

# Acronis

#CyberFit Academy  
Cyber Protect Cloud

## Cloud Tech Fundamentals

#CyberFit



# Acronis

## Cyber Protect Cloud

### Introductions



# Course Summary



Instructor-led sales training

Introductory course and designed to help establish a baseline knowledge

Assessment:



20 MCQ questions



60 Minutes working time



70% Passing Grade



Two Attempts given



Open Book

# Target Persona



**Managed Service Providers, Service Providers,  
Cloud Aggregators and Cloud Distributor  
representatives in a technical or support role**

- Works at MSP or Cloud Distribution
- Already has basic understanding of Cyber Protection

# Learning Objectives



**After finishing this instruction you will be able to**

- Understand need for Cyber Protection / Market position / Value proposition
- Understand the different components and deployments of the Acronis Cyber Protect Cloud, as well storing data and 3<sup>rd</sup> party integrations
- Navigate through the web interface
- Manage tenants
- Apply basic troubleshooting steps and use the correct recourses
- Provide solutions to the most common issues and errors

# Course Modules – Part 1



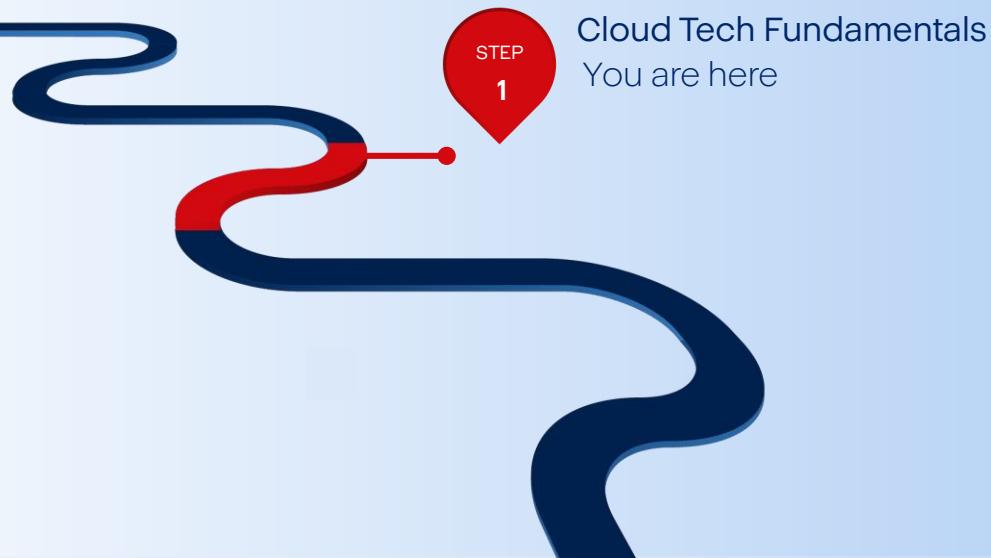
- 1. Introduction to Acronis Cyber Protection**
- 2. Product Overview**
- 3. Included Features**
  - Security
    - Management
- 4. Pay-as-you-go Features**
  - Backup
  - Files
  - Notary

- 5. Advanced Packs**
  - Backup
  - Disaster Recovery
  - Security
  - Management
  - Email Security
  - File Sync and Share

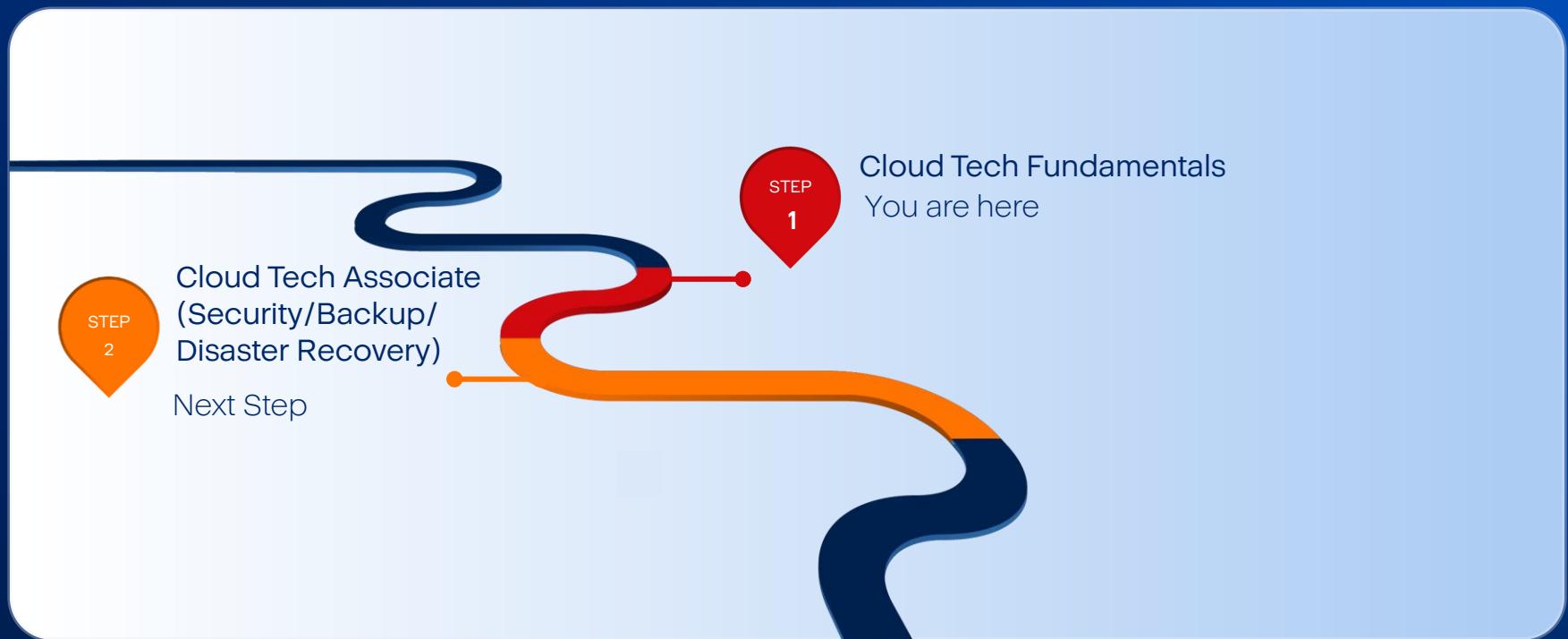
# Certification Track



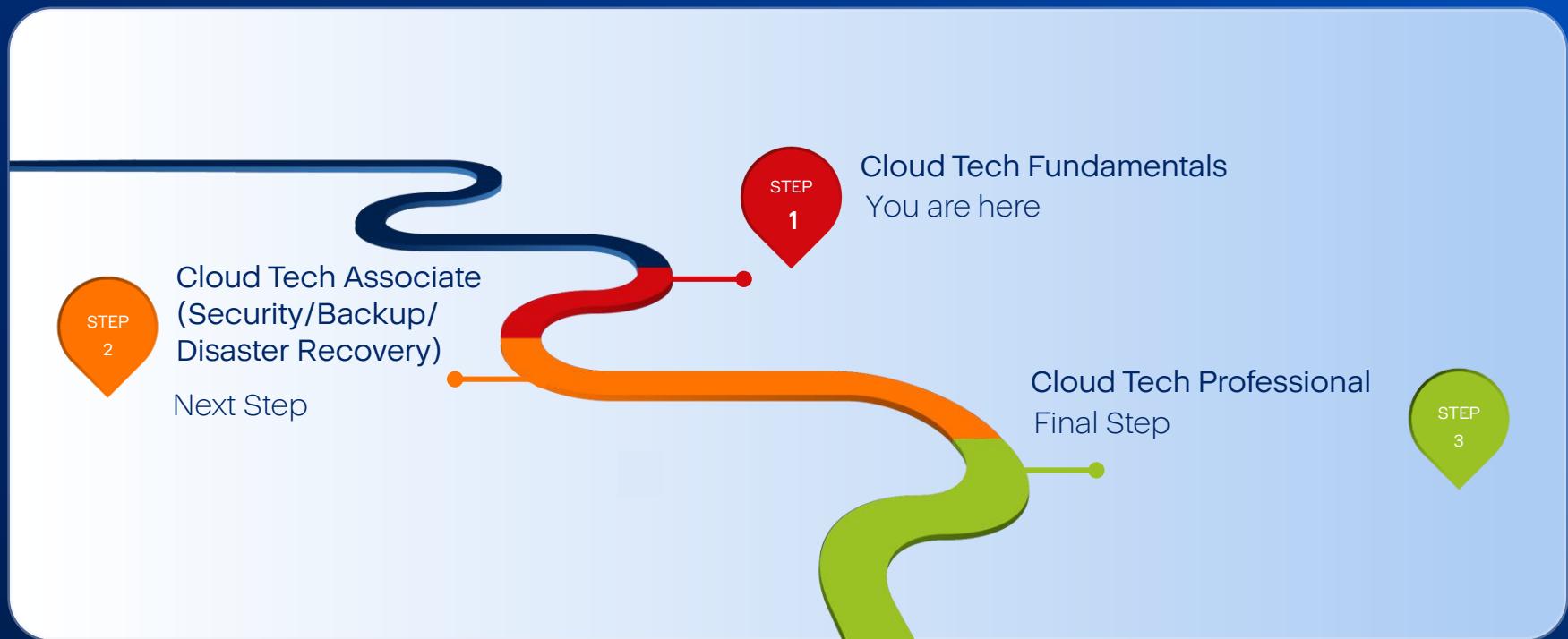
# Certification Track



# Certification Track



# Certification Track



# Certification Track

STEP  
1

## Acronis #CyberFit Cloud Tech Associate Certifications

Consists of the following courses (specializations)



# Acronis

## Cyber Protect Cloud

### Introduction to Acronis Cyber Protection



# Acronis is a Leader in Cyber Protection

Machine Intelligence (MI)-powered Cyber Protection, Cyber Cloud, Cyber Platform

Swiss



Since 2008  
Corporate HQ in  
Schaffhausen,  
Switzerland

Dual Headquarters for Dual Protection



Singaporean

Founded in 2003 in  
Singapore, currently  
the International HQ



Scale, Growth  
and Reach

\$275M+ ARR  
50%+ ARR growth  
80%+ Cloud growth  
20,000+ SPs  
750,000+ customers



Global Local  
Presence

1,700+ employees  
34+ locations  
150+ countries  
33+ languages  
DCs in 200+ countries  
in the next 24 months



Acronis Cyber  
Protect

1,800,000+ workloads  
protected  
1,000,000+ attacks  
prevented  
15,000+ Cloud  
partners providing



# Solution: Integrated and Autonomous Cyber Protection

Acronis mission is to protect all data, applications and systems (workloads)

## S

**Safety**

Nothing is lost:  
there is always a  
copy for recovery



## A

**Accessibility**

Access from  
anywhere  
at any time



## P

**Privacy**

Control over  
visibility  
and access



## A

**Authenticity**

Proof that a copy  
is an exact replica  
of the original



## S

**Security**

Protection against  
bad actors



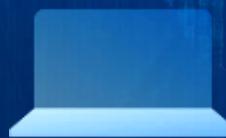
# The threat landscape is becoming more complex



**300%**  
spike in cybercrime  
during the COVID-19  
pandemic



**57%**  
of attacks are missed by  
traditional antivirus  
solutions



**69%**  
spent more time managing  
tools than defending against  
the threats



What if you could rely on  
just one integrated  
solution?

# What if you could rely on just one integrated solution?

## Boost your monthly recurring revenue

- Easier upsells using integrated solutions
- Simplified renewals with integrated reporting
- Greater ROI via pre-built marketing campaigns



## Cut cyber protection costs by up to 50%

- One console, one license, one agent
- Integration drives deeper automation
- Consolidate vendor expenses



## Deliver unmatched cyber protection

- Reduce risk with 100% coverage of client workloads
- Unique capabilities not available from your current security vendors
- Leader in independent testing (VB100, AV-Test, AV-Comparatives)



## Legacy Backup & AV solutions

### Complex

Complicated licensing, deployment, and training, as well as agent conflicts

### Expensive

Multiple tools, vendors, administration costs

### Unsecure

Lack of integration creates gaps in defenses, management burden compromises security

## Acronis Cyber Protect Cloud

### All services managed from one place

Remove the complexity and risks associated with non-integrated solutions

### Easy

### Smarter use of resources

Faster operations with integration and automation lets your team focus on your clients

### Efficient

### Total peace of mind for clients

Customize your services and deliver complete protection for every workload

### Secure

# Acronis Cyber Protect Cloud

## Next-generation cybersecurity

- Advanced AI-based behavioral detection engine for zero-day attack prevention



## Reliable backup and recovery

- Full-image and file-level backup, disaster recovery, and metadata collection for security forensics



## Enterprise protection management

- URL filtering, vulnerability assessments, patch management, remote management, drive health



Integration provides unmatched manageability for MSPs—increasing security and productivity while decreasing operating costs

# Acronis Data Centers



**34+6**

## DATA CENTERS

Strong presence in Asia-Pacific,  
Singapore, Japan, Australia



Acronis Data Centers



Google Data Centers



Azure Data Centers

# Acronis Data Centers

## AMERICAS

Vancouver, CA  
Ashburn, US  
St. Louis, US  
Dallas, US  
Phoenix, US  
Sao Paulo, BR

## EUROPE

London, UK  
Thessaloniki, GR  
Warsaw, PL  
Lisbon, PT  
Strasbourg, FR  
Billund, DK  
Cologne, DE  
Prague, CZ  
Frankfurt, DE  
Lupfig, CH  
Echen, LI  
Tel Aviv, IL  
Valencia, ES

## APAC

Nagano, JP  
Chennai, IN  
Thimphu, BT  
Seoul, KR  
Singapore, SG  
Sydney, AU  
Auckland, NZ  
Taipei, TW

