Acronis

# Acronis Cyber Protect 15

Beta

# Quick Start Guide

REV. 8

# Table of contents

# Introduction

Welcome to the Acronis Cyber Protect Beta program!

Acronis Cyber Protect is a unique integration of backup with full-stack next-generation anti-malware protection and comprehensive endpoint management tools.
Use this guide to learn about the unique cyber protection capabilities of Acronis Cyber Protect and get started with the v15 release.

**This Quick Start Guide presents an overview of the new features that are available in Acronis Cyber Protect Beta. The features and screenshots are subject to change.**

## Intended audience

This document is intended for IT professionals who have basic understanding of the principles, processes, and terminology of backup, vulnerability assessment, patch management, and anti-malware solutions, and who are familiar with Acronis Cyber Backup 12.5

## Prerequisites

Ensure that your environment meets the software requirements described at https://dl.managed-protection.com/u/cyberprotect/help/15/user/en-US/index.html#33784.html.
Verify that you have one or more machines for testing Acronis Cyber Protect capabilities.

## Prepare for testing

**Do not test Acronis Cyber Protect Beta on your production servers or endpoints. The beta version could exhibit technical issues, and may cause partial or full data loss, configuration, or an entire system.**

Acronis Cyber Protect Beta is designed to be tested for a wide range of scenarios. Feel free to perform any scenario and test any available feature and option. In this document, you can find sample scenarios that will give you a quick overview of the product capabilities.

For a better experience, we recommend that you perform the test with a small, dedicated disk volume that you can use to perform all of the required actions and see the results faster than in a regular use. If you do not have a dedicated small volume, you can follow the steps below and create a new volume:

1. In Windows, select the Start button and open **Computer Management**. Then, select **Control Panel** > **System and Security** > **Administrative Tools**, and then double-click **Computer Management**.
2. In the left-hand pane, under **Storage**, select **Disk Management**.
3. Right-click the system volume, and then click **Shrink volume**.
4. Define the size for a new volume.
   We recommend using the **1024** MB size for testing the Continuous Data Protection functionality.
5. Click **Shrink**.

6. Right-click on an unallocated region on your hard disk, and then select **New Simple Volume**.
7. In **New Simple Volume Wizard**, click **Next**.
8. Enter the size of the volume in megabytes (MB) that you want to create or accept the maximum default size, and then click **Next**.
9. Accept the default drive letter or choose a different drive letter to identify the partition, and then click **Next**.
10. In the **Format Partition** dialog box, do one of the following:
    - If you do not want to format the volume right now, select **Do not format this volume**, and then click **Next**.
    - To format the volume with the default settings, click **Next**.
11. Review your choices, and then click **Finish**.

# What's new in Acronis Cyber Protect 15 Beta

Before you start evaluating this product, please read about the new features we implemented. You can find detailed instructions for how to set up the functionality described in this document at https://dl.managed-protection.com/u/cyberprotect/help/15/user/en-US/index.html#36537.html.

| New feature | Details | Documentation link |
|---|---|---|
| Protection plan - a new approach to cover all cyber protection aspects | • Backup<br>• Anti-malware protection<br>• URL filtering<br>• Vulnerability Assessment<br>• Patch management<br>• Data Protection Map (Data discovery)<br>• Windows Defender Antivirus management<br>• Microsoft Security essentials management<br>• Conflicts handling – it's not possible to create and apply a wrong configuration | Protection plan and modules |
| Auto-discovery of new machines and remote installation of Acronis Cyber Protect agents – Simplify the process of installing multiple agents at once in the cloud and on-premises | • Network-based discovery<br>• Active Directory-based discovery<br>• Importing a list of computers from a file<br>• Protection plan auto apply<br>• Batch remote install of agents by using the discovery wizard | Auto-discovery of machines |
| Vulnerability assessment | • Scan for vulnerabilities<br>• Prioritize vulnerabilities by severity (critical to low)<br>• Implement dedicated patch cycles based on vendor releases and updates<br>• Respond and remediate when critical vulnerabilities are found (for example, WannaCry)<br>• Continuous update of your own vulnerability and patch management database on a daily basis<br>• Local network traffic optimization by using peer-to-peer update technology<br>• Windows and Linux support | Vulnerability assessment and patch management |
| Patch management<br>Fix the issue before the issue happens | • Auto-approval of patches<br>• Deployment on a schedule<br>• Manual deployment<br>• Flexible reboot and maintenance window options<br>• Staged deployment<br>• Windows desktops and servers support for Microsoft and third-party software | Vulnerability assessment and patch management |

