>`
Here, `<installation_path>` is the protection agent installation path. By default, it is `%ProgramFiles%\BackupClient`.
 - In Linux: `/usr/sbin/acropsh -m manage_creds --set-password <encryption_password>`

To reset the encryption settings on a machine

1. Log on as an administrator (in Windows) or root user (in Linux).
2. Run the following script:

- In Windows: `<installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset`
Here, `<installation_path>` is the protection agent installation path. By default, it is **%ProgramFiles%\BackupClient**.
- In Linux: `/usr/sbin/acropsh -m manage_creds --reset`

To change the encryption settings by using the Cyber Protect Monitor

1. Log on as an administrator in Windows or macOS.
2. Click the Cyber Protect Monitor icon in the notification area (in Windows) or the menu bar (in macOS).
3. Click the gear icon.
4. Click **Encryption**.
5. Do one of the following:
 - Select **Set a specific password for this machine**. Specify and confirm the encryption password.
 - Select **Use encryption settings specified in the protection plan**.
6. Click **OK**.

14.9.3 How the encryption works

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

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

14.10 Notarization

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Notarization enables you to prove that a file is authentic and unchanged since it was backed up. We recommend that you enable notarization when backing up your legal document files or other files that require proved authenticity.

Notarization is available only for file-level backups. Files that have a digital signature are skipped, because they do not need to be notarized.

Notarization is *not* available:

- If the backup format is set to **Version 11**
- If the backup destination is Secure Zone

14.10.1 How to use notarization

To enable notarization of all files selected for backup (except for the files that have a digital signature), enable the **Notarization** switch when creating a protection plan.

When configuring recovery, the notarized files will be marked with a special icon, and you can [verify the file authenticity](#).

14.10.2 How it works

During a backup, the agent calculates the hash codes of the backed-up files, builds a hash tree (based on the folder structure), saves the tree in the backup, and then sends the hash tree root to the notary service. The notary service saves the hash tree root in the Ethereum blockchain database to ensure that this value does not change.

When verifying the file authenticity, the agent calculates the hash of the file, and then compares it with the hash that is stored in the hash tree inside the backup. If these hashes do not match, the file is considered not authentic. Otherwise, the file authenticity is guaranteed by the hash tree.

To verify that the hash tree itself was not compromised, the agent sends the hash tree root to the notary service. The notary service compares it with the one stored in the blockchain database. If the hashes match, the selected file is guaranteed to be authentic. Otherwise, the software displays a message that the file is not authentic.

14.11 Starting a backup manually

1. Select a machine that has at least one applied protection plan.
2. Click **Protect**.
3. If more than one protection plans are applied, select the protection plan.
4. Do one of the following:
 - Click **Run now**. An incremental backup will be created.
 - If the backup scheme includes several backup methods, you can choose the method to use. Click the arrow on the **Run now** button, and then select **Full**, **Incremental**, or **Differential**.

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

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

14.12 Default backup options

The default values of [backup options](#) exist at the company, unit, and user level. When a unit or a user account is created within a company or within a unit, it inherits the default values set for the company or for the unit.

Company administrators, unit administrators, and every user without the administrator rights can change a default option value against the pre-defined one. The new value will be used by default in all protection plans created at the respective level 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. Do one of the following:
 - To change the default value for the company, sign in to the service console as a company administrator.
 - To change the default value for a unit, sign in to the service console as an administrator of the unit.
 - To change the default value for yourself, sign in to the service console by using an account without the administrator rights.
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**.

14.13 Backup options

To modify the backup options, click **Change** next to **Backup options** in the Backup module of the protection plan.

14.13.1 Availability of the backup options

The set of available backup options depends on:

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

The following table summarizes the availability of the backup options.

	Disk-level backup			File-level backup			Virtual machines			SQL and Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hypervisor-V	Virtuozzo	Windows
Alerts	+	+	+	+	+	+	+	+	+	+
Backup consolidation	+	+	+	+	+	+	+	+	+	-

Backup file name	+	+	+	+	+	+	+	+	+	+
Backup format	+	+	+	+	+	+	+	+	+	+
Backup validation	+	+	+	+	+	+	+	+	+	+
Changed block tracking (CBT)	+	-	-	-	-	-	+	+	-	-
Cluster backup mode	-	-	-	-	-	-	-	-	-	+
Compression level	+	+	+	+	+	+	+	+	+	+
Error handling										
Re-attempt, if an error occurs	+	+	+	+	+	+	+	+	+	+
Do not show messages and dialogs while processing (silent mode)	+	+	+	+	+	+	+	+	+	+
Ignore bad sectors	+	+	+	+	+	+	+	+	+	-
Re-attempt, if an error occurs during VM snapshot creation	-	-	-	-	-	-	+	+	+	-
Fast incremental/differential backup	+	+	+	-	-	-	-	-	-	-
File-level backup snapshot	-	-	-	+	+	+	-	-	-	-
File filters	+	+	+	+	+	+	+	+	+	-
Forensic data	+	-	-	-	-	-	-	-	-	-
Log truncation	-	-	-	-	-	-	+	+	-	SQL only
LVM snapshotting	-	+	-	-	-	-	-	-	-	-
Mount points	-	-	-	+	-	-	-	-	-	-

Multi-volume snapshot	+	+	-	+	+	-	-	-	-	-
Performance and backup window	+	+	+	+	+	+	+	+	+	+
Physical Data Shipping	+	+	+	+	+	+	+	+	+	-
Pre/Post commands	+	+	+	+	+	+	+	+	+	+
Pre/Post data capture commands	+	+	+	+	+	+	-	-	-	+
Scheduling										
Distribute start times within a time window	+	+	+	+	+	+	+	+	+	+
Limit the number of simultaneously running backups	-	-	-	-	-	-	+	+	+	-
Sector-by-sector backup	+	+	-	-	-	-	+	+	+	-
Splitting	+	+	+	+	+	+	+	+	+	+
Task failure handling	+	+	+	+	+	+	+	+	+	+
Task start conditions	+	+	-	+	+	-	+	+	+	+
Volume Shadow Copy Service (VSS)	+	-	-	+	-	-	-	+	-	+
Volume Shadow Copy Service (VSS) for virtual machines	-	-	-	-	-	-	+	+	-	-
Weekly backup	+	+	+	+	+	+	+	+	+	+
Windows event log	+	-	-	+	-	-	+	+	-	+

14.13.2 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.

14.13.3 Backup consolidation

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

The preset is: **Disabled**.

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

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

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

Important

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


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

- The backup destination is the cloud storage.
- The backup scheme is set to **Always incremental (single-file)**.
- The [backup format](#) is set to **Version 12**.

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.

14.13.4 Backup file name

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

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

What is a backup file?

Each protection plan creates one or more files in the backup location, depending on which backup scheme and which [backup format](#) is 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
Version 12 backup format	One TIBX file per backup chain (a full or differential backup, and all incremental backups that depend on it). If the size of a file stored in a local or network (SMB) folder exceeds 200 GB, the file is split to 200-GB files by default.	

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). This makes sense if you want to see the custom names on the **Backup storage** tab.

Where can I see backup file names?

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

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

Limitations for backup file names

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

Default backup file name

The default backup file name for backups of entire physical and virtual machines, disks/volumes, files/folders, Microsoft SQL Server databases, Microsoft Exchange Server databases, and ESXi configuration is [Machine Name]-[Plan ID]-[Unique ID]A.

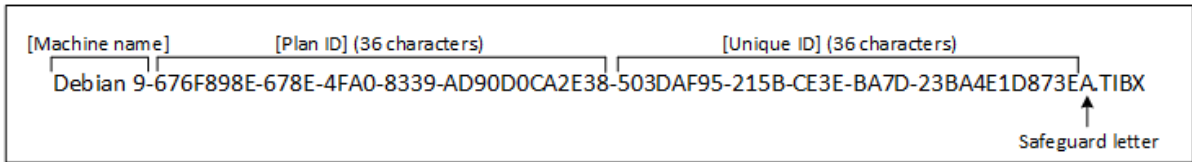
The default name for Exchange mailbox backups and Microsoft 365 mailbox backups created by a local Agent for Microsoft 365 is [Mailbox ID]_mailbox_[Plan ID]A.

The default name for cloud application backups created by cloud agents is [Resource Name]_[Resource Type]_[Resource ID]_[Plan ID]A.

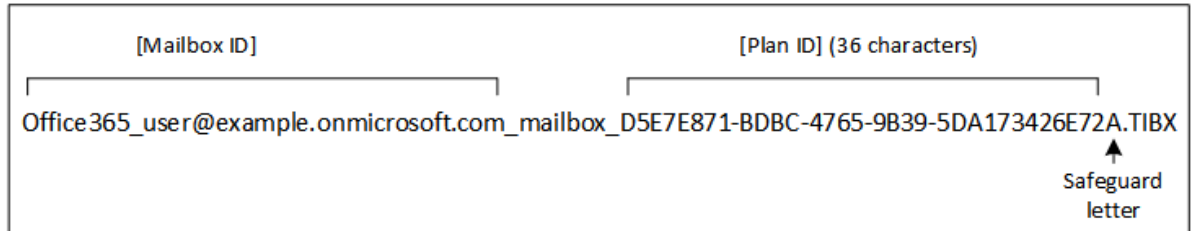
The default name consists of the following variables:

- [Machine Name] This variable is replaced with the name of the machine (the same name that is shown in the service console).
- [Plan ID], [Plan Id] These variables are replaced with the unique identifier of the protection plan. This value does not change if the plan is renamed.
- [Unique ID] This variable is replaced with the unique identifier of the selected machine. This value does not change if the machine is renamed.
- [Mailbox ID] This variable is replaced with the mailbox user's principal name (UPN).
- [Resource Name] This variable is replaced with the cloud data source name, such as the user's principal name (UPN), SharePoint site URL, or Shared drive name.
- [Resource Type] This variable is replaced with the cloud data source type, such as mailbox, 0365Mailbox, 0365PublicFolder, OneDrive, SharePoint, GDrive.
- [Resource ID] This variable is replaced with the unique identifier of the cloud data source. This value does not change if the cloud data source is renamed.
- "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 Microsoft 365 mailbox backups performed by a local agent.



Names without variables

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

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

```
MyBackup.tibx
```

For the version 12 format with other backup schemes:

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

Using variables

Besides the variables that are used by default, you can use the following variables:

- The [Plan name] variable, which is replaced with the name of the protection plan.
- The [Virtualization Server Type] variable, which is replaced with "vmwesx" if virtual machines are backed up by Agent for VMware or with "mshyperv" if virtual machines are backed up by Agent for Hyper-V.

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

Usage examples

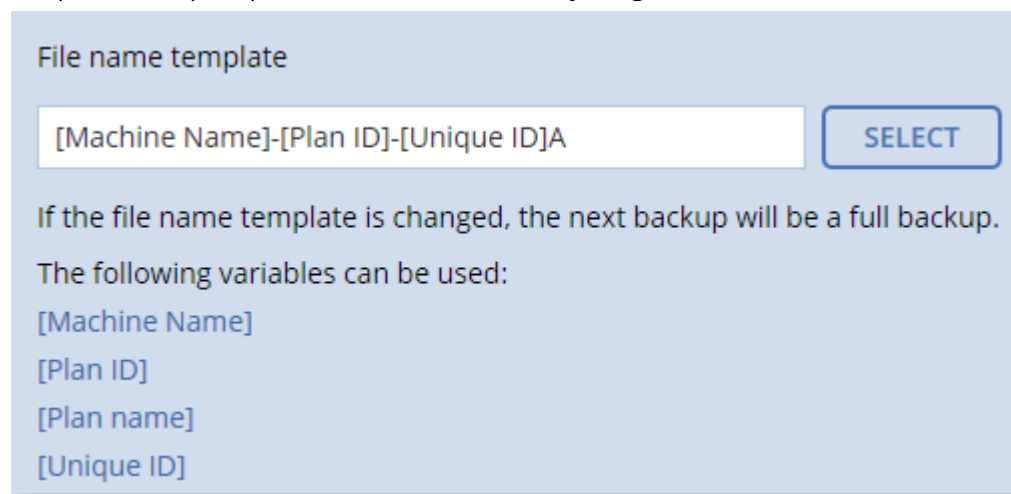
- **View user-friendly file names**

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 service 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. Just go this option, click **Select**, and select the required backup.

The **Select** 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.



The screenshot shows a dialog box titled "File name template". It contains a text input field with the value "[Machine Name]-[Plan ID]-[Unique ID]A" and a "SELECT" button to its right. Below the input field, there is a message: "If the file name template is changed, the next backup will be a full backup." followed by "The following variables can be used:". A list of variables is provided: "[Machine Name]", "[Plan ID]", "[Plan name]", and "[Unique ID]".

Note

The **Select** button is only available for protection plans that are created for and applied to a single device.

14.13.5 Backup format

The **Backup format** option defines the format of the backups created by the protection plan. This option is available only for protection plans that already use the version 11 backup format. If this is the case, you can change the backup format to version 12. After you switch the backup format to version 12, the option becomes unavailable.

- **Version 11**

The legacy format preserved for backward compatibility.

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.

- **Version 12**

The backup format that was introduced in Acronis Backup 12 for faster 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.

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. 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
Version 12 backup format	One TIBX file per backup chain (a full or differential backup, and all incremental backups that depend on it). If the size of a file stored in a local or network (SMB) folder exceeds 200 GB, the file is split to 200-GB files by default.	

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.

In-archive deduplication

The TIBX backup format of version 12 supports in-archive deduplication that brings the following advantages:

- Significantly reduced backup size, with built-in block-level deduplication for any type of data
- Efficient handling of hard links ensures that there are no storage duplicates
- Hash-based chunking

Note

In-archive deduplication is enabled by default for all backups in the TIBX format. You do not have to enable it in the backup options, and you cannot disable it.

14.13.6 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.

Note

Depending on the settings chosen by your service provider, validation might not be available when backing up to the cloud storage.

14.13.7 Changed block tracking (CBT)

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

The preset is: **Enabled**.

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

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

14.13.8 Cluster backup mode

Note

The availability of this feature depends on the service quotas that are enabled for your account.

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

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

Microsoft SQL Server

This option determines the backup mode for SQL Server Always On Availability Groups (AAG). For this option to be effective, Agent for SQL must be installed on all of the AAG nodes. For more information about backing up Always On Availability Groups, refer to ["Protecting Always On Availability Groups \(AAG\)"](#).

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

You can choose one of the following:

- **Secondary replica if possible**

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

- **Secondary replica**

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

- **Primary replica**

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

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

Microsoft Exchange Server

This option determines the backup mode for Exchange Server Database Availability Groups (DAG). For this option to be effective, Agent for Exchange must be installed on all of the DAG nodes. For

more information about backing up Database Availability Groups, refer to "Protecting Database Availability Groups (DAG)".

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

You can choose one of the following:

- **Passive copy if possible**

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

- **Passive copy**

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

- **Active copy**

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

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

14.13.9 Compression level

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

The preset is: **Normal**.

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

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

14.13.10 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 during a running backup, the software 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.

However, if the backup destination is not available when the backup starts, only 10 attempts will be made.

Cloud storage

If the cloud storage is selected as a backup destination, the option value is automatically set to **Enabled. Number of attempts: 300. Interval between attempts: 30 seconds.**

In this case, the actual number of attempts is unlimited, but the timeout before the backup failure is calculated as follows: (300 seconds + **Interval between attempts**) * (**Number of attempts** + 1).

Examples:

- With the default values, the backup will fail after (300 seconds + 30 seconds) * (300 + 1) = 99330 seconds, or ~27.6 hours.
- If you set **Number of attempts** to 1 and **Interval between attempts** to 1 second, the backup will fail after (300 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.

14.13.11 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.

14.13.12 File filters

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

File filters are available for disk-level backups, entire machine backups, and file-level backups, unless stated otherwise.

To enable file filters

1. Select the data to back up.
2. Click **Change** next to **Backup options**.
3. Select **File filters**.
4. Use any of the options described below.

Exclude files matching specific criteria

There are two options that function in an inverse manner.

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

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

Note

This filter is not effective for file-level backup if **Version 11** is selected in **Backup format** and the backup destination is NOT cloud storage.

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

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

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

Criteria

- **Full path**

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

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

- **Name**

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

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

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

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

[Only for backups in the **Version 12** format] The double asterisk (**) substitutes for zero or more characters in a file name and path, including the slash character. For example, the criterion ****/Docs/**/*.txt** matches all txt files in all subfolders of all folders **Docs**.

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

Exclude hidden files and folders

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

Exclude system files and folders

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

Note

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

14.13.13 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.

14.13.14 Forensic data

Malicious activities on a machine can be carried out by viruses, malware, and ransomware. The other case that may require investigations is stealing or changing data on a machine by means of different programs. Such activities may need to be investigated but it is possible only if you keep digital evidence on a machine to investigate. Unfortunately, evidence (files, traces, and so on) may be deleted or a machine may become unavailable.

The backup option called **Forensic data** allows you to collect digital evidence that can be used in forensic investigations. The following items can be used as digital evidence: a snapshot of the unused disk space, memory dumps, and a snapshot of running processes. The **Forensic data** functionality is available only for an entire machine backup.

Currently, the **Forensic data** option is available only for Windows machines with the following OS versions:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Note

- After a protection plan with the Backup module is applied to a machine, the forensic data settings cannot be modified. To use different forensic data settings, create a new protection plan.
 - Backups with forensic data collection are not supported for machines that are connected to your network through VPN and do not have direct access to the Internet.
-

The supported locations for backups with forensic data are:

- Cloud storage
- Local folder

Note

1. The local folder is supported only on an external hard disk connected via USB.
 2. Local dynamic disks are not supported as a location for forensic backups.
-

- Network folder

Backups with forensic data are automatically notarized. Forensic backups allow investigators to analyze disk areas that are usually not included in a regular disk backup.

Forensic backup process

The system performs the following during a forensic backup process:

1. Collects raw memory dump and the list of running processes.
2. Automatically reboots a machine into the bootable media.
3. Creates the backup that includes both the occupied and unallocated space.
4. Notarizes the backed-up disks.
5. Reboots into the live operating system and continues plan execution (for example, replication, retention, validation and other).

To configure forensic data collection

1. In the service console, go to **Devices > All devices**. Alternatively, the protection plan can be created from the **Plans** tab.
2. Select the device and click **Protect**.
3. In the protection plan, enable the **Backup** module.
4. In **What to back up**, select **Entire machine**.
5. In **Backup options**, click **Change**.
6. Find the **Forensic data** option.
7. Enable **Collect forensic data**. The system will automatically collect a memory dump and create a snapshot of running processes.

Note

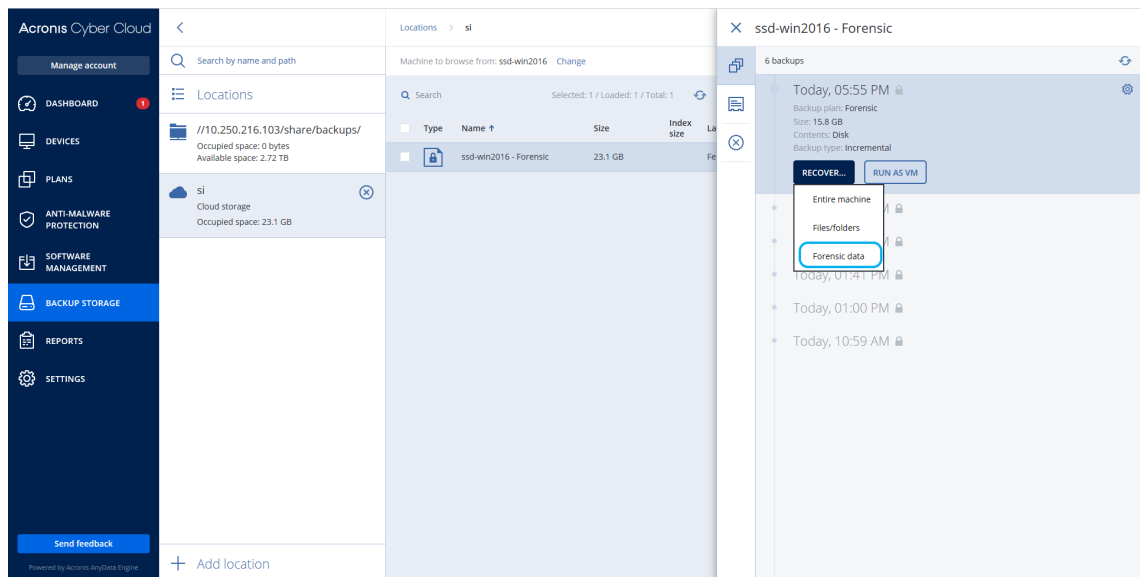
Full memory dump may contain sensitive data such as passwords.

- Specify the location.
- Click **Run Now** to perform a backup with forensic data right away or wait until the backup is created according to the schedule.
- Go to **Dashboard > Activities**, verify that the backup with forensic data was successfully created.

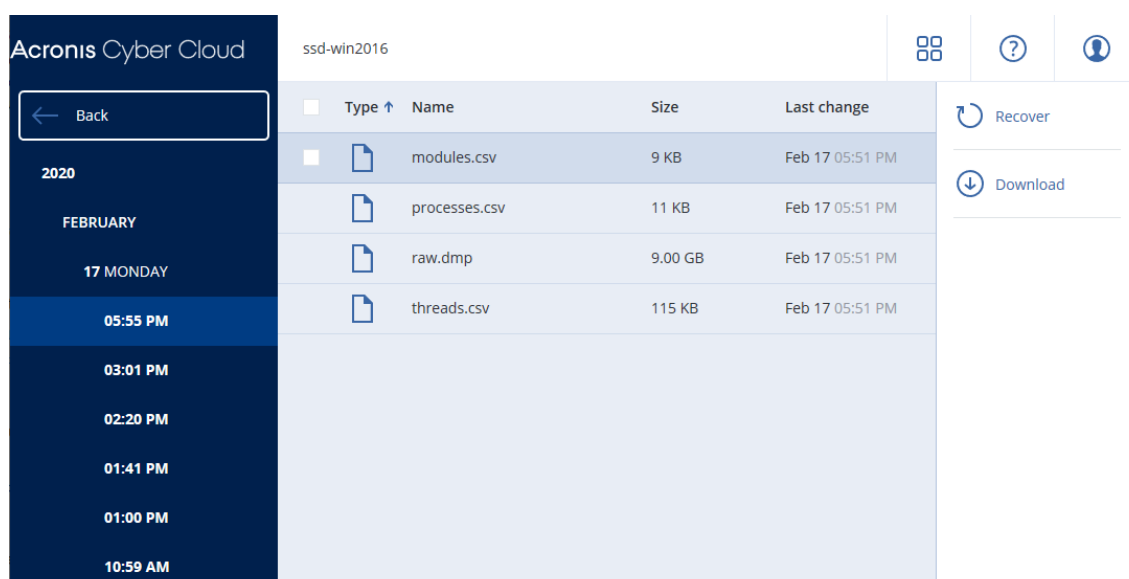
As a result, backups will include forensic data and you will be able to get them and analyze. Backups with forensic data are marked and can be filtered among other backups in **Backup storage > Locations** by using the **Only with forensic data** option.

How to get forensic data from a backup?

- In the service console, go to **Backup storage**, select the location with backups that include forensic data.
- Select the backup with forensic data and click **Show backups**.
- Click **Recover** for the backup with forensic data.
 - To get only the forensic data, click **Forensic data**.



The system will show a folder with forensic data. Select a memory dump file or any other forensic file and click **Download**.



- To recover a full forensic backup, click **Entire machine**. The system will recover the backup without the boot mode. Thus, it will be possible to check that the disk was not changed.

You can use the provided memory dump with several of third-party forensic software, for example, use Volatility Framework at <https://www.volatilityfoundation.org/> for further memory analysis.

Notarization of backups with forensic data

To ensure that a backup with forensic data is exactly the image that was taken and it was not compromised, the backup module provides the notarization of backups with forensic data.

How it works

Notarization enables you to prove that a disk with forensic data is authentic and unchanged since it was backed up.

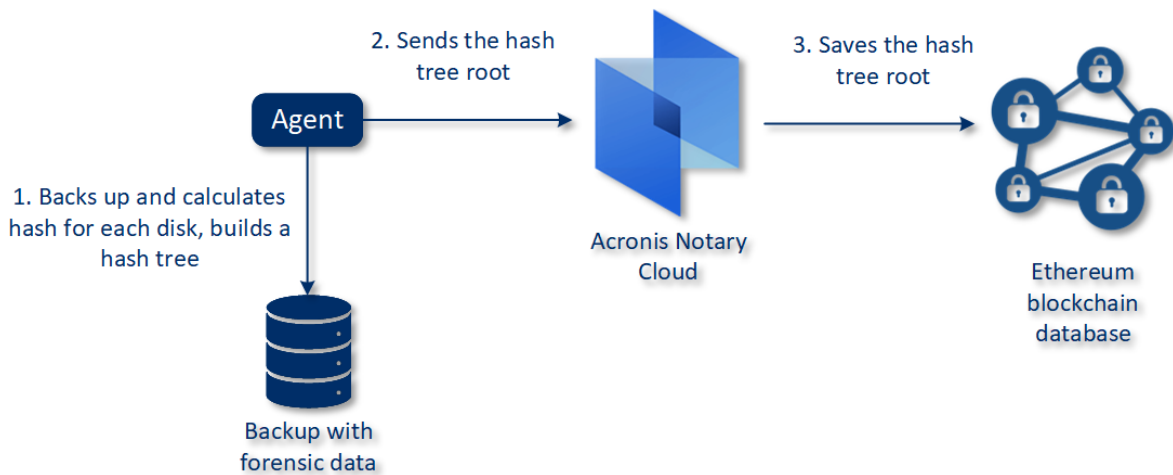
During a backup, the agent calculates the hash codes of the backed-up disks, builds a hash tree, saves the tree in the backup, and then sends the hash tree root to the notary service. The notary service saves the hash tree root in the Ethereum blockchain database to ensure that this value does not change.

When verifying the authenticity of the disk with forensic data, the agent calculates the hash of the disk, and then compares it with the hash that is stored in the hash tree inside the backup. If these hashes do not match, the disk is considered not authentic. Otherwise, the disk authenticity is guaranteed by the hash tree.

To verify that the hash tree itself was not compromised, the agent sends the hash tree root to the notary service. The notary service compares it with the one stored in the blockchain database. If the hashes match, the selected disk is guaranteed to be authentic. Otherwise, the software displays a message that the disk is not authentic.

The scheme below shows shortly the notarization process for backups with forensic data.

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.

The tool "tibxread" for getting the backed-up data

Cyber Protection provides the tool, called `tibxread`, for manual check of the backed-up disk integrity. The tool allows you to get data from a backup and calculate hash of the specified disk. The tool is installed automatically with the following components: Agent for Windows, Agent for Linux, and Agent for Mac.

The installation path: the same folder as the agent has (for example, `C:\Program Files\BackupClient\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
- 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> – a backup GUID.

<date> – a creation date of the backup. Format is “DD.MM.YYYY HH24:MM:SS”. In local timezone by default (can be changed by using the --utc option).

Output example:

```
GUID    Date    Date timestamp
-----
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Lists content in a recovery point.

SYNOPSIS:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Output template:

```
Disk    Size    Notarization status
-----
<number> <size> <notarization_status>
```

<number> – identifier of the disk.

<size> – size in bytes.

<notarization_status> – the following statuses are possible: Without notarization, Notarized, Next backup.

Output example:

Disk	Size	Notary status
1	123123465798	Notarized
2	123123465798	Notarized

get content

Writes content of the specified disk in the recovery point to the standard output (stdout).

SYNOPSIS:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -  
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Options

```
--loc=URI  
--arc=BACKUP_NAME  
--password  
--backup=RECOVERY_POINT_ID  
--disk=DISK_NUMBER  
--raw  
--log=PATH  
--progress
```

calculate hash

Calculates the hash of the specified disk in the recovery point by using the SHA-256 algorithm and writes it to the stdout.

SYNOPSIS:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_  
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Options

```
--loc=URI  
--arc=BACKUP_NAME  
--password  
--backup=RECOVERY_POINT_ID  
--disk=DISK_NUMBER  
--raw  
--log=PATH
```

Options description

Option	Description
--arc=BACKUP_NAME	The backup file name that you can get from the backup properties in the web console. The backup file must be specified with the extension .tibx.
--backup=RECOVERY_POINT_ID	The recovery point identifier
--disk=DISK_NUMBER	Disk number (the same as was written to the output of the "get content" command)
--loc=URI	<p>A backup location URI. The possible formats of the "--loc" option are:</p> <ul style="list-style-type: none"> 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] <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 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 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	<p>Hides the headers (2 first rows) in the command output. It is used when the command output should be parsed.</p> <p>Output example without "--raw":</p> <pre> GUID Date Date timestamp ----- 516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925 </pre> <p>Output with "--raw":</p>

	<div> 516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925 </div>
--utc	Shows dates in UTC
--progress	Shows progress of the operation. For example: <div> 1% 2% 3% 4% ... 100% </div>

14.13.15 Log truncation

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

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

The preset is: **Enabled**.

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

14.13.16 LVM snapshotting

This option is effective only for physical machines.

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

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

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

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

14.13.17 Mount points

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

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

- If such folder (a parent folder) is selected for backup, and the **Mount points** option is enabled, all files located on the mounted volume will be included in the backup. If the **Mount points** option is disabled, the mount point in the backup will be empty.

During recovery of a parent folder, the mount point content will or will not be recovered, depending on whether the [Mount points option for recovery](#) is enabled or disabled.

- If you select the mount point directly, or select any folder within the mounted volume, the selected folders will be considered as ordinary folders. They will be backed up regardless of the state of the **Mount points** option and recovered regardless of the state of the [Mount points option for recovery](#).

The preset is: **Disabled**.

Note

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

Example

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

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

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

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

14.13.18 Multi-volume snapshot

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

This option applies to disk-level backup. This option also applies to file-level backup when the file-level backup is performed by taking a snapshot. (The ["File-level backup snapshot"](#) 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**.
- 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.

14.13.19 Performance and backup window

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

This option is not available for backups executed by the cloud agents, such as website backups or backups of servers located on the cloud recovery site.

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

This option is effective only for the backup and backup replication processes. Post-backup commands and other operations included in a protection plan (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, corresponds to **Below normal**).
- Output speed: **Unlimited**.

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

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

Backup window

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

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

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

Performance and backup window settings

No

Yes

AM

00

03

06

09

PM

12

03

06

09

AM

00

Sun

Mon

Tue

Wed

Thu

Fri

Sat

CPU priority

Low

Output speed

-

100

+

%

CPU priority

Low

Output speed

-

25

+

%

No backing up

CPU priority

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

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

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



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

- This setting works only if the agent is running in Windows.

- 213

14.13.20 Physical Data Shipping

This option is effective if the backup destination is the cloud storage and the [backup format](#) is set to **Version 12**.

This option is effective for disk-level backups and file backups created by Agent for Windows, Agent for Linux, Agent for Mac, Agent for VMware, Agent for Hyper-V, and Agent for Virtuozzo.

This option determines whether the first full backup created by the protection plan will be sent to the cloud storage on a hard disk drive by using the Physical Data Shipping service. The subsequent incremental backups can be performed over the network.

The preset is: **Disabled**.

About the Physical Data Shipping service

The Physical Data Shipping service web interface is available only to administrators.

For detailed instructions about using the Physical Data Shipping service and the order creation tool, refer to the Physical Data Shipping Administrator's Guide. To access this document in the Physical Data Shipping service web interface, click the question mark icon.

Overview of the physical data shipping process

1. Create a new protection plan. In this plan, enable the **Physical Data Shipping** backup option. You can back up directly to the drive or back up to a local or a network folder, and then copy/move the backup(s) to the drive.

Important

Once the initial full backup is done, the subsequent backups must be performed by the same protection plan. Another protection plan, even with the same parameters and for the same machine, will require another Physical Data Shipping cycle.

2. After the first backup is complete, use the Physical Data Shipping service web interface to download the order creation tool and create the order.
To access this web interface, log in to the management portal, click **Overview > Usage**, and then click **Manage service** under **Physical Data Shipping**.
3. Package the drives and ship them to the data center.

Important

Ensure that you follow the packaging instructions provided in the [Physical Data Shipping Administrator's Guide](#).

4. Track the order status by using the Physical Data Shipping service web interface. Note that the subsequent backups will fail until the initial backup is uploaded to the cloud storage.

14.13.21 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:

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

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

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	Selected	Selected	Cleared	Cleared

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

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

Note

If a script fails due to a conflict related to a required library version in Linux, exclude the LD_LIBRARY_PATH and LD_PRELOAD environmental variables, by adding the following lines in your script:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

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**.

14.13.22 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

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	Perform the data capture after the command is executed despite execution failure or	N/A	Perform the data capture concurrently with the command and irrespective of the command

	the backup if the command execution fails.	success.		execution result.
--	--	----------	--	-------------------

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

Note

If a script fails due to a conflict related to a required library version in Linux, exclude the LD_LIBRARY_PATH and LD_PRELOAD environmental variables, by adding the following lines in your script:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Post-data capture command

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

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

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

	successfully executed.	failure or success.		command execution result.
--	------------------------	---------------------	--	---------------------------

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

14.13.23 Scheduling

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

The preset is: **Distribute backup start times within a time window. Maximum delay: 30 minutes.**

You can select one of the following:

- **Start all backups exactly as scheduled**

Backups of physical machines will start exactly as scheduled. Virtual machines will be backed up one by one.

- **Distribute start times within a time window**

Backups of physical machines will start with a delay from the scheduled time. The delay value for each machine is selected randomly and ranges from zero to the maximum value you specify. You may want to use this setting when backing up multiple machines to a network location, to avoid excessive network load. The delay value for each machine is determined when the protection plan is applied to the machine and remains the same until you edit the protection plan and change the maximum delay value.

Virtual machines will be backed up one by one.

- **Limit the number of simultaneously running backups by**

This option is available only when a protection plan is applied to multiple virtual machines. This option defines how many virtual machines an agent can back up simultaneously when executing the given protection plan.

If, according to the protection plan, an agent has to start backing up multiple machines at once, it will choose two machines. (To optimize the backup performance, the agent tries to match machines stored on different storages.) Once any of the two backups is completed, the agent chooses the third machine and so on.

You can change the number of virtual machines for an agent to simultaneously back up. The maximum value is 10. However, if the agent executes multiple protection plans that overlap in time, the numbers specified in their options are added up. You can [limit the total number of virtual machines](#) that an agent can back up simultaneously, no matter how many protection plans are running.

Backups of physical machines will start exactly as scheduled.

14.13.24 Sector-by-sector backup

The option is effective only for disk-level backup.

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

The preset is: **Disabled**.

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.

14.13.25 Splitting

This option enables you to select the method of splitting of large backups into smaller files.

The preset is:

- If the backup location is a local or network (SMB) folder, and the backup format is Version 12:
Fixed size - 200 GB

This setting allows the backup software to work with large volumes of data on the NTFS file system, without negative effects caused by file fragmentation.

- Otherwise: **Automatic**

The following settings are available:

- **Automatic**

A backup will be split if it exceeds the maximum file size supported by the file system.

- **Fixed size**

Enter the desired file size or select it from the drop-down list.

14.13.26 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**.

14.13.27 Task start conditions

This option is effective in Windows and Linux operating systems.

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

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

Wait until the conditions from the schedule are met

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

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

Skip the task execution

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

14.13.28 Volume Shadow Copy Service (VSS)

This option is effective only for Windows operating systems.

The option defines whether a Volume Shadow Copy Service (VSS) provider has to notify VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications; in particular, completion of all database transactions at the moment of taking the data snapshot by the backup software. Data consistency, in turn, ensures that the application will be recovered in the correct state and become operational immediately after recovery.

The preset is: **Enabled. Automatically select snapshot provider.**

You can select one of the following:

- **Automatically select snapshot provider**

Automatically select among the hardware snapshot provider, software snapshot providers, and Microsoft Software Shadow Copy provider.

- **Use Microsoft Software Shadow Copy provider**

We recommend choosing this option when backing up application servers (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint, or Active Directory).

Disable this option if your database is incompatible with VSS. Snapshots are taken faster, but data consistency of the applications whose transactions are not completed at the time of taking a snapshot cannot be guaranteed. You may use [Pre/Post data capture commands](#) to ensure that the data is backed up in a consistent state. For instance, specify pre-data capture commands that will suspend the database and flush all caches to ensure that all transactions are completed; and specify post-data capture commands that will resume the database operations after the snapshot is taken.

Note

If this option is enabled, files and folders that are specified in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** registry key are not backed up. In particular, offline Outlook Data Files (.ost) are not backed up because they are specified in the **OutlookOST** value of this key.

Enable VSS full backup

If this option is enabled, logs of Microsoft Exchange Server and of other VSS-aware applications (except for Microsoft SQL Server) will be truncated after each successful full, incremental or differential disk-level backup.

The preset is: **Disabled**.

Leave this option disabled in the following cases:

- If you use Agent for Exchange or third-party software for backing up the Exchange Server data. This is because the log truncation will interfere with the consecutive transaction log backups.
- If you use third-party software for backing up the SQL Server data. The reason for this is that the third-party software will take the resulting disk-level backup for its "own" full backup. As a result, the next differential backup of the SQL Server data will fail. The backups will continue failing until the third-party software creates the next "own" full backup.
- If other VSS-aware applications are running on the machine and you need to keep their logs for any reason.

Enabling this option does not result in the truncation of Microsoft SQL Server logs. To truncate the SQL Server log after a backup, enable the [Log truncation](#) backup option.

14.13.29 Volume Shadow Copy Service (VSS) for virtual machines

This option defines whether quiesced snapshots of virtual machines are taken. To take a quiesced snapshot, the backup software applies VSS inside a virtual machine by using VMware Tools, Hyper-V Integration Services, Virtuozzo Guest Tools, or Red Hat Virtualization Guest Tools, respectively.

The preset is: **Enabled**.

If this option is enabled, transactions of all VSS-aware applications running in a virtual machine are completed before taking snapshot. If a quiesced snapshot fails after the number of re-attempts specified in the "[Error handling](#)" option, and application backup is disabled, a non-quiesced snapshot is taken. If application backup is enabled, the backup fails.

If this option is disabled, a non-quiesced snapshot is taken. The virtual machine will be backed up in a crash-consistent state.

Note

This option does not affect Scale Computing HC3 virtual machines. For them, quiescing depends on whether the Scale tools are installed on the virtual machine.

14.13.30 Weekly backup

This option determines which backups are considered "weekly" in retention rules and backup schemes. A "weekly" backup is the first backup created after a week starts.

The preset is: **Monday**.

14.13.31 Windows event log

This option is effective only in Windows operating systems.

This option defines whether the agents have to log events of the backup operations in the Application Event Log of Windows (to see this log, run eventvwr.exe or select **Control Panel > Administrative tools > Event Viewer**). You can filter the events to be logged.

The preset is: **Disabled**.

14.14 Recovery

14.14.1 Recovery cheat sheet

The following table summarizes the available recovery methods. Use the table to choose a recovery method that best fits your need.

Note

Recovery through the web interface is not available for tenants in the Enhanced security mode.

What to recover	Recovery method
Physical machine (Windows or Linux)	Using the web interface Using bootable media
Physical machine (Mac)	Using bootable media
Virtual machine (VMware, Hyper-V, Red Hat Virtualization (oVirt), or Scale Computing HC3)	Using the web interface Using bootable media
Virtual machine or container (Virtuozzo, Virtuozzo Hybrid Server, or Virtuozzo Hybrid Infrastructure)	Using the web interface
ESXi configuration	Using bootable media
Files/Folders	Using the web interface

	Downloading files from the cloud storage Using bootable media Extracting files from local backups
System state	Using the web interface
SQL databases	Using the web interface
Exchange databases	Using the web interface
Exchange mailboxes	Using the web interface
Websites	Using the web interface
Microsoft 365	
Mailboxes (local Agent for Microsoft 365)	Using the web interface
Mailboxes (cloud Agent for Microsoft 365)	Using the web interface
Public folders	Using the web interface
OneDrive files	Using the web interface
SharePoint Online data	Using the web interface
Google Workspace	
Mailboxes	Using the web interface
Google Drive files	Using the web interface
Shared drive files	Using the web interface

Note for Mac users

- Starting with 10.11 El Capitan, certain system files, folders, and processes are flagged for protection with an extended file attribute com.apple.rootless. This feature is called System Integrity Protection (SIP). The protected files include preinstalled applications and most of the folders in /system, /bin, /sbin, /usr.
The protected files and folders cannot be overwritten during a recovery under the operating system. If you need to overwrite the protected files, perform the recovery under bootable media.
- Starting with macOS Sierra 10.12, rarely used files can be moved to iCloud by the Store in Cloud feature. Small footprints of these files are kept on the file system. These footprints are backed up

instead of the original files.

When you recover a footprint to the original location, it is synchronized with iCloud and the original file becomes available. When you recover a footprint to a different location, it cannot be synchronized and the original file will be unavailable.

14.14.2 Safe recovery

A backed-up OS image can have malware that can reinfect a machine after recovery.

The safe recovery functionality allows you to prevent recurrence of infections by using the integrated [antimalware scanning](#) and malware deletion during the recovery process.

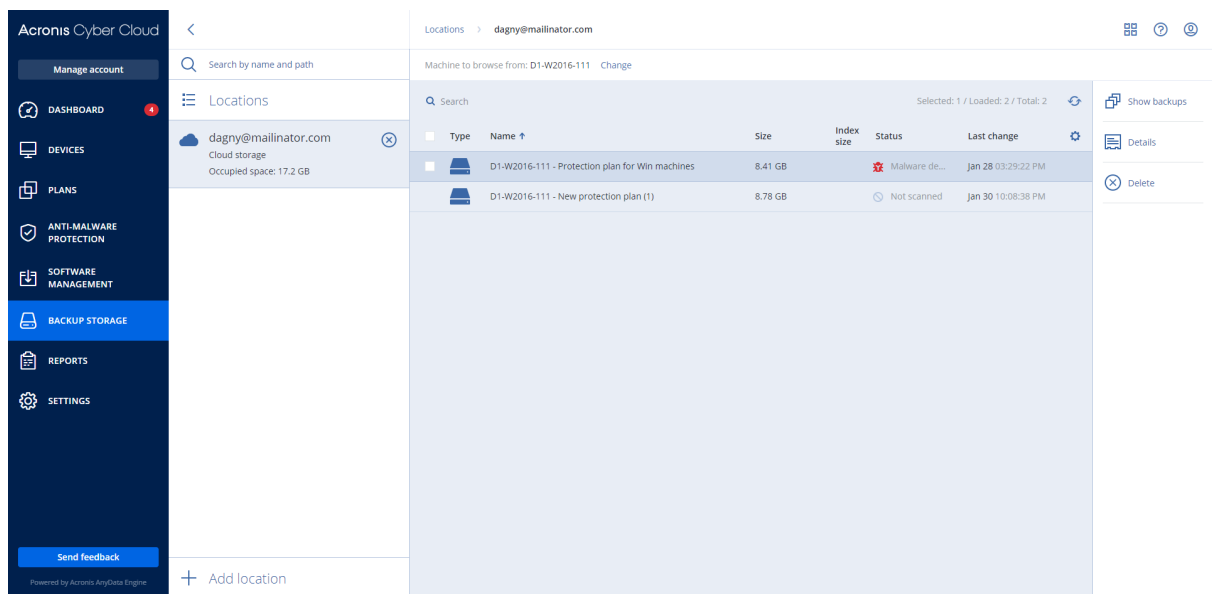
Limitations:

- Safe recovery is supported only for physical or virtual Windows machines with Agent for Windows installed inside the machine.
- The supported backup types are "Entire machine" or "Disks/volumes" backups.
- Safe recovery is supported only for the volumes with NTFS file system. Non-NTFS partitions will be recovered without anti-malware scanning.
- Safe recovery is not supported for [CDP backups](#). The machine will be recovered based on the last regular backup without the data in the CDP backup. To recover the CDP data, start a **Files/folders** recovery.

How it works

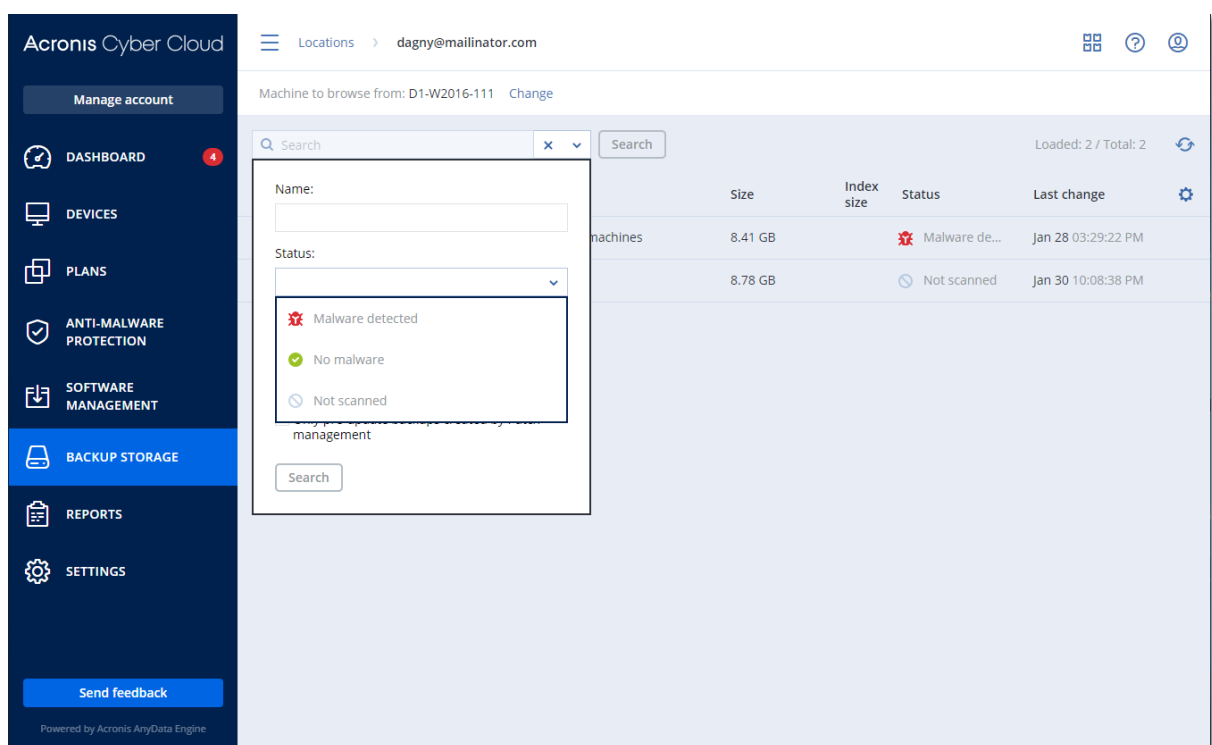
If you enable the Safe recovery option during the recovery process, then the system will perform the following:

1. Scan the image backup for malware and mark the infected files. One of the following statuses is assigned to a backup:
 - **No malware** – no malware was found in a backup during scanning.
 - **Malware detected** – malware was found in a backup during scanning.
 - **Not scanned** – backup was not scanned for malware.



1. Recover the backup to the selected machine.
2. Delete the detected malware.

You can filter backups by using the **Status** parameter.



14.14.3 Recovering a machine

Physical machine

This section describes recovery of physical machines by using the web interface.

Use bootable media instead of the web interface if you need to recover:

- A machine running macOS
- A machine from a tenant in the Enhanced security mode
- Any operating system to bare metal or to an offline machine
- The structure of logical volumes (volumes created by Logical Volume Manager in Linux). The media enables you to recreate the logical volume structure automatically.

Recovery of an operating system requires a reboot. You can choose whether to restart the machine automatically or assign it the **Interaction required** status. The recovered operating system goes online automatically.

To recover a physical machine

1. Select the backed-up machine.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

If the machine is offline, the recovery points are not displayed. Do any of the following:

- If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select a target machine that is online, and then select a recovery point.
- Select a recovery point on [the Backup storage tab](#).
- Recover the machine as described in ["Recovering disks by using bootable media"](#).

4. Click **Recover > Entire machine**.

The software automatically maps the disks from the backup to the disks of the target machine.

To recover to another physical machine, click **Target machine**, and then select a target machine that is online.

×

Recover machine

?

RECOVER TO
Physical machine ▾

TARGET MACHINE
ssd-win2016

DISK MAPPING
Disk 1 → Disk 1
Disk 2 → Disk 2
Disk 3 → Disk 3

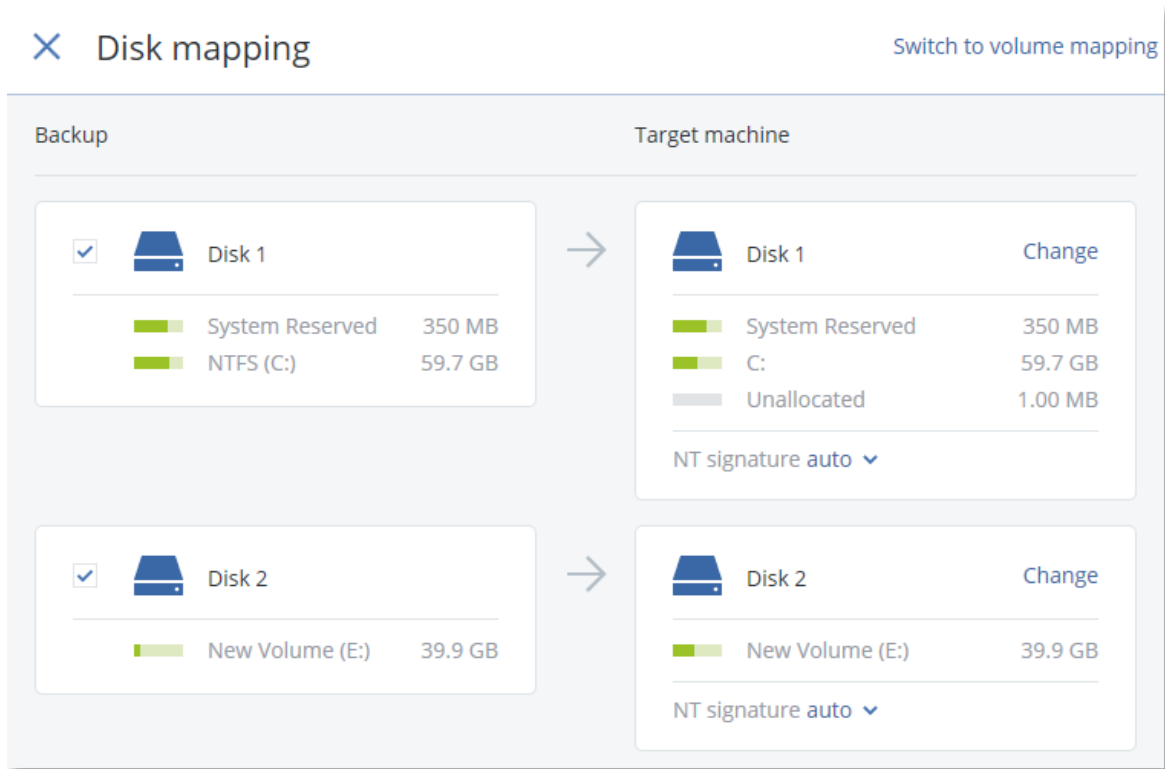
SAFE RECOVERY
☐ Off ⓘ

START RECOVERY

⚙️ RECOVERY OPTIONS

5. If you are unsatisfied with the mapping result or if the disk mapping fails, click **Volume mapping** to re-map the disks manually.

The mapping section also enables you to choose individual disks or volumes for recovery. You can switch between recovering disks and volumes by using the **Switch to...** link in the top-right corner.



6. [Optional] Enable **Safe recovery** to scan the backup for malware. If malware is detected, it will be marked in the backup and deleted right after the recovery process is completed.
7. Click **Start recovery**.
8. Confirm that you want to overwrite the disks with their backed-up versions. Choose whether to restart the machine automatically.

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

Physical machine to virtual

You can recover a physical machine to a virtual machine on one of the supported hypervisors. This is also a mechanism to migrate a physical machine to a virtual machine. For more information about supported P2V migration paths, refer to "[Machine migration](#)".

This section describes the recovery of a physical machine as a virtual machine by using the web interface. This operation can be performed if at least one agent for the relevant hypervisor is installed and registered in Acronis Management Server. For example, recovery to VMware ESXi requires at least one Agent for VMware, recovery to Hyper-V requires at least one Agent for Hyper-V installed and registered in the environment.

Recovery through the web interface is not available for tenants in the Enhanced security mode.

Note

You cannot recover macOS virtual machines to Hyper-V hosts, because Hyper-V does not support macOS. You can recover macOS virtual machines to a VMware host that is installed on Mac hardware.

Also, you cannot recover backups of macOS physical machines as virtual machines.

To recover a physical machine as a virtual machine

1. Select the backed-up machine.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.
If the machine is offline, the recovery points are not displayed. Do any of the following:
 - If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select a machine that is online, and then select a recovery point.
 - Select a recovery point on [the Backup storage tab](#).
 - Recover the machine as described in ["Recovering disks by using bootable media"](#).
4. Click **Recover > Entire machine**.
5. In **Recover to**, select **Virtual machine**.
6. Click **Target machine**.
 - a. Select the hypervisor.

Note

At least one agent for that hypervisor must be installed and registered in Acronis Management Server.

- b. Select whether to recover to a new or existing machine. The new machine option is preferable as it does not require the disk configuration of the target machine to exactly match the disk configuration in the backup.
 - c. Select the host and specify the new machine name, or select an existing target machine.
 - d. Click **OK**.
7. [Optional] When recovering to a new machine, you can also do the following:
 - [Not available for Virtuozzo Hybrid Infrastructure] Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore (storage) for the virtual machine.
 - Click **Disk mapping** to select the datastore (storage), interface, and provisioning mode for each virtual disk. The mapping section also enables you to choose individual disks for recovery.

For Virtuozzo Hybrid Infrastructure, you can only select the storage policy for the target disks. To do so, select the desired target disk, and then click Change. In the blade that opens, click the gear icon, select the storage policy, and then click Done.
 - [Optional for VMware ESXi, Hyper-V, and Red Hat Virtualization/oVirt] Click **VM settings** to change the memory size, the number of processors (for Virtuozzo Hybrid Infrastructure: select

Flavor), and the network connections of the virtual machine.

Note

For Virtuozzo Hybrid Infrastructure, selecting flavor is a required step.

RECOVER TO
Virtual machine

TARGET MACHINE
New machine on 10.250.22.17 [New](#)

DATASTORE
datastore1 (1)

DISK MAPPING
Disk 1 → datastore1 (1), 50.0 GB
Disk 2 → datastore1 (1), 50.0 GB

VM SETTINGS
Memory: 2.00 GB
Virtual processors: 2
Network adapters: 2

[START RECOVERY](#) [RECOVERY OPTIONS](#)

8. Click **Start recovery**.

9. When recovering to an existing virtual machine, confirm that you want to overwrite the disks.

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

Virtual machine

You can recover virtual machines from their backups.

Note

Recovery through the web interface is not available for tenants in the Enhanced security mode.

Prerequisites

- A virtual machine must be stopped during the recovery to this machine. By default, the software stops the machine without a prompt. When the recovery is completed, you have to start the

machine manually. You can change the default behavior by using the VM power management recovery option (click **Recovery options > VM power management**).

Procedure

1. Do one of the following:
 - Select a backed-up machine, click **Recovery**, and then select a recovery point.
 - Select a recovery point on [the Backup storage tab](#).
2. Click **Recover > Entire machine**.
3. If you want to recover to a physical machine, select **Physical machine** in **Recover to**. Otherwise, skip this step.

Recovery to a physical machine is possible only if the disk configuration of the target machine exactly matches the disk configuration in the backup.

If this is the case, continue to step 4 in "[Physical machine](#)". Otherwise, we recommend that you perform the V2P migration by [using bootable media](#).

4. [Optional] By default, the software automatically selects the original machine as the target machine. To recover to another virtual machine, click **Target machine**, and then do the following:
 - a. Select the hypervisor (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3**, or **oVirt**).

Only Virtuozzo virtual machines can be recovered to Virtuozzo. For more information about V2V migration, refer to "[Machine migration](#)".
 - b. Select whether to recover to a new or existing machine.
 - c. Select the host and specify the new machine name, or select an existing target machine.
 - d. Click **OK**.
5. Setup up the additional recovery options that you need.
 - [Optional] [Not available for Virtuozzo Hybrid Infrastructure and Scale Computing HC3] To select the datastore for the virtual machine, click **Datastore** for ESXi, **Path** for Hyper-V and Virtuozzo, or **Storage domain** for Red Hat Virtualization (oVirt), and then select the datastore (storage) for the virtual machine.
 - [Optional] To view the datastore (storage), interface, and the provisioning mode for each virtual disk, click **Disk mapping**. You can change these settings, unless you are recovering a Virtuozzo container or Virtuozzo Hybrid Infrastructure virtual machine.

For Virtuozzo Hybrid Infrastructure, you can only select the storage policy for the target disks. To do so, select the desired target disk, and then click **Change**. In the blade that opens, click the gear icon, select the storage policy, and then click **Done**.

The mapping section also enables you to choose individual disks for recovery.
 - [Optional] [Available only for VMware ESXi, Hyper-V, and Virtuozzo] Click **VM settings** to change the memory size and the number of processors (for Virtuozzo Hybrid Infrastructure: select **Flavor**), or the network connections of the virtual machine.

Note

For Virtuozzo Hybrid Infrastructure, selecting flavor is a required step.


RECOVER TO
Virtual machine

TARGET MACHINE
New machine on 10.250.22.17 New

DATASTORE
datastore1 (1)

DISK MAPPING
Disk 1 → datastore1 (1), 50.0 GB
Disk 2 → datastore1 (1), 50.0 GB

VM SETTINGS
Memory: 2.00 GB
Virtual processors: 2
Network adapters: 2

START RECOVERY  RECOVERY OPTIONS

6. Click **Start recovery**.
7. When recovering to an existing virtual machine, confirm that you want to overwrite the disks. The recovery progress is shown on the **Activities** tab.

Recovering disks by using bootable media

For information about how to create bootable media, refer to "Creating physical bootable media" (p. 522).

To recover disks by using bootable media

1. Boot the target machine by using bootable media.
2. [Only when recovering a Mac] If you are recovering APFS-formatted disks/volumes to a non-original machine or to bare metal, re-create the original disk configuration manually:
 - a. Click **Disk Utility**.
 - b. Erase and format the target disk into APFS. For instructions, refer to <https://support.apple.com/en-us/HT208496#erasedisk>.

- c. Re-create the original disk configuration. For instructions, refer to <https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15>.
- d. Click **Disk Utility** > **Quit Disk Utility**.
3. Click **Manage this machine locally** or click **Rescue Bootable Media** twice, depending on the media type you are using.
4. If a proxy server is enabled in your network, click **Tools** > **Proxy server**, and then specify the proxy server host name/IP address, port, and credentials. Otherwise, skip this step.
5. [Optional] When recovering Windows or Linux, click **Tools** > **Register media in the Cyber Protection service**, and then specify the registration token that you obtained when downloading the media. If you do this, you will not need to enter credentials or a registration code to access the cloud storage, as described in step 8.
6. On the welcome screen, click **Recover**.
7. Click **Select data**, and then click **Browse**.
8. 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.

When recovering Windows or Linux, you have the option to request a registration code and use it instead of the credentials. Click **Use registration code** > **Request the code**. The software shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. The registration code is valid for one hour.
 - 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.
9. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
10. In **Backup contents**, select the disks that you want to recover. Click **OK** to confirm your selection.
11. Under **Where to recover**, the software automatically maps the selected disks to the target disks. If the mapping is not successful or if you are unsatisfied with the mapping result, you can re-map disks manually.

Note

Changing disk layout may affect the operating system bootability. Please use the original machine's disk layout unless you feel fully confident of success.

12. [When recovering Linux] If the backed-up machine had logical volumes (LVM) and you want to reproduce the original LVM structure:
 - a. Ensure that the number of the target machine disks and each disk capacity are equal to or exceed those of the original machine, and then click **Apply RAID/LVM**.

- b. Review the volume structure, and then click **Apply RAID/LVM** to create it.
13. [Optional] Click **Recovery options** to specify additional settings.
14. Click **OK** to start the recovery.

Using Universal Restore

The most recent operating systems remain bootable when recovered to dissimilar hardware, including the VMware or Hyper-V platforms. If a recovered operating system does not boot, use the Universal Restore tool to update the drivers and modules that are critical for the operating system startup.

Universal Restore is applicable to Windows and Linux.

To apply Universal Restore

1. Boot the machine from the bootable media.
2. Click **Apply Universal Restore**.
3. If there are multiple operating systems on the machine, choose the one to apply Universal Restore to.
4. [For Windows only] [Configure the additional settings](#).
5. Click **OK**.

Universal Restore in Windows

Preparation

14.14.4 Prepare drivers

Before applying Universal Restore to a Windows operating system, make sure that you have the drivers for the new HDD controller and the chipset. These drivers are critical to start the operating system. Use the CD or DVD supplied by the hardware vendor or download the drivers from the vendor's website. The driver files should have the *.inf extension. If you download the drivers in the *.exe, *.cab or *.zip format, extract them using a third-party application.

The best practice is to store drivers for all the hardware used in your organization in a single repository sorted by device type or by the hardware configurations. You can keep a copy of the repository on a DVD or a flash drive; pick some drivers and add them to the bootable media; create the custom bootable media with the necessary drivers (and the necessary network configuration) for each of your servers. Or, you can simply specify the path to the repository every time Universal Restore is used.

14.14.5 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

14.14.6 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.

14.14.7 Mass storage drivers to install anyway

You need this setting if:

- The hardware has a specific mass storage controller such as RAID (especially NVIDIA RAID) or a fibre channel adapter.
- You migrated a system to a virtual machine that uses a SCSI hard drive controller. Use SCSI drivers bundled with your virtualization software or download the latest drivers versions from the software manufacturer website.
- If the automatic drivers search does not help to boot the system.

Specify the appropriate drivers by clicking **Add driver**. The drivers defined here will be installed, with appropriate warnings, even if the program finds a better driver.

Universal Restore process

After you have specified the required settings, click **OK**.

If Universal Restore cannot find a compatible driver in the specified locations, it will display a prompt about the problem device. Do one of the following:

- Add the driver to any of the previously specified locations and click **Retry**.

- If you do not remember the location, click **Ignore** to continue the process. If the result is not satisfactory, reapply Universal Restore. When configuring the operation, specify the necessary driver.

Once Windows boots, it will initialize the standard procedure for installing new hardware. The network adapter driver will be installed silently if the driver has the Microsoft Windows signature. Otherwise, Windows will ask for confirmation on whether to install the unsigned driver.

After that, you will be able to configure the network connection and specify drivers for the video adapter, USB and other devices.

Universal Restore in Linux

Universal Restore can be applied to Linux operating systems with a kernel version of 2.6.8 or later.

When Universal Restore is applied to a Linux operating system, it updates a temporary file system known as the initial RAM disk (initrd). This ensures that the operating system can boot on the new hardware.

Universal Restore adds modules for the new hardware (including device drivers) to the initial RAM disk. As a rule, it finds the necessary modules in the **/lib/modules** directory. If Universal Restore cannot find a module it needs, it records the module's file name into the log.

Universal Restore may modify the configuration of the GRUB boot loader. This may be required, for example, to ensure the system bootability when the new machine has a different volume layout than the original machine.

Universal Restore never modifies the Linux kernel.

Reverting to the original initial RAM disk

You can revert to the original initial RAM disk if necessary.

The initial RAM disk is stored on the machine in a file. Before updating the initial RAM disk for the first time, Universal Restore saves a copy of it to the same directory. The name of the copy is the name of the file, followed by the **_acronis_backup.img** suffix. This copy will not be overwritten if you run Universal Restore more than once (for example, after you have added missing drivers).

To revert to the original initial RAM disk, do any of the following:

- Rename the copy accordingly. For example, run a command similar to the following:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
```

- Specify the copy in the **initrd** line of the GRUB boot loader configuration.

14.14.8 Recovering files

Recovering files by using the web interface

Note

Recovery through the web interface is not available for tenants in the Enhanced security mode.

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 any of the following:
 - [Recommended] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select a target machine that is online, and then select a recovery point.
 - Select a recovery point on [the Backup storage tab](#).
 - [Download the files from the cloud storage](#).
 - [Use bootable media](#).
4. Click **Recover > Files/folders**.
5. Browse to the required folder or use search to obtain the list of the required files and folders. You can use one or more wildcard characters (* and ?). For more details about using wildcards, refer to ["File filters"](#).

Note

Search is not available for disk-level backups that are stored in the cloud storage.

6. Select the files that you want to recover.
7. If you want to save the files as a .zip file, click **Download**, select the location to save the data to, and click **Save**. Otherwise, skip this step.
Downloading is not available if your selection contains folders or the total size of the selected files exceeds 100 MB.
8. Click **Recover**.
In **Recover to**, you see one of the following:
 - The machine that originally contained the files that you want to recover (if an agent is installed on this machine).
 - The machine where Agent for VMware, Agent for Hyper-V, Agent for Virtuozzo, Agent for Scale Computing HC3, or Agent for oVirt is installed (if the files originate from an ESXi, Hyper-V, Virtuozzo, Scale Computing HC3, or Red Hat Virtualization/oVirt 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

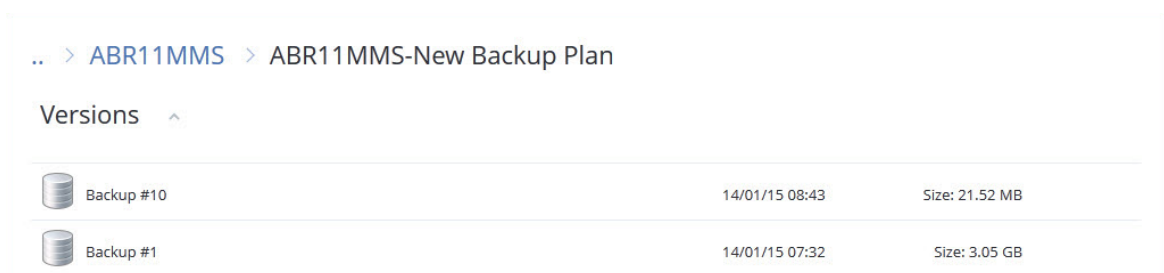
You can browse the cloud storage, view the contents of the backups, and download files that you need.

Limitations

- Backups of system state, SQL databases, and Exchange databases cannot be browsed.
- Downloading is not available if the total size of the selected files exceeds 100 MB.

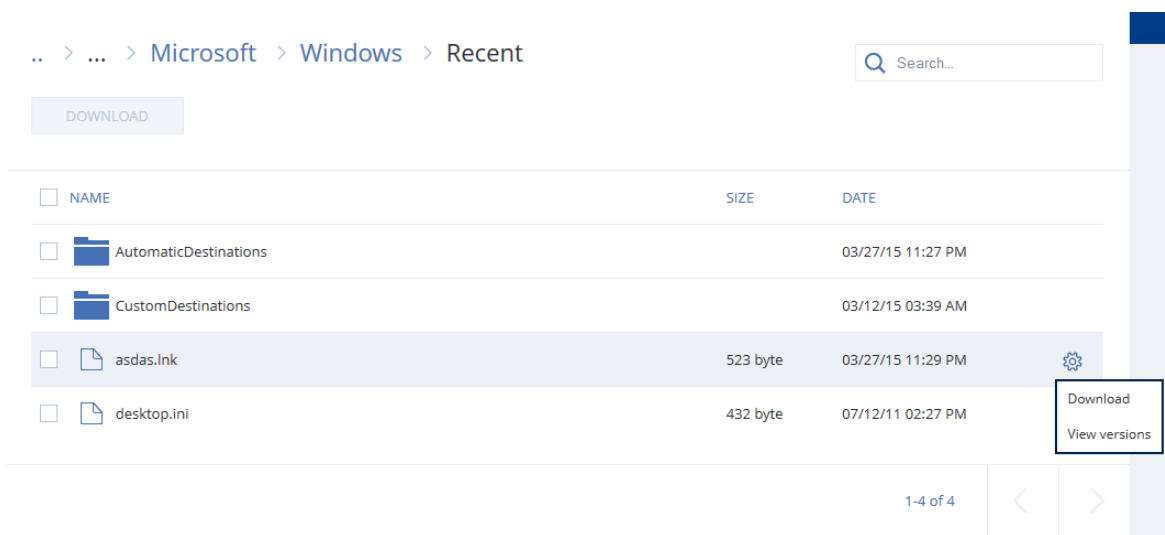
To download files from the cloud storage

1. Select a machine that was backed up.
2. Click **Recover** > **More ways to recover...** > **Download files**.
3. Enter the credentials of the account to which the backed up machine is assigned.
4. [When browsing disk-level backups] Under **Versions**, click the backup from which you want to recover the files.



[When browsing file-level backups] You can select the backup date and time in the next step, under the gear icon located to the right of the selected file. By default, files are recovered from the latest backup.

5. Browse to the required folder or use search to obtain the list of the required files.




6. Select the check boxes for the items you need to recover, and then click **Download**.
If you select a single file, it will be downloaded as is. Otherwise, the selected data will be archived into a .zip file.
7. Select the location to save the data to, and then click **Save**.

Verifying file authenticity with Notary Service

If notarization [was enabled during backup](#), you can verify the authenticity of a backed-up file.

To verify the file authenticity

1. Select the file as described in steps 1-6 of the "[Recovering files by using the web interface](#)" section, or steps 1-5 of the "[Downloading files from the cloud storage](#)" section.
2. Ensure that the selected file is marked with the following icon: . This means that the file is notarized.
3. Do one of the following:
 - Click **Verify**.
The software checks the file authenticity and displays the result.
 - Click **Get certificate**.
A certificate that confirms the file notarization is opened in a web browser window. The window also contains instructions that allow you to verify the file authenticity manually.

Signing a file with ASign

Note

The availability of this feature depends on the service quotas that are enabled for your account.

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, or steps 1-5 of the ["Downloading files from the cloud storage"](#) section.
2. Ensure that the correct date and time is selected on the left panel.
3. Click **Sign this file version**.
4. Specify the password for the cloud storage account under which the backup is stored. The login of the account is displayed in the prompt window.
The ASign service interface is opened in a web browser window.
5. Add other signees by specifying their email addresses. It is not possible to add or remove signees after sending invitations, so ensure that the list includes everyone whose signature is required.
6. Click **Invite to sign** to send invitations to the signees.
Each signee receives an email message with the signature request. When all the requested signees sign the file, it is notarized and signed through the notary service.
You will receive notifications when each signee signs the file and when the entire process is complete. You can access the ASign web page by clicking **View details** in any of the email messages that you receive.
7. Once the process is complete, go to the ASign web page and click **Get document** to download a .pdf document that contains:
 - The Signature Certificate page with the collected signatures.
 - The Audit Trail page with history of activities: when the invitation was sent to the signees, when each signee signed the file, and so on.

Recovering files by using bootable media

For information about how to create bootable media, refer to "[Creating bootable media](#)".

To recover files by using bootable media

1. Boot the target machine by using the bootable media.
2. Click **Manage this machine locally** or click **Rescue Bootable Media** twice, depending on the media type you are using.
3. If a proxy server is enabled in your network, click **Tools > Proxy server**, and then specify the proxy server host name/IP address, port, and credentials. Otherwise, skip this step.
4. [Optional] When recovering Windows or Linux, click **Tools > Register media in the Cyber Protection service**, and then specify the registration token that you obtained when downloading the media. If you do this, you will not need to enter credentials or a registration code to access the cloud storage, as described in step 7.
5. On the welcome screen, click **Recover**.
6. Click **Select data**, and then click **Browse**.
7. Specify the backup location:
 - To recover from cloud storage, select **Cloud storage**. Enter the credentials of the account to which the backed up machine is assigned.
When recovering Windows or Linux, you have the option to request a registration code and use it instead of the credentials. Click **Use registration code > Request the code**. The software shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. The registration code is valid for one hour.
 - To recover from a local or a network folder, browse to the folder under **Local folders** or **Network folders**.
Click **OK** to confirm your selection.
8. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
9. In **Backup contents**, select **Folders/files**.
10. Select the data that you want to recover. Click **OK** to confirm your selection.
11. Under **Where to recover**, specify a folder. Optionally, you can prohibit overwriting of newer versions of files or exclude some files from recovery.
12. [Optional] Click **Recovery options** to specify additional settings.
13. Click **OK** to start the recovery.

Extracting files from local backups

You can browse the contents of backups and extract files that you need.

Requirements

- This functionality is available only in Windows by using File Explorer.
- A protection agent must be installed on the machine from which you browse a backup.
- The backed-up file system must be one of the following: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS, or HFS+.
- The backup must be stored in a local folder or on a network share (SMB/CIFS).

To extract files from a backup

1. Browse to the backup location by using File Explorer.
2. Double-click the backup file. The file names are based on the following template:
 <machine name> - <protection plan GUID>
3. If the backup is encrypted, enter the encryption password. Otherwise, skip this step.
 File Explorer displays the recovery points.
4. Double-click the recovery point.
 File Explorer displays the backed-up data.
5. Browse to the required folder.
6. Copy the required files to any folder on the file system.

14.14.9 Recovering system state

Note

Recovery through the web interface is not available for tenants in the Enhanced security mode.

1. Select the machine for which you want to recover the system state.
2. Click **Recovery**.
3. Select a system state recovery point. Note that recovery points are filtered by location.
4. Click **Recover system state**.
5. Confirm that you want to overwrite the system state with its backed-up version.
The recovery progress is shown on the **Activities** tab.

14.14.10 Recovering ESXi configuration

To recover an ESXi configuration, you need Linux-based bootable media. For information about how to create bootable media, refer to "Creating physical bootable media" (p. 522).

If you are recovering an ESXi configuration to a non-original host and the original ESXi host is still connected to the vCenter Server, disconnect and remove this host from the vCenter Server to avoid unexpected issues during the recovery. If you want to keep the original host along with the recovered one, you can add it again after the recovery is complete.