34+6

## DATA CENTERS

Strong presence in Asia-Pacific,  
Singapore, Japan, Australia



Acronis Data Centers



Google Data Centers



Azure Data Centers

# Acronis Cyber Protection Operation Centers



Top-level compliance

Up-to-date protection

Support and threat investigation

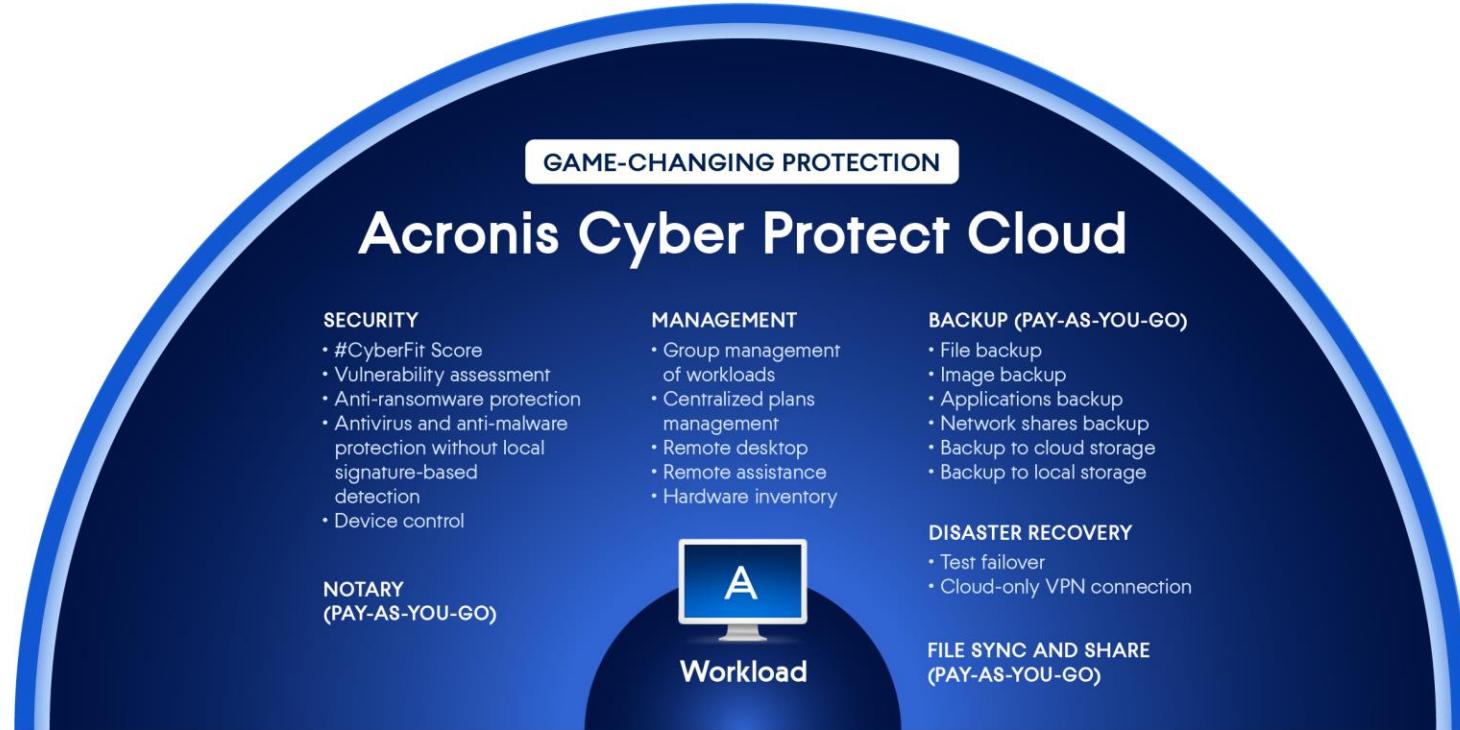
# Acronis

## Cyber Protect Cloud

### Product Overview



# Best-in-breed backup combined with integrated security and management



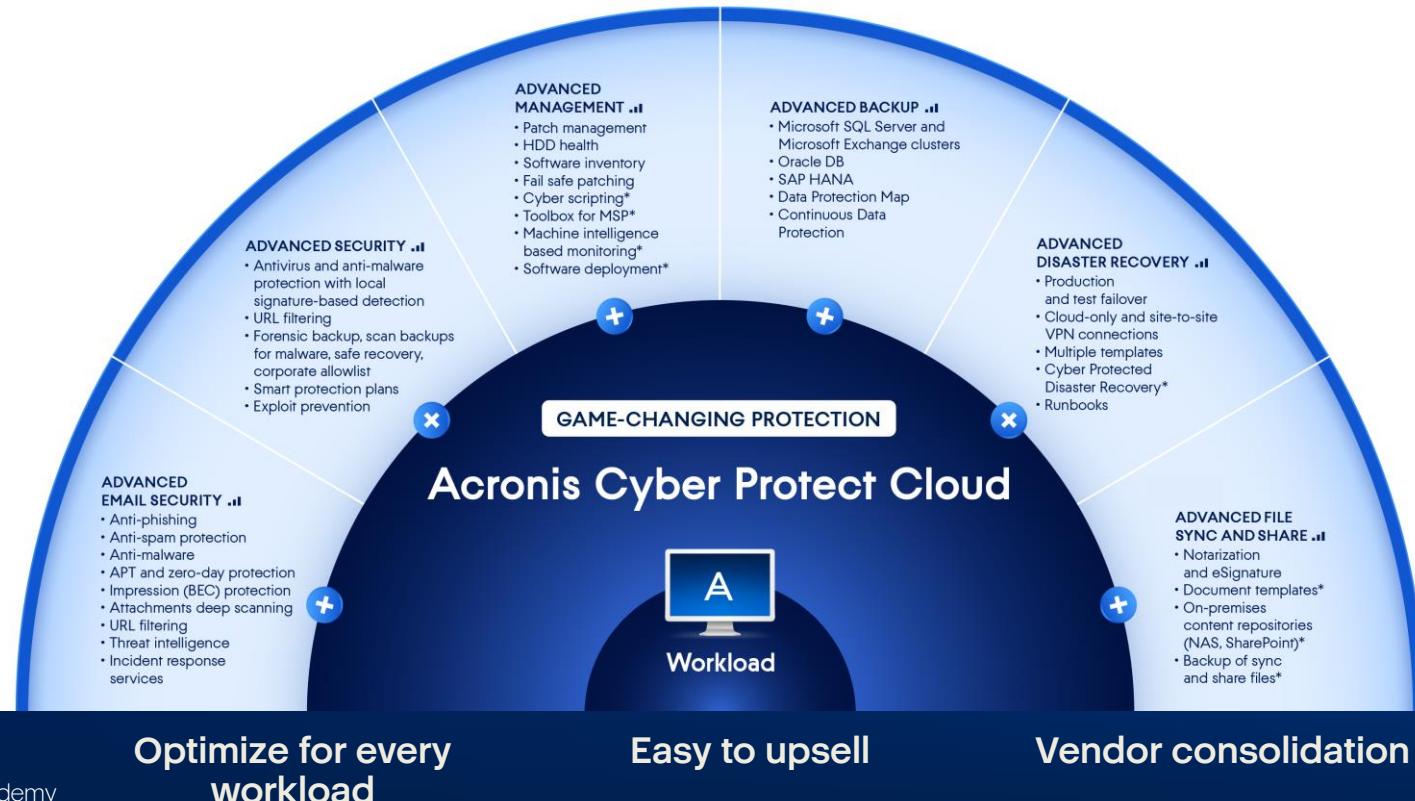
Protect every  
workload at no charge

Best-in-breed backup  
included

Strengthens your AV  
against zero-day threats

Accelerate security  
and manageability

# Add Advanced packs: Security, Management, Backup, Disaster Recovery, Email Security, File Sync and Share



# 2022 Roadmap for Service Providers



# Built for Service Providers

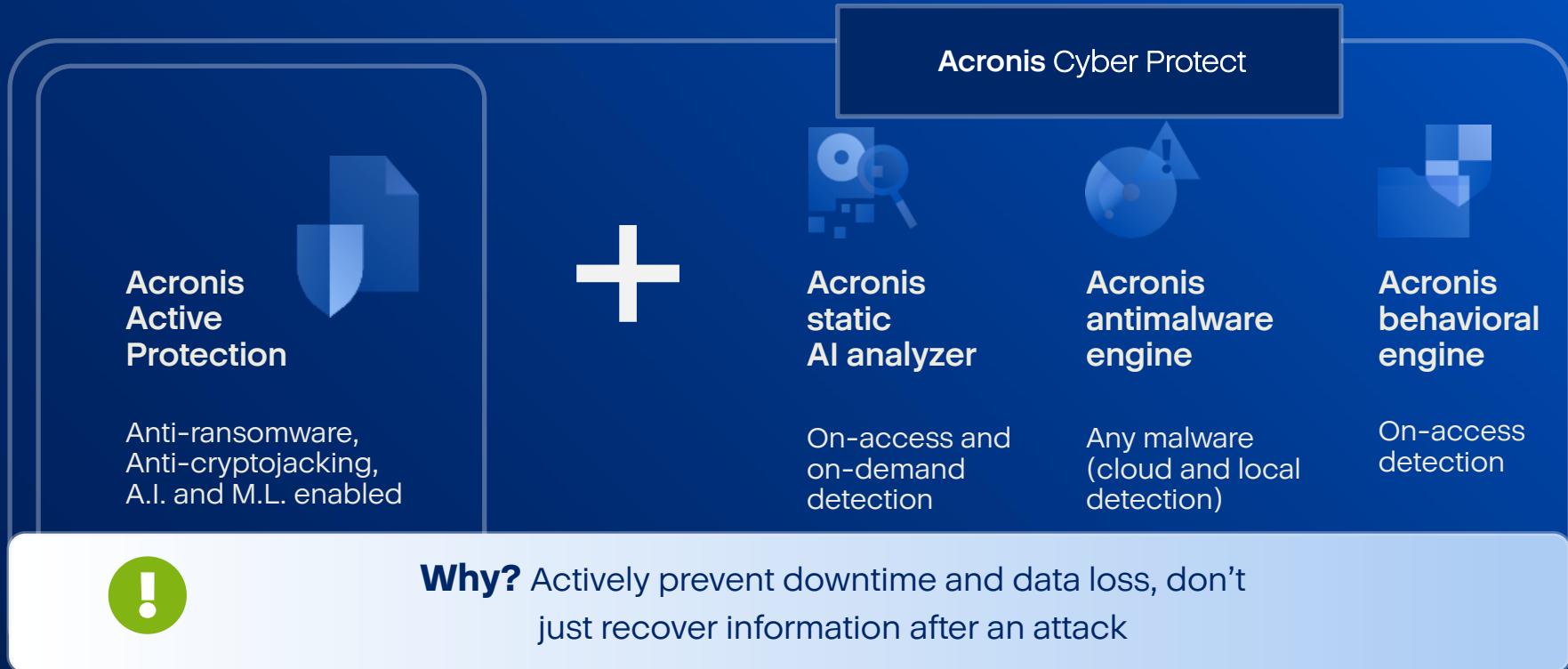
The screenshot displays two main sections of the Acronis Cloud web console:

- Left Sidebar:** Includes navigation links for Overview, Operations, Clients, Users, Alerts, Reports, and Settings. The "Acronis Cloud" logo and "Powered by Acronis AnyData Engine" are also present.
- Top Dashboard:** Features three main widgets:
  - ACTIVITIES FOR 24 HOURS:** A donut chart showing 120 total activities, with segments for OK (60), Warning (30), and Error (30).
  - ACTIVITIES FOR 7 DAYS:** A bar chart showing daily activity counts from Monday to Sunday.
  - MONTHLY STORAGE USAGE:** A line graph showing monthly storage usage in GB, with a current size of 351.65 GB.
- ALERTS:** A table listing alerts categorized by severity (Critical, Error, OK, Warning) and device. Examples include "Los Barrios" and "Mario Pizza".
- Bottom Dashboard:** Shows available integrations with logos for ConnectWise Manage, ConnectWise Automate, and Autotask, all labeled as "CERTIFIED INTEGRATOR".

## Service Provider Value:

- Easy, scalable management of customers' accounts via an easy-to-use web console
- Integration with Autotask, ConnectWise Automate, and ConnectWise Manage
- Integration with custom provisioning systems via RESTful management API
- Comprehensive white-labelling
- Straightforward pay-as-you-go pricing

# Next Generation Cyber Security



# Reliable Backup & Recovery

Protects more than **25** workloads and incorporates the backup industry's most advanced anti-ransomware technology, safeguarding data and systems in any environment – physical or virtualized, on-premises or in the cloud.



Azure	Windows Server	Windows PC	Exchange	SQL Server	Share Point	Active Directory	Hyper-V	Microsoft 365	Google Workspace	Linux Server	SAP HANA	Scale Computing
-------	----------------	------------	----------	------------	-------------	------------------	---------	---------------	------------------	--------------	----------	-----------------



ORACLE®



Amazon EC2	Mac	iPhone	iPad	Android	VMware vSphere	Oracle x86 VM Server	Oracle Database	Red Hat Virtualization	Linux KVM	Citrix XenServer	Virtuozzo	Nutanix
------------	-----	--------	------	---------	----------------	----------------------	-----------------	------------------------	-----------	------------------	-----------	---------

# Enterprise Protection & Management

## Identify

Infrastructure and devices auto-discovery

Vulnerability assessment

Data protection map

## Protect

Remote agent installation

Backup and Disaster Recovery

Unified protection policies management

## Detect

Defenses against malware / ransomware

Hard drive health control

Dashboards and reports

## Respond

Patch management integrated with backup

Malware quarantine

Rescue with bootable media

## Recover

Backup and Disaster Recovery

Forensic information in backups

Remote desktop



**Best practices approach to cybersecurity!**

Function areas grouped according to NIST Cybersecurity Framework

# Section Summary



- The threat landscape is becoming more complex due to more cyber crimes, remote work, unreliable traditional antivirus solutions, inefficient management - too many vendors, too many tools, a lot of manual work
- There is need for new all in one integrated solution that is easy to use, with multiple growth opportunities, efficient by achieving more with less and faster in operations and ensuring the optimal level of security delivering complete protection for every workload
- 28+6 Acronis DATA CENTERS for 24 hours global threats monitoring

# Section Summary



- Acronis Cyber Protect Cloud provides next generation cybersecurity, reliable backup and recovery and enterprise protection management
- Build for Service providers needs in mind it offers a single solution with multiple capabilities, enabling you to deliver customers complete piece of mind
- With Best-in-breed backup combined with integrated security and management as well continually growing advanced packs such as Security Management, Backup, Disaster Recovery, Email Security, File Sync and Share

# Acronis

## Cyber Protect Cloud

### **Cyber Protection Capabilities**



# Deep integration enables new capabilities

The screenshot shows a software interface titled 'Details' with a sidebar of icons. The main area lists several integrated features:

- Protection plan 1
- Backup: Entire machine to Cloud storage, Monday to Friday at 02:15 PM
- Disaster recovery: Recovery server: auto, Cloud network infrastructure: auto
- Antivirus & Antimalware protection: Self-protection on, Real-time protection on
- URL filtering: 0 denied, 44 allowed
- Vulnerability assessment: Microsoft products, Windows third-party products, Linux packages, at 10:00 AM, Sunday to...
- Patch management: Microsoft and Windows third-party products, at 02:35 PM, only on Monday
- Data protection map: 66 extensions, at 04:00 PM, Monday to Friday

An 'Add devices' button is located at the top right of the main area.

Integration at all levels: management, products, technology – and your business

- ✓ One agent
- ✓ One policy
- ✓ One UX/UI
- ✓ One license
- ✓ One vendor

# One Protection Plan

Efficiently enable, disable and configure services and policies on a per-client or group level (core and advanced packs):

- Backup
- Anti-malware protection
- Disaster Recovery
- URL filtering
- Vulnerability assessments
- Patch management
- Data discovery (via data protection map)
- Microsoft Defender Antivirus and Microsoft Security Essentials management



**Why?** Better protection with less effort, automated

Cyber Protection Plan Cancel Create

This protection plan requires the following advanced protection functionality based on your feature selection:

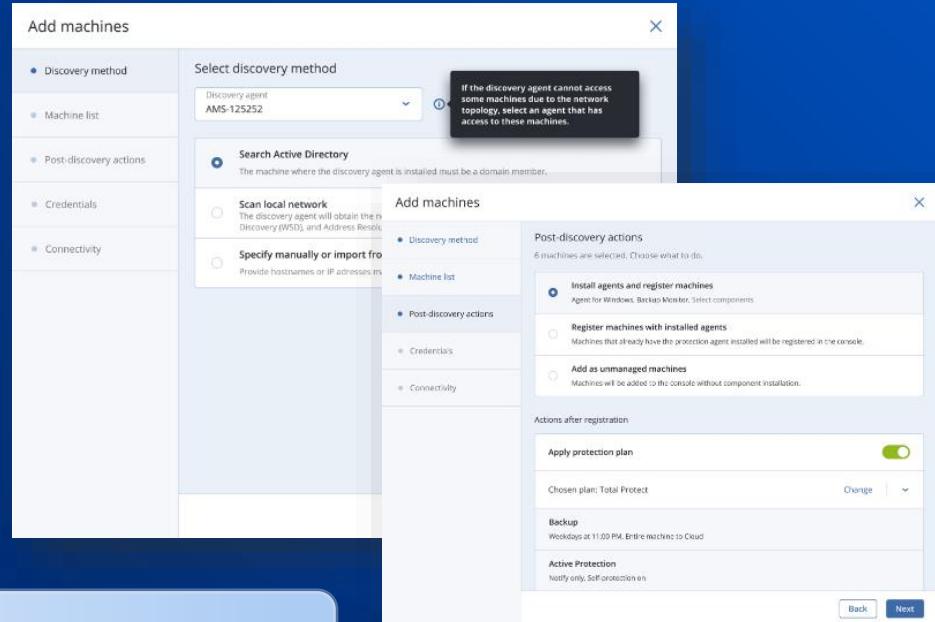
(i) ADVANCED BACKUP (i) ADVANCED SECURITY (i) ADVANCED MANAGEMENT

Backup	<input checked="" type="checkbox"/> Entire machine to Cloud storage, Monday to Friday at 11:45 PM	<input checked="" type="button"/>
Disaster recovery	<input checked="" type="checkbox"/> Recovery server: auto, Cloud network infrastructure: auto	<input checked="" type="button"/>
Antivirus & Antimalware protection	<input checked="" type="checkbox"/> Self-protection on, Real-time protection on	<input checked="" type="button"/>
URL filtering	<input checked="" type="checkbox"/> 0 denied, 44 allowed	<input checked="" type="button"/>
Windows Defender Antivirus	<input checked="" type="checkbox"/> Full scan, Real-time protection on, at 12:00 PM, only on Friday	<input checked="" type="button"/>
Microsoft Security Essentials	<input checked="" type="checkbox"/> Full scan, at 12:00 PM, only on Friday	<input checked="" type="button"/>
Vulnerability assessment	<input checked="" type="checkbox"/> Linux packages, Microsoft products, Windows third-party products, Apple produ...	<input checked="" type="button"/>
Patch management	<input checked="" type="checkbox"/> Microsoft and Windows third-party products, at 03:25 PM, only on Monday	<input checked="" type="button"/>
Data protection map	<input checked="" type="checkbox"/> 66 extensions, at 03:50 PM, Monday to Friday	<input checked="" type="button"/>
Device control	<input checked="" type="checkbox"/> Access to all device types is allowed. Allowlists are configured	<input checked="" type="button"/>

# Devices auto-discovery and remote agent installation

Simplify the process of installing multiple agents at once – both in the cloud and on-premises

- Network-based discovery
- Active Directory-based discovery
- Import a list of computers from the file
- Auto-apply a protection plan
- Batch remote agent installations with a discovery wizard



**Why?** Easier and faster onboarding. Fewer resources required. Completeness of protection.

# Innovative data protection scenarios



**Next-gen continuous data protection:** Avoid even the smallest data loss in key applications



**Safe endpoint recovery:** Integrate anti-malware updates and patches into the recovery process



**Fail-safe patching:** Automatically back up endpoints before installing any patches, enabling immediate rollback



**Data protection map:** Monitor the protection status of files with classification, reporting, and unstructured data analytics



**Forensic backup:** Image-based backups that capture additional data needed for forensic investigations



**Better protection with less resources:** Enable more aggressive scans and vulnerability assessments by offloading data to central storage, including the cloud



**Global and local allowlists:** Created from backups to support more aggressive heuristics, preventing false detections

# Section Summary



- Acronis Cyber Protect Cloud provides three integrated sets of functionality, including security, backup and management – when working together new capabilities of cyber protections are possible
- Deep integration at all levels with one: agent, policy, UX/UI, license and vendors
- One protection plan for better protection with less effort and automatization
- Devices auto-discovery and remote agent installation for easier and faster onboarding. Fewer resources required. Completeness of protection

# Acronis

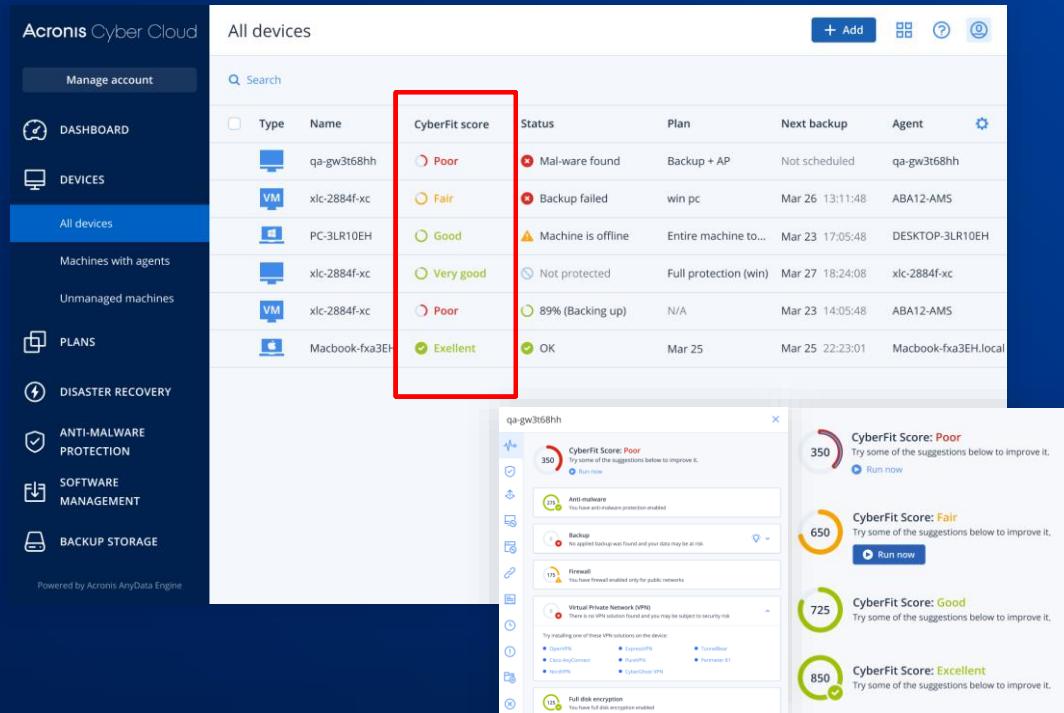
## Cyber Protect Cloud

### Included Features - Security



# Acronis #CyberFit Score

## Simplify MSP operations and service upselling



The screenshot shows the Acronis Cyber Cloud interface. On the left, a sidebar lists various management options: Manage account, DASHBOARD, DEVICES, All devices (which is selected), Machines with agents, Unmanaged machines, PLANS, DISASTER RECOVERY, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, and BACKUP STORAGE. Below this is a note: 'Powered by Acronis AnyData Engine'. The main area is titled 'All devices' and displays a table with columns: Type, Name, CyberFit score, Status, Plan, Next backup, and Agent. A red box highlights the 'CyberFit score' column, which contains color-coded icons: Poor (red), Fair (orange), Good (green), Very good (light green), Poor (red), and Excellent (green). Below the table, two small windows show detailed assessments for specific devices: 'qa-gw3t68hh' and 'Macbook-fxa3EH.local'. Each window provides a summary of the CyberFit score, a 'Run now' button, and a list of remediation suggestions.

Type	Name	CyberFit score	Status	Plan	Next backup	Agent
PC	qa-gw3t68hh	Poor	Malware found	Backup + AP	Not scheduled	qa-gw3t68hh
VM	xlc-2884f-xc	Fair	Backup failed	win pc	Mar 26 13:11:48	ABA12-AMS
PC	PC-3LR10EH	Good	Machine is offline	Entire machine to...	Mar 23 17:05:48	DESKTOP-3LR10EH
VM	xlc-2884f-xc	Very good	Not protected	Full protection (win)	Mar 27 18:24:08	xlc-2884f-xc
VM	xlc-2884f-xc	Poor	89% (Backing up)	N/A	Mar 23 14:05:48	ABA12-AMS
PC	Macbook-fxa3EH.local	Excellent	OK	Mar 25	Mar 25 22:23:01	Macbook-fxa3EH.local

Assess the level of protection of any machine:

- Is backup enabled?
- Is anti-malware installed?
- Is the firewall in place?
- Are HDDs encrypted?
- Is a VPN in use?