| | | |
|---|---|---|
| Anti-malware protection<br>Protection against ransomware and cryptominers | • Self protection – protect Acronis components (registry, service stopping, Acronis files protecting).<br>• Protect network folders mapped as local drives – protect the mapped data on the endpoint against local ransomware.<br>• Server-side protection – protect the data on shared resources against ransomware.<br>• Cryptomining process detection<br>• Ransomware detection<br>• Quarantine (with auto-removal of quarantined files)<br>• Exclusions | Anti-malware Protection |
| URL filtering  control access to malicious URLs<br>URL filtering allows you to permit or deny access to specific websites | • Third-party database<br>• In-house HTTP/HTTPS interceptor<br>• Black/white lists for URLs<br>• Payload analysis for malicious URLs | URL filtering |
| Next Generation Continuous Data Protection | • Define the list of critical apps for every device that users are working with most often. The Acronis agent monitors every change made in the listed applications. In case of malware infection, you can restore the data from the last backup and apply the latest collected changes to the last backup, so no data is lost.<br>• Choose files for continuous protection in 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. | Continuous data protection (CDP) |
| Malware scan of backups at centralized locations | • Scanning of disk backup in centralized locations in order to find malware infections. | Anti-malware scan of backups |
| Safe recovery* | • Safe recovery restores the operating system image without the discovered malware, to avoid reinfection after the restore. | Safe recovery |
| Smart Protection Plan* | • Acronis proposes smart remediation actions based on security alerts that come from the Acronis Cyber Protection Operations Centers (CPOC). | Threat feed |
| Pre-update backup* | • Forces creation of restore points with the current backup settings every time before installing software updates. | Patch management settings |
| Forensic backup | • Back up vital data and collect information that can be used as digital evidence in forensic investigations. | Forensic data |

| | | |
|---|---|---|
| Remote desktop* | Grants the ability to assist remote users and save valuable resources.<br>Reach systems that are sitting in a private network. No need to change firewall settings or establish additional VPN tunnels, because the outgoing connections (port 443) are used.<br>*Limitations*<br>• Acronis Remote Desktop can be used for connection to Windows machines where the Windows Remote Desktop feature is available. Therefore, Acronis Remote Desktop cannot be used for connection to, for example, Windows 10 Home and macOS systems. | Remote access (RDP and HTML5 clients) |
| Drive Health Monitoring*<br>Know about issues on your drives before the issues occur | • Uses a combination of machine learning and SMART reporting to predict HDD failures and warn the user. | Disk health forecast |
| Data Protection Map (Data discovery) | • Helps you discover whether your important files were backed up or not. | Data protection map |
| Corporate whitelist | • Scans backups by using anti-malware technologies (AI, behavioral heuristics, etc.), to whitelist organizational unique apps and avoid "false positives" in the future. | Corporate whitelist |
| Flexible Monitoring and Reporting | • The hardware health monitoring (HDD, SSD) uses a combination of machine learning and reports about S.M.A.R.T., drive size, drive vendor, etc. to predict HDD failures.<br>• Active alert control<br>• Missing updates control<br>• Customizable dashboard widgets<br>• Allows quickly identify problems<br>• Quick access to the management actions | Monitoring |
| Antivirus management: Windows Defender Antivirus or Microsoft Security Essentials | • Enforce settings across multiple machines.<br>• Ensure that antivirus definitions are up-to-date on all machines.<br>• Collect all Windows Defender detection events and display them in the management console. | Windows Defender Antivirus<br>Microsoft Security Essentials |

* Unavailable in beta. The feature will be implemented in the RTM release.