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

To recover an ESXi configuration

1. Boot the target machine by using the bootable media.
2. Click **Manage this machine locally**.
3. On the welcome screen, click **Recover**.
4. Click **Select data**, and then click **Browse**.
5. Specify the backup location:
 - Browse to the folder under **Local folders** or **Network folders**.Click **OK** to confirm your selection.
6. In **Show**, select **ESXi configurations**.
7. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
8. Click **OK**.
9. In **Disks to be used for new datastores**, do the following:
 - Under **Recover ESXi to**, select the disk where the host configuration will be recovered. If you are recovering the configuration to the original host, the original disk is selected by default.
 - [Optional] Under **Use for new datastore**, select the disks where new datastores will be created. Be careful because all data on the selected disks will be lost. If you want to preserve the virtual machines in the existing datastores, do not select any disks.
10. If any disks for new datastores are selected, select the datastore creation method in **How to create new datastores**: **Create one datastore per disk** or **Create one datastore on all selected HDDs**.
11. [Optional] In **Network mapping**, change the result of automatic mapping of the virtual switches present in the backup to the physical network adapters.
12. [Optional] Click **Recovery options** to specify additional settings.
13. Click **OK** to start the recovery.

14.14.11 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 machine s	SQL and Exchang e

	Windows	Linux	Bootable media	Windows	Linux	macOS	Bootable media	ESXi, Hyper-V, and Virtuozzo	Windows
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	-	-	-	-	-	-	-	+	-
Windows event log	+	-	-	+	-	-	-	Hyper-V only	+

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

Depending on the settings chosen by your service provider, validation might not be available when backing up to the cloud storage.

Boot mode

This option is effective when recovering a physical or a virtual machine from a disk-level backup that contains a Windows operating system.

This option enables you to select the boot mode (BIOS or UEFI) that Windows will use after the recovery. If the boot mode of the original machine is different from the selected boot mode, the software will:

- Initialize the disk to which you are recovering the system volume, according to the selected boot mode (MBR for BIOS, GPT for UEFI).
- Adjust the Windows operating system so that it can start using the selected boot mode.

The preset is: **As on the target machine**.

You can choose one of the following:

- **As on the target machine**

The agent that is running on the target machine detects the boot mode currently used by Windows and makes the adjustments according to the detected boot mode.

This is the safest value that automatically results in bootable system unless the limitations listed below apply. Since the **Boot mode** option is absent under bootable media, the agent on media always behaves as if this value is chosen.

- **As on the backed-up machine**

The agent that is running on the target machine reads the boot mode from the backup and makes the adjustments according to this boot mode. This helps you recover a system on a different machine, even if this machine uses another boot mode, and then replace the disk in the backed-up machine.

- **BIOS**

The agent that is running on the target machine makes the adjustments to use BIOS.

- **UEFI**

The agent that is running on the target machine makes the adjustments to use UEFI.

Once a setting is changed, the disk mapping procedure will be repeated. This will take some time.

Recommendations

If you need to transfer Windows between UEFI and BIOS:

- Recover the entire disk where the system volume is located. If you recover only the system volume on top of an existing volume, the agent will not be able to initialize the target disk properly.
- Remember that BIOS does not allow using more than 2 TB of disk space.

Limitations

- Transferring between UEFI and BIOS is supported for:
 - 64-bit Windows operating systems starting with Windows Vista SP1
 - 64-bit Windows Server operating systems starting with Windows Server 2008 SP1
- Transferring between UEFI and BIOS is not supported if the backup is stored on a tape device.

When transferring a system between UEFI and BIOS is not supported, the agent behaves as if the **As on the backed-up machine** setting is chosen. If the target machine supports both UEFI and BIOS, you need to manually enable the boot mode corresponding to the original machine. Otherwise, the system will not boot.

Date and time for files

This option is effective only when recovering files.

This option defines whether to recover the files' date and time from the backup or assign the files the current date and time.

If this option is enabled, the files will be assigned the current date and time.

The preset is: **Enabled**.

Error handling

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

Re-attempt, if an error occurs

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

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

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

The preset is: **Disabled**.

With the silent mode enabled, the program will automatically handle situations requiring user interaction where possible. If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

Save system information if a recovery with reboot fails

This option is effective for a disk or volume recovery to a physical machine running Windows or Linux.

The preset is: **Disabled**.

When this option is enabled, you can specify a folder on the local disk (including flash or HDD drives attached to the target machine) or on a network share where the log, system information, and crash dump files will be saved. This file will help the technical support personnel to identify the problem.

File exclusions

This option is effective only when recovering files.

The option defines which files and folders to skip during the recovery process and thus exclude from the list of recovered items.

Note

Exclusions override the selection of data items to recover. For example, if you select to recover file MyFile.tmp and to exclude all .tmp files, file MyFile.tmp will not be recovered.

File-level security

This option is effective when recovering files from disk- and file-level backups of NTFS-formatted volumes.

This option defines whether to recover NTFS permissions for files along with the files.

The preset is: **Enabled**.

You can choose whether to recover the permissions or let the files inherit their NTFS permissions from the folder to which they are recovered.

Flashback

This option is effective when recovering disks and volumes on physical and virtual machines, except for Mac.

This option works only if the volume layout of the disk being recovered exactly matches that of the target disk.

If the option is enabled, only the differences between the data in the backup and the target disk data are recovered. This accelerates recovery of physical and virtual machines. The data is compared at the block level.

When recovering a physical machine, the preset is: **Disabled**.

When recovering a virtual machine, the preset is: **Enabled**.

Full path recovery

This option is effective only when recovering data from a file-level backup.

If this option is enabled, the full path to the file will be re-created in the target location.

The preset is: **Disabled**.

Mount points

This option is effective only in Windows for recovering data from a file-level backup.

Enable this option to recover files and folders that were stored on the mounted volumes and were backed up with the enabled [Mount points](#) option.

The preset is: **Disabled**.

This option is effective only when you select for recovery a folder that is higher in the folder hierarchy than the mount point. If you select for recovery folders within the mount point or the mount point itself, the selected items will be recovered regardless of the **Mount points** option value.

Note

Please be aware that if the volume is not mounted at the moment of recovery, the data will be recovered directly to the folder that has been the mount point at the time of backing up.

Performance

This option defines the priority of the recovery process in the operating system.

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

The preset is: **Normal**.

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

Pre/Post commands

The option enables you to define the commands to be automatically executed before and after the data recovery.

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

- Launch the **Checkdisk** command in order to find and fix logical file system errors, physical errors or bad sectors to be started before the recovery starts or after the recovery ends.

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

A post-recovery command will not be executed if the recovery proceeds with reboot.

Pre-recovery command

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

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

Check box	Selection			
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 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.

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, Agent for Scale Computing HC3, or Agent for oVirt.

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, Agent for Virtio, Agent for Scale Computing HC3, or Agent for oVirt.

Power off target virtual machines when starting recovery

The preset is: **Enabled**.

Recovery to an existing virtual machine is not possible if the machine is online, and so the machine is powered off automatically as soon as the recovery starts. Users will be disconnected from the machine and any unsaved data will be lost.

Clear the check box for this option if you prefer to power off virtual machines manually before the recovery.

Power on the target virtual machine when recovery is complete

The preset is: **Disabled**.

After a machine is recovered from a backup to another machine, there is a chance the existing machine's replica will appear on the network. To be on the safe side, power on the recovered virtual machine manually, after you take the necessary precautions.

Windows event log

This option is effective only in Windows operating systems.

This option defines whether the agents have to log events of the recovery operations in the Application Event Log of Windows (to see this log, run eventvwr.exe or select **Control Panel > Administrative tools > Event Viewer**). You can filter the events to be logged.

The preset is: **Disabled**.

14.15 Operations with backups

14.15.1 The Backup storage tab

The **Backup storage** tab provides access to all backups, including backups of offline machines and machines that are no longer registered in the Cyber Protection service.

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.

An administrator can view backups to cloud on behalf of any account that belongs to the given unit or company and its child groups, by selecting the cloud storage for the account. To select the device that you want to use to obtain data from cloud, click **Change** in the **Machine to browse from** row. The **Backup storage** tab shows the backups of all machines ever registered under the selected account.

Backups created by the *cloud* Agent for Microsoft 365 and backups of Google Workspace data are shown not in the **Cloud storage** location, but in a separate section named **Cloud applications backups**.

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.

If you added or removed some backups by using a file manager, click the gear icon next to the location name, and then click **Refresh**.

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 use the backup replication instead of moving backup files manually.

A backup location (except for the cloud storage) disappears from the **Backup storage** tab if all machines that had ever backed up to the location were deleted from the Cyber Protection service. This ensures that you do not have to pay for the backups stored in this location. As soon as a backup to this location occurs, the location is re-added along with all backups that are stored in it.

On the **Backup storage** tab, you can filter backups in the list by using the following criteria:

- **Only with forensic data** – only [backups having forensic data](#) will be shown.
- **Only pre-update backups created by Patch management** – only [backups that were created during patch management run before patch installation](#) will be shown.

To select a recovery point by using the Backup storage tab

1. On the **Backup storage** tab, select the location where the backups are stored.
The software displays all backups that your account is allowed to view in the selected location. The backups are combined in groups. The group names are based on the following template:
<machine name> - <protection plan name>
2. Select a group from which you want to recover the data.
3. [Optional] Click **Change** next to **Machine to browse from**, and then select another machine.
Some backups can only be browsed by specific agents. For example, you must select a machine running Agent for SQL to browse the backups of Microsoft SQL Server databases.

Important

Please be aware that the **Machine to browse from** is a default destination for recovery from a physical machine backup. After you select a recovery point and click **Recover**, double check the **Target machine** setting to ensure that you want to recover to this specific machine. To change the recovery destination, specify another machine in **Machine to browse from**.

4. Click **Show backups**.
5. Select the recovery point.

14.15.2 Mounting volumes from a backup

Mounting volumes from a disk-level backup lets you access the volumes as though they were physical disks. Volumes are mounted in the read-only mode.

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.

To mount a volume 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 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 **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**.
The software unmounts the selected volume.

14.15.3 Deleting backups

Warning!

When a backup is deleted, all of its data is permanently erased. Deleted data cannot be recovered.

To delete backups of a machine that is online and present in the service console

1. On the **All devices** tab, select a machine whose backups you want to delete.
2. Click **Recovery**.
3. Select the location to delete the backups from.

4. Delete the desired backups. You can delete the whole backup chain or a single backup in it.
 - To delete the whole backup chain, click **Delete all**.
 - To delete a single backup in the selected chain:
 - a. Select the backup to delete, and then click the gear icon.
 - b. Click **Delete**.
5. Confirm your decision.

To delete backups of any machine

1. On the **Backup storage** tab, select the location from which you want to delete the backups.

The software displays all backups that your account is allowed to view in the selected location. The backups are combined in backup chains. The backup chain names are based on the following template:

 - <machine name> - <protection plan name>
 - <user name> OR <drive name> - <cloud service> - <protection plan name> - for cloud-to-cloud backups
2. Select a backup chain.
3. Delete the desired backups. You can delete the whole backup chain or a single backup in it.
 - To delete the whole backup chain, click **Delete**.
 - To delete a single backup in the selected chain:
 - a. Click **Show backups**.
 - b. Select the backup to delete, and then click the gear icon.
 - c. Click **Delete**.
4. Confirm your decision.

To delete backups directly from the cloud storage

1. Log in to the cloud storage, as described in "[Downloading files from the cloud storage](#)".
2. Click the name of the machine whose backups you want to delete.

The software displays one or more backup groups.
3. Click the gear icon corresponding to the backup group that you want to delete.
4. Click **Remove**.
5. Confirm the operation.

What to do if you deleted local backups by using a file manager

We recommend that you delete backups by using the service console, whenever possible. If you deleted local backups by using a file manager, do the following:

1. On the **Backup storage** tab, click the gear icon next to the location name.
2. Click **Refresh**.

This way you will inform the Cyber Protection service that the local storage usage is decreased.

14.16 Protecting Microsoft applications

14.16.1 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.

14.16.2 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.

14.16.3 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.

14.16.4 Recovering applications

The following table summarizes the available application recovery methods.

	From a database backup	From an application-aware backup	From a disk backup
Microsoft SQL Server	Databases to a live SQL Server instance Databases as files	Entire machine Databases to a live SQL Server instance Databases as files	Entire machine
Microsoft Exchange Server	Databases to a live Exchange Databases as files Granular recovery to a live Exchange or to Microsoft 365*	Entire machine Databases to a live Exchange Databases as files Granular recovery to a live Exchange or to Microsoft 365*	Entire machine
Microsoft SharePoint database servers	Databases to a live SQL Server instance Databases as files Granular recovery by using SharePoint Explorer	Entire machine Databases to a live SQL Server instance Databases as files Granular recovery by using SharePoint Explorer	Entire machine
Microsoft SharePoint front-end web servers	-	-	Entire machine
Active Directory Domain Services	-	Entire machine	-

* Granular recovery is also available from a mailbox backup. Recovery of Exchange data items to Microsoft 365, and vice versa, is supported on the condition that Agent for Microsoft 365 is installed locally.

14.16.5 Prerequisites

Before configuring the application backup, ensure that the requirements listed below are met.

To check the VSS writers state, use the `vssadmin list writers` command.

Common requirements

For Microsoft SQL Server, ensure that:

- At least one Microsoft SQL Server instance is started.
- The SQL writer for VSS is turned on.

For Microsoft Exchange Server, ensure that:

- The Microsoft Exchange Information Store service is started.
- Windows PowerShell is installed. For Exchange 2010 or later, the Windows PowerShell version must be at least 2.0.
- Microsoft .NET Framework is installed.
For Exchange 2007, the Microsoft .NET Framework version must be at least 2.0.
For Exchange 2010 or later, the Microsoft .NET Framework version must be at least 3.5.
- The Exchange writer for VSS is turned on.

Note

Agent for Exchange needs a temporary storage to operate. By default, the temporary files are located in %ProgramData%\Acronis\Temp. Ensure that you have at least as much free space on the volume where the %ProgramData% folder is located as 15 percent of an Exchange database size. Alternatively, you can change the location of the temporary files before creating Exchange backups as described in: <https://kb.acronis.com/content/40040>.

On a domain controller, ensure that:

- The Active Directory writer for VSS is turned on.

When creating a protection plan, ensure that:

- For physical machines 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 it will be impossible to perform a recovery of application data from such backups. If the plan is executed in the **Sector-by-sector** mode due to an automatic switch to this mode, then recovery of application data will also be impossible.

Requirements for ESXi virtual machines

If the application runs on a virtual machine that is backed up by Agent for VMware, ensure that:

- The virtual machine being backed up meets the requirements for application-consistent backup and restore listed in the article "Windows Backup Implementations" in the VMware documentation: <https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html>.
- VMware Tools is installed and up-to-date on the machine.
- User Account Control (UAC) is disabled on the machine. If you do not want to disable UAC, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

Requirements for Hyper-V virtual machines

If the application runs on a virtual machine that is backed up by Agent for Hyper-V, ensure that:

- The guest operating system is Windows Server 2008 or later.
- For Hyper-V 2008 R2: the guest operating system is Windows Server 2008/2008 R2/2012.
- The virtual machine has no dynamic disks.
- The network connection exists between the Hyper-V host and the guest operating system. This is required to execute remote WMI queries inside the virtual machine.
- User Account Control (UAC) is disabled on the machine. If you do not want to disable UAC, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when enabling application backup.
- The virtual machine configuration matches the following criteria:
 - Hyper-V Integration Services is installed and up-to-date. The critical update is <https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines>
 - In the virtual machine settings, the **Management > Integration Services > Backup (volume checkpoint)** option is enabled.
 - For Hyper-V 2012 and later: the virtual machine has no checkpoints.
 - For Hyper-V 2012 R2 and later: the virtual machine has a SCSI controller (check **Settings > Hardware**).

14.16.6 Database backup

Before backing up databases, ensure that the requirements listed in "[Prerequisites](#)" are met.

Select the databases as described below, and then specify other settings of the protection plan [as appropriate](#).

Selecting SQL databases

A backup of an SQL database contains the database files (.mdf, .ndf), log files (.ldf), and other associated files. The files are backed with the help of the SQL Writer service. The service must be running at the time that the Volume Shadow Copy Service (VSS) requests a backup or recovery.

The SQL transaction logs are truncated after each successful backup. SQL log truncation can be disabled in the [protection plan options](#).

To select SQL databases

1. Click **Devices > Microsoft SQL**.
The software shows the tree of SQL Server Always On Availability Groups (AAG), machines running Microsoft SQL Server, SQL Server instances, and databases.
2. Browse to the data that you want to back up.
Expand the tree nodes or double-click items in the list to the right of the tree.

3. Select the data that you want to back up. You can select AAGs, machines running SQL Server, SQL Server instances, or individual databases.
 - If you select an AAG, all databases that are included into the selected AAG will be backed up. For more information about backing up AAGs or individual AAG databases, refer to ["Protecting Always On Availability Groups \(AAG\)"](#).
 - If you select a machine running an SQL Server, all databases that are attached to all SQL Server instances running on the selected machine will be backed up.
 - If you select a SQL Server instance, all databases that are attached to the selected instance will be backed up.
 - If you select databases directly, only the selected databases will be backed up.
4. Click **Protect**. If prompted, provide credentials to access the SQL Server data. 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.

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, refer to "Protecting Database Availability Groups (DAG)".
 - If you select a machine running Microsoft Exchange Server, all databases that are mounted to the Exchange Server running on the selected machine will be backed up.
 - If you select databases directly, only the selected databases will be backed up.
 - If you configured Agent for Exchange as described in "[Mailbox backup](#)", you can select mailboxes for backup.
4. If prompted, provide the credentials to access the data.
 5. Click **Protect**.

Protecting Always On Availability Groups (AAG)

Note

The availability of this feature depends on the service quotas that are enabled for your account.

SQL Server high-availability solutions overview

The Windows Server Failover Clustering (WSFC) functionality enables you to configure a highly available SQL Server through redundancy at the instance level (Failover Cluster Instance, FCI) or at the database level (AlwaysOn Availability Group, AAG). You can also combine both methods.

In a Failover Cluster Instance, SQL databases are located on a shared storage. This storage can only be accessed from the active cluster node. If the active node fails, a failover occurs and a different node becomes active.

In an availability group, each database replica resides on a different node. If the primary replica becomes not available, a secondary replica residing on a different node is assigned the primary role.

Thus, the clusters are already serving as a disaster recovery solution themselves. However, there might be cases when the clusters cannot provide data protection: for example, in case of a database logical corruption, or when the entire cluster is down. Also cluster solutions do not protect from harmful content changes, as they usually immediately replicate to all cluster nodes.

Supported cluster configurations

This backup software supports *only* the Always On Availability Group (AAG) for SQL Server 2012 or later. Other cluster configurations, such as Failover Cluster Instances, database mirroring, and log shipping are *not* supported.

How many agents are required for cluster data backup and recovery?

For successful data backup and recovery of a cluster Agent for SQL has to be installed on each node of the WSFC cluster.

Backing up databases included in an AAG

1. Install Agent for SQL on each node of the WSFC cluster.

Note

After you install the agent on one of the nodes, the software displays the AAG and its nodes under **Devices > Microsoft SQL > Databases**. To install Agents for SQL on the rest of the nodes, select the AAG, click **Details**, and then click **Install agent** next to each of the nodes.

2. Select the AAG to backup as described in "Selecting SQL databases".

You must select the AAG itself to backup all databases of the AAG. To backup a set of databases, define this set of databases in all nodes of the AAG.

Warning!

The database set must be exactly the same in all nodes. If even one set is different, or not defined on all nodes, the cluster backup will not work correctly.

3. Configure the "[Cluster backup mode](#)" backup option.

Recovery of databases included in an AAG

1. Select the databases that you want to recover, and then select the recovery point from which you want to recover the databases.

When you select a clustered database under **Devices > Microsoft SQL > Databases**, and then click **Recover**, the software shows only the recovery points that correspond to the times when the selected copy of the database was backed up.

The easiest way to view all recovery points of a clustered database is to select the backup of the entire AAG [on the Backup storage tab](#). The names of AAG backups are based on the following template: <AAG name> - <protection plan name> and have a special icon.

2. To configure recovery, follow the steps described in "[Recovering SQL databases](#)", starting from step 5.

The software automatically defines a cluster node to which the data will be recovered. The node's name is displayed in the **Recover to** field. You can manually change the target node.

Important

A database that is included in an Always On Availability Group cannot be overwritten during a recovery because Microsoft SQL Server prohibits this. You need to exclude the target database from the AAG before the recovery. Or, just recover the database as a new non-AAG one. When the recovery is completed, you can reconstruct the original AAG configuration.

Protecting Database Availability Groups (DAG)

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Exchange Server clusters overview

The main idea of Exchange clusters is to provide high database availability with fast failover and no data loss. Usually, it is achieved by having one or more copies of databases or storage groups on the members of the cluster (cluster nodes). If the cluster node hosting the active database copy or the active database copy itself fails, the other node hosting the passive copy automatically takes over the operations of the failed node and provides access to Exchange services with minimal downtime. Thus, the clusters are already serving as a disaster recovery solution themselves.

However, there might be cases when failover cluster solutions cannot provide data protection: for example, in case of a database logical corruption, or when a particular database in a cluster has no copy (replica), or when the entire cluster is down. Also cluster solutions do not protect from harmful content changes, as they usually immediately replicate to all cluster nodes.

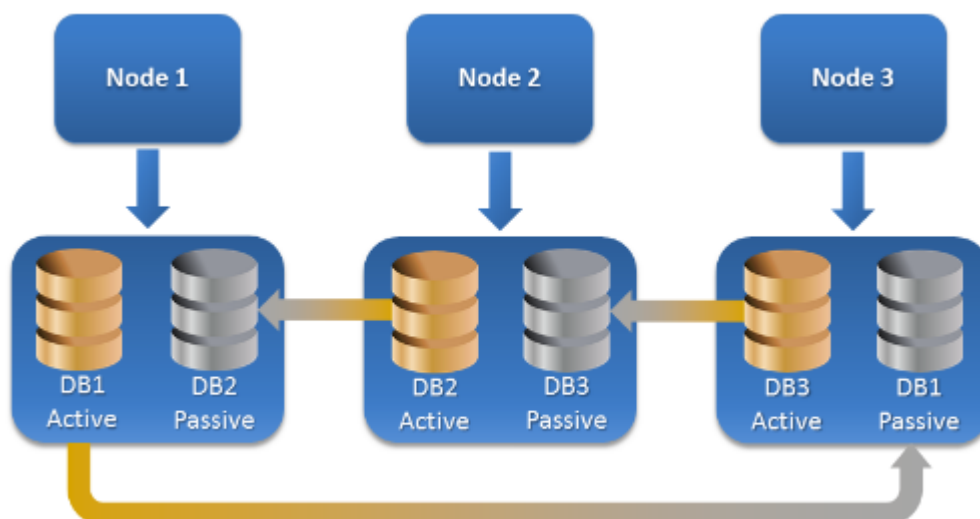
Cluster-aware backup

With cluster-aware backup, you back up only one copy of the clustered data. If the data changes its location within the cluster (due to a switchover or a failover), the software will track all relocations of this data and safely back it up.

Supported cluster configurations

Cluster-aware backup is supported *only* for Database Availability Group (DAG) in Exchange Server 2010 or later. Other cluster configurations, such as Single Copy Cluster (SCC) and Cluster Continuous Replication (CCR) for Exchange 2007, are *not* supported.

DAG is a group of up to 16 Exchange Mailbox servers. Any node can host a copy of mailbox database from any other node. Each node can host passive and active database copies. Up to 16 copies of each database can be created.



How many agents are required for cluster-aware backup and recovery?

For successful backup and recovery of clustered databases, Agent for Exchange has to be installed on each node of the Exchange cluster.

Note

After you install the agent on one of the nodes, the service console displays the DAG and its nodes under **Devices > Microsoft Exchange > Databases**. To install Agents for Exchange on the rest of the nodes, select the DAG, click **Details**, and then click **Install agent** next to each of the nodes.

Backing up the Exchange cluster data

1. When creating a protection plan, select the DAG as described in "[Selecting Exchange Server data](#)".
2. Configure the "[Cluster backup mode](#)" backup option.
3. Specify other settings of the protection plan [as appropriate](#).

Important

For cluster-aware backup, ensure to select the DAG itself. If you select individual nodes or databases inside the DAG, only the selected items will be backed up and the **Cluster backup mode** option will be ignored.

Recovering the Exchange cluster data

1. Select the recovery point for the database that you want to recover. Selecting an entire cluster for recovery is not possible.

When you select a copy of a clustered database under **Devices > Microsoft Exchange > Databases > <cluster name> > <node name>** and click **Recover**, the software shows only the recovery points that correspond to the times when this copy was backed up.

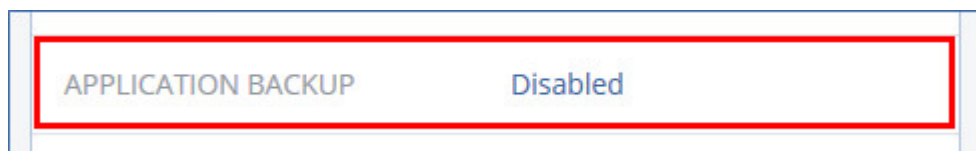
The easiest way to view all recovery points of a clustered database is to select its backup [on the Backup storage tab](#).

2. Follow the steps described in "Recovering Exchange databases", starting from step 5.
The software automatically defines a cluster node to which the data will be recovered. The node's name is displayed in the **Recover to** field. You can manually change the target node.

14.16.7 Application-aware backup

Application-aware disk-level backup is available for physical machines, ESXi virtual machines, and Hyper-V virtual machines.

When you back up a machine running Microsoft SQL Server, Microsoft Exchange Server, or Active Directory Domain Services, enable **Application backup** for additional protection of these applications' data.



Why use application-aware backup?

By using application-aware backup, you ensure that:

1. The applications are backed up in a consistent state and thus will be available immediately after the machine is recovered.
2. You can recover the SQL and Exchange databases, mailboxes, and mailbox items without recovering the entire machine.
3. The SQL transaction logs are truncated after each successful backup. SQL log truncation can be disabled in the [protection plan options](#). The Exchange transaction logs are truncated on virtual machines only. You can enable the [VSS full backup option](#) if you want to truncate Exchange transaction logs on a physical machine.
4. If a domain contains more than one domain controller, and you recover one of them, a nonauthoritative restore is performed and a USN rollback will not occur after the recovery.

What do I need to use application-aware backup?

On a physical machine, Agent for SQL and/or Agent for Exchange must be installed, in addition to Agent for Windows.

On a virtual machine, no agent installation is required; it is presumed that the machine is backed up by Agent for VMware (Windows) or Agent for Hyper-V.

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**.

Other requirements are listed in the ["Prerequisites"](#) and ["Required user rights"](#) sections.

Required user rights

An application-aware backup contains metadata of VSS-aware applications that are present on the disk. To access this metadata, the agent needs an account with the appropriate rights, which are listed below. You are prompted to specify this account when enabling application backup.

- For SQL Server:
The account must be a member of the **Backup Operators** or **Administrators** group on the machine, and a member of the **sysadmin** role on each of the instances that you are going to back up.

- For Exchange Server:
Exchange 2007: The account must be a member of the **Administrators** group on the machine, and a member of the **Exchange Organization Administrators** role group.
Exchange 2010 and later: The account must be a member of the **Administrators** group on the machine, and a member of the **Organization Management** role group.
- For Active Directory:
The account must be a domain administrator.

Additional requirement for virtual machines

If the application runs on a virtual machine that is backed up by Agent for VMware or Agent for Hyper-V, ensure that User Account Control (UAC) is disabled on the machine. If you do not want to disable UAC, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

14.16.8 Mailbox backup

Mailbox backup is supported for Microsoft Exchange Server 2010 Service Pack 1 (SP1) and later.

Mailbox backup is available if at least one Agent for Exchange is registered on the management server. The agent must be installed on a machine that belongs to the same Active Directory forest as Microsoft Exchange Server.

Before backing up mailboxes, you must connect Agent for Exchange to the machine running the **Client Access** server role (CAS) of Microsoft Exchange Server. In Exchange 2016 and later, the CAS role is not available as a separate installation option. It is automatically installed as part of the Mailbox server role. Thus, you can connect the agent to any server running the **Mailbox role**.

To connect Agent for Exchange to CAS

1. Click **Devices > Add**.
2. Click **Microsoft Exchange Server**.
3. Click **Exchange mailboxes**.
If no Agent for Exchange is registered on the management server, the software suggests that you install the agent. After the installation, repeat this procedure from step 1.
4. [Optional] If multiple Agents for Exchange are registered on the management server, click **Agent**, and then change the agent that will perform the backup.
5. In **Client Access server**, specify the fully qualified domain name (FQDN) of the machine where the **Client Access** role of Microsoft Exchange Server is enabled.
In Exchange 2016 and later, the Client Access services are automatically installed as part of the Mailbox server role. Thus, you can specify any server running the **Mailbox role**. We refer to this server as CAS later in this section.
6. In **Authentication type**, select the authentication type that is used by the CAS. You can select **Kerberos** (default) or **Basic**.

7. [Only for basic authentication] Select which protocol will be used. You can select **HTTPS** (default) or **HTTP**.
8. [Only for basic authentication with the HTTPS protocol] If the CAS uses an SSL certificate that was obtained from a certification authority, and you want the software to check the certificate when connecting to the CAS, select the **Check SSL certificate** check box. Otherwise, skip this step.
9. Provide the credentials of an account that will be used to access the CAS. The requirements for this account are listed in "[Required user rights](#)".
10. Click **Add**.

As a result, the mailboxes appear under **Devices > Microsoft Exchange > Mailboxes**.

Selecting Exchange Server mailboxes

Select the mailboxes as described below, and then specify other settings of the protection plan [as appropriate](#).

To select Exchange mailboxes

1. Click **Devices > Microsoft Exchange**.
The software shows the tree of Exchange databases and mailboxes.
2. Click **Mailboxes**, and then select the mailboxes that you want to back up.
3. Click **Protect**.

Required user rights

To access mailboxes, Agent for Exchange needs an account with the appropriate rights. You are prompted to specify this account when configuring various operations with mailboxes.

Membership of the account in the **Organization Management** role group enables access to any mailbox, including mailboxes that will be created in the future.

The minimum required user rights are as follows:

- The account must be a member of the **Server Management** and **Recipient Management** role groups.
- The account must have the **ApplicationImpersonation** management role enabled for all users or groups of users whose mailboxes the agent will access.
For information about configuring the **ApplicationImpersonation** management role, refer to the following Microsoft knowledge base article: <https://msdn.microsoft.com/en-us/library/office/dn722376.aspx>.

14.16.9 Recovering SQL databases

This section describes recovery from both database backups and application-aware backups.

You can recover SQL databases to a SQL Server instance, if Agent for SQL is installed on the machine running the instance. You will need to provide credentials for an account that is a member of the

Backup Operators or **Administrators** group on the machine and a member of the **sysadmin** role on the target instance.

Alternatively, you can recover the databases as files. This can be useful if you need to extract data for data mining, audit, or further processing by third-party tools. You can attach the SQL database files to a SQL Server instance, as described in ["Attaching SQL Server databases"](#).

If you use only Agent for VMware (Windows), recovering databases as files is the only available recovery method. Recovering databases by using Agent for VMware (Virtual Appliance) is not possible.

System databases are basically recovered in the same way as user databases. The peculiarities of system database recovery are described in ["Recovering system databases"](#).

To recover SQL databases to a SQL Server instance

1. Do one of the following:
 - When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
 - When recovering from a database backup, click **Devices > Microsoft SQL**, and then select the databases that you want to recover.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

If the machine is offline, the recovery points are not displayed. Do one of the following:

 - [Only when recovering from an application-aware backup] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for SQL, and then select a recovery point.
 - Select a recovery point on [the Backup storage tab](#).

The machine chosen for browsing in either of the above actions becomes a target machine for the SQL databases recovery.
4. Do one of the following:
 - When recovering from an application-aware backup, click **Recover > SQL databases**, select the databases that you want to recover, and then click **Recover**.
 - When recovering from a database backup, click **Recover > Databases to an instance**.
5. By default, the databases are recovered to the original ones. If the original database does not exist, it will be recreated. You can select another SQL Server instance (running on the same machine) to recover the databases to.

To recover a database as a different one to the same instance:

- a. Click the database name.
- b. In **Recover to**, select **New database**.
- c. Specify the new database name.
- d. Specify the new database path and log path. The folder you specify must not contain the original database and log files.

6. [Optional] [Not available for a database recovered to its original instance as a new database] To change the database state after recovery, click the database name, and then choose one of the following states:

- **Ready to use (RESTORE WITH RECOVERY)** (default)

After the recovery completes, the database will be ready for use. Users will have full access to it. The software will roll back all uncommitted transactions of the recovered database that are stored in the transaction logs. You will not be able to recover additional transaction logs from the native Microsoft SQL backups.

- **Non-operational (RESTORE WITH NORECOVERY)**

After the recovery completes, the database will be non-operational. Users will have no access to it. The software will keep all uncommitted transactions of the recovered database. You will be able to recover additional transaction logs from the native Microsoft SQL backups and thus reach the necessary recovery point.

- **Read-only (RESTORE WITH STANDBY)**

After the recovery completes, users will have read-only access to the database. The software will undo any uncommitted transactions. However, it will save the undo actions in a temporary standby file so that the recovery effects can be reverted.

This value is primarily used to detect the point in time when a SQL Server error occurred.

7. Click **Start recovery**.

The recovery progress is shown on the Activities tab.

To recover SQL databases as files

1. Do one of the following:

- When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
- When recovering from a database backup, click **Devices > Microsoft SQL**, and then select the databases that you want to recover.

2. Click **Recovery**.

3. Select a recovery point. Note that recovery points are filtered by location.

If the machine is offline, the recovery points are not displayed. Do one of the following:

- [Only when recovering from an application-aware backup] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for SQL or Agent for VMware, and then select a recovery point.
- Select a recovery point on [the Backup storage tab](#).

The machine chosen for browsing in either of the above actions becomes a target machine for the SQL databases recovery.

4. Do one of the following:

- When recovering from an application-aware backup, click **Recover > SQL databases**, select the databases that you want to recover, and then click **Recover as files**.
- When recovering from a database backup, click **Recover > Databases as files**.

5. Click **Browse**, and then select a local or a network folder to save the files to.
6. Click **Start recovery**.

The recovery progress is shown on the Activities tab.

Recovering system databases

All system databases of an instance are recovered at once. When recovering system databases, the software automatically restarts the destination instance in the single-user mode. After the recovery completes, the software restarts the instance and recovers other databases (if any).

Other things to consider when recovering system databases:

- System databases can only be recovered to an instance of the same version as the original instance.
- System databases are always recovered in the "ready to use" state.

Recovering the master database

System databases include the **master** database. The **master** database records information about all databases of the instance. Hence, the **master** database in a backup contains information about databases which existed in the instance at the time of the backup. After recovering the **master** database, you may need to do the following:

- Databases that have appeared in the instance after the backup was done are not visible by the instance. To bring these databases back to production, attach them to the instance manually by using SQL Server Management Studio.
- Databases that have been deleted after the backup was done are displayed as offline in the instance. Delete these databases by using SQL Server Management Studio.

Attaching SQL Server databases

This section describes how to attach a database in SQL Server by using SQL Server Management Studio. Only one database can be attached at a time.

Attaching a database requires any of the following permissions: **CREATE DATABASE**, **CREATE ANY DATABASE**, or **ALTER ANY DATABASE**. Normally, these permissions are granted to the **sysadmin** role of the instance.

To attach a database

1. Run Microsoft SQL Server Management Studio.
2. Connect to the required SQL Server instance, and then expand the instance.
3. Right-click **Databases** and click **Attach**.
4. Click **Add**.
5. In the **Locate Database Files** dialog box, find and select the .mdf file of the database.
6. In the **Database Details** section, make sure that the rest of database files (.ndf and .ldf files) are found.

Details. SQL Server database files may not be found automatically, if:

- They are not in the default location, or they are not in the same folder as the primary database file (.mdf). Solution: Specify the path to the required files manually in the **Current File Path** column.
- You have recovered an incomplete set of files that make up the database. Solution: Recover the missing SQL Server database files from the backup.

7. When all of the files are found, click **OK**.

14.16.10 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](#).

If you use only Agent for VMware (Windows), recovering databases as files is the only available recovery method. Recovering databases by using Agent for VMware (Virtual Appliance) is not possible.

We will refer to both databases and storage groups as "databases" throughout the below procedures.

To recover Exchange databases to a live Exchange Server

1. Do one of the following:
 - When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
 - When recovering from a database backup, click **Devices > Microsoft Exchange > Databases**, and then select the databases that you want to recover.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

If the machine is offline, the recovery points are not displayed. Do one of the following:

- [Only when recovering from an application-aware backup] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange, and then select a recovery point.
- Select a recovery point on [the Backup storage tab](#).

The machine chosen for browsing in either of the above actions becomes a target machine for the Exchange data recovery.

4. Do one of the following:
 - When recovering from an application-aware backup, click **Recover > Exchange databases**, select the databases that you want to recover, and then click **Recover**.
 - When recovering from a database backup, click **Recover > Databases to an Exchange server**.

5. By default, the databases are recovered to the original ones. If the original database does not exist, it will be recreated.

To recover a database as a different one:

- a. Click the database name.
 - b. In **Recover to**, select **New database**.
 - c. Specify the new database name.
 - d. Specify the new database path and log path. The folder you specify must not contain the original database and log files.
6. Click **Start recovery**.

The recovery progress is shown on the Activities tab.

To recover Exchange databases as files

1. Do one of the following:
 - When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
 - When recovering from a database backup, click **Devices > Microsoft Exchange > Databases**, and then select the databases that you want to recover.

2. Click **Recovery**.

3. Select a recovery point. Note that recovery points are filtered by location.

If the machine is offline, the recovery points are not displayed. Do one of the following:

- [Only when recovering from an application-aware backup] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
- Select a recovery point on [the Backup storage tab](#).

The machine chosen for browsing in either of the above actions becomes a target machine for the Exchange data recovery.

4. Do one of the following:

- When recovering from an application-aware backup, click **Recover > Exchange databases**, select the databases that you want to recover, and then click **Recover as files**.
 - When recovering from a database backup, click **Recover > Databases as files**.
5. Click **Browse**, and then select a local or a network folder to save the files to.
 6. Click **Start recovery**.

The recovery progress is shown on the Activities tab.

Mounting Exchange Server databases

After recovering the database files, you can bring the databases online by mounting them. Mounting is performed by using Exchange Management Console, Exchange System Manager, or Exchange Management Shell.

The recovered databases will be in a Dirty Shutdown state. A database that is in a Dirty Shutdown state can be mounted by the system if it is recovered to its original location (that is, information about the original database is present in Active Directory). When recovering a database to an alternate location (such as a new database or as the recovery database), the database cannot be mounted until you bring it to a Clean Shutdown state by using the `Eseutil /r <Enn>` command. `<Enn>` specifies the log file prefix for the database (or storage group that contains the database) into which you need to apply the transaction log files.

The account you use to attach a database must be delegated an Exchange Server Administrator role and a local Administrators group for the target server.

For details about how to mount databases, see the following articles:

- Exchange 2010 or later: <http://technet.microsoft.com/en-us/library/aa998871.aspx>
- Exchange 2007: [http://technet.microsoft.com/en-us/library/aa998871\(v=EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx)

14.16.11 Recovering Exchange mailboxes and mailbox items

This section describes how to recover Exchange mailboxes and mailbox items from database backups, from application-aware backups, and from mailbox backups. The mailboxes or mailbox items can be recovered to a live Exchange Server or to Microsoft 365.

The following items can be recovered:

- Mailboxes (except for archive mailboxes)
- Public folders
- Public folder items
- Email folders
- Email messages
- Calendar events
- Tasks
- Contacts

- Journal entries
- Notes

You can use search to locate the items.

Recovery to an Exchange Server

Granular recovery can be performed to Microsoft Exchange Server 2010 Service Pack 1 (SP1) and later. The source backup may contain databases or mailboxes of any supported Exchange version.

Granular recovery can be performed by Agent for Exchange or Agent for VMware (Windows). The target Exchange Server and the machine running the agent must belong to the same Active Directory forest.

When a mailbox is recovered to an existing mailbox, the existing items with matching IDs are overwritten.

Recovery of mailbox items does not overwrite anything. Instead, the full path to a mailbox item is recreated in the target folder.

Requirements on user accounts

A mailbox being recovered from a backup must have an associated user account in Active Directory.

User mailboxes and their contents can be recovered only if their associated user accounts are *enabled*. Shared, room, and equipment mailboxes can be recovered only if their associated user accounts are *disabled*.

A mailbox that does not meet the above conditions is skipped during recovery.

If some mailboxes are skipped, the recovery will succeed with warnings. If all mailboxes are skipped, the recovery will fail.

Recovery to Microsoft 365

Recovery of Exchange data items to Microsoft 365, and vice versa, is supported on the condition that Agent for Microsoft 365 is installed locally.

Recovery can be performed from backups of Microsoft Exchange Server 2010 and later.

When a mailbox is recovered to an existing Microsoft 365 mailbox, the existing items are kept intact, and the recovered items are placed next to them.

When recovering a single mailbox, you need to select the target Microsoft 365 mailbox. When recovering several mailboxes within one recovery operation, the software will try to recover each mailbox to the mailbox of the user with the same name. If the user is not found, the mailbox is skipped. If some mailboxes are skipped, the recovery will succeed with warnings. If all mailboxes are skipped, the recovery will fail.

For more information about recovery to Microsoft 365, refer to "[Protecting Microsoft 365 mailboxes](#)".

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 Microsoft 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 Microsoft 365 in your organization, install Agent for Microsoft 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 Microsoft 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 Microsoft 365, as described in "[Copying Microsoft Exchange libraries](#)".
2. Do one of the following:
 - When recovering from an application-aware backup: under **Devices**, select the machine that originally contained the data that you want to recover.
 - When recovering from a database backup, click **Devices > Microsoft Exchange > Databases**, and then select the database that originally contained the data that you want to recover.
3. Click **Recovery**.
4. Select a recovery point. Note that recovery points are filtered by location.

If the machine is offline, the recovery points are not displayed. Use other ways to recover:

 - [Only when recovering from an application-aware backup] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
 - Select a recovery point on [the Backup storage tab](#).

The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
5. Click **Recover > Exchange mailboxes**.
6. Select the mailboxes that you want to recover.

You can search mailboxes by name. Wildcards are not supported.



7. Click **Recover**.
8. [Only when recovering to Microsoft 365]:

- a. In **Recover to**, select **Microsoft 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.

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.

9. 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"](#).
10. [Optional] Click **Database to re-create any missing mailboxes** to change the automatically selected database.
11. Click **Start recovery**.

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

To recover a mailbox from a mailbox backup

1. Click **Devices > Microsoft Exchange > Mailboxes**.
2. Select the mailbox to recover, and then click **Recovery**.
You can search mailboxes by name. Wildcards are not supported.
If the mailbox was deleted, select it on [the Backup storage tab](#), and then click **Show backups**.
3. Select a recovery point. Note that recovery points are filtered by location.
4. Click **Recover > Mailbox**.
5. Perform steps 8-11 of the above procedure.

Recovering mailbox items

To recover mailbox items from an application-aware backup or a database backup

1. [Only when recovering from a database backup to Microsoft 365] If Agent for Microsoft 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 Microsoft 365 in your organization, install Agent for Microsoft 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 Microsoft 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 Microsoft 365, as described in ["Copying Microsoft Exchange libraries"](#).
2. Do one of the following:
 - When recovering from an application-aware backup: under **Devices**, select the machine that originally contained the data that you want to recover.

- When recovering from a database backup, click **Devices > Microsoft Exchange > Databases**, and then select the database that originally contained the data that you want to recover.
3. Click **Recovery**.
 4. Select a recovery point. Note that recovery points are filtered by location.
If the machine is offline, the recovery points are not displayed. Use other ways to recover:
 - [Only when recovering from an application-aware backup] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
 - Select a recovery point on [the Backup storage tab](#).

The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
 5. Click **Recover > Exchange mailboxes**.
 6. Click the mailbox that originally contained the items that you want to recover.
 7. Select the items that you want to recover.

The following search options are available. Wildcards are not supported.

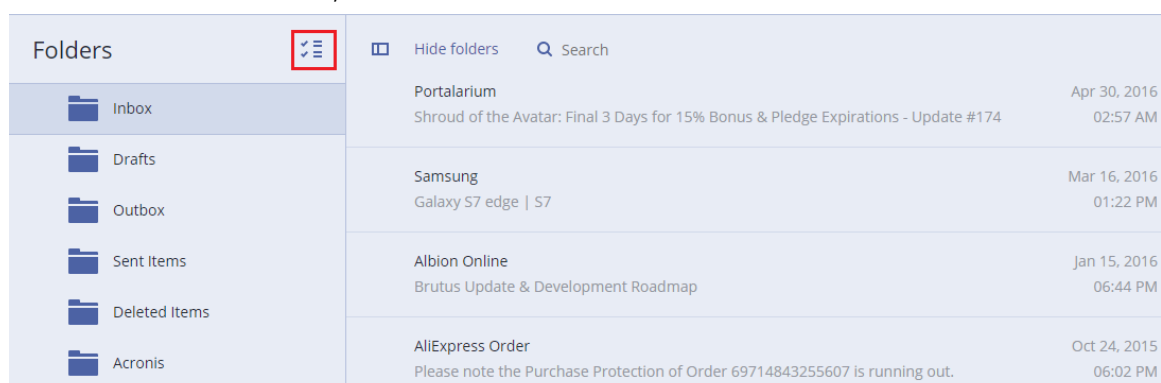
- For email messages: search by subject, sender, recipient, and date.
- For events: search by title and date.
- For tasks: search by subject and date.
- For contacts: search by name, email address, and phone number.

When an email message is selected, you can click **Show content** to view its contents, including attachments.

Note

Click the name of an attached file to download it.

To be able to select folders, click the recover folders icon.



8. Click **Recover**.
9. To recover to Microsoft 365, select **Microsoft 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](#)".

11. In **Target mailbox**, view, change, or specify the target mailbox.

By default, the original mailbox is selected. If this mailbox does not exist or a non-original target machine is selected, you must specify the target mailbox.

12. [Only when recovering email messages] In **Target folder**, view or change the target folder in the target mailbox. By default, the **Recovered items** folder is selected. Due to Microsoft Exchange limitations, events, tasks, notes, and contacts are restored to their original location regardless of any different **Target folder** specified.

13. Click **Start recovery**.

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

To recover a mailbox item from a mailbox backup

1. Click **Devices > Microsoft Exchange > Mailboxes**.

2. Select the mailbox that originally contained the items that you want to recover, and then click **Recovery**.

You can search mailboxes by name. Wildcards are not supported.

If the mailbox was deleted, select it on [the Backup storage tab](#), and then click **Show backups**.

3. Select a recovery point. Note that recovery points are filtered by location.
4. Click **Recover > Email messages**.
5. Select the items that you want to recover.

The following search options are available. Wildcards are not supported.

- For email messages: search by subject, sender, recipient, and date.
- For events: search by title and date.
- For tasks: search by subject and date.
- For contacts: search by name, email address, and phone number.

When an email message is selected, you can click **Show content** to view its contents, including attachments.

Note

Click the name of an attached file to download it.

When an email message is selected, you can click **Send as email** to send the message to an email address. The message is sent from your administrator account's email address.

To be able to select folders, click the recover folders icon:



6. Click **Recover**.
7. Perform steps 9-13 of the above procedure.

Copying Microsoft Exchange Server libraries

When [recovering Exchange mailboxes or mailbox items to Microsoft 365](#), you may need to copy the following libraries from the machine that was backed up (or from another machine with the same Microsoft Exchange Server version) to the machine with Agent for Microsoft 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	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
	esebcli2.dll	
	store.exe	
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	
	msvcpr110.dll	%WINDIR%\system32

The libraries should be placed in the folder **%ProgramData%\Acronis\ese**. If this folder does not exist, create it manually.

14.16.12 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**.

14.17 Protecting mobile devices

The 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.

14.17.1 Supported mobile devices

You can install the Cyber Protect app on a mobile device that runs one of the following operating systems:

- iOS 11.1 and later (iPhone, iPod, and iPads)
- Android 6.0 and later

14.17.2 What you can back up

- Contacts
- Photos
- Videos
- Calendars
- Reminders (only on iOS devices)

14.17.3 What you need to know

- You can back up the data only to the cloud storage.
- Any time you open the app, you will see the summary of data changes and can start a backup manually.
- The **Continuous backup** functionality is enabled by default. If this setting is turned on:
 - For Android 7.0 or higher, the Cyber Protect app automatically detects new data on-the-fly and uploads it to the Cloud,
 - For Android 6, it checks for changes every three hours. You can turn off continuous backup in the app settings.
- The **Use Wi-Fi only** option is enabled by default in the app settings. If this setting is turned on, the 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 Cyber Protect app from proper operation. To run backups on time, you should stop the battery optimization for the app.
- You have two ways to save energy:
 - The **Back up while charging** functionality which is disabled by default. If this setting is turned on, the 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** which is enabled by default. If this setting is turned on, the 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. This option is available for Android 8 or higher.
- You can access the backed-up data from any mobile device registered under your account. This helps you transfer the data from an old mobile device to a new one. Contacts and photos from an Android device can be recovered to an iOS device and vice versa. You can also download a photo, video, or contact to any device by using the service 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 Cyber Protect app, you can recover only the latest data versions. If you need to recover from a specific backup version, use the service 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.

14.17.4 Where to get the Cyber Protect app

Depending on your mobile device, install the app from the App Store or Google Play.

14.17.5 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 occurs 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**.
7. Allow the app access to your personal data. If you deny access to some data categories, they will not be backed up.

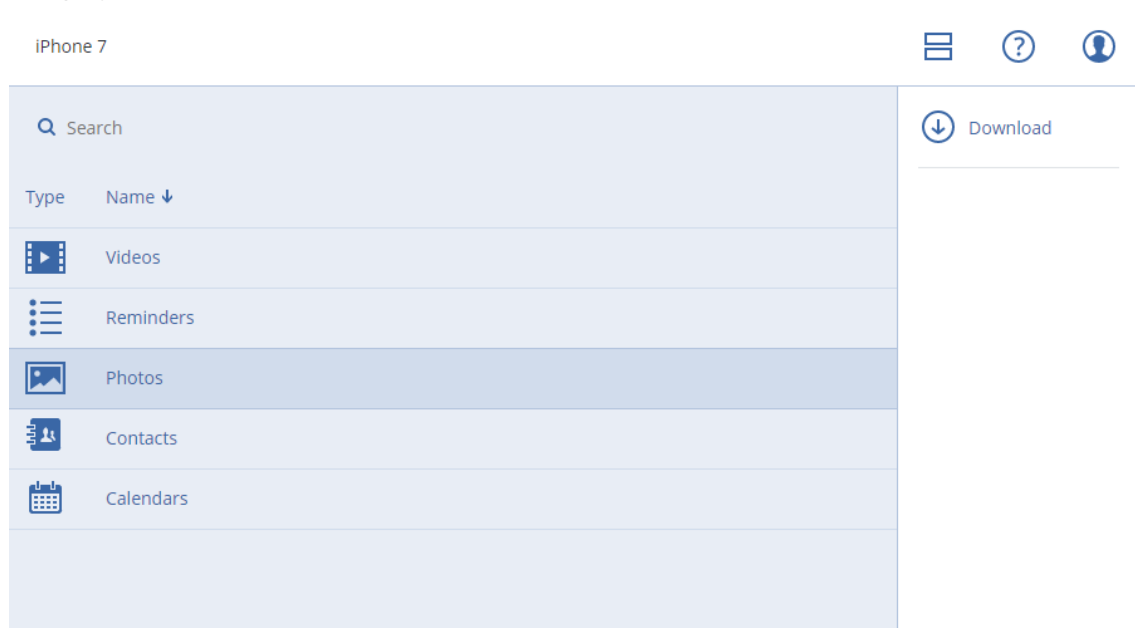
The backup starts.

14.17.6 How to recover data to a mobile device

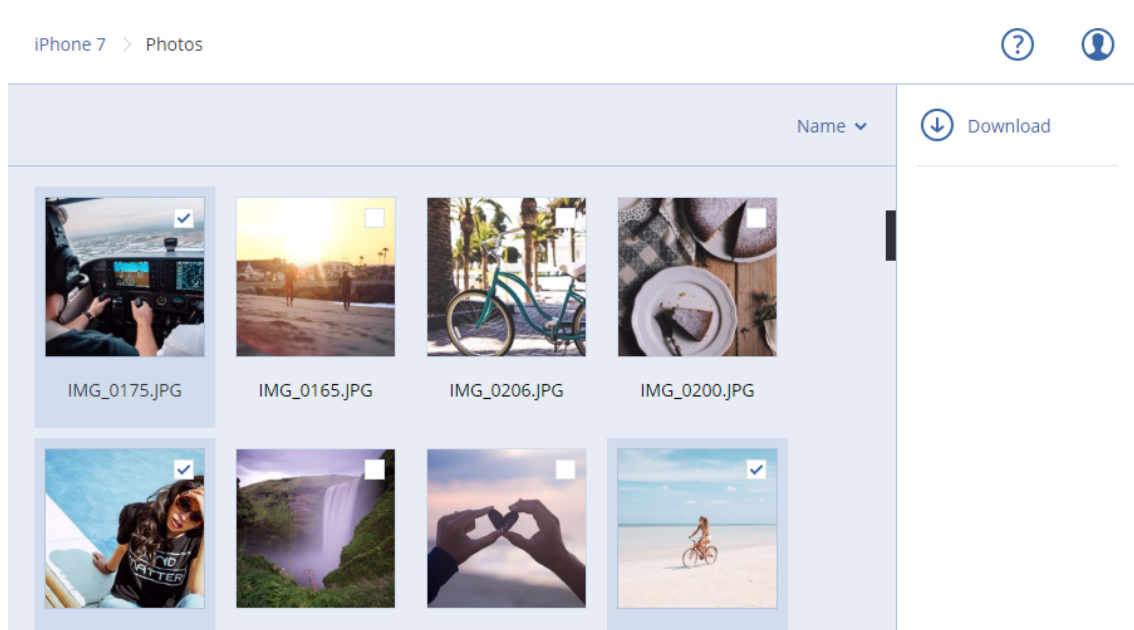
1. Open the Cyber Protect app.
2. Tap **Browse**.
3. Tap the device name.
4. Do one of the following:
 - To recover all of the backed-up data, tap **Recover all**. No more actions are required.
 - To recover one or more data categories, tap **Select**, and then tap the check boxes for the required data 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**.

14.17.7 How to review data via the service console

1. On a computer, open a browser and type the service console URL.
2. Sign in with your account.
3. In **All devices**, click **Recover** under your mobile device name.
4. Do any of the following:
 - To download all photos, videos, contacts, calendars, or reminders, select the respective data category. Click **Download**.



- To download individual photos, videos, contacts, calendars, or reminders, click the respective data category name, and then select the check boxes for the required data items. Click **Download**.



- To preview a photo, or a contact, click the respective data category name, and then click the required data item.

14.18 Protecting Hosted Exchange data

14.18.1 What items can be backed up?

You can back up user mailboxes, shared mailboxes, and group mailboxes. Optionally, you can choose to back up the archive mailboxes (**In-Place Archive**) of the selected mailboxes.

14.18.2 What items can be recovered?

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.

When recovering mailboxes, mailbox items, public folders, and public folder items, you can select whether to overwrite the items in the target location.

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.

14.18.3 Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the protection plan [as appropriate](#).

To select Exchange Online mailboxes

1. Click **Devices > Hosted Exchange**.
2. If multiple Hosted Exchange organizations were added to the Cyber Protection service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up the mailboxes of all users and all shared mailboxes (including mailboxes that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
 - To back up individual user or shared mailboxes, expand the **Users** node, select **All users**, select the users whose mailboxes you want to back up, and then click **Backup**.
 - To back up all group mailboxes (including mailboxes of groups that will be created in the future), expand the **Groups** node, select **All groups**, and then click **Group backup**.
 - To back up individual group mailboxes, expand the **Groups** node, select **All groups**, select the groups whose mailboxes you want to back up, and then click **Backup**.

14.18.4 Recovering mailboxes and mailbox items

Recovering mailboxes

1. Click **Devices > Hosted Exchange**.
2. If multiple Hosted Exchange organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
 - To recover a user mailbox, expand the **Users** node, select **All users**, select the user whose mailbox you want to recover, and then click **Recovery**.
 - To recover a shared mailbox, expand the **Users** node, select **All users**, select the shared mailbox that you want to recover, and then click **Recovery**.
 - To recover a group mailbox, expand the **Groups** node, select **All groups**, select the group whose mailbox you want to recover, and then click **Recovery**.


- If the user, group, or the shared mailbox was deleted, select the item in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search users and groups by name. Wildcards are not supported.

4. Select a recovery point.
5. Click **Recover > Entire mailbox**.
6. If multiple Hosted Exchange organizations are added to the Cyber Protection service, click **Hosted Exchange organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
7. In **Recover to 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 organization is selected, you must specify the target mailbox.
8. Click **Start recovery**.
9. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
10. Click **Proceed** to confirm your decision.

Recovering mailbox items

1. Click **Devices > Hosted Exchange**.
2. If multiple Hosted Exchange organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
 - To recover items from a user mailbox, expand the **Users** node, select **All users**, select the user whose mailbox originally contained the items that you want to recover, and then click **Recovery**.
 - To recover items from a shared mailbox, expand the **Users** node, select **All users**, select the shared mailbox that originally contained the items that you want to recover, and then click **Recovery**.
 - To recover items from a group mailbox, expand the **Groups** node, select **All groups**, select the group whose mailbox originally contained the items that you want to recover, and then click **Recovery**.
 - If the user, group, or the shared mailbox was deleted, select the item in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.
You can search users and groups by name. Wildcards are not supported.
4. Select a recovery point.
5. Click **Recover > Email messages**.
6. Browse to the required folder or use search to obtain the list of the required items.
The following search options are available. Wildcards are not supported.

- For email messages: search by subject, sender, recipient, attachment name, 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.
7. Select the items that you want to recover. To be able to select folders, click the "recover folders" icon:  icon:
Additionally, you can do any of the following:
 - When an item is selected, click **Show content** to view its contents, including attachments. Click the name of an attached file to download it.
 - When an email message or a calendar item is selected, click **Send as email** to send the item to the specified email addresses. You can select the sender and write a text to be added to the forwarded item.
 - Only if the backup is not encrypted, you used search, and selected a single item in the search results: click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
 8. Click **Recover**.
 9. If multiple Hosted Exchange organizations were added to the Cyber Protection service, click **Hosted Exchange organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
 10. In **Recover to 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 organization is selected, you must specify the target mailbox.
 11. [Only when recovering to a user or a shared mailbox] In **Path**, view or change the target folder in the target mailbox. By default, the **Recovered items** folder is selected.
Group mailbox items are always recovered to the **Inbox** folder.
 12. Click **Start recovery**.
 13. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
 14. Click **Proceed** to confirm your decision.

14.19 Protecting Microsoft 365 data

14.19.1 Why back up Microsoft 365 data?

Even though Microsoft 365 is a set of cloud services, 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 Exchange Online mailboxes if it is required for regulatory compliance.

14.19.2 Agent for Microsoft 365

Depending on the desired functionality, you can choose to install Agent for Microsoft 365 locally, use the agent installed in the cloud, or both. The following table summarizes the functionality of the local and the cloud agent.

	Local Agent for Microsoft 365	Cloud Agent for Microsoft 365
Data items that can be backed up	Exchange Online: user and shared mailboxes	<ul style="list-style-type: none"> • Exchange Online: user, shared, and group mailboxes; public folders • OneDrive: user files and folders • SharePoint Online: classic site collections, group (team) sites, communication sites, individual data items • Microsoft 365 Teams: entire teams, team channels, channel files, team mailboxes, files and email messages in team mailboxes, meetings, team sites
Backup of archive mailboxes (In-Place Archive)	No	Yes
Backup schedule	User-defined	Cannot be changed. Each protection plan runs daily at the same time of day.*
Backup locations	Cloud storage, local folder, network folder	Cloud storage only
Automatic protection of new Microsoft 365 users, groups, sites, and teams	No	Yes, by applying a protection plan to the All users, All groups, All sites, All teams groups
Protecting more than one Microsoft 365 organization	No	Yes
Granular recovery	Yes	Yes
Recovery to another user within one organization	Yes	Yes
Recovery to another organization	No	Yes
Recovery to an on-	No	No

premises Microsoft Exchange Server		
Maximum number of items that can be backed up without performance degradation	<p>When backing up to the cloud storage: 5000 mailboxes per company</p> <p>When backing up to other destinations: 2000 mailboxes per protection plan (no limitation for number of mailboxes per company)</p>	10 000 protected items (mailboxes, OneDrives, or sites) per company**
Maximum number of manual backup runs	No	10 manual runs during an hour
Maximum number of simultaneous recovery operations	No	10 operations, including Google Workspace recovery operations

* Because a cloud agent serves multiple customers, it determines the start time for each protection plan on its own, to ensure even load during a day and the equal quality of service for all customers.

Note

The protection schedule might be affected by the operation of third-party services, for example, the accessibility of Microsoft 365 servers, throttling settings on the Microsoft servers, and others. See also <https://docs.microsoft.com/en-us/graph/throttling>.

** It is recommended that you back up your protected items gradually and in this order:

1. Mailboxes.
2. After all mailboxes are backed up, proceed with OneDrives.
3. After OneDrive backup is completed, proceed with the SharePoint Online sites.

The first full backup may take several days, depending on the number of protected items and their size.

14.19.3 Limitations

- Only users with an assigned Microsoft 365 license can have their mailboxes and OneDrives 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.
- Automatic creation of users, public folders, groups, or sites during a recovery is not possible. For example, if you want to recover a deleted SharePoint Online site, first create a new site manually, and then specify it as the target site during a recovery.

- You cannot simultaneously recover items from different recovering points, even though you can select such items from the search results.
- During a backup, any sensitivity labels that are applied to the content will be preserved. Therefore, sensitive content might not be shown if it is recovered to a non-original location and its user has different access permissions.

14.19.4 Required user rights

In the Cyber Protection service

The local Agent for Microsoft 365 must be registered under a company administrator account and used on the customer tenant level. Company administrators acting on the unit level, unit administrators, and users cannot back up or recover Microsoft 365 data.

The cloud Agent for Microsoft 365 can be used both on a customer tenant level and on a unit level. For more information about these levels and their respective administrators, refer to "Administering Microsoft 365 organizations added on different levels" (p. 292).

In Microsoft 365

Your account must be assigned the global administrator role in Microsoft 365.

To back up and recover Microsoft 365 public folders, at least one of your Microsoft 365 administrator accounts must have a mailbox and read/write rights to the public folders that you want to back up.

- The local agent will log in to Microsoft 365 by using this account. To enable the agent to access the contents of all mailboxes, this account will be assigned the **ApplicationImpersonation** management role. If you change this account password, update the password in the service console, as described in "[Changing the Microsoft 365 access credentials](#)".
- The cloud agent does not log in to Microsoft 365. The agent is given the necessary permissions directly by Microsoft 365. You only need to confirm granting these permissions once, being signed in as a global administrator. The agent does not store your account credentials and does not use them to perform backup and recovery. Changing this account password or disabling this account or deleting this account in Microsoft 365 does not affect agent operation.

14.19.5 Using the locally installed Agent for Office 365

Adding a Microsoft 365 organization

To add a Microsoft 365 organization

1. Sign in to the service console as a company administrator.
2. Click the account icon in the top-right corner, and then click **Downloads > Agent for Office 365**.
3. Download the agent and install it on a Windows machine that is connected to the Internet.

4. After the installation is complete, click **Devices > Microsoft Office 365**, and then enter the Microsoft 365 global administrator credentials.

Important

There must be only one locally installed Agent for Microsoft 365 in an organization (company group).

As a result, your organization data items appear in the service console, on the **Microsoft Office 365** page.

Protecting Exchange Online mailboxes

What items can be backed up?

You can back up user mailboxes and shared mailboxes. Group mailboxes and archive mailboxes (**In-Place Archive**) cannot be backed up.

What items can be recovered?

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.

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.

Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the protection plan [as appropriate](#).

To select mailboxes

1. Click **Microsoft Office 365**.
2. If prompted, sign in as a global administrator to Microsoft 365.

3. Select the mailboxes that you want to back up.
4. Click **Backup**.

Recovering mailboxes and mailbox items

Recovering mailboxes

1. Click **Microsoft Office 365**.
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. 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.
6. Click **Start recovery**.

Recovering mailbox items

1. Click **Microsoft Office 365**.
2. Select the mailbox that originally contained the items that you want to recover, and then click **Recovery**.

You can search mailboxes by name. Wildcards are not supported.

If the mailbox was deleted, select it on [the Backup storage tab](#), and then click **Show backups**.

3. Select a recovery point. Note that recovery points are filtered by location.
4. Click **Recover > Email messages**.
5. Select the items that you want to recover.

The following search options are available. Wildcards are not supported.

- For email messages: search by subject, sender, recipient, attachment name, 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. 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**.
9. Confirm your decision.

The mailbox items are always recovered to the **Recovered items** folder of the target mailbox.

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. Click **Devices > Microsoft Office 365**.
2. Click **Specify credentials**.
3. Enter the Microsoft 365 global administrator credentials, and then click **OK**.
The agent will log in to Microsoft 365 by using this account. To enable the agent to access the contents of all mailboxes, this account will be assigned the **ApplicationImpersonation** management role.

14.19.6 Using the cloud Agent for Microsoft 365

Adding a Microsoft 365 organization

A Microsoft 365 organization can be added to a customer tenant or to a unit in this tenant.

Company administrators add organizations to customer tenants. Unit administrators and customer administrators acting on the unit level add organizations to units.

To add a Microsoft 365 organization

1. Depending on where you need to add the organization, sign in to the service console as a company administrator or unit administrator.
2. [For company administrators acting on the unit level] In the management portal, navigate to the desired unit.
3. Click **Devices > Add > Microsoft 365 Business**.
The software redirects you to the Microsoft 365 login page.
4. Sign in with the Microsoft 365 global administrator credentials.
Microsoft 365 displays a list of permissions that are necessary to back up and recover your organization's data.
5. Confirm that you grant the Cyber Protection service these permissions.

As a result, your Microsoft 365 organization appears under the **Devices** tab in the service console.

Useful tips

- The cloud agent synchronizes with Microsoft 365 every 24 hours, starting from the moment when the organization is added to the Cyber Protection service. If you add or remove a user, group, or site, you will not see this change in the service console immediately. To synchronize the change immediately, select the organization on the **Microsoft 365** page, and then click **Refresh**.
- If you applied a protection plan to the **All users**, **All groups**, or **All sites** group, the newly added items will be included in the backup only after synchronization.
- According to Microsoft policy, when a user, group, or site is removed from the Microsoft 365 graphical user interface, it remains available via an API for a few days. During this period, the removed item is inactive (grayed out) in the service console and is not backed up. When the removed item becomes unavailable via the API, it disappears from the service console. Its backups (if any) can be found at **Backup Storage > Cloud applications backups**.

Administering Microsoft 365 organizations added on different levels

Company administrators have full access to the Microsoft 365 organizations that are added to the customer tenant level.

Company administrators have limited access to the organizations that are added to a unit. In these organizations, shown with the unit name in brackets, company administrators can do the following:

- Recover data from backups.
Company administrators can recover data to all organizations in the tenant, regardless of the level on which these organizations are added.
- Browse backups and recovery points in backups.
- Delete backups and recovery points in backups.
- View alerts and activities.

Company administrators, when acting on the customer tenant level, cannot do the following:

- Add Microsoft 365 organizations to units.
- Delete Microsoft 365 organizations from units.
- Synchronize Microsoft 365 organizations that were added to a unit.
- View, create, edit, delete, apply, run, or revoke protection plans for data items in the Microsoft 365 organizations that are added to a unit.

Unit administrators and company administrators acting on the unit level have full access to the organizations that are added to a unit. However, they do not have access to any resources from the parent customer tenant, including the protection plans that are created in it.

Deleting a Microsoft 365 organization

Deleting a Microsoft 365 organization does not affect the existing backups of this organization's data. If you do not need these backups anymore, delete them first, and then delete the Microsoft 365 organization. Otherwise, the backups will still use cloud storage space that might be billed.

For more information about how to delete backups, see "To delete backups of any machine" (p. 254).

To delete a Microsoft 365 organization

1. Depending on where the organization is added, sign in to the service console as a company administrator or unit administrator.
2. [For company administrators acting on the unit level] In the management portal, navigate to the desired unit.
3. Go to **Devices > Microsoft 365**.
4. Select the organization, and then click **Delete group**.

As a result, the backup plans applied to this group will be revoked.

However, you should additionally revoke access rights of the Backup Service application to Microsoft 365 organization data manually.

To revoke access rights

1. Log in to Microsoft 365 under a global administrator.
2. Go to **Admin Center > Azure Active Directory > Enterprise applications > All applications**.
3. Select the **Backup Service** application and drill down to it.
4. Go to the **Properties** tab, and then, on the action panel, click **Delete**.
5. Confirm the deletion operation.

As a result, access rights to the Microsoft 365 organization data will be revoked from the Backup Service application.

Protecting Exchange Online data

What items can be backed up?

You can back up user mailboxes, shared mailboxes, and group mailboxes. Optionally, you can choose to back up the archive mailboxes (**In-Place Archive**) of the selected mailboxes.

Starting from version 8.0 of the Cyber Protection service, you can back up public folders. If your organization was added to the Cyber Protection service before the version 8.0 release, you need to re-add the organization to obtain this functionality. Do not delete the organization, simply repeat the steps described in "[Adding a Microsoft 365 organization](#)". As a result, the Cyber Protection service obtains the permission to use the corresponding API.

What items can be recovered?

The following items can be recovered from a mailbox backup:

- Mailboxes
- Email folders
- Email messages
- Calendar events

- Tasks
- Contacts
- Journal entries
- Notes

The following items can be recovered from a public folder backup:

- Subfolders
- Posts
- Email messages

You can use search to locate the items.

When recovering mailboxes, mailbox items, public folders, and public folder items, you can select whether to overwrite the items in the target location.

Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the protection plan [as appropriate](#).

To select Exchange Online mailboxes

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up the mailboxes of all users and all shared mailboxes (including mailboxes that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
 - To back up individual user or shared mailboxes, expand the **Users** node, select **All users**, select the users whose mailboxes you want to back up, and then click **Backup**.
 - To back up all group mailboxes (including mailboxes of groups that will be created in the future), expand the **Groups** node, select **All groups**, and then click **Group backup**.
 - To back up individual group mailboxes, expand the **Groups** node, select **All groups**, select the groups whose mailboxes you want to back up, and then click **Backup**.

Note

The cloud Agent for Microsoft 365 uses an account with the appropriate rights to access a group mailbox. Thus, to back up a group mailbox, at least one of the group owners must be licensed Microsoft 365 user with a mailbox. If the group is private or with hidden membership, the owner must also be a member of the group.

4. On the protection plan panel:

- Ensure that the **Microsoft 365 mailboxes** item is selected in **What to back up**.
If some of the individually selected users do not have the Exchange service included in their Microsoft 365 plan, you will not be able to select this option.
If some of the selected users for group backup do not have the Exchange service included in their Microsoft 365 plan, you will be able to select this option, but the protection plan will not be applied to those users.
- If you do not want to backup the archive mailboxes, disable the **Archive mailbox** switch.

Selecting public folders

Select the public folders as described below, and then specify other settings of the protection plan [as appropriate](#).

Note

Public folders consume licenses from your backup quota for Microsoft 365 seats.

To select Exchange Online public folders

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, expand the organization whose data you want to back up. Otherwise, skip this step.
3. Expand the **Public folders** node, and then select **All public folders**.
4. Do one of the following:
 - To back up all public folders (including public folders that will be created in the future), click **Group backup**.
 - To back up individual public folders, select the public folders that you want to back up, and then click **Backup**.
5. On the protection plan panel, ensure that the **Microsoft 365 mailboxes** item is selected in **What to back up**.

Recovering mailboxes and mailbox items

Recovering mailboxes

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
 - To recover a user mailbox, expand the **Users** node, select **All users**, select the user whose mailbox you want to recover, and then click **Recovery**.
 - To recover a shared mailbox, expand the **Users** node, select **All users**, select the shared mailbox that you want to recover, and then click **Recovery**.
 - To recover a group mailbox, expand the **Groups** node, select **All groups**, select the group whose mailbox you want to recover, and then click **Recovery**.

- If the user, group, or the shared mailbox was deleted, select the item in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search users and groups by name. Wildcards are not supported.

4. Select a recovery point.

Note

To see only the recovery points that contain mailboxes, select **Mailboxes** in **Filter by content**.

5. Click **Recover > Entire mailbox**.
6. If multiple Microsoft 365 organizations are added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
7. In **Recover to 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 organization is selected, you must specify the target mailbox.
You cannot create a new target mailbox during recovery. To recover a mailbox to a new one, first you need to create the target mailbox in the desired Microsoft 365 organization, and then let the cloud agent synchronize the change. The cloud agent automatically synchronizes with Microsoft 365 every 24 hours. To synchronize the change immediately, in the service console, select the organization on the **Microsoft 365** page, and then click **Refresh**.
8. Click **Start recovery**.
9. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
10. Click **Proceed** to confirm your decision.

Recovering mailbox items

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
 - To recover items from a user mailbox, expand the **Users** node, select **All users**, select the user whose mailbox originally contained the items that you want to recover, and then click **Recovery**.
 - To recover items from a shared mailbox, expand the **Users** node, select **All users**, select the shared mailbox that originally contained the items that you want to recover, and then click **Recovery**.
 - To recover items from a group mailbox, expand the **Groups** node, select **All groups**, select the group whose mailbox originally contained the items that you want to recover, and then click **Recovery**.