Suggests remediation options based on assessment

# Vulnerability Assessment

Discover an issue before an issue happens

Continuous, daily update of Acronis' vulnerability and patch management database

- Support for:
  - Microsoft:
    - a) Workstations – Windows 7 and later
    - b) Server – Windows Server 2008R2 and later
    - c) Microsoft Office (2010 and more) and related components
    - d) .NET Framework and server applications
  - Adobe, Oracle Java
  - Browsers and other software

The screenshot shows the Acronis Cyber Cloud interface. On the left is a sidebar with icons for Dashboard, Devices, Plans, Disaster Recovery, Anti-Malware Protection, Software Management, Patches, Vulnerabilities (which is selected), Backup Storage, and Reports. A 'Send Feedback' button is at the bottom. The main area is titled 'Vulnerabilities' and lists several entries:

Name	Affected products	Machines	Severity	Patches
CVE-2018-209654	Chrome, Firefox	12	CRITICAL	—
CVE-2018-1000016	Office 2010	3	HIGH	2
CVE-2018-1003	Acrobat Reader	3	HIGH	2
CVE-2018-10047	Hash Player for Chrome, Hash Pl...	7	MEDIUM	—
CVE-2018-3223	Windows Server 2016	14	LOW	1
CVE-2018-9800	Office 365 Client	9	NOTICE	3
CVE-2018-337894	Firefox	—	—	—

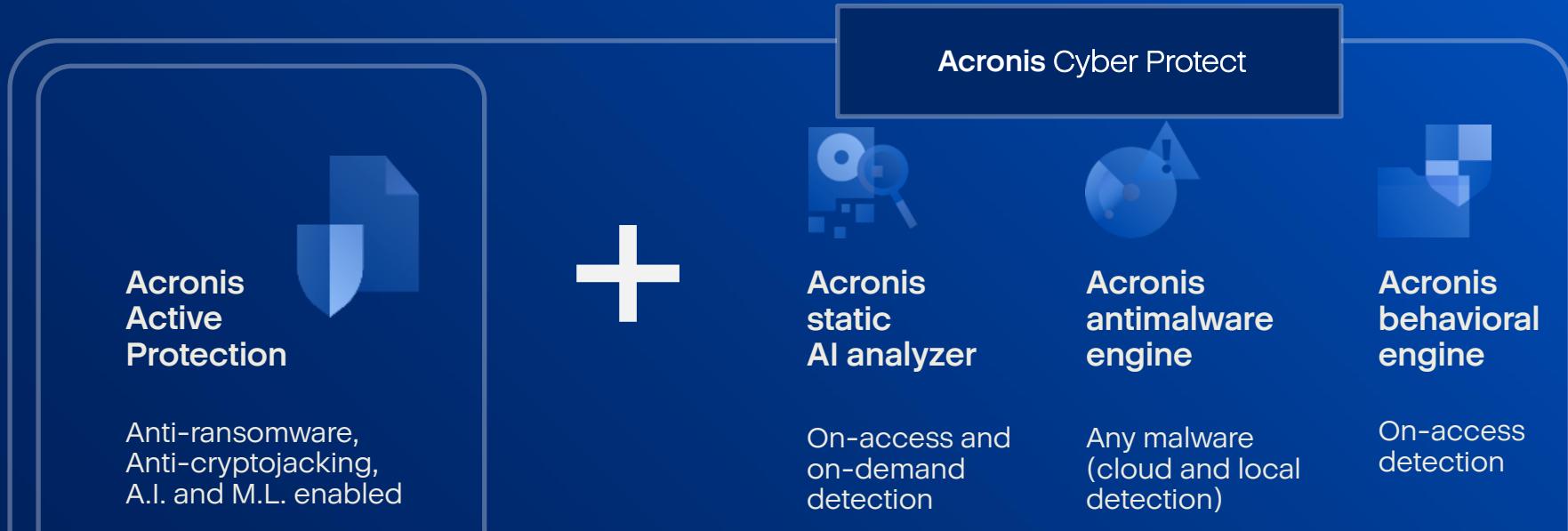
To the right of the main area is a 'What to scan' configuration dialog. It includes sections for Windows machines (checkboxes for Microsoft products and Other third-party products), Linux machines (checkbox for Scan linux packages), and Supported products. At the bottom are 'Reset to default', 'Cancel', and 'Done' buttons.



## Why?

Mitigates potential threats, prevents attacks.

# Next Generation Cyber Security



**Why?** Actively prevent downtime and data loss, don't just recover information after an attack

# Acronis Active Protection

## Backup industry's most advanced anti-ransomware technology



Persistently **guards files** including local backups from unauthorized modification and/or encryption



Relentlessly **defends backups** from alteration by hardening the Acronis agent application from attacks



**Instantly restores files** to the most recently backed up version should ransomware manage to get through the defense



Actively future-proofs your data protection because it is based on a **behavioral heuristic approach** and white-listing



Acronis provided excellent performance, is easy to use and has a rich feature set. On top of that it is the only solution in the test to provide dedicated protection from ransomware attacks. This earned Acronis **the first ever approved backup & data security certificate of AV-TEST**.

**David Walkiewicz**  
Director Test Research,  
[av-test.org](http://av-test.org)

# Acronis static AI analyzer

Next-gen static analysis to catch threats before they execute

Examine Windows executables (exe) and dynamic link libraries (DLLs) to determine whether or not a process is malicious prior to execution.

- Machine learning model – trained in Acronis Cloud Brain on millions of malicious and clean files via sandboxes and other security tools
- Proactive layer of protection against malware
- Continuous improvement (new models are trained every hour)

	Suspicious activity is detected	Oct 01, 2021, 09:28 AM
On machine 'WIN2K22DC03', injection process within program 'C:\Windows\System32\notepad.exe' modified file 'C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\DAT1.pdf'. The process has been stopped, and the file changes have been reverted.		
Device	WIN2K22DC03	
Process	C:\Windows\System32\notepad.exe	
Monitored because	Parent process certificate is not valid	
Suspicious because	Suspicious data has been written to several files.	
Action	Revert using cache	
Affected files	C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\DAT1.pdf C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\DAT1.pptx C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\im1.png C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\DAT1.docx C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\im12.png C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\pict10.jpg C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\pict11.jpg C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\pict12.jpg C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\DAT1.xlsx C:\KnowBe4\RsSimulator\TestFolder\Tests\16-Tests\DAT3.docx and 13 other files	
Support		Clear



## Why?

Detect malware triggered without execution

# Signature-based detection

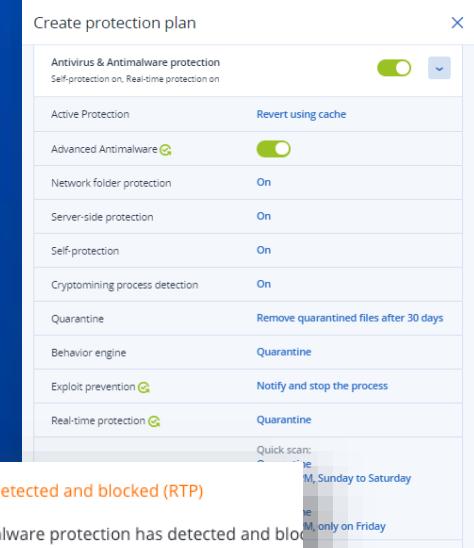
## Faster and more efficient detection

Cloud-based (in Acronis Cyber Protect Cloud as well):

- Based on AI- and behavior-based detections for faster detection

Enhanced local signature-based detection (Advanced Security):

- Better detection rate
- Improved detection speed
- Local detection even in cases with poor internet connections



**Why?** Better and faster protection:  
increase the known malware you can catch instantaneously

# Behavior-based detection

## Powerful behavioral heuristics to catch sophisticated threats

Analyze suspicious kernel-level events and all events coming from Windows OS to detect malicious attacks with detection-evasive behavior

- Effectively dealing with fileless, memory- and script-based attacks (part of APT invasion)
- Dynamic detection rules – catch polymorphic and obfuscated malware
- New malware techniques using symlinks for encrypting files, such as RIPlace, evade detection by most competitive technologies
- Effective detection of unknown, new, and developing threats

	A malicious process is detected	Oct 01, 2021, 09:28 AM
Anti-Malware Protection has detected the malicious process '973548515.axp'.		
Device	WIN2K22DC03	
Plan name	Protect Server 3	
File name	973548515.axp	
File path	C:\KnowBe4RSSimulator\TestFolder\Tests\19	
MD5	e9e1d6fa3580ace4be580faed138f986	
SHA1	87e1ef3e2eea66dfa2e71d00ee608abdb030ef9	
SHA256	01b67181f74c383cd8065172f15b114aecc9ffc60eb6743b83221f7180dbe182	
Threat name	Ransom.Collab.A	
Action	Moved to quarantine	
Support		
Clear		



### Why?

Prevent sophisticated attacks with detection-evasive behavior

# Section Summary



- Acronis Cyber Fit Score – provides and easy way to find out if the customer is up to certain level of service in terms of cyber protection
- Vulnerability Assessment – discover issue before the issue happens with daily updates and information of the latest version of supported workstations, servers, browsers, applications and components. Mitigates potential threats and prevents attacks.

# Section Summary



- Acronis Cyber Protect Cloud actively prevent downtime and data loss, don't just recover information after an attack
- Including powerful features as: Acronis Active Protection, Acronis static AI analyzer, Signature-based detection, Behavior-based detection

# Acronis

## Cyber Protect Cloud

### Included Features - Management



# Centralized backup plans management

Improve efficiency by managing backup plans from one tab

The new “Plans” tab shows all backup plans created in the account and their details.

You can create, edit, disable, enable, delete, start the execution and inspect the execution status of a plan

Type	Name	Devices	Status	Schedule	Destination	Actions
Entire machine to C...	Entire machine to C...	1	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	1	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Disks/volumes to Cl...	Disks/volumes to Cl...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Disks/volumes to Cl...	Disks/volumes to Cl...	0	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Disks/volumes to E/...	Disks/volumes to E/...	0	OK	Monday to Friday at 1...	E/1/	<span>Details</span>
Disks/volumes to E/...	Disks/volumes to E/...	0	OK	Monday to Friday at 1...	E/2/	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Files/folders to E/	Files/folders to E/	0	OK	Monday to Friday at 1...	E/	<span>Details</span>

The screenshot shows a user interface for managing backup plans. On the left is a sidebar with icons for Create plan, Import, Details, Run now, Stop, Edit, Activities, Alerts, Clone, Export, and Disable. The main area is titled "Backup plans" and contains a table with the following data:

Type	Name	Devices	Status	Schedule	Destination	Actions
Entire machine to C...	Entire machine to C...	1	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	1	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Disks/volumes to Cl...	Disks/volumes to Cl...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Disks/volumes to Cl...	Disks/volumes to Cl...	0	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Disks/volumes to E/...	Disks/volumes to E/...	0	OK	Monday to Friday at 1...	E/1/	<span>Details</span>
Disks/volumes to E/...	Disks/volumes to E/...	0	OK	Monday to Friday at 1...	E/2/	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 1...	Cloud storage	<span>Details</span>
Entire machine to C...	Entire machine to C...	0	OK	Monday to Friday at 0...	Cloud storage	<span>Details</span>
Files/folders to E/	Files/folders to E/	0	OK	Monday to Friday at 1...	E/	<span>Details</span>

A tooltip with the text "OK" is displayed over the status bar of the first plan in the list.

# Remote Desktop & Remote Assistance

Remotely operate any endpoint as if near the device

- Securely connect to remote machines even behind a firewall on a private network without changing firewall settings or establishing additional VPN tunnels
- Allows engineers to view user's screen and provide support with specific tasks or fix issues

All devices							+ Add	Actions
Type	Name	Account	#CyberFit Score	Status	Last backup	Next backup	More	More
VM	Win2k19 DC 02	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		#CyberFit Score
VM	WIN2K19DC02	Amos Dong (ad.tech)	625/850	OK	May 15 11:18:02 PM			Protect
VM	Win2k19 DC 01	Amos Dong (ad.tech)	Not supported	Not protected	Never			Disaster recovery
VM	WIN2K19DC01	Amos Dong (ad.tech)	625/850	Continuous Data P...	May 15 11:24:15 PM			Recovery
VM	Win10 Ent 01	Amos Dong (ad.tech)	Not supported	Not protected	Never			Cyber Protection Desktop
VM	WIN10ENT01	Amos Dong (ad.tech)	625/850	OK	May 18 04:30:48 PM			Patch
VM	VM Replica	Amos Dong (ad.tech)	Not supported	OK	Never			Details



## Why?

Fewer tools, plus less effort to connect, and faster reaction times, reduced costs

# Hardware inventory collection

- Discover all hardware assets on all protected endpoints of the organization (e.g. CPU, GPU, motherboard, RAM, network adapters, etc.)
- Get up-to-date information about hardware assets:
  - Regular scans can be scheduled to run automatically
  - On-demand scans can be manually triggered by engineers
- Get detailed hardware information about hardware assets such as model, manufacturer, serial number, etc.
- Browse all hardware assets, or search and filter by multiple criteria: processor model, processor cores, disk total size, memory capacity
- Generate hardware inventory reports

The screenshot shows a software interface for managing hardware inventory. On the left, a list of devices is displayed, including VMs like 'qa-gw3t68hh', 'MF\_2012\_R2', and several Oracle Linux instances. On the right, a detailed view is shown for the device 'DESKTOP-GLN477D'. This view includes tabs for Overview, Plans, Details, Software, Hardware (which is selected), and Activities. The Hardware tab displays information for the Motherboard (Z170X) and Processors (Intel Core i5-9600K). A modal window is open for the processor details, showing its manufacturer (Intel Corporation), model (9600K), max clock speed (3.7 GHz), and number of cores (4 Cores, 8 Logical Processors). An 'OK' button is visible in the bottom right corner of the modal.

Type	Name
VM	qa-gw3t68hh
VM	MF_2012_R2
VM	10.250.194.111
VM	Oracle 11 Linux
VM	APanin CentOS7
VM	vm-sql_2012
VM	DESKTOP-GLN477D
VM	qa-gw3t68hh
VM	dc_w2k12_r2
VM	T
VM	10.250.210.89
VM	HyperV_for12A

Motherboard	
Name	Z170X
Manufacturer	Gigabyte Technology Co. Ltd.
Model	Z170X Gaming
Serial number	132-LF-E657

Processors	
Processor	Intel(R) Core(TM) i5-9600K CPU
Manufacturer	Intel Corporation
Model	9600K
Max clock speed	3.7 GHz
Number of cores	4 Cores, 8 Logical Processors



## Why?

Fewer tools, plus less effort to connect, and faster reaction times, reduced costs

# Section Summary



- Centralized backup plan management for improved efficiency by managing backup plans from one tab- assign plans and operate from one central location
- Remote Desktop & Remote Assistance for remote operation of any endpoint as if near the device. Fewer tools, plus less effort to connect, and faster reaction times, reduced costs.
- Hardware inventory collection - saves time and effort with up-to-date hardware inventory information

# Acronis

## Cyber Protect Cloud

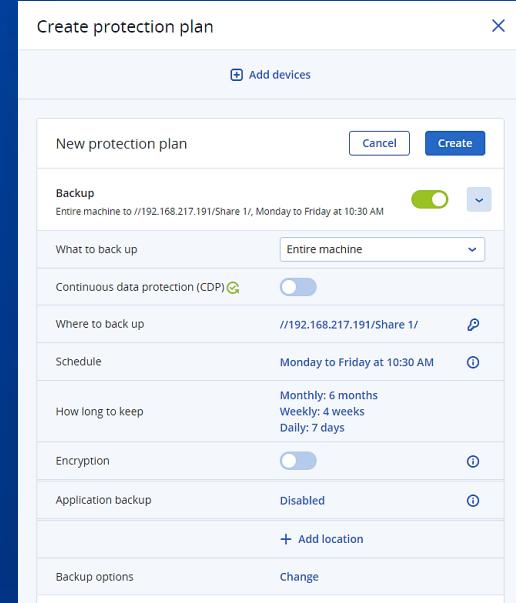
### Pay-as-you-go Features - Backup



# Full-image and file-level backups

Back up individual files or safeguard an entire business with a few clicks

- **File-level backup:** Use this option to protect specific data, reduce the backup size, and save storage space
- **Full-image backup:** Easily back up the entire system as a single file, ensuring bare metal restores
- In the event of data disaster, you can easily restore all information to new hardware



## Why?

Ensure business continuity with flexible backup options and avoid downtime and data loss

# Flexible storage options

Meet data sovereignty or cost requirements



Three turnkey cloud storage options



Other public clouds  
*(via gateway)*

Cloud storage



Your own or third-party cloud storage



Local disks



SMB/CIFS/DFS and  
NFS shares



Acronis  
Cyber Infrastructure

On-premises storage

“Other solutions shoehorned us into a situation where we had to tell our customers they couldn't do certain things. **With Acronis we have complete flexibility**, and this allows us to offer the best user experience.

**Jason Amato,**  
Marketing Manager at  
Centorrino Technologies

# Customizable Backup Settings

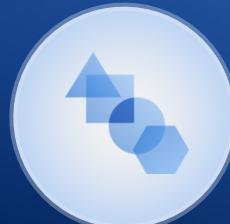
## Flexible retention policies

Set up a backup retention policy and apply it to a specific device or a number of machines. You can store backups indefinitely, limit the number of backups per machine, or specify how long to keep backup files.



## Multiple backup types

Back up disks/volumes (with all information required for the operating system to boot), individual files or folders, system state (for Microsoft Windows systems), or ESXi configuration.



## Customizable backup scheduling

Perform backups according to the desired schedule and frequency – monthly, weekly, daily, hourly, or even every 10 minutes. You can also limit the number of simultaneously running backups.