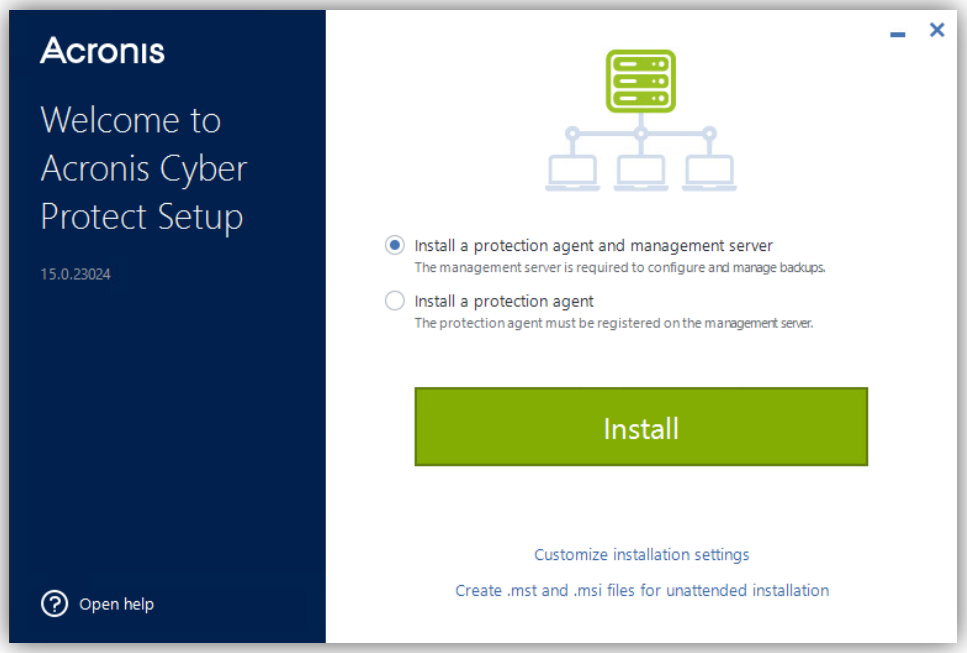
** Some links lead to the documentation for Acronis Cyber Protect Cloud. The actual functionality in this Beta version might differ from the full feature descriptions for Acronis Cyber Protection.

# Start testing Acronis Cyber Protect 15 Beta

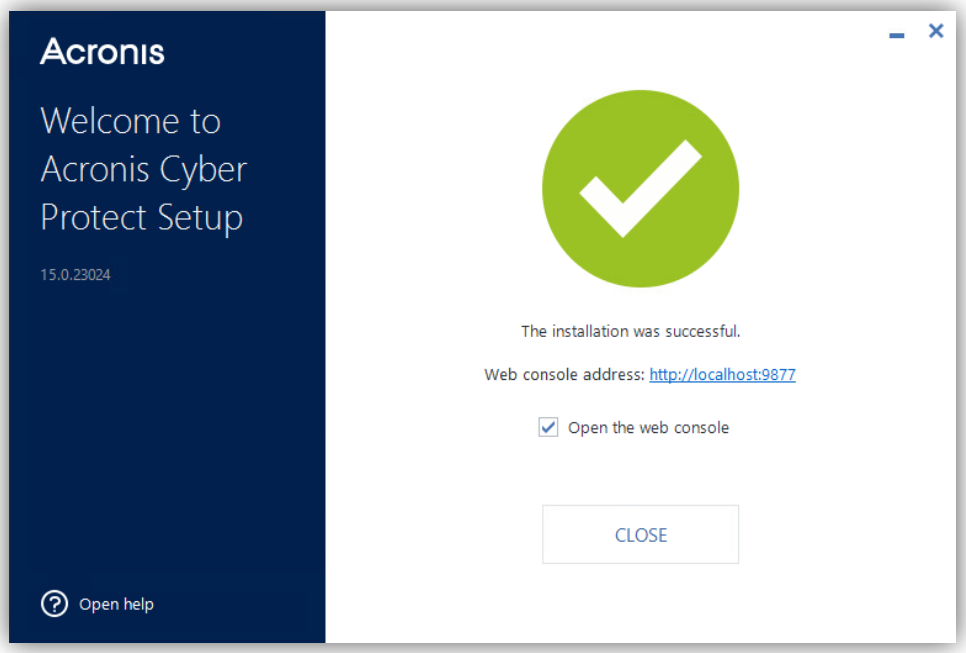
## Installing the software

1. Download the Acronis Cyber Protect installation program, at https://www.acronis.com/en-us/enterprise/download/cyber-protect/beta/.
2. Log in to the machine as an administrator and start the installation program.
3. Click **Install**.