- If the user, group, or the shared mailbox was deleted, select the item in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search users and groups by name. Wildcards are not supported.

4. Select a recovery point.

Note

To see only the recovery points that contain mailboxes, select **Mailboxes** in **Filter by content**.

5. Click **Recover > Email messages**.
6. Browse to the required folder or use search to obtain the list of the required items.
The following search options are available. Wildcards are not supported.
 - For email messages: search by subject, sender, recipient, attachment name, 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.
7. Select the items that you want to recover. To be able to select folders, click the "recover folders"

icon: 

Additionally, you can do any of the following:

- When an item is selected, click **Show content** to view its contents, including attachments. Click the name of an attached file to download it.
- When an email message or a calendar item is selected, click **Send as email** to send the item to the specified email addresses. You can select the sender and write a text to be added to the forwarded item.
- Only if the backup is not encrypted, you used search, and selected a single item in the search results: click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.

8. Click **Recover**.
9. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
10. In **Recover to 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 organization is selected, you must specify the target mailbox.
11. [Only when recovering to a user or a shared mailbox] In **Path**, view or change the target folder in the target mailbox. By default, the **Recovered items** folder is selected.
Group mailbox items are always recovered to the **Inbox** folder.
12. Click **Start recovery**.
13. Select one of the overwriting options:

- **Overwrite existing items**
- **Do not overwrite existing items**

14. Click **Proceed** to confirm your decision.

Recovering public folders and folder items

In order to recover a public folder or public folder items, at least one administrator of the target Microsoft 365 organization must have the **Owner's** rights for the target public folder. If the recovery fails with an error about denied access, assign these rights in the target folder properties, select the target organization in the service console, click **Refresh**, and then repeat the recovery.

To recover a public folder or folder items

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations are added to the Cyber Protection service, expand the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
 - Expand the **Public folders** node, select **All public folders**, select the public folder that you want to recover or that originally contained the items that you want to recover, and then click **Recovery**.
 - If the public folder was deleted, select it in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search public folders by name. Wildcards are not supported.

4. Select a recovery point.
5. Click **Recover data**.
6. Browse to the required folder or use search to obtain the list of the required items.
You can search email messages and posts by subject, sender, recipient, and date. Wildcards are not supported.
7. Select the items that you want to recover. To be able to select folders, click the "recover folders"

icon: 

Additionally, you can do any of the following:

- When an email message or a post is selected, click **Show content** to view its contents, including attachments. Click the name of an attached file to download it.
 - When an email message or a post is selected, click **Send as email** to send the item to specified email addresses. You can select the sender and write a text to be added to the forwarded item.
 - Only if the backup is not encrypted, you used search, and selected a single item in the search results: click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. Click **Recover**.
 9. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.

By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.

10. In **Recover to public folder**, view, change, or specify the target public folder.

By default, the original folder is selected. If this folder does not exist or a non-original organization is selected, you must specify the target folder.

11. In **Path**, view or change the target subfolder in the target public folder. By default, the original path will be recreated.
12. Click **Start recovery**.
13. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
14. Click **Proceed** to confirm your decision.

Protecting OneDrive files

What items can be backed up?

You can back up an entire OneDrive, or individual files and folders.

Files are backed up together with their sharing permissions. Advanced permission levels (**Design**, **Full**, **Contribute**) are not backed up.

What items can be recovered?

You can recover an entire OneDrive or any file or folder that was backed up.

You can use search to locate the items.

You can choose whether to recover the sharing permissions or let the files inherit the permissions from the folder to which they are recovered.

Sharing links for files and folders are not recovered.

Selecting OneDrive files

Select the files as described below, and then specify other settings of the protection plan [as appropriate](#).

To select OneDrive files

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up the files of all users (including users that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.

- To back up the files of individual users, expand the **Users** node, select **All users**, select the users whose files you want to back up, and then click **Backup**.
4. On the protection plan panel:
- Ensure that the **OneDrive** item is selected in **What to back up**.
If some of the individually selected users do not have the OneDrive service included in their Microsoft 365 plan, you will not be able to select this option.
If some of the selected users for group backup do not have the OneDrive service included in their Microsoft 365 plan, you will be able to select this option, but the protection plan will not be applied to those users.
 - In **Items to back up**, do one of the following:
 - Keep the default setting **[All]** (all files).
 - Specify the files and folders to back up by adding their names or paths.
You can use wildcard characters (*, **, and ?). For more details about specifying paths and using wildcards, refer to ["File filters"](#).
 - Specify the files and folders to back up by browsing.
The **Browse** link is available only when creating a protection plan for a single user.
 - [Optional] In **Items to back up**, click **Show exclusions** to specify the files and folders to skip during the backup.
File exclusions override the file selection; i.e. if you specify the same file in both fields, this file will be skipped during a backup.

Recovering OneDrive and OneDrive files

Recovering an entire OneDrive

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose OneDrive you want to recover, and then click **Recovery**.
If the user was deleted, select the user in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.
You can search users by name. Wildcards are not supported.
4. Select a recovery point.

Note

To see only the recovery points that contain OneDrive files, select **OneDrive** in **Filter by content**.

5. Click **Recover > Entire OneDrive**.
6. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.

By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.

7. In **Recover to drive**, view, change, or specify the target user.

By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user.

8. Select whether to recover the sharing permissions for the files.
9. Click **Start recovery**.
10. Select one of the overwriting options:
 - **Overwrite existing files**
 - **Overwrite an existing file if it is older**
 - **Do not overwrite existing files**
11. Click **Proceed** to confirm your decision.

Recovering OneDrive files

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose OneDrive files you want to recover, and then click **Recovery**.

If the user was deleted, select the user in the **Cloud Applications Backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search users by name. Wildcards are not supported.

4. Select a recovery point.

Note

To see only the recovery points that contain OneDrive files, select **OneDrive** in **Filter by content**.

5. Click **Recover > Files/folders**.
6. Browse to the required folder or use search to obtain the list of the required files and folders. The search is not available if the backup is encrypted.
7. Select the files that you want to recover.

If the backup is not encrypted and you selected a single file, you can click **Show versions** to select the file version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download a file, select the file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.

By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.

11. In **Recover to drive**, view, change, or specify the target user.

By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user.

12. In **Path**, view or change the target folder in the target user's OneDrive. By default, the original location is selected.
13. Select whether to recover the sharing permissions for the files.
14. Click **Start recovery**.
15. Select one of the file overwriting options:
 - **Overwrite existing files**
 - **Overwrite an existing file if it is older**
 - **Do not overwrite existing files**
16. Click **Proceed** to confirm your decision.

Protecting SharePoint Online sites

What items can be backed up?

You can back up SharePoint classic site collections, group (modern team) sites, and communication sites. Also, you can select individual subsites, lists, and libraries for backup.

The following items are *skipped* during a backup:

- The **Look and Feel** site settings (except for **Title, description, and logo**).
- Site page comments and page comments settings (comments **On/Off**).
- The **Site features** site settings.
- Web part pages and web parts embedded in the wiki pages (due to SharePoint Online API limitations).
- Checked out files—files that are manually checked out for editing and all files that are created or uploaded in libraries, for which the option **Require Check Out** was enabled. To backup these files, first check them in.
- OneNote files (due to SharePoint Online API limitations).
- External data and Managed Metadata types of columns.
- The default site collection "domain-my.sharepoint.com". This is a collection where all of the organization users' OneDrive files reside.
- The contents of the recycle bin.

Limitations

- Titles and descriptions of sites/subsites/lists/columns are truncated during a backup if the title/description size is greater than 10000 bytes.

- You cannot back up previous versions of files created in SharePoint Online. Only the latest versions of the files are protected.
- You cannot back up the Preservation Hold library.
- You cannot back up sites created in the Business Productivity Online Suite (BPOS), the predecessor of Microsoft 365.
- You cannot back up the settings for sites that use the managed path /portals (for example, <https://<tenant>.sharepoint.com/portals/...>).
- Information Rights Management (IRM) settings of a list or a library can be recovered only if IRM is enabled in the target Microsoft 365 organization.

What items can be recovered?

The following items can be recovered from a site backup:

- Entire site
- Subsites
- Lists
- List items
- Document libraries
- Documents
- List item attachments
- Site pages and wiki pages

You can use search to locate the items.

Items can be recovered to the original or a non-original site. The path to a recovered item is the same as the original one. If the path does not exist, it is created.

You can choose whether to recover the sharing permissions or let the items inherit the permissions from the parent object after the recovery.

What items cannot be recovered?

- Subsites based on the **Visio Process Repository** template.
- Lists of the following types: **Survey list**, **Task list**, **Picture library**, **Links**, **Calendar**, **Discussion Board**, **External**, and **Import Spreadsheet**.
- Lists for which multiple content types are enabled.

Selecting SharePoint Online data

Select the data as described below, and then specify other settings of the protection plan [as appropriate](#).

To select SharePoint Online data

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up all classic SharePoint sites in the organization, including sites that will be created in the future, expand the **Site collections** node, select **All site collections**, and then click **Group backup**.
 - To back up individual classic sites, expand the **Site collections** node, select **All site collections**, select the sites that you want to back up, and then click **Backup**.
 - To back up all group (modern team) sites, including sites that will be created in the future, expand the **Groups** node, select **All groups**, and then click **Group backup**.
 - To back up individual group (modern team) sites, expand the **Groups** node, select **All groups**, select the groups whose sites you want to back up, and then click **Backup**.
4. On the protection plan panel:
 - Ensure that the **SharePoint sites** item is selected in **What to back up**.
 - In **Items to back up**, do one of the following:
 - Keep the default setting **[All]** (all items of the selected sites).
 - Specify the subsites, lists, and libraries to back up by adding their names or paths.

To back up a subsite or a top-level site list/library, specify its display name in the following format: /display name/**

To back up a subsite list/library, specify its display name in the following format: /subsite display name/list display name/**

The display names of subsites, lists, and libraries are shown on the **Site contents** page of a SharePoint site or subsite.
 - Specify the subsites to back up by browsing.

The **Browse** link is available only when creating a protection plan for a single site.
 - [Optional] In **Items to back up**, click **Show exclusions** to specify the subsites, lists, and libraries to skip during the backup.

Item exclusions override the item selection; i.e. if you specify the same subsite in both fields, this subsite will be skipped during a backup.

Recovering SharePoint Online data

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
 - To recover data from a group (modern team) site, expand the **Groups** node, select **All groups**, select the group whose site originally contained the items that you want to recover, and then click **Recovery**.

- To recover data from a classic site, expand the **Site Collections** node, select **All site collections**, select the site that originally contained the items that you want to recover, and then click **Recovery**.
- If the site was deleted, select it in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search groups and sites by name. Wildcards are not supported.

4. Select a recovery point.

Note

To see only the recovery points that contain SharePoint sites, select **SharePoint sites** in **Filter by content**.

5. Click **Recover SharePoint files**.
6. Browse to the required folder or use search to obtain the list of the required data items.
The search is not available if the backup is encrypted.
7. Select the items that you want to recover.
If the backup is not encrypted, you used search, and selected a single item in the search results, you can click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download an item, select the item, click **Download**, select the location to save the item to, and click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
11. In **Recover to site**, view, change, or specify the target site.
By default, the original site is selected. If this site does not exist or a non-original organization is selected, you must specify the target site.
12. Select whether to recover the sharing permissions of the recovered items.
13. Click **Start recovery**.
14. Select one of the overwriting options:
 - **Overwrite existing files**
 - **Overwrite an existing file if it is older**
 - **Do not overwrite existing files**
15. Click **Proceed** to confirm your decision.

Protecting Microsoft 365 Teams

What items can be backed up?

You can back up entire teams. This includes team name, team members list, team channels and their content, team mailbox and meetings, and team site.

What items can be recovered?

- Entire team
- Team channels
- Channel files
- Team mailbox
- Email folders in the team mailbox
- Email messages in the team mailbox
- Meetings
- Team site

You cannot recover conversations in team channels, but you can download them as a single html file.

Limitations

The following items are not backed up:

- The settings of the general channel (moderation preferences) – due to a [Microsoft Teams beta API](#) limitation.
- The settings of the custom channels (moderation preferences) – due to a [Microsoft Teams beta API](#) limitation.
- Meeting notes, chats.
- Stickers and praises.

Backup and recovery are supported for the following channel tabs:

- Word
- Excel
- PowerPoint
- PDF
- Document Library

Files that are shared in private channels are backed up, but not restored due to an API limitation.

Note

These files are stored in specific locations, separately from the files that are shared in public channels.

Selecting teams

Select teams as described below, and then specify other settings of the protection plan [as appropriate](#).

To select teams

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose teams you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up all the teams in the organization (including teams that will be created in the future), expand the **Teams** node, select **All teams**, and then click **Group backup**.
 - To back up individual teams, expand the **Teams** node, select **All teams**, select the teams that you want to back up, and then click **Backup**.

You can search teams by name. Wildcards are not supported.

4. On the protection plan panel:
 - Ensure that the **Microsoft Teams** item is selected in **What to back up**.
 - [Optional] In **How long to keep**, set the cleanup options.
 - [Optional] If you want to encrypt your backup, enable the **Encryption** switch, and then set your password and select the encryption algorithm.

Recovering an entire team

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up teams you want to recover. Otherwise, skip this step.
3. Expand the **Teams** node, select **All teams**, select the team that you want to recover, and then click **Recovery**.

You can search teams by name. Wildcards are not supported.

4. Select a recovery point.
5. Click **Recover > Entire Team**.

If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.

By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.

6. In **Recover to team**, view, change, or specify the target team.

By default, the original team is selected. If this team does not exist or a non-original organization is selected, you must specify the target team.

7. Click **Start recovery**.
8. Select one of the overwriting options:

- **Overwrite existing content if it is older**
- **Overwrite existing content**
- **Do not overwrite existing content**

9. Click **Proceed** to confirm your decision.

When you delete a channel in Microsoft Teams' graphic interface, it is not immediately removed from the system. Thus, when you recover the whole team, this channel's name cannot be used and a postfix will be added to it.

Conversations are recovered as a single html file in the **Files** tab of the channel. You can find this file in a folder named according to the following pattern: <Team name>_<Channel name>_conversations_backup_<date of recovery>T<time of recovery>Z.

Note

After recovering a team or team channels, go to Microsoft Teams, select the channels that were recovered, and then click their **Files** tab. Otherwise, the subsequent backups of these channels will not include this tab's content – due to a [Microsoft Teams beta API](#) limitation.

Recovering team channels or files in team channels

To recover team channels

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up teams you want to recover. Otherwise, skip this step.
3. Expand the **Teams** node, select **All teams**, select the team whose channels you want to recover, and then click **Recovery**.
4. Select a recovery point.
5. Click **Recover > Channels**.
6. Select the channels that you want to recover, and then click **Recover**. To select a channel in the main pane, select the check box in front of its name.
The following search options are available:
 - For **Conversations**: sender, subject, content, language, attachment name, date or date range.
 - For **Files**: file name or folder name, file type, size, date or date range of the last change.
7. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
8. In **Recover to team**, view, change, or specify the target team.
By default, the original team is selected. If this team does not exist or a non-original organization is selected, you must specify the target team.
9. In **Recover to channel**, view, change, or specify the target channel.
10. Click **Start recovery**.
11. Select one of the overwriting options:

- **Overwrite existing content if it is older**
- **Overwrite existing content**
- **Do not overwrite existing content**

12. Click **Proceed** to confirm your decision.


Conversations are recovered as a single html file in the **Files** tab of the channel. You can find this file in a folder named according to the following pattern: <Team name>_<Channel name>_conversations_backup_<date of recovery>T<time of recovery>Z.

Note

After recovering a team or team channels, go to Microsoft Teams, select the channels that were recovered, and then click their **Files** tab. Otherwise, the subsequent backups of these channels will not include this tab's content – due to a [Microsoft Teams beta API](#) limitation.

To recover files in a team channel

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up teams you want to recover. Otherwise, skip this step.
3. Expand the **Teams** node, select **All teams**, select the team whose channels you want to recover, and then click **Recovery**.
4. Select a recovery point.
5. Click **Recover > Channels**.
6. Select the desired channel, and then open the **Files** folder.
Browse to the required items or use search to obtain the list of the required items. The following search options are available: file name or folder name, file type, size, date or date range of the last change.
7. Select the items that you want to recover, and then click **Recover**
8. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click Microsoft 365 organization to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
9. In **Recover to team**, view, change, or specify the target team.
By default, the original team is selected. If this team does not exist or a non-original organization is selected, you must specify the target team.
10. In **Recover to channel**, view, change, or specify the target channel.
11. Select whether to recover the sharing permissions of the recovered items.
12. Click **Start recovery**.
13. Select one of the overwriting options:
 - **Overwrite existing content if it is older**
 - **Overwrite existing content**
 - **Do not overwrite existing content**
14. Click **Proceed** to confirm your decision.

You cannot recover individual conversations. In the main pane, you can only browse the **Conversation** folder or download its content as a single html file. To do so, click the "recover folders" icon , select the desired **Conversations** folder, and then click **Download**.


You can search the messages in the **Conversation** folder by:

- Sender
- Content
- Attachment name
- Date

Recovering a team mailbox

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up teams you want to recover. Otherwise, skip this step.
3. Expand the **Teams** node, select **All teams**, select the team whose mailbox you want to recover, and then click **Recovery**.

You can search teams by name. Wildcards are not supported.

4. Select a recovery point.
5. Click **Recover > Email messages**.
6. Click the "recover folders" icon , select the root mailbox folder, and then click **Recover**.

Note

You can also recover individual folders from the selected mailbox.

7. Click **Recover**.
8. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
9. In **Recover to 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 organization is selected, you must specify the target mailbox.
10. Click **Start recovery**.
11. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
12. Click **Proceed** to confirm your decision.

Recovering email messages and meetings

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up teams you want to recover. Otherwise, skip this step.
3. Expand the **Teams** node, select **All teams**, select the team whose email messages or meetings you want to recover, and then click **Recovery**.
You can search teams by name. Wildcards are not supported.
4. Select a recovery point.
5. Click **Recover > Email messages**.
6. Browse to the required item or use search to obtain the list of the required items.
The following search options are available:
 - For email messages: search by subject, sender, recipient, and date.
 - For meetings: search by event name and date.
7. Select the items that you want to recover, and then click **Recover**.

Note

You can find the meetings in the **Calendar** folder.

Additionally, you can do any of the following:

- When an item is selected, click **Show content** to view its contents, including attachments. Click the name of an attached file to download it.
 - When an email message or a meeting is selected, click **Send as email** to send the item to the specified email addresses. You can select the sender and write a text to be added to the forwarded item.
8. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
 9. In **Recover to 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 organization is selected, you must specify the target mailbox.
 10. Click **Start recovery**.
 11. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
 12. Click **Proceed** to confirm your decision.

Recovering a team site or specific items of a site

1. Click **Microsoft 365**.
2. If multiple Microsoft 365 organizations were added to the Cyber Protection service, select the organization whose backed-up teams you want to recover. Otherwise, skip this step.
3. Expand the **Teams** node, select **All teams**, select the team whose site you want to recover, and then click **Recovery**.
You can search teams by name. Wildcards are not supported.
4. Select a recovery point.
5. Click **Recover > Team site**.
6. Browse to the required item or use search to obtain the list of the required items.
The search is not available if the backup is encrypted.
7. Select the items that you want to recover, and then click **Recover**.
8. If multiple Microsoft 365 organizations were added to the Cyber Protection service, click **Microsoft 365 organization** to view, change, or specify the target organization.
By default, the original organization and team are selected. If this organization is no longer registered in the Cyber Protection service, you must specify the target organization.
9. In **Recover to team**, view, change, or specify the target team.
By default, the original team is selected. If this team does not exist or a non-original organization is selected, you must specify the target site.
10. Select whether to recover the sharing permissions of the recovered items.
11. Click **Start recovery**.
12. Select one of the overwriting options:
 - **Overwrite existing content if it is older**
 - **Overwrite existing content**
 - **Do not overwrite existing content**
13. Click **Proceed** to confirm your decision.

Upgrading the cloud agent

This section describes how to upgrade to the current version of the backup solution for Microsoft 365. This version supports OneDrive and SharePoint Online backup, and provides improved backup and recovery performance. Starting from version 8.0 of the Cyber Protection service, the following functionality is no longer supported by the old solution: editing, deleting, applying, and revoking a protection plan.

The upgrade availability depends on the data center readiness and the settings made by your service provider. If the upgrade is available, the service console shows a notification at the top of the **Microsoft Office 365 (v1)** tab.

The upgrade process

During the upgrade, your Microsoft 365 organization users are added to the new backup solution. The protection plans are migrated and applied to the appropriate users.

The earlier created backups are copied from one location in the cloud to another. On the **Backup storage** tab, the copied backups are shown in a separate section named **Cloud applications backups**, while the original backups remain in the **Cloud storage** location. When the upgrade process is complete, the original backups are deleted from the **Cloud storage** location.

The upgrade may take several hours, or even days, depending on the number of users in the organization, the number of backups, and the Microsoft 365 access speed. During the upgrade, recovery from the earlier created backups is possible. However, backups and protection plans created during the upgrade will be lost.

In the unlikely case of an upgrade failure, the backup solution remains fully operational and the upgrade can be restarted from the point of failure.

To start the upgrade process

1. Click **Microsoft Office 365 (v1)**.
2. Click **Upgrade** in the notification at the top of the screen.
3. Confirm that you want to start the upgrade process.
4. Select the Microsoft data center used by your organization.
The software redirects you to the Microsoft 365 login page.
5. Sign in with the Microsoft 365 global administrator credentials.
Microsoft 365 displays a list of permissions that are necessary to back up and recover your organization's data.
6. Confirm that you grant the Cyber Protection service these permissions.
You are redirected to the service console and the upgrade process begins. The upgrade progress is shown on the **Microsoft 365 > Activities** panel.

14.20 Protecting Google Workspace data

14.20.1 What does Google Workspace protection mean?

- Cloud-to-cloud backup and recovery of Google Workspace user data (Gmail mailboxes, Calendars, Contacts, Google Drives) and Google Workspace Shared drives.
- Granular recovery of emails, files, contacts, and other items.
- Support for several Google Workspace organizations and cross-organization recovery.
- Optional notarization of the backed-up files by means of the Ethereum blockchain database.
When enabled, you can prove that a file is authentic and unchanged since it was backed up.
- Optional full-text search. When enabled, you can search emails by their content.

- Up to 5000 items (mailboxes, Google Drives, and Shared drives) per company can be protected without performance degradation.

14.20.2 Required user rights

In the Cyber Protection service

In the Cyber Protection service, you need to be a company administrator acting on a customer tenant level. Company administrators acting on a unit level, unit administrators, and users cannot back up or recover Google Workspace data.

In Google Workspace

To add your Google Workspace organization to the Cyber Protection service, you must be signed in as a Super Admin with enabled API access (**Security > API reference > Enable API access** in the Google Admin console).

The Super Admin password is not stored anywhere and is not used to perform backup and recovery. Changing this password in Google Workspace does not affect Cyber Protection service operation.

If the Super Admin who added the Google Workspace organization is deleted from Google Workspace or assigned a role with less privileges, the backups will fail with an error like "access denied". In this case, repeat the ["Adding a Google Workspace organization"](#) procedure and specify valid Super Admin credentials. To avoid this situation, we recommend creating a dedicated Super Admin user for backup and recovery purposes.

14.20.3 About the backup schedule

Because the cloud agent serves multiple customers, it determines the start time for each protection plan on its own, to ensure an even load during a day and an equal quality of service for all of the customers.

Each protection plan runs daily at the same time of day.

14.20.4 Limitations

- Only users with an assigned Google Workspace license can have their mailboxes and Google Drives backed up.
- Search in encrypted backups is not supported.
- Documents in the native Google formats are backed up as generic office documents and are shown with a different extension in the service console – such as .docx or .pptx, for example. The documents are converted back to their original format during recovery.
- No more than [10 manual backup runs during an hour](#).
- No more than 10 simultaneous recovery operations (this number includes both Microsoft 365 and Google Workspace recovery).

- You cannot simultaneously recover items from different recovering points, even though you can select such items from the search results.

14.20.5 Adding a Google Workspace organization

You can add a Google Workspace organization to the Cyber Protection service in the following ways:

- By using a dedicated personal Google Cloud project.
- By using the Cyber Protect app in Google marketplace.

Adding a Google Workspace organization via a dedicated personal Google Cloud project might result in faster backups. For more information about how to create and configure such a project, refer to "Creating a personal Google Cloud project" (p. 316).

To add a Google Workspace organization by using a dedicated personal Google Cloud project

1. Sign in to the service console as a company administrator.
2. Click **Devices > Add > Google Workspace**.
3. Enter the email address of a Super Administrator of your Google Workspace account.
4. Browse for the JSON file that contains the private key of the service account that you created in your Google Cloud project. You can also paste the file content as text.
5. Click **Confirm**.

As a result, your Google Workspace organization appears under the **Devices** tab in the service console.

To add a Google Workspace organization by using the Cyber Protect app in Google marketplace

1. Sign in to the service console as a company administrator.
2. Click **Devices > Add > Google Workspace**.
3. Click **Add a Google Workspace organization with the Acronis Google marketplace app**.
4. Follow the instructions displayed by the software:
 - a. Click **Open marketplace**.
 - b. Sign in with the Super Administrator credentials.
 - c. Click **Domain install**.
 - d. Confirm the domain-wide installation.
Google Workspace displays a list of permissions that are necessary to back up and recover your organization's data.
 - e. Confirm that you grant the Cyber Protection service these permissions.
 - f. Complete the installation wizard.
 - g. Go to the Apps launcher icon, find the Cyber Protection Service application in the list, and then click on it.

You are redirected back to the service console. As a result, your Google Workspace organization appears under the **Devices** tab in the service console.

Useful tips

- After adding a Google Workspace organization, the user data and Shared drives in both the primary domain and all the secondary domains, if there are any, will be backed up. The backed-up resources will be displayed in one list, and will not be grouped by their domain.
- The cloud agent synchronizes with Google Workspace every 24 hours, starting from the moment when the organization is added to the Cyber Protection service. If you add or remove a user or Shared drive, you will not see this change in the service console immediately. To synchronize the change immediately, select the organization on the **Google Workspace** page, and then click **Refresh**.
- If you applied a protection plan to the **All users** or **All Shared drives** group, the newly added items will be included in the backup only after the synchronization.
- According to Google policy, when a user or Shared drive is removed from the Google Workspace graphical user interface, it remains available via an API for a few days. During this period, the removed item is inactive (grayed out) in the service console and is not backed up. When the removed item becomes unavailable via the API, it disappears from the service console. Its backups (if any) can be found at **Backup storage > Cloud applications backups**.

14.20.6 Creating a personal Google Cloud project

To add your Google Workspace organization to the Cyber Protection service by using a dedicated Google Cloud project, you need to do the following:

1. Create a new Google Cloud project.
2. Enable the required APIs for this project.
3. Configure the credentials for this project:
 - a. Configure the OAuth consent screen.
 - b. Create and configure the service account for the Cyber Protection service.
4. Grant the new project access to your Google Workspace account.

Note

This topic contains a description of third-party user interface that might be subject to change without prior notice.

To create a new Google Cloud project

1. Sign in to the Google Cloud Platform (console.cloud.google.com) as a Super Administrator.
2. In the Google Cloud Platform console, click **Select a project > New project**.
3. Specify a name for your new project.
4. Click **Create**.

As a result, your new Google Cloud project is created.

To enable the required APIs for this project

1. In the Google Cloud Platform console, select your new project.
2. From the navigation menu, select **APIs & Services > Dashboard**.
3. Disable all the APIs that are enabled by default in this project, one by one:
 - a. Scroll down the **Dashboard** page, and then click the name of an enabled API.
The **Overview** page of the selected API opens.
 - b. Click **Disable API**, and then confirm your choice by clicking **Disable**.
 - c. Go back to **APIs & Services > Dashboard**, and disable the next API.
4. From the navigation menu, select **APIs & Services > Library**.
5. In the API library, enable the following APIs, one by one:
 - Gmail API
 - Google Drive API
 - Admin SDK
 - Google Calendar API
 - People APIUse the search bar to find the required APIs. To enable an API, click its name, and then click **Enable**. To search for the next API, go back to the API library, by selecting **APIs & Services > Library** from the navigation menu.

To configure the OAuth consent screen

1. From the navigation menu in the Google Cloud Platform, select **APIs & Services > OAuth consent screen**.
2. In the window that opens, select **Internal** for user type, and then click **Create**.
3. In the **App name** field, specify a name for your application.
4. In the **User support email** field, enter the Super Administrator email.
5. In the **Developer contact information** field, enter the Super Administrator email.
6. Leave all other fields blank, and then click **Save and continue**.
7. On the **Scopes** page, click **Save and continue**, without changing anything.
8. On the **Summary** page, verify your settings, and then click **Back to dashboard**.

To create and configure the service account for the Cyber Protection service

1. From the navigation menu in the Google Cloud Platform, select **IAM & Admin > Service accounts**.
2. Click **Create service account**.
3. Specify a name for the service account.
4. Specify a description for the service account.
5. Click **Create**.
6. Do not change anything in the **Grant this service account access to the project** and **Grant users access to this service account** steps.
7. Click **Done**.
The **Service accounts** page opens.

8. On the **Service accounts** page, select the new service account, and then under **Actions**, click **Edit**.
9. Expand the **Show domain-wide delegation** section, and then select the **Enable Google Workspace domain-wide delegation** check box.
10. Under **Keys**, click **Add key > Create new key**, and then select the **JSON** key type.
11. Click **Create**.

As a result, a JSON file with the private key of the service account is automatically downloaded to your machine. Store this file securely because you need it to add your Google Workspace organization to the Cyber Protection service.

To grant the new project access to your Google Workspace account

1. From the navigation menu in the Google Cloud Platform, select **APIs and Services > Credentials**.
2. In the **OAuth 2.0 Client IDs** section, under **Client ID**, copy the client ID of your service account client.
3. Sign in to the Google Admin console (admin.google.com) as a Super Administrator.
4. From the navigation menu, select **Security > API controls**.
5. Scroll down the **API controls** page, and then under **Domain-wide delegation**, click **Manage domain-wide delegation**.

The **Domain-wide delegation** page opens.

6. On the **Domain-wide delegation** page, click **Add new**.
The **Add a new client ID** window opens.
7. In the **Client ID** field, enter the client ID of your service account client.
8. In the **OAuth scopes** field, add the following scopes, one by one:

- <https://mail.google.com>
- <https://www.googleapis.com/auth/contacts>
- <https://www.googleapis.com/auth/calendar>
- <https://www.googleapis.com/auth/admin.directory.user.readonly>
- <https://www.googleapis.com/auth/admin.directory.domain.readonly>
- <https://www.googleapis.com/auth/drive>
- <https://www.googleapis.com/auth/gmail.modify>

9. Click **Authorise**.

As a result, your new Google Cloud project can access the data in your Google Workspace account. To back up the data, you need to link this project to the Cyber Protection service. For more information on how to do this, refer to "To add a Google Workspace organization by using a dedicated personal Google Cloud project" (p. 315)

If you need to revoke the access of your Google Cloud project to your Google Workspace account, and respectively the access of the Cyber Protection service, delete the API client that your project uses.

To revoke access to your Google Workspace account

1. In the Google Admin console (admin.google.com), sign in as a Super Administrator.
2. From the navigation menu, select **Security > API controls**.
3. Scroll down the **API controls** page, and then under **Domain-wide delegation**, click **Manage domain-wide delegation**.
The **Domain-wide delegation** page opens.
4. On the **Domain-wide delegation** page, select the API client that your project uses, and then click **Delete**.
As a result, your Google Cloud project and the Cyber Protection service will not be able to access your Google Workspace account and back up the data in it.

14.20.7 Protecting Gmail data

What items can be backed up?

You can back up Gmail users' mailboxes. A mailbox backup also includes the Calendar and Contacts data. Optionally, you can choose to back up the shared calendars.

The following items are *skipped* during a backup:

- The **Birthdays, Reminders, Tasks** calendars
- Folders attached to calendar events
- The **Directory** folder in Contacts

The following Calendar items are *skipped*, due to Google Calendar API limitations:

- Appointment slots
- The conferencing field of an event
- The calendar setting **All-day event notifications**
- The calendar setting **Auto-accept invitations** (in calendars for rooms or shared spaces)

The following Contacts items are *skipped*, due to Google People API limitations:

- The **Other contacts** folder
- The external profiles of a contact (**Directory profile, Google profile**)
- The contact field **File as**

What items can be recovered?

The following items can be recovered from a mailbox backup:

- Mailboxes
- Email folders (According to Google terminology, "labels". **Labels** are presented in the backup software as folders, for consistency with other data presentation.)
- Email messages
- Calendar events
- Contacts

You can use search to locate items in a backup, unless the backup is encrypted. Search in encrypted backups is not supported.

When recovering mailboxes and mailbox items, you can select whether to overwrite the items in the target location.

Limitations

- Contact photos cannot be recovered
- The **Out of office** calendar item is recovered as a regular calendar event, due to Google Calendar API limitations

Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the protection plan [as appropriate](#).

To select Gmail mailboxes

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up the mailboxes of all users (including mailboxes that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
 - To back up individual user mailboxes, expand the **Users** node, select **All users**, select the users whose mailboxes you want to back up, and then click **Backup**.
4. On the protection plan panel:
 - Ensure that the **Gmail** item is selected in **What to back up**.
 - If you want to back up calendars that are shared with the selected users, enable the **Include shared calendars** switch.
 - Decide whether you need [full-text search](#) through the backed-up email messages. To access this option, click the gear icon > **Backup options** > **Full-text search**.

Full-text search

This option defines whether the email messages content is indexed by the cloud agent.

The preset is: **Enabled**.

If this option is enabled, the messages content is indexed and you can search messages by their content. Otherwise, only searching by subject, sender, recipient, or date is available.

Note

Search in encrypted backups is not supported.

The indexing process does not affect the backup performance because it is performed by a different software component. Indexing of the first (full) backup may take some time, therefore, there may be a delay between the backup completion and the content appearing in the search results.

The index occupies 10-30 percent of storage space occupied by the mailbox backups. To learn the exact value, click **Backup storage > Cloud applications backups** and view the **Index size** column. You may want to disable full-text search in order to save this space. The value in the **Index size** column will decrease to a few megabytes after the next backup. This minimal amount of metadata is necessary to perform a search by subject, sender, recipient, or date.

When you re-enable full-text search, the software indexes all of the backups previously created by the protection plan. This also takes some time.

Recovering mailboxes and mailbox items

Recovering mailboxes

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose mailbox you want to recover, and then click **Recovery**.

If the user was deleted, select the user in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search users and groups by name. Wildcards are not supported.

4. Select a recovery point.

Note

To see only the recovery points that contain mailboxes, select **Gmail** in **Filter by content**.

5. Click **Recover > Entire mailbox**.
6. If multiple Google Workspace organizations are added to the Cyber Protection service, click **Google Workspace organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must select a new target organization from the available registered organizations.
7. In **Recover to 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 organization is selected, you must specify the target mailbox.
You cannot create a new target mailbox during recovery. To recover a mailbox to a new one, first you need to create the target mailbox in the desired Google Workspace organization, and then let the cloud agent synchronize the change. The cloud agent automatically synchronizes with Google Workspace every 24 hours. To synchronize the change immediately, in the service console, select the organization on the **Google Workspace** page, and then click **Refresh**.


8. Click **Start recovery**.
9. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
10. Click **Proceed** to confirm your decision.

Recovering mailbox items

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose mailbox originally contained the items that you want to recover, and then click **Recovery**.
If the user was deleted, select the user in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.
You can search users and groups by name. Wildcards are not supported.
4. Select a recovery point.

Note

To see only the recovery points that contain mailboxes, select **Gmail** in **Filter by content**.

5. Click **Recover > Email messages**.
6. Browse to the required folder. If the backup is not encrypted, you can use search to obtain the list of the required items.
The following search options are available. Wildcards are not supported.
 - For email messages: search by subject, sender, recipient, date, attachment name, and message content. The last two options yield results only if the **Full-text search** option was enabled during backup. The language of the message fragment being searched can be specified as an additional parameter.
 - For events: search by title and date.
 - For contacts: search by name, email address, and phone number.
7. Select the items that you want to recover. To be able to select folders, click the "recover folders" icon: 
Additionally, you can do any of the following:
 - When an item is selected, click **Show content** to view its contents, including attachments. Click the name of an attached file to download it.
 - Only if the backup is not encrypted, you used search, and selected a single item in the search results: click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. Click **Recover**.

9. If multiple Google Workspace organizations were added to the Cyber Protection service, click **Google Workspace organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must select a new target organization from the available registered organizations.
10. In **Recover to 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 organization is selected, you must specify the target mailbox.
11. In **Path**, view or change the target folder in the target mailbox. By default, the original folder is selected.
12. Click **Start recovery**.
13. Select one of the overwriting options:
 - **Overwrite existing items**
 - **Do not overwrite existing items**
14. Click **Proceed** to confirm your decision.

14.20.8 Protecting Google Drive files

What items can be backed up?

You can back up an entire Google Drive, or individual files and folders. Optionally, you can choose to back up files that are shared with the Google Drive user.

Files are backed up together with their sharing permissions.

The following items are *skipped* during a backup:

- A shared file, if the user has a commenter or viewer access to the file and the file owner disabled the options to download, print, and copy for commenters and viewers.
- The **Computers** folder (created by the Backup and Sync client)

Limitations

- Out of Google-specific file formats, only Google docs, Google sheets, Google slides, and Google Drawings are backed up.

What items can be recovered?

You can recover an entire Google Drive, or any file or folder that was backed up.

You can use search to locate items in a backup, unless the backup is encrypted. Search in encrypted backups is not supported.

You can choose whether to recover the sharing permissions or let the files inherit the permissions from the folder to which they are recovered.

Limitations

- Comments in files are not recovered.
- Sharing links for files and folders are not recovered.
- The read-only **Owner settings** for shared files (**Prevent editors from changing access and adding new people** and **Disable options to download, print and copy for commenters and viewers**) cannot be changed during a recovery.
- Ownership of a shared folder cannot be changed during a recovery if the **Prevent editors from changing access and adding new people** option is enabled for this folder. This setting prevents the Google Drive API from listing the folder permissions. Ownership of the files in the folder is recovered correctly.

Selecting Google Drive files

Select the files as described below, and then specify other settings of the protection plan [as appropriate](#).

To select Google Drive files

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up the files of all users (including users that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
 - To back up the files of individual users, expand the **Users** node, select **All users**, select the users whose files you want to back up, and then click **Backup**.
4. On the protection plan panel:
 - Ensure that the **Google Drive** item is selected in **What to back up**.
 - In **Items to back up**, do one of the following:
 - Keep the default setting **[All]** (all files).
 - Specify the files and folders to back up by adding their names or paths.
You can use wildcard characters (*, **, and ?). For more details about specifying paths and using wildcards, refer to ["File filters"](#).
 - Specify the files and folders to back up by browsing.
The **Browse** link is available only when creating a protection plan for a single user.
 - [Optional] In **Items to back up**, click **Show exclusions** to specify the files and folders to skip during the backup.
File exclusions override the file selection; i.e. if you specify the same file in both fields, this file will be skipped during a backup.
 - If you want to back up the files that are shared with the selected users, enable the **Include shared files** switch.

- If you want to enable notarization of all files selected for backup, enable the **Notarization** switch. For more information about notarization, refer to "[Notarization](#)".

Recovering Google Drive and Google Drive files

Recovering an entire Google Drive

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose Google Drive you want to recover, and then click **Recovery**.

If the user was deleted, select the user in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search users by name. Wildcards are not supported.

4. Select a recovery point.

Note

To see only the recovery points that contain Google Drive files, select **Google Drive** in **Filter by content**.

5. Click **Recover > Entire Drive**.
6. If multiple Google Workspace organizations were added to the Cyber Protection service, click **Google Workspace organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must select a new target organization from the available registered organizations.
7. In **Recover to drive**, view, change, or specify the target user or the target Shared drive.
By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user or the target Shared drive.
If the backup contains shared files, the files will be recovered to the root folder of the target drive.
8. Select whether to recover the sharing permissions for the files.
9. Click **Start recovery**.
10. Select one of the overwriting options:
 - **Overwrite existing files**
 - **Overwrite an existing file if it is older**
 - **Do not overwrite existing files**
11. Click **Proceed** to confirm your decision.

Recovering Google Drive files

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose Google Drive files you want to recover, and then click **Recovery**.

If the user was deleted, select the user in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search users by name. Wildcards are not supported.

4. Select a recovery point.

Note

To see only the recovery points that contain Google Drive files, select **Google Drive** in **Filter by content**.

5. Click **Recover > Files/folders**.
6. Browse to the required folder or use search to obtain the list of the required files and folders.
The search is not available if the backup is encrypted.
7. Select the files that you want to recover.
If the backup is not encrypted and you selected a single file, you can click **Show versions** to select the file version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download a file, select the file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple Google Workspace organizations were added to the Cyber Protection service, click **Google Workspace organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must select a new target organization from the available registered organizations.
11. In **Recover to drive**, view, change, or specify the target user or the target Shared drive.
By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user or the target Shared drive.
12. In **Path**, view or change the target folder in the target user's Google Drive or in the target Shared drive. By default, the original location is selected.
13. Select whether to recover the sharing permissions for the files.
14. Click **Start recovery**.
15. Select one of the file overwriting options:
 - **Overwrite existing files**
 - **Overwrite an existing file if it is older**

- **Do not overwrite existing files**

16. Click **Proceed** to confirm your decision.

14.20.9 Protecting Shared drive files

What items can be backed up?

You can back up an entire Shared drive, or individual files and folders.

Files are backed up together with their sharing permissions.

Limitations

- A Shared drive without members cannot be backed up, due to Google Drive API limitations.
- Out of Google-specific file formats only Google docs, Google sheets, Google slides, and Google Drawings are backed up.

What items can be recovered?

You can recover an entire Shared drive, or any file or folder that was backed up.

You can use search to locate items in a backup, unless the backup is encrypted. Search in encrypted backups is not supported.

You can choose whether to recover the sharing permissions or let the files inherit the permissions from the folder to which they are recovered.

The following items are not recovered:

- Sharing permissions for a file that was shared with a user outside the organization are not recovered if sharing outside the organization is disabled in the target Shared drive.
- Sharing permissions for a file that was shared with a user who is not a member of the target Shared drive are not recovered if **Sharing with non-members** is disabled in the target Shared drive.

Limitations

- Comments in files are not recovered.
- Sharing links for files and folders are not recovered.

Selecting Shared drive files

Select the files as described below, and then specify other settings of the protection plan [as appropriate](#).

To select Shared drive files

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
 - To back up the files of all Shared drive (including Shared drive that will be created in the future), expand the **Shared drives** node, select **All Shared drives**, and then click **Group backup**.
 - To back up the files of individual Shared drives, expand the **Shared drives** node, select **All Shared drives**, select the Shared drives to back up, and then click **Backup**.
4. On the protection plan panel:
 - In **Items to back up**, do one of the following:
 - Keep the default setting **[All]** (all files).
 - Specify the files and folders to back up by adding their names or paths.
You can use wildcard characters (*, **, and ?). For more details about specifying paths and using wildcards, refer to ["File filters"](#).
 - Specify the files and folders to back up by browsing.
The **Browse** link is available only when creating a protection plan for a single Shared drive.
 - [Optional] In **Items to back up**, click **Show exclusions** to specify the files and folders to skip during the backup.
File exclusions override the file selection; i.e. if you specify the same file in both fields, this file will be skipped during a backup.
 - If you want to enable notarization of all files selected for backup, enable the **Notarization** switch. For more information about notarization, refer to ["Notarization"](#).

Recovering Shared drive and Shared drive files

Recovering an entire Shared drive

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Shared drives** node, select **All Shared drives**, select the Shared drive that you want to recover, and then click **Recovery**.
If the Shared drive was deleted, select it in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.
You can search Shared drives by name. Wildcards are not supported.
4. Select a recovery point.
5. Click **Recover > Entire Shared drive**.
6. If multiple Google Workspace organizations were added to the Cyber Protection service, click **Google Workspace organization** to view, change, or specify the target organization.

By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must select a new target organization from the available registered organizations.

7. In **Recover to drive**, view, change, or specify the target Shared drive or the target user. If you specify a user, the data will be recovered to this user's Google Drive.

By default, the original Shared drive is selected. If this Shared drive does not exist or a non-original organization is selected, you must specify the target Shared drive or the target user.

8. Select whether to recover the sharing permissions for the files.
9. Click **Start recovery**.
10. Select one of the overwriting options:
 - **Overwrite existing files**
 - **Overwrite an existing file if it is older**
 - **Do not overwrite existing files**
11. Click **Proceed** to confirm your decision.

Recovering Shared drive files

1. Click **Google Workspace**.
2. If multiple Google Workspace organizations were added to the Cyber Protection service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Shared drives** node, select **All Shared drives**, select the Shared drive that originally contained the files you want to recover, and then click **Recovery**.

If the Shared drive was deleted, select it in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.

You can search Shared drives by name. Wildcards are not supported.

4. Select a recovery point.
5. Click **Recover > Files/folders**.
6. Browse to the required folder or use search to obtain the list of the required files and folders.
The search is not available if the backup is encrypted.
7. Select the files that you want to recover.
If the backup is not encrypted and you selected a single file, you can click **Show versions** to select the file version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download a file, select the file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple Google Workspace organizations were added to the Cyber Protection service, click **Google Workspace organization** to view, change, or specify the target organization.
By default, the original organization is selected. If this organization is no longer registered in the Cyber Protection service, you must select a new target organization from the available registered organizations.

11. In **Recover to drive**, view, change, or specify the target Shared drive or the target user. If you specify a user, the data will be recovered to this user's Google Drive.
By default, the original Shared drive is selected. If this Shared drive does not exist or a non-original organization is selected, you must specify the target Shared drive or the target user.
12. In **Path**, view or change the target folder in the target Shared drive or the target user's Google Drive. By default, the original location is selected.
13. Select whether to recover the sharing permissions for the files.
14. Click **Start recovery**.
15. Select one of the file overwriting options:
 - **Overwrite existing files**
 - **Overwrite an existing file if it is older**
 - **Do not overwrite existing files**
16. Click **Proceed** to confirm your decision.

14.20.10 Notarization

Notarization enables you to prove that a file is authentic and unchanged since it was backed up. We recommend that you enable notarization when backing up your legal document files or other files that require proved authenticity.

Notarization is available only for backups of Google Drive files and Google Workspace Shared drive files.

How to use notarization

To enable notarization of all files selected for backup, enable the **Notarization** switch when creating a protection plan.

When configuring recovery, the notarized files will be marked with a special icon, and you can [verify the file authenticity](#).

How it works

During a backup, the agent calculates the hash codes of the backed-up files, builds a hash tree (based on the folder structure), saves the tree in the backup, and then sends the hash tree root to the notary service. The notary service saves the hash tree root in the Ethereum blockchain database to ensure that this value does not change.


When verifying the file authenticity, the agent calculates the hash of the file, and then compares it with the hash that is stored in the hash tree inside the backup. If these hashes do not match, the file is considered not authentic. Otherwise, the file authenticity is guaranteed by the hash tree.

To verify that the hash tree itself was not compromised, the agent sends the hash tree root to the notary service. The notary service compares it with the one stored in the blockchain database. If the hashes match, the selected file is guaranteed to be authentic. Otherwise, the software displays a message that the file is not authentic.

Verifying file authenticity with Notary Service

If notarization was enabled during backup, you can verify the authenticity of a backed-up file.

To verify the file authenticity

1. Do one of the following:
 - To verify the authenticity of a Google Drive file, select the file as described in steps 1-7 of the ["Recovering Google Drive files"](#) section.
 - To verify the authenticity of a Google Workspace Shared drive file, select the file as described in steps 1-7 of the ["Recovering Shared drive files"](#) section.
2. Ensure that the selected file is marked with the following icon: . This means that the file is notarized.
3. Do one of the following:
 - Click **Verify**.
The software checks the file authenticity and displays the result.
 - Click **Get certificate**.
A certificate that confirms the file notarization is opened in a web browser window. The window also contains instructions that allow you to verify the file authenticity manually.

14.21 Protecting Oracle Database

Protection of Oracle Database is described in a separate document available at https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper.pdf

Note

The availability of this feature depends on the service quotas that are enabled for your account.

14.22 Protecting SAP HANA

Protection of SAP HANA is described in a separate document available at https://dl.managed-protection.com/u/pdf/SAP%20HANA_backup_whitepaper.pdf

Note

The availability of this feature depends on the service quotas that are enabled for your account.

14.23 Protecting websites and hosting servers

14.23.1 Protecting websites

A website can be corrupted as a result of unauthorized access or a malware attack. Back up your website if you want to easily revert it to a healthy state, in case of corruption.

What do I need to back up a website?

The website must be accessible via the SFTP or SSH protocol. You do not need to install an agent, just add a website as described later in this section.

What items can be backed up?

You can back up the following items:

- **Website content files**

All files accessible to the account you specify for the SFTP or SSH connection.

- **Linked databases (if any) hosted on MySQL servers.**

All databases accessible to the MySQL account you specify.

If your website employs databases, we recommend that you back up both the files and the databases, to be able to recover them to a consistent state.

Limitations

- The only backup location available for website backup is the cloud storage.
- It is possible to apply several protection plans to a website, but only one of them can run on a schedule. Other plans need to be started manually.
- The only available backup option is "[Backup file name](#)".
- The website protection plans are not shown on the **Plans > Protection** tab.

Backing up a website

To add a website

1. Click **Devices > Add**.
2. Click **Website**.
3. Configure the following access settings for the website:
 - In **Website name**, create and type a name for your website. This name will be displayed in the service console.
 - In **Host**, specify the host name or IP address that will be used to access the website via SFTP or SSH. For example, `my.server.com` or `10.250.100.100`.
 - In **Port**, specify the port number.
 - In **User name** and **Password**, specify the credentials of the account that can be used to access the website via SFTP or SSH.

Important

Only the files that are accessible to the specified account will be backed up.

Instead of a password, you can specify your private SSH key. To do this, select the **Use SSH private key instead of password** check box, and then specify the key.

4. Click **Next**.
5. If your website uses MySQL databases, configure the access settings for the databases. Otherwise, click **Skip**.
 - a. In **Connection type**, select how to access the databases from the cloud:
 - **Via SSH from host**—The databases will be accessed via the host specified in step 3.
 - **Direct connection**—The databases will be accessed directly. Choose this setting only if the databases are accessible from the Internet.
 - b. In **Host**, specify the name or IP address of the host where the MySQL server is running.
 - c. In **Port**, specify the port number for the TCP/IP connection to the server. The default port number is 3306.
 - d. In **User name** and **Password**, specify the MySQL account credentials.

Important

Only the databases that are accessible to the specified account will be backed up.

- e. Click **Create**.

The website appears in the service console under **Devices > Websites**.

To change the connection settings

1. Select the website under **Devices > Websites**.
2. Click **Details**.
3. Click the pencil icon next to the website or the database connection settings.
4. Do the necessary changes, and then click **Save**.

To create a protection plan for websites

1. Select a website or several websites under **Devices > Websites**.
2. Click **Protect**.
3. [Optional] Enable backup of databases.

If several websites are selected, backup of databases is disabled by default.
4. [Optional] Change the [retention rules](#).
5. [Optional] Enable [encryption of backups](#).
6. [Optional] Click the gear icon to edit the **Backup file name** option. This makes sense in two cases:
 - If you backed up this website earlier and want to continue the existing sequence of backups
 - If you want to see the custom name on the **Backup storage** tab
7. Click **Apply**.

You can edit, revoke, and delete protection plans for websites in the same way as for machines. These operations are described in "Operations with protection plans".

Recovering a website

To recover a website

1. Do one of the following:
 - Under **Devices > Websites**, select the website that you want to recover, and then click **Recovery**.
You can search websites by name. Wildcards are not supported.
 - If the website was deleted, select it in the **Cloud applications backups** section of [the Backup storage tab](#), and then click **Show backups**.
To recover a deleted website, you need to add the target site as a device.
2. Select the recovery point.
3. Click **Recover**, and then select what you want to recover: **Entire website**, **Databases** (if any), or **Files/folders**.
To ensure that your website is in a consistent state, we recommend recovering both files and databases, in any order.
4. Depending on your choice, follow one of the procedures described below.

To recover the entire website

1. In **Recover to website**, view or change the target website.
By default, the original website is selected. If it does not exist, you must select the target website.
2. Select whether to recover the sharing permissions of the recovered items.
3. Click **Start recovery**, and then confirm the action.

To recover the databases

1. Select the databases that you want to recover.
2. If you want to download a database as a file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
3. Click **Recover**.
4. In **Recover to website**, view or change the target website.
By default, the original website is selected. If it does not exist, you must select the target website.
5. Click **Start recovery**, and then confirm the action.

To recover the website files/folders

1. Select the files/folders that you want to recover.
2. If you want to save a file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
3. Click **Recover**.
4. In **Recover to website**, view or change the target website.
By default, the original website is selected. If it does not exist, you must select the target website.
5. Select whether to recover the sharing permissions of the recovered items.
6. Click **Start recovery**, and then confirm the action.

14.23.2 Protecting web hosting servers

Web hosting administrators that use the Plesk or cPanel platforms can integrate these platforms with the Cyber Protection service.

The integration enables an administrator to do the following:

- Back up an entire Plesk or cPanel server to the cloud storage, with disk-level backup
- Recover the entire server, including all of the websites
- For Plesk: perform granular recovery of websites, individual files, mailboxes, or databases
- For cPanel: perform granular recovery of websites, individual files, mailboxes, mail filters, mail forwarders, databases, and accounts
- Enable self-service recovery for Plesk and cPanel customers

The integration is performed by using the Cyber Protection service extension. If you need the extension for Plesk or cPanel, contact the provider of the Cyber Protection service.

Supported Plesk and cPanel versions

- Plesk for Linux 17.0 and later
- Any cPanel version with PHP 5.6 and later

Quotas

Each backed-up Plesk or cPanel server consumes the **Web hosting servers** quota. If this quota is disabled or the overage for this quota is exceeded, the following will happen:

- If the server is physical, the **Servers** quota will be used. If this quota is disabled or the overage for this quota is exceeded, the backup will fail.
- If the server is virtual, the **Virtual machines** quota will be used. If this quota is disabled or the overage for this quota is exceeded, the backup will fail.

14.24 Special operations with virtual machines

14.24.1 Running a virtual machine from a backup (Instant Restore)

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

We recommend running this temporary virtual machine for up to three days. Then, you can completely remove it or convert it to a regular virtual machine (finalize) without downtime.

As long as the temporary virtual machine exists, retention rules cannot be applied to the backup being used by that machine. Backups of the original machine can continue to run.

Usage examples

- **Disaster recovery**

Instantly bring a copy of a failed machine online.

- **Testing a backup**

Run the machine from the backup and ensure that the guest OS and applications are functioning properly.

- **Accessing application data**

While the machine is running, use application's native management tools to access and extract the required data.

Prerequisites

- At least one Agent for VMware or Agent for Hyper-V must be registered in the Cyber Protection service.
- The backup can be stored in a network folder or in a local folder of the machine where Agent for VMware or Agent for Hyper-V is installed. If you select a network folder, it must be accessible from that machine. A virtual machine can also be run from a backup stored in the cloud storage, but it works slower because this operation requires intense random-access reading from the backup.
- The backup must contain an entire machine or all of the volumes that are required for the operating system to start.
- Backups of both physical and virtual machines can be used. Backups of Virtuozzo *containers* cannot be used.
- Backups that contain Linux logical volumes (LVM) must be created by Agent for VMware or Agent for Hyper-V. The virtual machine must be of the same type as the original machine (ESXi or Hyper-V).

Running the machine

1. Do one of the following:
 - Select a backed-up machine, click **Recovery**, and then select a recovery point.
 - Select a recovery point on [the Backup storage tab](#).
2. Click **Run as VM**.



The software automatically selects the host and other required parameters.

X
Run 'Windows 8 x64' as VM

TARGET MACHINE Windows 8 x64_temp on 10.255.154.182
DATASTORE datastore3
VM SETTINGS Memory: 2.00 GB Network adapters: 1
POWER STATE On ▼
<div>RUN NOW</div>

- [Optional] Click **Target machine**, and then change the virtual machine type (ESXi or Hyper-V), the host, or the virtual machine name.
- [Optional] Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore for the virtual machine.

Changes to the virtual disks accumulate while the machine is running. Ensure that the selected datastore has enough free space. If you are planning to preserve these changes by [making the virtual machine permanent](#), select a datastore that is suitable for running the machine in production.
- [Optional] Click **VM settings** to change the memory size and network connections of the virtual machine.
- [Optional] Select the VM power state (**On/Off**).
- Click **Run now**.

As a result, the machine appears in the web interface with one of the following icons:  or . Such virtual machines cannot be selected for backup.

Deleting the machine

We do not recommend to delete a temporary virtual machine directly in vSphere/Hyper-V. This may lead to artifacts in the web interface. Also, the backup from which the machine was running may remain locked for a while (it cannot be deleted by retention rules).

To delete a virtual machine that is running from a backup

1. On the **All devices** tab, select a machine that is running from a backup.
2. Click **Delete**.

The machine is removed from the web interface. It is also removed from the vSphere or Hyper-V inventory and datastore (storage). All changes that occurred to the data while the machine was running are lost.

Finalizing the machine

While a virtual machine is running from a backup, the virtual disks' content is taken directly from that backup. Therefore, the machine will become inaccessible or even corrupted if the connection is lost to the backup location or to the protection agent.

You have the option to make this machine permanent, i.e. recover all of its virtual disks, along with the changes that occurred while the machine was running, to the datastore that stores these changes. This process is named finalization.

Finalization is performed without downtime. The virtual machine will *not* be powered off during finalization.

The location of the final virtual disks is defined in the parameters of the **Run as VM** operation (**Datastore** for ESXi or **Path** for Hyper-V). Prior to starting the finalization, ensure that free space, sharing capabilities, and performance of this datastore are suitable for running the machine in production.

Note

Finalization is not supported for Hyper-V running in Windows Server 2008/2008 R2 and Microsoft Hyper-V Server 2008/2008 R2 because the necessary API is missing in these Hyper-V versions.

To finalize a machine that is running from a backup

1. On the **All devices** tab, select a machine that is running from a backup.
2. Click **Finalize**.
3. [Optional] Specify a new name for the machine.
4. [Optional] Change the disk provisioning mode. The default setting is **Thin**.
5. Click **Finalize**.

The machine name changes immediately. The recovery progress is shown on the **Activities** tab. Once the recovery is completed, the machine icon changes to that of a regular virtual machine.

What you need to know about finalization

Finalization vs. regular recovery

The finalization process is slower than a regular recovery for the following reasons:

- During a finalization, the agent performs random access to different parts of the backup. When an entire machine is being recovered, the agent reads data from the backup sequentially.
- If the virtual machine is running during the finalization, the agent reads data from the backup more often, to maintain both processes simultaneously. During a regular recovery, the virtual machine is stopped.

Finalization of machines running from cloud backups

Because of intensive access to the backed-up data, the finalization speed highly depends on the connection bandwidth between the backup location and the agent. The finalization will be slower for backups located in the cloud as compared to local backups. If the Internet connection is very slow or unstable, the finalization of a machine running from a cloud backup may fail. We recommend to run virtual machines from local backups if you are planning to perform finalization and have the choice.

14.24.2 Working in VMware vSphere

This section describes operations that are specific for VMware vSphere environments.

Replication of virtual machines

Replication is available only for VMware ESXi virtual machines.

Replication is the process of creating an exact copy (replica) of a virtual machine, and then maintaining the replica in sync with the original machine. By replicating a critical virtual machine, you will always have a copy of this machine in a ready-to-start state.

The replication can be started manually or on the schedule you specify. The first replication is full (copies the entire machine). All subsequent replications are incremental and are performed with [Changed Block Tracking](#), unless this option is disabled.

Replication vs. backing up

Unlike scheduled backups, a replica keeps only the latest state of the virtual machine. A replica consumes datastore space, while backups can be kept on a cheaper storage.

However, powering on a replica is much faster than a recovery and faster than running a virtual machine from a backup. When powered on, a replica works faster than a VM running from a backup and does not load the Agent for VMware.

Usage examples

- **Replicate virtual machines to a remote site.**

Replication enables you to withstand partial or complete datacenter failures, by cloning the virtual machines from a primary site to a secondary site. The secondary site is usually located in a remote facility that is unlikely to be affected by environmental, infrastructure, or other factors that might cause the primary site failure.

- **Replicate virtual machines within a single site (from one host/datastore to another).**

Onsite replication can be used for high availability and disaster recovery scenarios.

What you can do with a replica

- **Test a replica**

The replica will be powered on for testing. Use vSphere Client or other tools to check if the replica works correctly. Replication is suspended while testing is in progress.

- **Failover to a replica**

Failover is a transition of the workload from the original virtual machine to its replica. Replication is suspended while a failover is in progress.

- **Back up the replica**

Both backup and replication require access to virtual disks, and thus impact the performance of the host where the virtual machine is running. If you want to have both a replica and backups of a virtual machine, but don't want to put additional load on the production host, replicate the machine to a different host, and set up backups of the replica.

Restrictions

The following types of virtual machines cannot be replicated:

- Fault-tolerant machines running on ESXi 5.5 and lower.
- Machines running from backups.
- Replicas of virtual machines.

Creating a replication plan

A replication plan must be created for each machine individually. It is not possible to apply an existing plan to other machines.

To create a replication plan

1. Select a virtual machine to replicate.
2. Click **Replication**.
The software displays a new replication plan template.
3. [Optional] To modify the replication plan name, click the default name.
4. Click **Target machine**, and then do the following:

- a. Select whether to create a new replica or use an existing replica of the original machine.
- b. Select the ESXi host and specify the new replica name, or select an existing replica.
The default name of a new replica is **[Original Machine Name]_replica**.
- c. Click **OK**.
5. [Only when replicating to a new machine] Click **Datastore**, and then select the datastore for the virtual machine.
6. [Optional] Click **Schedule** to change the replication schedule.
By default, replication is performed on a daily basis, Monday to Friday. You can select the time to run the replication.
If you want to change the replication frequency, move the slider, and then specify the schedule.
You can also do the following:
 - Set a date range for when the schedule is effective. Select the **Run the plan within a date range** check box, and then specify the date range.
 - Disable the schedule. In this case, replication can be started manually.
7. [Optional] Click the gear icon to modify the [replication options](#).
8. Click **Apply**.
9. [Optional] To run the plan manually, click **Run now** on the plan panel.

As a result of running a replication plan, the virtual machine replica appears in the **All devices** list

with the following icon: 

Testing a replica

To prepare a replica for testing

1. Select a replica to test.
2. Click **Test replica**.
3. Click **Start testing**.
4. Select whether to connect the powered-on replica to a network. By default, the replica will not be connected to a network.
5. [Optional] If you chose to connect the replica to the network, select the **Stop original virtual machine** check box to stop the original machine before powering on the replica.
6. Click **Start**.

To stop testing a replica

1. Select a replica for which testing is in progress.
2. Click **Test replica**.
3. Click **Stop testing**.
4. Confirm your decision.

Failing over to a replica

To failover a machine to a replica

1. Select a replica to failover to.
2. Click **Replica actions**.
3. Click **Failover**.
4. Select whether to connect the powered-on replica to a network. By default, the replica will be connected to the same network as the original machine.
5. [Optional] If you chose to connect the replica to the network, clear the **Stop original virtual machine** check box to keep the original machine online.
6. Click **Start**.

While the replica is in a failover state, you can choose one of the following actions:

- **Stop failover**
Stop failover if the original machine was fixed. The replica will be powered off. Replication will be resumed.
- **Perform permanent failover to the replica**
This instant operation removes the 'replica' flag from the virtual machine, so that replication to it is no longer possible. If you want to resume replication, edit the replication plan to select this machine as a source.
- **Failback**
Perform failback if you failed over to the site that is not intended for continuous operations. The replica will be recovered to the original or a new virtual machine. Once the recovery to the original machine is complete, it is powered on and replication is resumed. If you choose to recover to a new machine, edit the replication plan to select this machine as a source.

Stopping failover

To stop a failover

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Stop failover**.
4. Confirm your decision.

Performing a permanent failover

To perform a permanent failover

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Permanent failover**.
4. [Optional] Change the name of the virtual machine.
5. [Optional] Select the **Stop original virtual machine** check box.
6. Click **Start**.

Failing back

To failback from a replica

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Failback from replica**.

The software automatically selects the original machine as the target machine.
4. [Optional] Click **Target machine**, and then do the following:
 - a. Select whether to failback to a new or existing machine.
 - b. Select the ESXi host and specify the new machine name, or select an existing machine.
 - c. Click **OK**.
5. [Optional] When failing back to a new machine, you can also do the following:
 - Click **Datastore** to select the datastore for the virtual machine.
 - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.
6. [Optional] Click **Recovery options** to modify the [failback options](#).
7. Click **Start recovery**.
8. Confirm your decision.

Replication options

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

Changed Block Tracking (CBT)

This option is similar to the backup option "[Changed Block Tracking \(CBT\)](#)".

Disk provisioning

This option defines the disk provisioning settings for the replica.

The preset is: **Thin provisioning**.

The following values are available: **Thin provisioning**, **Thick provisioning**, **Keep the original setting**.

Error handling

This option is similar to the backup option "[Error handling](#)".

Pre/Post commands

This option is similar to the backup option "[Pre/Post commands](#)".

Volume Shadow Copy Service VSS for virtual machines

This option is similar to the backup option "[Volume Shadow Copy Service VSS for virtual machines](#)".

Failback options

To modify the failback options, click **Recovery options** when configuring failback.

Error handling

This option is similar to the recovery option "[Error handling](#)".

Performance

This option is similar to the recovery option "[Performance](#)".

Pre/Post commands

This option is similar to the recovery option "[Pre/Post commands](#)".

VM power management

This option is similar to the recovery option "[VM power management](#)".

Seeding an initial replica

To speed up replication to a remote location and save network bandwidth, you can perform replica seeding.

Important

To perform replica seeding, Agent for VMware (Virtual Appliance) must be running on the target ESXi.

To seed an initial replica

1. Do one of the following:
 - If the original virtual machine can be powered off, power it off, and then skip to step 4.
 - If the original virtual machine cannot be powered off, continue to the next step.
2. [Create a replication plan](#).

When creating the plan, in **Target machine**, select **New replica** and the ESXi that hosts the original machine.
3. Run the plan once.

A replica is created on the original ESXi.
4. Export the virtual machine (or the replica) files to an external hard drive.
 - a. Connect the external hard drive to the machine where vSphere Client is running.
 - b. Connect vSphere Client to the original vCenter\ESXi.
 - c. Select the newly created replica in the inventory.
 - d. Click **File > Export > Export OVF template**.
 - e. In **Directory**, specify the folder on the external hard drive.
 - f. Click **OK**.
5. Transfer the hard drive to the remote location.
6. Import the replica to the target ESXi.

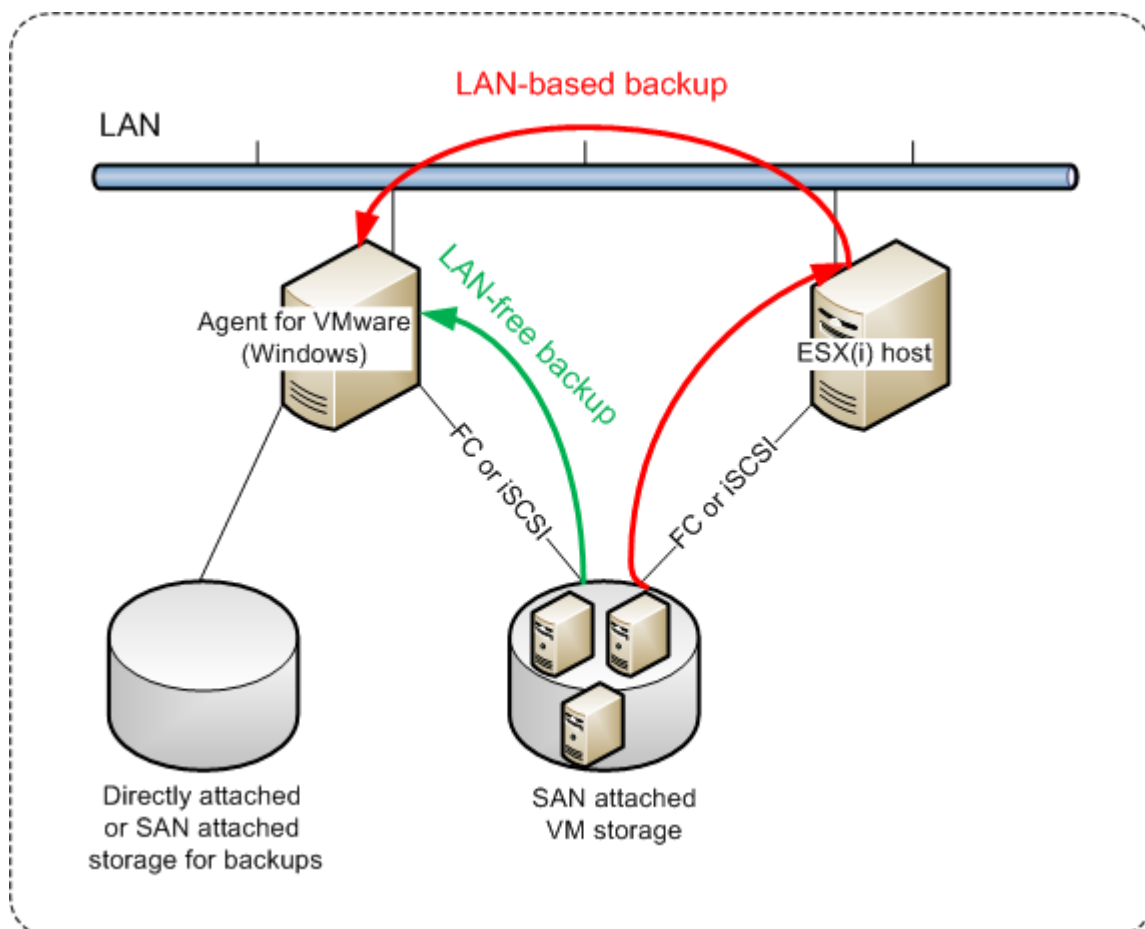
- a. Connect the external hard drive to the machine where vSphere Client is running.
 - b. Connect vSphere Client to the target vCenter\ESXi.
 - c. Click **File > Deploy OVF template**.
 - d. In **Deploy from a file or URL**, specify the template that you exported in step 4.
 - e. Complete the import procedure.
7. Edit the replication plan that you created in step 2. In **Target machine**, select **Existing replica**, and then select the imported replica.

As a result, the software will continue updating the replica. All replications will be incremental.

Agent for VMware - 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. This capability is called a LAN-free backup.

The diagram below illustrates a LAN-based and a LAN-free backup. LAN-free access to virtual machines is available if you have a fibre channel (FC) or iSCSI Storage Area Network. To completely eliminate transferring the backed-up data via LAN, store the backups on a local disk of the agent's machine or on a SAN attached storage.



To enable the agent to access a datastore directly

1. Install Agent for VMware on a Windows machine that has network access to the vCenter Server.
2. Connect the logical unit number (LUN) that hosts the datastore to the machine. Consider the following:
 - Use the same protocol (i.e. iSCSI or FC) that is used for the datastore connection to the ESXi.
 - The LUN *must not* be initialized and must appear as an "offline" disk in **Disk Management**. If Windows initializes the LUN, it may become corrupted and unreadable by VMware vSphere.

As a result, the agent will use the SAN transport mode to access the virtual disks, i.e. it will read raw LUN sectors over iSCSI/FC without recognizing the VMFS file system (which Windows is not aware of).

Limitations

- In vSphere 6.0 and later, the agent cannot use the SAN transport mode if some of the VM disks are located on a VMware Virtual Volume (VVol) and some are not. Backups of such virtual machines will fail.
- Encrypted virtual machines, introduced in VMware vSphere 6.5, will be backed up via LAN, even if you configure the SAN transport mode for the agent. The agent will fall back on the NBD transport because VMware does not support SAN transport for backing up encrypted virtual disks.

Example

If you are using an iSCSI SAN, configure the iSCSI initiator on the machine running Windows where Agent for VMware is installed.

To configure the SAN policy

1. Log on as an administrator, open the command prompt, type `diskpart`, and then press **Enter**.
2. Type `san`, and then press **Enter**. Ensure that **SAN Policy : Offline All** is displayed.
3. If another value for SAN Policy is set:
 - a. Type `san policy=offlineall`.
 - b. Press **Enter**.
 - c. To check that the setting has been applied correctly, perform step 2.
 - d. Restart the machine.