# Provide Protection for 25+ Workload Types from Infrastructure to SaaS apps



Azure	Windows Server	Windows PC	Exchange	SQL Server	Share Point	Active Directory	Hyper-V	Microsoft 365	Google Workspace	Linux Server	SAP HANA	Scale Computing
-------	----------------	------------	----------	------------	-------------	------------------	---------	---------------	------------------	--------------	----------	-----------------

aws	Mac	iPhone	iPad	Android	VMware vSphere	Oracle x86 VM Server	Oracle Database	Red Hat Virtualization
Amazon EC2								
Red Hat Virtualization	Linux KVM	Citrix XenServer	Virtuozzo	Nutanix				

Streamline delivery  
of cyber protection  
using just one  
solution

A

# Complete Microsoft 365 Protection



Backup for  
Microsoft  
Exchange Online



Backup for  
Microsoft OneDrive  
for Business



Backup  
for Microsoft  
SharePoint Online



Backup for  
Microsoft Teams  
Including call protection

- ✓ Back up from Microsoft data centers directly to cloud storage
- ✓ Automatically protect new Microsoft 365 users, groups and sites
- ✓ Search through Microsoft 365 backups to get quick access to your backed-up data

New

Unlimited Acronis cloud storage for personal Microsoft 365 mailboxes

# Google Workspace Backup

Google Workspace



Get an efficient  
cloud-to-cloud solution with  
nothing to install



Ready-to-use cloud storage  
options include Google, Microsoft,  
and Acronis



Protection for Gmail, Drive  
(including Team Drives), Calendar  
and Contacts



Flexible restore options – from  
single items to a user's entire Drive  
or Gmail data



Search Google Workspace  
backups – with metadata and full-  
text (email body copy) capabilities



Verify authenticity  
of files in Drive backups with  
blockchain

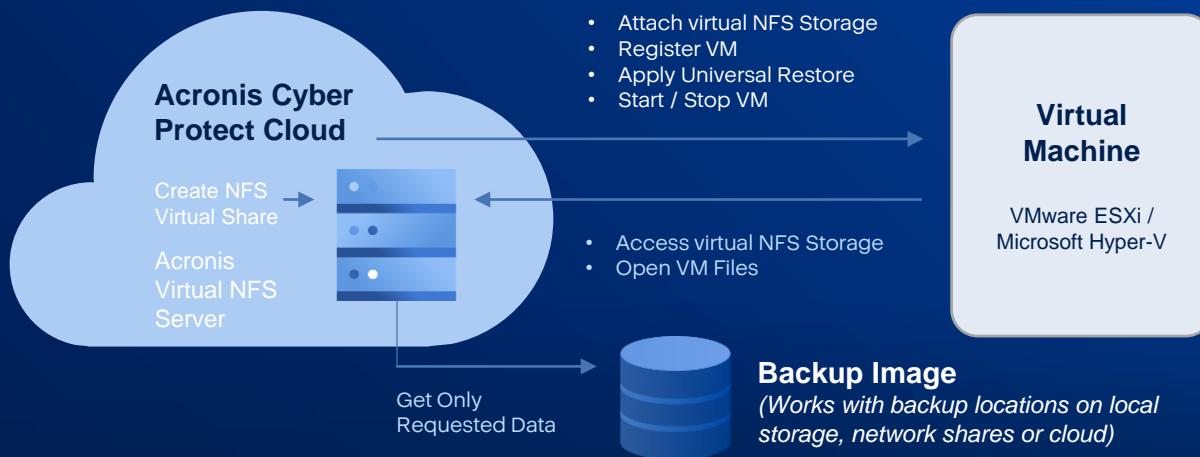
New

Unlimited Acronis-hosted storage for Google Drive

# Best-In-Industry RTOs with Acronis Instant Restore

Acronis Instant Restore is patented technology that allows you to recover systems in seconds by starting any Windows or Linux system (physical or virtual) directly from the backup storage on your existing Microsoft Hyper-V or VMware vSphere ESXi host – without moving data.

## How it works



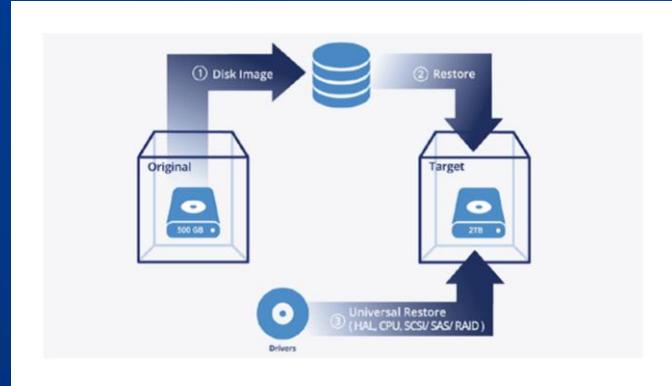
### Benefits

- RTO in seconds
- Recover any virtual, physical or cloud server, Windows or Linux
- Reduced network consumption

# Acronis Universal Restore

## Restore Windows and Linux systems to dissimilar hardware

- Quick and easy system recovery to dissimilar hardware, including bare-metal physical, virtual, or cloud environments
- After recovering a disk-image as-is, Acronis Universal Restore analyzes the new hardware platform and tunes the Windows or Linux settings to match the new requirements



### Why?

Ensure quick, easy system migration with a few clicks, reduce RTOs and minimize expensive downtime

# Section Summary



- Full-image and file-level backups - ensures business continuity with flexible backup options and avoid downtime and data loss
- Flexible storage options - complete flexibility allowing to offer the best user experience
- Customizable Backup Settings – including flexible retention policies, multiple backup types and customizable backup scheduling
- Acronis protects over 25+ workloads - Increase productivity and keep user-error at bay working with just one solution for all customer needs, rather than switching between per-use-case tools

# Section Summary



- Complete Microsoft 365 Protection – with unlimited Acronis cloud storage for personal Microsoft 365 mailboxes
- Google Workspace Backup -With fast backups, reliable point-in-time recovery, flexible restore and cloud storage options, as well as quick-search functionality, Acronis Cyber Backup Cloud gives you a lot to offer your customers – with no additional installation required
- Best-In-Industry RTOs with Acronis Instant Restore – provides RTO in seconds, recover any virtual, physical or cloud server, Windows or Linux, reduced network consumption

# Acronis

## Cyber Protect Cloud

### Pay-as-you-go Features – Files, Sync and Share



# File, Sync and Share

An easy, efficient and secure file sync and share solution designed for service providers



**Easy** – Easy to sell, easy to deploy, and easy for end customers to use

**Efficient** – Turnkey solution for end-customer's business across all platforms (phones, tablets, Macs, Windows)

**Secure** – 100% control over data location, management and privacy



## Why?

Easy to sell and implement, File, Sync and Share expands your product portfolio and helps you quickly attract new customers, realize incremental revenues and reduce customer churn.

# File, Sync and Share for End Customers

Safely share files with co-workers or external contacts

Supports collaboration  
using web, desktop, mobile

Enables full-text search  
capability

Allows users to edit office  
files via the mobile app

Helps users meet data  
governance regulations

Maintains a history  
of all transactions

Protects against data loss

Stays stable on slow  
internet connections

Proves safer than Box,  
Dropbox, and others



# File, Sync and Share for Service Providers

Sell more storage and services

Expand product portfolio with no additional investments

Utilize provisioning API for PSA/RMM integrations

Deliver strong reliability, availability, and serviceability requirements

Utilize full integration with Acronis Cyber Cloud Services and Portal

Use any storage - Acronis Cyber Infrastructure, SWIFT, Ceph, NAS, S3, Azure

“Lock in” customers, prevent revenue loss, reduce customer churn



# File, Sync and Share – What's Cool

## User

- Sync and access from any device (web, desktop, mobile devices)
- Edit or comment in Office files directly via the mobile app
- Share files with co-workers or external contacts
- Full support for MS Office mobile app

## Safety

- Browse and restore previous versions of files
- Store files in a known, secure location with anywhere access
- Restore deleted files
- Gain in-transit and on-device encryption

## Platforms

- Full BYOD support
- Desktop and Laptop: PC, Mac
- Mobile: iOS, Android
- Web browser support

## Deployment

- Hybrid or hosted by Acronis
- Multi-tenant with multi-tier support for resellers

## Customization

- Branding
- UI look and feel customization
- Multi language support

## Integration

- Provisioning API for integration with third party or in-house Control Panels
- Usage reporting for billing systems
- Acronis Cyber Infrastructure repository

# Top 5 Reasons to Choose File, Sync and Share

**1**

**Easy**

- Easy to sell and deploy
- Easy to use with second-generation refined user experience
- Simple, unified pricing with Acronis Backup Cloud for easy incremental revenue

**2**

**Efficient**

- Turnkey solution for service providers
- Advanced mobile, desktop and web clients
- Rich file-sharing and collaboration features
- Built-in PDF and Microsoft Office editing
- Integration with Microsoft mobile applications

**3**

**Secure**

- Customers and service providers control where files are stored
- Compliance with data sovereignty laws
- Strong protection options for mobile content
- Leverages Acronis Storage with Acronis CloudRAID

**4**

**Proven**

- A decade in development
- Trusted by top Fortune 500 companies globally
- 100Ks of users
- 9 data centers worldwide

And...

**5**

**Better than all others!**

- Easy to install, configure, manage and use
- Integrated and optimized to work with Acronis products
- Consistent user experience across all Acronis products
- Provisioning and performance automation

# Section Summary



- File, Sync and Share -provides office and mobile users with safe file access, sync, and share in an easy-to-use, complete, and secure hosted cloud solution
- Easy to sell and implement, expands your product portfolio and helps you quickly attract new customers, realize incremental revenues and reduce customer churn.
- Safely share files with co-workers or external contacts
- It is efficient, secure, proven and provides consistent user experience across all Acronis products and allows you to sell more storage and services

# Acronis

## Cyber Protect Cloud

### Pay-as-you-go Features – Notary



# Gain the Notary Advantage

- Ensure the integrity of business-critical data
  - Eliminates the need for third parties to guarantee the immutability of data
- Achieve greater regulatory transparency
  - Reduces the cost and time needed to conduct an audit
- Reduce risks to data security
  - Adds an extra layer of protection, powered by a mathematical proof
- Accelerate and automate the signature process
  - Execute every step of the document workflow, eliminate manual tasks, and connect with the tools and systems you're already using

The screenshot shows the 'NOTARIZED FILES' section of the Acronis Cyber Cloud interface. It displays a table with columns for Name, Status, Blockchain, Notarized, and Uploaded. A single file, 'Contract\_Test\_01.pdf', is listed with a status of 'In progress', blockchain 'Ethereum', and uploaded on '29 Sep, 2020 09:45 AM'. There are buttons for 'Add files' and a search bar.

The screenshot shows a 'NOTARIZATION CERTIFICATE' page. It includes a QR code, a digital signature icon, and a message stating 'Successfully signed! You have successfully signed MyContract.pdf. You will receive a notification when all signees sign the file.' The certificate details are as follows:

File name	Contract_Test_01.pdf
Notarization timestamp	29 Sep, 2020 09:47 AM UTC +0300
File size	234.33 KB (239,956 bytes)
File hash (SHA-256)	ac1ac9a6445c8bede47272b06d4f982f77d1964056d1d3bd331cafb7e706621d
Requestor	Acronis demo stand
Requestor GUID	c35a109-9c59-4c7-aef-aec84017cf08
Signer	Notary
Transaction ID	0x1331f46cb8dee1db0a41c74e4858e69d0e35f793698d7fb02b8644a3
Certificate ID	4de2a58b15f9379dd959ee88c4d92a28d35884c27874542b829ba56a1dd7e4

# How Your Business Can Benefit From Data Notarization?

- Verify that a document is unchanged or changed
- Confirm that a creative work originated on a certain date
- Prove a legal document existed when you claim it did
- Corroborate that bills were paid
- Prove a document was signed by certain parties on a specific date

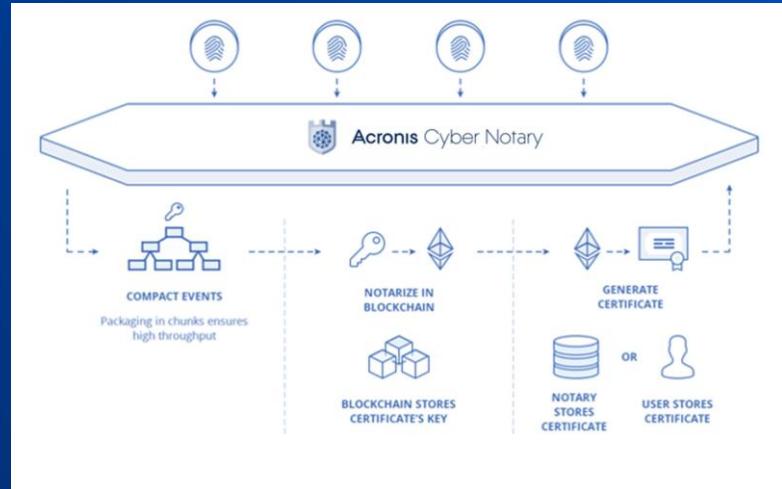


Any Industry. Any Document. Any Data.

# Blockchain notarization

Ensure data integrity with innovative blockchain-based Acronis Cyber Notary

- Highly scalable micro-service architecture
- API interface (REST), queue interface (AMQP) for integration
- High throughput (xx10,000 objects per blockchain transaction)
- Notarization certificates with built-in verification



**Why?** Ensure the integrity of business critical data, achieve greater regulatory transparency and reduce security risks

# Notary

Ethereum blockchain

Advanced E-signature  
functionality

Easy-to-use web interface

Helps users meet data  
governance regulations

Smooth integration via API

Protects against data loss

Any type of data

Trusted, independent  
verification

Comprehensive white-labeling



# Section Summary



- Notary- Blockchain - based authentication system ensuring that the stored data is as authentic as placed in the repository
- Notary ensures the integrity of business critical data, achieves greater regulatory transparency and reduces security risks for any industry, any document, any data
- With highly scalable micro-service architecture, easy-to-use web interface, trusted, independent verification, smooth integration via API and advanced E-signature functionality

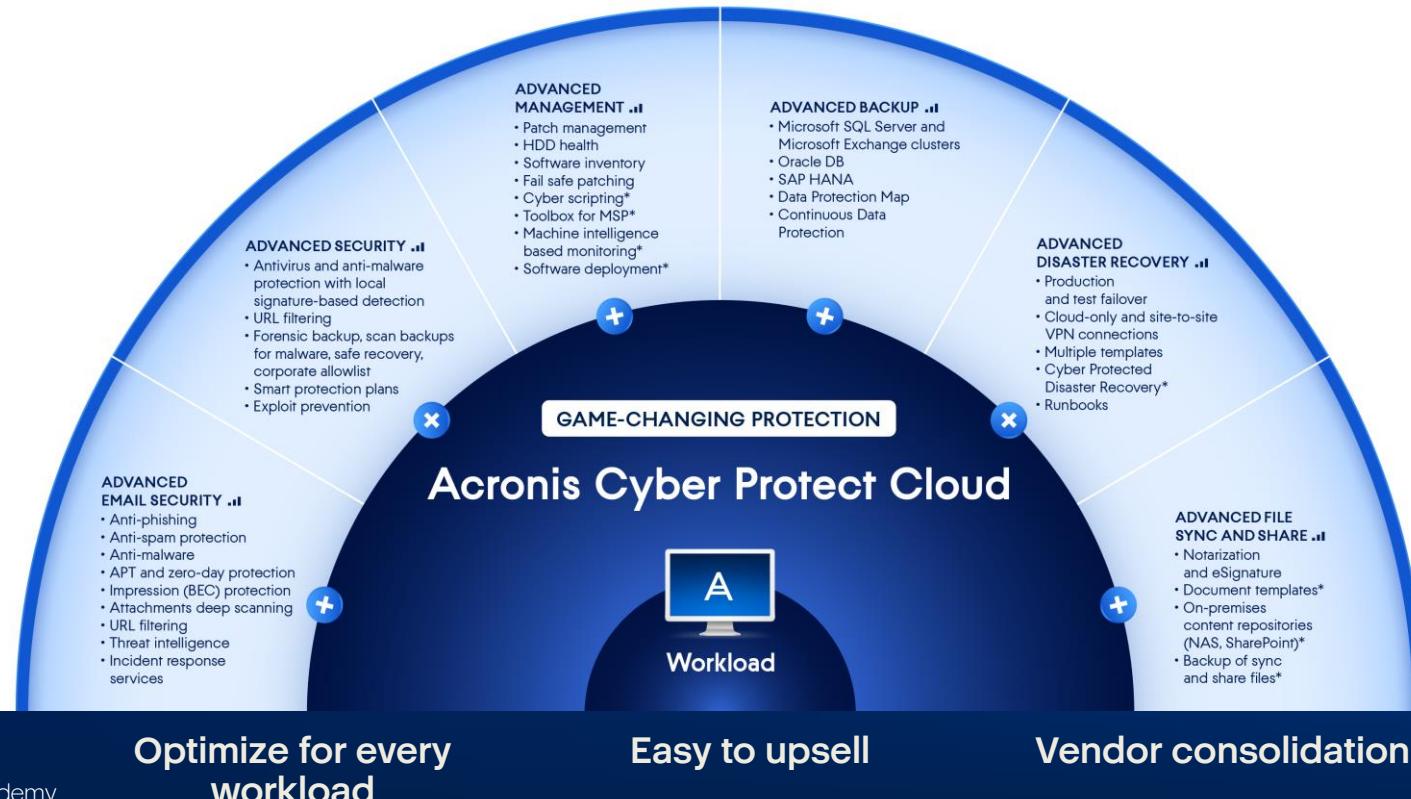
# Acronis

## Cyber Protect Cloud

### Advanced Packs – Overview



# Add Advanced packs: Email Security, Security, Management, Backup, Disaster Recovery, File Sync and Share



# Acronis Cyber Protect Cloud with Advanced Email Security powered by

Improve client security by detecting any email-borne threat before it reaches end-users



## Stop phishing and spoofing attempts

Minimize client risks with powerful threat intelligence, signature-based detection, URL reputation checks, unique image-recognition algorithms, and machine learning with DMARC, DKIM, and SPF record checks.



## Catch advanced evasion techniques

Detect hidden malicious content by recursively unpacking embedded files and URLs and separately analyzing them with dynamic and static detection engines.



## Prevent APTs and zero-day attacks

Prevent advanced email threats that evade conventional defenses with Perception Point's unique CPU-level technology, which acts earlier in the attack chain to block exploits before malware is released, delivering a clear verdict within seconds.

# Acronis Cyber Protect Cloud with Advanced Security

Improve security by detecting more threats, save on simplified security management, and deliver better remediation with integrated cyber protection



## Full-stack antimalware

Acronis Active Protection, enhanced with exploit prevention, URL filtering, antimalware detection for backed-up data, and improved detection rate to catch more threats faster



## Security automation

Smart protection plans, auto-allowlist custom apps, automatic malware scans and AV definitions updates as part of recovery process to deliver services more effortlessly



## Efficient forensics

Collect digital evidence and safe it in a secure central repository to enable thorough post-incident investigations and proper remediation, while keeping costs down.

# Acronis Cyber Protect Cloud with Advanced Management

Improve clients' protection by keeping systems up-to-date  
while decreasing the management burden and TCO



## Advanced patch management

Keep systems up-to-date and proactively mitigate vulnerabilities.



## Patch management automation

Save time and effort with patch management automation and fail-safe patching technology



## Comprehensive management tools

Streamline your planning with software inventory collection, report scheduling, and drive health monitoring.

# Acronis Cyber Protect Cloud with Advanced Backup

Protect your clients' data confidently with best-in-breed backup  
enhanced with cyber protection



## Increase automation and productivity

Scheduled backup reports, paired with cloud backup enhancements – like continuous data protection – helps you save time while saving your clients from data loss



## Deliver the most secure backup

Acronis delivers a unique approach by combining cloud backup with cyber protection features, such as antimalware and antivirus – helping you keep clients' data secure



## Protect more workloads on more platforms

From a single console, protect more than 20 workload types, including Microsoft Exchange, Microsoft SQL Server, Oracle DBMS Real Application clusters, and SAP HANA

# Acronis Cyber Protect Cloud with Advanced Disaster Recovery

Protect clients with the flip of a switch



## Less downtime

Get clients running in mere minutes by spinning up IT systems in the Acronis cloud with full site-to-site connectivity and the ability to recover them to similar or dissimilar hardware



## Minimize complexity

No need to add, learn, or manage another platform. It's one solution for any workload managed from a single interface that enables you to build a complete cyber protection service



## Grow recurring revenue

Deliver more value, deepen client relationships, and increase retention by offering clients the disaster recovery services they are looking for – while increasing your monthly recurring revenue

# Acronis

## Cyber Protect Cloud

### Advanced Packs – Backup



# Backup enhanced with cyber protection

## Acronis Cyber Protect Cloud

- File-level, disk-level, image and application backups
- Backup popular workloads like Mac, Windows, Linux, Microsoft 365, Google Workspace, Hyper-V, VMware, and more
- Flexible backup storage options
- Acronis Active Protection
- Archive encryption
- Incremental and differential backups
- Antimalware and anti-virus protection
- Vulnerability assessments
- Instant restore with RunVM
- and more...