PICTURE 1 ACRONIS CYBER PROTECT INSTALLATION



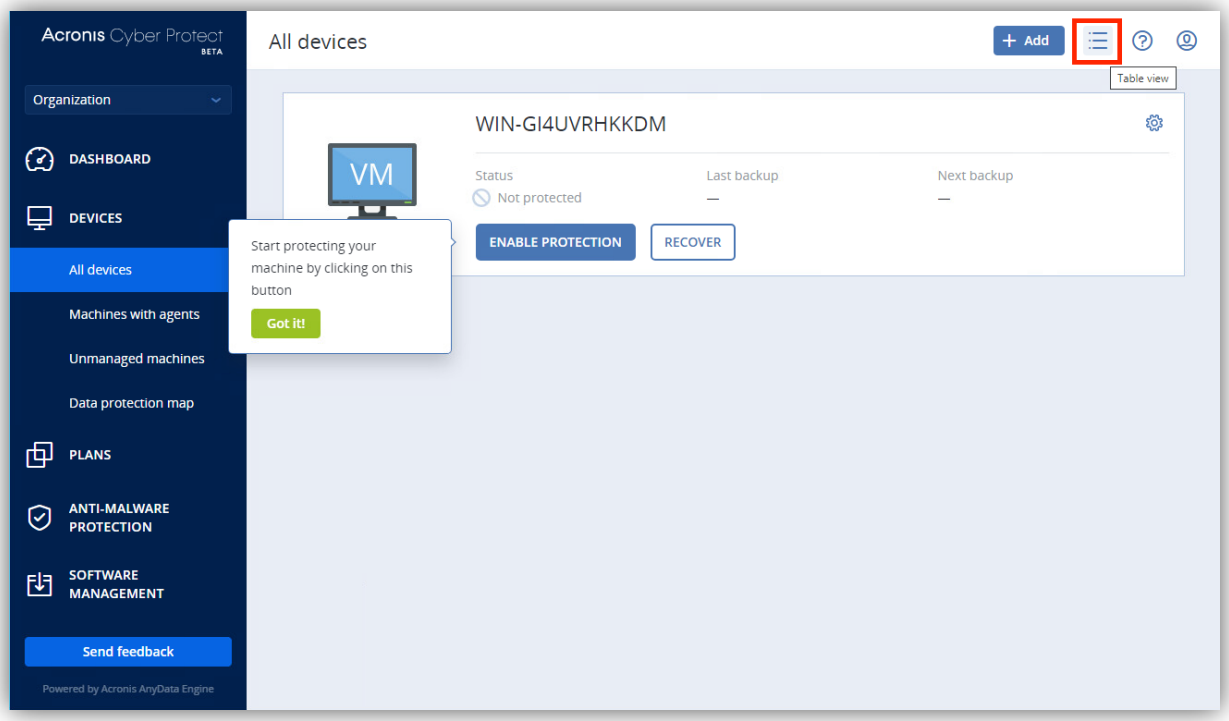

PICTURE 2 INSTALLATION COMPLETED



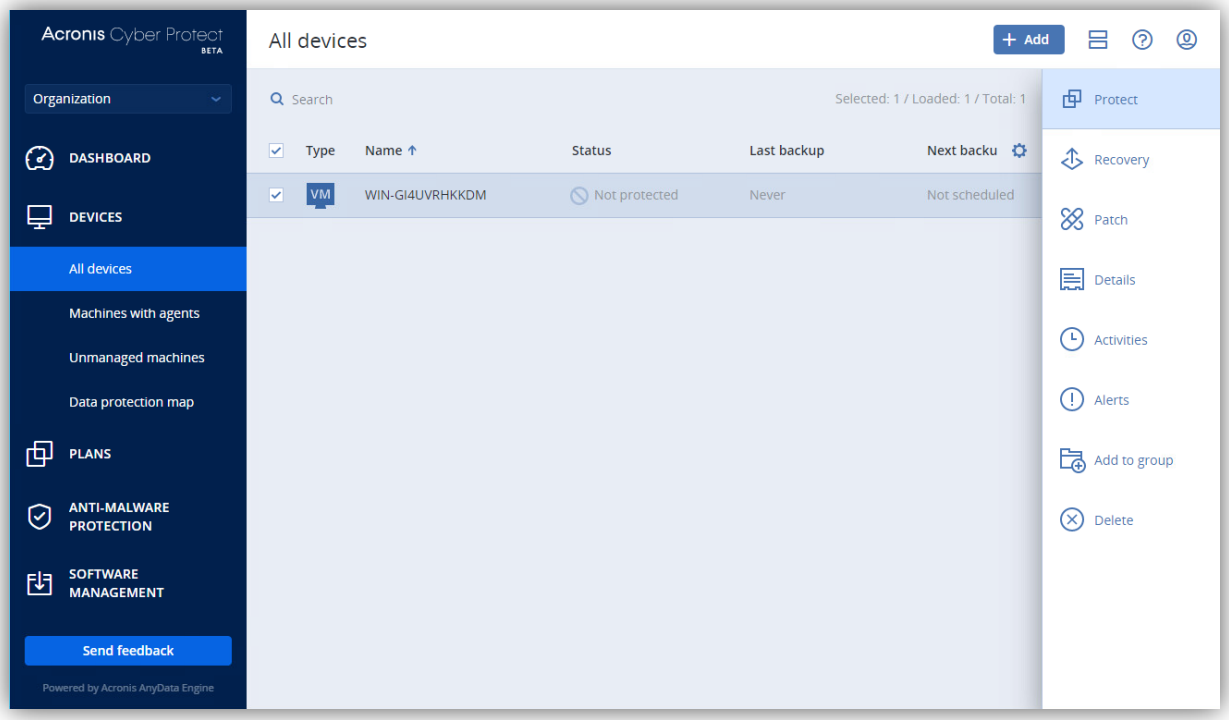

4. Click **Close**.

The Cyber Protect web console opens.
This document describes the operations accessible from the table view. To enable the table view, click on the corresponding icon as illustrated in Picture 3.