To configure an iSCSI initiator

1. Go to **Control Panel > Administrative Tools > iSCSI Initiator**.

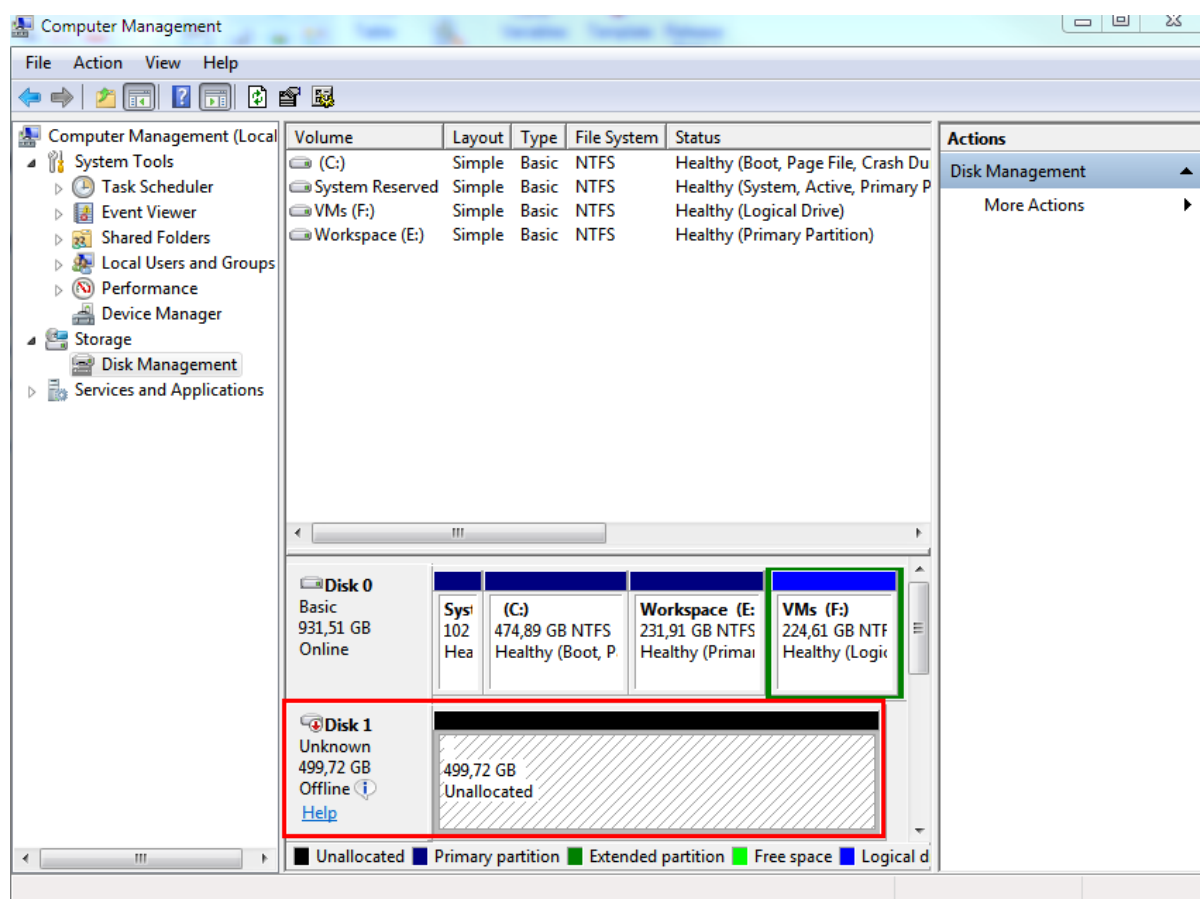
Note

To find the **Administrative Tools** applet, you may need to change the **Control Panel** view to something other than **Home** or **Category**, or use search.

2. If this is the first time that Microsoft iSCSI Initiator is launched, confirm that you want to start the Microsoft iSCSI Initiator service.

3. On the **Targets** tab, type the fully qualified domain name (FQDN) name or the IP address of the target SAN device, and then click **Quick Connect**.
4. Select the LUN that hosts the datastore, and then click **Connect**.
If the LUN is not displayed, ensure that the zoning on the iSCSI target enables the machine running the agent to access the LUN. The machine must be added to the list of allowed iSCSI initiators on this target.
5. Click **OK**.

The ready SAN LUN should appear in **Disk Management** as shown in the screenshot below.



Using a locally attached storage

You can attach an additional disk to Agent for VMware (Virtual Appliance) so the agent can back up to this locally attached storage. This approach eliminates the network traffic between the agent and the backup location.

A virtual appliance that is running on the same host or cluster with the backed-up virtual machines has direct access to the datastore(s) where the machines reside. This means the appliance can attach the backed-up disks by using the HotAdd transport, and therefore the backup traffic is directed from one local disk to another. If the datastore is connected as **Disk/LUN** rather than **NFS**, the backup will be completely LAN-free. In the case of NFS datastore, there will be network traffic between the datastore and the host.

Using a locally attached storage presumes that the agent always backs up the same machines. If multiple agents work within the vSphere, and one or more of them use locally attached storages, you need to [manually bind](#) each agent to all machines it has to back up. Otherwise, if the machines are redistributed among the agents by the management server, a machine's backups may be dispersed over multiple storages.

You can add the storage to an already working agent or when deploying the agent [from an OVF template](#).

To attach a storage to an already working agent

1. In VMware vSphere inventory, right click the Agent for VMware (Virtual Appliance).
2. Add the disk by editing the settings of the virtual machine. The disk size must be at least 10 GB.

Warning!

Be careful when adding an already existing disk. Once the storage is created, all data previously contained on this disk will be lost.

3. Go to the virtual appliance console. The **Create storage** link is available at the bottom of the screen. If it is not, click **Refresh**.
4. Click the **Create storage** link, select the disk and specify a label for it. The label length is limited to 16 characters, due to file system restrictions.

To select a locally attached storage as a backup destination

When [creating a protection plan](#), in **Where to back up**, select **Local folders**, and then type the letter corresponding to the locally attached storage, for example, **D:**.

Virtual machine binding

This section gives you an overview of how the Cyber Protection service organizes the operation of multiple agents within VMware vCenter.

The below distribution algorithm works for both virtual appliances and agents installed in Windows.

Distribution algorithm

The virtual machines are automatically evenly distributed between Agents for VMware. By evenly, we mean that each agent manages an equal number of machines. The amount of storage space occupied by a virtual machine is not counted.

However, when choosing an agent for a machine, the software tries to optimize the overall system performance. In particular, the software considers the agent and the virtual machine location. An agent hosted on the same host is preferred. If there is no agent on the same host, an agent from the same cluster is preferred.

Once a virtual machine is assigned to an agent, all backups of this machine are delegated to this agent.

Redistribution

Redistribution takes place each time the established balance breaks, or, more precisely, when a load imbalance among the agents reaches 20 percent. This may happen when a machine or an agent is added or removed, or a machine migrates to a different host or cluster, or if you manually bind a machine to an agent. If this happens, the Cyber Protection service 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 Cyber Protection service will assign the most appropriate machines to the new agent. The old agents' load will reduce.

When you remove an agent from the Cyber Protection service, 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 vSphere. Redistribution will start only after you remove such agent from the web interface.

Viewing the distribution result

You can view the result of the automatic distribution:

- in the **Agent** column for each virtual machine on the **All devices** section
- in the **Assigned virtual machines** section of the **Details** panel when an agent is selected in the **Settings > Agents** section

Manual binding

The Agent for VMware binding lets you exclude a virtual machine from this distribution process by specifying the agent that must always back up this machine. The overall balance will be maintained, but this particular machine can be passed to a different agent only if the original agent is removed.

To bind a machine with an agent

1. Select the machine.
2. Click **Details**.
In the **Assigned agent** section, the software shows the agent that currently manages the selected machine.
3. Click **Change**.
4. Select **Manual**.
5. Select the agent to which you want to bind the machine.
6. Click **Save**.

To unbind a machine from an agent

1. Select the machine.
2. Click **Details**.

In the **Assigned agent** section, the software shows the agent that currently manages the selected machine.

3. Click **Change**.
4. Select **Automatic**.
5. Click **Save**.

Disabling automatic assignment for an agent

You can disable the automatic assignment for Agent for VMware to exclude it from the distribution process by specifying the list of machines that this agent must back up. The overall balance will be maintained between other agents.

Automatic assignment cannot be disabled for an agent if there are no other registered agents, or if automatic assignment is disabled for all other agents.

To disable automatic assignment for an agent

1. Click **Settings > Agents**.
2. Select Agent for VMware for which you want to disable the automatic assignment.
3. Click **Details**.
4. Disable the **Automatic assignment** switch.

Usage examples

- Manual binding comes in handy if you want a particular (very large) machine to be backed up by Agent for VMware (Windows) via a fibre channel while other machines are backed up by virtual appliances.
- It is necessary to bind VMs to an agent if the agent has a locally attached storage.
- Disabling the automatic assignment enables you to ensure that a particular machine is predictably backed up on the schedule you specify. The agent that only backs up one VM cannot be busy backing up other VMs when the scheduled time comes.
- Disabling the automatic assignment is useful if you have multiple ESXi hosts that are separated geographically. If you disable the automatic assignment, and then bind the VMs on each host to the agent running on the same host, you can ensure that the agent will never back up any machines running on the remote ESXi hosts, thus saving network traffic.

Support for VM migration

This section informs you about what to expect when virtual machines migrate within a vSphere environment, including migration between ESXi hosts that are part of a vSphere cluster.

vMotion

vMotion moves a virtual machine's state and configuration to another host while the machine's disks remain in the same location on shared storage.

- vMotion of Agent for VMware (Virtual Appliance) is not supported and is disabled.
- vMotion of a virtual machine is disabled during a backup. Backups will continue to run after the migration is completed.

Storage vMotion

Storage vMotion moves virtual machine disks from one datastore to another.

- Storage vMotion of Agent for VMware (Virtual Appliance) is not supported and is disabled.
- Storage vMotion of a virtual machine is disabled during a backup. Backups will continue to run after the migration.

Managing virtualization environments

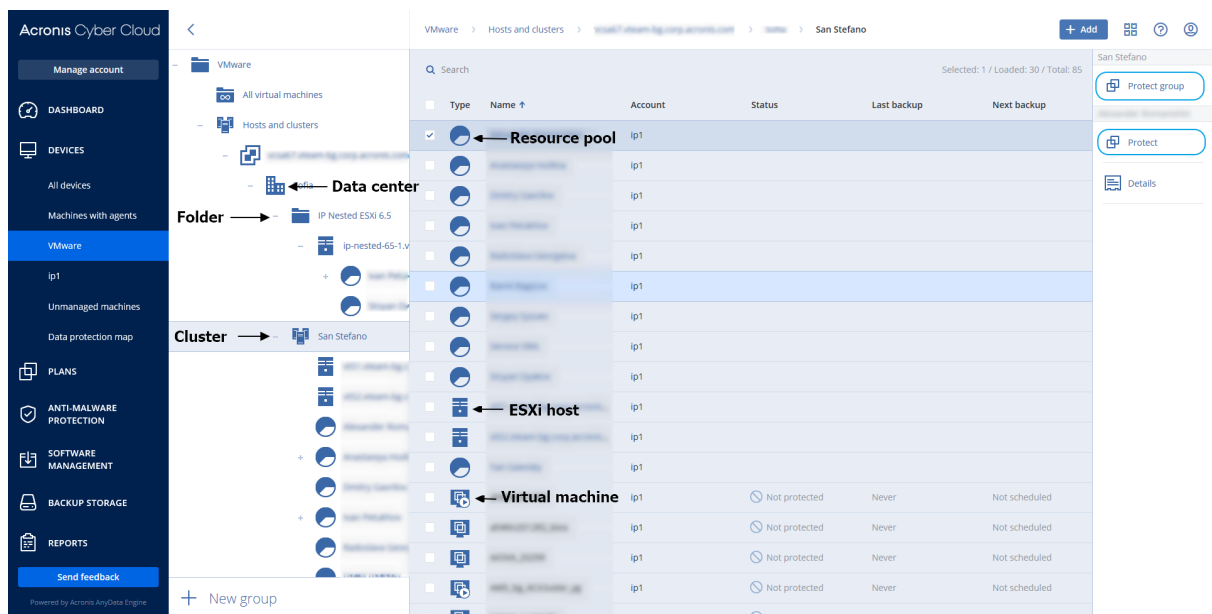
You can view the vSphere, Hyper-V, and Virtuozzo environments in their native presentation. Once the corresponding agent is installed and registered, the **VMware**, **Hyper-V**, or **Virtuozzo** tab appears under **Devices**.

In the **VMware** tab, you can back up the following vSphere infrastructure objects:

- Data center
- Folder
- Cluster
- ESXi host
- Resource pool

Each of these infrastructure objects works as a group object for virtual machines. When you apply a protection plan to any of these group objects, all virtual machines included in it, will be backed up. You can back up either the selected group machines by clicking **Protect**, or the parent group machines in which the selected group is included by clicking **Protect group**.

For example, you have selected the San Stefano cluster and then selected the resource pool inside it. If you click **Protect**, all virtual machines included in the selected resource pool will be backed up. If you click **Protect group**, all virtual machines included in the San Stefano cluster will be backed up.



The **VMware** tab enables you to change access credentials for the vCenter Server or stand-alone ESXi host without re-installing the agent.

To change the vCenter Server or ESXi host access credentials

1. Under **Devices**, click **VMware**.
2. Click **Hosts and Clusters**.
3. In the **Hosts and Clusters** list (to the right of the **Hosts and Clusters** tree), select the vCenter Server or stand-alone ESXi host that was specified during the Agent for VMware installation.
4. Click **Details**.
5. Under **Credentials**, click the user name.
6. Specify the new access credentials, and then click **OK**.

Viewing backup status in vSphere Client

You can view backup status and the last backup time of a virtual machine in vSphere Client.

This information appears in the virtual machine summary (**Summary** > **Custom attributes/Annotations/Notes**, depending on the client type and vSphere version). You can also enable the **Last backup** and **Backup status** columns on the **Virtual Machines** tab for any host, datacenter, folder, resource pool, or the entire vCenter Server.

To provide these attributes, Agent for VMware must have the following privileges in addition to those described in "[Agent for VMware - necessary privileges](#)":

- **Global** > **Manage custom attributes**
- **Global** > **Set custom attribute**

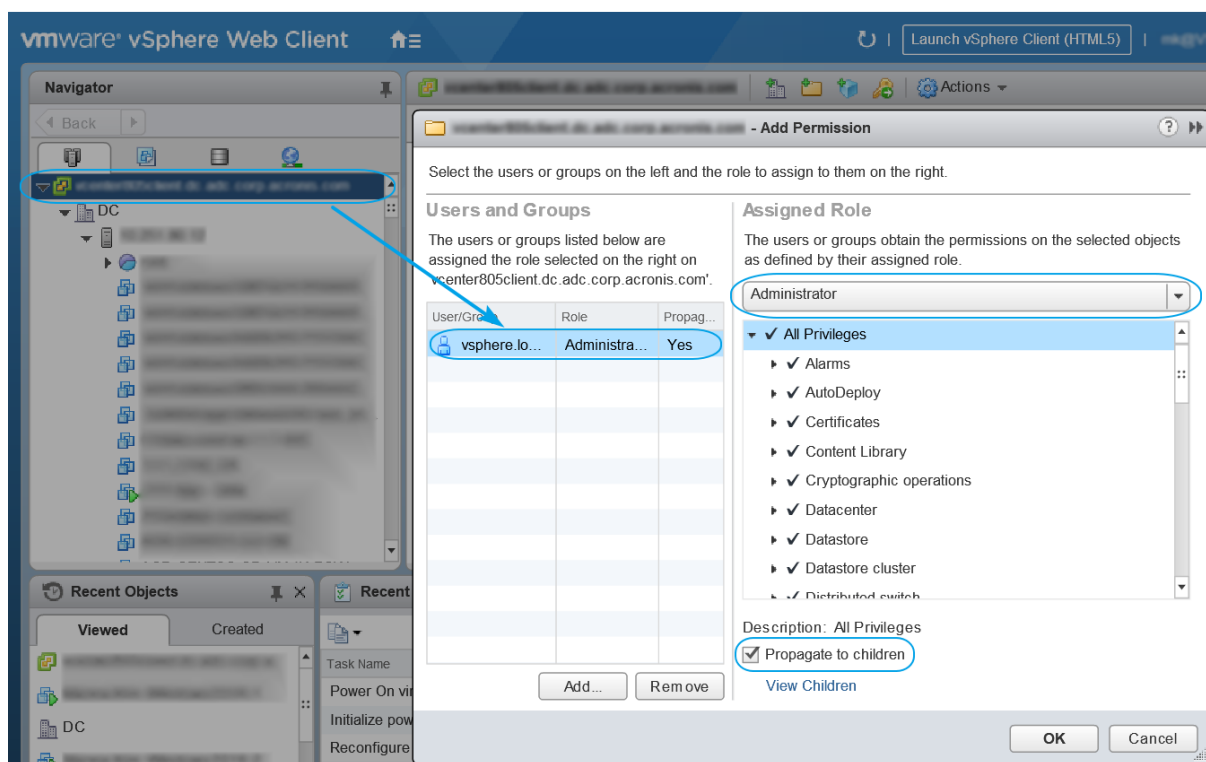
Agent for VMware - necessary privileges

To perform any operations with vCenter objects, such as virtual machines, ESXi hosts, clusters, vCenter, and more, Agent for VMware authenticates on vCenter or ESXi host by using the vSphere credentials provided by a user. The vSphere account, used for connection to vSphere by Agent for VMware, must have the required privileges on all levels of vSphere infrastructure starting from the vCenter level.

Specify the vSphere account with the necessary privileges during Agent for VMware installation or configuration. If you need to change the account at a later time, refer to the "[Managing virtualization environments](#)" section.

To assign the permissions to a vSphere user on the vCenter level, do the following:

1. Log in to vSphere web client.
2. Right-click on vCenter and then click **Add permission**.
3. Select or add a new user with the required role (the role must include all the required permissions from the table below).
4. Select the **Propagate to children** option.



Object	Privilege	Operation			
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup

Cryptographic operations (starting with vSphere 6.5)	Add disk	++			
	Direct Access	++			
Datastore	Allocate space		+	+	+
	Browse datastore				+
	Configure datastore	+	+	+	+
	Low level file operations				+
Global	Licenses	+	+	+	+
	Disable methods	+	+	+	
	Enable methods	+	+	+	
	Manage custom attributes	+	+	+	
	Set custom attribute	+	+	+	
Host > Configuration	Storage partition configuration				+
Host > Local operations	Create VM				+
	Delete VM				+
	Reconfigure VM				+
Network	Assign network		+	+	+
Resource	Assign VM to resource pool		+	+	+
Virtual machine > Configuration	Add existing disk	+	+		+
	Add new disk		+	+	+
	Add or remove device		+		+
	Advanced	+	+	+	
	Change CPU count		+		
	Disk change tracking	+		+	
	Disk lease	+		+	
	Memory		+		

	Remove disk	+	+	+	+
	Rename		+		
	Set annotation				+
	Settings		+	+	+
Virtual machine > Guest Operations	Guest Operation Program Execution	***			
	Guest Operation Queries	***			
	Guest Operation Modifications	***			
Virtual machine > Interaction	Acquire guest control ticket (in vSphere 4.1 and 5.0)				+
	Configure CD media		+	+	
	Guest operating system management by VIX API (in vSphere 5.1 and later)				+
	Power off			+	+
	Power on		+	+	+
Virtual machine > Inventory	Create from existing		+	+	+
	Create new		+	+	+
	Register				+
	Remove		+	+	+
	Unregister				+
Virtual machine > Provisioning	Allow disk access		+	+	+
	Allow read-only disk access	+		+	
	Allow virtual machine download	+	+	+	+
Virtual machine > State	Create snapshot	+		+	+
	Remove snapshot	+		+	+
vApp	Add virtual machine				+

* This privilege is required for backing up encrypted machines only.

** This privilege is required for application-aware backups only.

14.24.3 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 in the Cyber Protection service.

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, 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.

14.24.4 Limiting the total number of simultaneously backed-up virtual machines

The **Scheduling** backup option defines how many virtual machines an agent can back up simultaneously when executing the given protection plan.

When multiple protection plans overlap in time, the numbers specified in their backup options are added up. Even though the resulting total number is programmatically limited to 10, overlapping plans can affect the backup performance and overload both the host and the virtual machine storage.

You can further reduce the total number of virtual machines that an Agent for VMware or Agent for Hyper-V can back up simultaneously.

To limit the total number of virtual machines that Agent for VMware (Windows) or Agent for Hyper-V can back up

1. On the machine running the agent, create a new text document and open it in a text editor, such as Notepad.
2. Copy and paste the following lines into the file:

```
Windows Registry Editor Version 5.00
```



```
[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Replace 00000001 with the hexadecimal value of the limit that you want to set. For example, 00000001 is 1 and 0000000A is 10.
4. Save the document as **limit.reg**.
5. Run the file as an administrator.
6. Confirm that you want to edit the Windows registry.
7. Do the following to restart the agent:
 - a. In the **Start** menu, click **Run**, and then type: **cmd**
 - b. Click **OK**.
 - c. Run the following commands:

```
net stop mms
net start mms
```

To limit the total number of virtual machines that Agent for VMware (Virtual Appliance) can back up

1. To start the command shell, press CTRL+SHIFT+F2 while in the virtual appliance UI.
2. Open the file **/etc/Acronis/MMS.config** in a text editor, such as **vi**.
3. Locate the following section:

```
<key name="SimultaneousBackupsLimits">
  <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Replace 10 with the decimal value of the limit that you want to set.
5. Save the file.
6. Execute the reboot command to restart the agent.

14.24.5 Machine migration

You can perform machine migration by recovering its backup to a non-original machine.

The following table summarizes the available migration options.

Backed-up machine type	Available recovery destinations							
	Physical machine	ESXi virtual machine	Hyper-V virtual machine	Virtuozzo virtual machine	Virtuozzo container	Virtuozzo Hybrid Infrastructure virtual machine	Scale Computing HC3 virtual machine	RHV/o Virt virtual machine
Physical machine	+	+	+	-	-	+	-	+
VMware ESXi virtual machine	+	+	+	-	-	+	-	+
Hyper-V virtual machine	+	+	+	-	-	+	-	+
Virtuozzo virtual machine	+	+	+	+	-	+	-	+
Virtuozzo container	-	-	-	-	+	-	-	-
Virtuozzo Hybrid Infrastructure virtual machine	+	+	+	-	-	+	-	+
Scale Computing HC3 virtual machine	+	+	+	-	-	+	+	+
Red Hat Virtualization/oVirt virtual machine	+	+	+	-	-	+	-	+

Note

You cannot recover macOS virtual machines to Hyper-V hosts, because Hyper-V does not support macOS. You can recover macOS virtual machines to a VMware host that is installed on Mac hardware.

For instructions on how to perform migration, refer to the following sections:

- Physical-to-virtual (P2V) - "[Physical machine to virtual](#)"
- Virtual-to-virtual (V2V) - "[Virtual machine](#)"
- Virtual-to-physical (V2P) - "[Virtual machine](#)" or "[Recovering disks by using bootable media](#)"

Although it is possible to perform V2P migration in the web interface, we recommend using bootable media in specific cases. Sometimes, you may want to use the media for migration to ESXi or Hyper-V.

The media enables you to do the following:

- Perform P2V migration or V2P migration or V2V migration from Virtuozzo, of a Linux machine containing logical volumes (LVM). Use Agent for Linux or bootable media to create the backup and bootable media to recover.
- Provide drivers for specific hardware that is critical for the system bootability.

14.24.6 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.

The difference from a physical machine is that Windows Azure and Amazon EC2 virtual machines cannot be booted from bootable media. If you need to recover to a new Windows Azure or Amazon EC2 virtual machine, follow the procedure below.

To recover a machine as a Windows Azure or Amazon EC2 virtual machine

1. Create a new virtual machine from an image/template in Windows Azure or Amazon EC2. The new machine must have the same disk configuration as the machine that you want to recover.
2. Install Agent for Windows or Agent for Linux on the new machine.
3. Recover the backed-up machine as described in "[Physical machine](#)". When configuring the recovery, select the new machine as the target machine.

15 Disaster recovery

Note

This functionality is available only with the Disaster Recovery add-on of the Cyber Protection service.

15.1 About Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) – a part of Cyber Protection that provides disaster recovery as a service (DRaaS). Cyber Disaster Recovery Cloud provides you with a fast and stable solution to launch the exact copies of your machines on the cloud site and switch the workload from the corrupted original machines to the recovery servers in the cloud in case of a man-made or a natural disaster.

You can set up and configure disaster recovery in the following ways:

- Create a protection plan that includes the disaster recovery module and apply it to your devices. This will automatically set up default disaster recovery infrastructure. See [Create a disaster recovery protection plan](#).
- Set up the disaster recovery cloud infrastructure manually and control each step. See "Setting up recovery servers" (p. 398).

15.1.1 The key functionality

Note

Some features might require additional licensing, depending on the applied licensing model.

- Manage the Cyber Disaster Recovery Cloud service from a single console
- Extend up to five local networks to the cloud, by using a secure VPN tunnel
- Establish the connection to the cloud site without any VPN appliance¹ deployment (the cloud-only mode)
- Establish the point-to-site connection to your local and cloud sites
- Protect your machines by using recovery servers in the cloud
- Protect applications and appliances by using primary servers in the cloud
- Perform automatic disaster recovery operations for encrypted backups
- Perform a test failover in the isolated network
- Use runbooks to spin up the production environment in the cloud

¹[Disaster Recovery] A special virtual machine that enables connection between the local network and the cloud site via a secure VPN tunnel. The VPN appliance is deployed on the local site.

15.2 Software requirements

15.2.1 Supported operating systems

Protection with a recovery server has been tested for the following operating systems:

- CentOS 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server

Windows desktop operating systems are not supported due to Microsoft product terms.

The software may work with other Windows operating systems and Linux distributions, but this is not guaranteed.

15.2.2 Supported virtualization platforms

Protection of virtual machines with a recovery server has been tested for the following virtualization platforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 with Hyper-V
- Windows Server 2012/2012 R2 with Hyper-V
- Windows Server 2016 with Hyper-V – all installation options, except for Nano Server
- Windows Server 2019 with Hyper-V – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

The VPN appliance has been tested for the following virtualization platforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 with Hyper-V
- Windows Server 2012/2012 R2 with Hyper-V
- Windows Server 2016 with Hyper-V – all installation options, except for Nano Server
- Windows Server 2019 with Hyper-V – all installation options, except for Nano Server

- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

The software may work with other virtualization platforms and versions, but this is not guaranteed.

15.2.3 Limitations

The following platforms and configurations are not supported in Cyber Disaster Recovery Cloud:

1. Unsupported platforms:

- Agents for Virtuozzo
- macOS

2. Unsupported configurations:

Microsoft Windows:

- Dynamic disks are not supported
- Windows desktop operating systems are not supported (due to Microsoft product terms)
- Active Directory service with FRS replication is not supported
- Removable media without either GPT or MBR formatting (so-called "superfloppy") are not supported

Linux:

- Linux machines that have logical volumes (LVM) or volumes formatted with the XFS file system
- File system without a partition table

3. Unsupported backup types:

- Continuous data protection (CDP) recovery points are incompatible.

Important

If you create a recovery server from a backup having a CDP recovery point, then during the failback or creating backup of a recovery server, you will lose the data contained in the CDP recovery point.

- Forensic backups cannot be used for creating recovery servers.

A recovery server has one network interface. If the original machine has several network interfaces, only one is emulated.

Cloud servers are not encrypted.

15.3 Setting up the disaster recovery functionality

Note

Some features might require additional licensing, depending on the applied licensing model.

To set up the disaster recovery functionality

1. Configure the connectivity type to the cloud site:
 - [Point-to-site connection](#)
 - [Site-to-site OpenVPN connection](#)
 - [Multi-site IPsec VPN connection](#)
 - [Cloud-only mode](#)
2. Create a protection plan with the backup module enabled and select the entire machine or system plus boot volumes for backing up. At least one protection plan is required for creating a recovery server.
3. Apply the protection plan to the local servers to be protected.
4. [Create the recovery servers](#) for each of your local servers that you want to protect.
5. [Perform a test failover](#) to check how it works.
6. [Optional] [Create the primary servers](#) for application replication.

As a result, you have set up the disaster recovery functionality to protect your local servers from a disaster.

If a disaster occurs, you can [fail over the workload](#) to the recovery servers in the cloud. At least one recovery point must be created before failing over to recovery servers. When your local site is recovered from a disaster, you can switch the workload back to your local site by performing failback. For more information about the failback process, see "Performing failback to a virtual machine" (p. 406) and "Performing failback to a physical machine" (p. 409).

15.4 Create a disaster recovery protection plan

Create a protection plan that includes the disaster recovery module and apply it to your devices.

By default, when creating a new protection plan, the Disaster recovery module is disabled. After you enable the disaster recovery functionality and apply the plan to your machines, the cloud network infrastructure is created, including a *recovery server* for each protected machine. The *recovery server* is a virtual machine in the cloud that is a copy of the selected device. For each of the selected devices a recovery server with default settings is created in a standby state (virtual machine not running). The recovery server is sized automatically depending on the CPU and RAM of the protected machine. Default cloud network infrastructure is also created automatically: VPN gateway and networks on the cloud site, to which the recovery servers are connected.

If you revoke, delete, or switch off the disaster recovery module of a protection plan, the recovery servers and cloud networks are not deleted automatically. You can remove the disaster recovery infrastructure manually, if needed.

Note

- It is recommended to configure disaster recovery in advance. You will be able to perform the test or production failover from any of the recovery points generated after the recovery server was created for the device. Recovery points that were generated when a device was not protected with disaster recovery (e.g. recovery server was not created) cannot be used for failover.
 - A disaster recovery protection plan cannot be enabled if the IP address of a device cannot be detected, for example, when virtual machines are backed up agentless and are not assigned an IP address.
 - When you apply a protection plan, the same networks and IP addresses are assigned in the cloud site. The IPsec VPN connectivity requires that network segments of the cloud and local sites do not overlap. If a Multi-site IPsec VPN connectivity is configured, and you apply a protection plan to one or several devices later, you must additionally update the cloud networks and reassign the IP addresses of the cloud servers. For more information, see "Reassigning IP addresses" (p. 391).
-

To create a disaster recovery protection plan

1. In the service console, go to **Devices > All devices**.
2. Select the machines that you want to protect.
3. Click **Protect**, and then click **Create plan**.
The protection plan default settings open.
4. Configure the backup options.
To use the disaster recovery functionality, the plan must back up the entire machine, or only the disks, required for booting up and providing the necessary services, to a cloud storage.
5. Enable the Disaster recovery module by clicking the switch next to the module name.
6. Click **Create**.
The plan is created and applied to the selected machines.

What to do next

- You can edit the default configuration of the recovery server. For more information, see "Setting up recovery servers" (p. 398).
- You can edit the default networking configuration. For more information, see "Setting up connectivity" (p. 366).
- You can learn more about the recovery server default parameters and the cloud network infrastructure. For more information, see "Editing the Recovery server default parameters" (p. 364) and "Cloud network infrastructure" (p. 366).

15.4.1 Editing the Recovery server default parameters

When you create and apply a disaster recovery protection plan, a recovery server with default parameters is created. You can edit these default parameters later.

Note

A recovery server is created only if it does not exist. Existing recovery servers are not changed or recreated.

To edit the recovery server default parameters

1. Go to **Devices > All devices**.
2. Select a device, and click **Disaster recovery**.
3. Edit the recovery server default parameters.

The recovery server parameters are described in the following table.

Recovery server parameter	Default value	Description
CPU and RAM	auto	The number of virtual CPUs and the amount of RAM for the recovery server. The default settings will be automatically determined based on the original device CPU and RAM configuration.
Cloud network	auto	Cloud network to which the server will be connected. For details on how cloud networks are configured, see Cloud network infrastructure .
IP address in production network	auto	The IP address that the server will have in the production network. By default, the IP address of the original machine is set.
Test IP address	disabled	Test IP address gives you the capability to test a failover in the isolated test network and to connect to the recovery server via RDP or SSH during a test failover. In the test failover mode, the VPN gateway will replace the test IP address with the production IP address by using the NAT protocol. If a test IP address is not specified, the console will be the only way to access the server during a test failover.
Internet Access	enabled	Enable the recovery server to access the Internet during a real or test failover. By default, TCP port 25 is denied for outbound connections.
Use Public address	disabled	Having a public IP address makes the recovery server available from the Internet during a failover or test failover. If you do not use a public IP address, the server will be available only in your production network. To use a public IP address, you must enable internet access. The public IP address will be shown after you complete the

		configuration. By default, TCP port 443 is open for inbound connections.
Set RPO threshold	disabled	RPO threshold defines the maximum allowable time interval between the last recovery point and the current time. The value can be set within 15 – 60 minutes, 1 – 24 hours, 1 – 14 days.

15.4.2 Cloud network infrastructure

The cloud network infrastructure consists of the VPN gateway on the cloud site and the cloud networks to which the recovery servers will be connected.

Note

Applying a disaster recovery protection plan creates recovery cloud network infrastructure only if it does not exist. Existing cloud networks are not changed or recreated.

The system checks devices IP addresses and if there are no existing cloud networks where an IP address fits, it automatically creates suitable cloud networks. If you already have existing cloud networks where the recovery servers IP addresses fit, the existing cloud networks will not be changed or recreated.

- If you do not have existing cloud networks or you setup disaster recovery configuration for the first time, the cloud networks will be created with maximum ranges recommended by IANA for private use (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) based on your devices IP address range. You can narrow your network by editing the network mask.
- If you have devices on multiple local networks, the network on the cloud site may become a superset of the local networks. You may reconfigure networks in the **Connectivity** section. See "Managing networks" (p. 385).
- If you need to set up Site-to-site Open VPN connectivity, download the VPN appliance and set up it. See "Configuring Site-to-site Open VPN" (p. 377). Make sure your cloud networks ranges match your local network ranges connected to the VPN appliance.
- To change the default network configuration, click the **Go to connectivity** link on the Disaster Recovery module of the Protection plan, or navigate to **Disaster Recovery > Connectivity**.

15.5 Setting up connectivity

This section explains the network concepts necessary for you to understand how it all works in Cyber Disaster Recovery Cloud. You will learn how to configure different types of connectivity to the cloud site, depending on your needs. Finally, you will learn how to manage your networks in the cloud and manage the settings of the VPN appliance and VPN gateway.

15.5.1 Networking concepts

Note

Some features might require additional licensing, depending on the applied licensing model.

With Cyber Disaster Recovery Cloud you can define the following connectivity types to the cloud site:

- **Cloud-only mode**

This type of connection does not require a VPN appliance deployment on the local site.

The local and cloud networks are independent networks. This type of connection implies either the failover of all the local site's protected servers or partial failover of independent servers that do not need to communicate with the local site.

Cloud servers on the cloud site are accessible through the point-to-site VPN, and public IP addresses (if assigned).

- **Site-to-site Open VPN connection**

This type of connection requires a VPN appliance deployment on the local site.

The Site-to-site Open VPN connection allows to extend your networks to the cloud and retain the IP addresses.

Your local site is connected to the cloud site by means of a secure VPN tunnel. This type of connection is suitable in case you have tightly dependent servers on the local site, such as a web server and a database server. In case of partial failover, when one of these servers is recreated on the cloud site while the other stays on the local site, they will still be able to communicate with each other via a VPN tunnel.

Cloud servers on the cloud site are accessible through the local network, point-to-site VPN, and public IP addresses (if assigned).

- **Multi-site IPsec VPN connection**

This type of connection requires a local VPN device that supports IPsec IKE v2.

When you start configuring the Multi-site IPsec VPN connection, Disaster Recovery Cloud automatically creates a cloud VPN gateway with a public IP address.

With Multi-site IPsec VPN your local sites are connected to the cloud site by means of a secure IPsec VPN tunnel.

This type of connection is suitable for Disaster Recovery scenarios when you have one or several local sites hosting critical workloads or tightly dependent services.

In case of partial failover of one of the servers, the server is recreated on the cloud site while the others remain on the local site, and they are still able to communicate with each other through an IPsec VPN tunnel.

In case of partial failover of one of the local sites, the rest of the local sites remain operational, and will still be able to communicate with each other through an IPsec VPN tunnel.

- **Point-to-site remote VPN access**

A secure Point-to-site remote VPN access to your cloud and local site workloads from outside by using your endpoint device.

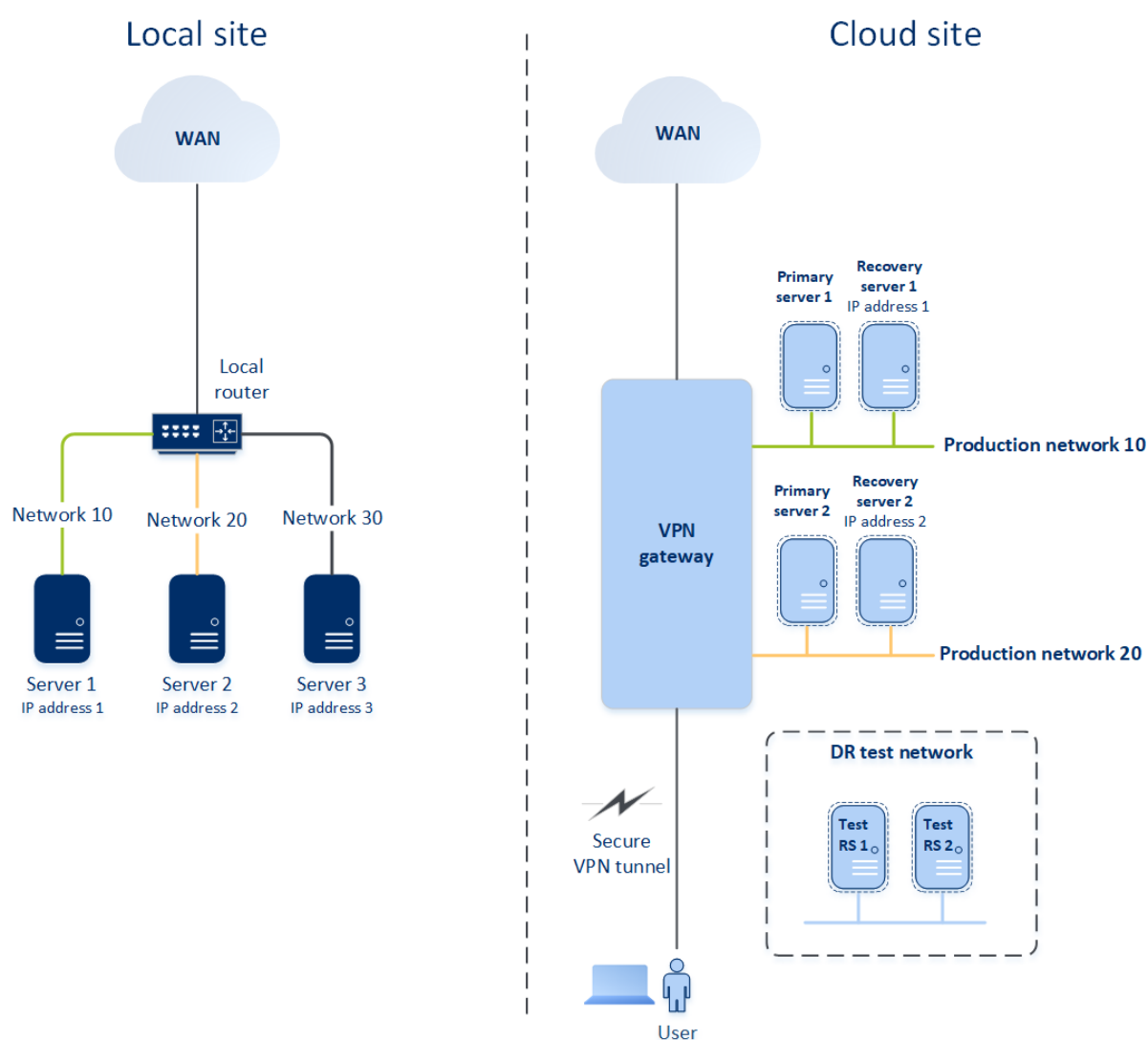
For a local site access, this type of connection requires a VPN appliance deployment on the local site.

Cloud-only mode

The cloud-only mode does not require a VPN appliance deployment on the local site. It implies that you have two independent networks: one on the local site, another on the cloud site. Routing is performed with the router on the cloud site.

How routing works

In case the cloud-only mode is established, routing is performed with the router on the cloud site so that servers from different cloud networks can communicate with each other.



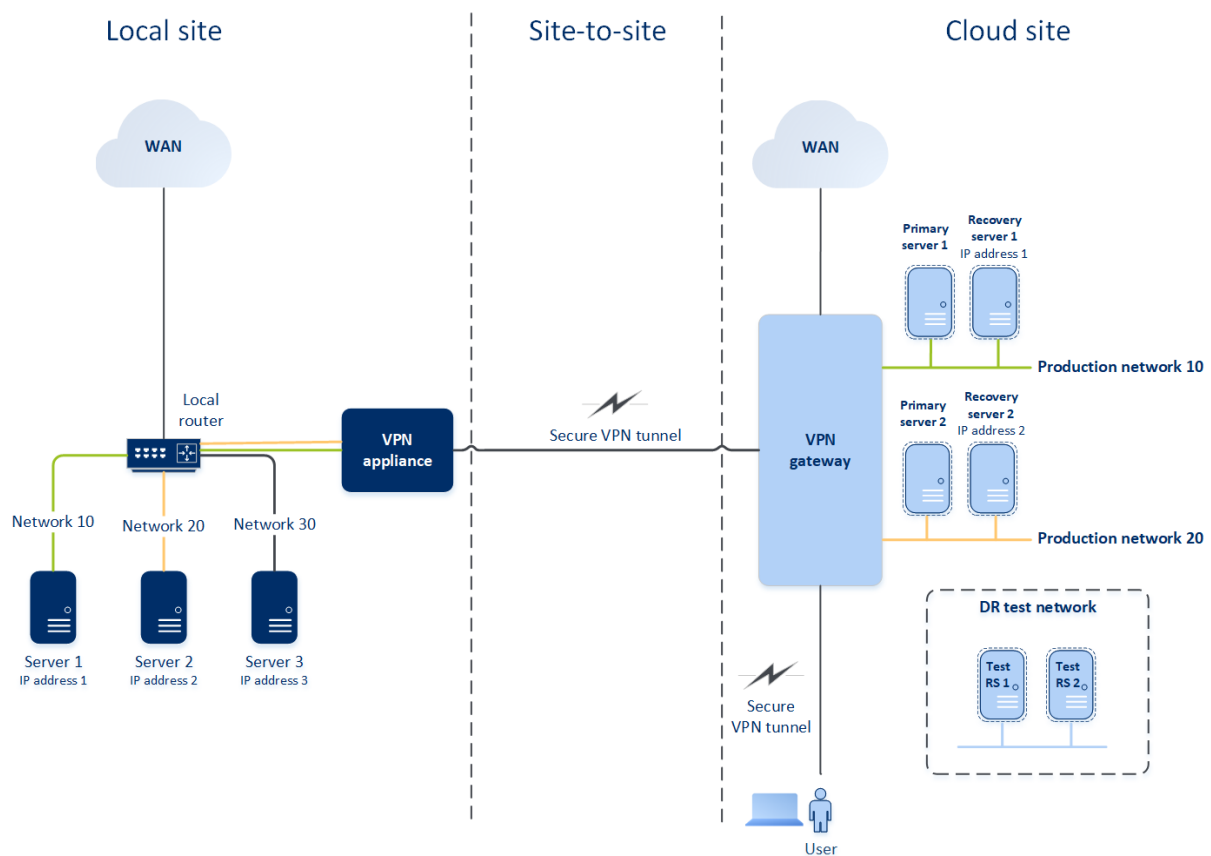
Site-to-site Open VPN connection

Note

The availability of this feature depends on the service quotas that are enabled for your account.

To understand how networking works in Cyber Disaster Recovery Cloud, we will consider a case when you have three networks with one machine each in the local site. You are going to configure the protection from a disaster for the two networks – Network 10 and Network 20.

On the diagram below, you can see the local site where your machines are hosted, and the cloud site where the cloud servers are launched in case of a disaster. With the Cyber Disaster Recovery Cloud solution you can fail over all the workload from the corrupted machines in the local site to the cloud servers in the cloud. You can protect up to five networks with Cyber Disaster Recovery Cloud.



To establish a Site-to-site Open VPN communication between the local and cloud sites, a **VPN appliance** and a **VPN gateway** are used. When you start configuring the Site-to-site Open VPN connection in the service console, the VPN gateway is automatically deployed in the cloud site. Then, you must deploy the VPN appliance on your local site, add the networks to be protected, and register the appliance in the cloud. Cyber Disaster Recovery Cloud creates a replica of your local network in the cloud. A secure VPN tunnel is established between the VPN appliance and the VPN gateway. It provides your local network extension to the cloud. The production networks in the cloud are bridged with your local networks. The local and cloud servers can communicate through

this VPN tunnel as if they are all in the same Ethernet segment. Routing is performed with your local router.

For each source machine to be protected, you must create a recovery server on the cloud site. It stays in the **Standby** state until a failover event happens. If a disaster happens and you start a failover process (in the **production mode**), the recovery server representing the exact copy of your protected machine is launched in the cloud. It may be assigned the same IP address as the source machine and it can be launched in the same Ethernet segment. Your clients can continue working with the server, without noticing any background changes.

You can also start a failover process in the **test mode**. This means that the source machine is still working and at the same time the respective recovery server with the same IP address is launched in the cloud. To prevent IP address conflicts, a special virtual network is created in the cloud – **test network**. The test network is isolated to prevent duplication of the source machine IP address in one Ethernet segment. To access the recovery server in the test failover mode, when you create a recovery server, you must assign a **Test IP address** to it. There are other parameters for the recovery server that can be specified, they will be considered in the respective sections below.

How routing works

When a Site-to-site connection is established, routing between cloud networks is performed with your local router. The VPN server does not perform routing between cloud servers located in different cloud networks. If a cloud server from one network wants to communicate to a server from another cloud network, the traffic goes through the VPN tunnel to the local router on the local site, then the local router routes it to another network, and it goes back through the tunnel to the destination server on the cloud site.

VPN gateway

The major component that allows communication between the local and cloud sites is the **VPN gateway**. It is a virtual machine in the cloud on which special software is installed, and network is specifically configured. The VPN gateway has the following functions:

- Connects the Ethernet segments of your local network and production network in the cloud in the L2 mode.
- Provides iptables and ebtables rules.
- Works as a default router and NAT for the machines in the test and production networks.
- Works as a DHCP server. All machines in the production and test networks get the network configuration (IP addresses, DNS settings) via DHCP. Every time a cloud server will get the same IP address from the DHCP server. If you need to set up the custom DNS configuration, you should contact the support team.
- Works as a caching DNS.

VPN gateway network configuration

The VPN gateway has several network interfaces:

- External interface, connected to the Internet
- Production interfaces, connected to the production networks
- Test interface, connected to the test network

In addition, two virtual interfaces are added for Point-to-site and Site-to-site connections.

When the VPN gateway is deployed and initialized, the bridges are created – one for the external interface, and one for the client and production interfaces. Though the client-production bridge and the test interface use the same IP addresses, the VPN gateway can route packages correctly by using a specific technique.

VPN appliance

The **VPN appliance** is a virtual machine on the local site with Linux that has special software installed, and a special network configuration. It allows communication between the local and cloud sites.

Recovery servers

A **recovery server** – a replica of the original machine based on the protected server backups stored in the cloud. Recovery servers are used for switching workloads from the original servers in case of a disaster.

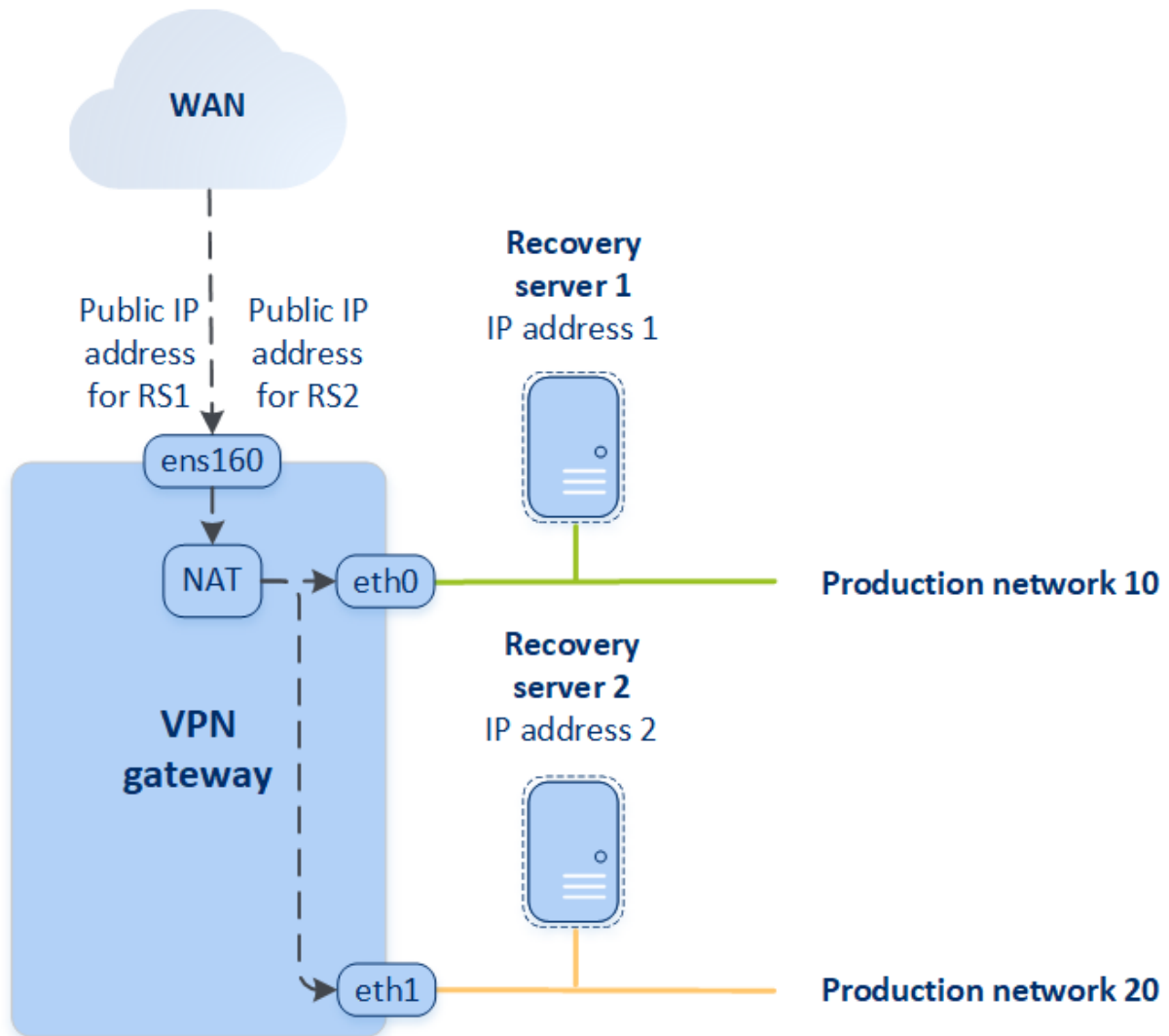
When creating a recovery server, you must specify the following network parameters:

- **Cloud network** (required): a cloud network to which a recovery server will be connected.
- **IP address in production network** (required): an IP address with which a virtual machine for a recovery server will be launched. This address is used in both the production and test networks. Before launching, the virtual machine is configured for getting the IP address via DHCP.
- **Test IP address** (optional): an IP address to access a recovery server from the client-production network during the test failover, to prevent the production IP address from being duplicated in the same network. This IP address is different from the IP address in the production network. Servers in the local site can reach the recovery server during the test failover via the test IP address, while access in the reverse direction is not available. Internet access from the recovery server in the test network is available if the **Internet access** option was selected during the recovery server creation.
- **Public IP address** (optional): an IP address to access a recovery server from the Internet. If a server has no public IP address, it can be reached only from the local network.
- **Internet access** (optional): it allows a recovery server to access the Internet (in both the production and test failover cases).

Public and test IP address

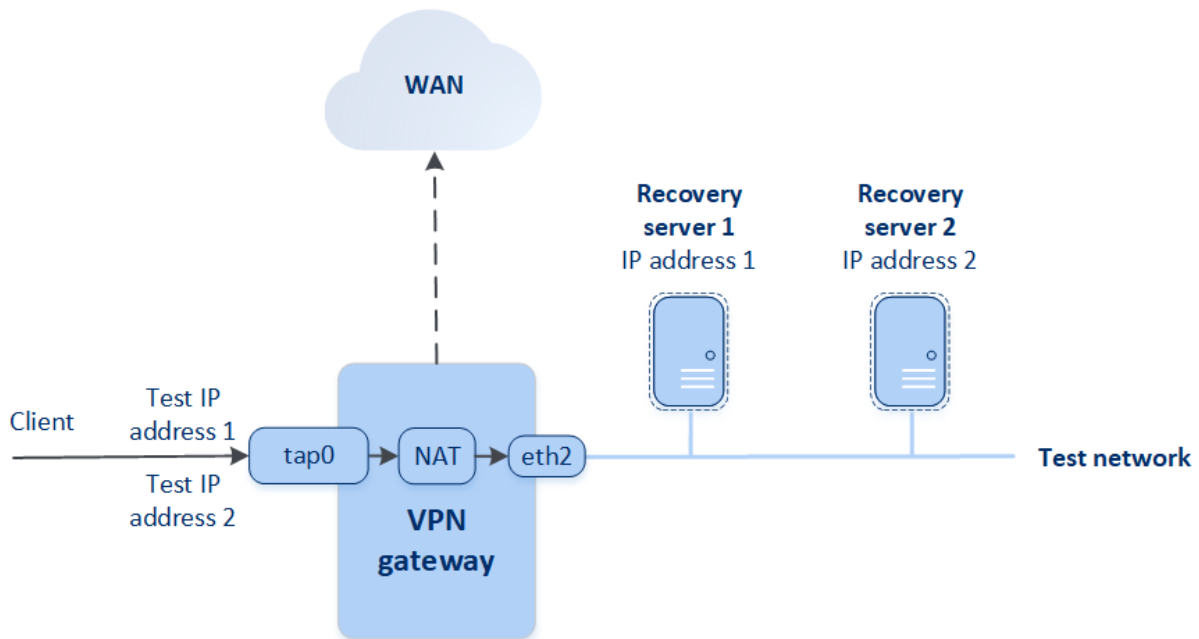
If you assign the public IP address when creating a recovery server, the recovery server becomes available from the Internet through this IP address. When a packet comes from the Internet with the destination public IP address, the VPN gateway remaps it to the respective production IP address by using NAT, and then sends it to the corresponding recovery server.

Cloud site



If you assign the test IP address when creating a recovery server, the recovery server becomes available in the test network through this IP address. When you perform the test failover, the original machine is still running while the recovery server with the same IP address is launched in the test network in the cloud. There is no IP address conflict as the test network is isolated. The recovery servers in the test network are reachable by their test IP addresses, which are remapped to the production IP addresses through NAT.

Cloud site



Primary servers

A **primary server** – a virtual machine that does not have a linked machine on the local site if compared to a recovery server. Primary servers are used for protecting an application by replication, or running various auxiliary services (such as a web server).

Typically, a primary server is used for real-time data replication across servers running crucial applications. You set up the replication by yourself, using the application's native tools. For example, Active Directory replication, or SQL replication, can be configured among the local servers and the primary server.

Alternatively, a primary server can be included in an AlwaysOn Availability Group (AAG) or Database Availability Group (DAG).

Both methods require a deep knowledge of the application and the administrator rights. A primary server constantly consumes computing resources and space on the fast disaster recovery storage. It needs maintenance on your side: monitoring the replication, installing software updates, and backing up. The benefits are the minimal RPO and RTO with a minimal load on the production environment (as compared to backing up entire servers to the cloud).

Primary servers are always launched only in the production network and have the following network parameters:

- **Cloud network** (required): a cloud network to which a primary server will be connected.
- **IP address in production network** (required): an IP address that the primary server will have in the production network. By default, the first free IP address from your production network is set.

- **Public IP address** (optional): an IP address to access a primary server from the Internet. If a server has no public IP address, it can be reached only from the local network, not through the Internet.
- **Internet access** (optional): allows a primary server to access the Internet.

Multi-site IPsec VPN connection

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can use the Multi-site IPsec VPN connectivity to connect a single local site, or multiple local sites to the Disaster Recovery Cloud through a secure L3 IPsec VPN connection.

This connectivity type is useful for Disaster Recovery scenarios if you have one of the following use cases:

- you have one local site hosting critical workloads.
- you have multiple local sites hosting critical workloads, for example offices in different locations.
- you use third-party software sites, or managed service providers sites and are connected to them through an IPsec VPN tunnel.

To establish a Multi-site IPsec VPN communication between the local sites and the cloud site, a **VPN gateway** is used. When you start configuring the Multi-site IPsec VPN connection in the service console, the VPN gateway is automatically deployed in the cloud site. You should configure the cloud network segments and make sure that they do not overlap with the local network segments. A secure VPN tunnel is established between local sites and the cloud site. The local and cloud servers can communicate through this VPN tunnel as if they are all in the same Ethernet segment.

For each source machine to be protected, you must create a recovery server on the cloud site. It stays in the **Standby** state until a failover event happens. If a disaster happens and you start a failover process (in the **production mode**), the recovery server representing the exact copy of your protected machine is launched in the cloud. Your clients can continue working with the server, without noticing any background changes.

You can also launch a failover process in the **test mode**. This means that the source machine is still working and at the same time the respective recovery server is launched in the cloud in a special virtual network that is created in the cloud – **test network**. The test network is isolated to prevent duplication of IP addresses in the other cloud network segments.

VPN gateway

The major component that allows communication between the local sites and the cloud site is the **VPN gateway**. It is a virtual machine in the cloud on which the special software is installed, and the network is specifically configured. The VPN gateway serves the following functions:

- Connects the Ethernet segments of your local network and production network in the cloud in the L3 IPsec mode.

- Works as a default router and NAT for the machines in the test and production networks.
- Works as a DHCP server. All machines in the production and test networks get the network configuration (IP addresses, DNS settings) via DHCP. Every time a cloud server will get the same IP address from the DHCP server.

If you prefer, you can set up a custom DNS configuration. For more information, see "Configuring custom DNS servers" (p. 392).

- Works as a caching DNS.

How routing works

Routing between the cloud networks is performed with the router on the cloud site so that servers from different cloud networks can communicate with each other.

Point-to-site remote VPN access

Note

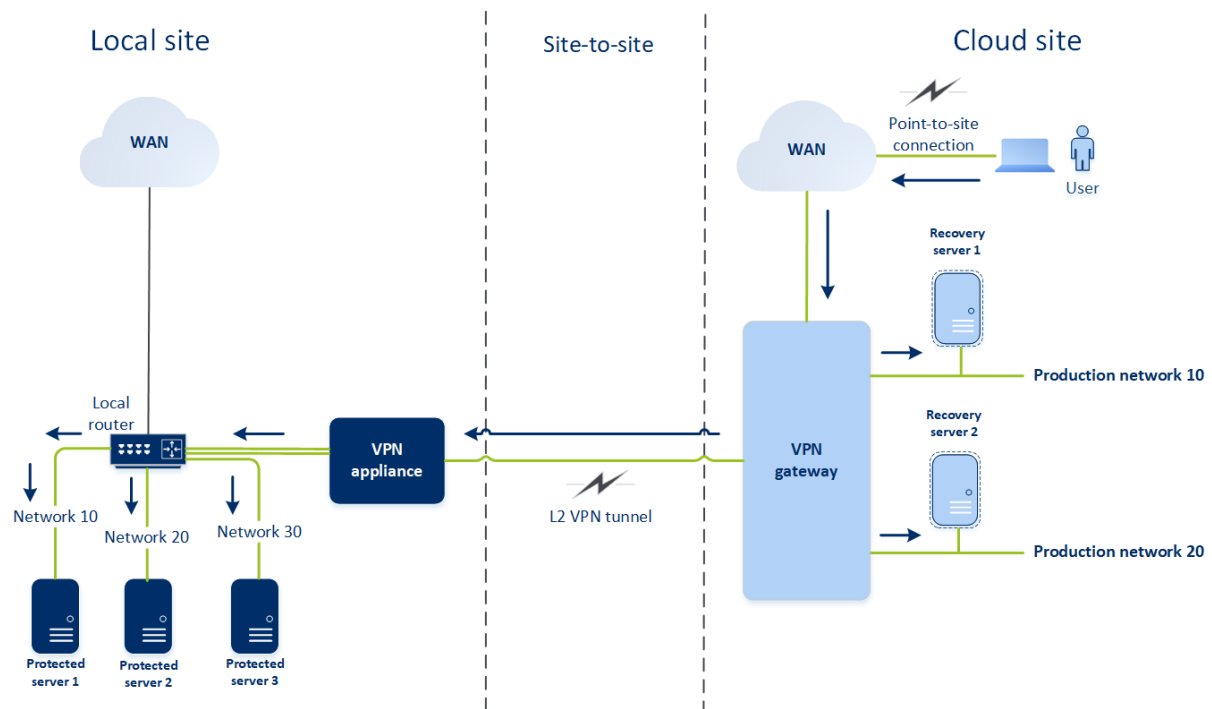
The availability of this feature depends on the service quotas that are enabled for your account.

The Point-to-site connection is a secure connection from the outside by using your endpoint devices (such as computer or laptop) to the cloud and local sites through a VPN. It is available after you establish a Site-to-site Open VPN connection to the Cyber Disaster Recovery Cloud site. This type of connection is useful in the following cases:

- In many companies, the corporate services and web resources are available only from the corporate network. You can use the Point-to-site connection to securely connect to the local site.
- In case of a disaster, when a workload is switched to the cloud site and your local network is down, you may need direct access to your cloud servers. This is possible through the Point-to-site connection to the cloud site.

For the Point-to-site connection to the local site, you need to install the VPN appliance on the local site, configure the Site-to-site connection, and then the Point-to-site connection to the local site. Thus, your remote employees will have access to the corporate network through L2 VPN.

The scheme below shows the local site, cloud site, and communications between servers highlighted in green. The L2 VPN tunnel connects your local and cloud sites. When a user establishes a Point-to-site connection, the communications to the local site are performed through the cloud site.



The Point-to-site configuration uses certificates to authenticate to the VPN client. Additionally user credentials are used for authentication. Note the following about the Point-to-site connection to the local site:

- Users should use their Cyber Cloud credentials to authenticate in the VPN client. They must have either a "Company Administrator" or a "Cyber Protection" user role.
- If you [re-generated the OpenVPN configuration](#), you need to provide the updated configuration to all of the users using the Point-to-site connection to the cloud site.

Automatic deletion of unused customer environments on the cloud site

The Disaster Recovery service tracks the usage of the customer environments created for disaster recovery purposes and automatically deletes them if they are unused.

The following criteria are used to define if the customer tenant is active:

- Currently, there is at least one cloud server or there were cloud server(s) in the last seven days.
OR
- The **VPN access to local site** option is enabled and either the Site-to-site Open VPN tunnel is established or there are data reported from the VPN appliance for the last 7 days.

All the rest of the tenants are considered as inactive tenants. For such tenants the system performs the following:

- Deletes the VPN gateway and all cloud resources related to the tenant.
- Unregisters the VPN appliance.

The inactive tenants are rolled back to their state before the connectivity was configured.

15.5.2 Initial connectivity configuration

This section describes connectivity configuration scenarios.

Configuring Cloud-only mode

To configure a connection in the cloud-only mode

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Select **Cloud-only** and click **Configure**.
As a result, the VPN gateway and cloud network with the defined address and mask are deployed on the cloud site.

To learn how to manage your networks in the cloud and set up the VPN gateway settings, refer to "[Managing cloud networks](#)".

Configuring Site-to-site Open VPN

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Requirements for the VPN appliance

System requirements

- 1 CPU
- 1 GB RAM
- 8 GB disk space

Ports

- TCP 443 (outbound) – for VPN connection
- TCP 80 (outbound) – for automatic [update of the appliance](#)

Ensure that your firewalls and other components of your network security system allow connections through these ports to any IP address.

Configuring a Site-to-site Open VPN connection

The VPN appliance extends your local network to the cloud through a secure VPN tunnel. This kind of connection is often referred to as a "Site-to-site" (S2S) connection. You can follow the procedure below or watch the [video tutorial](#).

To configure a connection through the VPN appliance

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Select **Site-to-site Open VPN connection**, and click **Configure**.

The system starts deploying the VPN gateway in the cloud. This will take some time. Meanwhile, you can proceed to the next step.

Note

The VPN gateway is provided without additional charge. It will be deleted if the Disaster Recovery functionality is not used, i.e. no primary or recovery server is present in the cloud for seven days.

3. In the **VPN appliance** block, click **Download and deploy**. Depending on the virtualization platform you are using, download the VPN appliance for VMware vSphere or Microsoft Hyper-V.
4. Deploy the appliance and connect it to the production networks.

In vSphere, ensure that **Promiscuous mode** and **Forged transmits** are enabled and set to **Accept** for all virtual switches that connect the VPN appliance to the production networks. To access these settings, in vSphere Client, select the host > **Summary** > **Network**, and then select the switch > **Edit settings...** > **Security**.

In Hyper-V, create a **Generation 1** virtual machine with 1024 MB of memory. We also recommend enabling **Dynamic Memory** for the machine. Once the machine is created, go to **Settings** > **Hardware** > **Network Adapter** > **Advanced Features** and select the **Enable MAC address spoofing** check box.

5. Power on the appliance.
6. Open the appliance console and log in with the "admin"/"admin" user name and password.
7. [Optional] Change the password.
8. [Optional] Change the network settings if needed. Define which interface will be used as the WAN for Internet connection.
9. Register the appliance in the Cyber Protection service by using the credentials of the company administrator.

These credentials are only used once to retrieve the certificate. The data center URL is predefined.

Note

If two-factor authentication is configured for your account, you will also be prompted to enter the TOTP code. If two-factor authentication is enabled but not configured for your account, you cannot register the VPN appliance. First, you must go to the service console login page and complete the two-factor authentication configuration for your account. For more details on two-factor authentication, go to the Management Portal Administrator's Guide.

Once the configuration is complete, the appliance will have the **Online** status. The appliance connects to the VPN gateway and starts to report information about networks from all active interfaces to the Cyber Disaster Recovery Cloud service. The service console shows the interfaces, based on the information from the VPN appliance.

Configuring Multi-site IPsec VPN

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can configure a Multi-site IPsec VPN connection in the following two ways:

- from the **Disaster Recovery > Connectivity** tab.
- by applying a protection plan on one or several devices, and then manually switching from the automatically created Site-to-site Open VPN connection to a Multi-site IPsec VPN connection, configuring the Multi-site IPsec VPN settings, and reassigning IP addresses.

To configure a Multi-site IPsec VPN connection from the Connectivity tab

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. In the **Multi-site VPN connection** section, click **Configure**.
A VPN gateway is deployed on the cloud site.
3. [Configure the Multi-site IPsec VPN settings](#).

To configure a Multi-site IPsec VPN connection from a protection plan

1. In the service console, go to **Devices**.
2. Apply a protection plan to one or multiple devices from the list.
The recovery server and the cloud infrastructure settings are automatically configured for Site-to-site Open VPN connectivity.
3. Go to **Disaster Recovery > Connectivity**.
4. Click **Show properties**.
5. Click **Switch to Multi-site IPsec VPN**.
6. [Configure the Multi-site IPsec VPN settings](#).
7. [Reassign the IP addresses](#) of the cloud network and cloud servers.

Configuring the Multi-site IPsec VPN settings

Note

The availability of this feature depends on the service quotas that are enabled for your account.

After you configure a Multi-site IPsec VPN, you must configure the cloud site and the local sites settings on the **Disaster Recovery > Connectivity** tab.

15.5.3 Prerequisites

- A configured Multi-site IPsec VPN connectivity. For more information about configuring the Multi-site IPsec VPN connectivity, see "Configuring Multi-site IPsec VPN" (p. 379).
- Public IP address of each the local IPsec VPN gateway.

- Plan your cloud network to have enough IP addresses for the cloud servers that are copies of your protected machines (in the production network), and for the recovery servers (with one or two IP addresses, depending on your needs).
- If you use firewall between the local sites and the cloud site, you must allow the following IP protocols and UDP ports on the local sites: IP Protocol ID 50 (ESP), UDP Port 500 (IKE), and UDP Port 4500.

To configure a Multi-site IPsec VPN connection

1. Add one or more networks to the cloud site.

- a. Click **Add Network**.

Note

When you add a cloud network, a corresponding test network is added automatically with the same network address and mask for performing test failovers. The cloud servers in the test network have the same IP addresses as the ones in the cloud production network. If you need to access a cloud server from the production network during a test failover, when you create a recovery server, assign it a second test IP address.

- b. In the **Network address** field, type the IP address of the network.
 - c. In the **Network mask** field, type the mask of the network.
 - d. Click **Add**.
- #### 2. Configure the settings for each local site that you want to connect to the cloud site, following the recommendations for the local sites. For more information about these recommendations, see "General recommendations for local sites" (p. 381).
- a. Click **Add Connection**.
 - b. Enter a name for the of the local VPN gateway.
 - c. Enter the public IP address of the local VPN gateway.
 - d. [Optional] Enter a description of the local VPN gateway.
 - e. Click **Next**.
 - f. In the **Pre-shared key** field, type the pre-shared key, or click **Generate a new pre-shared key** to use an automatically generated value.

Note

You must use the same pre-shared key for the local and the cloud VPN gateways.

- g. Click **IPsec/IKE security settings** to configure the settings. For more information about the settings that you can configure, see "IPsec/IKE security settings" (p. 381).

Note

You can use the default settings, which are populated automatically, or use custom values. Only IKEv2 protocol connections are supported. The default **Startup action** when establishing the VPN is **Add** (your local VPN gateway initiates the connection), but you can change it to **Start** (the cloud VPN gateway initiates the connection) or **Route** (suitable for firewalls that support the route options).

h. Configure the **Network policies**.

The network policies specify the networks to which the IPsec VPN connects. Type the IP address and mask of the network using the CIDR format. The local and cloud network segments should not overlap.

i. Click **Save**.

General recommendations for local sites

Note

The availability of this feature depends on the service quotas that are enabled for your account.

When you configure the local sites for your Multi-site IPsec VPN connectivity, consider the following recommendations:

- For each IKE Phase, set at least one of the values that are configured in the cloud site for the following parameters: Encryption algorithm, Hash algorithm, and Diffie-Hellman group numbers.
- Enable Perfect forward secrecy with at least one of the values for Diffie-Hellman group numbers that is configured in the cloud site for IKE Phase 2.
- Configure the same value for the **Lifetime** for IKE Phase 1 and IKE Phase 2 as in the cloud site.
- Note that the **Startup action** configuration defines which side initiates the connection. The default value **Add** means that the local site initiates the connection, and cloud site is waiting for the connection initiation. Change the value to **Start** if you want the cloud site to initiate the connection, or to **Route** if you want both sides to be able to initiate the connection (suitable for firewalls that support the route option).

For more information and configuration examples for different solutions, see:

- The series of knowledge based articles: <https://kb.acronis.com/disaster-recovery-ipsec-vpn>.
- The video example: <https://go.acronis.com/ipsec>.

IPsec/IKE security settings

Note

The availability of this feature depends on the service quotas that are enabled for your account.

The following table provides more information about the Psec/IKE security parameters.

Parameter	Description
Encryption algorithm	The encryption algorithm that will be used to ensure that data is not viewable while in transit. By default, all algorithms are selected. You must configure at least one of the selected algorithms on your local gateway device for each IKE phase.
Hash algorithm	The hash algorithm that will be used to verify the data integrity and authenticity. By default, all algorithms are selected. You must configure at least one of the selected algorithms on your local gateway device for each IKE phase.
Diffie-Hellman group numbers	<p>The Diffie-Hellman group numbers define the strength of the key that is used in the Internet Key Exchange (IKE) process.</p> <p>Higher group numbers are more secure but require additional time for the key to compute.</p> <p>By default, all groups are selected. You must configure at least one of the selected groups on your local gateway device for each IKE phase.</p>
Lifetime (seconds)	<p>The lifetime value determines the duration of a connection instance with a set of encryption/authentication keys for user packets, from successful negotiation to expiry.</p> <p>Range for Phase 1: 900-28800 seconds with default 28800.</p> <p>Range for Phase 2: 900-3600 seconds with default 3600.</p> <p>The lifetime for Phase 2 must be less than the lifetime for Phase 1.</p> <p>The connection is re-negotiated through the keying channel before it expires, see Rekey margin time. If the local and the remote side do not agree on the lifetime, a clutter of superseded connections will occur on the side with the longer lifetime. See also Rekey margin time and Rekey fuzz.</p>
Rekey margin time (seconds)	The margin time before connection expiration or keying-channel expiration, during which the local side of the VPN connection attempts to negotiate a replacement. The exact time of the rekey is randomly selected based on the value of Rekey fuzz . Relevant only locally, the remote side does

Parameter	Description
	not need to agree on it. Range: 900-3600 seconds. The default value is 3600.
Replay window size (packet)	<p>The IPsec replay window size for this connection.</p> <p>The default -1 uses the value configured with charon.replay_window in the strongswan.conf file.</p> <p>Values larger than 32 are supported only when using the Netlink backend.</p> <p>A value of 0 disables the IPsec replay protection.</p>
Rekey fuzz (%)	<p>The maximum percentage by which marginbytes, marginpackets and margintime are randomly increased to randomize rekeying intervals (important for hosts with many connections).</p> <p>The Rekey fuzz value can exceed 100%. The value of marginTYPE, after the random increase, must not exceed lifeTYPE, where TYPE is one of bytes, packets or time.</p> <p>The value 0% disables randomization. Relevant only locally, the remote side does not need to agree on it.</p>
DPD timeout (seconds)	Time after which a dead peer detection (DPD) timeout occurs. You can specify value 30 or higher. The default value is 30.
Dead peer detection (DPD) timeout action	<p>The action to take after a dead peer detection (DPD) timeout occurs.</p> <p>Restart - Restart the session when DPD timeout occurs.</p> <p>Clear - End the session when DPD timeout occurs.</p> <p>None - Take no action when DPD timeout occurs.</p>
Startup action	<p>Determines which side initiates the connection and establishes the tunnel for the VPN connection.</p> <p>Add - your local VPN gateway initiates the connection.</p> <p>Start - the cloud VPN gateway initiates the connection.</p> <p>Route - suitable for VPN gateways that support the route option. The tunnel is up only when there is traffic initiated from either the local VPN gateway,</p>

Parameter	Description
	or the cloud VPN gateway.

Recommendations for the Active Directory Domain Services availability

If your protected workloads need to authenticate in a domain controller, we recommend that you have an Active Directory Domain Controller (AD DC) instance at the Disaster Recovery site.

Active Directory Domain Controller for L2 Open VPN connectivity

With the L2 Open VPN connectivity, the IP addresses of the protected workloads are retained in the cloud site during a test failover or a production failover. Therefore, the AD DC during a test failover or a production failover has the same IP address as in the local site.