## Advanced Backup

- Backup support for Microsoft SQL Server Clusters, Microsoft Exchange Clusters, Oracle DB, SAP HANA
- Data protection map and compliance reporting
- Scheduled backup reports

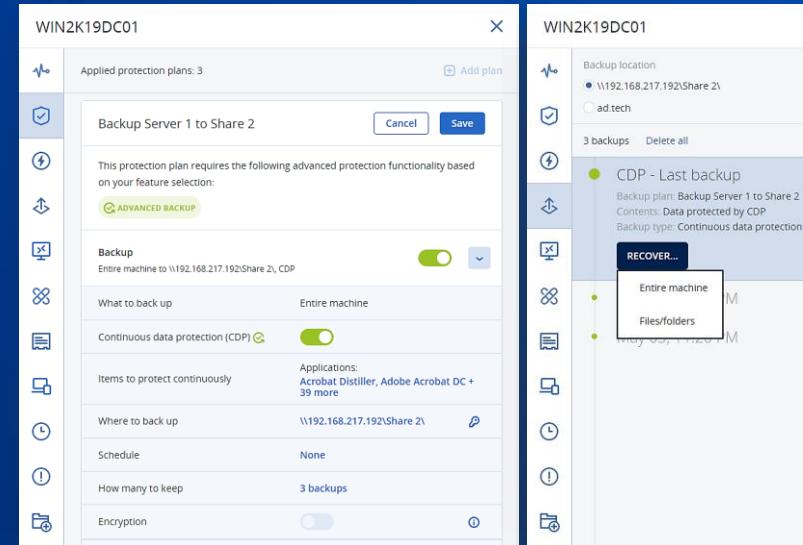
# Continuous Data Protection

Gain safe and instant remediation without data loss and close to zero RPOs

Define the list of critical apps for every device users are working with most often. Acronis' agent monitors every change made in listed applications.

In case of a malware infection, restore data from the last backup and apply the latest collected changes so no data is lost.

- Ensures users won't lose their work in-progress
- Control what is continuously backed up – Office documents, financial forms, logs, graphic files, etc.



**Why?** Protects client data even between backups

# Cluster-aware backup of Microsoft SQL Server and Microsoft Exchange Server

- Enable backup and reliable recovery of clustered Microsoft applications data, even in case of a database logical corruption or a cluster-wide disaster.
- Acronis Cyber Protect Cloud discovers and takes into account the structure of the cluster and tracks all data relocation to enable safe backups.

The screenshot shows a software interface for managing databases in a Microsoft Exchange environment. On the left, there's a navigation tree with 'Microsoft Exchange' selected, followed by 'Databases', then 'dag13'. Under 'dag13', several databases are listed: 'm1.d13.local' (selected), 'm2.d13.local', and 'm3.d13.local'. Below these are 'Mailboxes' with 'All' and 'm1.d13.local' options. On the right, a table lists the databases with columns for Type, Name, Status, and Last backup. The databases shown are 1, 2, 3, 'Jack Of All Trades', and 'newdb1', all marked as 'OK' with a green checkmark. A toolbar at the top right includes 'Group backup' and 'Specify credentials' buttons.

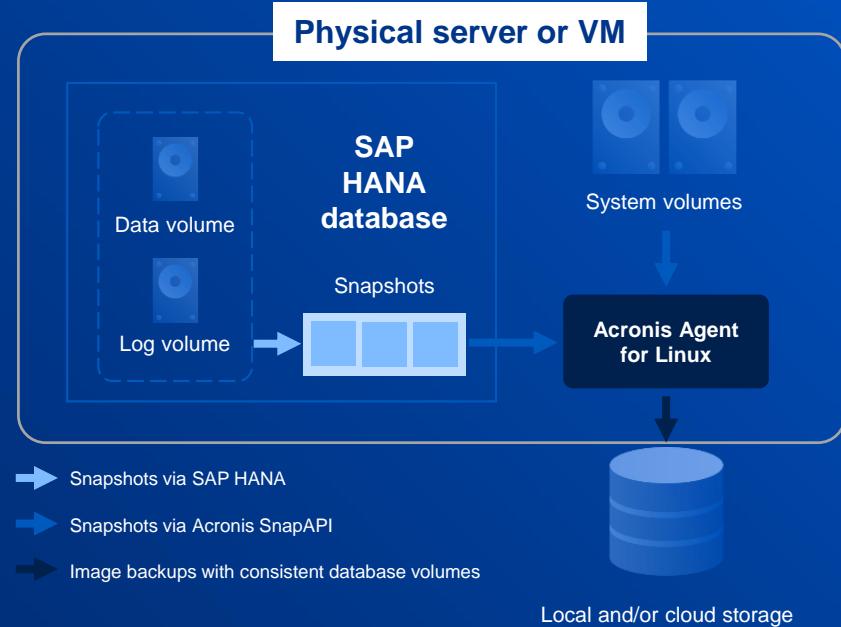
Type	Name	Status	Last backup
1	m1.d13.local	OK	Apr 22 03:10
2	m2.d13.local	OK	Apr 22 03:12
3	m3.d13.local	OK	Apr 22 03:15
	'Jack Of All Trades'	OK	Apr 22 03:18
	'newdb1'	OK	Apr 22 03:22



**Why?** Keep Microsoft applications data safe with built-in capabilities for easy back up and recovery.

# Application-aware SAP HANA backup

- Protect the database data from disk storage failures and logical errors, by creating consistent disk-level backups of servers running SAP HANA in a simple, straightforward manner that does not require any SAP HANA knowledge or expertise.
- You can then reliably recover SAP HANA servers to bare metal, same or different hardware, migrate them from a physical machine to a virtual machine and vice versa – the SAP HANA data inside the backup will be consistent.



**Why?** Enable quick, reliable recovery of SAP HANA database servers.

# Data compliance reporting and Data Protection Map

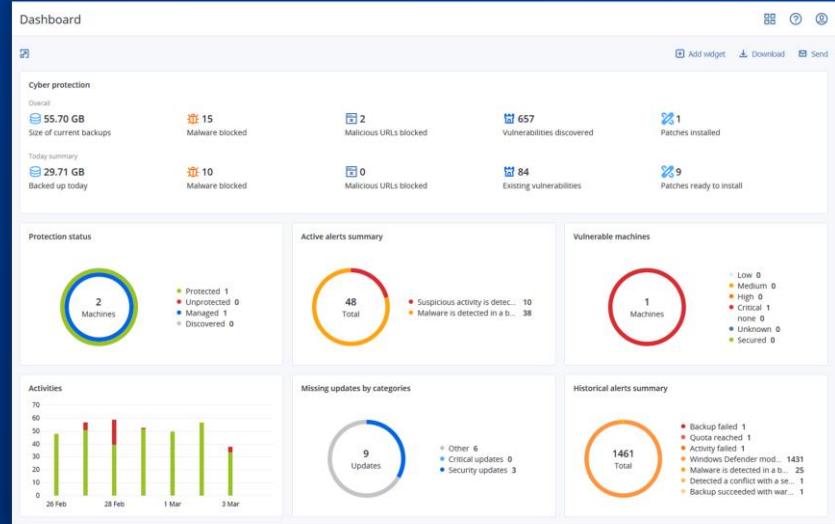
- Use automatic data classifications to track the protection status of important files. IT will be alerted as to whether the files were backed up or not.
- Data distribution across endpoints is clearly visible
- Protection of specific files and inclusion in backup plans is easily confirmed
- Risk mitigation steps are easy to execute
- Collected data is used as the basis for compliance reports



**Why?** Complete protection that's easy, with no important data missed

# Flexible Monitoring and Reporting

- Hardware health monitoring (HDD, SSD)
- Active alert control
- Missing updates control
- Customizable dashboard widgets
- Quickly identify problems
- Fast access to management actions



**Why?** Single pane of glass, faster operations, helps demonstrate MSP value and simplify renewals

# Section Summary



- Advanced Backup Pack comes on top of the pay-as –you-go Acronis Cyber Protect Cloud features, including additional powerful features as:
- Continuous Data Protection for protection of clients data event between backups
- Cluster-aware backup of Microsoft SQL Server and Microsoft Exchange Server, that keep Microsoft applications data safe with built-in capabilities for easy back up and recovery

# Section Summary



- Application-aware SAP HANA backup that Enable quick, reliable recovery of SAP HANA database servers
- Data compliance reporting and Data Protection Map for complete protection that's easy, with no important data missed
- Flexible Monitoring and Reporting including single pane of glass, faster operations, helps demonstrate MSP value and simplify renewals

# Acronis

## Cyber Protect Cloud

### Advanced Packs – Disaster Recovery



# Disaster Recovery with Cyber Protection

## Acronis Cyber Protect Cloud

- File-level, disk-level, image and application backups
- Backup popular workloads like Mac, Windows, Linux, Microsoft 365, Google Workspace, Hyper-V, VMware, and more
- Flexible backup storage options
- Acronis Active Protection
- Archive encryption
- Incremental and differential backups
- Antimalware and anti-virus protection
- Vulnerability assessments
- Instant restore with RunVM
- and more...



## Advanced Disaster Recovery

- Production and test failover to Acronis Cloud
- Runbooks: disaster recovery orchestration
- VPN-less deployment option
- IPsec Multisite VPN support, L2 site-to-site open VPN
- Multiple templates
- Custom DNS configuration
- Free of charge DR testing

# Who Needs Disaster Recovery?

## Companies that:

- Rely on mission-critical applications and data
- Are subject to regulated compliance requirements
- Are partners in stringent supply chains
- Are located in disaster-prone areas
- Lack technical resources
- Have heavy reliance on IT for business functions
- Lack disaster recovery experience

## Key industries:



Financial Services



Healthcare



Legal



Transportation



Business Services



Manufacturing



Construction

# Make Disaster Recovery Painless



Disaster recovery for virtual and physical workloads



Backup-based replication of production machines



Disaster recovery orchestration with runbooks



Easy extension of local networks to the cloud recovery site

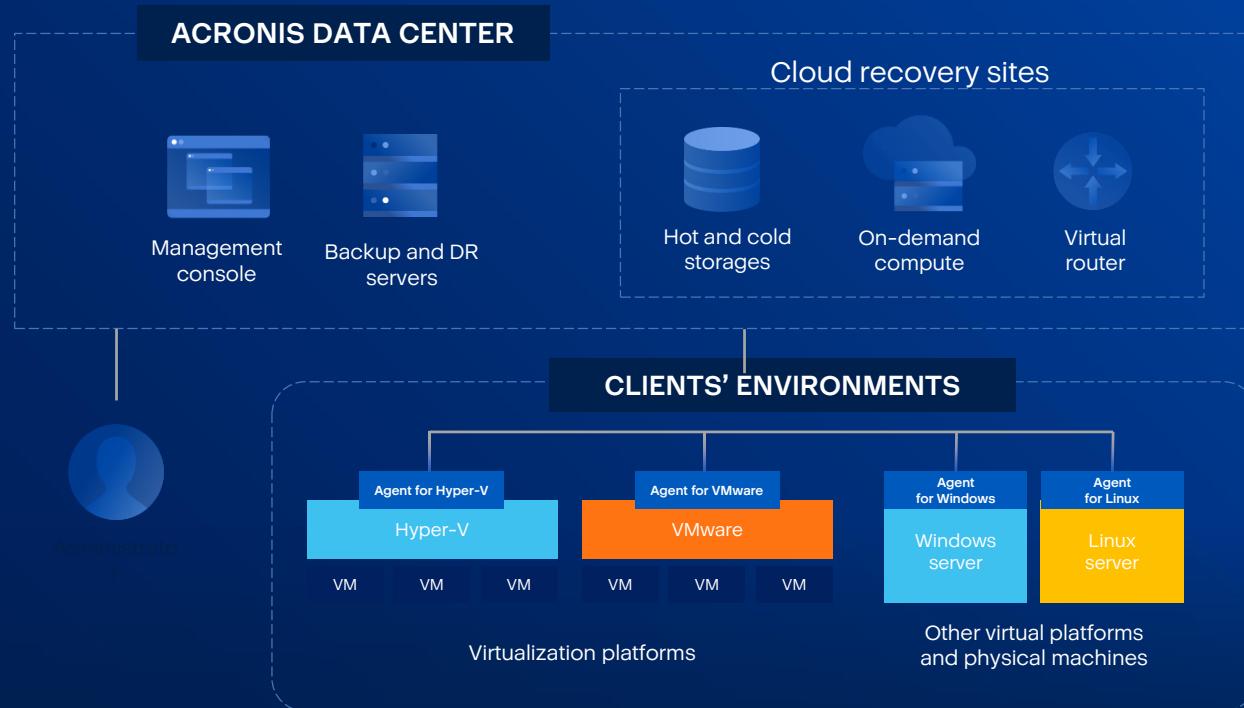


Test failover in isolated environments - without business disruption



Multiple points in time for recovery

# Simplify Clients' Disaster Recovery With a Turn-Key SaaS Solution



- ✓ All components out-of-the-box
- ✓ Easier and quicker PoC and deployment stages
- ✓ Single console helps you easily offer disaster recovery for your clients

# Disaster Recovery for Any Workload

## Physical and virtual machines

- Windows

- Linux

## Virtualization platforms

- VMware vSphere
- Microsoft Hyper-V
- Linux KVM

- Virtualization
- Citrix XenServer

## Cloud servers for real-time application replication

- For applications with built-in replication like SQL Server AlwaysOn



Windows Server

Exchange

SQL Server

Share Point

Active Directory

Hyper-V



Citrix XenServer



Linux Server



VMware vSphere



Red Hat Virtualization



Linux KVM

# Improve RTOs and Automate Disaster Recovery with Runbooks

- Runbooks simplify and speed up failover of multiple machines to a cloud recovery site
- Allows efficient operations to automate failover and testing and ensure systems are recovered in the right order to address interdependencies between applications on different machines

Production failover

Step 1

- Failover server DBSERVER2012 - recovery Continue if already done
- Start server APPSERVER2012 - recovery Continue if already done

Step 2

- Execute runbook My cool runbook

Step 3

- Manual operation Change MX record to x.x.x

Add step

Test Failover

Name	Description
Test Failover	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Execution history

Start and end time	Status	Mode
14 Apr., 08:01PM	Started	Production
14 Apr., 08:01PM - 14 Apr., 10:23PM	Completed	Test
14 Apr., 08:01PM - 14 Apr., 10:23PM	Completed	Production
14 Apr., 08:01PM - 14 Apr., 10:23PM	Completed	Production
14 Apr., 08:01PM - 14 Apr., 10:23PM	Completed	Production



## Why?

Ensures that all systems are recovered in the right order

# Runbooks Improve RTOs and Automate Recovery



## Design

Use the intuitive **drag-and-drop editor** to define groups of machines and sequences of action with these groups



## Test

Verify the integrity of your disaster recovery plans by executing runbooks in the **test mode** in the web console



## Execute

**Execute runbooks in a few clicks** when the real disaster strikes and minimize RTOs with fast failover and fallback of multiple servers



## Monitor

Gain disaster recovery orchestration visibility with a detailed **runbook execution real-time view** and **execution history**

# Automated failback for virtual machines

## Achieve near-zero downtime

- Achieve best-in-class failback times and safeguard your clients' data by transferring it to the local site, while the virtual machine in the cloud is still running. Receive system progress updates and expected downtimes estimates to effectively plan the failback process.
- Streamline your efforts by managing the whole process in one panel
- Benefit from one of the lowest switchover downtimes on the market
- Eliminate confusion with easy user instructions in the interface

The screenshot shows the Acronis Cyber Cloud web interface. On the left is a sidebar with navigation links: DASHBOARD, DEVICES, PLANS, DISASTER RECOVERY (selected), Servers, Runbooks, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, and INFRASTRUCTURE. The main area has a title bar 'Acronis Cyber Cloud' and 'Servers'. Below the title bar are tabs: RECOVER SERVERS (selected) and PRIMARY SERVERS. A sub-menu for 'DR\_Server\_W2K3\_SP2\_x64' is open, showing options: Edit, Console, Power off. Below the tabs are sections: Name (with a dropdown arrow), Search, and a list of servers: DR\_Server\_W2K3\_SP2\_x64, DR\_Server\_W2K3\_SP3\_x64, and DR\_Server\_W2K3\_SP4\_x64. To the right is a detailed view for 'DR\_Server\_W2K3\_SP2\_x64'. At the top of this view are buttons: Details, Activities, Backup, and Failback. The 'Failback parameters' section includes a progress bar with steps: Planning, Data transfer, Switchover, and Validation. A button 'Switchover!' is highlighted in blue. Below the progress bar, a message says: 'Data is being transferred to the local site and the virtual machine is running. To reduce downtime, start the switchover after at least 90% of the data is transferred to the local site. After the switchover starts, the virtual machine is powered off.' A section titled 'How the failback works' provides technical details: Progress (16 GB of 2 TB), Downtime estimation (7 h 15 m), Target (Virtual machine), Target machine location (HyperV: VMware ESXi Host: 10.250.194.69), Agent (125Acronis-Backup-VA-ESXi-host82), Target machine settings (Virtual processors: 1, Memory: 1 GB, Network adapters: 2), Datastore (2TB\_HDD\_Datastore\_11), Provisioning mode (Thin), and Target machine name (DR\_Server\_W2K3\_SP2\_x64).



## Why?

Achieve near-zero downtime, ensure business continuity,  
and safeguard your clients' data

# Section Summary



- Advanced Disaster Recovery Pack comes on top of the pay-as – you-go Acronis Cyber Protect Cloud features, including additional powerful features as:
- Production and test failover to Acronis Cloud
- Runbooks: disaster recovery orchestration and more
- Acronis securely and cost effectively allows you to establish a disaster recovery strategy with minimal effort so you can sleep better at night
- Acronis Disaster Recovery eliminates the need to spend money on a second location, duplicate hardware, and media handling since the solution is ready-made.

# Acronis

## Cyber Protect Cloud

### Advanced Packs – Security



# Cyber Protection with Advanced Security

## Acronis Cyber Protect Cloud

- File-level, disk-level, image and application backups
- Backup popular workloads like Mac, Windows, Linux, Microsoft 365, Google Workspace, Hyper-V, VMware, and more
- Flexible backup storage options
- Acronis Active Protection
- Archive encryption
- Incremental and differential backups
- Antimalware and anti-virus protection
- Vulnerability assessments
- Instant restore with RunVM
- and more...