PICTURE 3 MACHINE IN MANAGEMENT CONSOLE




PICTURE 4 TABLE VIEW FOR THE DEVICE



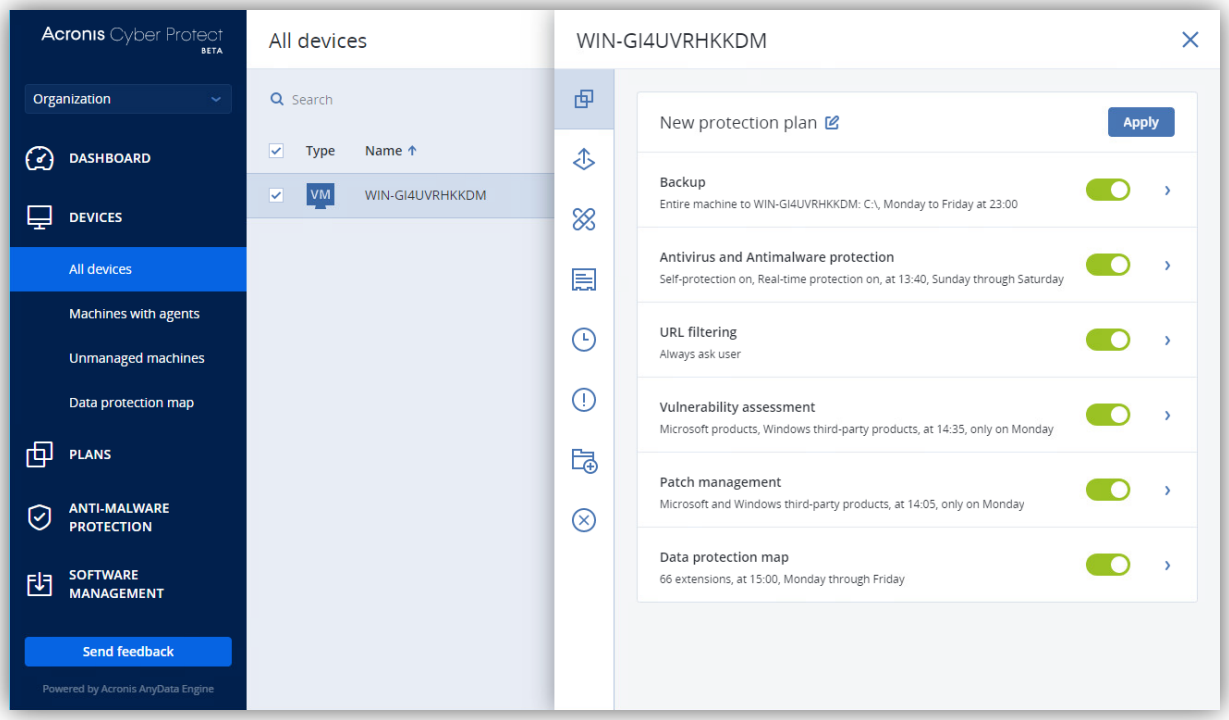
## Creating a protection plan

A protection plan consists of multiple rules that specify how a given machine will be protected.

### 1.1.1 Create a protection plan from the Devices page

1. Open the web console and select **Devices**.
2. From the list of devices, select the device that you want to protect.
3. On the action menu to the right, click **Protect**.
4. Click **Create plan**.
5. [optional] To change the protection plan name, click the **pencil icon**.
6. [optional] Enable the required modules in the protection plan.
7. [optional] To modify the plan parameters, click the corresponding section of the plan module. You can modify the following modules:
    a. Backup
    b. Anti-Malware Protection
    c. URL filtering
    d. Windows Defender Antivirus
    e. Microsoft Security Essentials
    f. Vulnerability assessment
    g. Patch management
    h. Data Protection Map
8. Expand the module settings to modify the backup settings.
9. In **What to back up**, select **Disks/volumes**.
10. Click **Items** to back up.
11. In **Select items for backup**, select **Directly**.
12. For the machine included in the protection plan, select the check boxes next to the disks or volumes to back up. For optimal results, select the disk that you created in the Prerequisites section.
13. Click **Done**.
14. Click **Create.**

PICTURE 1 PROTECTION PLAN




### 1.1.2 Create a protection plan from the Plans page

1. Open the web console and go to **Plans** > **Protection** > **Create plan**.
2. [optional] To modify the plan parameters, click the corresponding section of the plan module. You can modify the following modules:
    a. Backup
    b. Anti-Malware Protection
    c. URL filtering
    d. Windows Defender Antivirus
    e. Microsoft Security Essentials
    f. Vulnerability assessment
    g. Patch management
    h. Data Protection Plan
3. Use the **Add devices** button to select the devices that you want to protect with this plan .