With custom DNS you can set your own custom DNS server for all cloud servers. For more information, see "Configuring custom DNS servers" (p. 392).

Active Directory Domain Controller for L3 IPsec VPN connectivity

With L3 IPsec VPN connectivity, the IP addresses of the protected workloads are not retained in the cloud site. Therefore, we recommend that you have an additional dedicated AD DC instance as a primary server in the cloud site before you perform a production failover.

The recommendations for a dedicated AD DC instance that is configured as a primary server in the cloud site are the following:

- Turn off Windows firewall.
- Join the primary server to the Active Directory service.
- Ensure that the primary server has Internet access.
- Add the Active Directory feature.
- Add the cloud domain controller as a read-only domain controller.

With custom DNS you can set your own custom DNS server for all cloud servers. For more information, see "Configuring custom DNS servers" (p. 392).

Configuring Point-to-site remote VPN access

Note

The availability of this feature depends on the service quotas that are enabled for your account.

If you need to connect to your local site remotely, you can configure the Point-to-site connection to the local site. You can follow the procedure below or watch the [video tutorial](#).

Prerequisites

- A Site-to-site Open VPN connectivity is configured.
- The VPN appliance is installed on the local site.

To configure the Point-to-site connection to the local site

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Click **Show properties**.
3. Enable the **VPN access to local site** option.
4. Ensure that your user who needs to establish the Point-to-site connection to the local site has:
 - a user account in Cyber Cloud. These credentials are used for authentication in the VPN client. Otherwise, [create a user account in Cyber Cloud](#).
 - a "Company Administrator" or "Cyber Protection" user role.
5. Configure the OpenVPN client:
 - a. Download the OpenVPN client version 2.4.0 or later from the following location <https://openvpn.net/community-downloads/>.
 - b. Install the OpenVPN client on the machine from which you want to connect to the local site.
 - c. Click **Download configuration for OpenVPN**. The configuration file is valid for users in your organization with the "Company Administrator" or "Cyber Protection" user role.
 - d. Import the downloaded configuration to OpenVPN.
 - e. Log in to the OpenVPN client with your Cyber Cloud user credentials (see step 4 above).
 - f. [Optional] If two-factor authentication is enabled for your organization, then you should provide the [one-time generated TOTP code](#).

Important

If you enabled two-factor authentication for your account, you need to re-generate the configuration file and renew it for your existing OpenVPN clients. Users must re-log in to Cyber Cloud to set up two-factor authentication for their accounts.

As a result, your user will be able to connect to machines on the local site.

15.5.4 Network management

This section describes network management scenarios.

Managing networks

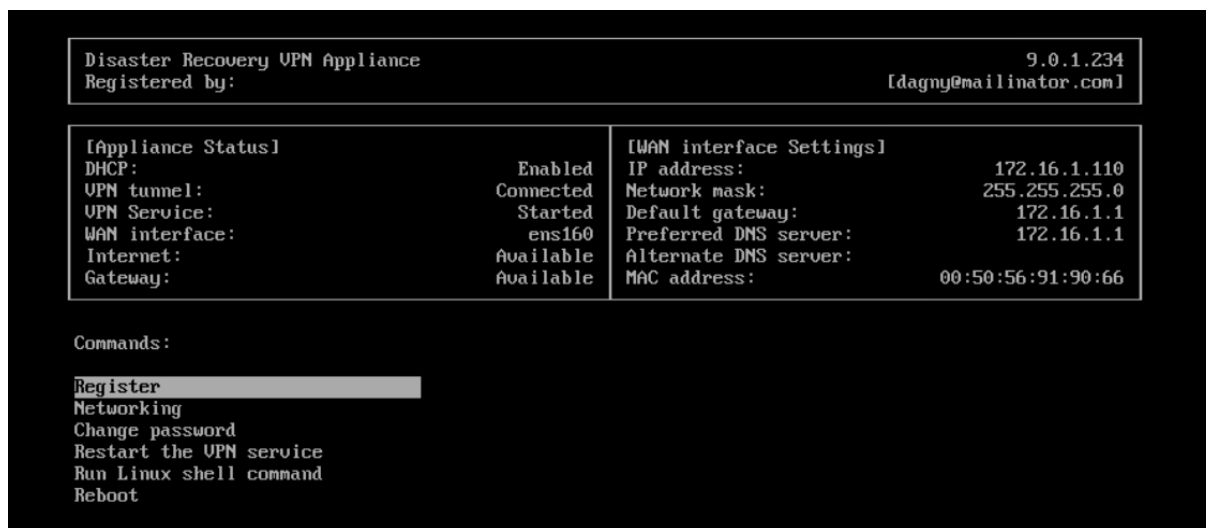
Note

Some features might require additional licensing, depending on the applied licensing model.

Site-to-site Open VPN connection

To add a network on the local site and extend it to the cloud

1. On the VPN appliance, set up the new network interface with the local network that you want to extend in the cloud.
2. Log in to the VPN appliance console.
3. In the **Networking** section, set up network settings for the new interface.



The VPN appliance starts to report information about networks from all active interfaces to Cyber Disaster Recovery Cloud. The service console shows the interfaces based on the information from the VPN appliance.

To delete a network extended to the cloud

1. Log in to the VPN appliance console.
2. In the **Networking** section, select the interface that you want to delete, and then click **Clear network settings**.
3. Confirm the operation.

As a result, the local network extension to the cloud via a secure VPN tunnel will be stopped. This network will operate as an independent cloud segment. If this interface is used to pass the traffic from (to) the cloud site, all of your network connections from (to) the cloud site will be disconnected.

To change the network parameters

1. Log in to the VPN appliance console.
2. In the **Networking** section, select the interface that you want to edit.
3. Click **Edit network settings**.
4. Select one of the two possible options:
 - For automatic network configuration via DHCP, click **Use DHCP**. Confirm the operation.
 - For manual network configuration, click **Set static IP address**. The following settings are available for editing:
 - **IP address**: the IP address of the interface in the local network.
 - **VPN gateway IP address**: the special IP address which is reserved for the cloud segment of network for the proper Cyber Disaster Recovery Cloud service work.
 - **Network mask**: network mask of the local network.
 - **Default gateway**: default gateway on the local site.
 - **Preferred DNS server**: primary DNS server on the local site.
 - **Alternate DNS server**: secondary DNS server on the local site.

```
Disaster Recovery VPN Appliance
Registered by:
9.0.1.234
[ldagny@mailinator.com]

Command: Networking \ configure ens160

Usage:
<Up>, <Down> - to select parameter
<Esc> - to cancel the command

IP address:
VPN gateway IP address:
Network mask:
Default gateway:
Preferred DNS server:
Alternate DNS server:
```

- Make the necessary changes and confirm them by pressing Enter.

Cloud-only mode

You can have up to five networks in the cloud.

To add a new cloud network

1. Go to **Disaster Recovery > Connectivity**.
2. On **Cloud site**, click **Add cloud network**.
3. Define the cloud network parameters: the network address and mask. When ready, click **Done**.

As a result, the additional cloud network with the defined address and mask will be created on the cloud site.

To delete a cloud network

Note

You cannot delete a cloud network if there is at least one cloud server in it. First, delete the cloud server, and then delete the network.

1. Go to **Disaster Recovery > Connectivity**.
2. On **Cloud site**, click the network address that you want to delete.
3. Click **Delete** and confirm the operation.

To change cloud network parameters

1. Go to **Disaster Recovery > Connectivity**.
2. On **Cloud site**, click the network address that you want to edit.
3. Click **Edit**.
4. Define the network address and mask, and click **Done**.

IP address reconfiguration

For proper disaster recovery performance, the IP addresses assigned to the local and cloud servers must be consistent. If there is any inconsistency or mismatch in IP addresses, you will see the exclamation mark next to the corresponding network in **Disaster Recovery > Connectivity**.

Some of the commonly known reasons of IP address inconsistency are listed below:

1. A recovery server was migrated from one network to another or the network mask of the cloud network was changed. As a result, cloud servers have the IP addresses from networks to which they are not connected.
2. The connectivity type was switched from one without Site-to-site connection to a Site-to-site connection. As a result, a local server is placed in the network different from the one that was created for the recovery server on the cloud site.
3. The connectivity type was switched from Site-to-site Open VPN to Multi-site IPsec VPN, or from Multi-site IPsec VPN to Site-to-site Open VPN. For more information about this scenario, see [Switching connections](#) and [Reassigning IP addresses](#).
4. Editing the following network parameters on the VPN appliance site:
 - Adding an interface via the network settings
 - Editing the network mask manually via the interface settings
 - Editing the network mask via DHCP
 - Editing the network address and mask manually via the interface settings
 - Editing the network mask and address via DHCP

As a result of the actions listed above, the network on the cloud site may become a subset or superset of the local network, or the VPN appliance interface may report the same network settings for different interfaces.

To resolve the issue with network settings

1. Click the network that requires IP address reconfiguration.
You will see a list of servers in the selected network, their status, and IP addresses. The servers whose network settings are inconsistent are marked with the exclamation mark.
2. To change network settings for a server, click **Go to server**. To change network settings for all servers at once, click **Change** in the notification block.
3. Change the IP addresses as needed by defining them in the **New IP** and **New test IP** fields.
4. When ready, click **Confirm**.

Move servers to a suitable network

When you create a disaster recovery protection plan and apply it on selected devices, the system checks devices IP addresses and automatically creates cloud networks if there are not existing cloud networks where IP address fits. By default, the cloud networks are configured with maximum ranges recommended by IANA for private use (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). You can narrow your network by editing the network mask.

In case if the selected devices was on the multiple local networks, the network on the cloud site may become a superset of the local networks. In this case, to reconfigure cloud networks:

1. Click the cloud network that requires network size reconfiguration and then click **Edit**.
2. Reconfigure the network size with the correct settings.
3. Create other required networks.
4. Click the notification icon next to the number of devices connected to the network.

5. Click **Move to a suitable network**.
6. Select the servers that you want to move to suitable networks and then click **Move**.

Managing the VPN appliance settings

Note

The availability of this feature depends on the service quotas that are enabled for your account.

In the service console (**Disaster Recovery > Connectivity**), you can:

- Download log files.
- Unregister the appliance (if you need to reset the VPN appliance settings or switch to the cloud-only mode).

To access these settings, click the **i** icon in the **VPN appliance** block.

In the VPN appliance console, you can:

- Change the password for the appliance.
- View/change the network settings and define which interface to use as the WAN for the Internet connection.
- Register/change the registration account (by repeating the registration).
- Restart the VPN service.
- Reboot the VPN appliance.
- Run the Linux shell command (only for advanced troubleshooting cases).

Enabling and disabling the Site-to-site connection

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can enable the Site-to-site connection in the following cases:

- If you need the cloud servers on the cloud site to communicate with servers on the local site.
- After a failover to the cloud, the local infrastructure is recovered, and you want to fail back your servers to the local site.

To enable the site-to-site connection

1. Go to **Disaster Recovery > Connectivity**.
2. Click **Show properties**, and then enable the **Site-to-site connection** option.

As a result, the site-to-site VPN connection is enabled between the local and cloud sites. The Cyber Disaster Recovery Cloud service gets the network settings from the VPN appliance and extends the local networks to the cloud site.

If you do not need cloud servers on the cloud site to communicate with servers on the local site, you can disable the Site-to-site connection.

To disable the site-to-site connection

1. Go to **Disaster Recovery > Connectivity**.
2. Click **Show properties**, and then disable the **Site-to-site connection** option.

As a result, the local site is disconnected from the cloud site.

Switching the Site-to-site connection type

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can easily switch from a Site-to-site Open VPN connection to a Multi-site IPsec VPN connection, and from a Multi-site IPsec VPN connection to a Site-to-site Open VPN connection.

When you switch the connectivity type, the active VPN connections are deleted, but the cloud servers and network configurations are preserved. However, you will still need to reassign the IP addresses of the cloud networks and servers.

The following table compares the basic characteristics of the Site-to-site Open VPN connection and the Multi-site IPsec VPN connection.

	Site-to-site Open VPN	Multi-site IPsec VPN
Local site support	Single	Single, Multiple
VPN Gateway mode	L2 Open VPN	L3 IPsec VPN
Network segments	Extends the local network to the cloud network	Local networks and cloud network segments should not overlap
Supports Point-to-Site access to local site	Yes	No
Supports Point-to-Site access to cloud site	Yes	Yes
Requires a public IP offering item	No	Yes

To switch from a Site-to-site Open VPN connection to a Multi-site IPsec VPN connection

1. In the service console, go to **Disaster Recovery -> Connectivity**.
2. Click **Show properties**.
3. Click **Switch to multi-site IPsec VPN**.
4. Click **Reconfigure**.
5. [Reassign the IP addresses](#) of the cloud network and cloud servers.
6. [Configure the Multi-site IPsec connection settings](#).

To switch from a Multi-site IPsec VPN connection to a Site-to-site Open VPN connection

1. In the service console, go to **Disaster Recovery** -> **Connectivity**.
2. Click **Show properties**.
3. Click **Switch to site-to-site Open VPN**.
4. Click **Reconfigure**.
5. [Reassign the IP addresses](#) of the cloud network and cloud servers.
6. [Configure the Site-to-site connection settings](#).

Reassigning IP addresses

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You must reassign the IP addresses of the cloud networks and the cloud servers in order to complete the configuration in the following cases:

- After you switch from Site-to-site Open VPN to Multi-site IPsec VPN, or the opposite.
- After you apply a protection plan (if the Multi-site IPsec VPN connectivity is configured).

To reassign the IP address of a cloud network

1. In the **Connectivity** tab, click the IP address of the cloud network.
2. In the **Network** pop-up, click **Edit**.
3. Type the new the network address and network mask.
4. Click **Done**.

After you reassign the IP address of a cloud network, you must reassign the cloud servers that belong to the reassigned cloud network.

To reassign the IP address of a server

1. In the **Connectivity** tab, click the IP address of the server in the cloud network.
2. In the **Servers** pop-up, click **Change IP address**.
3. In the **Change IP address** pop-up, type the new IP address of the server, or use the automatically generated IP address which is part of the reassigned cloud network.

Note

Disaster Recovery Cloud automatically assigns IP addresses from the cloud network to all cloud servers that were part of the cloud network before the reassignment of the network IP address. You can use the suggested IP addresses to reassign the IP addresses of all the cloud servers at once.

4. Click **Confirm**.

Configuring custom DNS servers

Note

The availability of this feature depends on the service quotas that are enabled for your account.

When you configure a connectivity, Disaster Recovery Cloud creates your cloud network infrastructure. The cloud DHCP server automatically assigns default DNS servers to the recovery servers and primary servers, but you can change the default settings and configure custom DNS servers. The new DNS settings will be applied at the time of the next request to the DHCP server.

Prerequisites:

- One of the connectivity types to the cloud site must be set.

To configure a custom DNS server

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Click **Show properties**.
3. Click **Default (Provided by Cloud Site)**.
4. Select **Custom servers**.
5. Type the IP address of the DNS server.
6. [Optional] If you want to add another DNS server, click **Add**, and type the DNS server IP address.

Note

After you add the custom DNS servers, you can also add the default DNS servers. In that way, if the custom DNS servers are unavailable, Disaster Recovery Cloud will use the default DNS servers.

7. Click **Done**.

Deleting custom DNS servers

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can delete DNS servers from the custom DNS list.

Prerequisites:

Custom DNS servers are configured.

To delete a custom DNS server

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Click **Show properties**.
3. Click **Custom servers**.
4. Click the delete icon next to the DNS server.

Note

The delete operation is disabled when only one custom DNS server is available. If you want to delete all custom DNS servers, select **Default (provided by Cloud Site)** .

5. Click **Done**.

Configuring local routing

In addition to your local networks that are extended to the cloud through the VPN appliance, you may have other local networks that are not registered in the VPN appliance but have servers which need to communicate with cloud servers. To establish the connectivity between such local servers and cloud servers, you need to configure the local routing settings.

To configure local routing

1. Go to **Disaster Recovery>Connectivity**.
2. Click **Show properties**, and then click **Local routing**.
3. Specify the local networks in the CIDR notation.
4. Click **Save**.

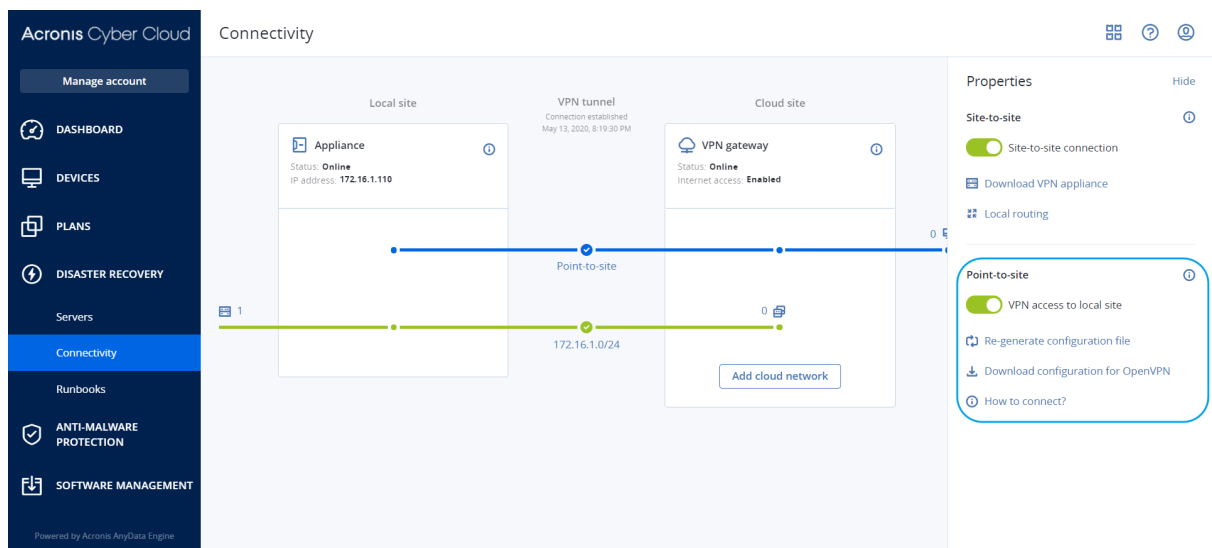
As a result, the servers from the specified local networks can communicate with the cloud servers.

Managing point-to-site connection settings

Note

The availability of this feature depends on the service quotas that are enabled for your account.

In the service console, go to **Disaster Recovery > Connectivity** and then click **Show properties** in the upper right corner.



VPN access to local site

This option is used for managing VPN access to the local site. By default it is enabled. If it is disabled, then the Point-to-site access to the local site will be not allowed.

Download configuration for OpenVPN

This will download the configuration file for the OpenVPN client. The file is required to establish a Point-to-site connection to the cloud site.

Re-generate configuration

You can re-generate the configuration file for the OpenVPN client.

This is required in the following cases:

- If you suspect that the configuration file is compromised.
- If two-factor authentication was enabled for your account.

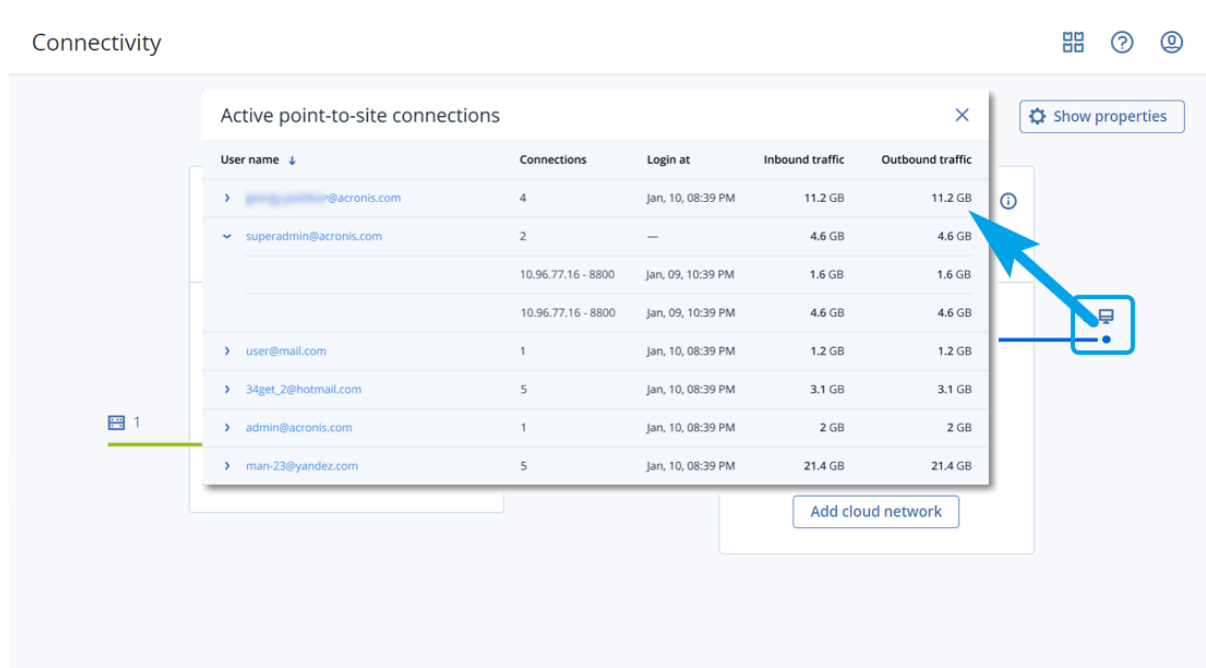
As soon as the configuration file is updated, connecting by means of the old configuration file becomes not possible. Make sure to distribute the new file among the users who are allowed to use the Point-to-site connection.

Active point-to-site connections

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can view all active point-to-site connections in **Disaster recovery > Connectivity**. Click the machine icon on the blue **Point-to-site** line and you will see the detailed information about active point-to-site connections grouped by the user name.



Troubleshooting the IPsec VPN configuration

Note

The availability of this feature depends on the service quotas that are enabled for your account.

When you configure or use the IPsec VPN connection, you might experience problems.

You can learn more about the problems that you encountered in the IPsec log files, and check the Troubleshooting IPsec VPN configuration issues topic for possible solutions of some of the common problems that might occur.

Troubleshooting IPsec VPN configuration issues

Note

The availability of this feature depends on the service quotas that are enabled for your account.

The following table describes the IPsec VPN configuration problems that occur most often, and explains how to troubleshoot them.

Problem	Possible solution
I see the following error message: IKE phase 1 negotiation error. Check the IPsec IKE settings on the Cloud and the Local sites.	Click Retry and check if a more specific error message appears. For example, a more specific error message may be an error message about an algorithm mismatch or an incorrect Pre-shared key.

Problem	Possible solution
	<p>Note</p> <p>For security reasons, the following restrictions apply to the IPsec VPN connectivity:</p> <ul style="list-style-type: none"> • IKEv1 is called for deprecation in RFC8247 and is not supported due to security risks. Only IKEv2 protocol connections are supported. • The following Encryption algorithms are not considered secure and are not supported: DES, and 3DES. • The following Hash algorithms are not considered secure and are not supported: SHA1, and MD5. • Diffie-Hellman group number 2 is not considered secure and is not supported.
The connection between my local site and the cloud site stays in status Connecting .	<p>Check:</p> <ul style="list-style-type: none"> • If the UDP port 500 is open (when you use a firewall). • The connectivity between the local site and the cloud site. • If the IP address of the local site is correct.
The connection between my local site and the cloud site stays in status Waiting for a connection .	<p>You see this status when the Startup action for cloud site is set to Add, which means that the cloud site is waiting for the local site to initiate the connection.</p> <p>Initiate connection from the local site.</p>
The connection between my local site and the cloud site stays in status Waiting for traffic .	<p>You see this status when the Startup action for cloud site is set to Route.</p> <p>If you are expecting a connection from the local site, do the following:</p> <ul style="list-style-type: none"> • From the local site, try to ping the virtual machine in the cloud site. This is a standard behavior necessary for establishing a tunnel for some devices, for example Cisco ASA. (Route mode) • Ensure that the local site established a tunnel by setting the Startup action of the local site to Start.
The connection between my local site and the cloud site is established, but I	<p>This issue may be due to the following reasons:</p> <ul style="list-style-type: none"> • Network mapping in the cloud IPsec site is

Problem	Possible solution
can see that one or more of the network policies are down.	<p>different from the network mapping in the local site.</p> <p>Ensure that the network mappings and the sequence of the network policies in the local and cloud sites match exactly.</p> <ul style="list-style-type: none"> This state is correct when the Startup action of the local site and/or of the cloud site is set to Route (for example, on Cisco ASA devices), and currently there is no traffic. You can try to ping to make sure that the tunnel is established. If the ping is not working, check the network mapping on the local and the cloud site.
I want restart a specific IPsec connection.	<p>To restart a specific IPsec connection:</p> <ol style="list-style-type: none"> 1. In the Disaster recovery > Connectivity screen, click the IPsec connection. 2. Click Disable connection. 3. Click the IPsec connection again. 4. Click Enable connection.

Downloading the IPsec VPN log files

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can find additional information about the IPsec connectivity in the log files on the VPN server. The log files are compressed in a .zip archive that you can download and extract.

15.5.5 Prerequisites

Multi-site IPsec VPN connectivity is configured.

To download the .zip archive with the log files

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Click the gear icon next to the VPN gateway of the cloud site.
3. Click **Download log**.

Multi-site IPsec VPN log files

Note

The availability of this feature depends on the service quotas that are enabled for your account.

The following list provides more information about the IPsec VPN log files that are part of the zip archive, and the information that they contain.

- ip.txt - The file contains the logs from the configuration of the network interfaces. You must see two IP addresses - a public IP address, and a local IP address. If you do not see these IP addresses in the log, there is a problem. Contact the Support team.

Note

The mask for the public IP address must be 32.

- swanctl-list-loaded-config.txt - The file contains information about all IPsec sites.
If you do not see a site in the file, then the IPsec configuration was not applied. Try to update the configuration and save it, or contact the Support team.
- swanctl-list-active-sas.txt - The file contains connections and policies that are in status active or a connecting.

15.6 Setting up recovery servers

This section describes the concepts of failover and failback, creation of a recovery server, and the disaster recovery operations.

15.6.1 Creating a recovery server

You can follow the instructions below or watch the [video tutorial](#).

Prerequisites

- A protection plan must be applied to the original machine that you want to protect. This plan must back up the entire machine, or only the disks, required for booting up and providing the necessary services, to a cloud storage.
- One of the connectivity types to the cloud site must be set.

To create a recovery server

1. On the **All devices** tab, select the machine that you want to protect.
2. Click **Disaster recovery**, and then click **Create recovery server**.
3. Select the number of virtual cores and the size of RAM.
Be aware of the compute points next to every option. The number of compute points reflects the cost of running the recovery server per hour.
4. Specify the cloud network to which the server will be connected.
5. Specify the IP address that the server will have in the production network. By default, the IP address of the original machine is set.

Note

If you use a DHCP server, add this IP address to the server exclusion list in order to avoid IP address conflicts.

6. [Optional] Select the **Test IP address** check box, and then specify the IP address.

This will give you the capability to test a failover in the isolated test network and to connect to the recovery server via RDP or SSH during a test failover. In the test failover mode, the VPN gateway will replace the test IP address with the production IP address by using the NAT protocol.

If you leave the check box cleared, the console will be the only way to access the server during a test failover.

Note

If you use a DHCP server, add this IP address to the server exclusion list, in order to avoid IP address conflicts.

You can select one of the proposed IP addresses or type in a different one.

7. [Optional] Select the **Internet access** check box.

This will enable the recovery server to access the Internet during a real or test failover. By default, the TCP port 25 is open for outbound connections to public IP addresses.

8. [Optional] Set the **RPO threshold**.

The RPO threshold defines the maximum time interval allowed between the last suitable recovery point for a failover and the current time. The value can be set within 15 – 60 minutes, 1 – 24 hours, 1 – 14 days.

9. [Optional] Select the **Use public IP address** check box.

Having a public IP address makes the recovery server available from the Internet during a failover or test failover. If you leave the check box cleared, the server will be available only in your production network.

The **Use public IP address** option requires the **Internet access** option to be enabled.

The public IP address will be shown after you complete the configuration. By default, TCP port 443 is open for inbound connections to public IP addresses.

10. [Optional] If the backups for the selected machine are encrypted, you can specify the password that will be automatically used when creating a virtual machine for the recovery server from the encrypted backup. Click **Specify**, and then define the credential name and password. By default, you will see the most recent backup in the list. To view all the backups, select **Show all backups**.
11. [Optional] Change the recovery server name.
12. [Optional] Type a description for the recovery server.
13. [Optional] Click the **Cloud firewall rules** tab to edit the default firewall rules. For more information, see "Setting firewall rules for cloud servers " (p. 414).
14. Click **Create**.

The recovery server appears in the **Disaster Recovery > Servers > Recovery servers** tab of the service console. You can also view its settings by selecting the original machine and clicking **Disaster recovery**.

The screenshot shows the Acronis Cyber Cloud interface. On the left is a dark blue sidebar with navigation options: Manage account, DISASTER RECOVERY (selected), Servers (selected), Connectivity, Runbooks, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, BACKUP STORAGE, REPORTS, and SETTINGS. The main area is titled 'Servers' and has tabs for 'RECOVERY SERVERS' (active) and 'PRIMARY SERVERS'. Below the tabs is a search bar and a table of servers.

Name	Status	State	RPO compliance	VM state	
Win16	OK	Standby	—	—	...
cen7-sg7	OK	Standby	—	—	...
Cen_vg-1	OK	Failover	Not set	On	...
Cen_mb-3	OK	Testing failover	Not set	On	...
Cen_mb-2	OK	Failback	Not set	Off	...
Cen_mb-1	OK	Failback	Not set	Off	...

15.6.2 How failover works

Production failover

Note

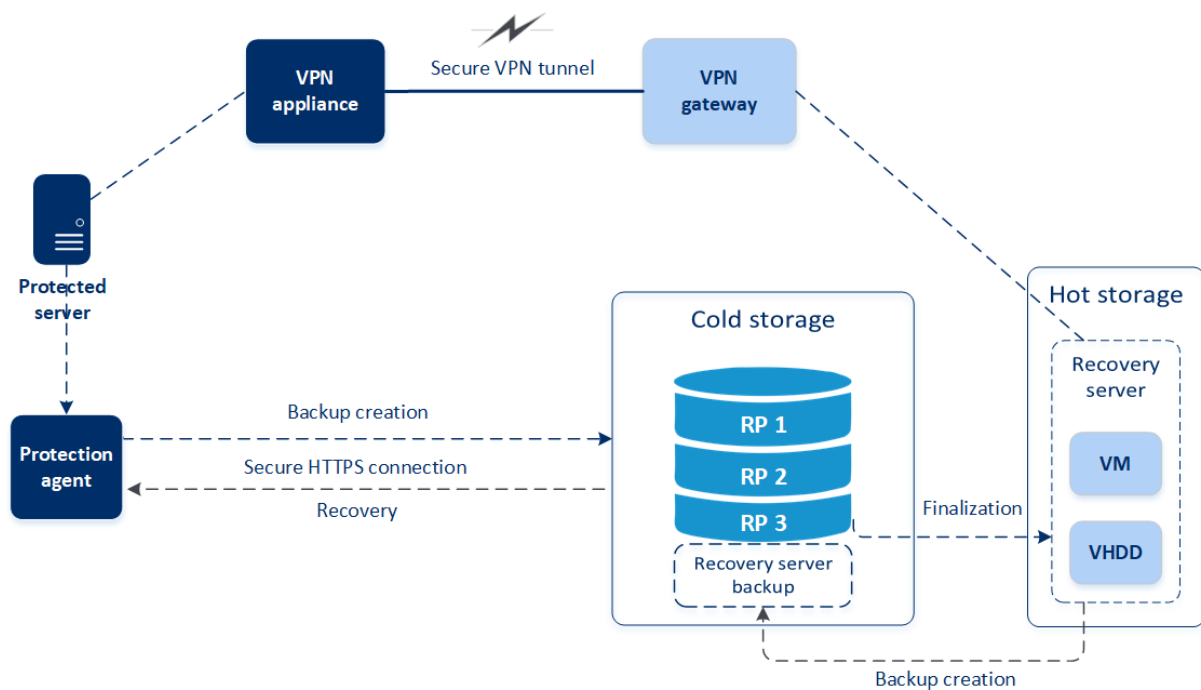
The availability of this feature depends on the service quotas that are enabled for your account.

When a recovery server is created, it stays in the **Standby** state. The corresponding virtual machine does not exist until you initiate the failover. Before starting the failover process, you need to create at least one disk image backup (with bootable volume) of your original machine.

When starting the failover process, you select the recovery point of the original machine from which a virtual machine with the predefined parameters is created. The failover operation uses the "run VM from a backup" functionality. The recovery server gets the transition state **Finalization**. This process implies transferring the server's virtual disks from the backup storage ("cold" storage) to the disaster recovery storage ("hot" storage). During the finalization, the server is accessible and operable although the performance is lower than normal. When the finalization is completed, the server performance reaches its normal value. The server state changes to **Failover**. The workload is now switched from the original machine to the recovery server in the cloud site.

If the recovery server has a protection agent inside, the agent service is stopped in order to avoid interference (such as starting a backup or reporting outdated statuses to the backup component).

On the diagram below, you can see both the failover and failback processes.



Test failover

During a **test failover**, a virtual machine is not finalized. This means that the agent reads the virtual disks' content directly from the backup – that is, performs random access to different parts of the backup. for more information about the test failover process, see "Performing a test failover" (p. 401).

Performing a test failover

Testing a failover means starting a recovery server in a test VLAN that is isolated from your production network. You can test several recovery servers at a time in order to check their interaction. In the test network, the servers communicate using their production IP addresses, but they cannot initiate TCP or UDP connections to the machines in your local network.

Though testing a failover is optional, we recommend that you make it a regular process with a frequency that you find adequate in terms of cost and safety. A good practice is creating a runbook – a set of instructions describing how to spin up the production environment in the cloud.

It is recommended to [create a recovery server](#) in advance to protect your devices from a disaster. You will be able to perform the test failover from any of the recovery points generated after the recovery server was created for the device.

To run a test failover

1. Select the original machine or select the recovery server that you want to test.
2. Click **Disaster Recovery**.
The description of the recovery server opens.
3. Click **Failover**.

4. Select the failover type **Test failover**.
5. Select the recovery point, and then click **Test failover**.

When the recovery server starts, its state changes to **Testing failover**.

The screenshot shows the Acronis Cyber Cloud interface. On the left, a sidebar contains navigation options: Manage account, DISASTER RECOVERY, Servers (highlighted), Connectivity, Runbooks, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, BACKUP STORAGE, REPORTS, and SETTINGS. The main area is titled 'Servers' and has tabs for 'RECOVERY SERVERS' and 'PRIMARY SERVERS'. A search bar is present. Below it, a table lists servers with columns for Name and Status. The servers listed are Win16, cen7-sg7, Cen_vg-1, Cen_mb-3 (selected), Cen_mb-2, and Cen_mb-1, all with a status of 'OK'. On the right, a details panel for 'Cen_mb-3' is open, showing fields for Name, Description, Original device (Has been deleted), Status (OK), State (Testing failover), VM state (On), CPU and RAM (1 vCPU, 2 GB RAM, 1 compute point), IP address (172.16.2.6), and Internet access (Enabled).

6. Test the recovery server by using any of the following methods:
 - In **Disaster Recovery > Servers**, select the recovery server, and then click **Console**.
 - Connect to the recovery server by using RDP or SSH, and the test IP address that you specified when creating the recovery server. Try the connection from both inside and outside the production network (as described in "Point-to-site connection").
 - Run a script within the recovery server.
The script may check the login screen, whether applications are started, the Internet connection, and the ability of other machines to connect to the recovery server.
 - If the recovery server has access to the Internet and a public IP address, you may want to use TeamViewer.
7. When the test is complete, click **Stop testing**.
The recovery server is stopped. All changes made to the recovery server during the test failover are not preserved.

Performing a failover

Note

The availability of this feature depends on the service quotas that are enabled for your account.

A failover is a process of moving a workload from your premises to the cloud, and also the state when the workload remains in the cloud.

When you initiate a failover, the recovery server starts in the production network. All protection plans are revoked from the original machine. A new protection plan is automatically created and applied to the recovery server.

At least one recovery point must be created before failing over to a recovery server.

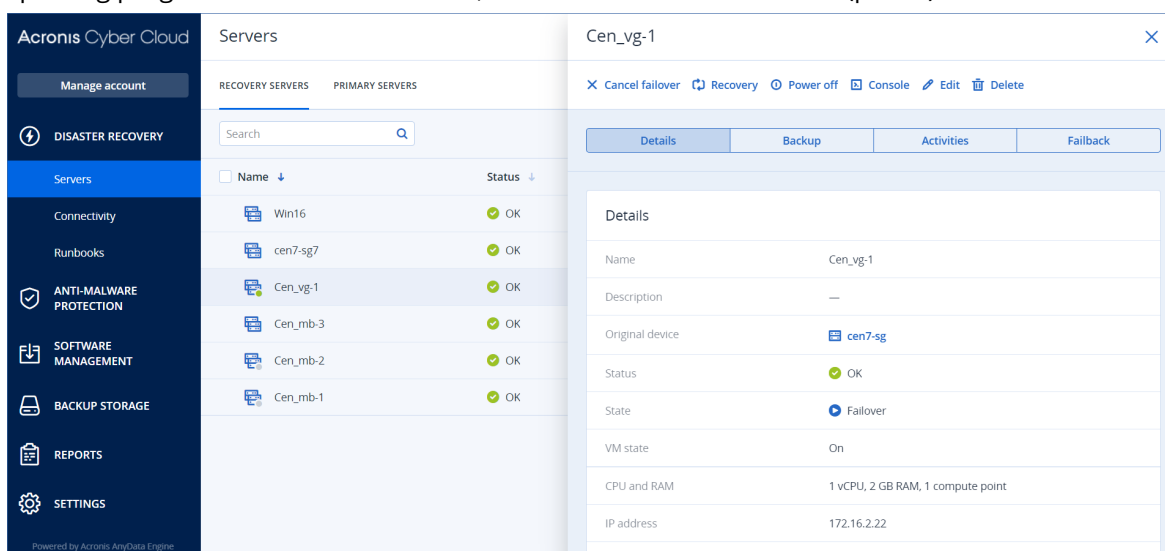
A good practice is to [create a recovery server](#) in advance to protect your devices from a disaster. You will be able to perform the production failover from any of the recovery points generated after the recovery server was created for the device.

You can follow the instructions below or watch the [video tutorial](#).

To perform a failover

1. Ensure that the original machine is not available on the network.
2. In the service console, go to **Disaster recovery > Servers > Recovery servers** and select the recovery server.
3. Click **Failover**.
4. Select the type of failover **Production failover**.
5. Select the recovery point, and then click **Start production failover**.

When the recovery server starts, its state changes to **Finalization**, and after some time to **Failover**. It is critical to understand that the server is available in both states, despite the spinning progress indicator. For details, refer to "How failover works" (p. 400).



6. Ensure that the recovery server is started by viewing its console. Click **Disaster Recovery > Servers**, select the recovery server, and then click **Console**.
7. Ensure that the recovery server can be accessed using the production IP address that you specified when creating the recovery server.

Once the recovery server is finalized, a new protection plan is automatically created and applied to it. This protection plan is based on the protection plan that was used for creating the recovery server, with certain limitations. In this plan, you can change only the schedule and retention rules. For more information, refer to "[Backing up the cloud servers](#)".

If you want to cancel failover, select the recovery server and click **Cancel failover**. All changes starting from the failover moment except the recovery server backups will be lost. The recovery server will return back to the **Standby** state.

If you want to perform failback, select the recovery server and click **Failback**.

How to perform failover of servers using local DNS

If you use DNS servers on the local site for resolving machine names, then after a failover the recovery servers, corresponding to the machines relying on the DNS, will fail to communicate because the DNS servers used in the cloud are different. By default, the DNS servers of the cloud site are used for the newly created cloud servers. If you need to apply custom DNS settings, contact the support team.

How to perform failover of a DHCP server

Your local infrastructure may have the DHCP server located on a Windows or Linux host. When such a host is failed over to the cloud site, the DHCP server duplication issue occurs because the VPN gateway in the cloud also performs the DHCP role. To resolve this issue, do one of the following:

- If only the DHCP host was failed over to the cloud, while the rest local servers are still on the local site, then you must log in to the DHCP host in the cloud and turn off the DHCP server on it. Thus, there will be no conflicts and only the VPN gateway will work as the DHCP server.
- If your cloud servers already got the IP addresses from the DHCP host, then you must log in to the DHCP host in the cloud and turn off the DHCP server on it. You must also log in to the cloud servers and renew the DHCP lease to assign new IP addresses allocated from the correct DHCP server (hosted on the VPN gateway).

15.6.3 How failback works

Note

The availability of this feature depends on the service quotas that are enabled for your account.

A failback is a process of moving the workload from the cloud back to a physical or virtual machine on your local site. You can perform a failback on a recovery server in **Failover** state, and continue using the server on your local site.

During the failback process to a target virtual machine, you can transfer the backup data to your local site while the virtual machine in the cloud continues to run. This technology helps you to achieve a very short downtime period, which is estimated and displayed in the service console. You can view it and use this information to plan your activities and, if necessary, warn your clients about an upcoming downtime period.

The failback process to target virtual machines and target physical machines is different. For more information about the phases of the failback process, see "Failback to a target virtual machine" (p. 405) and "Failback to a target physical machine" (p. 409).

Note

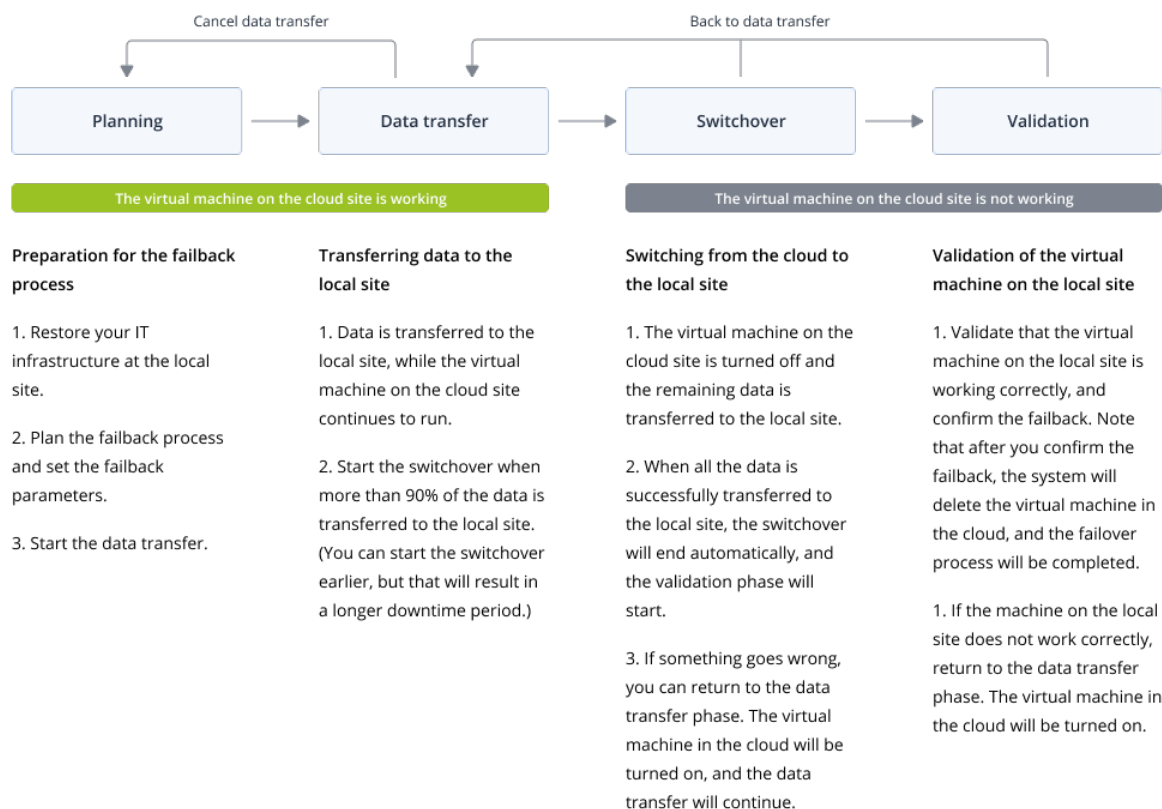
Runbook operations support the failback to a physical machine only. This means that if you start the failback process by executing a runbook that includes a **Failback server** step, the procedure will require a manual interaction - you must manually recover the machine, and confirm or cancel the failback process from the **Disaster Recovery>Servers** tab.

Failback to a target virtual machine

Note

The availability of this feature depends on the service quotas that are enabled for your account.

The failback process to a target virtual machine consists of four phases.



1. **Planning.** During this phase, you restore the IT infrastructure at your local site, such as the hosts and the network configurations, configure the failback parameters, and plan when to start the data transfer.

Note

To minimize the total time for the failback process, we recommend that you start the **Data transfer** phase immediately after you set up your local servers, and then continue configuring the network and setting up the rest of the local infrastructure during the **Data transfer** phase.

2. **Data transfer.** During this phase, the data is transferred from the cloud site to the local site while the virtual machine in the cloud continues to run. You can start the next phase - **Switchover**, at any time during the **Data transfer** phase, but you should consider the following relations:

The longer you remain in the **Data transfer** phase,

- the longer the virtual machine in the cloud continues to run
- the bigger amount of data will be transferred to your local site
- the higher the cost you will pay (you spend more compute points)
- the shorter the downtime period that you will experience during the **Switchover** phase.

If you want to minimize the downtime, start the **Switchover** phase after more than 90 % of the data is transferred to the local site.

If you can afford to experience a longer downtime period, and do not want to spend more compute points for running the virtual machine in the cloud, you can start the **Switchover** phase earlier.

If you cancel the failback process during the **Data transfer** phase, the transferred data will not be deleted from the local site. To avoid potential issues, manually delete the transferred data before you start a new failback process. The following data transfer process will start from the beginning.

3. **Switchover.** During this phase, the virtual machine in the cloud is turned off and the remaining data, including the last backup increment, is transferred to the local site. Note that when the **Switchover** phase completes, all data is transferred to the local site - there is no data loss, and the virtual machine on the local site is an exact copy of the virtual machine in the cloud. You can view the estimated time to finish (downtime period) of this phase in the service console. When all the data is transferred to the local site, the virtual machine on the local site is recovered, and the **Validation** phase starts automatically.
4. **Validation.** During this phase, the virtual machine on the local site is ready and you can turn it on. You can verify if the virtual machine is working correctly, and:
- If everything is working as expected, confirm the failback. After the failback confirmation, the virtual machine in the cloud is deleted, and the recovery server returns to the **Standby** state. This is the end of the failback process.
 - If something is wrong, you can cancel the switchover and return to the **Data transfer** phase.

Performing failback to a virtual machine

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can perform failback to a target virtual machine on your local site.

Prerequisites

- The agent that you will use to perform failback is online and is not currently used for another failback operation.

- Your Internet connection is stable.

To perform a failback to a virtual machine

1. In the service console, go to **Disaster recovery > Servers**.
2. Select the recovery server that is in the **Failover** state.
3. Click the **Failback** tab.
4. In the **Failback parameters** section, select **Virtual machine** as a **Target**, and configure the other parameters.

Note that by default, some of the **Failback parameters** are populated automatically with suggested values, but you can change them.

The following table provides more information about the **Failback parameters**.

Parameter	Description
Backup size	<p>Amount of data that will be transferred to your local site during the failback process.</p> <p>After you start the failback process to a target virtual machine, the Backup size will be increasing during the Data transfer phase, because the virtual machine in the cloud will continue to run and generate new data.</p> <p>To calculate the estimated downtime period during the failback process to a target virtual machine, take 10% of the Backup size value (as we recommend that you start the Switchover phase after 90% of the data is transferred to your local site), and divide it by the value of your Internet speed.</p> <hr/> <p>Note</p> <p>The value of the Internet speed will decrease when you perform several failback processes at the same time.</p> <hr/>
Target	Type of workload on your local site to which you will recover the cloud server: Virtual machine or Physical machine .
Target machine location	<p>Failback location: a VMware ESXi host or a Microsoft Hyper-V host.</p> <p>You can select from all the hosts that have an agent which is registered with the Cyber Protection service.</p>
Agent	<p>Agent which will perform the failback operation.</p> <p>You can use one agent to perform one failback operation at the same time.</p> <p>You can select an agent that is online and is not currently used for another failback process, has a version which supports the failback functionality, and has rights to access the backup.</p> <p>Note that you can install several agents on VMware ESXi hosts, and start a separate failback process using each of them. These failback processes can be performed at the same time.</p>

Parameter	Description
Target machine settings	<p>Virtual machine settings:</p> <ul style="list-style-type: none"> • Virtual processors. Select the number of virtual processors. • Memory. Select how much memory the virtual machine will have. • Units. Select the units for the memory. • [Optional] Network adapters. To add a network adapter, click Add, and select a network in the Network field. <p>When you are ready with the changes, click Done.</p>
Path	<p>(For Microsoft Hyper-V hosts) Folder on the host where your machine will be stored.</p> <p>Ensure that there is enough free memory space on the host for the machine.</p>
Datastore	<p>(For VMware ESXi hosts) Datastore on the host where your machine will be stored.</p> <p>Ensure that there is enough free memory space on the host for the machine.</p>
Provisioning mode	<p>Method of allocation of the virtual disk.</p> <p>For Microsoft Hyper-V hosts:</p> <ul style="list-style-type: none"> • Dynamically expanding (default value). • Fixed size. <p>For Microsoft Hyper-V hosts:</p> <ul style="list-style-type: none"> • Thin (default value). • Thick.
Target machine name	<p>Name of the target machine. By default, the target machine name is the same as the recovery server name.</p> <p>The target machine name must be unique on the selected Target machine location.</p>

- Click **Start data transfer**, and then in the confirmation window, click **Start**.

The **Data transfer** phase starts. The console displays the following information:

- **Progress.** The parameter shows how much data is already transferred to the local site, and the total amount of data that must be transferred. Note that the total amount of data includes the data from the last backup before the data transfer phase was started, and the backups of the newly generated data (backup increments), as the virtual machine continues to run during the **Data transfer** phase. For this reason, both values of the **Progress** parameter increase with time.
- **Downtime estimation.** The parameter shows how much time the virtual machine will be unavailable, if you start the **Switchover** phase now. The value is calculated based on the values of the **Progress**, and decreases with time.

- Click **Switchover**, and then in the confirmation window, click **Switchover** again.

The **Switchover** phase starts. The console displays the following information:

- **Progress.** The parameter shows the progress of restoring the virtual machine on the local site.
 - **Estimated time to finish.** The parameter shows the approximate time when the **Switchover** phase will be completed and you will be able to turn on the virtual machine on the local site.
7. After the **Switchover** phase completes, validate that the virtual machine on your local site is working as expected.
 8. Click **Confirm failback**, and then in the confirmation window, click **Confirm** to finalize the process.

The virtual machine in the cloud is deleted, and the recovery server returns to the **Standby** state.

Failback to a target physical machine

Note

The availability of this feature depends on the service quotas that are enabled for your account.

The failback process to a target physical machine differs from the failback process to a target virtual machine. The data transfer from the backup in the cloud to the local site is not part of the automated workflow, and is done manually after the virtual machine in the cloud is turned off. For this reason, when performing failback to a physical machine, expect a longer downtime period.

The failback process to a target physical machine consists of the following phases:

1. **Planning.** During this phase, you restore the IT infrastructure at your local site, such as the hosts and the network configurations, configure the failback parameters, and plan when to start the data transfer.
2. **Switchover.** During this phase, the virtual machine in the cloud is turned off and the newly generated data is backed up. When the backup is complete, you recover the machine to the local site manually. You can either recover the disk by using bootable media, or recover the entire machine from the cloud backup storage.
3. **Validation.** During this phase, you verify that the physical machine is working correctly, and confirm the failback. After the confirmation, the virtual machine on the cloud site is deleted, and the recovery server returns to the **Standby** state.

Performing failback to a physical machine

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can perform failback to a target physical machine on your local site.

To perform a failback to a physical machine

1. In the service console, go to **Disaster recovery > Servers**.
2. Select the recovery server that is in the **Failover** state.
3. Click the **Failback** tab.
4. In the **Select target** field, select **Physical machine**.

5. [Optional] Calculate the estimated downtime period during the failback process, by dividing the **Backup size** value by the value of your Internet speed.

Note

The value of the Internet speed will decrease when you perform several failback processes at the same time.

6. Click **Switchover**, and then in the confirmation window, click **Switchover** again.
The virtual machine on the cloud site is turned off.
7. Recover the server from a backup to the physical machine on your local site.
 - If you are using bootable media, proceed as described in "Recovering disks by using bootable media" in the Cyber Protection User Guide. Ensure that you sign in to the cloud by using the account for which the server is registered and that you select the most recent backup.
 - If the target machine is online, you can use the service console. On the **Backup storage** tab, select the cloud storage. In **Machine to browse from**, select the target physical machine. The selected machine must be registered for the same account for which the server is registered. Find the most recent backup of the server, click **Recover entire machine**, and then set up other recovery parameters. For detailed instructions, refer to "Recovering a machine" in the Cyber Protection User Guide.
8. Ensure that the recovery is completed and the recovered machine works properly, and click **Machine is restored**.
9. If everything is working as expected, click **Confirm failback**, and then in the confirmation window, click **Confirm** again.
The recovery server and recovery points become ready for the next failover. To create new recovery points, apply a protection plan to the new local server.

15.6.4 Working with encrypted backups

You can create recovery servers from the encrypted backups. For your convenience, you can set up an automatic password application to an encrypted backup during the failover to a recovery server.

When creating a recovery server, you can [specify the password to be used for automatic disaster recovery operations](#). It will be saved to the Credentials store, a secure storage of credentials that can be found in **Settings > Credentials** section.

One credential can be linked to several backups.

To manage the saved passwords in the Credentials store

1. Go to **Settings > Credentials**.
2. To manage a specific credential, click the icon in the last column. You can view the items linked to this credential.
 - To unlink the backup from the selected credential, click the recycle bin icon near the backup. As a result, you will have to specify the password manually during the failover to the recovery

server.

- To edit the credential, click **Edit**, and then specify the name or password.
- To delete the credential, click **Delete**. Note that you will have to specify the password manually during the failover to the recovery server.

15.7 Setting up primary servers

This section describes how to create and manage your primary servers.

15.7.1 Creating a primary server

Prerequisites

- One of the connectivity types to the cloud site must be set.

To create a primary server

1. Go to **Disaster Recovery > Servers > Primary servers** tab.
2. Click **Create**.
3. Select a template for the new virtual machine.
4. Select the number of virtual cores and the size of RAM.
Pay attention to the compute points next to every option. The number of compute points reflects the cost of running the primary server per hour.
5. [Optional] Change the virtual disk size. If you need more than one hard disk, click **Add disk**, and then specify the new disk size. Currently, you can add no more than 10 disks for a primary server.
6. Specify the cloud network in which the primary server will be included.
7. Specify the IP address that the server will have in the production network. By default, the first free IP address from your production network is set.

Note

If you use a DHCP server, add this IP address to the server exclusion list in order to avoid IP address conflicts.

8. [Optional] Select the **Internet access** check box.
This will enable the primary server to access the Internet. By default, TCP port 25 is open for outbound connections to public IP addresses.
9. [Optional] Select the **Use public IP address** check box.
Having a public IP address makes the primary server available from the Internet. If you leave the check box cleared, the server will be available only in your production network.
The public IP address will be shown after you complete the configuration. By default, TCP port 443 is open for inbound connections to public IP addresses.
10. [Optional] Select **Set RPO threshold**.

RPO threshold defines the maximum allowable time interval between the last recovery point and the current time. The value can be set within 15 – 60 minutes, 1 – 24 hours, 1 – 14 days.

11. Define the primary server name.
12. [Optional] Specify a description for the primary server.
13. [Optional] Click the **Cloud firewall rules** tab to edit the default firewall rules. For more information, see "Setting firewall rules for cloud servers " (p. 414).
14. Click **Create**.

The primary server becomes available in the production network. You can manage the server by using its console, RDP, SSH, or TeamViewer.

The screenshot shows the Acronis Cyber Cloud interface. On the left is a sidebar with navigation options: Manage account, DISASTER RECOVERY, Servers, Connectivity, Runbooks, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, BACKUP STORAGE, REPORTS, and SETTINGS. The main area is titled 'Servers' and has two tabs: 'RECOVERY SERVERS' and 'PRIMARY SERVERS'. The 'PRIMARY SERVERS' tab is active, showing a table with one entry: 'New primary server' with a status of 'OK'. A modal window titled 'New primary server' is open on the right, showing details for the new server. The modal has tabs for 'Details', 'Backup', and 'Activities'. The 'Details' tab is active, showing the following information:

Details	
Name	New primary server
Description	—
Status	OK
State	Ready
VM state	On
CPU and RAM	1 vCPU, 2 GB RAM, 1 compute point
IP address	172.16.2.10
Internet access	Enabled

15.7.2 Operations with a primary server

The primary server appears in the **Disaster Recovery > Servers > Primary servers** tab in the service console.

To start or stop the server, click **Power on** or **Power off** on the primary server panel.

To edit the primary server settings, stop the server, and then click **Edit**.

To apply a protection plan to the primary server, select it and on the **Plan** tab click **Create**. You will see a predefined protection plan where you can change only the schedule and retention rules. For more information, refer to "[Backing up the cloud servers](#)".

15.8 Managing the cloud servers

To manage the cloud servers, go to **Disaster Recovery > Servers**. There are two tabs there: **Recovery servers** and **Primary servers**. To show all optional columns in the table, click the gear icon.

You can find the following information about each cloud server by selecting it.

Column name	Description
Name	A cloud server name defined by you
Status	The status reflecting the most severe issue with a cloud server (based on the active alerts)
State	A cloud server state
VM state	The power state of a virtual machine associated with a cloud server
Active location	The location where a cloud server is hosted. For example, Cloud .
RPO threshold	The maximum time interval allowed between the last suitable recovery point for failover and the current time. The value can be set within 15-60 minutes, 1-24 hours, 1-14 days.
RPO compliance	<p>The RPO compliance is the ratio between the actual RPO and RPO threshold. The RPO compliance is shown if the RPO threshold is defined.</p> <p>It is calculated as follows:</p> $\text{RPO compliance} = \text{Actual RPO} / \text{RPO threshold}$ <p>where</p> $\text{Actual RPO} = \text{current time} - \text{last recovery point time}$ <p>RPO compliance statuses</p> <p>Depending on the value of the ratio between the actual RPO and RPO threshold, the following statuses are used:</p> <ul style="list-style-type: none"> • Compliant. The RPO compliance < 1x. A server meets the RPO threshold. • Exceeded. The RPO compliance <= 2x. A server violates the RPO threshold. • Severely exceeded. The RPO compliance <= 4x. A server violates the RPO threshold more than 2x times. • Critically exceeded. The RPO compliance > 4x. A server violates the RPO threshold more than 4x times. • Pending (no backups). The server is protected with the protection plan but the backup is being created and not completed yet.
Actual RPO	The time passed since the last recovery point creation
Last recovery point	The date and time when the last recovery point was created

15.9 Firewall rules for cloud servers

You can configure firewall rules to control the inbound and outbound traffic of the primary and recovery servers on your cloud site.

You can configure inbound rules after you provision a public IP address for the cloud server. By default, TCP port 443 is allowed, and all other inbound connections are denied. You can change the default firewall rules, and add or remove Inbound exceptions. If a public IP is not provisioned, you can only view the inbound rules, but cannot configure them.

You can configure outbound rules after when you provision Internet access for the cloud server. By default, TCP port 25 is denied, and all other outbound connections are allowed. You can change the default firewall rules, and add or remove outbound exceptions. If Internet access is not provisioned, you can only view the outbound rules, but cannot configure them.

Note

For security reasons, there are predefined firewall rules that you cannot change.

For inbound and outbound connections:

- Permit ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

For inbound connections only:

- Non-configurable part: Deny all

For outbound connections only:

- Non-configurable part: Reject all
-

15.9.1 Setting firewall rules for cloud servers

You can edit the default firewall rules for the primary and recovery servers in the cloud.

To edit the firewall rules of a server on your cloud site

1. In the service console, go to **Disaster Recovery> Servers**.
2. If you want to edit the firewall rules of a recovery server, click the **Recovery servers** tab.
Alternatively, if you want to edit the firewall rules of a primary server, click the **Primary servers** tab.
3. Click the server, and then click **Edit**.
4. Click the **Cloud firewall rules** tab.
5. If you want to change the default action for the inbound connections:

- a. In the **Inbound** drop-down field, select the default action.

Action	Description
Deny all	Denies any inbound traffic. You can add exceptions and allow traffic from specific IP addresses, protocols, and ports.
Allow all	Allows all inbound TCP and UDP traffic. You can add exceptions and deny traffic from specific IP addresses, protocols, and ports.

Note

Changing the default action invalidates and removes the configuration of existing inbound rules.

- b. [Optional] If you want to save the existing exceptions, in the confirmation window, select **Save filled-in exceptions**.
- c. Click **Confirm**.
6. If you want to add an exception:
- a. Click **Add exception**.
- b. Specify the firewall parameters.

Firewall parameter	Description
Protocol	Select the protocol for the connection. The following options are supported: <ul style="list-style-type: none">• TCP• UDP• TCP+UDP
Server port	Select the ports to which the rule applies. You can specify the following: <ul style="list-style-type: none">• a specific port number (for example, 2298)• a range of port numbers (for example, 6000-6700)• any port number. Use * if you want the rule to apply to any port number.
Client IP address	Select the IP addresses to which the rule applies. You can specify the following: <ul style="list-style-type: none">• a specific IP address (for example, 192.168.0.0)• a range of IP addresses using the CIDR notation (for example, 192.168.0.0/24)• any IP address. Use * if you want the rule to apply to any IP address.

7. If you want to remove an existing inbound exception, click the bin icon next to it.
8. If you want to change the default action for the outbound connections:
 - a. In the **Outbound** drop-down field, select the default action.

Action	Description
Deny all	Denies any outbound traffic. You can add exceptions and allow traffic to specific IP addresses, protocols, and ports.
Allow all	Allows all outbound traffic. You can add exceptions and deny traffic from specific IP addresses, protocols, and ports.

Note

Changing the default action invalidates and removes the configuration of existing outbound rules.

- b. [Optional] If you want to save the existing exceptions, in the confirmation window, select **Save filled-in exceptions**.
 - c. Click **Confirm**.
9. If you want to add an exception:
 - a. Click **Add exception**.
 - b. Specify the firewall parameters.

Firewall parameter	Description
Protocol	Select the protocol for the connection. The following options are supported: <ul style="list-style-type: none">• TCP• UDP• TCP+UDP
Server port	Select the ports to which the rule applies. You can specify the following: <ul style="list-style-type: none">• a specific port number (for example, 2298)• a range of port numbers (for example, 6000-6700)• any port number. Use * if you want the rule to apply to any port number.
Client IP address	Select the IP addresses to which the rule applies. You can specify the following: <ul style="list-style-type: none">• a specific IP address (for example, 192.168.0.0)• a range of IP addresses using the CIDR notation (for example, 192.168.0.0/24)

Firewall parameter	Description
	<ul style="list-style-type: none"> any IP address. Use * if you want the rule to apply to any IP address.

10. If you want to remove an existing outbound exception, click the bin icon next to it.

11. Click **Save**.

15.9.2 Checking the cloud firewall activities

After an update of the configuration of the firewall rules of a cloud server, a log of the update activity becomes available in the service console. You can view the log and check the following information:

- user name of the user who updated the configuration
- date and time of the update
- firewall settings for inbound and outbound connections
- the default actions for inbound and outbound connections
- the protocols, ports and IP addresses of the exceptions for inbound and outbound connections

To view the details about a cloud firewall rules configuration change

1. In the service console, click **Dashboard** > **Activities**.
2. Click the corresponding activity, and click **All Properties**.

The description of the activity should be **Updating cloud server configuration**.

3. In the **context** field, inspect the information that you are interested in.

15.10 Backing up the cloud servers

Primary and recovery servers are backed up by Agent for VMware, which is installed on the cloud site. In the initial release, this backup is somewhat restricted in functionality as compared to a backup performed by local agents. These limitations are temporary and will be removed in future releases.

- The only possible backup location is the cloud storage.
- A protection plan cannot be applied to multiple servers. Each server must have its own protection plan, even if all of the protection plans have the same settings.
- Only one protection plan can be applied to a server.
- Application-aware backup is not supported.
- Encryption is not available.
- Backup options are not available.

When you delete a primary server, its backups are also deleted.

A recovery server is backed up only in the failover state. Its backups continue the backup sequence of the original server. When a failback is performed, the original server can continue this backup sequence. So, the backups of the recovery server can only be deleted manually or as a result of applying the retention rules. When a recovery server is deleted, its backups are always kept.

Note

The protection plans for cloud servers are performed according to UTC time.

15.11 Orchestration (runbooks)

Note

Some features might require additional licensing, depending on the applied licensing model.

A runbook is a set of instructions describing how to spin up the production environment in the cloud. You can create runbooks in the service console. To access the **Runbooks** tab, select **Disaster recovery > Runbooks**.

15.11.1 Why use runbooks?

Runbooks let you:

- Automate a failover of one or multiple servers
- Automatically check the failover result by pinging the server IP address and checking the connection to the port you specify
- Set the sequence of operations for servers running distributed applications
- Include manual operations in the workflow
- Verify the integrity of your disaster recovery solution, by executing runbooks in the test mode.

15.11.2 Creating a runbook

You can follow the instruction below or watch the [video tutorial](#).

To start creating a runbook, click **Create runbook > Add step > Add action**. You can use drag and drop to move actions and steps. Do not forget to give a distinctive name to the runbook. While creating a long runbook, click **Save** from time to time. Once you are finished, click **Close**.

The screenshot shows the 'New runbook' interface. On the left, a 'Step 1' box contains an action card for 'Failover server' with a 'recovery' status and the instruction 'Continue if already done'. Below the step box is an 'Add step' button. On the right, a configuration panel for the 'Failover server' action is shown. It includes a 'Server' dropdown menu, a 'Completion check' section with checkboxes for 'Ping IP address' (set to 10.0.3.35) and 'Connect to port' (set to 10.0.3.35: 443), and a 'Timeout in minutes' field set to 10. At the top right of the interface are buttons for 'Close' and 'Save'.

Steps and actions

A runbook consists of steps that are executed consecutively. A step consists of actions that start simultaneously. An action may consist of:

- An operation to be performed with a cloud server (**Failover server**, **Start server**, **Stop server**, **Failback server**). To define this operation, you need to choose the operation, the cloud server, and the operation parameters.
- A manual operation that you need to describe verbally. Once the operation is completed, a user must click the confirmation button to allow the runbook to proceed.
- Execution of another runbook. To define this operation, you need to choose the runbook.
A runbook can include only one execution of a given runbook. For example, if you added the action "execute Runbook A", you can add the action "execute Runbook B", but cannot add another action "execute Runbook A".

Note

In this product version a user has to perform a failback manually. A runbook shows the prompt when it is required.

Action parameters

All operations with cloud servers have the following parameters:

- **Continue if already done** (enabled by default)
This parameter defines the runbook behavior when the required operation is already done (for example, a failover has already been performed or a server is already running). When enabled,

the runbook issues a warning and proceeds. When disabled, the operation fails and the runbook fails.

- **Continue if failed** (disabled by default)

This parameter defines the runbook behavior when the required operation fails. When enabled, the runbook issues a warning and proceeds. When disabled, the operation fails and the runbook fails.

Completion check

You can add completion checks to the **Failover server** and **Start server** actions, to ensure that the server is available and provides the necessary services. If any of the checks fail, the action is considered failed.

- **Ping IP address**

The software will ping the production IP address of the cloud server until the server replies or the timeout expires, whichever comes first.

- **Connect to port** (443 by default)

The software will try to connect to the cloud server by using its production IP address and the port you specify, until the connection is established or the timeout expires, whichever comes first. This way, you can check if the application that listens on the specified port is running.

The default timeout is 10 minutes. You can change it if you wish.

15.11.3 Operations with runbooks

Note

The availability of this feature depends on the service quotas that are enabled for your account.

To access the list of operations, hover on a runbook and click the ellipsis icon. When a runbook is not running, the following operations are available:

- **Execute**
- **Edit**
- **Clone**
- **Delete**

Executing a runbook

Every time you click **Execute**, you are prompted for the execution parameters. These parameters apply to all failover and failback operations included in the runbook. The runbooks specified in the **Execute runbook** operations inherit these parameters from the main runbook.

- **Failover and failback mode**

Choose whether you want to run a test failover (by default) or a real (production) failover. The failback mode will correspond to the chosen failover mode.

- **Failover recovery point**

Choose the most recent recovery point (by default) or select a point in time in the past. If the latter is the case, the recovery points closest before the specified date and time will be selected for each server.

Stopping a runbook execution

During a runbook execution, you can select **Stop** in the list of operations. The software will complete all of the already started actions except for those that require user interaction.

Viewing the execution history

When you select a runbook on the **Runbooks** tab, the software displays the runbook details and execution history. Click the line corresponding to a specific execution to view the execution log.

Runbooks

Name ↑

Failback 3-2

Rb0 000

Runbook with ConfirmManualOperation

Runbook with ConfirmManualOperation

jk one server with checking port

New runbook (10)

Failover/Failback (centos-1) (Clone)

New runbook (9)

Runbook #009.

Runbook #010.

Rb0 000

Execute

Edit

Clone

Delete

Details

NameRb0 000

Description-

Execution history

Start and end time	Result	Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM	Failed	Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM	Failed	Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM	Completed	Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM	Completed	Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM	Completed	Test

16 Antimalware and web protection

Note

On Windows machines, the antimalware protection and URL filtering features require the installation of Agent for Antimalware protection and URL filtering. It will be installed automatically for protected workloads if the **Antivirus & Antimalware protection** or the **URL filtering module** is enabled in their protection plans.

Antimalware protection in Cyber Protection provides you with the following benefits:

- Top protection on all the stages: proactive, active, and reactive.
 - Four different antimalware technologies inside to provide the best of the breed multi-layered protection.
 - Management of Microsoft Security Essentials and Microsoft Defender Antivirus.
-

Note

The availability of this feature depends on the service quotas that are enabled for your account.

16.1 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: [Supported features by operating system](#).

Antivirus & Antimalware protection is supported and registered in Windows Security Center.

16.1.1 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

16.1.2 Scanning types

You can configure antivirus and antimalware protection to run constantly in the background or on demand.

Real-time protection

Note

The availability of this feature depends on the service quotas that are enabled for your account.

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:

- **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 machine system files.
- **Full scan** checks all files on your machine.

You can monitor the results of antimalware scanning in **Dashboard > Overview > [Recently affected](#)** widget.

16.1.3 Antivirus and antimalware protection settings

To learn how to create a protection plan with the **Antivirus & Antimalware protection** module, refer to "[Creating a protection plan](#)".

The following features can be configured for the **Antivirus & Antimalware protection** module.

Note

This section includes descriptions of the available settings for all supported operating systems. Check the table of Cyber Protect features supported by operating system for reference about the features applicable to your workloads: "Supported Cyber Protect features by operating system" (p. 18).

Some features might require additional licensing, depending on the applied licensing model.

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.

Default setting: **Enabled**.

For Windows, 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 protected machine. The agent version must be 12.0.4290 (released in October 2017) or later. For more information on how to update an agent, refer to "Updating agents" (p. 109).

For Linux, Active Protection is available for machines running:

- CentOS 6.10, 7.8 and later minor versions
- CloudLinux 6.10, 7.8 and later minor versions
- Ubuntu 16.04.7 and later minor versions

Agent for Linux must be installed on the protected machine. The agent version must be 15.0.26077 (released in December 2020) or later. For a list of supported Linux kernel versions, see <https://kb.acronis.com/acronis-cyber-protect-cloud-active-protection-for-linux-kernel-versions>.

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**.

Advanced antimalware

Note

The availability of this feature depends on the service quotas that are enabled for your account.

The **Advanced Antimalware** switch enables local signature-based engine. This engine uses enhanced database of virus signatures to improve the efficiency of antimalware detection in both quick and full scans.

Real-time protection is available only with the local signature-based engine.

Antivirus and Antimalware protection for macOS and Linux also requires the local signature-based engine. For Windows, Antivirus and Antimalware protection is available with or without this engine.

Network folder protection

The **Protect network folders mapped as local drives** setting defines whether Active protection protects from local malicious processes network folders that are mapped as local drives.

This setting 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 setting. The default folder is C:\ProgramData\Acronis\Restored Network Files. If this folder does not exist, it will be created. If you want to change this path, specify a local folder.

Network folders, including folders on mapped drives, are not supported.

Default setting: **Enabled**.

Server-side protection

This setting defines whether Active 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**.

Note

Server-side protection is not supported for Linux.

Setting trusted and blocked connections

To configure a trusted or blocked connection:

1. In the Server-side protection dialog, select a tab:
 - To specify connections that are allowed to modify any data, select the **Trusted** tab.
 - To specify connections that are not allowed to modify any data, select the **Blocked** tab.
2. Enter the following data:
 - Computer name and Account of the machine where the protection agent is installed.
For example, MyComputer\TestUser.
 - Host name of the machine that is allowed to connect to the machine with the agent.
3. Click the check mark to the right to save the connection definition.
4. To add more connections, click the **Add** button.

Self-protection

Self-protection prevents unauthorized changes to the software's own processes, registry records, executable and configuration files, and backups located in local folders. We do not recommend disabling this feature.

Default setting: **Enabled**.

Note

Self-protection is not supported for Linux.

Password protection

Password protection prevents unauthorized users or software from uninstalling Agent for Windows or modifying its components. These actions are only possible with a password that an administrator can provide.