## Advanced Security

- URL filtering
- Exploit prevention
- Enhanced signature-based detection
- Anti-malware scans of data in the Acronis Cloud: Offload client endpoints to enable more aggressive scans and ensure malware-free backups
- Forensics data in backups
- Smart protect plans
- Automatic allowlisting
- Safe recovery: AV definition updates and antimalware scans as part of recovery process to prevent threat recurrence
- Remote device wipe
- Windows anti-malware management

# Enhanced protection

## Features added by Advanced Security:

- URL filtering
- Exploit prevention
- Anti-malware protection for backed-up data
- Enhanced virus signature database

## Features in Acronis Cyber Protect Cloud:

- AI-based static analyzer
- Behavior-based detection
- Anti-ransomware

## Expand your security services, earn more and deliver better protection

- ✓ Increase profitability – up-sell and cross-sell opportunities
- ✓ Minimize risk for clients with a full-stack anti-malware solution
- ✓ Cover more attack vectors – stop web-based attacks and exploits
- ✓ Increase detection rate and speed
- ✓ Prevent threat recurrence

# Enhanced protection

## Features added by Advanced Security:

- Safe recovery
- Forensics data in backups

## Features in Acronis Cyber Protect Cloud:

- Backup and recovery
- Automatic ransomware rollback
- Instant Restore
- Restore to dissimilar hardware
- P2C2V migrations

## Enable complete, fast, and cost-effective remediation

- ✓ Ensure breaches are fully remediated with forensic insights
- ✓ Cut remediation costs and ease the process – simplify security investigations with collected digital evidence
- ✓ Protect the recovery process to prevent threat recurrence
- ✓ Store digital evidence in a secure, central repository

# Simplified management

## Features added by Advanced Security:

- Smart protection plans – auto-adjustment of protection policies
- Auto-allowlist of custom apps
- Malware scans in Acronis Cloud
- Windows native anti-malware management
- Remote device wipe

## Features in Acronis Cyber Protect Cloud:

- Centralized protect management
- Monitoring and reporting
- Vulnerability assessments
- Device control – essential data loss prevention (DLP)
- #CyberFit Score – security gap assessments

**Improve your engineers' efficiency, save time, and serve more customers better**

- ✓ Manage a single, integrated solution – reduce resources needed to deliver services
- ✓ Cut costs through solution consolidation
- ✓ Improve reaction times
- ✓ Ensure no false positives
- ✓ Reduce load on clients' endpoints with malware scans in Acronis Cloud
- ✓ Prevent data leakage from lost or stolen devices

# Section Summary



- Advanced Pack Security comes on top of the pay-as -you-go Acronis Cyber Protect Cloud features, including additional powerful features
- Stop more cyberthreats for clients with fewer resources. The Advanced Security add-on extends the endpoint protection capabilities of Acronis Cyber Protect Cloud, enabling you to lower the risks for your clients with full-stack anti-malware protection and remediation services. Simplify deployment, configuration, and management tasks with advanced integration and automation

# Acronis

## Cyber Protect Cloud

### Advanced Management Pack



# Cyber Protection with Advanced Management

## Acronis Cyber Protect Cloud

- File-level, disk-level, image and application backups
- Backup popular workloads like Mac, Windows, Linux, Microsoft 365, Google Workspace, Hyper-V, VMware, and more
- Flexible backup storage options
- Acronis Active Protection
- Archive encryption
- Incremental and differential backups
- Antimalware and anti-virus protection
- Vulnerability assessments
- Instant restore with RunVM
- and more...



## Advanced Management

- Automated patch management
- Software inventory collection
- Drive health monitor
- Fail-safe patching
- Report scheduling

# Comprehensive patch management

## Features added by Advanced Management:

- Patch management

## Features in Acronis Cyber Protect Cloud:

- Vulnerability assessment



## MSPs can proactively prevent exploitation of a wide array of vulnerabilities

- ✓ Keep clients' systems up-to-date
- ✓ Proactively prevent attacks from taking advantage of system vulnerabilities
- ✓ Remediate gaps in clients defenses
- ✓ Enable better vulnerability management with fewer resources

# Increased service effectiveness

## Features added by Advanced Management:

- Patch management automation
- Fail-safe patching

## Features in Acronis Cyber Protect Cloud:

- Auto-discovery and remote installation

## Increase your engineers productivity and reduce patch management complexity

- ✓ Save time and effort while keeping systems up-to-date with automatic patching
- ✓ Eliminate the risk from downtime due to failed patches
- ✓ Address vulnerabilities faster
- ✓ Strengthen compliance – set specific deadlines by which patches must be applied

# Efficient maintenance planning

## Features added by Advanced Management:

- Software inventory collection
- Drive health monitoring
- Report scheduling

## Features in Acronis Cyber Protect Cloud:

- Centralized and group management
- Hardware inventory collection
- #CyberFit Score
- Remote desktop assistance
- Monitoring and reporting

## Streamline your workflows, save time, reduce the number of human errors

- ✓ Reduce management burden – more efficient management of clients and their workloads with less resources
- ✓ Ease and increase the efficiency of work planning
- ✓ Gain thorough visibility over data protection, assets and applications
- ✓ Proactively minimize unplanned downtime – due to disk failure
- ✓ Deploy your resources more effectively and efficiently

# Section Summary



- Advanced Pack Management comes on top of the pay-as –you-go Acronis Cyber Protect Cloud features, including additional powerful features
- Keep your clients' systems up-to date and simplify protection management
- With Advanced Management, service providers can spend less time juggling solutions and more time focusing on protecting their clients' data, applications and systems. The add-on package enables automated patch management and easy work planning to reduce your administrative burden.

# Acronis

## Cyber Protect Cloud

### Advanced Pack- Email Security



# Higher profitability

## Unlock new revenue streams



### Expand/Enhance your stack of services

Expand or enhance your stack of services with email security



### Start planning your services' upgrade

Start planning the upgrade of your services without worrying for the time needed to implement, email security is enabled with the flip of a switch.



### Upgrade your costs, margins, profitability

Upgrade your costs, margins, profitability, and business plan and secure additional revenue streams



### Leverage consumption-based pricing

Leverage pricing per protected mailbox (unique mailbox per user)

# Stronger protection

## Protect your clients' #1 threat vector from any attack



### Minimize clients' risks

Minimize risks to clients when communicating via email and stop threats before they reach end-users' Microsoft 365, Google Workspace, or Open-Xchange mailboxes



### Prevent email-borne threats

Prevent spam, phishing, business email compromise (BEC), spoofing, malware, malicious URLs, zero-days and APTs (Advanced Persistent Threats)



### Block advanced attacks

Block sophisticated attacks that evade conventional defenses: APTs, Zero- and N-days



### Cover 100% of traffic

Analyze every bit of content at any scale



### Don't disrupt processes

Ensure minimum delays and receive clear verdict within 3 seconds on average with near-zero false positives, compared to 7-20 mins for sandboxing solutions



### Leverage a leading technology

Build your services on top of a leading technology in independent evaluations (SELabs)

# Stronger protection

## Protect your clients' #1 threat vector from any attack



### Consolidate solutions

Manage a single solution integrating email security, backup, disaster recovery, anti-malware, and cyber protection management – reduce resources needed to deliver services



### Cut costs

Cut costs through consolidation of solutions



### Reduce deployment complexity

Greatly reduce email security deployment complexity, reducing deployment times to a few minutes and eliminating the need for additional configurations



### Increase threat visibility

Gain increased visibility over all email security alerts and incidents



### Get access to security professionals

Empower your service delivery and security pros teams with direct access to cyber analysts and email security experts

# Advanced Email Security: Stop any email-borne threat



Malware and ransomware



Phishing



Business email  
compromise (BEC)



Internal phishing



Account takeover



Zero-days and APTs



Evasion techniques

# Acronis Cyber Protect Cloud with Advanced Email Security

powered by



Improve client security by detecting any email-borne threat before it reaches end-users



## Stop phishing and spoofing attempts

Minimize client risks with powerful threat intelligence, signature-based detection, URL reputation checks, unique image-recognition algorithms, and machine learning with DMARC, DKIM, and SPF record checks.



## Catch advanced evasion techniques

Detect hidden malicious content by recursively unpacking embedded files and URLs and separately analyzing them with dynamic and static detection engines.



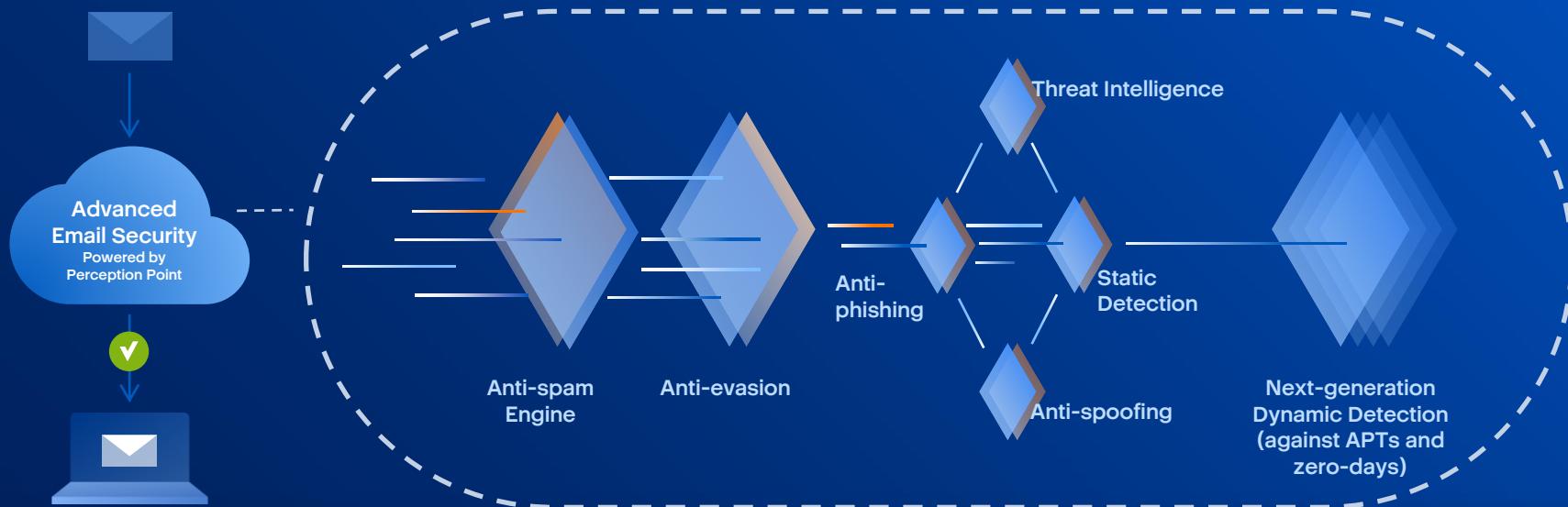
## Prevent APTs and zero-day attacks

Prevent advanced email threats that evade conventional defenses with Perception Point's unique CPU-level technology, which acts earlier in the attack chain to block exploits before malware is released, delivering a clear verdict within seconds.

\*Product UI supports English only

# Multi-layered protection

7 layers of protection against any email-borne threat



**Why?**

Block any email-borne threat before it reaches end-users

# Unmatched detection speed

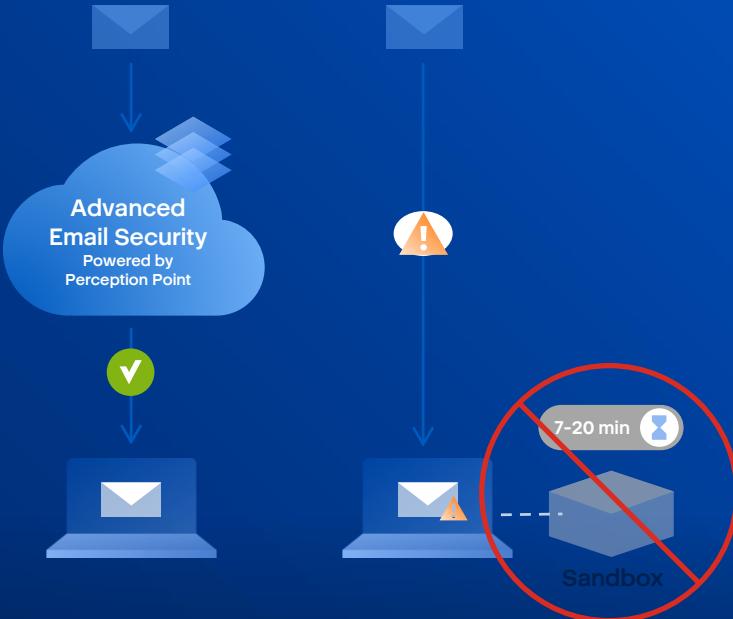
Get proactive and move from detection to prevention due near-zero delays

Legacy sandboxing technologies, are inherently slow: waiting to see how the malware acts, which leads to detection delays and forces CISOs to:

- Move their security solution to detection mode, with post-email delivery analysis
- Scan only a fraction of all incoming data, which leaves gaps in defenses, especially against unknown attack techniques

Moreover, Content Disarm and Reconstruction (CDR) solutions can make harm reconstructed content or make it unusable.

**Perception Point's technology shortens content scanning from up to 20 minutes to under 30 seconds, with no tampering of any kind**



# Enhance your Microsoft 365 native defenses

Excel where native Microsoft defenses fall short – prevent more threats and leverage lightning-fast detection

Functionality	Advanced Email Security (powered by Perception Point)	Microsoft 365
Detection speed	< 30 sec	5-20 mins
Detection accuracy	.....	•
Threat coverage	.....	...
URL scanning	.....	....
Detection of zero-days	.....	...
Prevention of APTs	.....	✗
Anti-evasion	.....	✗
Incident response services	.....	✗

# Section Summary



- Improve client security, by detecting any email-borne threat before it reaches end-users
- Block email threats – including spam, phishing, business email compromise (BEC), malware, advanced persistent threats (APTs), and zero-days – before they reach end-users' Microsoft 365, Google Workspace, Open-Xchange, or on-premises mailboxes. Leverage a next-gen cloud-based email security solution powered by Perception Point.



# Acronis

## Cyber Protect Cloud

### **Advanced Pack- File Sync and Share**

# Acronis Cyber Protect Cloud with Advanced File Sync and Share

Take full control over data location, management, and privacy with a superior file sync and share service extended with fully remote notarization, verification, and online signing



## Maximize productivity and collaboration

Support your clients' digital transformation with simple file and link sharing, controlled access with custom permissions, eSigning, and file notarization



## Mitigate security risks

Leverage a HIPAA-compliant file sync and share service with encryption at rest and in transit, full control over data location, and data authenticity powered by the Ethereum blockchain to record and verify notarizations



## Boost revenue growth

Increase client retention and generate new revenue streams by expanding your offering with an advanced file sync and share service that supports all platforms

# Fully remote file notarization

Provide confidence that business data is authentic

- Accelerate the pace of your client's business by digitizing their notarization processes
- Deter fraud and forgery: falsifying records or destroying entries to conceal malicious activity is not possible
- Eliminate the need to rely on a trusted third-party to guarantee immutability of records
- Elevate the credibility of a document
- Generate a time-stamped, blockchain-based certificate
- Prove data is original and unaltered



Reduce the cost and time necessary to notarize a file

# File Notarization: Step by step

1. Select an existing file you need to notarize directly from the file sync and share interface, or upload a new one
2. Click on the Notarize file button
3. Wait until the file is notarized or check the status: notarization in progress, notarization failed, current version - notarized
4. Receive a certificate when notarization process is finished

## Best for:

- Interdepartmental communication request forms
- Media (video, image, recordings, etc.)
- Power of attorney

The screenshot shows the Acronis Cyber Cloud interface. On the left, there is a file sync and share interface displaying a list of files including PDFs, Excel spreadsheets, Word documents, and various media files. A context menu is open over a file, with the 'Notarize File' option highlighted. On the right, a detailed view of a file's notarization status is shown. The file is a 16.00 MB PDF named '10m\_log\_signature\_certificate\_2021\_04\_05T07\_40\_48 (2).pdf'. The status bar indicates 'Notarization in progress' with a timestamp of '2021-04-26 04:31:34'. Below this, another file is listed as '20.00 MB' with a timestamp of '2021-04-28 19:38:06'. At the bottom of the interface, a QR code is visible.

Sync Type Name -

Status Size Modified Link

Download  
Revisions  
Rename  
Copy  
Move  
Email Link  
Get Link  
Notarize File

10m\_log\_signature\_certificate\_2021\_04\_05T07\_40\_48 (2).pdf  
16Mts  
1-2.0.5092867411010774-mm54.xls  
20.xlsx  
24.docx  
26MB.xlsx  
540c727f-843f-4034-aed1-aaa0stab00f6\_e\_b74.pdf  
AcronisFileAdvancedSetup.exe  
APDC.docx  
Bear.mp4  
BigDocument.docx  
bla.txt  
ConnectWiseControl\_Integration\_en-US (1).zip  
curl-7.74.0 (1).zip  
image

Acronis Cyber Cloud

**NOTARIZATION CERTIFICATE**

This is to certify that this dataset or file referred to hereunder was notarized at the date and time printed below, through the creation of a self-authenticating digital record using Ethereum blockchain technology.