4. Expand the module settings to modify the backup settings.
5. In **What to back up**, select **Disks/volumes**.
6. Click **Items** to back up.
7. In **Select items for backup**, select **Directly**.
8. For each machine included in the protection plan, select the check boxes next to the disks or volumes to back up. For optimal results, select the disk that you created in the Prerequisites section.

9. Click **Done**.
10. Click **Create**.

As a result, the selected device(s) will be protected according to the protection plan that you configured.

Verify that the resulting backup corresponds to the protection plan settings.

## Technical support and feedback

Acronis Cyber Exceed is a dedicated portal for sharing feature suggestions and reporting bugs for Acronis Cyber Protect Beta.

If you encounter an issue, please go to
https://exceed.acronis.dev/servicedesk/customer/portal/3
and report a bug or provide a suggestion. Click here for detailed instructions.

You will be able to track your ticket, provide additional details, and be in touch with Acronis team.

Alternatively, you can describe your issue by sending an email to beta15@exceed.acronis.dev.

We may ask you to collect system logs from the test machine. To do so, follow the steps below:

1. Open the backup console.
2. Do one of the following:
    - In the web console, under **Devices**, select the machine that you want to collect the logs from, and then:
        - (for simple view) Click the cog icon, and then select and click **Activities** from the menu.
        - (for table view) Click **Activities**.
    - Under **Settings** > **Agents**, select the machine that you want to collect the logs from, and then click **Details**.
3. Click **Collect system information**.
4. If prompted by your web browser, specify where to save the file.

The agent log will be saved to a .zip file. Provide a link to a file in the feedback email, to help our technical support engineers to identify the problem.