A password is never required for the following actions:

- Updating the installation by running the setup program locally
- Updating the installation by using the Cyber Protection web console
- Repairing the installation

Default setting: **Disabled**

For more information about how to enable Password protection, refer to [Preventing unauthorized uninstallation or modification of agents](#).

Cryptomining process detection

This setting defines whether Active protection detects potential cryptomining malware.

Cryptomining malware degrades the performance of useful applications, increases electricity bills, may cause system crashes and even hardware damage due to abuse. To protect your workloads, we recommend that you add cryptomining malware to the **Harmful** processes list.

Default setting: **Enabled**.

Note

Cryptomining process detection is not supported for Linux.

Cryptomining process detection settings

In **Action on detection**, select the action that the software will perform when a cryptomining process 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 for keeping 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**.

For more information about this feature, refer to [Quarantine](#).

Behavior detection

Acronis Cyber Protection 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**.

Note

Behavior detection is not supported for Linux.

Behavior detection settings

In **Action on detection**, select the action that the software will perform when detecting a malware activity, and then click **Done**.

You can select one of the following:

- **Notify only**
The software will generate an alert about the process suspected of malware activity.
- **Stop the process**
The software will generate an alert and stop the process suspected of malware activity.
- **Quarantine**
The software will generate an alert, stop the process, and move the executable file to the quarantine folder.

Default setting: **Quarantine**.

Exploit prevention

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Exploit prevention detects and prevents infected processes from spreading and exploiting the software vulnerabilities on Windows systems. When an exploit is detected, the software can generate an alert and stop the process suspected of exploit activities.

Exploit prevention is available only with agent versions 12.5.23130 (21.08, released in August 2020) or later.

Default setting: **Enabled** for newly created protection plans, and **Disabled** for existing protection plans, created with previous agent versions.

Note

Exploit prevention is not supported for Linux.

Exploit prevention settings

You can select what should the program do when an exploit is detected, and which exploit prevention methods are applied by the program.

Under **Enabled Action on detection**, select what to do when an exploit is detected, and then click **Done**.

- **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.

Default setting: **Stop the process**

Under **Enabled exploit prevention techniques**, enable or disable the methods that you want to be applied, and then click **Done**.

You can select one of the following:

- **Memory protection**

Detects and prevents suspicious modifications of the execution rights on memory pages. Malicious processes apply such modifications to page properties, to enable the execution of shell codes from non-executable memory areas like stack and heaps.

- **Return-oriented programming (ROP) protection**

Detects and prevents attempts the ROP exploit technique that allows an attacker to execute code in the presence of security defenses, such as executable space protection and code signing. The attacker takes control over the call stack, and then hijacks the program control flow and executes malicious code.

- **Privilege escalation protection**

Detects and prevents attempts for elevation of privileges made by an unauthorized code or application. Privilege escalation is used by malicious code to gain full access of the attacked machine, and then perform critical and sensitive tasks. Unauthorized code is not allowed to access critical system resources or modify system settings.

- **Code injection protection**

Detects and prevents malicious code injection into remote processes. Code injection is used to hide malicious intent of an application behind clean or benign processes, to evade detection by antimalware products.

Default setting: **All methods are enabled**.

Note

Processes that are listed as trusted processes in the Exclusions list will not be scanned for exploits.

Allowing processes to modify backups

The **Allow specific processes to modify backups** setting is only available when the **Self-protection** setting is enabled.

It applies to files that have extensions .tibx, .tib, .tia, and are located in local folders.

This setting 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 setting 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 setting 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**.

Real-time protection

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Real-time protection constantly checks your machine system for viruses and other threats for the entire time that you system is powered on.

Default setting: **Enabled**.

Important

Real-time protection is available only when the local signature-based engine is turned on. For real-time protection, you need to enable both the **Real-time protection** switch and the **Advanced Antimalware** switch.

Configuring the action on detection for real-time protection

In **Action on detection**, select the action that the software will perform when a virus or other malicious threat is detected, and then click **Done**.

You can select one of the following:

- **Block and notify**

The software blocks the process and generates an alert about the process suspected of malware activities.

- **Quarantine**

The software generates an alert, stops the process, and moves the executable file to the quarantine folder.

Default setting: **Quarantine**.

Configuring the scan mode for real-time protection

In **Scan mode**, select the action that the software will perform when a virus or other malicious threat is detected, and then click **Done**.

You can select one of the following:

- **Smart on-access** – Monitors all system activities and automatically scans files when they are accessed for reading or writing, or whenever a program is launched.
- **On-execution** – Automatically scans only executable files when they are launched to ensure that they are clean and will not cause any damage to your computer or data.

Default setting: **Smart on-access**.

Schedule scan

You can define schedule according to which your machine will be checked for malware, by enabling the **Schedule scan** setting.

Action on detection:

- **Quarantine**

The software generates an alert and moves the executable file to the quarantine folder.

- **Notify only**

The software generates an alert about the process that is suspected to be malware.

Default setting: **Quarantine**.

Scan mode:

- **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.

You can schedule both **Quick** and **Full** scan in one protection plan.

Default setting: **Quick** and **Full** scan are scheduled.

Schedule the task run using the following events:

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.

Note

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

Schedule type:

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

Start at – Select the exact time when the task will run.

Run within a date range – Set a range in which the configured schedule will be effective.

Start conditions – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "[Start conditions](#)". 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.

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 pens and external hard drives)
- **CDs/DVDs**

Note

Scan removable drives is not supported for Linux.

Exclusions

To minimize the resources used by the heuristic analysis and to eliminate the so-called false positives when a trusted program is considered a ransomware or other malware, you can define the following settings:

On the **Trusted** tab, you can specify:

- Processes that will never be considered as malware. Processes signed by Microsoft are always trusted.
- Folders in which file changes will not be monitored.
- Files and folders in which the scheduled scan will not be performed.

On the **Blocked** tab, you can specify:

- Processes that will always be blocked. These processes will not be able to start as long as Active Protection or Antimalware Protection is enabled on the machine.
- Folders in which any processes will be blocked

Default setting: No exclusions are defined by default.

You can use a wildcard (*) to add items to the exclusion lists.

You can also use variables to add items to the exclusion lists. Note the following limitations:

- For Windows, only SYSTEM variables are supported. User specific variables, for example, %USERNAME%, %APPDATA% are not supported. Variables with {username} are not supported. For more information, see <https://ss64.com/nt/syntax-variables.html>.
- For macOS, environment variables are not supported.
- For Linux, environment variables are not supported.

Examples of supported formats:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\ *

16.2 Active Protection in the Cyber Backup Standard edition

In Cyber Backup Standard edition, 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 all other editions of the Cyber Protection service, Active Protection is part of the Antivirus and Antimalware protection module.

Default setting: **Enabled**.

For Windows, 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 protected machine. The agent version must be 12.0.4290 (released in October 2017) or later. For more information on how to update an agent, refer to "Updating agents" (p. 109).

For Linux, Active Protection is available for machines running:

- CentOS 6.10, 7.8 and later minor versions
- CloudLinux 6.10, 7.8 and later minor versions
- Ubuntu 16.04.7 and later minor versions

Agent for Linux must be installed on the protected machine. The agent version must be 15.0.26077 (released in December 2020) or later. For a list of supported Linux kernel versions, see <https://kb.acronis.com/acronis-cyber-protect-cloud-active-protection-for-linux-kernel-versions>.

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, as specified in the protection plan.

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.

16.2.1 Active protection settings in Cyber Backup Standard

In the Cyber Backup Standard edition, you can configure the following Active Protection features:

- [Action on detection](#)
- [Self-protection](#)
- [Network folder protection](#)
- [Server-side protection](#)
- [Cryptomining process detection](#)
- [Exclusions](#)

Note

Active Protection for Linux supports the following settings: Action on detection, Network folder protection, and Exclusions. Network folder protection is always on and not configurable.

Action on detection

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**.

Self-protection

Self-protection prevents unauthorized changes to the software's own processes, registry records, executable and configuration files, and backups located in local folders. We do not recommend disabling this feature.

Default setting: **Enabled**.

Note

Self-protection is not supported for Linux.

Password protection

Password protection prevents unauthorized users or software from uninstalling Agent for Windows or modifying its components. These actions are only possible with a password that an administrator can provide.

A password is never required for the following actions:

- Updating the installation by running the setup program locally
- Updating the installation by using the Cyber Protection web console
- Repairing the installation

Default setting: **Disabled**

For more information about how to enable Password protection, refer to [Preventing unauthorized uninstallation or modification of agents](#).

Network folder protection

The **Protect network folders mapped as local drives** setting defines whether Active protection protects from local malicious processes network folders that are mapped as local drives.

This setting 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 setting. The default folder is C:\ProgramData\Acronis\Restored Network Files. If this folder does not exist, it will be created. If you want to change this path, specify a local folder. Network folders, including folders on mapped drives, are not supported.

Default setting: **Enabled**.

Server-side protection

This setting defines whether Active 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**.

Note

Server-side protection is not supported for Linux.

Setting trusted and blocked connections

To configure a trusted or blocked connection:

1. In the Server-side protection dialog, select a tab:
 - To specify connections that are allowed to modify any data, select the **Trusted** tab.
 - To specify connections that are not allowed to modify any data, select the **Blocked** tab.
2. Enter the following data:
 - Computer name and Account of the machine where the protection agent is installed.
For example, MyComputer\TestUser.
 - Host name of the machine that is allowed to connect to the machine with the agent.
3. Click the check mark to the right to save the connection definition.
4. To add more connections, click the **Add** button.

Cryptomining process detection

This setting defines whether Active protection detects potential cryptomining malware.

Cryptomining malware degrades the performance of useful applications, increases electricity bills, may cause system crashes and even hardware damage due to abuse. To protect your workloads, we recommend that you add cryptomining malware to the **Harmful** processes list.

Default setting: **Enabled**.

Note

Cryptomining process detection is not supported for Linux.

Cryptomining process detection settings

In **Action on detection**, select the action that the software will perform when a cryptomining process 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**.

Exclusions

To minimize the resources used by the heuristic analysis and to eliminate the so-called false positives when a trusted program is considered a ransomware or other malware, you can define the following settings:

On the **Trusted** tab, you can specify:

- Processes that will never be considered as malware. Processes signed by Microsoft are always trusted.
- Folders in which file changes will not be monitored.
- Files and folders in which the scheduled scan will not be performed.

On the **Blocked** tab, you can specify:

- Processes that will always be blocked. These processes will not be able to start as long as Active Protection or Antimalware Protection is enabled on the machine.
- Folders in which any processes will be blocked

Default setting: No exclusions are defined by default.

You can use a wildcard (*) to add items to the exclusion lists.

You can also use variables to add items to the exclusion lists. Note the following limitations:

- For Windows, only SYSTEM variables are supported. User specific variables, for example, %USERNAME%, %APPDATA% are not supported. Variables with {username} are not supported.

For more information, see <https://ss64.com/nt/syntax-variables.html>.

- For macOS, environment variables are not supported.
- For Linux, environment variables are not supported.

Examples of supported formats:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\ *

16.3 URL filtering

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Malware is often distributed by malicious or infected sites and uses the so called [Drive-by download](#) method of infection.

The URL filtering functionality allows you to protect machines from threats like malware and phishing coming from the Internet. You can protect your organization by blocking user access to the websites that may have malicious content. The URL filtering database also includes data about the websites having disputed information about COVID-19, scam and phishing URLs. Thus, such websites will be automatically blocked by the system when a user tries to open them.

The URL filtering also allows you to control web usage to comply with the external regulations and internal company policies. You can configure access to the websites depending on the category they relate to. The URL filtering supports currently 44 website categories and allows to manage access to them.

Currently, the HTTP/HTTPS connections on Windows machines will be checked by the protection agent.

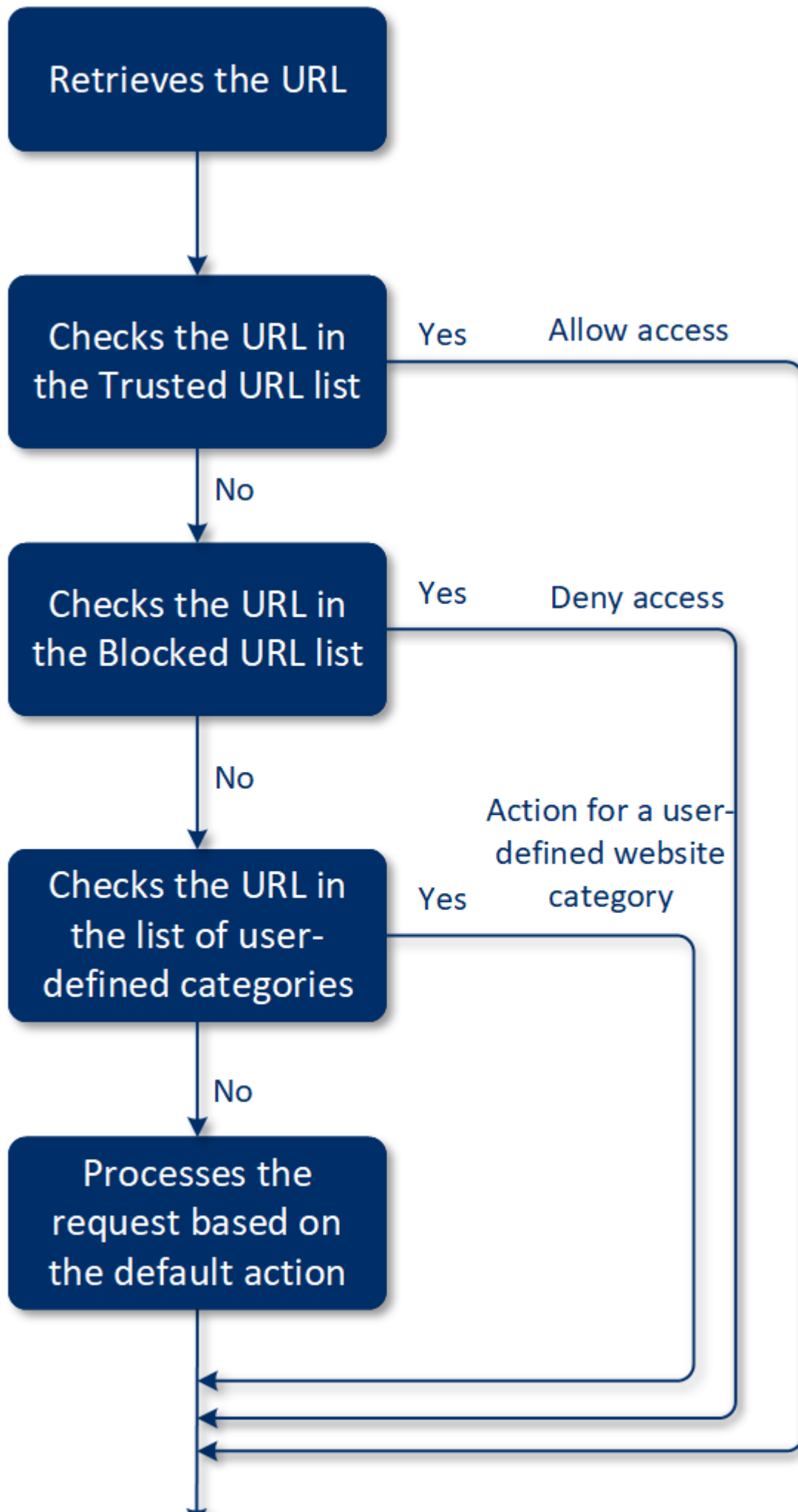
Note

To prevent possible compatibility issues with Cyber Protection agent builds 15.0.26692 (release C21.03 HF1) and earlier, the URL filtering functionality will be automatically disabled if another antivirus solution is detected, or if the Windows Security Center service is not present on the system.

In later Cyber Protection agents, the compatibility issues are resolved so URL filtering is always enabled according to the policy.

16.3.1 How it works

A user enters a URL link in a browser. The Interceptor gets the link and sends it to the protection agent. The agent gets the URL, parses it, and then checks the verdict. The Interceptor redirects a user to the page with the message with available actions to manually proceed to the requested page.




16.3.2 URL filtering configuration workflow

Generally, the URL filtering configuration consists of the following steps:

1. You [create a protection plan](#) with the enabled **URL filtering** module.
2. Specify the URL filtering settings (see below).
3. Assign the protection plan to the machines.

To check which URLs have been blocked, go to **Dashboard > Alerts**.

 **Malicious URL was blocked**

Oct 26, 2019, 04:43 PM

Web Protection blocked a malicious URL.

Device	Win2012-FileServer
Plan name	New protection plan
Threat name	MALWARE.BlockedURL
URL	xanhcity.vn/nofij3ksa/pin/10365911.xls

Clear

16.3.3 URL filtering settings

The following settings can be specified for the URL filtering module.

Malicious website access

Specify which action will be performed when a user opens a malicious website:

- **Block** – block access to the malicious website. A user will not be able to access the website and a warning alert will be generated.
- **Always ask user** – ask a user whether to proceed to the website anyway or return back.

Categories to filter

There are 44 website categories for which you can configure access:

- **Allow** – allow access to websites related to the selected category.
- **Deny** – deny access to websites related to the selected category.

By default all categories are allowed.

Show all notifications for blocked URLs by categories – if enabled, you will get all notifications shown in the tray for blocked URLs by categories. If a website has several sub-domains, then the system also generates notifications for them, therefore the number of notifications may be big.

In the table below, you can find category descriptions:

	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.
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	<p>This category covers websites that provide online games, typically based on Adobe Flash or Java applets. It does not matter for detection whether the game is free or requires a subscription, however, casino-style websites are detected in the Gambling category.</p> <p>This category does not cover:</p> <ul style="list-style-type: none"> • 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	<p>This category is a broad category related to hate, violence and racism, and it is intended to block the following categories of websites:</p> <ul style="list-style-type: none"> • Websites belonging to terrorist organizations • Websites with racist or xenophobic content • 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	<p>This category covers websites related to software piracy, including:</p> <ul style="list-style-type: none"> • 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.
25	Online dating	<p>This category covers online dating websites – paid and free - where users can search for other people by using some criteria. They may also post their profiles to let others search them. This category includes both free and paid online dating websites.</p> <p>Because most of the popular social networks can be used as online dating websites, some popular websites like Facebook are also detected in this category. It's recommended to use this category with the Social networks category.</p>
26	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.
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	<p>This category covers websites discussing, sharing, and offering violent cartoons or manga that may be inappropriate for minors due to violence, explicit language, or sexual content.</p> <p>This category doesn't cover the websites that offer mainstream cartoons such as "Tom and Jerry".</p>
42	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	<p>This category covers websites that provide web proxy services. This is a “browser inside a browser” type website when a user opens a web page, enters the requested URL into a form, and clicks “Submit”. The web proxy site downloads the actual page and shows it inside the user browser.</p> <p>These are the following reasons this type is detected (and might need to be blocked):</p> <ul style="list-style-type: none"> • 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 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. <p>Since the SDK analyzes the HTML page (if provided), and not just URLs, for some categories the SDK will still be able to detect the content. Other reasons, however, cannot be avoided just by using the SDK.</p>

Exclusions

Domain names or IP addresses that are known as safe can be added to the list of trusted URLs. Domain names or IP addresses that represent a threat can be added to the list of blocked URLs.

To add a host to the trusted URLs, click **Add** on the **Trusted** tab and specify the specific domain name or IP address.

To add a host to the blocked URLs, click **Add** on the **Blocked** tab and specify the specific domain name or IP address.

Note

All addresses from the domain that you entered will be treated as trusted or blocked. For example, if you entered xyz.com as a trusted domain, all paths or sub-domains under xyz.com are treated as trusted.

Do not include the "www." prefix when you enter the domain name.

16.4 Microsoft Defender Antivirus and Microsoft Security Essentials

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Microsoft Defender Antivirus

Microsoft Defender Antivirus is a built-in antimalware component of Microsoft Windows that is delivered starting from Windows 8.

The Microsoft Defender Antivirus (WDA) module allows you to configure Microsoft Defender Antivirus security policy and track its status via the Cyber Protection service console.

This module is applicable for the machines on which Microsoft Defender Antivirus is installed.

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 Protection service console.

This module is applicable for the machines on which Microsoft Security Essentials is installed.

The settings for Microsoft Security Essentials are similar to the settings for Microsoft Defender Antivirus, but you cannot configure real-time protection, and cannot define exclusions via the Cyber Protection service console.

16.4.1 Schedule scan

Specify the schedule for scheduled scanning.

Scan mode:

- **Full** – a full check of all files and folders additionally to the items scanned in the quick scan. It required more machine resources for execution 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 for execution.

Define the time and day of 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 setting for Microsoft Defender Antivirus, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings>

16.4.2 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 actions will be taken.
- **Block** – block the detected malware.

For more details about the default actions settings for Microsoft Defender Antivirus, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings>

16.4.3 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 real-time protection settings for Microsoft Defender Antivirus, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings>

16.4.4 Advanced

Specify the advanced scan settings:

- **Scan archive files** – include archived files such as .zip or .rar files into 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 WDA user interface will not be available to a user. You can manage the WDA policies via Cyber Protection service console.
- **MAPS (Microsoft Active Protection Service)** – online community that helps you choose how to respond to potential threats.
 - **I don't want to join MAPS** – no information will be sent to Microsoft about the software that was detected.
 - **Basic membership** – basic information will be sent to Microsoft about the software that was detected.
 - **Advanced membership** – more detailed information will be sent to Microsoft about the software that was detected.

For more details, refer to <https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/>

For more details about the advanced settings for Microsoft Defender Antivirus, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings>

16.4.5 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 exclusion settings for Microsoft Defender Antivirus, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings>

16.5 Quarantine

Quarantine is a special isolated folder on a machine's hard disk where the suspicious files detected by Antivirus and 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.

16.5.1 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.

16.5.2 Managing quarantined files

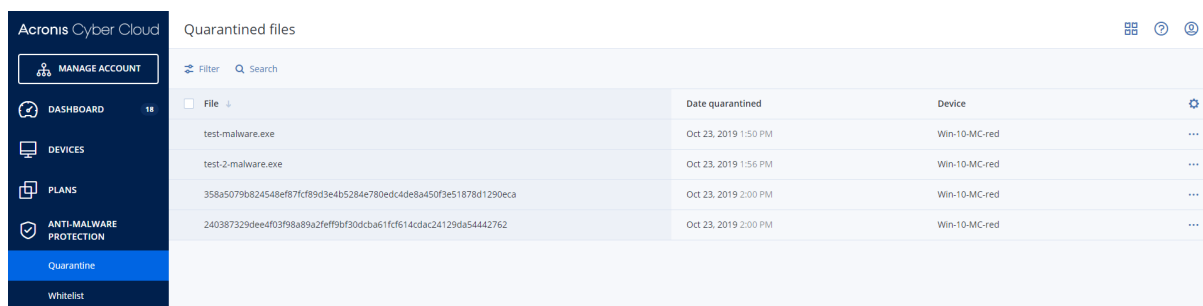
To manage the quarantined files, go to **Antimalware protection > Quarantine**. You will see a list with quarantined files from all machines.

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. You can delete all files with the same file hash. You can restore all files with the same file hash. Group the files by hash, select needed files and then delete them.
- **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. Note that the restored file will be added to the whitelist and skipped during further antimalware scans.



File	Date quarantined	Device
test-malware.exe	Oct 23, 2019 1:50 PM	Win-10-MC-red
test-2-malware.exe	Oct 23, 2019 1:56 PM	Win-10-MC-red
358a5079b824548ef877cf89d3e4b5284e780edc4de8a450f3e51878d1290eca	Oct 23, 2019 2:00 PM	Win-10-MC-red
240387329deedf03f98a89a2eff96f30dcba61fc614cdac24129da54442762	Oct 23, 2019 2:00 PM	Win-10-MC-red

16.5.3 Quarantine location on machines

The default location for quarantined files is:

For a Windows machine: %ProgramData%\%product_name%\Quarantine

For a Mac/Linux machine: /usr/local/share/%product_name%/quarantine

The quarantine storage is under the service provider's self-defense protection.

16.6 Corporate whitelist

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 Protection 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 is created for each customer, and is based only on this customer's data.

The whitelist can be enabled and disabled. When it is disabled, the files added to it are temporarily hidden.

Note

Only accounts with the administrator role (for example, Cyber Protection administrator; company administrator; partner administrator who acts on behalf of a company administrator; unit administrator) can configure and manage the whitelist. This functionality is not available for a read-only administrator account or a user account.

16.6.1 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](#).

2. In the whitelist settings, enable the **Automatic generation of whitelist** switch.

16.6.2 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 service console, go to **Antimalware protection > Whitelist**.
2. Click **Add file**.
3. Specify the path to the file, and then click **Add**.

16.6.3 Adding quarantined files to the whitelist

You can add files that are quarantined to the whitelist.

1. In the service console, go to **Antimalware protection > Quarantine**.
2. Select a quarantined file, and then click **Add to whitelist**.

16.6.4 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.

16.7 Antimalware scan of backups

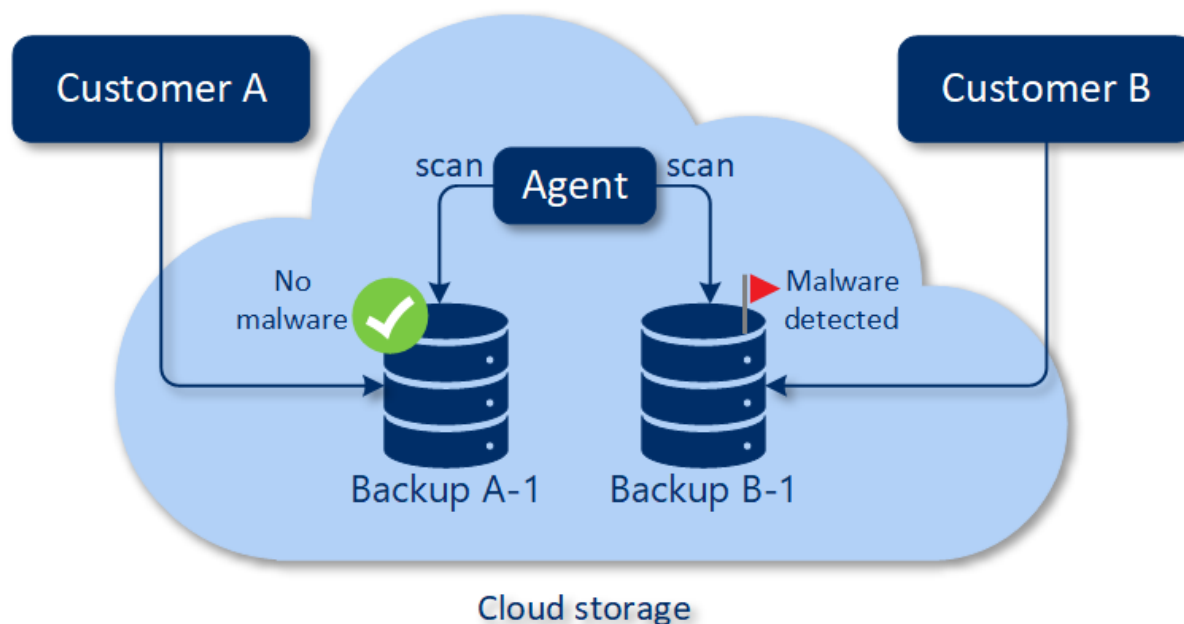
The backup scanning functionality allows you to prevent restoring infected files from backups. By using this functionality, you can check if your backups are clean (not infected by malware). The backup scanning functionality is supported only for Windows operating systems.

Backup scanning is performed by the cloud agent in the environment outside of an end-user machine – in the Acronis cloud. Every new backup scanning plan creates a new scanning task, the task is put in the common queue for the current data center and processed according to its order in

the queue. The time required for scanning depends on a backup size, thus, you may experience some delay after creating a backup scanning plan and its execution.

If the backup scanning was not performed, then the backups stay in the **Not scanned** status. After backup scanning was performed, the backups get one of the following statuses:

- **No malware**
- **Malware detected**



The backup scanning can be configured by using a backup scanning plan.

16.7.1 How to configure backup scanning in the cloud

Note the following:

- The supported backup types are "Entire machine" or "Disks/volumes" backups.
- Only volumes with the NTFS file system with GPT and MBR partitioning will be scanned.
- The supported backup location is cloud storage (currently, only Acronis hosted).
- The backups that have [CDP recovery points](#) can be selected for scanning but only regular recovery points (excluding CDP recovery points) will be scanned.
- When the CDP backup was selected for safe recovery of an entire machine, the machine will be safely recovered without the data in the CDP recovery point. To restore the CDP data, start the Files/folders recovery activity.

To configure backup scanning in the cloud, create a [backup scanning plan](#).

The results of backup scanning can be found on the dashboard in the "[Backup scanning details](#)" widget.

17 Protection of collaboration and communication applications

Zoom, Cisco Webex Meetings, Citrix Workspace, and Microsoft Teams are now widely used for video/web conferencing and communications. The Cyber Protection service allows you to protect your collaboration tools.

The protection configuration for Zoom, Cisco Webex Meetings, Citrix Workspace, and Microsoft Teams is similar. In the example below, we will consider configuration for Zoom.

To set up Zoom protection

1. [Install the protection agent](#) on the machine where the collaboration application is installed.
2. Log in to the service console and [apply a protection plan](#) that has 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

18 Vulnerability assessment and patch management

Vulnerability assessment (VA) is a process of identifying, quantifying, and prioritizing found vulnerabilities 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" (p. 455).
- macOS. For more information, see "Supported Apple and third-party products" (p. 456).
- Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure) machines. For more information, see "Supported Linux products" (p. 457).

Use the **Patch management** (PM) functionality to manage patches (updates) for applications and operating systems installed on your machines, and keep your systems up-to-date. In the patch management module you can automatically or manually approve update installations on your machines.

Patch management is supported for machines with the Windows operating systems. For more information, see "Supported Microsoft and third-party products" (p. 455).

18.1 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](#).
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 **Dashboard > Overview > Vulnerabilities / Existing vulnerabilities** widgets.

18.1.1 Supported Microsoft and third-party products

The following Microsoft products and third-party products for Windows operating systems are supported for vulnerability assessment:

Supported Microsoft products

Windows OS

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

Windows Server OS

- 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 OS related components

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio and Applications
- Components of operating system

Server applications

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Supported third-party products for Windows OS

Remote work becomes more and more wide-spread across the world, therefore collaboration and communication tools, VPN clients are now important to be always up-to-date and checked on possible vulnerabilities. The Cyber Protection service supports the vulnerability assessment and patch management for such applications.

Collaboration and communication tools, VPN clients

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

For more information about the supported third-party products for Windows OS, refer to <https://kb.acronis.com/content/62853>.

18.1.2 Supported Apple and third-party products

The following Apple products and third-party products for macOS are supported for vulnerability assessment:

Supported Apple products

macOS

- macOS 10.14.x and later

macOS built-in applications

- Safari, iTunes, and others.

Supported third-party products for macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox

- Opera
- Zoom
- Skype
- Thunderbird
- VLC media player

18.1.3 Supported Linux products

The following Linux distributions and versions are supported for VA:

- 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

18.1.4 Vulnerability assessment settings

To learn how to create a protection plan with the Vulnerability assessment module, refer to "[Creating a protection plan](#)". You can perform VA scanning by schedule or on demand (by using the **Run now** action in a protection plan).

You can specify the following settings in the Vulnerability assessment module.

What to scan

Define which software products you want to scan for vulnerabilities:

- Windows machines:
 - **Microsoft products**
 - **Windows third-party products** (for more information about the supported third-party products for Windows OS, refer to <https://kb.acronis.com/content/62853>)
- macOS machines:
 - **Apple products**
 - **macOS third-party products**
- Linux machines:
 - **Scan Linux packages**

Schedule

Define the schedule according to which to perform the vulnerability assessment scan on the selected machines:

Schedule the task run using the following events:

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.

Note

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

Schedule type:

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

Start at – Select the exact time when the task will run.

Run within a date range – Set a range in which the configured schedule will be effective.

Start conditions – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "[Start conditions](#)". 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.

18.1.5 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 service console, [create a protection plan](#) and enable the **Vulnerability assessment** module.
2. Specify the vulnerability assessment settings:
 - **What to scan** – select **Microsoft products**, **Windows third-party products**, or both.
 - **Schedule** – define the schedule for performing the vulnerability assessment.For more information about the **Schedule** options, see "Vulnerability assessment settings" (p. 457).
3. [Assign the plan to the Windows machines](#).

After a vulnerability assessment scan, you can see a [list of found vulnerabilities](#). You can process the information and decide which of the found vulnerabilities must be fixed.

To monitor the results of the vulnerability assessment, see the **Dashboard > Overview > Vulnerabilities / Existing vulnerabilities** widgets.

18.1.6 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 service 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. 457).
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 the **Dashboard > Overview > Vulnerabilities / Existing vulnerabilities** widgets.

18.1.7 Vulnerability assessment for macOS devices

You can scan macOS devices for operating system-level and application-level vulnerabilities.

To configure the vulnerability assessment for macOS devices

1. In the service console, [create a protection plan](#) and enable the **Vulnerability assessment** module.
2. Specify the vulnerability assessment settings:
 - **What to scan** – select **Apple products**, **macOS third-party products**, or both.
 - **Schedule** – define the schedule for performing the vulnerability assessment.For more information about the **Schedule** options, see "Vulnerability assessment settings" (p. 457).
3. [Assign the plan to the macOS devices](#).

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 the **Dashboard > Overview > Vulnerabilities / Existing vulnerabilities** widgets.

18.1.8 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): <ul style="list-style-type: none">• Critical: 9 - 10 CVSS• High: 7 - 9 CVSS• Medium: 3 - 7 CVSS• Low: 0 - 3 CVSS• None
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.

Acronis Cyber Cloud Manage account ANTI-MALWARE PROTECTION SOFTWARE MANAGEMENT Patches Vulnerabilities BACKUP STORAGE REPORTS SETTINGS 2 <small>Powered by Acronis AnyData Engine</small>		Vulnerabilities Filter Search Loaded: 30 / Total: 82				
<input type="checkbox"/>	Name ↓	Affected products ↓	Machines ↓	Severity ↓	Patches ↓	
	CVE-2015-16723	Microsoft Windows 8.1	1	CRITICAL	2	
	CVE-2015-0016	Microsoft Windows 8.1	1	CRITICAL	1	
	CVE-2014-4073	Microsoft Windows 8.1	1	CRITICAL	1	
<input type="checkbox"/>	CVE-2010-3190	Microsoft Visual Studio 2008	1	CRITICAL	1	
	CVE-2015-1756	Microsoft Windows 8.1	1	CRITICAL	1	
	CVE-2014-4121	Microsoft Windows 8.1	1	CRITICAL	1	
	CVE-2016-3236	Microsoft Windows 8.1	1	CRITICAL	1	
	CVE-2014-6324	Microsoft Windows 8.1	1	CRITICAL	1	

To start the vulnerability remediation process

1. In the service console, go to **Software management > Vulnerabilities**.
2. Select the vulnerability in the list and click **Install patches**. The vulnerability remediation wizard will open.
3. Select the patches to be installed on the selected machines. Click **Next**.
4. Select the machines that you want to install patches for.
5. Select if the machine reboot must be performed after patch installation:
 - **No** – reboot will never be initiated after the update installation.
 - **If required** – reboot is done only if it is required for applying the updates.
 - **Yes** – reboot will be always initiated after the updates. You can always specify the reboot delay.

Do not reboot until backup is finished – if the backup process is running, the machine reboot will be delayed until the backup is completed.

When ready, click **Install patches**.

As a result, the selected patches are installed on the selected machines.

18.2 Patch management

Note

The availability of this feature depends on the service quotas that are enabled for your account.

Use the patch management functionality to:

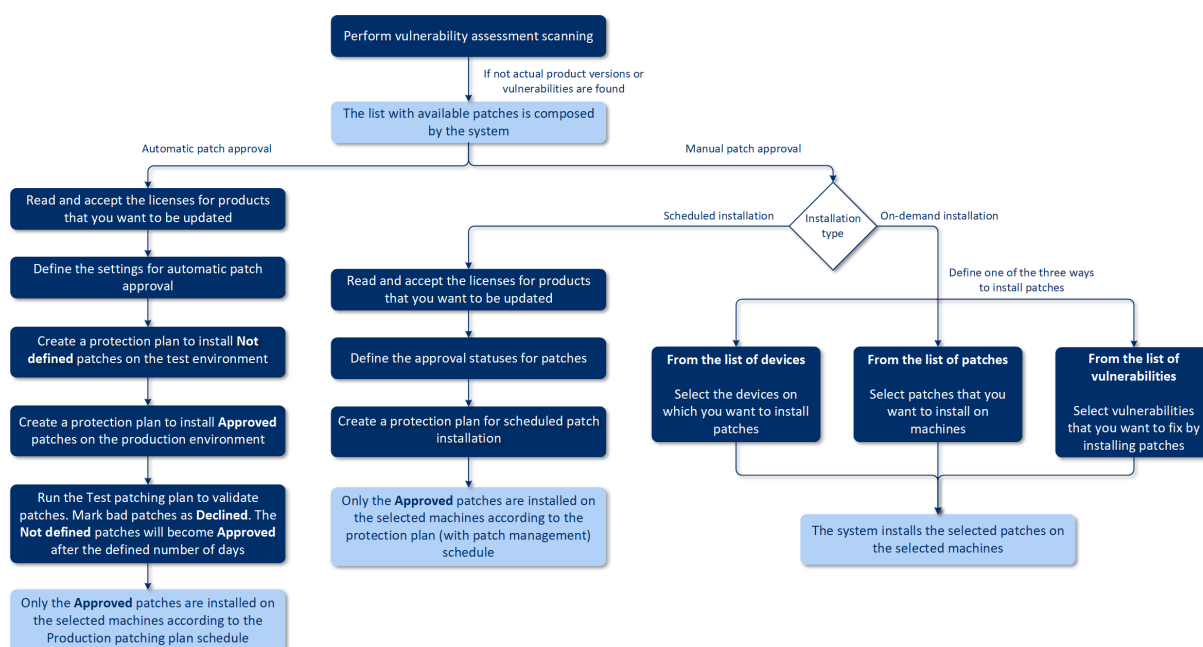
- install OS-level and application-level updates
- approve patches manually or automatically
- install patches on-demand or according to a schedule

- 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

Cyber Protection introduces peer-to-peer technology to minimize network bandwidth traffic. You can choose one or more dedicated agents that will download updates from the Internet and distribute them among other agents in the network. All agents will also share updates with each other as peer-to-peer agents.

18.2.1 How it works

You can configure either automatic or manual patch approval. In the scheme below, you can see the automatic and manual patch approval workflows.



1. First, you need to perform at least one **vulnerability assessment scan** by using the protection plan with the **Vulnerability assessment** module enabled. After the scan was performed, the lists of **found vulnerabilities** and **available patches** are composed by the system.
2. Then, you can configure the **automatic patch approval** or use **manual patch approval** approach.
3. Define how to install patches – according to a schedule or on-demand. There are three alternative ways to install patches on-demand:
 - Go to the list of patches (**Software management > Patches**) and install the necessary patches.

Name	Severity	Product	Installed versions	Version	Microsoft KB	Machines	Approval status
2020-03 Preview of Monthly Quality Rollup f.	MEDIUM	Windows Server ...	—	—	KB4541334	1	Not defined
Mozilla Thunderbird	MEDIUM	Thunderbird	68.5.0	68.6.0	—	1	Not defined
Notepad++ Team Notepad++	MEDIUM	Notepad++	7.8.4	7.8.5	—	1	Not defined

- Go to the list of vulnerabilities (**Software management** > **Vulnerabilities**) and start the remediation process which includes patch installation.
- Go to the list of devices (**Devices** > **All devices**), select the particular machines that you want to update, and install the patches on them.

You can monitor the results of the patch installation in **Dashboard** > **Overview** > **Patch installation history** widget.

18.2.2 Patch management settings

To learn how to create a protection plan with the patch management module, refer to "[Creating a protection plan](#)". By using the protection plan, you can specify what updates for Microsoft products and other third-party products for Windows OS to automatically install on the defined machines.

Note

The availability of this feature depends on the service quotas that are enabled for your account.

The following settings can be specified for the patch management module.

Microsoft products

To install the Microsoft updates on the selected machines, enable the **Update Microsoft products** option.

Select what updates you want to be installed:

- **All updates**
- **Only Security and Critical updates**
- **Updates of specific products:** you can define custom settings for different products. If you want to update specific products, for each product you can define which updates to install by [category](#), [severity](#), or [approval status](#).

Updates of specific products ✕

	Products	Category	Severity	Approval status
<input type="checkbox"/>	Windows Server 2012 R2 L...	Custom	Custom	Custom
<input checked="" type="checkbox"/>	Windows Server 2012 R2	ServicePacks, Upd...	Critical, High, Medi...	Approved
<input checked="" type="checkbox"/>	Windows Server 2012	CriticalUpdates	Critical, High	Approved
<input type="checkbox"/>	Windows Server 2016 and ...	—	—	—
<input checked="" type="checkbox"/>	Windows Server 2016	SecurityUpdates	Critical	Approved

[Reset to default](#)
Cancel
Save

Windows third-party products

To install the third-party updates for Windows OS on the selected machines, enable the **Windows third-party products** option.

Select what updates you want to be installed:

- **Only last major updates** allows you to install the latest available version of the update.
- **Only last minor updates** allows you to install the minor version of the update.
- **Updates of specific products:** you can define custom settings for different products. If you want to update specific products, for each product you can define which updates to install by [category](#), [severity](#), or [approval status](#).

Updates of specific products ✕

	Products	Category	Severity	Approval status
<input type="checkbox"/>	Adobe Reader	—	—	—
<input type="checkbox"/>	Adobe Flash Player for Chr...	—	—	—
<input type="checkbox"/>	Adobe Flash Player for Fire...	—	—	—
<input checked="" type="checkbox"/>	Oracle Java Runtime Envir...	Major updates	Critical	Approved
<input checked="" type="checkbox"/>	Mozilla Firefox	Minor updates	All	Approved
<input type="checkbox"/>	Google Chrome	—	—	—

[Reset to default](#)
Cancel
Save

Schedule

Define the schedule according to which the updates will be installed on the selected machines.

Schedule the task run using the following events:

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.

Note

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

Schedule type:

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

Start at – Select the exact time when the task will run.

Run within a date range – Set a range in which the configured schedule will be effective.

Start conditions – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "[Start conditions](#)". 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.

Reboot after update – define whether reboot is initiated after installing updates:

- **Never** – reboot will never be initiated after the updates.
- **If required** – reboot is done only if it is required for applying the updates.
- **Always** – reboot will be always initiated after the updates. You can always specify the reboot delay.

Do not reboot until backup is finished – if the backup process is running, the machine reboot will be delayed until the backup is completed.

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 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.

18.2.3 Managing list of patches

After vulnerability assessment scanning was done, you will find the available patches in **Software management > Patches**.

Name	Description
Name	The name of the patch
Severity	The severity of the patch: <ul style="list-style-type: none"> • Critical • High • Medium • Low • None
Vendor	The vendor of the patch
Product	Product for which the patch is applicable
Installed versions	Product versions that are already installed
Version	Version of the patch
Category	The category to which the patch belongs: <ul style="list-style-type: none"> • Critical update – broadly released fixes for specific problems addressing critical, non-security related bugs. • Security update – broadly released fixes for specific products addressing security

	<p>issues.</p> <ul style="list-style-type: none"> • 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.
Microsoft KB	If the patch for Microsoft product, the KB article ID is provided
Release date	The date when the patch was released
Machines	Number of affected machines
Approval status	<p>The approval status is mainly needed for automatic approval scenario and to be able to define in the protection plan which updates to install by status.</p> <p>You can define one of the following statuses for a patch:</p> <ul style="list-style-type: none"> • 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 • Not defined – the patch status is unclear and should be validated
License agreement	<ul style="list-style-type: none"> • Read and accept • Disagreed. If you disagree with the license agreement, then the patch status becomes Declined and it will not be installed
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

18.2.4 Automatic patch approval

Automatic patch approval allows you to make the process of installing updates on machines easier. Let's consider the example how it works.

How it works

You should have two environments: test and production. The test environment is used for testing the patch installation and ensuring that they do not break anything. After you tested patch installation on the test environment, you can automatically install these safe patches on the production environment.

Configuring automatic patch approval

To configure automatic patch approval

1. For each vendor whose products you are planning to update, you must read and accept the license agreements. Otherwise, automatic patch installation will not be possible.
2. Configure the settings for automatic approval.
3. [Prepare the protection plan](#) (for example, "Test patching") with the enabled **Patch management** module and apply it to the machines in the test environment. Specify the following condition of patch installation: the patch approval status must be **Not defined**. This step is needed to validate the patches and check if the machines work properly after patch installation.
4. [Prepare the protection plan](#) (for example, "Production patching") with the enabled **Patch management** module and apply it to the machines in the production environment. Specify the following condition of patch installation: the patch status must be **Approved**.
5. Run the Test patching plan and check the results. The approval status for those machines that have no issues can be preserved as **Not defined** while the status for machines working incorrectly must be set to **Declined**.
6. According to the number of days set in the **Automatic approval** option, those patches that were **Not defined** will become **Approved**.
7. When the Production patching plan is launched, only those patches that are **Approved** will be installed on the production machines.

The manual steps are listed below.

Step 1. Read and accept the license agreements for the products that you want to update

1. In the service console, go to **Software management > Patches**.
2. Select the patch, then read and accept the license agreement.

Step 2. Configure the settings for automatic approval

1. In the service console, go to **Software management > Patches**.
2. Click **Settings**.
3. Enable the **Automatic approval** option and specify the number of days. This means that after the specified number of days starting from the first attempt of patch installation, the patches with the status **Not defined** will become **Approved** automatically.

For example, you specified 10 days. You performed the Test patching plan for test machines and installed patches. Those patches that broke the machines, you marked as **Declined** while the rest of patches stay as **Not defined**. After 10 days passed, the patches in the **Not defined** status will be automatically switched to **Approved**.

4. Enable the **Automatically accept the license agreements** option. This is needed for automatic license acceptance during patch installation, no confirmation is required from a user.

Step 3. Prepare the Test patching protection plan

1. In the service console, go to **Plans > Protection**.
2. Click **Create plan**.
3. Enable the **Patch management** module.
4. Define which updates to install for Microsoft and third-party products, schedule, and pre-update backup. For more details about these settings, refer to "[Patch management settings](#)".

Important

For all the products to be updated, define **Approval status** as **Not defined**. When the time to update comes, the agent will install only **Not defined** patches on the selected machines in the test environment.

Updates of specific products ✕

<input checked="" type="checkbox"/>	Products ↓	Category	Severity	Approval status
<input checked="" type="checkbox"/>	Products ↓	Custom ↓	Custom ↓	Not defined ↓
<input checked="" type="checkbox"/>	Active Directory Rights Ma...	CriticalUpdates, Se... ↓	Critical ↓	Not defined ↓
<input checked="" type="checkbox"/>	Antigen for Exchange/SMTP	None ↓	All ↓	Not defined ↓
<input checked="" type="checkbox"/>	ASP.NET Web Frameworks	Updates ↓	Critical, High, Medi... ↓	Not defined ↓
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	None ↓	All ↓	Not defined ↓
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	None ↓	All ↓	Not defined ↓

[Reset to default](#) Cancel Save

Step 4. Prepare the Production patching protection plan

1. In the service console, go to **Plans > Protection**.
2. Click **Create plan**.
3. Enable the **Patch management** module.
4. Define which updates to install for Microsoft and third-party products, schedule, and pre-update backup. For more details about these settings, refer to "[Patch management settings](#)".

Important

For all the products to be updated, define **Approval status** as **Approved**. When the time to update comes, the agent will install only **Approved** patches on the selected machines in the production environment.

Updates of specific products ✕

<input checked="" type="checkbox"/>	Products ↓	Category	Severity	Approval status
<input checked="" type="checkbox"/>	Products ↓	Custom ↓	Custom ↓	Approved ↓
<input checked="" type="checkbox"/>	Active Directory Rights Ma...	CriticalUpdates, Se... ↓	Critical ↓	Approved ↓
<input checked="" type="checkbox"/>	Antigen for Exchange/SMTP	All ↓	All ↓	Approved ↓
<input checked="" type="checkbox"/>	ASP.NET Web Frameworks	Updates ↓	Critical, High, Medi... ↓	Approved ↓
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	All ↓	All ↓	Approved ↓
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	All ↓	All ↓	Approved ↓

[Reset to default](#) Cancel Save

Step 5. Run the Test patching protection plan and check the results

1. Run the Test patching protection plan (by schedule or on-demand).
2. After that, check which of the installed patches are safe and which are not.
3. Go to **Software management > Patches** and set the **Approval status** as **Declined** for those patches that are not safe.

18.2.5 Manual patch approval

The manual patch approval process is the following:

1. In the service console, go to **Software management > Patches**.
2. Select the patches that you want to install, then read and accept the license agreements.
3. Set **Approval status** to **Approved** for the patches that you approve for installation.
4. Create a [protection plan with the enabled Patch management](#) module. You can either configure the schedule or launch the plan on-demand by clicking **Run now** in the patch management module settings.

As a result, only the approved patches will be installed on the selected machines.

18.2.6 On-demand patch installation

On-demand patch installation can be done in three ways according to your preferences:

- Go to the list of patches (**Software management > Patches**) and install the necessary patches.
- Go to the list of vulnerabilities (**Software management > Vulnerabilities**) and start the remediation process which includes patch installation as well.
- Go to the list of devices (**Devices > All devices**), select the particular machines that you want to update, and install patches on them.

Let's consider patch installation from the list of patches:

1. In the service console, go to **Software management > Patches**.

2. Accept the license agreements for the patches that you want to install.

3. Select the patches that you want to install and click **Install**.

4. Select the machines on which patches must be installed.

If you want to have a rollback option in case of patch installation damages the system, select the **Run backup before installing software updates** option. The system checks right away if there is a protection plan with the Backup module enabled (the entire machine backup is required). If there is no such protection plan assigned to the machine, then such machines are marked with the red icon. You can unselect these machines and proceed.

5. Define whether reboot is initiated after installing patches:

- **Never** – reboot will never be initiated after the patches.
- **If required** – reboot is done only if it is required for applying the patches.
- **Always** – reboot will be always initiated after the patches. You can always specify the reboot delay.

Do not reboot until backup is finished – if the backup process is running, the machine reboot will be delayed until the backup is completed.

6. Click **Install patches**.

The selected patches will be installed on the selected machines.

18.2.7 Patch lifetime in the list

To keep the list of patches up-to-date, go to **Software management > Patches > Settings** and specify the **Lifetime in list** option.

The **Lifetime in list** option defines how long will the detected available patch be kept in the list of patches. Generally, the patch is removed from the list if it is successfully installed on all the machines where its absence is detected or the defined time lapses.

- **Forever** – the patch always stays in the list.
- **7 days** – the patch is removed if after its first installation seven days passed.

For example, you have two machines where patches must be installed. One of them is online, another – offline. The patch was installed on the first machine. After 7 days, the patch will be removed from the list of patches even if it is not installed on the second machine because it was offline.

- **30 days** – the patch is removed if after its first installation thirty days passed.

19 Software inventory

The software inventory feature enables you to view all the software applications that are available on all Windows and macOS devices with Cyber Protect (Essentials, Standard, or Advanced) licenses.

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.

19.1 Enabling the software inventory scanning

When software inventory scanning is enabled on devices with assigned Cyber Protect license and service quota, the system automatically collects the software data every 12 hours.

The Software inventory scanning feature is enabled by default, but you can change the setting when necessary.

Note

Customer tenants can enable or disable the software inventory scanning. Unit tenants can only view the software inventory scanning settings, but cannot change them.

To enable the software inventory scanning

1. In the service console, go to **Settings**.
2. Click **Protection**.
3. Click **Inventory scanning**.
4. Enable the **Software inventory scanning** module by clicking the switch next to the module name.

To disable the software inventory scanning

1. In the service console, go to **Settings**.
2. Click **Protection**.
3. Click **Inventory scanning**.
4. Disable the **Software inventory scanning** module by clicking the switch next to the module name.

19.2 Running a software inventory scan manually

You can manually run a software inventory scan from the **Software inventory** screen, or from the **Software** tab in the **Inventory** screen.

Prerequisites

- The device uses Windows or macOS operating system.
- The device has a Cyber Protect license.

To run a software inventory scan from the Software inventory screen

1. In the service console, go to **Software management**.
2. Click **Software inventory**.
3. In the **Group by:** drop-down field, select **Devices**.
4. Find the device which you want to scan, and click **Scan now**.

To run a software inventory scan from the Software tab in the Inventory screen

1. In the service console, go to **Devices**.
2. Click the device which you want to scan, and click **Inventory**.
3. In the **Software** tab, click **Scan now**.

19.3 Browsing the software inventory

You can view and browse the data for all software applications that are available on all company devices.

Prerequisites

- The devices use Windows or macOS operating system.
- The devices have a Cyber Protect license.
- Software inventory scan on the devices has finished successfully.

To view all software applications that are available on all Windows and macOS company devices

1. In the service 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.

Column	Description
Status	Status of the application. <ul style="list-style-type: none"> • 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 who installed the application.
System type	For Windows devices only. Bit type of the application. <ul style="list-style-type: none"> • 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 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

Filter	Description
	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 you want to open.
 - In the drop-down field, select the page number of the page you want to open.

19.4 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, as well as 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 a Cyber Protect license.
- Software inventory scan on the device has finished successfully.

To view the software inventory of a single device from the Software Inventory screen

1. In the service console, go to **Software management**.
2. Click **Software inventory**.
3. In the **Group by:** drop-down field, select **Devices**.
4. Find the device you want to inspect using one of the following options.
 - Find the device using the **Filter**:
 - a. Click **Filter**.
 - b. In the **Device name** field, select the name of the device you want to view.
 - c. Click **Apply**.
 - Find the device using the dynamic **Search**:
 - a. Click **Search**.
 - b. Type the full device name or part of the device name.

To view the software inventory of a single device from Devices screen

1. In the service console, go to **Devices**.
2. Click the device which you want to view, and click **Inventory**.

3. Click the **Software** tab.

20 Hardware inventory

The hardware inventory feature enables you to 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 Virtuozzo Hybrid Infrastructure. For more information about the supported versions of the virtualization platforms, see "Supported virtualization platforms" (p. 29).

Note

The Hardware inventory feature for virtual machines is not supported in the Cyber Protect legacy editions.

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 company devices
- view detailed information about a hardware component.

20.1 Enabling 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.

The hardware inventory scanning feature is enabled by default, but you can change the setting when necessary.

Note

Customer tenants can enable or disable the hardware inventory scanning. Unit tenants can only view the hardware inventory scanning settings, but cannot change them.

To enable the hardware inventory scanning

1. In the service console, go to **Settings**.
2. Click **Protection**.
3. Click **Inventory scanning**.
4. Enable the **Hardware inventory scanning** module by clicking the switch next to the module name.

To disable the hardware inventory scanning

1. In the service console, go to **Settings**.
2. Click **Protection**.
3. Click **Inventory scanning**.
4. Disable the **Hardware inventory scanning** module by clicking the switch next to the module name.

20.2 Running a hardware inventory scan manually

You can manually run 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

- (For all devices) The device uses a Windows or macOS operating system.
- (For all devices) The devices have a license that supports the Hardware inventory feature. Note that the Hardware inventory feature for virtual machines is not supported in the Cyber Protect legacy editions.
- (For all devices) A protection agent is installed on the device.
- (For virtual machines) The machine runs on one of the supported virtualization platforms. For more information, see "Hardware inventory" (p. 477).

To run a hardware inventory scan on a single device

1. In the service console, go to **Devices**.
2. Click the device which you want to scan, and click **Inventory**.
3. In the **Hardware** tab, click **Scan now**.

20.3 Browsing the hardware inventory

You can view and browse the data for all hardware components that are available on all company devices.

Prerequisites

- (For all devices) The devices use Windows or macOS operating system.
- (For all devices) The devices have a license that supports the Hardware inventory feature. Note that the Hardware inventory feature for virtual machines is not supported in the Cyber Protect legacy editions.
- (For all devices) A protection agent is installed on the device.
- (For all devices) Hardware inventory scan on the devices has finished successfully.
- (For virtual machines) The machine runs on one of the supported virtualization platforms. For more information, see "Hardware inventory" (p. 477).

To view all hardware components that are available on the Windows and macOS company devices

1. In the service console, go to **Devices**.
2. In the **View:** drop-down field, select **Hardware**.

Note

The view is a set of columns which determines what data is visible in the screen. The predefined views are **Standard** and **Hardware**. You can create and save custom views which 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. <ul style="list-style-type: none">• Completed.• Not started.• Not supported. status is shown for workloads for which hardware inventory functionality is not supported, i.e. virtual machines, mobile devices, Linux devices.• Update agent. shown in case the outdated version of agent is installed on the device. Clicking on this action will redirect to Settings > Agents page, where admin can perform the agent update.• Upgrade quota. Clicking on it will open a dialog where admin can switch the current license to one of other available for tenant licenses

Column	Description
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.
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. To add columns in the table, click the column options icon, and select the columns that you want to be visible in the table.
4. 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. To sort the data in an ascending order, click a column name.

20.4 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

- (For all devices) The device uses Windows or macOS operating system.
- (For all devices) The devices have a license that supports the Hardware inventory feature. Note that the Hardware inventory feature for virtual machines is not supported in the Cyber Protect legacy editions.
- (For all devices) A protection agent is installed on the device.
- (For all devices) Hardware inventory scan on the device has finished successfully.
- (For virtual machines) The machine runs on one of the supported virtualization platforms. For more information, see "Hardware inventory" (p. 477).

To view the detailed information about the hardware of a specific device

1. In the service 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.

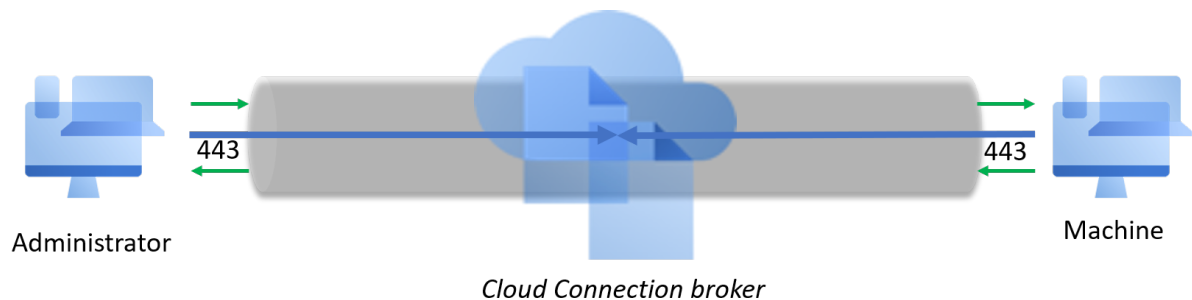
Hardware component	Information displayed
Motherboard	Name, manufacturer, model, and serial number of the motherboard of the device.
Processors	Manufacturer, model, max clock speed, and number of cores of each processor of the device.
Memory	Capacity, manufacturer, and serial number of the memory of the device.

Hardware component	Information displayed
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, BIOS version, boot device, system locale, and time zone of the system.

21 Remote desktop access

21.1 Remote access (RDP and HTML5 clients)

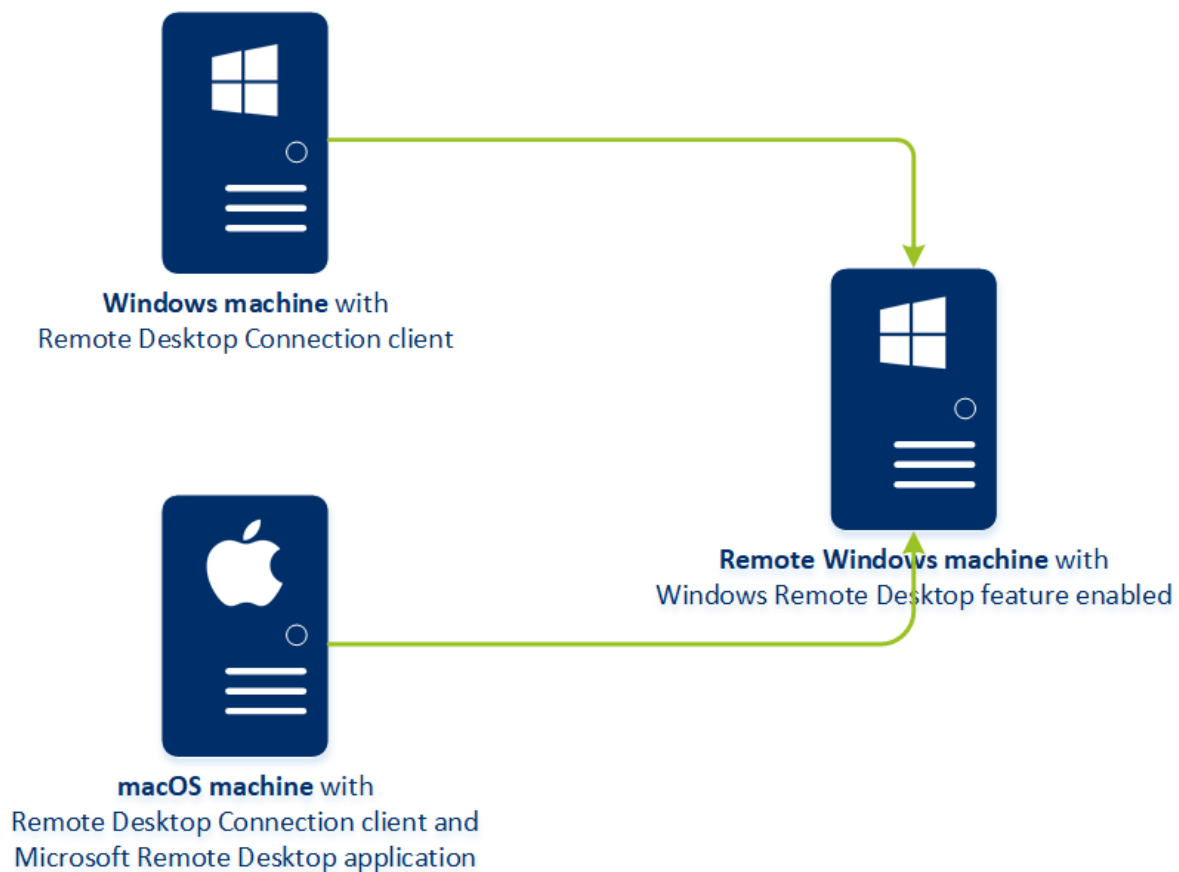
Cyber Protection provides you with remote access capability. You can connect and manage your end user machines through a remote connection. You can copy and paste text to and from the remote machine with the HTML5 client. With the RDP client, you can copy and paste text and files. This allows you to easily assist your end users in resolving issues on their machines.



Prerequisites:

- A remote machine is registered in Cyber Protection and the protection agent is installed.
- The Cyber Protect quota exists or was already acquired for a machine.
- For RDP connections, the Remote Desktop Connection client is installed on a machine from which the connection is launched.

An RDP session can be established from both Windows and macOS machines. An HTML5 remote connection session can be established from any browser with HTML5 support.



The remote access functionality can be used for connections to Windows machines with the Windows Remote Desktop feature available. Thus, remote access cannot be used, for example, for a connection to Windows 10 Home and macOS systems.

To establish a connection from a macOS machine to a remote machine, ensure that the following applications are installed on the macOS machine:

- The Remote Desktop Connection client
- The Microsoft Remote Desktop application

21.1.1 How it works

When you try to connect to a remote machine, the system first checks if this machine has a Cyber Protect quota. If the service quota needed for the remote RDP functionality exists for the Customer tenant, but is not acquired for the machine, the system prompts you to manually acquire this service quota. Then, the system checks that the connection via the HTML5 or RDP client is possible. You initiate a connection via the RDP or HTML5 client. The system establishes a tunnel to the remote machine and checks that the remote desktop connections are enabled on the remote machine. Then, you enter the credentials and, if their validation is successful, you get access to the machine.

21.1.2 How to connect to a remote machine

To connect to a remote machine, do the following:

1. In the service console, go to **Devices > All devices**.
2. Click the machine to which you want to connect remotely and then click **Cyber Protection Desktop > Connect via RDP client / Connect via HTML5 client**.
The system checks if this machine has a Cyber Protect quota. If the service quota needed for the remote RDP functionality exists for the Customer tenant, but is not acquired for the machine, the system prompts you to manually acquire this service quota.
3. If prompted, select one of the suggested service quotas and click **Change and connect**.
4. [Optional, only for connection via RDP client] Download and install the Remote Desktop Connection Client. Initiate the connection to the remote machine.
5. Specify the login and password to access the machine and click **Connect**.

As a result, you are connected to the remote machine and can manage it.

21.1.3 How to run a remote assistance session

Remote assistance allows concurrent access to the same remote desktop session. For example, when you need to fix a problem on a remote user computer, you can use remote assistance to connect to the computer. The user and the remote administrator share one session and the user can share and reproduce an issue.

1. In the service console, go to **Devices > All devices**.
2. Click on the machine to which you want to connect remotely and then click **Cyber Protection Desktop > Run remote assistance**.
The system checks if this machine has a Cyber Protect quota. If the service quota needed for the remote RDP functionality exists for the Customer tenant, but is not acquired for the machine, the system prompts you to manually acquire this service quota.
3. If prompted, select one of the suggested service quotas and click **Change and connect**.
4. Copy the remote assistance session password and click **Connect**. If the session does not start, download and install the connectivity agent on your machine, and retry the connection.
5. If there are ongoing interactive sessions, click **Connect to session**.
6. Enter the remote assistance session password.

As a result, you have remote desktop access to the remote machine and can assist the user.

21.2 Share a remote connection with users

Users who work remotely and need to have access to a remote machine can access the machine without a configured a VPN or other tools for remote connection.

The Cyber Protection service provides you with the capability to share an RDP link with end-users, thus providing them with the remote access to their machines.

1. Enable the remote connection functionality
 - a. In the service console, go to **Settings > Protection > Remote connection**.
 - b. Enable **Share remote desktop connection**.

The option **Share remote connection** appears in the right menu when you select a device.

2. Generate the link to share the remote connection.

a. In the service console, go to **Devices > All devices** and select the device to which you want provide the remote connection.

b. Click **Cyber Protection Desktop > Share remote connection**.

c. Click **Get link**. In the opened window, copy the generated link.

The link is valid for 10 hours.

3. Share the link with the user.

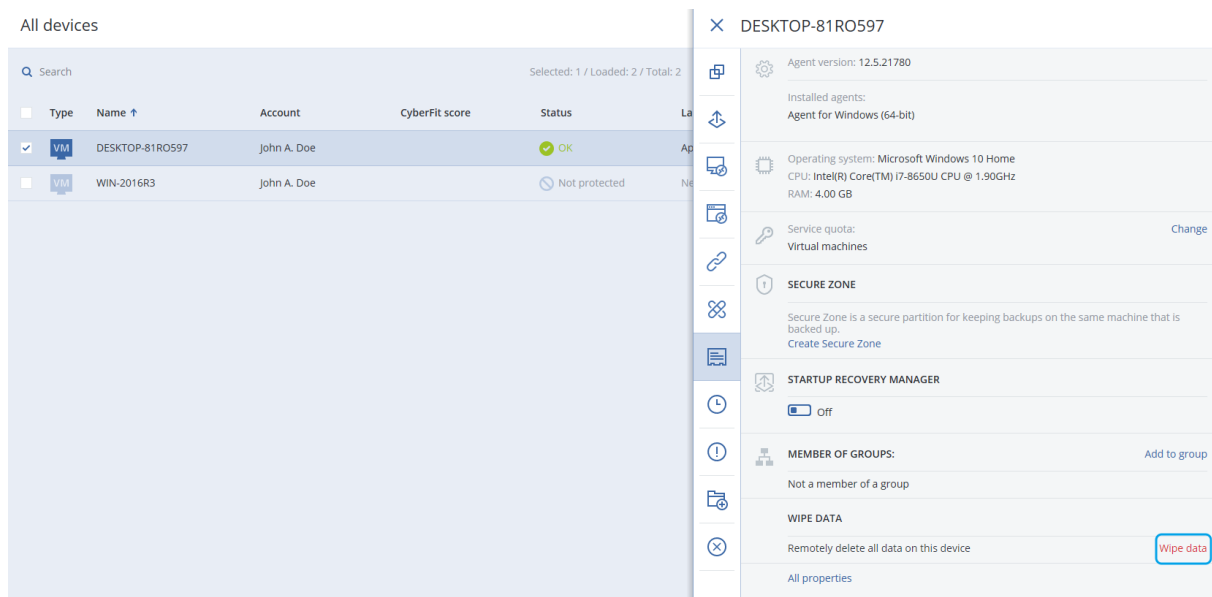
The link redirects the user to the page where the connection type must be selected:

- Connect via RDP client. This connection will prompt downloading and installing the Remote Connection Client.
- Connect via HTML5 client. This connection does not require the installation of an RDP client on the user's machine. The user will be redirected to the login screen where the user's credentials to the remote machine have to be entered.

22 Remote wipe

Remote wipe allows a Cyber Protection service administrator and a machine owner to delete the data on a managed machine – for example, if it gets lost or stolen. Thus, any unauthorized access to sensitive information will be prevented.

Remote wipe is only available for machines running Windows 10. To receive the wipe command, the machine must be turned on and connected to the Internet.



To wipe data from a machine

1. In the service 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**.

23 Smart protection

23.1 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.

Some security alerts can be resolved by following a set of specific actions that are provided by the security experts. Other security alerts just notify you about the upcoming threats but no recommended actions are available.

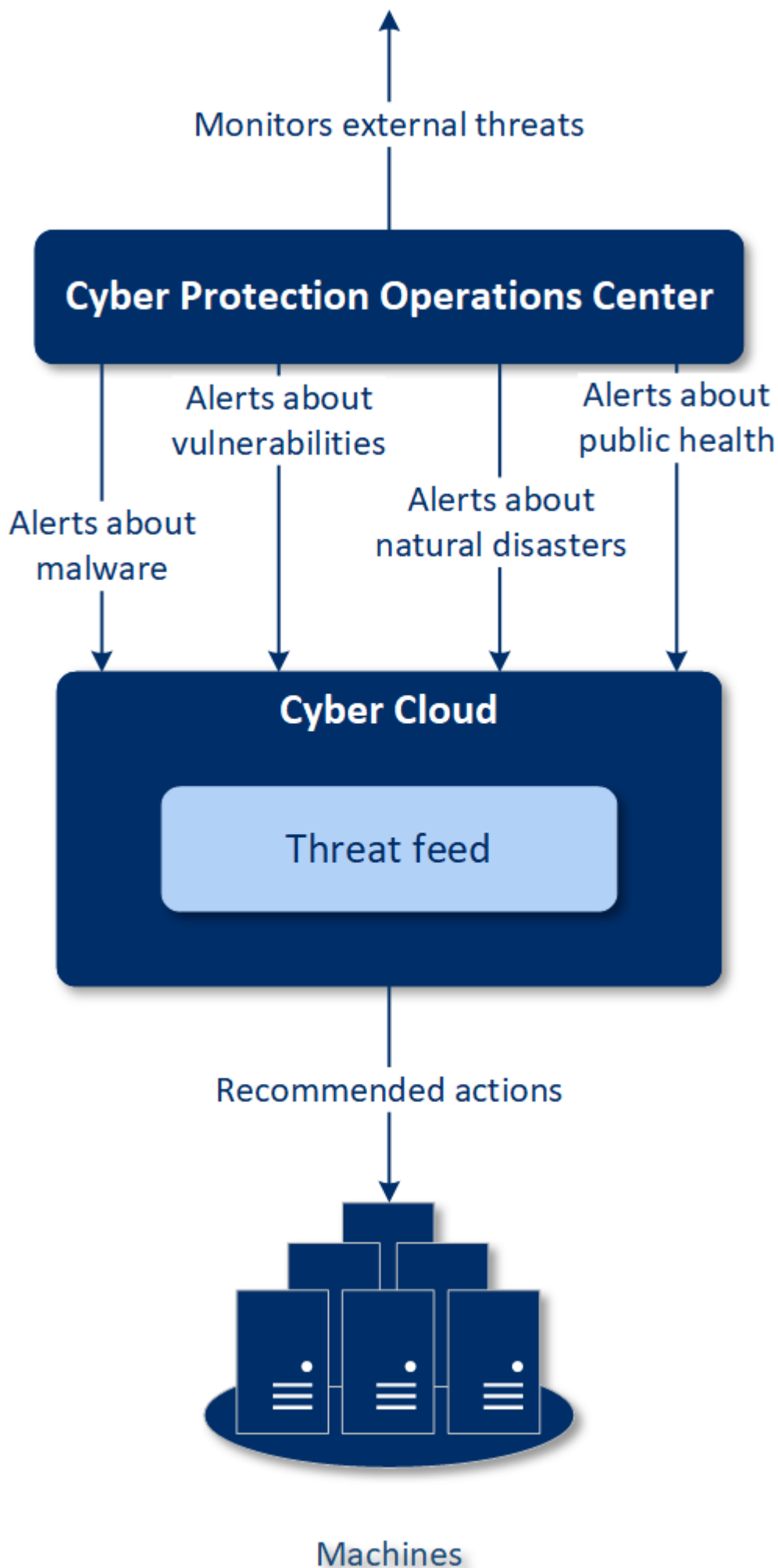
Note

Malware alerts are generated only for machines that have the agent for Antimalware protection installed.

23.1.1 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 service console, in the **Threat feed** section. You can perform respective recommended actions depending on the type of alert.

The main workflow of the threat feed is illustrated in the diagram below.