File name: E-signature1 now.gif  
Notarization timestamp: 27 May, 2021 11:30 PM UTC +0800  
File size: 1.1 MB (1 145 476 bytes)  
File hash (SHA-256): 34412ca5e1080868a4059fcfc38dbf99e55894/d8c154bc8994c1a1205d22266  
Requestor: Lachumanan.customer  
Requestor GUID: 09eddbdb-653f-42e7-3a6c-cd4ec09899e  
Signer: Notary  
Transaction ID: 0x094481ec85ac5e2935a483a0fe1586f2b8037450tx.a8d165e94d04731e748

Notarization in progress  
Owner: vasilkalchevski89+205@gmail.com  
vasilkalchevski89+205@gmail.com

2021-04-26 04:31:34

2021-04-28 19:44:19

20.00 MB  
2021-04-28 19:38:06

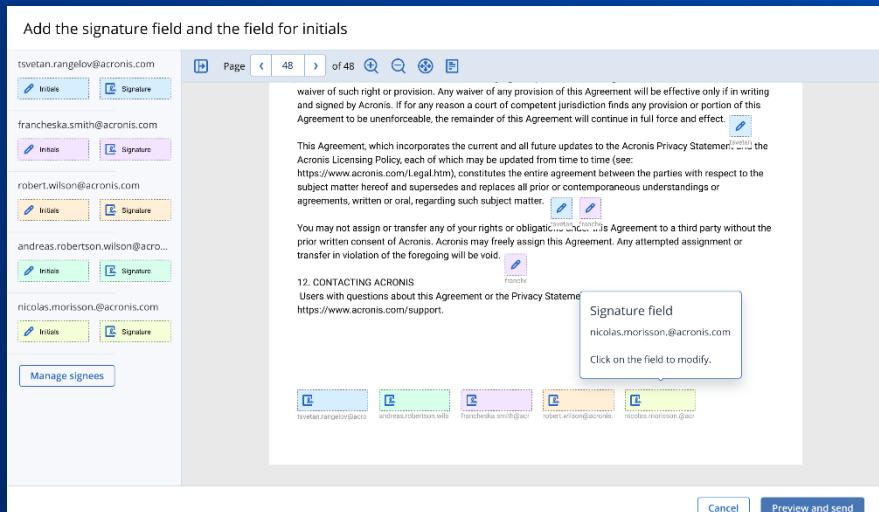
# Embedded eSigning

## Streamline and secure document workflows

- Turn data into decisions by enabling clients to quickly sign off on vital documents with an embedded eSignature
- Enable compliance with the relevant regulatory bodies
- Address privacy concerns with the most stringent global security standards and data encryption
- Generate a certificate to guarantee the signature's integrity
- Gain instant status visibility: always know where a file is in the signing process

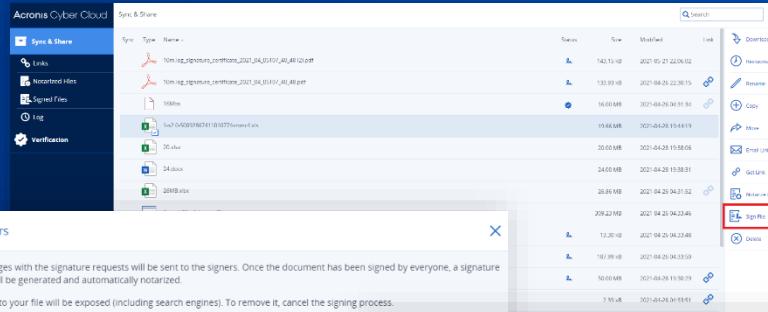


Why?  
Eliminate manual tasks, reduce errors, and increase convenience for your clients



# eSigning: Step by step

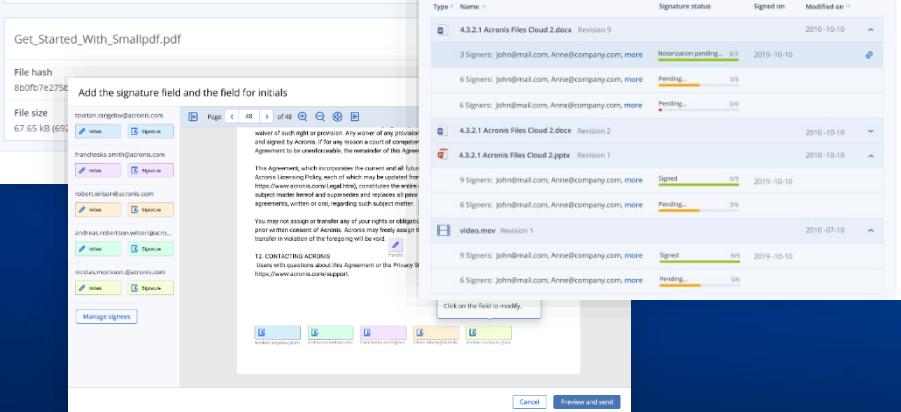
1. Select an existing file you need to eSign directly from the file sync and share interface, or upload a new one
2. Click on the Sign file button
3. Specify the signers by inserting their email addresses
4. All participants authenticate themselves, then sign the file online with embedded eSignatures
5. When all signatures are sent, the requestor receives a certificate, proving the integrity of the signatures
6. You can then get and email a link to an eSigned document



The screenshot shows the Acronis Cyber Cloud Sync & Share interface. On the left, there's a sidebar with options like Sync & Share, Links, Notarized files, Signed files, Tag, and Verification. The main area displays a list of files including '10m.log.signature\_centerhome\_2021\_04\_0101\_40\_40.pdf', '10m.log.signature\_centerhome\_2021\_04\_0101\_40\_40.pdf', '10m.pdf', 'Swf\_04/09/2018/31/1/1077/Smart.pdf', '20.xlsx', '24.docx', and '26MB.xlsx'. A red box highlights the 'Sign file' button in the toolbar on the right.


The screenshot shows the 'Add signers' dialog box. It has a list of email addresses: 'rangan.acronis@gmail.com', 'mancheksa.smith@acronis.com', 'robert.wilson@acronis.com', 'andreas.reichen@acronis.com', 'nicola.evans@acronis.com', and 'michael.jones@acronis.com'. Below the list is a 'Send invite to:' input field containing 'rangan.acronis@gmail.com'.

The screenshot shows the 'Signed files' interface. It lists several documents with their signature status:

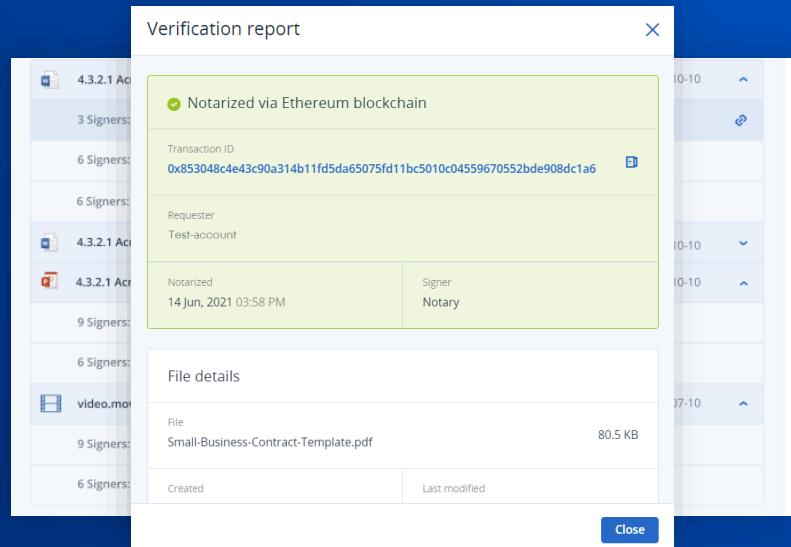
- 4.3.2.1 Acronis Files Cloud 2.docx: Revision 9, 3 Signers: john@mail.com, Anne@company.com, more, Notarization pending, 3/3
- 4.3.2.1 Acronis Files Cloud 2.Zdoc: Revision 2, 6 Signers: john@mail.com, Anne@company.com, more, Pending, 3/6
- 4.3.2.1 Acronis Files Cloud 2.xlsx: Revision 1, 6 Signers: john@mail.com, Anne@company.com, more, Pending, 3/6
- video.mov: Revision 1, 9 Signers: john@mail.com, Anne@company.com, more, Signed, 9/9
- video.mov: Revision 1, 6 Signers: john@mail.com, Anne@company.com, more, Pending, 3/6

At the bottom, there's a large button labeled 'Click on the field to modify...' with a red box around it, and a 'Cancel' and 'Preview and send' button.

# Auditing and file verification

## Enable trusted and independent file verification

- Empower your clients with an enterprise-class audit trail, including a history of all transactions
- Drastically reduce the cost and time necessary to conduct an audit
- Verify that a document is unchanged, or confirm that it's been changed, by leveraging the Ethereum blockchain
- Integrate the data verification process within notarization and eSignature



### Why?

Automate the process with conclusive verification. No intermediary needed.

# File verification: Step by step

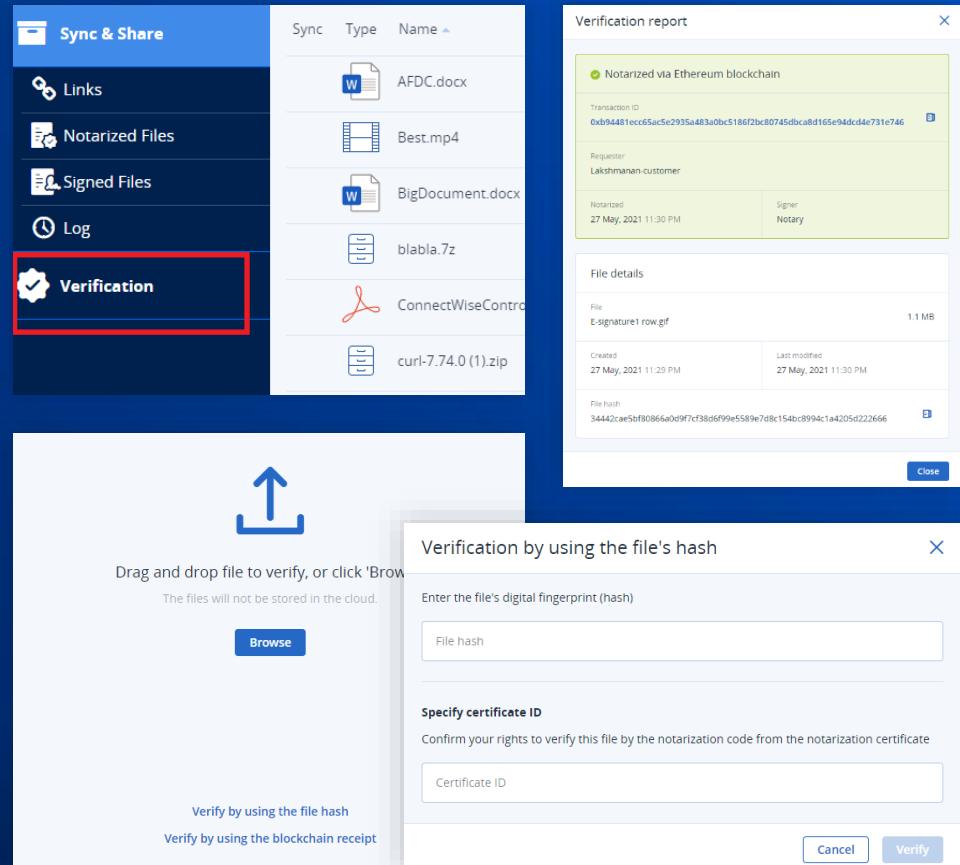
After a file is notarized, signed or both, clients can verify it at any time. Two options are possible:

## 1. File verification directly from the file sync and share interface:

- Select an existing file you need to verify or upload a new one
- Check the status of the document

## 2. File verification through the blockchain ledger:

- Copy the Transaction ID from the notarization certificate
- Paste it here:  
<https://ropsten.etherscan.io/>



The screenshot displays three windows related to file verification:

- Main Interface:** Shows a sidebar with "Sync & Share" and links for "Links", "Notarized Files", "Signed Files", "Log", and "Verification". The "Verification" link is highlighted with a red box.
- Verification Dialog:** A modal window titled "Verification by using the file's hash" contains a large blue upload icon and the text "Drag and drop file to verify, or click 'Browse'". Below this, it says "The files will not be stored in the cloud." and has a "Browse" button.
- Verification Report:** A separate window titled "Verification report" shows a summary of a notarized file. It includes:
  - Notarized via Ethereum blockchain**
  - Transaction ID:** 0xb94481ecc65ac5e2935a483a0bc5186f2bc80745dbc8d165e94dc4e731e746
  - Requester:** Lakshmanan-customer
  - Notarized:** 27 May, 2021 11:30 PM
  - Signer:** NotaryIt also shows "File details" for a file named "E-signature1 row.gif" with a size of 1.1 MB, created on 27 May, 2021 11:29 PM, last modified on 27 May, 2021 11:30 PM, and a file hash of 34442cae5bf80866a0df97cf38d6f99e5589e7d8c154b:8994c1a4205d222666.

# Drive transformation across industries

## Healthcare



- Share patient documents and records **without violating any regulations**
- **Access medical records from a mobile device** and make any needed changes while on the go
- **Notarize and electronically sign** patient onboarding processes, patient intake forms, billing and consent documents

## Education



- **Meet regulatory requirements** with secure cloud storage, and complete audit trails that show who accessed which records and when
- **Automate the processes** of handling administrative documents
- **Get student and other contracts eSigned** quickly and effortlessly
- Confirm that **a creative work originated** on a certain date

## Financial services



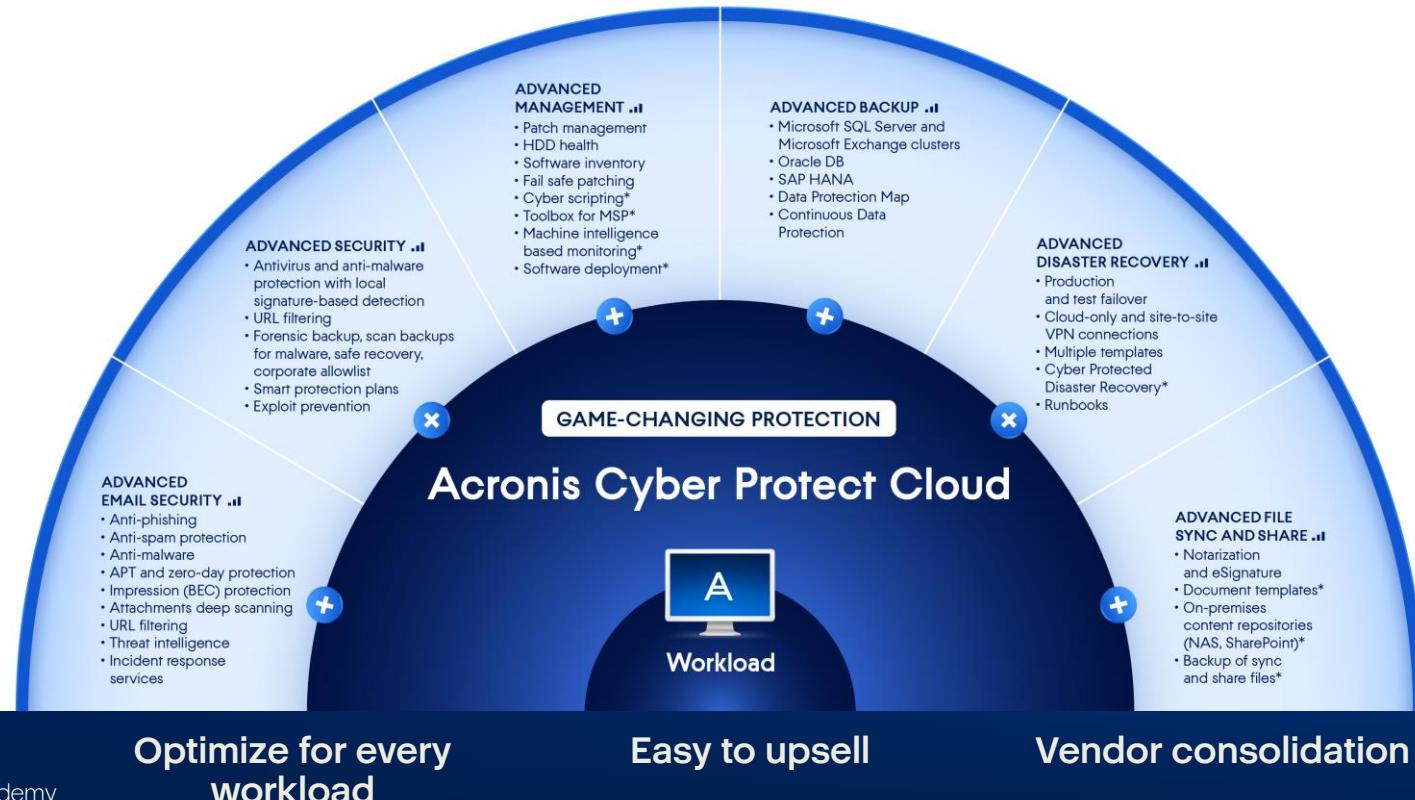
- **Monitor and report** on content access, permissions, and sensitive data like customer information, financial assets, and PII
- Manage content lifecycle through **retention policies**
- **Securely capture eSignatures** for account openings, consumer loans, internal approvals, employee policy agreements, etc.

# Section Summary



- Advanced File Sync and Share offer secure collaboration services with imbedded data authenticity
- Improve the collaboration and productivity of your clients' teams. The Advanced File Sync and Share pack extends Acronis Cyber Protect Cloud's integrated secure file-sharing capabilities with fully remote notarization, verification, and electronic signing. Ensure data authenticity and reduce fraud by layering advanced features on top of the essential, pay-as-you-go service.
- Ensure the integrity of business-critical data .Take full control over data location, management, and privacy with a superior file sync and share service. Includes a transaction ledger to enable notarization and eSigning capabilities, and supports all platforms.

# Add Advanced packs: Email Security, Security, Management, Backup, Disaster Recovery, File Sync and Share



# Acronis Cyber Protect Cloud with Advanced Email Security powered by



Improve client security by detecting any email-borne threat before it reaches end-users



## Stop phishing and spoofing attempts

Minimize client risks with powerful threat intelligence, signature-based detection, URL reputation checks, unique image-recognition algorithms, and machine learning with DMARC, DKIM, and SPF record checks.



## Catch advanced evasion techniques

Detect hidden malicious content by recursively unpacking embedded files and URLs and separately analyzing them with dynamic and static detection engines.



## Prevent APTs and zero-day attacks

Prevent advanced email threats that evade conventional defenses with Perception Point's unique CPU-level technology, which acts earlier in the attack chain to block exploits before malware is released, delivering a clear verdict within seconds.

# Acronis Cyber Protect Cloud with Advanced Security

Improve security by detecting more threats, save on simplified security management, and deliver better remediation with integrated cyber protection



## Full-stack antimalware

Acronis Active Protection, enhanced with exploit prevention, URL filtering, antimalware detection for backed-up data, and improved detection rate to catch more threats faster



## Security automation

Smart protection plans, auto-allowlist custom apps, automatic malware scans and AV definitions updates as part of recovery process to deliver services more effortlessly



## Efficient forensics

Collect digital evidence and safe it in a secure central repository to enable thorough post-incident investigations and proper remediation, while keeping costs down.

# Acronis Cyber Protect Cloud with Advanced Management

Improve clients' protection by keeping systems up-to-date  
while decreasing the management burden and TCO



## Advanced patch management

Keep systems up-to-date and proactively mitigate vulnerabilities.



## Patch management automation

Save time and effort with patch management automation and fail-safe patching technology



## Comprehensive management tools

Streamline your planning with software inventory collection, report scheduling, and drive health monitoring.