To run the recommended actions on received alerts from Acronis Cyber Protection Operations Center, do the following:

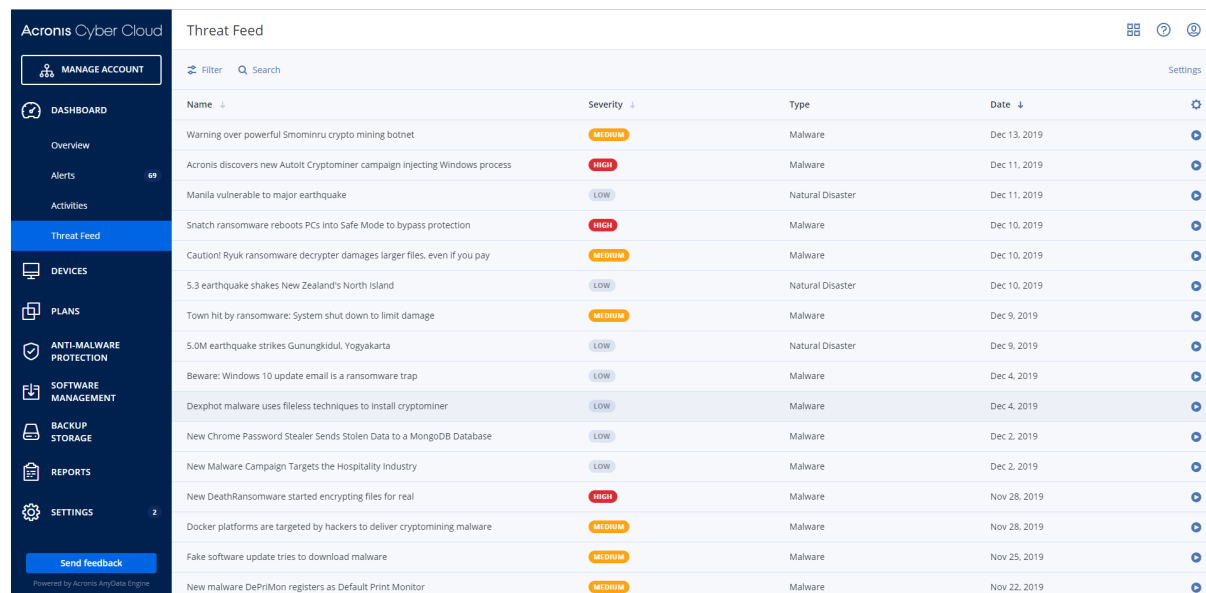
1. In the service console, go to **Dashboard > Threat feed** to review if there are any existing security alerts.
2. Select an alert in the list and review the provided details.
3. Click **Start** to launch the wizard.
4. Enable the actions that you want to be performed and machines to which these actions must be applied. The following actions can be suggested:

- **Vulnerability assessment** – to scan machines for vulnerabilities
- **Patch management** – to install patches on the selected machines
- **Antimalware Protection** – to run full scan of the selected machines

Note

This action is available only for machines that have the agent for Antimalware protection installed.

- **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.



Name	Severity	Type	Date
Warning over powerful Smominru crypto mining botnet	MEDIUM	Malware	Dec 13, 2019
Acronis discovers new Autoit Cryptominer campaign injecting Windows process	HIGH	Malware	Dec 11, 2019
Manilla vulnerable to major earthquake	LOW	Natural Disaster	Dec 11, 2019
Snatch ransomware reboots PCs into Safe Mode to bypass protection	HIGH	Malware	Dec 10, 2019
Caution! Ryuk ransomware decrypter damages larger files, even if you pay	MEDIUM	Malware	Dec 10, 2019
5.3 earthquake shakes New Zealand's North Island	LOW	Natural Disaster	Dec 10, 2019
Town hit by ransomware: System shut down to limit damage	MEDIUM	Malware	Dec 9, 2019
5.0M earthquake strikes Gunungkidul, Yogyakarta	LOW	Natural Disaster	Dec 9, 2019
Beware: Windows 10 update email is a ransomware trap	LOW	Malware	Dec 4, 2019
Dexphot malware uses fileless techniques to install cryptominer	LOW	Malware	Dec 4, 2019
New Chrome Password Stealer Sends Stolen Data to a MongoDB Database	LOW	Malware	Dec 2, 2019
New Malware Campaign Targets the Hospitality Industry	LOW	Malware	Dec 2, 2019
New DeathRansomware started encrypting files for real	HIGH	Malware	Nov 28, 2019
Docker platforms are targeted by hackers to deliver cryptominer malware	MEDIUM	Malware	Nov 28, 2019
Fake software update tries to download malware	MEDIUM	Malware	Nov 25, 2019
New malware DePrIMon registers as Default Print Monitor	MEDIUM	Malware	Nov 22, 2019

23.1.2 Deleting all alerts

Automatic clean-up from the threat feed is made after the following time periods:

- Natural disaster – 1 week
- Vulnerability – 1 month

- Malware – 1 month
- Public health – 1 week

23.2 Data protection map

The Data protection map functionality allows you

- To get detailed information about stored data (classification, locations, protection status, and additional information) on your machines.
- To detect whether data are protected or not. The data are considered protected if they are protected with backup (a protection plan with the backup module enabled).
- To perform actions for data protection.

23.2.1 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.
3. You can also go to **Devices > Data protection map** and find there information about unprotected files per device.
4. You can take actions to protect the detected unprotected files on devices.

23.2.2 Managing the detected unprotected files

To protect the important files that were detected as unprotected, do the following:

1. In the service 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**.

23.2.3 Data protection map settings

To learn how to create a protection plan with the Data protection map module, refer to "[Creating a protection plan](#)".

The following settings can be specified for the Data protection map module.

Schedule

You can define different settings to create the schedule according to which the task for data protection map will be performed.

Schedule the task run using the following events:

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.

Note

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

Schedule type:

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

Start at – Select the exact time when the task will run.

Run within a date range – Set a range in which the configured schedule will be effective.

Start conditions – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "[Start conditions](#)". 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.

Extensions and exception rules

On the **Extensions** tab, you can define the list of file extensions that will be considered as important during data discovery and checked whether they are protected. Use the following format for defining extensions:

.html, .7z, .docx, .zip, .pptx, .xml

On the **Exception rules** tab, you can define which files and folders not to check on protection status during data discovery.

- **Hidden files and folders** – if selected, hidden files and folders will be skipped during data examination.
- **System files and folders** – if selected, system files and folders will be skipped during data examination.

24 Enhanced security mode

The Enhanced security mode provides special settings for clients with increased security demands. This mode requires mandatory encryption for all backups and allows only locally set encryption passwords.

With the Enhanced security mode, all backups created in a customer tenant and its units are automatically encrypted with the AES algorithm and 256-bit key. Users can set their encryption passwords only on the protected devices, and cannot set the encryption passwords in the protection plans.

Cloud services cannot access the encryption passwords. Due to this limitation, the following features are not available for tenants in the Enhanced security mode:

- Recovery through the service console
- File-level browsing of backups through the service console
- Cloud-to-cloud backup
- Website backup
- Application backup
- Backup of mobile devices
- Antimalware scan of backups
- Safe recovery
- Automatic creation of corporate whitelists
- Data protection map
- Disaster recovery
- Reports and dashboards related to the unavailable features

24.1 Limitations

- The Enhanced security mode is compatible only with agents whose version is 15.0.26390 or higher.
- The Enhanced security mode is not available for devices running Red Hat Enterprise Linux 4.x or 5.x, and their derivatives.

24.2 Setting the encryption password

You must set the encryption password locally, on the protected device. You cannot set the encryption password in the protection plan. Without a password, creating backups will fail.

You can set the encryption password in the following ways:

1. During the installation of a protection agent (for Windows, macOS, and Linux).
2. By using the command line (for Windows and Linux).

For more information on how to set an encryption password with the **Acropsh** tool, refer to "To

save the encryption settings on a machine" (p. 181).

3. In the Cyber Protect Monitor (for Windows and macOS).

Warning!

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

To set the encryption password in the Cyber Protect Monitor

1. On the protected device, log on 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.
4. Click **Encryption**.
5. Set the encryption password.
6. Click **OK**.

24.3 Changing the encryption password

You can change the encryption password before a protection plan creates any backups.

It is not recommended to change the encryption password after backups are created because the subsequent backups will fail. To continue protecting the same machine, you must create a new protection plan for it. Changing both the encryption password and the protection plan will result in creating new backups that are encrypted with the changed password. The backups that were created before these changes will not be affected.

Alternatively, you can keep the applied protection plan, and change only the backup file name in it. This will also result in creating new backups that are encrypted with the changed password. To learn more about the backup file name, refer to "Backup file name" (p. 188).

You can change the encryption password in the following ways:

1. In the Cyber Protect Monitor (for Windows and macOS).
2. By using the command line (for Windows and Linux).

For more information on how to set an encryption password with the **Acropsh** tool, refer to "To save the encryption settings on a machine" (p. 181).

24.4 Recovering backups

With the Enhanced security mode, you cannot recover backups through the service console.

The following options are available:

- Recovering an entire machine, its disks, or files, by using a bootable media.
- Extracting files from local backups of Windows machines with installed agent, by using Windows File Explorer.

25 Device control

A part of the Cyber Protection service protection plans, the device control module¹ leverages a functional subset of the agent for Data Loss Prevention² on each protected computer to detect and prevent unauthorized access and transmission of data over local computer channels. It provides fine-grained control over a wide range of data leakage pathways including data exchange using removable media, printers, virtual and redirected devices, and the Windows clipboard.

The module is available for Cyber Protect Essentials, Cyber Protect Standard, and Cyber Protect Advanced editions that are licensed per workload.

Note

On Windows machines, the device control features require the installation of Agent for Data Loss Prevention. It will be installed automatically for protected workloads if the **Device control** module is enabled in their protection plans.

The device control module relies on the data loss prevention³ functions of the agent to enforce contextual control over data access and transfer operations on the protected computer. These include user access to peripheral devices and ports, document printing, clipboard copy / paste operations, media format and eject operations, as well as synchronizations with locally connected mobile devices. The agent for Data Loss Prevention includes a framework for all central management and administration components of the device control module, and therefore it must be installed on every computer to be protected with the device control module. The agent allows, restricts, or denies user actions based on the device control settings it receives from the protection plan that is applied to the protected computer.

The device control module controls access to various peripheral devices, whether used directly on protected computers or redirected in virtualization environments hosted on protected computers. It recognizes devices redirected in Microsoft Remote Desktop Server, Citrix XenDesktop / XenApp / XenServer, and VMware Horizon. It can also control data copy operations between the clipboard of the guest operating system running on VMware Workstation / Player, Oracle VM VirtualBox, or

¹As part of a protection plan, the device control module leverages a functional subset of the data loss prevention agent on each protected computer to detect and prevent unauthorized access and transmission of data over local computer channels. These include user access to peripheral devices and ports, document printing, clipboard copy/paste operations, media format and eject operations, as well as synchronizations with locally connected mobile devices. The device control module provides granular, contextual control over the types of devices and ports that users are allowed to access on the protected computer and the actions that users can take on those devices.

²A data loss prevention system's client component that protects its host computer from unauthorized use, transmission, and storage of confidential, protected, or sensitive data by applying a combination of context and content analysis techniques and enforcing centrally managed data loss prevention policies. Cyber Protection provides a fully featured data loss prevention agent. However, the functionality of the agent on a protected computer is limited to the set of data loss prevention features available for licensing in Cyber Protection, and depends upon the protection plan applied to that computer.

³A system of integrated technologies and organizational measures aimed at detecting and preventing accidental or intentional disclosure / access to confidential, protected, or sensitive data by unauthorized entities outside or inside the organization, or the transfer of such data to untrusted environments.

Windows Virtual PC, and the clipboard of the host operating system running on the protected computer.

The device control module can protect computers running the following operating systems:

- Microsoft Windows 7 Service Pack 1 and later
- Microsoft Windows Server 2008 R2 and later
- macOS 10.15 (Catalina) and later
- macOS 11.2.3 (Big Sur) and later

Note

Agent for Data Loss Prevention might be installed on unsupported macOS systems because it is an integral part of Agent for Mac. In this case, the Cyber Protect console will display that Agent for Data Loss Prevention is installed on the computer, but the device control functionality will not work. Device control functionality will only work on [macOS systems that are supported by Agent for Data Loss Prevention](#).

25.0.1 Limitation on the use of the agent for Data Loss Prevention with Hyper-V

Do not install Agent for Data Loss Prevention on Hyper-V hosts in Hyper-V clusters because it might cause BSOD issues, mainly in Hyper-V clusters with Clustered Shared Volumes (CSV).

If you use any of the following versions of Agent for Hyper-V, you need to manually remove Agent for Data Loss Prevention:



- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

To remove Agent for Data Loss Prevention, on the Hyper-V host, run the installer manually and clear the Agent for Data Loss Prevention check box, or run the following command:

```
<installer_name> --remove-components=agentForDlp -quiet
```

You can enable and configure the device control module in the **Device control** section of your protection plan in the service console. For instructions, see [steps to enable or disable device control](#).

The **Device control** section displays a summary of the module's configuration:

Device control Access to 7 device types is limited. Allowlists are configured			
Access settings	Restricted: USB, Removable, Printers and 4 more		
Device types allowlist	1 allowed		
USB devices allowlist	1 allowed		
Exclusions	2 excluded		

- [Access settings](#) - Shows a summary of device types and ports with restricted (denied or read-only) access, if any. Otherwise, indicates that all device types are allowed. Click this summary to view or change the access settings (see [steps to view or change access settings](#)).
- [Device types allowlist](#) - Shows how many device subclasses are allowed by excluding from device access control, if any. Otherwise, indicates that the allowlist is empty. Click this summary to view or change the selection of allowed device subclasses (see [steps to exclude device subclasses from access control](#)).
- [USB devices allowlist](#) - Shows how many USB devices/models are allowed by excluding from device access control, if any. Otherwise, indicates that the allowlist is empty. Click this summary to view or change the list of allowed USB devices/models (see [steps to exclude individual USB devices from access control](#)).
- [Exclusions](#) - Shows how many access control exclusions have been set for Windows clipboard, screenshot capture, printers, and mobile devices.

25.1 Using device control

This section covers step-by-step instructions for basic tasks when using the device control module.

25.1.1 Enable or disable device control

You can enable device control when [creating a protection plan](#). You can change an existing protection plan to enable or disable device control.

To enable or disable device control

1. In the service console, go to **Devices > All devices**.
2. Do one of the following to open the protection plan panel:
 - If you are going to create a new protection plan, select a machine to protect, click **Protect**, and then click **Create plan**.

- If you are going to change an existing protection plan, select a protected machine, click **Protect**, click the ellipsis (...) next to the name of the protection plan, and then click **Edit**.
3. In the protection plan panel, navigate to the **Device control** area, and click to turn the **Device control** switch on or off.
 4. Do one of the following to apply your changes:
 - If creating a protection plan, click **Create**.
 - If editing a protection plan, click **Save**.

You might also access the protection plan panel from the [Plans tab](#). However, this capability is not available in all editions of the Cyber Protection service.

25.1.2 View or change access settings

From the protection plan panel, you can manage access settings for the device control module. In this way, you can allow or deny access to certain types of devices, as well as enable or disable notifications and alerts.

To view or change access settings

1. Open the protection plan panel for a protection plan and enable device control in that plan (see [steps to enable or disable device control](#)).
2. Click the arrow icon next to the **Device control** switch to expand the settings, and then click the link next to **Access settings**.
3. On the [page for managing access settings](#) that appears, view or change access settings as appropriate.

Enable or disable OS notification and service alerts

When managing access settings, you can enable or disable [OS notification and service alerts](#), informing of user attempts to perform actions that are not allowed.

To enable or disable OS notification

1. Follow the [steps to view or change access settings](#).
2. On the [page for managing access settings](#), select or clear the **Show OS notification to end users if they try to use a blocked device type or port** check box.

To enable or disable service alerts

1. Follow the [steps to view or change access settings](#).
2. On the [page for managing access settings](#), select or clear the **Show alert** check box for the desired device type/s.

The **Show alert** check box is available only for device types with restricted access (Read-only or Denied access), except screenshot capture.

25.1.3 Exclude device subclasses from access control

From the protection plan panel, you can choose device subclasses to exclude from access control. As a result, access to those devices is allowed regardless of the device control access settings.

To exclude device subclasses from access control

1. Open the protection plan panel for a protection plan and enable device control in that plan (see [steps to enable or disable device control](#)).
2. Click the arrow icon next to the **Device control** switch to expand the settings, and then click the link next to **Device types allowlist**.
3. On the [page for managing the allowlist](#) that appears, view or change the selection of device subclasses to exclude from access control.

25.1.4 Exclude individual USB devices from access control

From the protection plan panel, you can specify individual USB devices or USB device models to exclude from access control. As a result, access to those devices is allowed regardless of the device control access settings.

To exclude a USB device from access control

1. Open the protection plan panel for a protection plan and enable device control in that plan (see [steps to enable or disable device control](#)).
2. Click the arrow icon next to the **Device control** switch to expand the settings, and then click the link next to **USB devices allowlist**.
3. On the [page for managing the allowlist](#) that appears, click **Add from database**.
4. On the [page for selecting USB devices](#) that appears, select the desired device/s from those registered with the [USB devices database](#).
5. Click the **Add to allowlist** button.

To stop excluding a USB device from access control

1. Open the protection plan panel for a protection plan and enable device control in that plan (see [steps to enable or disable device control](#)).
2. Click the arrow icon next to the **Device control** switch to expand the settings, and then click the link next to **USB devices allowlist**.
3. On the [page for managing the allowlist](#) that appears, click the delete icon at the end of list item representing the desired USB device.

Add or remove USB devices from the database

To exclude a particular USB device from access control, you need to add it to the [USB devices database](#). Then, you can add devices to the allowlist by selecting from that database.

The following procedures apply to protection plans that have the device control feature enabled.

To add USB devices to the database

1. Open the protection plan of a device for editing:
Click the ellipsis (...) next to the name of the protection plan and select **Edit**.

Note

Device control must be enabled in the plan, so you can access the Device control settings.

2. Click the arrow icon next to the **Device control** switch to expand the settings, and then click the link next to **USB devices allowlist**.
3. On the **USB devices allowlist** page that appears, click **Add from database**.
4. On the USB devices database management page that appears, click **Add to database**.
5. On the **Add USB device** dialog that appears, click the machine to which the USB device is connected.
Only machines that are online are displayed in the list of computers.
The list of USB devices is displayed only for machines that have the agent for Data Loss Prevention installed.
The USB devices are listed in tree view. The first level of the tree represents a device model. The second level represents a specific device of that model.
A blue icon next to the description of the device indicates that the device is currently attached to the computer. If the device is not attached to the computer, the icon is grayed out.
6. Select the check boxes for the USB devices that you want to add to the database, and then click **Add to database**.
The selected USB devices are added to the database.
7. Close or save the protection plan.

To add USB devices to the database from the computer Details panel

Note

This procedure applies only for devices that are online and have the agent for Data Loss Prevention installed on them. You cannot view the list of USB devices for a computer that is offline or does not have the Data Loss Prevention agent installed.

1. In the service console, go to **Devices > All devices**.
2. Select a computer to which the desired USB device has ever been connected, and, in the menu to the right, click **Inventory**.
The computer details panel opens.
3. On the computer details panel, click the **USB Devices** tab.
The list of USB devices that are known on the selected computer opens.
The USB devices are listed in tree view. The first level of the tree represents a device model. The second level represents a specific device of that model.
A blue icon next to the description of the device indicates that the device is currently attached to the computer. If the device is not attached to the computer, the icon is grayed out.
4. Select the check boxes for the USB devices that you want to add to the database and click **Add to database**.

To add USB devices to the database from service alerts

1. In the service console, go to **Dashboard > Alerts**.
2. [Locate a device control alert](#) that informs of denying access to the USB device.
3. In the alert simple view, click **Allow this USB device**.

This excludes the USB device from access control, and adds it to the database for further reference.

To add USB devices by importing a list of devices to the database

You can import a JSON file with a list of USB devices to the database. See "Import a list of USB devices to the database" (p. 511).

To remove USB devices from the database

1. Open the protection plan of a device for editing:
Click the ellipsis (...) next to the name of the protection plan and select **Edit**.

Note

Device control must be enabled in the plan, so you can access the Device control settings.

2. Click the arrow next to the **Device control** switch to expand the settings, and then click the **USB devices allowlist** row.
3. On the [page for managing the allowlist](#) that appears, click **Add from database**.
4. On the [page for selecting USB devices from the database](#), click ellipsis (...) at the end of the list item representing the device, click **Delete**, and confirm the deletion.
The USB devices are deleted from the database.
5. Close or save the protection plan.

25.1.5 View device control alerts

The device control module can be configured to raise alerts that inform of denied user attempts to use certain device types (see [Enable or disable OS notification and service alerts](#)). Use the following steps to view those alerts.

To view device control alerts

1. In the service console, go to **Dashboard > Alerts**.
2. Look for alerts with the following status: "Peripheral device access is blocked".

See [Device control alerts](#) for further details.

25.2 Access settings

On the **Access settings** page, you can allow or deny access to devices of certain types, as well as enable or disable OS notification and device control alerts.

The access settings allow you to limit user access to the following device types and ports:

- **Removable** (access control by device type) - Devices with any interface for connecting to a computer (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc.) that are recognized by the operating system as removable storage devices (for example, USB sticks, card readers, magneto-optical drives, etc.). The device control classifies all hard drives connected via USB, FireWire, and PCMCIA as removable devices. It also classifies some hard drives (usually with SATA and SCSI) as removable devices if they support the hot-plug function and do not have the running operating system installed on them.

You can allow full access, read-only access, or deny access to removable devices to control data copy operations to and from any removable device on a protected computer. Access rights do not affect devices that are encrypted with BitLocker.

These device types are supported on both Windows and macOS.

- **Encrypted removable** (access control by device type) - Removable devices that are encrypted with BitLocker drive encryption.

You can allow full access, read-only access, or deny access to encrypted removable devices to control data copy operations to and from any encrypted removable device on a protected computer. Access rights affect only devices that are encrypted with BitLocker.

Encrypted removable devices on macOS are removable drives that are encrypted with the FileVault disk encryption program.

Only encrypted removable drives using the HFS+ (also known as HFS Plus or Mac OS Extended, or HFS Extended) file system are supported.

Encrypted removable drives using the APFS file system are treated as removable drives.

These device types are supported on both Windows and macOS.

- **Printers** (access control by device type) - Physical printers with any interface for connecting to a computer (USB, LPT, Bluetooth, etc.), as well as printers accessed from a computer on the network.

You can allow or deny access to printers to control the printing of documents on any printer on a protected computer.

Note

When you change the access setting for printers to **Deny**, the applications and processes accessing the printers must be restarted to enforce the newly configured access settings. To ensure that access settings are enforced correctly, restart the protected workloads.

- **Clipboard** (access control by device type) - Windows clipboard.

You can allow or deny access to the clipboard to control the copy and paste operations through the Windows clipboard on a protected computer.

Note

When you change the access setting for clipboard to **Deny**, the applications and processes accessing the clipboard must be restarted to enforce the newly configured access settings. To ensure that access settings are enforced correctly, restart the protected workloads.

- **Screenshot capture** (access control by device type) - Enables capturing of screenshots of the entire screen, the active window, or of selected portion of the screen.

You can allow or deny access to the screenshot capture to control the screenshot capturing on a protected computer.

Note

When you change the access setting for screenshot capture to **Deny**, the applications and processes accessing the screenshot capture must be restarted to enforce the newly configured access settings. To ensure that access settings are enforced correctly, restart the protected workloads.

- **Mobile devices** (access control by device type) - Devices (such as Android-based smartphones, etc.) that communicate with a computer via Media Transfer Protocol (MTP), with any interface used for connecting to a computer (USB, IP, Bluetooth).

You can allow full access, allow read-only access, or deny access to mobile devices to control data copy operations to and from any MTP-based mobile device on a protected computer.

Note

When you change the access setting for mobile devices to **Read-only** or **Deny**, the applications and processes accessing the mobile devices must be restarted to enforce the newly configured access settings. To ensure that access settings are enforced correctly, restart the protected workloads.

- **Bluetooth** (access control by device type) - External and internal Bluetooth devices with any interface for connecting to a computer (USB, PCMCIA, etc.). This setting controls the use of the devices of this type rather than data exchange using such devices.

You can allow or deny access to Bluetooth to control the use of any Bluetooth devices on a protected computer.

Note

On macOS, the access rights for Bluetooth do not affect Bluetooth HID devices. The access to these devices is always allowed to prevent wireless HID devices (mice and keyboards) from being disabled on iMac and Mac Pro hardware. Settings for unsupported device subclasses are ignored if these settings are configured in the applied protection plan.

These device types are supported on both Windows and macOS.

- **Optical drives** (access control by device type) - External and internal CD/DVD/BD drives (including writers) with any interface for connecting to a computer (IDE, SATA, USB, FireWire, PCMCIA, etc.).

You can allow full access, allow read-only access, or deny access to optical drives to control data copy operations to and from any optical drive on a protected computer.

These device types are supported on both Windows and macOS.

- **Floppy drives** (access control by device type) - External and internal floppy drives with any interface for connecting to a computer (IDE, USB, PCMCIA, etc.). There are some models of floppy drives that the operating system recognizes as removable drives, in which case the device control also identifies these drives as removable devices.

You can allow full access, allow read-only access, or deny access to floppy drives to control data copy operations to and from any floppy drive on a protected computer.

- **USB** (access control by device interface) - Any devices connected to a USB port, except hubs. You can allow full access, allow read-only access, or deny access to USB port to control data copy operations to and from devices connected to any USB port on a protected computer.

These device types are supported on both Windows and macOS.

- **FireWire** (access control by device interface) - Any devices connected to a FireWire (IEEE 1394) port, except hubs.

You can allow full access, allow read-only access, or deny access to FireWire port to control data copy operations to and from devices connected to any FireWire port on a protected computer.

These device types are supported on both Windows and macOS.

- **Redirected devices** (access control by device interface) - Mapped drives (hard, removable and optical drives), USB devices, and the clipboard redirected to virtual application/desktop sessions. The device control recognizes devices redirected via the Microsoft RDP, Citrix ICA, VMware PCoIP, and HTML5/WebSockets remoting protocols in the Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer, and VMware Horizon virtualization environments hosted on protected Windows computers. It can also control data copy operations between the Windows clipboard of the guest operating system running on VMware Workstation, VMware Player, Oracle VM VirtualBox, or Windows Virtual PC, and the clipboard of the host operating system running on a protected Windows computer.

You can configure access to redirected devices as follows:

- **Mapped drives** - Allow full access, allow read-only access, or deny access to control data copy operations to and from any hard drive, removable drive, or optical drive redirected to the session hosted on a protected computer.
- **Clipboard incoming** - Allow or deny access to control data copy operations through the clipboard to the session hosted on a protected computer.

Note

When you change the access setting for clipboard incoming to **Deny**, the applications and processes accessing the clipboard must be restarted to enforce the newly configured access settings. To ensure that access settings are enforced correctly, restart the protected workloads.

- **Clipboard outgoing** - Allow or deny access to control data copy operations through the clipboard from the session hosted on a protected computer.

Note

When you change the access setting for clipboard outgoing to **Deny**, the applications and processes accessing the clipboard must be restarted to enforce the newly configured access settings. To ensure that access settings are enforced correctly, restart the protected workloads.

- **USB ports** - Allow or deny access to control data copy operations to and from devices connected to any USB port redirected to the session hosted on a protected computer.

Device control settings affect all users equally. For example, if you deny access to removable devices, you prevent any user from copying data to and from such devices on a protected computer. It is possible to selectively allow access to individual USB devices by excluding them from access control (see [Device types allowlist](#) and [USB devices allowlist](#)).

When access to a device is controlled by both its type and its interface, denying access at the interface level takes precedence. For example, if access to USB ports is denied (device interface), then access to mobile devices connected to a USB port is denied regardless of whether access to mobile devices is allowed or denied (device type). To allow access to such a device, you must allow both its interface and type.

Important

When a removable device, an encrypted removable device, a printer, or a Bluetooth device is connected to a USB port, allowing access to that device overrides the access denial set at the USB interface level. If you allow such a device type, access to the device is allowed regardless of whether access to the USB port is denied.

See also [steps to view or change access settings](#).

25.2.1 OS notification and service alerts

You can configure the device control to display OS notification to end users if they try to use a blocked device type on protected computers. When the **Show OS notification to end users if they try to use a blocked device type or port** check box is selected in the access settings, the agent displays a pop-up message in the notification area of the protected computer if any of the following events occurs:

- A denied attempt to use a device on a USB or FireWire port. This notification appears whenever the user plugs in a USB or FireWire device that is denied at the interface level (for example, when denying access to the USB port) or at the type level (for example, when denying the use of removable devices). The notification informs that the user is not allowed to access the specified device/drive.
- A denied attempt to copy a data object (such as a file) from a certain device. This notification appears when denying read access to the following devices: floppy drives, optical drives, removable devices, encrypted removable devices, mobile devices, redirected mapped drives, and redirected clipboard incoming data. The notification informs that the user is not allowed to get

the specified data object from the specified device.

The denied read notification is also displayed when denying read/write access to Bluetooth, FireWire port, USB port, and redirected USB port.

- A denied attempt to copy a data object (such as a file) to a certain device. This notification appears when denying write access to the following devices: floppy drives, optical drives, removable devices, encrypted removable devices, mobile devices, local clipboard, screenshot capture, printers, redirected mapped drives, and redirected clipboard outgoing data. The notification informs that the user is not allowed to send the specified data object to the specified device.

User attempts to access blocked device types on protected computers can raise alerts that are logged in the service console. It is possible to enable alerts for each device type (excluding screenshot capture) or port separately by selecting the **Show alert** check box in the access settings. For example, if access to removable devices is restricted to read-only, and the **Show alert** check box is selected for that device type, an alert is logged every time a user on a protected computer attempts to copy data to a removable device. See [Device control alerts](#) for further details.

See also [steps to enable or disable OS notification and service alerts](#).

25.3 Device types allowlist

On the **Device types allowlist** page, you can choose device subclasses to exclude from device access control. As a result, access to those devices is allowed regardless of the access settings in the device control module.

The device control module provides the option to allow access to devices of certain subclasses within a denied device type. This option allows you to deny all devices of a certain type, except for some subclasses of devices of this type. It can be useful, for example, when you need to deny access to all USB ports while allowing the use of a USB keyboard and mouse at the same time.

When configuring the device control module, you can specify which device subclasses to exclude from device access control. When a device belongs to an excluded subclass, access to that device is allowed regardless of whether or not the device type or port is denied. You can selectively exclude the following device subclasses from device access control:

- **USB HID (mouse, keyboard, etc.)** - When selected, allows access to Human Interface Devices (mouse, keyboard, and so on) connected to a USB port even if USB ports are denied. By default, this item is selected so that denying access to the USB port does not disable the keyboard or mouse.
Supported on both Windows and macOS.
- **USB and FireWire network cards** - When selected, allows access to network cards connected to a USB or FireWire (IEEE 1394) port even if USB ports and/or FireWire ports are denied.
Supported on both Windows and macOS.
- **USB scanners and still image devices** - When selected, allows access to scanners and still image devices connected to a USB port even if USB ports are denied.

- **USB audio devices** - When selected, allows access to audio devices, such as headsets and microphones, connected to a USB port even if USB ports are denied.
- **USB cameras** - When selected, allows access to Web cameras connected to a USB port even if USB ports are denied.
- **Bluetooth HID (mouse, keyboard, etc.)** - When selected, allows access to Human Interface Devices (mouse, keyboard, and so on) connected via Bluetooth even if Bluetooth is denied.
- **Clipboard copy/paste within application** - When selected, allows copying/pasting of data through the clipboard within the same application even if the clipboard is denied.

When allowlisting device types, consider the following:

- With the device types allowlist, you can only allow a whole subclass of device. You cannot allow a specific device model, while denying all other devices of the same subclass. For example, by excluding USB cameras from device access control, you allow the use of any USB camera, no matter their model and vendor. On how to allow individual devices/models, see [USB devices allowlist](#).
- Device types can only be selected from a closed list of device subclasses. If the device to allow is of a different subclass, then it cannot be allowed by using device types allowlist. For example, such a subclass as USB smartcard readers cannot be added to the allowlist. To allow a USB smartcard reader when USB ports are denied, follow the instructions in [USB devices allowlist](#).
- The device types allowlist only works for devices that use standard Windows drivers. The device control may not recognize the subclass of some USB devices with proprietary drivers. As a result, you cannot allow access to such USB devices by using the device types allowlist. In this case, you could allow access on a per-device/model basis (see [USB devices allowlist](#)).

See also [steps to exclude device subclasses from access control](#).

25.4 USB devices allowlist

The allowlist is intended to allow using certain USB devices regardless of any other device control settings. You can add individual devices or device models to the allowlist to disable the access control for those devices. For example, if you add a mobile device with a unique ID to the allowlist, you allow the use of that particular device even though any other USB devices are denied.

On the **USB devices allowlist** page, you can specify individual USB devices or USB device models to exclude from device access control. As a result, access to those devices is allowed regardless of the access settings in the device control module.

There are two ways to identify devices in the allowlist:

- **Model of device** - Collectively identifies all devices of a certain model. Each device model is identified by vendor ID (VID) and product ID (PID), such as USB\VID_0FCE&PID_E19E. This combination of VID and PID does not identify a specific device, but an entire device model. By adding a device model to the allowlist, you allow access to any device of that model. For example, this way you can allow the use of USB printers of a particular model.

- **Unique device** - Identifies a certain device. Each unique device is identified by vendor ID (VID), product ID (PID), and serial number, such as USB\VID_0FCE&PID_E19E\D55E7FCA.

Not all USB devices are assigned a serial number. You can add a device to the allowlist as a unique device only if the device has been assigned a serial number during production. For example, a USB stick that has a unique serial number.

To add a device to the allowlist, you first need to add it to the [USB devices database](#). Then, you can add devices to the allowlist by selecting from that database.

The allowlist is managed on a separate configuration page called **USB devices allowlist**. Each item in the list represents a device or device model and has the following fields:

- **Description** - The operating system assigns a certain description when connecting the USB device. You can modify the description of the device in the USB devices database (see [USB database management page](#)).
- **Device type** - Displays Unique if the list item represents a unique device, or Model if it represents a device model.
- **Read-only** - When selected, allows only receiving data from the device. If the device does not support read-only access, then access to the device is blocked. Clear this check box to allow full access to the device.
- **Reinitialize** - When selected, causes the device to simulate disconnecting/reconnecting when a new user logs in. Some USB devices require reinitializing in order to function, so it is recommended to select this check box for such devices (mouse, keyboard, etc.). It is also advisable to clear this check box for data storage devices (USB sticks, optical drives, external hard drives, etc.).

The device control may not be able to reinitialize some USB devices with proprietary drivers. If there is no access to such a device, you must remove the USB device from the USB port, and then insert it back.

Note

The **Reinitialize** field is hidden by default. To display it in the table, click the gear icon in the upper right corner of the table, and then select the **Reinitialize** check box.

Note

The **Read-only** and **Reinitialize** fields are not supported on macOS. If these fields are configured in the applied protection plan, they will be ignored.

You can add or remove devices/models from the allowlist as follows:

- Click **Add from database** above the list and then select the desired device/s from those registered with the [USB devices database](#). The selected device is added to the list, where you can configure its settings and confirm the changes.
- Click **Allow this USB device** in an alert informing that access to the USB device is denied (see [Device control alerts](#)). This adds the device to the allowlist and to the USB devices database.

- Click the delete icon at the end of a list item. This removes the respective device/model from the allowlist.

See also [steps to exclude individual USB devices from access control](#).

25.4.1 USB devices database

The device control module maintains a database of USB devices from which you can add devices to the list of exclusions (see [USB devices allowlist](#)). A USB device can be registered with the database in any of these ways:

- Add a device on the page that appears when adding a device to the exclusion list (see [USB devices database management page](#)).
- Add a device from the USB Devices tab of a computer's Inventory pane in the service console (see [List of USB devices on a computer](#)).
- Allow the device from an alert on denying access to the USB device (see [Device control alerts](#)).

See also [steps to add or remove USB devices from the database](#).

USB devices database management page

When configuring the allowlist for USB devices, you have the option to add a device from the database. If you choose this option, a management page appears with a list of devices. On this page you can view the list of all devices that are registered with the database, you can select devices to add to the allowlist, and perform the following operations:

Register a device with the database

1. Click **Add to database** at the top of the page.
2. On the **Add USB device** dialog that appears, choose the machine to which the USB device is connected.
Only machines that are online are displayed in the list of computers.
The list of USB devices is displayed only for machines that have the agent for Data Loss Prevention installed.
The USB devices are listed in tree view. The first level of the tree represents a device model. The second level represents a specific device of that model.
A blue icon next to the description of the device indicates that the device is currently attached to the computer. If the device is not attached to the computer, the icon is grayed out.
3. Select the check box for the USB device that you want to register, and click **Add to database**.

Change the description of a device

1. On the **USB devices database** page click ellipsis (...) at the end of the list item representing the device and then click **Edit**.
2. Make changes to the description in the dialog box that appears.

Remove a device from the database

1. Click the ellipsis (...) at the end of the list item representing the device.
2. Click **Delete**, and confirm the deletion.

For each device, the list on the page provides the following information:

- **Description** - A readable identifier of the device. You can change the description as needed.
- **Device type** - Displays Unique if the list item represents a unique device, or Model if it represents a device model. A unique device must have a serial number along with a vendor ID (VID) and product ID (PID), whereas a device model is identified by a combination of VID and PID.
- **Vendor ID, Product ID, Serial number** - These values together make up the device ID in the form USB\VID_<vendor ID>&PID_<product ID>\<serial number>.
- **Account** - Indicates the tenant to which this device belongs. This is the tenant that contains the user account that was used to register the device with the database.

Note

This column is hidden by default. To display it in the table, click the gear icon in the upper right corner of the table, and then select **Account**.

The leftmost column is intended to select the devices to add to the allowlist: Select the check box for each device to add, and then click the **Add to allowlist** button. To select or clear all check boxes, click the check box in the column header.

You can search or filter the list of devices:

- Click **Search** at the top of the page and enter a search string. The list displays devices whose description matches the string you typed.
- Click **Filter**, and then configure and apply a filter in the dialog box that appears. The list is limited to devices with the type, vendor ID, product ID, and account that you selected when configuring the filter. To cancel the filter and list all devices, click **Reset to default**.

Export the list of USB devices in the database

You can export the list of USB devices that are added to the database.

1. Open the protection plan of a device for editing.
2. Click the arrow icon next to the **Device control** switch to expand the settings, and then click the **USB devices allowlist** row.
3. On the USB devices allowlist page, click **Add from database**.
4. On the USB devices database management page that appears, click **Export**.
The standard Browse dialog opens.
5. Select the location to which you want to save the file, enter a new file name if needed, and click **Save**.

The list of USB devices is exported to a JSON file.

You can edit the resulting JSON file to add or remove devices from it, and make mass changes of device descriptions.

Import a list of USB devices to the database

Instead of adding USB devices from the service console user interface, you can import a list of USB devices. The list is a file in JSON format.

Note

You can import JSON files to a database that does not contain the devices described in the file. To import a modified file to the database from which it was exported, you must clear the database first because you cannot import duplicate entries. If you export the list of USB devices, modify it, and try to import to the same database without clearing it, the import will fail.

1. Open the protection plan of a device for editing.
2. Click the arrow icon next to the **Device control** switch to expand the settings, and then click the **USB devices allowlist** row.
3. On the USB devices allowlist page, click **Add from database**.
4. On the USB devices database management page that appears, click **Import**.
The dialog Import USB devices from file opens.
5. Use drag and drop (or browse) for the file that you want to import.

The service console checks if the list contains duplicate entries that already exist in the database and skips them. The USB devices that are not found in the database are appended to it.

List of USB devices on a computer

The Inventory panel of a computer in the service console includes the **USB Devices** tab. If the computer is online and the agent for Data Loss Prevention is installed on it, the **USB Devices** tab displays a list all USB devices that have ever been connected to that computer.

The USB devices are listed in tree view. The first level of the tree represents a device model. The second level represents a specific device of that model.

For each device, the list provides the following information:

- **Description** - The operating system assigns a description when connecting the USB device. This description can serve as a readable identifier of the device.
A blue icon next to the description of the device indicates that the device is currently attached to the computer. If the device is not attached to the computer, the icon is grayed out.
- **Device ID** - The identifier that the operating system assigned to the device. This identifier has the following format: USB\VID_<vendor ID>&PID_<product ID>\<serial number> where <serial number> is optional. Examples: USB\VID_0FCE&PID_ADDE\55E7FCA (device with a serial number); USB\VID_0FCE&PID_ADDE (device without serial number).

To add devices to the USB devices database, select the check boxes of the desired devices, and then click the **Add to database** button.

25.5 Excluding processes from access control

The access to Windows clipboard, screenshot capture, printers, and mobile devices is controlled through hooks injected into processes. If processes are not hooked, the access to these devices will

not be controlled.

Note

Excluding processes from access control is not supported on macOS. If a list of excluded processes is configured in the applied protection plan, it will be ignored.

On the **Exclusions** page, you can specify a list of processes that will not be hooked. This means that clipboard (local and redirected), screenshot capture, printer, and mobile device access controls will not be applied to such processes.

For example, you applied a protection plan that denies access to printers, then started the Microsoft Word application. An attempt to print from this application will be blocked. But if you add the Microsoft Word process to the list of exclusions, then the application will not be hooked. As a result, printing from Microsoft Word will not be blocked, while printing from other applications will still be blocked.

To add processes to exclusions

1. Open the protection plan of a device for editing:
Click the ellipsis (...) next to the name of the protection plan and select **Edit**.

Note

Device control must be enabled in the plan, so you can access the Device control settings.

2. Click the arrow next to the **Device control** switch to expand the settings, and then click the **Exclusions** row.
3. On the **Exclusions** page, in the **Processes and folders** row, click **+Add**.
4. Add the processes that you want to exclude from the access control.
For example, `C:\Folder\subfolder\process.exe`.
You can use wildcards:
 - * replaces any number of characters.
 - ? replaces one character.For example:
`C:\Folder*`
`*\Folder\SubFolder?*`
`*\process.exe`
5. Click the check mark, and then click **Done**.
6. In the protection plan, click **Save**.
7. Restart the processes that you excluded to ensure that the hooks are properly removed.

The excluded processes will have access to clipboard, screenshot capture, printers, and mobile devices regardless of the access settings for those devices.

To remove a process from exclusions

Open the protection plan of a device for editing:

Click the ellipsis (...) next to the name of the protection plan and select **Edit**.

Note

Device control must be enabled in the plan, so you can access the Device control settings.

1. Click the arrow next to the **Device control** switch to expand the settings, and then click the **Exclusions** row.
2. On the **Exclusions** page, click the trash can icon next to the process that you want to remove from the exclusions.
3. Click **Done**.
4. In the protection plan, click **Save**.
5. Restart the process to ensure that hooks are properly injected.

The access settings from the protection plan will be applied to the processes that you removed from the exclusions.

To edit a process in exclusions

1. Open the protection plan of a device for editing:
Click the ellipsis (...) next to the name of the protection plan and select **Edit**.

Note

Device control must be enabled in the plan, so you can access the Device control settings.

2. Click the arrow next to the **Device control** switch to expand the settings, and then click the **Exclusions** row.
3. On the **Exclusions** page, click the **Edit** icon next to the process that you want to edit.
4. Apply the changes and click the check mark to confirm.
5. Click **Done**.
6. In the protection plan, click **Save**.
7. Restart the affected processes to ensure that your changes are applied correctly.

25.6 Device control alerts

The device control maintains an event log by tracking user attempts to access controlled device types, ports, or interfaces. Certain events can raise alerts that are logged in the service console. For example, the device control module can be configured to prevent the use of removable devices, with an alert logged whenever a user tries to copy data to or from such a device.

When configuring the device control module, you can enable alerts for most items listed under device Type (except screenshot capture) or Ports. If alerts are enabled, each attempt by a user to perform an operation that is not allowed generates an alert. For example, if access to removable devices is restricted to read-only, and the **Show alert** option is selected for that device type, an alert

is generated every time a user on a protected computer attempts to copy data to a removable device.

To view alerts in the service console, go to **Dashboard > Alerts**. Within each device control alert, the console provides the following information about the respective event:

- **Type** - Warning.
- **Status** - Displays "Peripheral device access is blocked".
- **Message** - Displays "Access to '<device type or port>' on '<computer name>' is blocked". For example, "Access to 'Removable' on 'accountant-pc' is blocked".
- **Date and time** - The date and time that the event occurred.
- **Workload** - The name of the computer on which the event occurred.
- **Plan name** - The name of the protection plan that caused the event.
- **Source** - The device type or port involved in the event. For example, in the event of a denied user attempt to access a removable device, this field reads Removable device.
- **Action** - The operation that caused the event. For example, in the event of a denied user attempt to copy data to a device, this field reads Write. For more information, see [Action field values](#).
- **Name** - The name of the event target object, such as the file the user attempted to copy or the device the user attempted to use. Not displayed if the target object cannot be identified.
- **Information** - Additional information about the event target device, such as the device ID for USB devices. Not displayed if no additional information about the target device is available.
- **User** - The name of the user who caused the event.
- **Process** - The fully qualified path to the executable file of the application that caused the event. In some cases, the process name might be displayed instead of the path. Not displayed if process information is not available.

If an alert applies to a USB device (including removable devices and encrypted removable devices), then, directly from the alert, the administrator can add the device to the allowlist, which prevents the device control module from restricting access to that particular device. Clicking **Allow this USB device** adds it to the USB devices allowlist in the device control module's configuration, and also adds it to the [USB devices database](#) for further reference.

See also [steps to view device control alerts](#).

25.6.1 Action field values

Alert **Action** field can contain the following values:

- **Read** - Get data from the device or port.
- **Write** - Send data to the device or port.
- **Format** - Direct access (formatting, check disk, etc.) to the device. In the case of a port, applies to the device connected to that port.
- **Eject** - Remove the device from the system or eject the media from the device. In the case of a port, applies to the device connected to that port.
- **Print** - Send a document to the printer.

- **Copy audio** - Copy/paste audio data via the local clipboard.
- **Copy file** - Copy/paste a file via the local clipboard.
- **Copy image** - Copy/paste an image via the local clipboard.
- **Copy text** - Copy/paste text via the local clipboard.
- **Copy unidentified content** - Copy/paste other data via the local clipboard.
- **Copy RTF data (image)** - Copy/paste an image via the local clipboard using Rich Text Format.
- **Copy RTF data (file)** - Copy/paste a file via the local clipboard using Rich Text Format.
- **Copy RTF data (text, image)** - Copy/paste text along with an image via the local clipboard using Rich Text Format.
- **Copy RTF data (text, file)** - Copy/paste text along with a file via the local clipboard using Rich Text Format.
- **Copy RTF data (image, file)** - Copy/paste an image along with a file via the local clipboard using Rich Text Format.
- **Copy RTF data (text, image, file)** - Copy/paste text along with an image and a file via the local clipboard using Rich Text Format.
- **Delete** - Delete data from the device (for example, a removable device, a mobile device, and so on).
- **Device access** - Access to some device or port (for example, a Bluetooth device, a USB port, and so on).
- **Incoming audio** - Copy/paste audio data from the client computer to the hosted session via the redirected clipboard.
- **Incoming file** - Copy/paste a file from the client computer to the hosted session via the redirected clipboard.
- **Incoming image** - Copy/paste an image from the client computer to the hosted session via the redirected clipboard.
- **Incoming text** - Copy/paste text from the client computer to the hosted session via the redirected clipboard.
- **Incoming unidentified content** - Copy/paste other data from the client computer to the hosted session via the redirected clipboard.
- **Incoming RTF data (image)** - Copy/paste an image from the client computer to the hosted session via the redirected clipboard using Rich Text Format.
- **Incoming RTF data (file)** - Copy/paste a file from the client computer to the hosted session via the redirected clipboard using Rich Text Format.
- **Incoming RTF data (text, image)** - Copy/paste text along with an image from the client computer to the hosted session via the redirected clipboard using Rich Text Format.
- **Incoming RTF data (text, file)** - Copy/paste text along with a file from the client computer to the hosted session via the redirected clipboard using Rich Text Format.
- **Incoming RTF data (image, file)** - Copy/paste an image along with a file from the client computer to the hosted session via the redirected clipboard using Rich Text Format.
- **Incoming RTF data (text, image, file)** - Copy/paste text along with an image and a file from the client computer to the hosted session via the redirected clipboard using Rich Text Format.

- **Insert** - Connect a USB device or a FireWire device.
- **Outgoing audio** - Copy/paste audio data from the hosted session to the client computer via the redirected clipboard.
- **Outgoing file** - Copy/paste a file from the hosted session to the client computer via the redirected clipboard.
- **Outgoing image** - Copy/paste an image from the hosted session to the client computer via the redirected clipboard.
- **Outgoing text** - Copy/paste text from the hosted session to the client computer via the redirected clipboard.
- **Outgoing unidentified content** - Copy/paste other data from the hosted session to the client computer via the redirected clipboard.
- **Outgoing RTF data (image)** - Copy/paste an image from the hosted session to the client computer via the redirected clipboard using Rich Text Format.
- **Outgoing RTF data (file)** - Copy/paste a file from the hosted session to the client computer via the redirected clipboard using Rich Text Format.
- **Outgoing RTF data (text, image)** - Copy/paste text along with an image from the hosted session to the client computer via the redirected clipboard using Rich Text Format.
- **Outgoing RTF data (text, file)** - Copy/paste text along with a file from the hosted session to the client computer via the redirected clipboard using Rich Text Format.
- **Outgoing RTF data (image, file)** - Copy/paste an image along with a file from the hosted session to the client computer via the redirected clipboard using Rich Text Format.
- **Outgoing RTF data (text, image, file)** - Copy/paste text along with an image and a file from the hosted session to the client computer via the redirected clipboard using Rich Text Format.
- **Rename** - Rename files on a device (for example, on removable devices, mobile devices, and others).

26 The Plans tab

Note

The availability of this feature depends on the service quotas that are enabled for your account.

You can manage protection plans and other plans by using the **Plans** tab.

Each section of the **Plans** tab contains all plans of a specific type. The following sections are available:

- **Protection**
- **Backup scanning**
- **Cloud applications backup**
- **VM replication**

26.1 Protection plan

To create the protection plan

1. In the service console, go to **Plans > Protection**.
2. Click **Create plan**.
3. Select the machines that you want to protect.
4. Click **Protect**. You will see the protection plan with the default settings.
5. [Optional] To modify the protection plan name, click on the pencil icon next to the name.
6. [Optional] To enable or disable the plan module, click the switch next to the module name.
7. [Optional] To configure the module parameters, click the corresponding section of the protection plan.
8. Click **Add devices** to select the machines to which you want to apply the plan.
9. When ready, click **Create**.

As a result, the selected devices will be protected with the protection plan.

You can perform the following operations with protection plans:

- Create, view, edit, clone, disable, enable, and delete a protection plan
- View activities related to each protection plan
- View alerts related to each protection plan
- Export a plan to a file
- Import a previously exported plan

26.2 Backup scanning plan

If you need to scan backups on malware, you can create a backup scanning plan.

Note the following:

- The backups that have [CDP recovery points](#) can be selected for scanning but only regular recovery points (excluding CDP recovery points) will be scanned.
- When the CDP backup was selected for safe recovery of an entire machine, the machine will be safely recovered without the data in the CDP recovery point. To restore the CDP data, start the Files/folders recovery activity.

To create a backup scanning plan

1. In the service console, go to **Plans > Backup scanning**.
2. Click **Create plan**.
3. Specify the name of the plan and the following parameters:
 - **Scan type:**
 - **Cloud** – this option cannot be redefined. The backups will be scanned in the cloud data center by the cloud agent. The system automatically selects the cloud agent that will perform scanning.
 - **Backups to scan:**
 - **Locations** – select locations with backups that you want to scan.
 - **Backups** – select backups that you want to scan.
 - **Scan for:**
 - **Malware** – this option cannot be redefined. It checks backups on malware presence.
 - **Encryption** – provide a password to scan encrypted backups. If a vault or multiple backups are selected, then you can specify a single password for all backups. If the password does not suit to a backup, the system will create an alert.
 - **Schedule** – this option cannot be redefined. The scan activity will be started in the cloud storage automatically.
4. When ready, click **Create**.

As a result, the backup scanning plan is created. The specified locations or backups will be scanned by the cloud agent automatically.

26.3 Backup plans for cloud applications

The **Plans > Cloud applications backup** section shows cloud-to-cloud backup plans. These plans back up applications running in the cloud by means of agents that run in the cloud and use the cloud storage as a backup location.

In this section, you can perform the following operations:

- Create, view, run, stop, edit, and delete a backup plan
- View activities related to each backup plan
- View alerts related to each backup plan

For more information about cloud applications backup, refer to:

- [Protecting Microsoft 365 data](#)
- [Protecting Google Workspace data](#)

Running cloud-to-cloud backups manually

To prevent disrupting the Cyber Protection service, the number of manual cloud-to-cloud backup runs is limited to 10 runs per Microsoft 365 or Google Workspace organization during an hour. After this number has been reached, the number of runs allowed is reset to one per hour, and then an additional run becomes available each hour thereafter (e.g. hour 1, 10 runs; hour 2, 1 run; hour 3, 2 runs) until a total of 10 runs per hour is reached.

Backup plans applied to groups of devices (mailboxes, drives, sites) or containing more than 10 devices cannot be run manually.

27 Bootable media

Bootable media is a CD, DVD, USB flash drive, or other removable media that allows you to run the Cyber Protection agent either in a Linux-based environment or a Windows Preinstallation Environment/Windows Recovery Environment (WinPE/WinRE), without the help of an operating system. The main purpose of the bootable media is to recover an operating system that cannot start.

Note

Bootable media does not support hybrid drives.

27.1 Custom or ready-made bootable media?

By using Bootable Media Builder, you can create custom bootable media (Linux-based or WinPE-based) for Windows, Linux, or macOS computers. In the both Linux-based and WinPE/WinRE-based custom bootable media, you can configure additional settings, such as automatic registration, network settings, or proxy server settings. In the WinPE/WinRE-based custom bootable media, you can also add additional drivers.

Alternatively, you can download a ready-made bootable media (Linux-based only). You can use the ready-made bootable media for recovery operations and access to the Universal Restore feature.

27.2 Linux-based or WinPE/WinRE-based bootable media?

27.2.1 Linux-based

Linux-based bootable media contains a Cyber Protection agent based on a 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.

27.2.2 WinPE/WinRE-based

WinPE-based bootable media contains a minimal Windows system called Windows Preinstallation Environment (WinPE) and a Cyber Protection plugin for WinPE, that is, a modification of the Cyber Protection agent that can run in the preinstallation environment. WinRE-based bootable media uses Windows Recovery Environment and does not require installation of additional Windows packages.

WinPE proved to be the most convenient bootable solution in large environments with heterogeneous hardware.

Advantages:

- Using Cyber Protection in Windows Preinstallation Environment provides more functionality than using Linux-based bootable media. Having booted PC-compatible hardware into WinPE, you can

use not only the Cyber 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 allows 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).

27.3 Creating physical bootable media

We highly recommend that you create and test the 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 Cyber 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 physical bootable media in Windows or Linux

1. Create a custom bootable media ISO file or download the ready-made ISO file.
To create a custom ISO file, use "Bootable Media Builder" (p. 523).
To download the ready-made ISO file, in the Cyber Protection service console, select a machine, and then click **Recover > More ways to recover... > Download ISO image**.
2. [Optional] In the Cyber Protection service console, generate a registration token. The registration token is displayed automatically when you download a ready-made ISO file.
This token allows the bootable media to access the cloud storage, without prompting you to enter a login and password.
3. Create physical bootable media in one of the following ways:
 - Burn the ISO file to a CD/DVD.
 - 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, and Win32DiskImager for a BIOS machine. In Linux, using the dd utility makes sense.
For virtual machines, you can connect the ISO file as a CD/DVD drive to the machine that you want to recover.

To create physical 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.

27.4 Bootable Media Builder

Bootable Media Builder is a dedicated tool for creating bootable media. It is installed as an optional component on the machine where the Cyber Protection agent is installed.

27.4.1 Why use Bootable Media Builder?

The ready-made bootable media that is available for download in the service console is based on a Linux kernel. Unlike Windows PE, it does not allow injecting custom drivers on the fly.

Bootable Media Builder allows you to create customized Linux-based and WinPE-based bootable media images.

27.4.2 32-bit or 64-bit?

Bootable Media Builder creates bootable 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).

27.4.3 Linux-based bootable media

To create a Linux-based bootable media

1. Start **Bootable Media Builder**.
2. In **Bootable media type**, select **Default (Linux-based media)**.
3. Select how volumes and network resources will be represented:
 - Bootable media with a Linux-like volume representation displays the volumes as, for example, hda1 and sdb2. It tries to reconstruct MD devices and logical volumes (LVM) before starting a recovery.
 - Bootable media with Windows-like volume representation displays the volumes as, for example, C: and D:. It provides access to dynamic volumes (LDM).
4. [Optional] Specify the parameters of the Linux kernel. Separate multiple parameters with spaces. For example, to be able to select a display mode for the bootable agent each time the media starts, type: **vga=ask**. For more information about the available parameters, refer to "Kernel parameters" (p. 524).
5. [Optional] Select the language for the bootable media.
6. [Optional] Select the boot mode (BIOS or UEFI) that Windows will use after the recovery.
7. Select the component to be placed on the media – the Cyber Protection bootable agent.

8. [Optional] Specify the timeout interval for the boot menu. 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.
9. [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. For more information about the scripts, refer to "Scripts in bootable media" (p. 526).
10. [Optional] Select how to register the bootable media in the Cyber Protection service on booting up. For more information about the registration settings, refer to "Registering the bootable media" (p. 534).
11. Specify the network settings for the network adapters of the booted machine or keep the automatic DHCP configuration.
12. [Optional] If a proxy server is enabled in your network, specify its host name/IP address and port.
13. Select the file type of the created bootable media:
 - ISO image
 - ZIP file
14. Specify a file name for the bootable media file.
15. Check your settings in the summary screen, and then click **Proceed**.

Kernel parameters

You can specify one or more parameters of the Linux kernel that will be automatically applied when the bootable media starts. These parameters are typically used when you experience 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 you are in the boot menu.

Parameters

When specifying multiple parameters, separate them with spaces.

- **acpi=off**
Disables Advanced Configuration and Power Interface (ACPI). You may want to use this parameter when experiencing problems with a particular hardware configuration.
- **noapic**
Disables Advanced Programmable Interrupt Controller (APIC). You may want to use this parameter when experiencing problems with a particular hardware configuration.
- **vga=ask**
Prompts for the video mode to be used by the bootable media's graphical user interface. Without the **vga** parameter, the video mode is detected automatically.
- **vga= *mode_number***
Specifies the video mode to be used by the bootable media's graphical user interface. The mode number is given by *mode_number* in the hexadecimal format—for example: **vga=0x318**

The 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 you are in the boot menu.

If this parameter is removed, 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 the detection of PCMCIA hardware.

- **nomouse**

Disables the mouse support.

- **module_name=off**

Disables the module whose name is given by *module_name*. For example, to disable the use of the SATA module, specify: **sata_sis=off**

- **pci=bios**

Forces the use of PCI BIOS instead of accessing the hardware device directly. You may want to use this parameter if the machine has a non-standard PCI host bridge.

- **pci=nobios**

Disables the use of PCI BIOS; only direct hardware access methods will be allowed. You may want to use this parameter when the bootable media fails to start, which may be caused by the BIOS.

- **pci=biosirq**

Uses PCI BIOS calls to get the interrupt routing table. You may want to use this parameter if the kernel is unable to allocate interrupt requests (IRQs) or discover secondary PCI buses on the motherboard.

These calls might not work properly on some machines. But this may be the only way to get the interrupt routing table.

- **LAYOUTS=en-US, de-DE, fr-FR, ...**

Specifies the keyboard layouts that can be used in the bootable media's graphical user interface. Without this parameter, only two layouts can be used: English (USA) and the layout that corresponds to the language selected in the media's boot menu.

You can specify any of the following layouts:

Belgian: **be-BE**

Czech: **cz-CZ**

English: **en-GB**

English (USA): **en-US**

French: **fr-FR**

French (Swiss): **fr-CH**

German: **de-DE**

German (Swiss): **de-CH**

Italian: **it-IT**

Polish: **pl-PL**

Portuguese: **pt-PT**

Portuguese (Brazilian): **pt-BR**

Russian: **ru-RU**

Serbian (Cyrillic): **sr-CR**

Serbian (Latin): **sr-LT**

Spanish: **es-ES**

When working under a bootable media, use CTRL + SHIFT to cycle through the available layouts.

Scripts in bootable media

If you want the bootable media to perform a predefined set of operations, you can specify a script while creating the media with Bootable Media Builder. Thus, every time a machine is booted from the media, the specified script will run and the user interface will not be shown.

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:

- Recovery from the cloud storage (**entire_pc_cloud**)
- Recovery from a network share (**entire_pc_share**)

The scripts are located in the following folders on the machine where Bootable Media Builder is installed:

- In Windows: **%ProgramData%\Acronis\MediaBuilder\scripts**
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Recovery from the cloud storage

In Bootable Media Builder, specify the following script parameters:

1. The backup file name.
2. [Optional] A password that the script will use to access encrypted backups.

Recovery from a network share

In Bootable Media Builder, specify the following script parameters:

- The path to the network share.
- The user name and password for the network share.
- The backup file name. To find out the backup file name:
 - a. In the Cyber Protection service 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**.
- [Optional] A password that the script will use to access encrypted backups.

Custom scripts

Important

Creating custom scripts requires the knowledge of the Bash command language and JavaScript Object Notation (JSON). If you are not familiar with Bash, a good place to learn it is <http://www.tldp.org/LDP/abs/html>. The JSON specification is available at <http://www.json.org>.

Files of a script

Your script must be located in the following directories on the machine where Bootable Media Builder is installed:

- In Windows: %**ProgramData%**\Acronis\MediaBuilder\scripts\
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

The script must consist of at least three files:

- **<script_file>.sh** - a file with your Bash script. When creating the script, use only a limited set of shell commands, which you can find at <https://busybox.net/downloads/BusyBox.html>. Also, the following commands can be used:

- **acrocmd** - the command-line utility for backup and recovery
- **product** - the command that starts the bootable media user interface

This file and any additional files that the script includes (for example, by using the dot command) must be located in the **bin** subfolder. In the script, specify the additional file paths as **/ConfigurationFiles/bin/<some_file>**.

- **autostart** - a file for starting **<script_file>.sh**. The file contents must be as follows:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - a JSON file that contains the following:
 - The script name and description to be displayed in Bootable Media Builder.
 - The names of the script variables to be configured via Bootable Media Builder.
 - The parameters of controls that will be displayed in Bootable Media Builder for each variable.

Structure of autostart.json

27.4.4 Top-level object

Pair		Required	Description
Name	Value type		
displayName	string	Yes	The script name to be displayed in Bootable Media Builder.
description	string	No	The script description to be displayed in Bootable Media Builder.
timeout	number	No	A timeout (in seconds) for the boot menu before starting the script. If the pair is not specified, the timeout will be ten seconds.
variables	object	No	Any variables for <script_file>.sh that you want to configure via Bootable Media Builder. The value should be a set of the following pairs: the string identifier of a variable and the object of the variable (see the table below).

27.4.5 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 only)	number	No	The minimum value of the spin control in a spin box. If the pair is not specified, the value will be 0.
max (for spinner only)	number	No	The maximum value of the spin control in a spin box. If the pair is not specified, the value will be 100.
step (for spinner only)	number	No	The step value of the spin control in a spin box. If the pair is not specified, the value will be 1.
items (for enum only)	array of strings	Yes	The values for a drop-down list.
required (for string, multiString, password, and enum)	number	No	Specifies if the control value can be empty (0) or not (1). If the pair is not specified, the control value can be empty.

27.4.6 Control type

Name	Description
string	A single-line, unconstrained text box used to enter or edit short strings.
multiString	A multi-line, unconstrained text box used to enter or edit long strings.

password	A single-line, unconstrained text box used to enter passwords securely.
number	A single-line, numeric-only text box used to enter or edit numbers.
spinner	A single-line, numeric-only text box used to enter or edit numbers, with a spin control. Also, called a spin box.
enum	A standard drop-down list, with a fixed set of predetermined values.
checkbox	A check box with two states - the cleared state or the selected state.

The sample **autostart.json** below contains all possible types of controls that can be used to configure variables for **<script_file>.sh**.

```
{
  "displayName": "Autostart script name",
  "description": "This is an autostart script description.",
  "variables": {
    "var_string": {
      "displayName": "VAR_STRING",
      "type": "string", "order": 1,
      "description": "This is a 'string' control:", "default": "Hello,
world!"
    },
    "var_multistring": {
      "displayName": "VAR_MULTISTRING",
      "type": "multiString", "order": 2,
      "description": "This is a 'multiString' control:",
      "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
    },
    "var_number": {
      "displayName": "VAR_NUMBER",
      "type": "number", "order": 3,
      "description": "This is a 'number' control:", "default": 10
    },
    "var_spinner": {
      "displayName": "VAR_SPINNER",
```

```

        "type": "spinner", "order": 4,

        "description": "This is a 'spinner' control:",

        "min": 1, "max": 10, "step": 1, "default": 5
    },

    "var_enum": {

        "displayName": "VAR_ENUM",

        "type": "enum", "order": 5,

        "description": "This is an 'enum' control:",

        "items": ["first", "second", "third"], "default": "second"
    },

    "var_password": {

        "displayName": "VAR_PASSWORD",

        "type": "password", "order": 6,

        "description": "This is a 'password' control:", "default": "qwe"
    },

    "var_checkbox": {

        "displayName": "VAR_CHECKBOX",

        "type": "checkbox", "order": 7,

        "description": "This is a 'checkbox' control", "default": 1
    }
}

```

27.4.7 WinPE-based and WinRE-based bootable media

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, 8.1, 10 (32-bit and 64-bit)

- Windows Server 2012, 2016, 2019 (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 for Windows 10)

Bootable Media Builder supports both 32-bit and 64-bit WinPE distributions. The 32-bit WinPE distributions can also work on 64-bit hardware. However, you need a 64-bit distribution to boot a machine that uses Unified Extensible Firmware Interface (UEFI).

Note

PE images based on WinPE 4 and later require approximately 1 GB of RAM to work.

Creating WinPE or WinRE bootable media

Bootable Media Builder provides two methods of integrating Cyber Protection with WinPE and WinRE:

- Creating an ISO file with the Cyber Protection plugin from scratch.
- Adding the Cyber Protection plugin to a WIM file for any future purpose (manual ISO building, adding other tools to the image and so on).

To create WinPE or WinRE bootable media

1. On the machine where the Cyber Protection agent is installed, run Bootable Media Builder.
2. In **Bootable media type**, select **Windows PE** or **Windows PE (64-bit)**. A 64-bit media is required to boot a machine that uses Unified Extensible Firmware Interface (UEFI).
3. Select the subtype of the bootable media: **WinRE** or **WinPE**.

Creating WinRE bootable media does not require installation of any additional packages.

To create a 64-bit WinPE media, you must download Windows Automated Installation Kit (AIK) or Windows Assessment and Deployment Kit (ADK). To create 32-bit WinPE media, in addition to downloading the AIK or ADK, you need to do the following:

- a. Click **Download the Plug-in for WinPE (32-bit)**.
 - b. Save the plugin to **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Optional] Select the language for the bootable media.
 5. [Optional] Select the boot mode (BIOS or UEFI) that Windows will use after the recovery.

6. Specify the network settings for the network adapters of the booted machine or keep the automatic DHCP configuration.
7. [Optional] Select how to register the bootable media in the Cyber Protection service on booting up. For more information about the registration settings, refer to "Registering the bootable media" (p. 534).
8. [Optional] Specify the Windows drivers to be added to the bootable media.
After you boot a machine into Windows PE or Windows RE, the drivers can help you access the device where the backup is located. Add 32-bit drivers if you use a 32-bit WinPE or WinRE distribution or 64-bit drivers if you use a 64-bit WinPE or WinRE distribution.
To add the drivers:
 - Click **Add**, and then 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 or WinRE media.
9. Select the file type of the created bootable media:
 - ISO image
 - WIM image
10. Specify the full path to the resulting image file, including the file name.
11. Check your settings in the summary screen, and then click **Proceed**.

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:\RecoveryWIMMedia.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.

Preparation: WinPE 2.x and 3.x

To be able to create or modify PE 2.x or 3.x images, install Bootable Media Builder on a machine where Windows Automated Installation Kit (AIK) is installed. If you do not have a machine with AIK, prepare it as follows.

To prepare a machine with AIK

1. Download and install Windows Automated Installation Kit.
Automated Installation Kit (AIK) for Windows Vista (PE 2.0):

<http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en>

Automated Installation Kit (AIK) for Windows Vista SP1 and Windows Server 2008 (PE 2.1):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en>

Automated Installation Kit (AIK) for Windows 7 (PE 3.0):

<http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en>

Automated Installation Kit (AIK) Supplement for Windows 7 SP1 (PE 3.1):

<http://www.microsoft.com/download/en/details.aspx?id=5188>

You can find system requirements for installation by following the above links.

2. [Optional] Burn the WAIK to DVD or copy it to a flash drive.
3. Install the Microsoft .NET Framework from this kit (NETFXx86 or NETFXx64, depending on your hardware).
4. Install Microsoft Core XML (MSXML) 5.0 or 6.0 Parser from this kit.
5. Install Windows AIK from this kit.
6. Install Bootable Media Builder on the same machine.

Preparation: WinPE 4.0 and later

To be able to create or modify PE 4 or later images, install Bootable Media Builder on a machine where Windows Assessment and Deployment Kit (ADK) is installed. If you do not have a machine with ADK, prepare it as follows.

To prepare a machine with ADK

1. Download the setup program of Assessment and Deployment Kit.
Assessment and Deployment Kit (ADK) for Windows 8 (PE 4.0): <http://www.microsoft.com/en-us/download/details.aspx?id=30652>.
Assessment and Deployment Kit (ADK) for Windows 8.1 (PE 5.0): <http://www.microsoft.com/en-US/download/details.aspx?id=39982>.
Assessment and Deployment Kit (ADK) for Windows 10 (PE for Windows 10):
<https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx>.
You can find system requirements for installation by following the above links.
2. Install Assessment and Deployment Kit on the machine.
3. Install Bootable Media Builder on the same machine.

27.4.8 Registering the bootable media

Registering the bootable media in the Cyber Protection service allows accessing the cloud storage for your backups. You can preconfigure the registration while creating the bootable media. If the registration is not preconfigured, you can register the media after booting a machine with it.

To preconfigure the registration in the Cyber Protection service

1. In Bootable Media Builder, navigate to **Bootable media registration**.
2. In **Service URL**, specify the Cyber Protection service address.
3. [Optional] In **Display name**, specify a name for the booted machine.
4. To set the automatic registration in the Cyber Protection service, select the **Register the bootable media automatically** check box, and then select the level of automatic registration:
 - **Ask for registration token at booting up**
The token has to be provided every time when a machine is booted from this bootable media.
 - **Use the following token**
The machine will be registered automatically when it is booted from this bootable media.

To register the bootable media after booting a machine from it

1. Boot the machine from the bootable media.
2. In the startup window, click **Register media**.
3. In **Server**, specify the Cyber Protection service address.
4. In **Registration token**, enter the registration token.
5. Click **Register**.

27.4.9 Network settings

While creating bootable media, you can preconfigure the network connections that will be used by the bootable agent. The following parameters can be preconfigured:

- IP address
- Subnet mask
- Gateway
- DNS server
- WINS server

After 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 preconfigured, the agent uses DHCP auto configuration.

You can also configure the network settings manually when the bootable agent is running on the machine.

Preconfiguring multiple network connections

You can preconfigure TCP/IP settings for up to ten network interface cards (NICs). 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 and saved 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.

After the bootable agent starts on the server, it retrieves the list of available NICs. This list is sorted by the slots that the NICs occupy, the closest to the processor is on top.

The bootable agent assigns each known NIC the appropriate settings, and identifies the NICs by their MAC addresses. After the NICs with known MAC addresses are configured, the remaining NICs are assigned the settings that you made for non-existent NICs, starting from the upper non-assigned NIC.

You can customize the 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 not find the NICs with known MAC addresses and will configure the NICs in the same order as you did.

Example

The bootable agent can use one of the network adapters for communication with the management console through the production network. Automatic configuration can be done for this connection. Sizeable data for recovery can be transferred through the second NIC, included in the dedicated backup network by means of static TCP/IP settings.

27.5 Connecting to a machine booted from bootable media

27.5.1 Local connection

To operate directly on the machine booted from bootable media, click **Manage this machine locally** in the startup window.

After a machine boots from bootable media, the machine terminal displays a startup window with the IP addresses obtained from DHCP or set according to the preconfigured values.

27.5.2 Configuring network settings

To change the network settings for a current session, in the startup window, click **Configure network**. The **Network Settings** window that appears allows you to configure the network settings for each network interface card (NIC) of the machine.

The changes that are made during a session will be lost after the machine reboots.

Adding VLANs

In the **Network Settings** window, you can add virtual local area networks (VLANs). Use this functionality if you need access to a backup location that is included in a specific VLAN.

VLANs are mainly used to divide a local area network into segments. A NIC that is connected to an access port of the switch always has access to the VLAN specified in the port configuration. A NIC

connected to a *trunk* port of the switch can access the VLANs allowed in the port configuration only if you specify the VLANs in the network settings.

To enable access to a VLAN via a trunk port

1. Click **Add VLAN**.
2. Select the NIC that provides access to the local area network that includes the required VLAN.
3. Specify the VLAN identifier.

After you click **OK**, a new entry appears in the list of network adapters.

If you need to remove a VLAN, click the required VLAN entry, and then click **Remove VLAN**.

27.6 Operations with bootable media

Operations with bootable media are similar to the recovery operations that are performed under a running operating system. The differences are as follows:

1. Under bootable media with a Windows-like volume representation, a volume has the same drive letter as in Windows. Volumes that do not have drive letters in Windows (such as the System Reserved volume) are assigned free letters in order of their sequence on the disk.

If the bootable media cannot detect Windows on the machine or detects more than one, all volumes, including those without drive letters, are assigned letters in order of their sequence on the disk. Thus, the volume letters may differ from those seen in Windows. For example, the D: drive under the bootable media might correspond to the E: drive in Windows.

Note

It is advisable to assign unique names to the volumes.

2. The bootable media with a Linux-like volume representation shows local disks and volumes as unmounted (sda1, sda2...).
3. Tasks cannot be scheduled. If you need to repeat an operation, configure it from scratch.
4. The log lifetime is limited to the current session. You can save the entire log or the filtered log entries to a file.
5. Centralized vaults are not shown in the folder tree of the **Archive** window.

To access a managed vault, enter the following string in the **Path** field:

bsp://node_address/vault_name/

To access an unmanaged centralized vault, specify the full path to the vault's folder.

After entering the access credentials, you will see a list of archives that are located in the vault.

27.6.1 Setting up a display mode

When you boot a machine via Linux-based bootable media, a display video mode is detected automatically based on the hardware configuration (monitor and graphics card specifications). If the video mode is detected incorrectly, do the following:

1. In the boot menu, press F11.
2. On the command line, enter **vga=ask**, and then proceed with booting.
3. From the list of supported video modes, choose the appropriate mode by typing its number (for example, **318**), and then press **Enter**.

If you do not want to follow this procedure every time you boot a given hardware configuration, recreate the bootable media with the appropriate mode number (in the example above, **vga=0x318**) specified in the **Kernel parameters** field.

27.6.2 Recovery

1. Boot your machine from the bootable media.
2. Click **Manage this machine locally**.
3. Click **Recover**.
4. In **What to recover**, click **Select data**.
5. Select the backup file that you want to recover from.
6. In the lower left pane, select the drives/volumes or files/folders that you want to recover, and then click **OK**.
7. Configure the overwriting rules.
8. Configure the recovery exclusions.
9. Configure the recovery options.
10. Check that your settings are correct, and then click **OK**.

27.7 Startup Recovery Manager

Startup Recovery Manager is a bootable component that resides on the Windows system disk or on the Linux /boot partition. With Startup Recovery Manager, you can start the bootable rescue utility without using separate bootable media.

Startup Recovery Manager is especially useful for traveling users. If a failure occurs, reboot the machine, wait for the prompt **Press F11 for Acronis Startup Recovery Manager** to appear, and then press F11. The program starts and you can perform recovery. On machines with the GRUB boot loader installed, you select the Startup Recovery Manager from the boot menu, instead of pressing F11 during a reboot.

To use Startup Recovery Manager, you have to activate it first. Thus, you enable the boot-time prompt **Press F11 for Acronis Startup Recovery Manager** (or add the **Startup Recovery Manager** item to GRUB menu if you use the GRUB boot loader).

Note

To activate Startup Recovery Manager, you need at least 100 MB of free space on the Windows system disk or the Linux /boot partition.

Unless you use the GRUB boot loader and it is installed in the Master Boot Record (MBR), Startup Recovery Manager activation overwrites the MBR with its own boot code. Thus, you may need to reactivate third-party boot loaders if such boot loaders are installed.

In Linux, when using a boot loader other than GRUB (such as LILO, for example), consider installing it to a Linux root (or boot) partition boot record instead of the MBR, before activating Startup Recovery Manager. Otherwise, reconfigure the boot loader manually after the activation.

To activate Startup Recovery Manager on a machine with Agent for Windows or Agent for Linux

1. In the Cyber Protection service console, select the machine that you want to activate Startup Recovery Manager on.
2. Click **Details**.
3. Enable the **Startup Recovery Manager** switch.
4. Wait while the software activates Startup Recovery Manager.

To activate Startup Recovery Manager on a machine without an agent

1. Boot the machine from bootable media.
2. Click **Tools > Activate Startup Recovery Manager**.
3. Wait while the software activates Startup Recovery Manager.

To deactivate Startup Recovery Manager, repeat the activation procedure and select the respective opposite actions. The deactivation disables the boot-time prompt **Press F11 for Acronis Startup Recovery Manager** (or the menu item in GRUB).

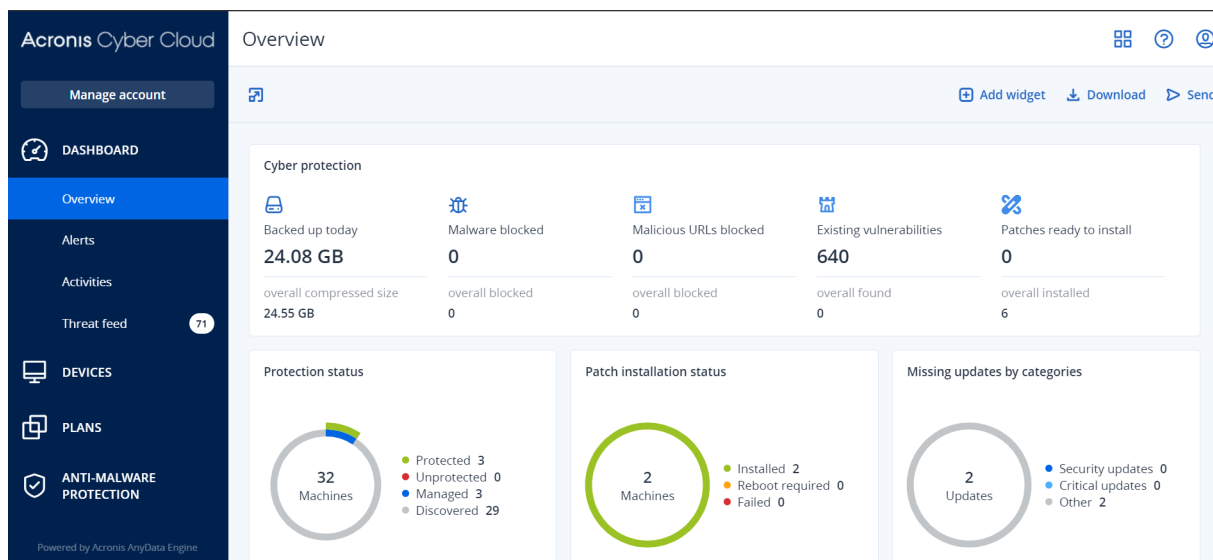
28 Monitoring

The **Overview** dashboard provides a number of customizable widgets that give an overview of operations related to the Cyber Protection service. Widgets for other services will be available in future releases.

The widgets are updated every five minutes. The widgets have clickable elements that enable you to investigate and troubleshoot issues. You can download the current state of the dashboard or send it via email in the .pdf or/and .xlsx format.

You can choose from a variety of widgets, presented as tables, pie charts, bar charts, lists, and tree maps. You can add multiple widgets of the same type with different filters.

The buttons **Download** and **Send** in **Dashboard > Overview** are not available in the Standard editions of the Cyber Protection service.



To rearrange the widgets on the dashboard

Drag and drop the widgets by clicking on 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 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 **Customize** when the widget is selected. After editing the widget, click **Done**.

To remove a widget

Click the X sign next to the widget name.

The **Activities** dashboard provides a list of events that occurred during the past 90 days.

You can search by the following criteria:

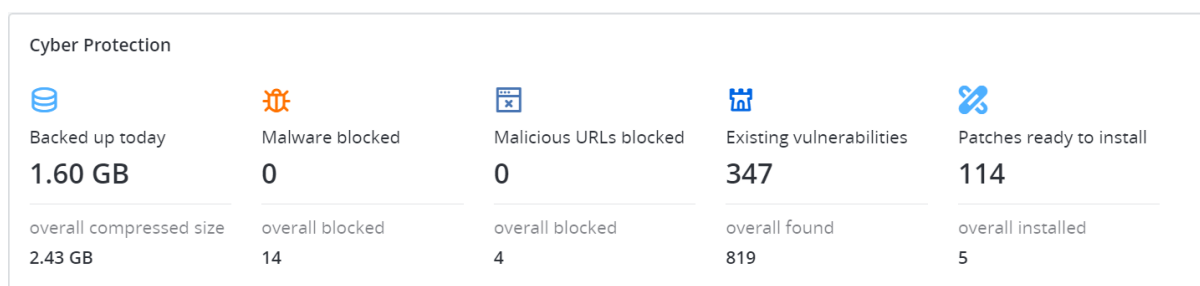
- Device name
- The user who started the activity, for example, a backup.

You can also filter the activities by the following properties:

- Status, for example, succeeded, failed, in progress, and so on.
- Type, for example protection plan, applying plan, deleting backups, and so on.
- Time frame, for example, the most recent activities or a specific period of time.

28.1 Cyber Protection

This widget shows the overall information about the size of backups, blocked malware, blocked URLs, found vulnerabilities, and installed patches.



The upper row shows the current statistics:

- **Backed up today** – the sum of recovery point sizes for the last 24 hours
- **Malware blocked** – the number of currently active alerts about malware blocked
- **URLs blocked** – the number of currently active alerts about URLs blocked
- **Existing vulnerabilities** – the number of currently existing vulnerabilities
- **Patches ready to install** – the number of currently available patches to be installed

The lower row shows the overall statistics:

- The compressed size of all backups
- The accumulated number of blocked malware across all machines
- The accumulated number of blocked URLs across all machines
- The accumulated number of discovered vulnerabilities across all machines
- The accumulated number of installed updates/patches across all machines

28.2 Protection status

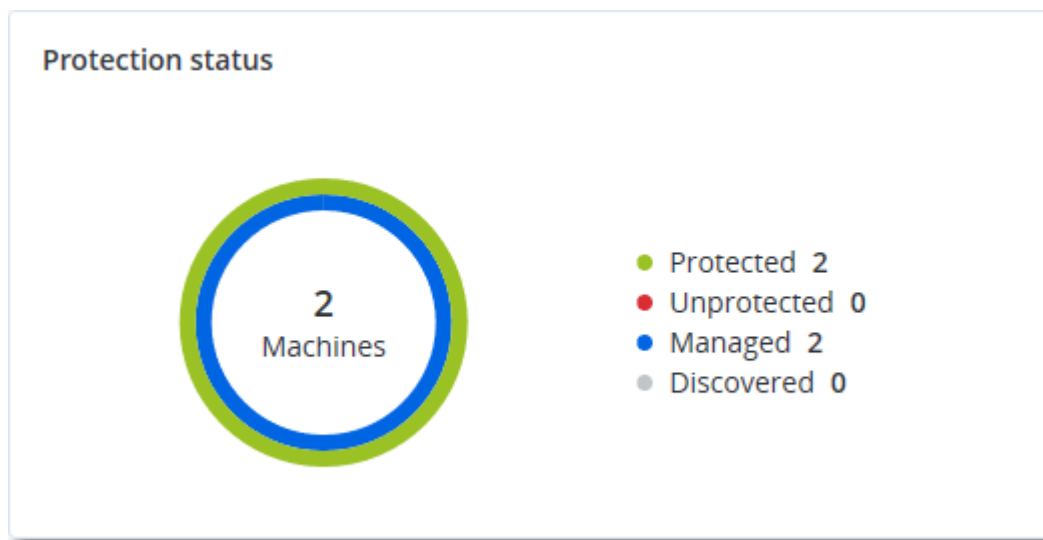
28.2.1 Protection status

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.



28.2.2 Discovered machines

This widget shows the list of discovered machines during the specified time range.

Discovered machines				
Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSC				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSC	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSC	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSC	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSC	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSC	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual











28.3 #CyberFit Score by machine

This widget shows for each machine the total #CyberFit Score, its compound scores, and findings for each of the assessed metrics:

- Antimalware
- Backup
- Firewall
- VPN
- Encryption
- NTLM traffic

To improve the score of each of the metrics, you can view the recommendations that are available in the report.

For more details about the #CyberFit Score, refer to "[#CyberFit Score for machines](#)".

#CyberFit Score by machine 			
Metric	#CyberFit Score	Findings	
▼  DESKTOP-2N2TRE8	 625 / 850		
Anti-malware	 275 / 275	You have anti-malware protection enabled	
Backup	 175 / 175	You have a backup solution protecting your data	
Firewall	 175 / 175	You have a firewall enabled for public and private networks	
VPN	 0 / 75	No VPN solution was found, your connection to public and shared networks is n...	
Encryption	 0 / 125	No disk encryption was found, your device is at risk from physical tampering	
NTLM traffic	 0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...	

28.4 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.
- On NVMe drives, disk health monitoring is supported only for drives that communicate the SMART data via the Windows API. Disk health monitoring is not supported for NVMe drives that require reading the SMART data directly from the drive.

The disk health is represented by one of the following statuses:

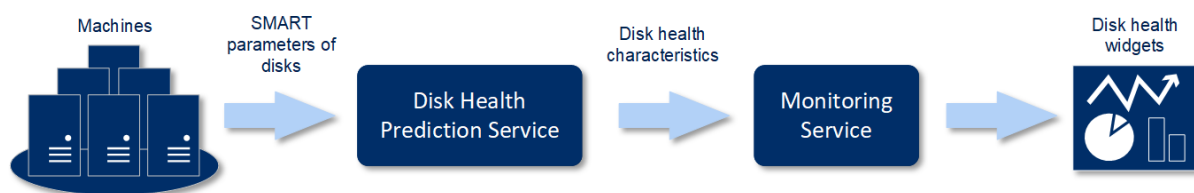
- **OK**
Disk health is between 70% and 100%.
- **Warning**
Disk health is between 30% and 70%.
- **Critical**
Disk health is between 0% and 30%.
- **Calculating disk data**
The current disk status and forecast are being calculated.

28.4.1 How it works

The 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 the 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. The Disk Health Prediction Service processes the received SMART parameters, makes forecasts, and then 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 one month.
3. The Monitoring Service receives these characteristics, and then shows the relevant information in the disk health widgets in the service console.



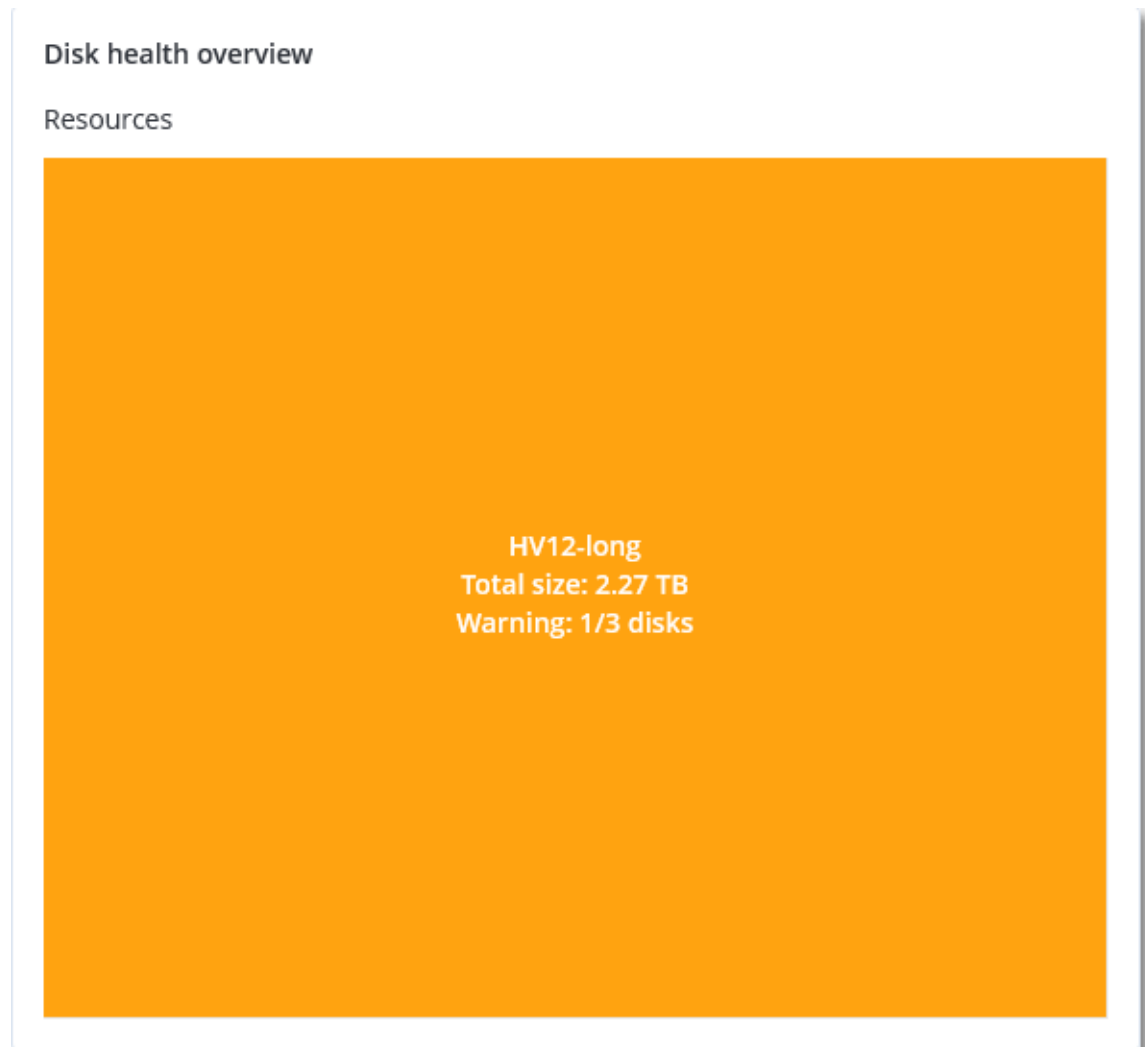
28.4.2 Disk health widgets

The results of the disk health monitoring are presented in the following widgets that are available in the service 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 health status of the selected customer machines. Only the most critical disk status is shown. The other statuses are shown in a tooltip when you hover over a particular block. The machine block size depends on the total size of all disks of the machine. The machine block color depends on the most critical disk status found.



- Disk level

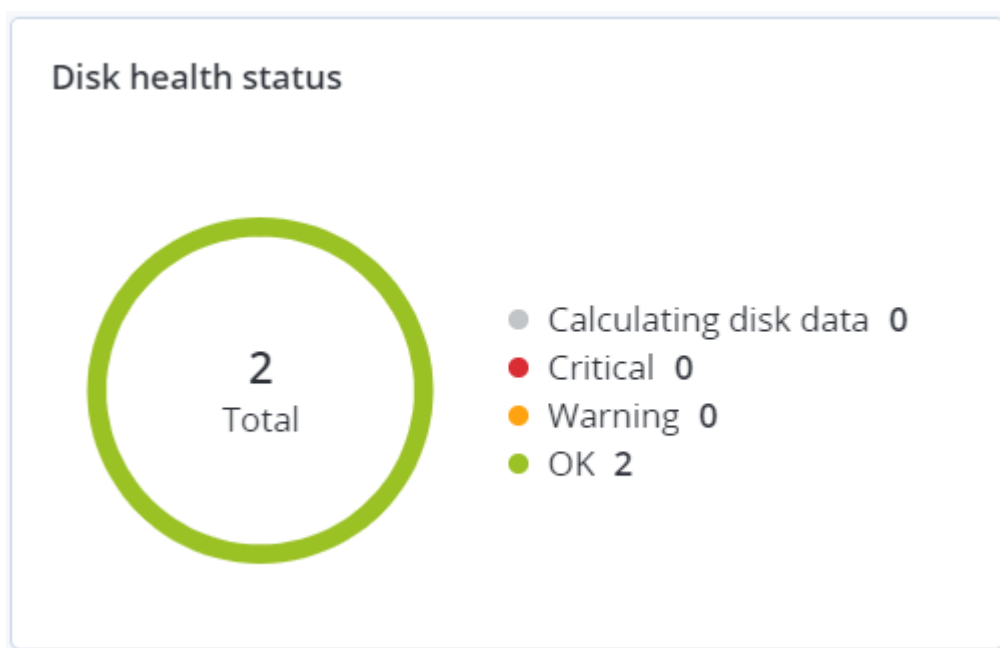
Shows the current disk health status of all disks for the selected machine. Each disk block shows one of the following disk health forecasts and its probability in percentage:

- Will be degraded
- Will stay stable

- Will be improved



- **Disk health status** is a pie chart widget that shows the number of disks for each status.



28.4.3 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 changes from **Warning** to **Critical**, an alert always is 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.

28.5 Data protection map

The data protection map feature allows you to discover all data that are important for you and get detailed information about number, size, location, protection status of all important files in a treemap scalable view.

Each block size depends on the total number/size of all important files that belong to a customer/machine.

Note

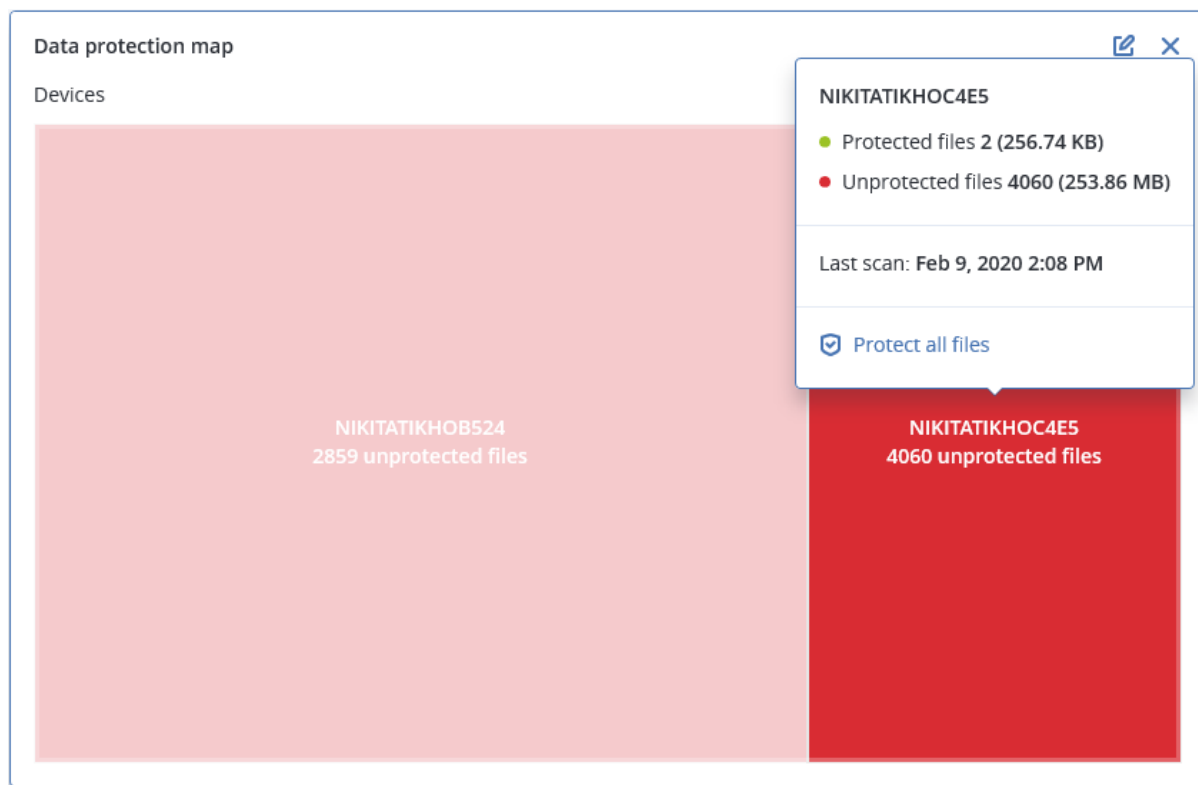
The availability of this feature depends on the service quotas that are enabled for your account.

Files can have one of the following protection statuses:

- **Critical** – there are 51-100% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **Low** – there are 21-50% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **Medium** – there are 1-20% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **High** – all files with the extensions specified by you are protected (backed up) for the selected machine/location.

The results of the data protection examination can be found on the dashboard in the Data Protection Map widget, a treemap widget that shows details on a machine level:

- Machine level – shows information about the protection status of important files per machines of the selected customer.



To protect files that are not protected, hover over the block and click **Protect all files**. In the dialog window, you can find 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.

28.6 Vulnerability assessment widgets

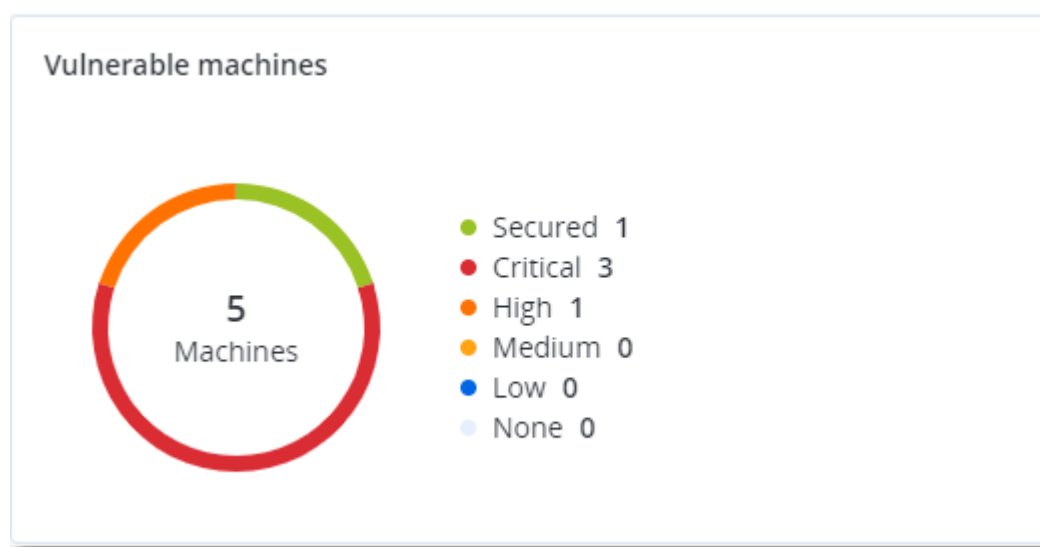
28.6.1 Vulnerable machines

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



28.6.2 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.

Machine name	Vendor	Product	Vulnerability name/ID	Severity ↓	Last detected	First detected	⚙
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
More							

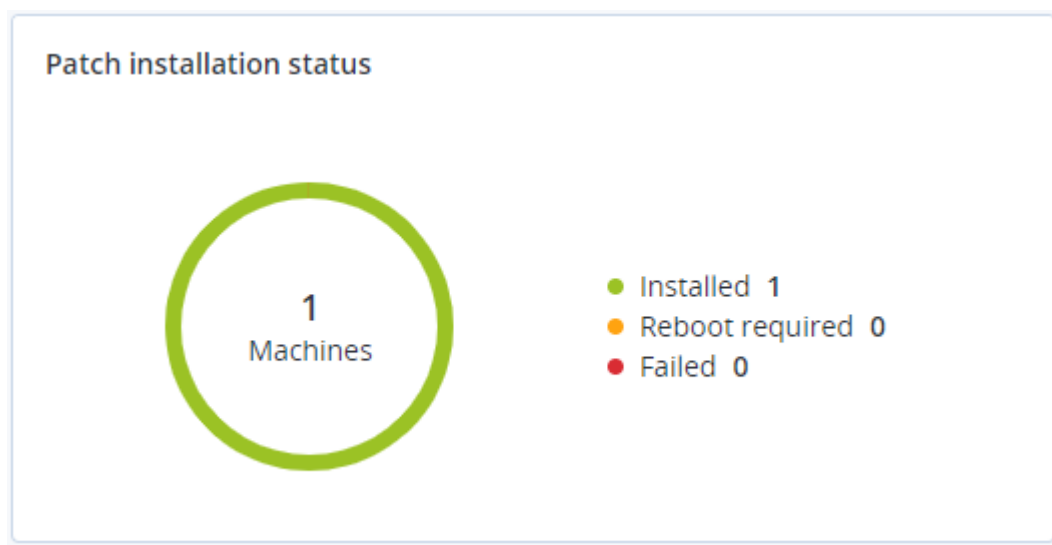
28.7 Patch installation widgets

There are four widgets related to the patch management functionality.

28.7.1 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



28.7.2 Patch installation summary

This widget shows the summary of patches on machines by the patch installation status.

Patch installation summary							
Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

28.7.3 Patch installation history

This widget shows the detailed information about patches on machines.

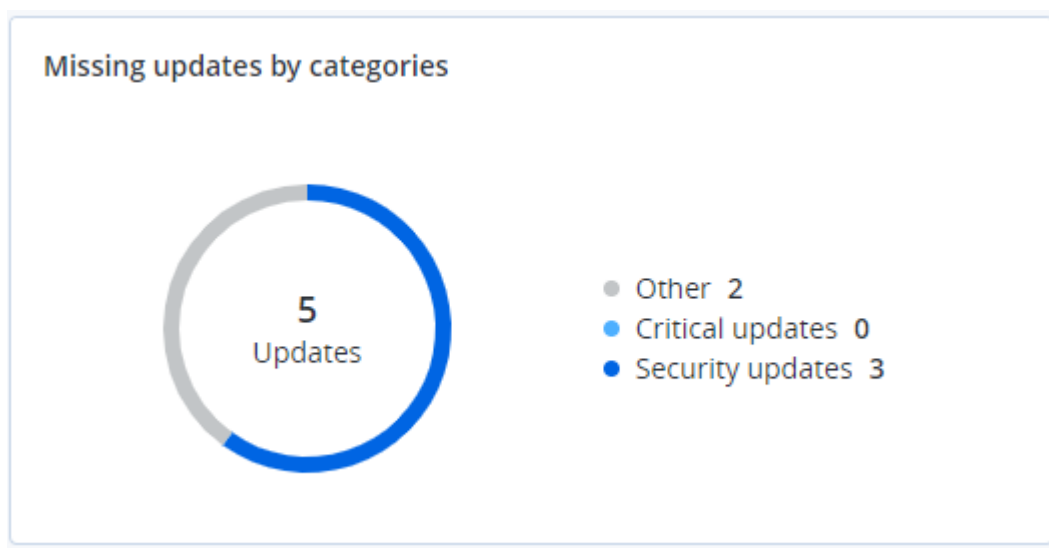
Patch installation history						
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

28.7.4 Missing updates by categories

This widget shows the number of missing updates per category. The following categories are shown:

- Security updates
- Critical updates

- Other



28.8 Backup scanning details

This widget shows the detailed information about the detected threats in backups.

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM	

More

28.9 Recently affected

This widget shows the detailed information about recently infected machines. You can find information about what threat was detected and how many files were infected.

Recently affected					
Machine name	Protection plan	Threat	Affected files	Detection time	⚙
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlyIgen2	15	27.12.2	<div>Folder</div> <div>Customer</div> <div>✓ Machine name</div> <div>✓ Protection plan</div> <div>Detected by</div> <div>✓ Threat</div> <div>File name</div> <div>File path</div> <div>✓ Affected files</div> <div>✓ Detection time</div>

28.10 Cloud applications

This widget shows detailed information about cloud-to-cloud resources:

- Microsoft 365 users (mailbox, OneDrive)
- Microsoft 365 groups (mailbox, group site)
- Microsoft 365 public folders
- Microsoft 365 site collections
- Microsoft 365 Teams
- Google Workspace users (Gmail, Google Drive)
- Google Workspace shared drives

Cloud applications					✎ ✕
Device name	Protection status ↑	Last successful backup	Next backup	Number of backups	⚙
👤 HR - Onboarding	✓ OK	06/17/2020 10:48 AM	06/18/2020 7:34 AM	1	
👤 Sales and Marketing	✓ OK	06/17/2020 10:49 AM	06/18/2020 4:48 AM	1	
👤 HR Leadership Team	✓ OK	06/17/2020 10:48 AM	06/18/2020 6:51 AM	1	
👤 Retail	✓ OK	06/17/2020 10:47 AM	06/18/2020 2:53 AM	1	
👤 Contoso	✓ OK	06/17/2020 10:47 AM	06/17/2020 3:23 PM	1	
👤 U.S. Sales	✓ OK	06/17/2020 10:48 AM	06/18/2020 3:30 AM	1	
👤 IT	✓ OK	06/17/2020 10:48 AM	06/17/2020 10:35 PM	1	
👤 Mark 8 Project Team	⚠ Warning	06/17/2020 10:49 AM	06/18/2020 3:06 AM	1	
👤 Finance	✓ OK	06/17/2020 10:47 AM	06/17/2020 4:38 PM	1	
👤 Sales	⚠ Warning	06/17/2020 10:47 AM	06/17/2020 2:06 PM	1	
More					

Additional information about cloud-to-cloud resources is also available in the following widgets:

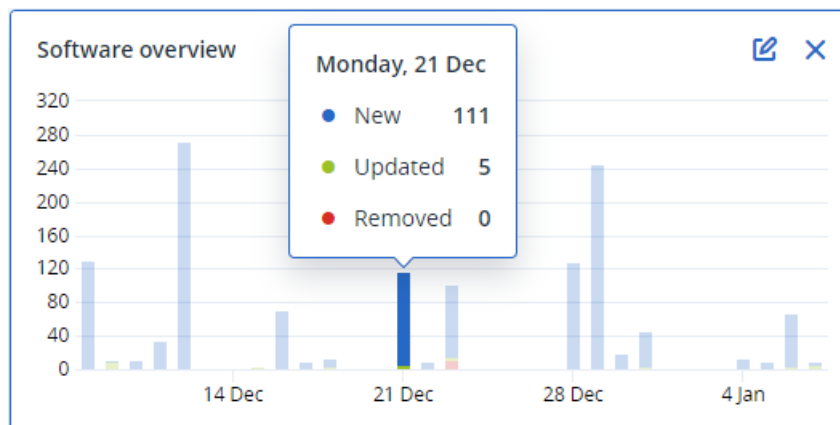
- Activities
- Activity list
- 5 latest alerts
- Alerts history
- Active alerts summary
- Historical alerts summary
- Active alert details
- Locations summary

28.11 Software inventory widgets

The **Software inventory** table widget shows detailed information about the all the software that is installed on Windows and macOS devices in your organization.

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
Ivelins-Mac-mini-2.local									
Ivelins-Mac-mini-2.local	-	15.0.26046	-	No change	-	12/12/2020, 3:26 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Pages.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Keynote.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Numbers.a...	root
Ivelins-Mac-mini-2.local	Canon iScanner2	4.0.0	Canon Inc. (XE2XNRRKZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon iScanner4	4.0.0	Canon Inc. (XE2XNRRKZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon iScanner6	4.0.0	Canon Inc. (XE2XNRRKZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	commandFilter	1.71	EPSON (TXAEAVSRN4)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Printers/EPSON/...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Assis...	1	Acronis International Gm...	No change	-	12/13/2020, 10:01 AM	12/14/2020, 10:24 AM	/Applications/Utilities/Cy...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Unin...	1	Acronis International Gm...	No change	-	12/13/2020, 3:28 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root

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).



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.

28.12 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.

Hardware inventory												
Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard serial	BIOS version	Domain	Registered owner	Registered organization	Scan date and time
Ivelins-Mac-mini-2.local	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 AM
00003079.corp...	Microsoft Windows...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details						
Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1	Mac-7BA5B2DFE22DD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

[More](#)

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).

Hardware changes						
Machine name	Hardware category	Status	Old value	New value	Modification date and time	
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3, ...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM	
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Toronto 5C1, PF0PJ810	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM	

[More](#)

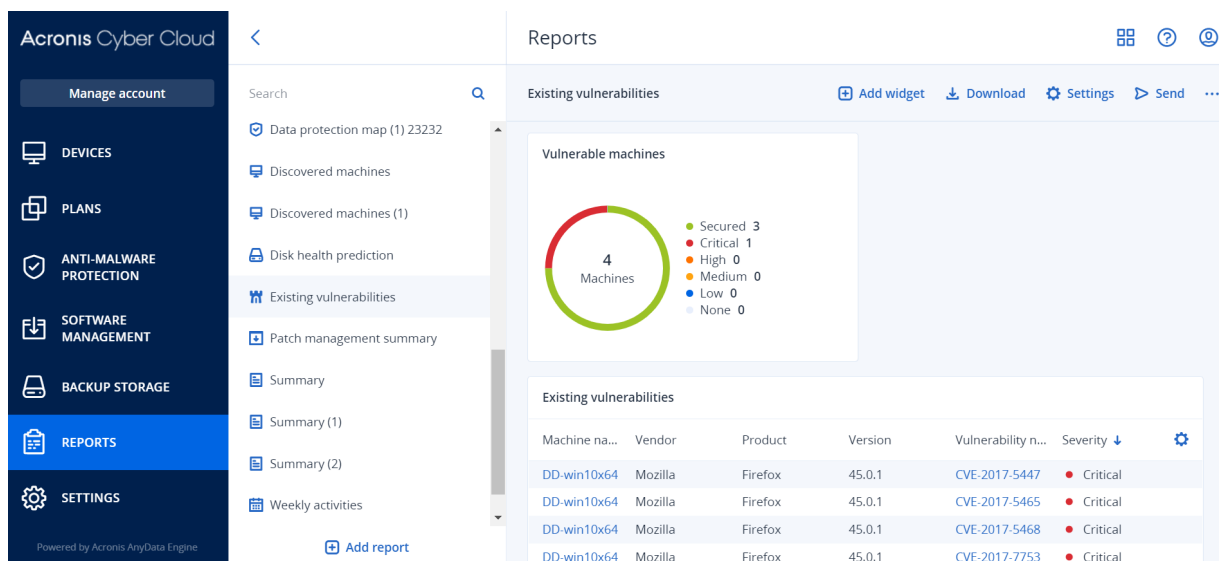
29 Reports

Note

The availability of this feature depends on the service quotas that are enabled for your account.

A report about operations can include any set of the [dashboard widgets](#). All of the widgets show the summary information for the entire company. All of the widgets show the parameters for the same time range. You can change this range in the report settings.

You can use default reports or create a custom report.



The set of default reports depends on the Cyber Protection service edition that you have. The default reports are listed below:

Report name	Description
#CyberFit Score by machine	Shows the #CyberFit Score, based on the evaluation of security metrics and configurations for each machine, and recommendations for improvements.
Alerts	Shows alerts that occurred during a specified time period.
Backup scanning details	Shows the detailed information about detected threats in the backups.
Daily activities	Shows the summary information about activities performed during a specified time period.
Data protection map	Shows the detailed information about the number, size, location, protection status of all important files on machines.
Detected threats	Shows the details of the affected machines by number of blocked threats and the healthy and vulnerable machines.
Discovered	Shows all found machines in the organization network.

machines	
Disk health prediction	Shows predictions when your HDD/SSD will break down and current disk status.
Existing vulnerabilities	Shows the existing vulnerabilities for OS and applications in your organization. The report also displays the details of the affected machines in your network for every product that is listed.
Software inventory	Shows information about the software that is installed on your company devices.
Hardware inventory	Shows information about the hardware that is available on your company devices.
Patch management summary	Shows the number of missing patches, installed patches, and applicable patches. You can drill down the reports to get the missing/installed patch information and details of all the systems.
Summary	Shows the summary information about the protected devices for a specified time period.
Weekly activities	Shows the summary information about activities performed during a specified time period.

To view a report, click its name.

To access operations with a report, click the ellipsis icon on the report line. The same operations are available from within the report.

29.0.1 Adding 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**, click the report name (the names assigned by default look like **Custom(1)**), and then add widgets to the report.
3. [Optional] Drag and drop the widgets to rearrange them.
4. [Optional] Edit the report as described below.

29.0.2 Editing a report

To edit a report, click its name, and then click **Settings**. When editing a 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

General

Name

Backup scanning details

☐ Set one tenant for all widgets

Range

7 days

Scheduled



Recipients

user1@example.com; user2@example.com

File format

Excel and PDF

Language

English

Days of week

Monthly

SUN

MON

TUE

WED

THU

FRI

SAT

Send at

12:00 AM

29.0.3 Scheduling a report

1. Click the report name, and then click **Settings**.
2. Enable the **Scheduled** switch.
3. Specify the recipients' email addresses.
4. Select the report format: .pdf, .xlsx, or both.

5. Select the days and the time when the report will be sent.
6. Click **Save** in the upper right corner.

Note

The maximum number of exported items is: in a .pdf file—1000; in an .xlsx file—10 000.

29.0.4 Exporting and importing the report structure

You can export and import the report structure (the set of widgets and the report settings) to a .json file.

To export the report structure, click the report name, click the ellipsis icon in the top-right corner, and then click **Export**.

To import the report structure, click **Add report**, and then click **Import**.

29.0.5 Downloading a report

You can download a report, click **Download** and select the formats needed:

- Excel and PDF
- Excel
- PDF

29.0.6 Dumping the report data

You can send a dump of the report data in a .csv file via email. The dump includes all of the report data (without filtering) for a custom time range. The timestamps in CSV reports are in the UTC format whereas in Excel and PDF reports the timestamps are in the current system time zone.

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. Click the report name.
2. Click the ellipsis icon in the top-right corner, and then click **Dump data**.
3. Specify the recipients' email addresses.
4. In **Time range**, specify the time range.
5. Click **Send**.

Note

The maximum number of items exported in a .csv file is 150 000.

30 Troubleshooting

This section describes how to save an agent log to a .zip file. If a backup fails for an unclear reason, this file will help the technical support personnel to identify the problem.

To collect logs

1. Select the machine that you want to collect the logs from.
2. Click **Activities**.
3. Click **Collect system information**.
4. If prompted by your web browser, specify where to save the file.

Glossary

B

Backup set

A group of backups to which an individual retention rule can be applied. For the Custom backup scheme, the backup sets correspond to the backup methods (Full, Differential, and Incremental). In all other cases, the backup sets are Monthly, Daily, Weekly, and Hourly. A monthly backup is the first backup created after a month starts. A weekly backup is the first backup created on the day of the week selected in the Weekly backup option (click the gear icon, then Backup options > Weekly backup). If a weekly backup is the first backup created after a month starts, this backup is considered monthly. In this case, a weekly backup will be created on the selected day of the next week. A daily backup is the first backup created after a day starts, unless this backup falls within the definition of a monthly or weekly backup. An hourly backup is the first backup created after an hour starts, unless this backup falls within the definition of a monthly, weekly, or daily backup.

C

Cloud server

[Disaster Recovery] General reference to a recovery or a primary server.

Cloud site (or DR site)

[Disaster Recovery] Remote site hosted in the cloud and used for running recovery infrastructure, in case of a disaster.

D

Data loss prevention (formerly, data leak prevention)

A system of integrated technologies and organizational measures aimed at detecting and preventing accidental or intentional disclosure / access to confidential, protected, or sensitive data by unauthorized entities outside or inside the organization, or the transfer of such data to untrusted environments.

Data loss prevention agent

A data loss prevention system's client component that protects its host computer from unauthorized use, transmission, and storage of confidential, protected, or sensitive data by applying a combination of context and content analysis techniques and enforcing centrally managed data loss prevention policies. Cyber Protection provides a fully featured data loss prevention agent. However, the functionality of the agent on a protected computer is limited to the set of data loss prevention features available for licensing in Cyber Protection, and depends upon the protection plan applied to that computer.

Device control module

As part of a protection plan, the device control module leverages a functional subset of the data loss prevention agent on each protected computer to detect and prevent unauthorized access and transmission of data over local computer channels. These include user access to peripheral devices and ports, document printing, clipboard copy/paste operations, media format and eject operations, as well as synchronizations with locally connected mobile

devices. The device control module provides granular, contextual control over the types of devices and ports that users are allowed to access on the protected computer and the actions that users can take on those devices.

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

Failback

Switching a workload from a spare server (such as a virtual machine replica or a recovery server running in the cloud) back to the production server.

Failover

Switching a workload from a production server to a spare server (such as a virtual machine replica or a recovery server running in the cloud).

Finalization

The operation that makes a temporary virtual machine that is running from a backup into a permanent virtual machine. Physically, this means recovering all of the virtual machine disks, along with the changes that occurred while the machine was running, to the datastore that stores these changes.

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.

L

Local site

[Disaster Recovery] The local infrastructure deployed on your company's premises.

M

Module

Module is a part of protection plan providing a particular data protection functionality, for example, the backup module, the Antivirus & Antimalware protection module, and so on.

P

Physical machine

A machine that is backed up by an agent installed in the operating system.

Point-to-site (P2S) connection

[Disaster Recovery] A secure VPN connection from outside to the cloud and local sites by using your endpoint devices (such as a computer or laptop).

Primary server

[Disaster Recovery] A virtual machine that does not have a linked machine on the local site (such as a recovery server). Primary servers are used for protecting an application or running

various auxiliary services (such as a web server).

Production network

[Disaster Recovery] The internal network extended by means of a VPN tunneling and covering both local and cloud sites. Local servers and cloud servers can communicate with each other in the production network.

Protection agent

Protection agent is the agent to be installed on machines for data protection.

Protection plan

Protection plan is a plan that combines the data protection modules including Backup, Antivirus & Antimalware protection, URL filtering, Windows Defender Antivirus, Microsoft Security Essentials, Vulnerability assessment, Patch management, Data protection map, Device control.

Public IP address

[Disaster Recovery] An IP address that is needed to make cloud servers available from the Internet.

R

Recovery point objective (RPO)

[Disaster Recovery] Amount of data lost from outage, measured as the amount of time from a planned outage or disaster event. RPO threshold defines the maximum time interval allowed between the last suitable recovery point for a failover and the current time.

Recovery server

[Disaster Recovery] A VM replica of the original machine, based on the protected server backups stored in the cloud. Recovery servers are used for switching workloads from the original servers, in case of a disaster.

Runbook

[Disaster Recovery] Planned scenario consisting of configurable steps that automate disaster recovery actions.

S

Single-file backup format

A backup format, in which the initial full and subsequent incremental backups are saved to a single .tibx file. 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.

Site-to-site (S2S) connection

[Disaster Recovery] Connection extending the local network to the cloud, via a secure VPN tunnel.

T

Test IP address

[Disaster Recovery] An IP address that is needed in case of a test failover, to prevent duplication of the production IP address.

Test network

[Disaster Recovery] Isolated virtual network that is used to test the failover process.

U

USB devices database

[Device control] The device control module maintains a database of USB devices from which they can be added to the list of exclusions from device access control. The database registers USB devices by device ID, which can be entered by hand or selected from known devices in the service console.

V

Virtual machine

A virtual machine that is backed up at a hypervisor level by an external agent such as Agent for VMware or Agent for Hyper-V. A virtual machine with an agent inside is treated as physical from the backup standpoint.

VPN appliance

[Disaster Recovery] A special virtual machine that enables connection between the local network and the cloud site via a secure VPN tunnel. The VPN appliance is deployed on the local site.

VPN gateway (formerly, VPN server or connectivity gateway)

[Disaster Recovery] A special virtual machine providing a connection between the local site and the cloud site networks via a secure VPN tunnel. The VPN gateway is deployed on the cloud site.

Index

#

#CyberFit Score by machine 543
#CyberFit Score for machines 140
#CyberFit scoring mechanism 140

.

...I lost the second-factor device? 40
...I want to change the second-factor device? 40

3

32-bit or 64-bit? 523

A

A device plan conflicts with a group plan 138
About Cyber Disaster Recovery Cloud 360
About Secure Zone 163
About the backup schedule 314
About the Physical Data Shipping service 214
Access settings 502
Accessing the Cyber Protection service 41
Action field values 515
Action on detection 435
Action parameters 419
Activating the account 39
Active Directory Domain Controller for L2 Open VPN connectivity 384
Active Directory Domain Controller for L3 IPsec VPN connectivity 384
Active point-to-site connections 394

Active Protection 424

Active Protection in the Cyber Backup Standard edition 433

Active Protection settings 424

Active protection settings in Cyber Backup Standard 434

Add or remove USB devices from the database 500

Adding a Google Workspace organization 315

Adding a Microsoft 365 organization 288, 291

Adding a report 556

Adding devices to static groups 124

Adding quarantined files to the whitelist 451

Adding VLANs 536

Additional parameters 65, 70

Additional requirement for virtual machines 265

Additional requirements for application-aware backups 257

Additional scheduling options 167

Administering Microsoft 365 organizations added on different levels 292

Advanced 448

Advanced protection 17

Advanced storage option 163

Agent for Data Loss Prevention 25

Agent for Exchange (for mailbox backup) 25

Agent for Hyper-V 27

Agent for Linux 26

Agent for Mac 27

Agent for Microsoft 365 26, 286

- Agent for Oracle 26
- Agent for oVirt 28
- Agent for oVirt – required roles and ports 105
- Agent for Scale Computing HC3 28
- Agent for Scale Computing HC3 – required roles 94
- Agent for SQL, Agent for Active Directory, Agent for Exchange (for database backup and application-aware backup) 25
- Agent for Virtuozzo 28
- Agent for Virtuozzo Hybrid Infrastructure 28
- Agent for VMware - LAN-free backup 345
- Agent for VMware - necessary privileges 353
- Agent for VMware (Virtual Appliance) 27
- Agent for VMware (Windows) 27
- Agent for Windows 24
- Alerts 187
- Allowing processes to modify backups 429
- Antimalware and web protection 422
- Antimalware features 422
- Antimalware scan of backups 451
- Antivirus and antimalware protection 422
- Antivirus and antimalware protection settings 424
- Application-aware backup 263
- Applying a protection plan to a group 130
- Applying several plans to a device 137
- Are the required packages already installed? 48
- Attaching SQL Server databases 269
- Autodiscovery and manual discovery 81
- Autodiscovery of machines 78

- Automatic adding to the whitelist 450
- Automatic deletion of unused customer environments on the cloud site 376
- Automatic driver search 235
- Automatic patch approval 467
- Automatic updates for components 115
- Availability of the backup options 184
- Availability of the recovery options 243
- Available actions with a protection plan 138

B

- Backing up a website 332
- Backing up clustered Hyper-V machines 356
- Backing up databases included in an AAG 261
- Backing up the cloud servers 417
- Backing up the Exchange cluster data 263
- Backup 146
- Backup and recovery 146
- Backup consolidation 187
- Backup file name 188
- Backup format 191
- Backup format and backup files 192
- Backup options 184
- Backup plans for cloud applications 519
- Backup scanning details 551
- Backup scanning plan 518
- Backup schemes 166
- Backup validation 193, 244
- Backup window 211
- Basic parameters 62, 68
- Before you start 88, 91, 94, 102

- Behavior detection 427
- Behavior detection settings 428
- Boot mode 245
- Bootable media 521
- Bootable Media Builder 523
- Browsing the hardware inventory 478
- Browsing the software inventory 473
- Built-in groups 123

C

- Cache storage 117
- calculate hash 206
- Categories to filter 440
- Changed block tracking (CBT) 193
- Changed Block Tracking (CBT) 343
- Changing the backup format to version 12 (TIBX) 192
- Changing the encryption password 495
- Changing the logon account on Windows machines 59
- Changing the Microsoft 365 access credentials 291
- Changing the ports used by the Cyber Protection agent 47
- Changing the service quota of machines 118
- Changing the SQL Server or Exchange Server access credentials 278
- Check access to the drivers in bootable environment 234
- Check device IP address 177
- Checking the cloud firewall activities 417
- Cloud-only mode 368, 387
- Cloud applications 552

- Cloud network infrastructure 366
- Cloud storage 196
- Cluster-aware backup 262
- Cluster backup mode 194
- Common backup rule 35
- Common installation rule 35
- Common requirements 256
- Comparison of editions 15
- Compatibility with encryption software 35
- Completion check 420
- Compression level 195
- Configuring a Site-to-site Open VPN connection 377
- Configuring automatic patch approval 468
- Configuring Cloud-only mode 377
- Configuring custom DNS servers 392
- Configuring local routing 393
- Configuring Multi-site IPsec VPN 379
- Configuring network settings 536
- Configuring networks in Virtuozzo Hybrid Infrastructure 95
- Configuring Point-to-site remote VPN access 384
- Configuring Site-to-site Open VPN 377
- Configuring the action on detection for real-time protection 430
- Configuring the Multi-site IPsec VPN settings 379
- Configuring the scan mode for real-time protection 430
- Configuring the virtual appliance 89, 93, 99, 104

- Configuring user accounts in Virtuozzo Hybrid Infrastructure 96
- Connecting to a machine booted from bootable media 536
- Continuous data protection (CDP) 156
- Control type 529
- Copying Microsoft Exchange Server libraries 278
- Corporate whitelist 450
- CPU priority 212
- Create a disaster recovery protection plan 363
- Creating a dynamic group 124
- Creating a personal Google Cloud project 316
- Creating a primary server 411
- Creating a protection plan 133
- Creating a recovery server 398
- Creating a replication plan 340
- Creating a runbook 418
- Creating a static group 124
- Creating physical bootable media 522
- Creating the .mst transform and extracting the installation packages 61
- Creating WinPE or WinRE bootable media 532
- Criteria 198
- Custom groups 123
- Custom or ready-made bootable media? 521
- Custom scripts 527
- Cyber Backup edition 15
- Cyber Protect edition 15
- Cyber Protection 541
- Cyber Protection service editions and sub-editions 15

- Cyber Protection services installed in your environment 118

D

- Data Deduplication 38
- Data protection map 491, 547
- Data protection map settings 492
- Database backup 258
- Date and time for files 246
- Default actions 447
- Default backup file name 189
- Default backup options 183
- Default plan options 134
- Default protection plans 133
- Deleting a Microsoft 365 organization 292
- Deleting all alerts 490
- Deleting backups 253
- Deleting custom DNS servers 392
- Deleting the machine 338
- Deploying Agent for oVirt (Virtual Appliance) 102
- Deploying Agent for Scale Computing HC3 (Virtual Appliance) 91
- Deploying Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance) 94
- Deploying Agent for VMware (Virtual Appliance) 88
- Deploying agents through Group Policy 106
- Deploying the OVA template 103
- Deploying the OVF template 89
- Deploying the QCOW2 template 92, 98
- Device control 496

- Device control alerts 514
- Device groups 123
- Device types allowlist 507
- Direct selection 151, 153
- Disable automatic DRS for the agent 89
- Disabling automatic assignment for an agent 350
- Disaster recovery 360
- Disaster Recovery add-on 15
- Discovered machines 542
- Disk health monitoring 543
- Disk health status alerts 547
- Disk health widgets 544
- Disk provisioning 343
- Distribution algorithm 348
- Do not show messages and dialogs while processing (silent mode) 196, 246
- Do not start when connected to the following Wi-Fi networks 176
- Do not start when on metered connection 176
- Download configuration for OpenVPN 394
- Downloading a report 558
- Downloading Cyber Protection agents 54
- Downloading files from the cloud storage 238
- Downloading the IPsec VPN log files 397
- Dumping the report data 558
- Dynamic installation and uninstallation of components 60

E

- Editing a report 556
- Editing the Recovery server default

- parameters 364
- Enable or disable device control 498
- Enable or disable OS notification and service alerts 499
- Enable VSS full backup 222
- Enabling and disabling the Site-to-site connection 389
- Enabling the hardware inventory scanning 477
- Enabling the software inventory scanning 472
- Encryption 180
- Encryption as a machine property 181
- Encryption in a protection plan 180
- Enhanced security mode 494
- Error handling 195, 246, 343-344
- Event properties 171
- Example 97-98, 173-177
 - "Bad block" emergency backup 171
 - Installing the packages manually in Fedora 14 50
- Examples 66, 72-74
- Exchange Server clusters overview 262
- Exclude device subclasses from access control 500
- Exclude files matching specific criteria 197
- Exclude hidden files and folders 198
- Exclude individual USB devices from access control 500
- Exclude system files and folders 198
- Excluding processes from access control 512
- Exclusions 445, 448
- Executing a runbook 420
- Existing vulnerabilities 549

Exploit prevention 428

Exploit prevention settings 428

Exporting and importing the report
structure 558

Extensions and exception rules 493

Extracting files from local backups 241

F

Failback options 343

Failback to a target physical machine 409

Failback to a target virtual machine 405

Failing back 342

Failing over to a replica 341

Fast incremental/differential backup 197

File-level backup snapshot 199

File-level security 247

File exclusions 247

File filters 197

Files of a script 527

Finalization of machines running from cloud
backups 339

Finalization vs. regular recovery 339

Finalizing the machine 338

Firewall rules for cloud servers 413

Fits the time interval 174

Flashback 247

Forensic backup process 200

Forensic data 199

Full-text search 320

Full path recovery 248

G

General recommendations for local sites 381

get content 206

Getting the certificate for backups with forensic
data 203

H

Hardware inventory 477

Hardware inventory widgets 554

High Availability of a recovered machine 356

How creating Secure Zone transforms the
disk 164

How do files get into the quarantine
folder? 449

How failback works 404

How failover works 400

How it works 79, 140, 157, 183, 202, 225, 330,
434, 438, 462, 468, 484, 488, 491, 544

How many agents are required for cluster-
aware backup and recovery? 263

How many agents are required for cluster data
backup and recovery? 260

How many agents do I need? 89, 91, 95, 102

How routing works 368, 370, 375

How the encryption works 182

How to assign the user rights 60

How to configure backup scanning in the
cloud 452

How to connect to a remote machine 484

How to create Secure Zone 165

How to delete Secure Zone 166

How to distinguish backups that are protected

- on continuous basis 161
- How to get forensic data from a backup? 201
- How to perform failover of a DHCP server 404
- How to perform failover of servers using local DNS 404
- How to recover data to a mobile device 281
- How to recover your entire machine to the latest state 162
- How to review data via the service console 281
- How to run a remote assistance session 485
- How to start backing up your data 280
- How to use notarization 183, 330

I

- Ignore bad sectors 196
- In-archive deduplication 192
- In bootable media 54
- In Google Workspace 314
- In Linux 52, 114
- In macOS 53, 114
- In Microsoft 365 288
- In the Cyber Protection service 288, 314
- In Windows 51, 114
- Information parameters 71
- Initial connectivity configuration 377
- Installation parameters 62, 68
- Installing Cyber Protection agents 54
- Installing Cyber Protection agents in Linux 56
- Installing Cyber Protection agents in macOS 58
- Installing Cyber Protection agents in Windows 55

- Installing or uninstalling the product by specifying parameters manually 62
- Installing the packages from the repository 49
- Installing the packages manually 50
- Installing the product by using the .mst transform 61
- Installing the software 42
- IP address reconfiguration 387
- IPsec/IKE security settings 381

K

- Kernel parameters 524

L

- License issue 138
- Limitations 33, 95, 103, 156, 164, 238, 246, 287, 302, 306, 314, 320, 323-324, 327, 332, 346, 362, 494, 543
- Limitations for backup file names 189
- Limiting the total number of simultaneously backed-up virtual machines 356
- Linux 153
- Linux-based 521
- Linux-based bootable media 523
- Linux-based or WinPE/WinRE-based bootable media? 521
- Linux packages 47
- list backups 204
- list content 205
- List of USB devices on a computer 512
- Local connection 536
- Log truncation 208
- LVM snapshotting 208

M

- Mac 153
- Machine discovery process 80
- Machine migration 357
- Mailbox backup 265
- Malicious website access 440
- Managing discovered machines 86
- Managing found vulnerabilities 460
- Managing list of patches 466
- Managing networks 385
- Managing point-to-site connection settings 393
- Managing quarantined files 449
- Managing the cloud servers 412
- Managing the detected unprotected files 491
- Managing the VPN appliance settings 389
- Managing virtualization environments 351
- Manual adding to the whitelist 451
- Manual binding 349
- Manual patch approval 470
- Mass storage drivers to install anyway 235
- McAfee Endpoint Encryption and PGP Whole Disk Encryption 36
- Microsoft BitLocker Drive Encryption 35
- Microsoft Defender Antivirus 446
- Microsoft Defender Antivirus and Microsoft Security Essentials 446
- Microsoft Exchange Server 194
- Microsoft products 463
- Microsoft Security Essentials 446
- Microsoft SQL Server 194

- Missing updates by categories 550
- Monitoring 540
- Mount points 209, 248
- Mounting Exchange Server databases 272
- Mounting volumes from a backup 252
- Multi-site IPsec VPN connection 374
- Multi-site IPsec VPN log files 397
- Multi-volume snapshot 209
- Multitenancy support 131

N

- Names without variables 190
- Network management 385
- Network requirements for the Agent for
Virtuozzo Hybrid Infrastructure (Virtual
Appliance) 96
- Network settings 535
- Networking concepts 367
- No successful backups for a specified number
of consecutive days 187
- Notarization 182, 330
- Notarization of backups with forensic data 202
- Note for Mac users 224

O

- On-demand patch installation 470
- On Windows Event Log event 171
- Operations with a primary server 412
- Operations with backups 251
- Operations with bootable media 537
- Operations with protection plans 138
- Operations with runbooks 420

- Operators 129
- Options description 207
- Orchestration (runbooks) 418
- OS notification and service alerts 506
- Output speed during backup 213
- Overview of the physical data shipping process 214
- oVirt/Red Hat Virtualization 4.2 and 4.3 105
- oVirt/Red Hat Virtualization 4.4 105

P

- Parameters 524
- Parameters for legacy features 71
- Passwords with special characters or blank spaces 78
- Patch installation history 550
- Patch installation status 549
- Patch installation summary 550
- Patch installation widgets 549
- Patch lifetime in the list 471
- Patch management 461
- Patch management settings 463
- Performance 248, 344
- Performance and backup window 210
- Performing a failover 402
- Performing a permanent failover 342
- Performing a test failover 401
- Performing failback to a physical machine 409
- Performing failback to a virtual machine 406
- Physical Data Shipping 214
- Physical machine 226
- Physical machine to virtual 228

- Plan conflicts with already applied plans 137
- Point-to-site remote VPN access 375
- Ports 377
- Ports required by the Downloader component 47
- Post-backup command 216
- Post-data capture command 218
- Post-recovery command 250
- Power off target virtual machines when starting recovery 250
- Power on the target virtual machine when recovery is complete 251
- Pre-backup command 215
- Pre-data capture command 217
- Pre-recovery command 249
- Pre-update backup 466
- Pre/Post commands 215, 248, 343-344
- Pre/Post data capture commands 216
- Preconfiguring multiple network connections 535
- Predefined scripts 526
- Preparation 45, 234
 - WinPE 2.x and 3.x 533
 - WinPE 4.0 and later 534
- Prepare drivers 234
- Preparing a machine for remote installation 83
- Prerequisites 79, 106, 109, 156, 256, 336, 379, 384, 392, 397-398, 406, 411, 473, 475, 478-479, 481
- Preventing unauthorized uninstallation or modification of agents 113
- Primary servers 373
- Privileges required for the logon account 59

- Production failover 400
- Protecting a domain controller 255
- Protecting Always On Availability Groups (AAG) 260
- Protecting Database Availability Groups (DAG) 261
- Protecting Exchange Online data 293
- Protecting Exchange Online mailboxes 289
- Protecting Gmail data 319
- Protecting Google Drive files 323
- Protecting Google Workspace data 313
- Protecting Hosted Exchange data 282
- Protecting Microsoft 365 data 285
- Protecting Microsoft 365 Teams 306
- Protecting Microsoft applications 255
- Protecting Microsoft SharePoint 255
- Protecting Microsoft SQL Server and Microsoft Exchange Server 255
- Protecting mobile devices 279
- Protecting OneDrive files 299
- Protecting Oracle Database 331
- Protecting SAP HANA 331
- Protecting Shared drive files 327
- Protecting SharePoint Online sites 302
- Protecting web hosting servers 335
- Protecting websites 331
- Protecting websites and hosting servers 331
- Protection of collaboration and communication applications 453
- Protection plan 518
- Protection plan and modules 132
- Protection plan cheat sheet 148

- Protection status 541
- Proxy server settings 51
- Public and test IP address 371

Q

- Quarantine 427, 449
- Quarantine location on machines 450
- Quotas 335

R

- Re-attempt, if an error occurs 195, 246
- Re-attempt, if an error occurs during VM snapshot creation 196
- Re-generate configuration 394
- Real-time protection 423, 430, 447
- Reassigning IP addresses 391
- Recently affected 551
- Recommendations 246
- Recommendations for the Active Directory Domain Services availability 384
- Recovering a machine 226
- Recovering a team mailbox 310
- Recovering a team site or specific items of a site 312
- Recovering a website 333
- Recovering an entire Google Drive 325
- Recovering an entire OneDrive 300
- Recovering an entire Shared drive 328
- Recovering an entire team 307
- Recovering applications 255
- Recovering backups 495
- Recovering disks by using bootable media 232

- Recovering email messages and meetings 311
- Recovering ESXi configuration 242
- Recovering Exchange databases 270
- Recovering Exchange mailboxes and mailbox items 272
- Recovering files 237
- Recovering files by using bootable media 241
- Recovering files by using the web interface 237
- Recovering Google Drive and Google Drive files 325
- Recovering Google Drive files 326
- Recovering mailbox items 275, 284, 290, 296, 322
- Recovering mailboxes 274, 283, 290, 295, 321
- Recovering mailboxes and mailbox items 283, 290, 295, 321
- Recovering OneDrive and OneDrive files 300
- Recovering OneDrive files 301
- Recovering public folders and folder items 298
- Recovering Shared drive and Shared drive files 328
- Recovering Shared drive files 329
- Recovering SharePoint Online data 304
- Recovering SQL databases 266
- Recovering system databases 269
- Recovering system state 242
- Recovering team channels or files in team channels 308
- Recovering the Exchange cluster data 263
- Recovering the master database 269
- Recovery 223, 538
- Recovery cheat sheet 223
- Recovery from a network share 527
- Recovery from the cloud storage 527
- Recovery of databases included in an AAG 261
- Recovery options 243
- Recovery servers 371
- Recovery to an Exchange Server 273
- Recovery to Microsoft 365 273
- Redistribution 349
- Registering machines manually 75
- Registering the bootable media 534
- Registration parameters 64, 69
- Remote access (RDP and HTML5 clients) 483
- Remote connection 117
- Remote desktop access 483
- Remote wipe 487
- Removing Agent for VMware (Virtual Appliance) 115
- Removing machines from the service console 115
- Replication 179
- Replication of virtual machines 339
- Replication options 343
- Replication vs. backing up 339
- Reports 555
- Required ports 106
- Required roles 105
- Required user rights 264, 266, 288, 314
- Requirements 242, 253
- Requirements for ESXi virtual machines 257
- Requirements for Hyper-V virtual machines 258
- Requirements for the VPN appliance 377

- Requirements on User Account Control (UAC) 84
- Requirements on user accounts 273
- Resolving plan conflicts 137
- Restrictions 340
- Retention rules 178
- Reverting to the original initial RAM disk 236
- Rules for Linux 151
- Rules for macOS 152
- Rules for Windows 151
- Rules for Windows, Linux, and macOS 151
- Running a #CyberFit Score scan 144
- Running a hardware inventory scan manually 478
- Running a software inventory scan manually 473
- Running a virtual machine from a backup (Instant Restore) 335
- Running cloud-to-cloud backups manually 520
- Running the machine 336

S

- Safe recovery 225
- Save battery power 175
- Save system information if a recovery with reboot fails 247
- Scanning types 422
- Schedule 166, 457, 464, 492
- Schedule by events 169
- Schedule scan 431, 446
- Scheduled scan 423
- Scheduling 219

- Scheduling a report 557
- Scripts in bootable media 526
- Search criteria 125
- Sector-by-sector backup 219
- Security settings 115
- Seeding an initial replica 344
- Selecting a destination 162
- Selecting components for installation 85
- Selecting data to back up 150
- Selecting disks/volumes 150
- Selecting ESXi configuration 155
- Selecting Exchange Server data 259
- Selecting Exchange Server mailboxes 266
- Selecting files/folders 153
- Selecting Google Drive files 324
- Selecting mailboxes 283, 289, 294, 320
- Selecting OneDrive files 299
- Selecting public folders 295
- Selecting Shared drive files 327
- Selecting SharePoint Online data 303
- Selecting SQL databases 258
- Selecting system state 155
- Selecting teams 307
- Selection rules for Linux 154
- Selection rules for macOS 155
- Selection rules for Windows 154
- Service console 120
- Services installed in macOS 119
- Services installed in Windows 118
- Setting firewall rules for cloud servers 414
- Setting the encryption password 494

- Setting up a display mode 537
- Setting up connectivity 366
- Setting up primary servers 411
- Setting up recovery servers 398
- Setting up the disaster recovery functionality 362
- Share a remote connection with users 485
- SID changing 250
- Signing a file with ASign 239
- Site-to-site Open VPN connection 369, 385
- Skip the task execution 221
- Smart protection 488
- Software-specific recovery procedures 35
- Software inventory 472
- Software inventory widgets 553
- Software requirements 24, 361
- Special operations with virtual machines 335
- Splitting 220
- SQL Server high-availability solutions overview 260
- Start conditions 172
- Starting a backup manually 183
- Startup Recovery Manager 538
- Step 1 45
 - Generating a registration token 106
- Step 1. Read and accept the license agreements for the products that you want to update 468
- Step 2 45
 - Creating the .mst transform and extracting the installation package 108
- Step 2. Configure the settings for automatic approval 468
- Step 3 45
 - Setting up the Group Policy objects 108
- Step 3. Prepare the Test patching protection plan 469
- Step 4 46
 - Step 4. Prepare the Production patching protection plan 469
- Step 5 46
 - Step 5. Run the Test patching protection plan and check the results 470
- Step 6 47
- Steps and actions 419
- Stopping a runbook execution 421
- Stopping failover 342
- Storage vMotion 351
- Structure of autostart.json 528
- Support for VM migration 350
- Supported Apple and third-party products 456
- Supported Apple products 456
- Supported cluster configurations 260, 262
- Supported Cyber Protect features by operating system 18
- Supported data sources and destinations for continuous data protection 157
- Supported file systems 37
- Supported Linux products 457
- Supported locations 179
- Supported Microsoft and third-party products 455
- Supported Microsoft Exchange Server versions 28
- Supported Microsoft products 455

- Supported Microsoft SharePoint versions 29
- Supported Microsoft SQL Server versions 28
- Supported mobile devices 279
- Supported operating systems 361
- Supported operating systems and environments 24
- Supported Oracle Database versions 29
- Supported Plesk and cPanel versions 335
- Supported SAP HANA versions 29
- Supported third-party products for macOS 456
- Supported third-party products for Windows OS 456
- Supported virtualization platforms 29, 361
- Supported web browsers 24
- Switching the Site-to-site connection type 390
- System requirements 377
- System requirements for agents 44
- System requirements for the agent 88, 91, 95, 102

T

- Task failure handling 220
- Task start conditions 220
- TCP ports required for backup and replication of VMware virtual machines 46
- Test failover 401
- Testing a replica 341
- The backup location's host is available 173
- The Backup storage tab 251
- The key functionality 360
- The Plans tab 518
- The tool "tibxread" for getting the backed-up

- data 203

- The upgrade process 313
- The way of using Secure Zone 35
- Threat feed 488
- Top-level object 528
- Troubleshooting 87, 559
- Troubleshooting IPsec VPN configuration issues 395
- Troubleshooting the IPsec VPN configuration 395
- Two-factor authentication 39

U

- Unattended installation and uninstallation in macOS 72
- Unattended installation or uninstallation 61
- Unattended installation or uninstallation in Linux 67
- Unattended installation or uninstallation in Windows 61
- Unattended installation or uninstallation parameters 62, 68
- Uninstallation parameters 65, 71
- Uninstalling agents 114
- Universal Restore in Linux 236
- Universal Restore in Windows 234
- Universal Restore process 235
- Universal Restore settings 235
- Updating agents 109
- Updating agents automatically 111
- Updating agents manually 109
- Updating the Cyber Protection definitions by schedule 116

- Updating the Cyber Protection definitions on-demand 117
- Upgrading the cloud agent 312
- URL filtering 438
- URL filtering configuration workflow 440
- URL filtering settings 440
- Usage examples 179, 191, 336, 340, 350
- USB devices allowlist 508
- USB devices database 510
- USB devices database management page 510
- Useful tips 292, 316
- User is idle 173
- Users logged off 174
- Using a locally attached storage 347
- Using device control 498
- Using policy rules 151, 154
- Using the cloud Agent for Microsoft 365 291
- Using the locally installed Agent for Office 365 288
- Using Universal Restore 234
- Using variables 190

V

- Variable object 528
- Verifying file authenticity with Notary Service 239, 331
- View device control alerts 502
- View or change access settings 499
- Viewing backup status in vSphere Client 352
- Viewing the distribution result 349
- Viewing the execution history 421
- Viewing the hardware of a single device 481

- Viewing the software inventory of a single device 475
- Virtual machine 230
- Virtual machine binding 348
- VM power management 250, 344
- vMotion 350
- Volume Shadow Copy Service (VSS) 221
- Volume Shadow Copy Service (VSS) for virtual machines 222
- Volume Shadow Copy Service VSS for virtual machines 343
- VPN access to local site 394
- VPN appliance 371
- VPN gateway 370, 374
- VPN gateway network configuration 370
- Vulnerability assessment 454
- Vulnerability assessment and patch management 454
- Vulnerability assessment for Linux machines 459
- Vulnerability assessment for macOS devices 459
- Vulnerability assessment for Windows machines 459
- Vulnerability assessment settings 457
- Vulnerability assessment widgets 548
- Vulnerable machines 548

W

- Wait until the conditions from the schedule are met 221
- Weekly backup 223
- What do I need to back up a website? 332

What do I need to use application-aware backup? 264
 What does a disk or volume backup store? 152
 What does Google Workspace protection mean? 313
 What else you need to know 179
 What if... 40
 What is a backup file? 188
 What items can be backed up? 282, 289, 293, 299, 302, 306, 319, 323, 327, 332
 What items can be recovered? 282, 289, 293, 299, 303, 306, 319, 323, 327
 What items cannot be recovered? 303
 What to do next 364
 What to scan 457
 What you can back up 279
 What you can do with a replica 340
 What you need to know 279
 What you need to know about finalization 339
 Where can I see backup file names? 188
 Where to get the Cyber Protect app 280
 Which agent do I need? 42
 Whitelist settings 451
 Why back up Microsoft 365 data? 285
 Why use application-aware backup? 264
 Why use Bootable Media Builder? 523
 Why use runbooks? 418
 Why use Secure Zone? 163
 Windows 152
 Windows Azure and Amazon EC2 virtual machines 359
 Windows event log 223, 251
 Windows third-party products 464
 WinPE-based and WinRE-based bootable media 531
 WinPE images 532
 WinPE/WinRE-based 521
 WinRE images 531
 Working in VMware vSphere 339
 Working with encrypted backups 410