# Acronis Cyber Protect Cloud with Advanced Backup

Protect your clients' data confidently with best-in-breed backup  
enhanced with cyber protection



## Increase automation and productivity

Scheduled backup reports, paired with cloud backup enhancements – like continuous data protection – helps you save time while saving your clients from data loss



## Deliver the most secure backup

Acronis delivers a unique approach by combining cloud backup with cyber protection features, such as antimalware and antivirus – helping you keep clients' data secure



## Protect more workloads on more platforms

From a single console, protect more than 20 workload types, including Microsoft Exchange, Microsoft SQL Server, Oracle DBMS Real Application clusters, and SAP HANA

# Acronis Cyber Protect Cloud with Advanced Disaster Recovery

Protect clients with the flip of a switch



## Less downtime

Get clients running in mere minutes by spinning up IT systems in the Acronis cloud with full site-to-site connectivity and the ability to recover them to similar or dissimilar hardware



## Minimize complexity

No need to add, learn, or manage another platform. It's one solution for any workload managed from a single interface that enables you to build a complete cyber protection service



## Grow recurring revenue

Deliver more value, deepen client relationships, and increase retention by offering clients the disaster recovery services they are looking for – while increasing your monthly recurring revenue

# Acronis

## Understand Acronis Cyber Protect Cloud

### Introducing Cloud Services



# Section Modules - Part 2



1. Components & Deployments
2. Storing Data
3. Acronis Cyber Protect Cloud 3rd Party Integrations
4. Navigating the Web Interface

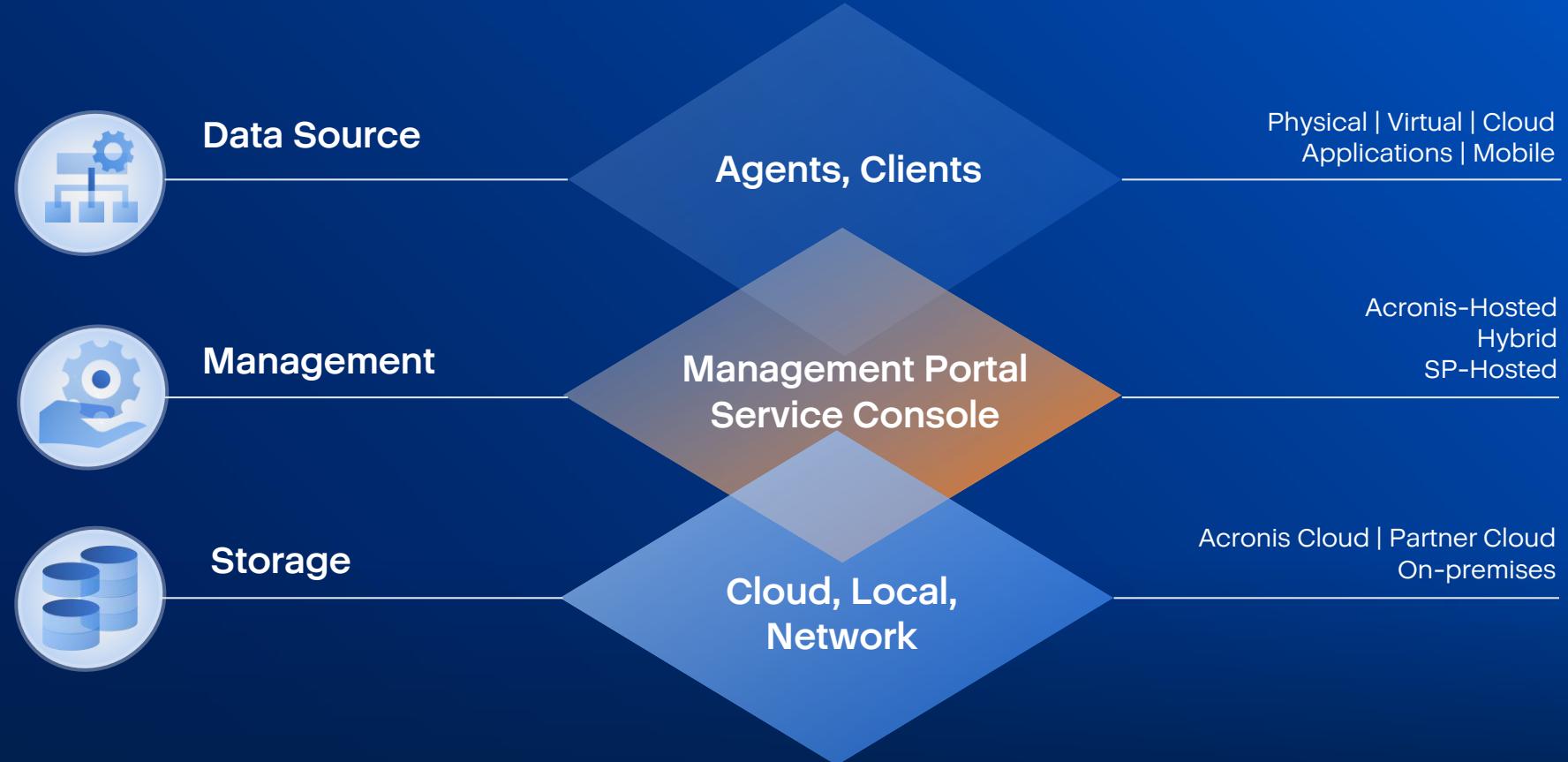
# Acronis

## Understand Cyber Protect Cloud

### **Software Components and Types of Deployments**



# 3-Tier Architecture



# Cyber Protect Cloud Components

## Data Source

Install on devices to be protected

- Agent for Windows
- Agent for Linux
- Agent for Mac
- Agent for VMware (Virtual Appliance)
- Agent for VMware (Windows)
- Agent for Hyper-V
- Agent for Virtuozzo
- Agent for Office 365
- Agent for Exchange
- Agent for SQL
- Agent for Active Directory
- Agent for Oracle
- Cyber Protect iOS app
- Cyber Protect Android app

## Management

For managing tenants and the service

- Management Portal
- Cyber Protection service console

## Storage

Where can data be stored

- Local folder
- Network folder – SMB or NFS shares
- Acronis Cloud Storage
- Service Provider Cloud Storage



# Cyber Protect Cloud Components

## Ancillary

Components to enable additional functionality

- Bootable media
- Cyber Protection monitor
- Command-line tool
- Acronis SharePoint Explorer



# Cyber Files Components

## Data Source

Install on devices to enable file sync & share

### For mobile devices

- Cyber Files Cloud iOS app
- Cyber Files Cloud Android app
- Web browser

### For desktops

- Cyber Files Cloud PC client
- Cyber Files Cloud Mac client
- Web browser

## Management

For managing tenants and the service

- Management Portal
- Cyber Files service console

## Storage

Where can data be stored

- Local folder
- Acronis Cloud Storage
- Service Provider Cloud Storage



# Cyber Notary Components

## Data Source

Install on devices to enable file notarization and e-signature

- Web browser

## Management

For managing tenants and services

- Management Portal
- Cyber Notary service console

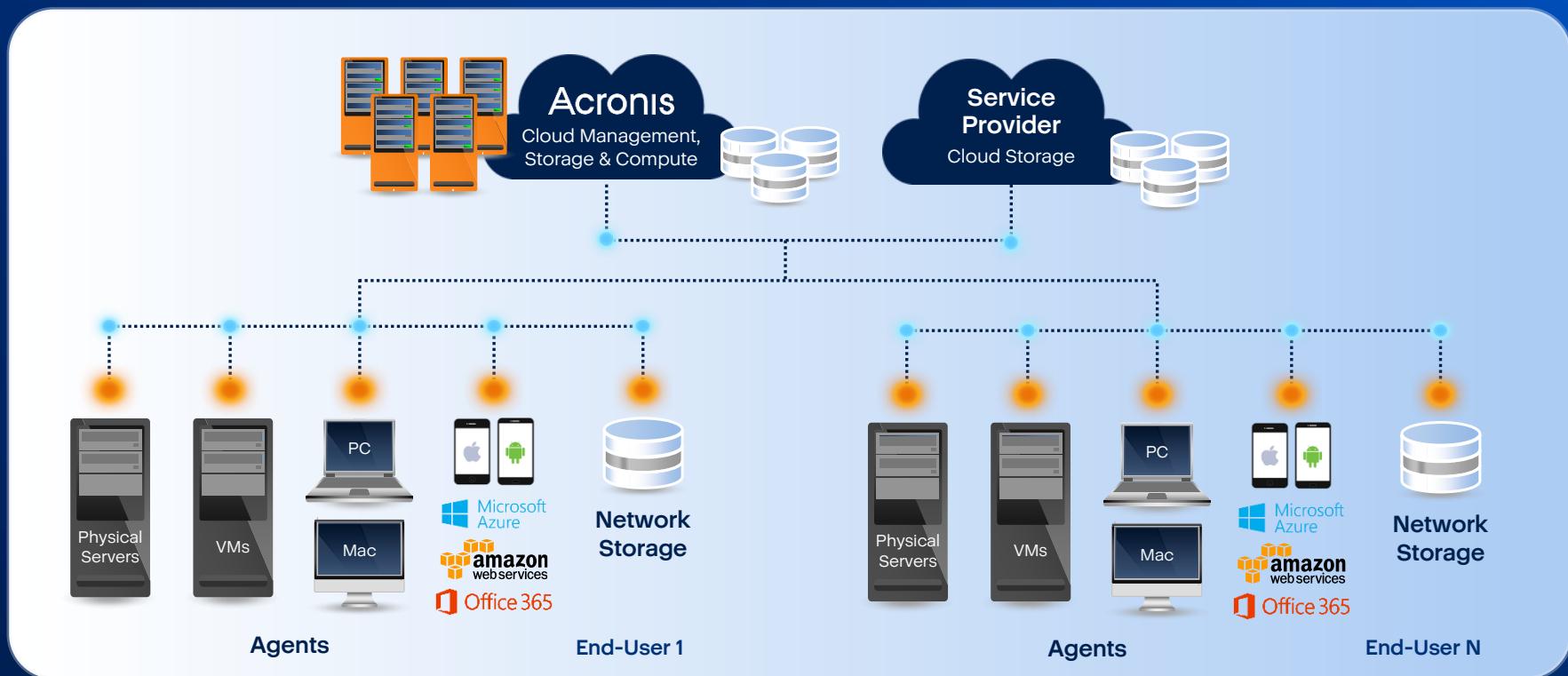
## Storage

Where can data be stored

- Acronis Cloud



# Cyber Protect Cloud Deployment



# Section Summary



- Acronis Cyber Protect Cloud has 3 levels of the system- Data Sources, Management Console and Storage
- As an Agent based system, each workload will need to download and install an agent to the target.
- There are additional downloadable components depending on the circumstance

# Acronis

## Understand Cyber Protect Cloud Supported Storage Locations



# Storage Locations

Location	Backups	Synced Files Acronis Cyber Files Cloud	Notarized & E-Signature Files Acronis Cyber Notary Cloud
Cloud Storage	Acronis cloud storage & Service Provider cloud storage	Acronis cloud storage & Service Provider cloud storage	Acronis cloud storage only
Local folder	Internal or external drive	Internal drive <sup>1</sup>	NA <sup>2</sup>
Network folder	SMB/CIFS shares & NFS folders (Linux and Mac OS X only)	NA	NA
Acronis Secure Zone	Secure partition on local disk	NA	NA

Files can be synced from and to local folders

<sup>2</sup> Files to be notarized or for e-signatures can be uploaded to Acronis cloud from local folders

# Supported File Systems For Backup & Recovery

File System <sup>1</sup>	Supported By				Limitations of File System
	Agents	Linux-based bootable media	Win-PE based bootable media	Mac	
FAT16/32	All agents	✓	✓	✓	– No limitations – For APFS, disk configuration should be re-created manually when recovering to a non-original machine or bare-metal
NTFS		✓	✓	✓	
ext2/ext3/ext4		✓	✓		
HFS+/APFS	Agent for Mac			✓	– Files cannot be excluded from a disk backup
JFS	Agent for Linux	✓	✓		
ResierFS3		✓	✓		
ResierFS4		✓	✓		– Files cannot be excluded from a disk backup – Volumes cannot be resized during a recovery
ReFS	All Agents	✓	✓	✓	
XFS		✓	✓	✓	
Linux Swap	Agent for Linux	✓	✓		– No limitations

# Hyperscale Cloud Storage

Cloud Storage	Geography	Region	Location
Google Cloud Platform  Google Cloud Platform	Americas	northamerica-northeast1	Montreal, Canada
	Americas	us-west1	The Dallas, OR USA
	Europe	europe-west2	London, UK
Microsoft Azure  Azure	Americas	US-Central	Iowa
	Europe	EU-North	Dublin

# Service Provider Cloud Storage

## Acronis Cyber Infrastructure

- Enables software-defined storage, compute and networking on industry-standard hardware
- Cloud storage for storing backups from Cyber Protect Cloud is **free-of-charge**
- Use of compute (virtualization) and software-defined networking (SDN) functionality-**free-of-charge**

## Hybrid deployment model



# Section Summary



- Acronis supports a wide range of storage locations for data
- Service providers can use either the Acronis Cloud or their own cloud as a storage location
- Reference the File Systems cheatsheet when presented with an unusual configuration to see what is supported

# Acronis

## Understand Cyber Protect Cloud

### **3rd Party Integrations – Supported RMM and PSA Tools**



# Integration via RESTful API and APS

## Acronis Cyber Protect Cloud

- Supports automation integration via packages and plugins for various management platforms
- Integration packages and plugins are based on either **RESTful API or APS** (Application Packaging Standard)
- Operations possible include but are not limited to:
  - Selling customized services
  - Automating billing



# Supported Platforms

Odin



APS STANDARD

RESTful API  
GET PUT POST DELETE

plesk

**Autotask®**

**cPanel**



**flexiant™**  
your cloud simplified

**HostBill**

 **iPortalis**



**resello**



**Windows Azure Pack™**



**WHMCS**



**C**onnectWise  
**AUTOMATE™**  
formerly **LabTech**



**C**onnectWise  
**MANAGE™**



**i**nterworks.**cloud**

# Section Summary



- Acronis Cyber Protect Cloud supports automation integration via packages and plugins for various management platforms
- Integration via RESTful API and APS
- Over 15 supported Platforms such as Odin, Autotask, APSStandard, Windows Azure Pack
- Variety of operations possible such as:
  - Selling customized services
  - Automating billing

# Acronis

## Understand Cyber Protect Cloud

### Navigating the Web Interface



# Services & Management Portal Selector

My services

AD Customer 1 (ad.cust1)

Customer 1

Cyber Protection

Physical Data Shipping

File Sync & Share

Notary

Management Portal

# Services & Management Portal Selector

The screenshot shows a user interface for selecting services. At the top left is a dark blue header bar with the text "My services" on the left and "AD Customer 1 (ad.cust1)" on the right. On the far right of the header is a small icon with a double arrow. Below the header is a light gray main area. In the center, there is a white rectangular box labeled "Customer 1". Inside this box are five service icons arranged horizontally:

- Cyber Protection (Icon: two overlapping squares)
- Physical Data Shipping (Icon: truck)
- File Sync & Share (Icon: circular arrows)
- Notary (Icon: checkmark inside a circle)
- Management Portal (Icon: document with a grid)

Below each icon is its corresponding service name. To the right of the "Customer 1" box is a green callout box with the text "Services & Management Portal Selector" in white. An arrow points from the top edge of the green box down towards the "Management Portal" icon.

# Management Portal

~Service Provider

+ New ? !

**OVERVIEW** Cyber Protect Cyber Infrastructure ⚙️

**CLIENTS** Protection File Sync & Share Physical Data Shipping Notary ⚙️

Name <span>↑</span>	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup		
					No Data	<span>Cloud</span>	<span>Upload</span>	<span>Sync</span>	<span>Backup</span>
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB	0 GB	0	0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	No Data	0 GB	0 GB	0	0 GB
Partner 1	...	Active	Per workload, Per gigabyte	Disabled	By service provider	No Data	0 GB	0 GB	0 GB

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

# Management Portal

The screenshot shows the Acronis Cyber Cloud Management Portal interface. At the top, there is a breadcrumb navigation bar with the path: ~Service Provider > Breadcrumb. The main content area is titled "Protection" and displays a table of clients. The table columns include Name, Tenant status, Billing mode, 2FA status, Management mode, 7-day history, Totals, and Local backup. The data in the table is as follows:

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB	0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	-	0 GB	0 GB
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider	-	0 GB	0 GB

On the left side, there is a vertical sidebar with navigation links: Overview, Clients, Users, Reports, Audit Log, and Settings. The "Clients" link is currently selected. At the bottom of the sidebar, it says "Powered by Acronis AnyData Engine".

# Management Portal

~Service Provider

**Add New, Search, Help, Account Settings**

+ New    Q    ?    @

**OVERVIEW**

Cyber Protect    Cyber Infrastructure

**CLIENTS**

Protection    File Sync & Share    Physical Data Shipping    Notary

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB	0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	-	0 GB	0 GB
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider	-	0 GB	0 GB

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

# Management Portal

The screenshot shows the Acronis Cyber Cloud Management Portal interface. The top navigation bar includes a user icon (~Service Provider), a search bar, and buttons for '+ New', '?', and '@'. The left sidebar has icons for Overview, Clients, Users, Reports, Audit Log, and Settings. The main content area is titled 'Cyber Protect' and shows tabs for Protection, File Sync & Share, Physical Data Shipping, and Notary. A green callout box with the text 'Switch between Services' points to the tabs. Below the tabs is a table with columns: Name, Tenant status, Billing mode, 2FA status, Management mode, 7-day history, Totals, and Local backup. The table lists three entries: Customer 1 (Active, Per workload, Disabled, By service provider, No Data, 0 GB, 0 GB, 0, 0 GB), Group 1 (Active, Per workload, Per gigabyte, -, -, 0 GB, 0 GB, 0, 0 GB), and Partner 1 (Active, Per workload, Per gigabyte, Disabled, By service provider, 0 GB, 0 GB, 0, 0 GB). The bottom of the page features the text 'Acronis Cyber Cloud' and 'Powered by Acronis AnyData Engine'.

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB	0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	-	0 GB	0 GB
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider	-	0 GB	0 GB

# Management Portal

~Service Provider

+ New ? !

**OVERVIEW** Cyber Protect Cyber Infrastructure

**CLIENTS** Protection File Sync & Share Physical Data Shipping Notary

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Show more columns ⋮

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup
					No Data	0 GB	0 GB
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB	0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	No Data	0 GB	0 GB
Partner 1	...	Per workload, Per gigabyte	Disabled	By service provider	No Data	0 GB	0 GB

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

# Management Portal

The screenshot shows the Acronis Cyber Cloud Management Portal interface. On the left is a vertical sidebar with icons for Overview, Clients (selected), Users, Reports, Audit Log, and Settings. The main content area has a header with tabs: Cyber Protect, Cyber Infrastructure, and a search bar with '+ New', a magnifying glass, a question mark, and a user icon. Below the header is a sub-header with Protection, File Sync & Share, Physical Data Shipping, and Notary. The main table displays client information:

Name	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup
Customer 1	Per workload	Disabled	By service provider	No Data	0 GB 0 GB 0	0 GB
Group 1	Per workload, Per gigabyte	-	-	-	0 GB 0 GB 0	0 GB
Partner 1	Per workload, Per gigabyte	Disabled	By service provider	-	0 GB 0 GB 0	0 GB

A green box highlights the 'Clients' tab in the sidebar and the 'Protection' tab in the sub-header. An arrow points from the text 'Tabs/Menus' to the 'Clients' tab. The bottom of the page features the text 'Acronis Cyber Cloud' and 'Powered by Acronis AnyData Engine'.

# Management Portal

The screenshot shows the Acronis Cyber Cloud Management Portal interface. The top navigation bar includes a user icon (~Service Provider), a search bar, and buttons for '+ New', '?', and '@'. The left sidebar has icons for Overview, Clients, Users, Reports, Audit Log, and Settings. The main content area has tabs for Cyber Protect and Cyber Infrastructure, with Cyber Protect selected. Below these are sub-tabs: Protection, File Sync & Share, Physical Data Shipping, and Notary. The main table lists tenants with columns for Name, Tenant status, Billing mode, 2FA status, Management mode, 7-day history, Totals, and Local backup. Three tenants are listed: Customer 1 (Active, Per workload, Disabled, By service provider, No Data, 0 GB, 0 GB, 0, 0 GB), Group 1 (Active, Per workload, Per gigabyte, -, -, 0 GB, 0 GB, 0, 0 GB), and Partner 1 (Active, Per workload, Per gigabyte, Disabled, By service provider, 0 GB, 0 GB, 0, 0 GB). A green callout box labeled 'List of Tenants' points to the tenant list table.

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB	0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	-	0 GB	0 GB
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider	-	0 GB	0 GB

Acronis Cyber Cloud  
Powered by Acronis AnyData Engine

List of Tenants

# Cyber Protection Service Console

Acronis Cyber Cloud

Manage account

DASHBOARD (27)

DEVICES

All devices

Machines with agents

VMware

Hyper-V

AD Cloud Tech 19-APR-2021

Unmanaged machines

Data protection map

PLANS

DISASTER RECOVERY

Powered by Acronis AnyData Engine

## All devices

+ Add ≡ grid ? refresh

Selected: 1 / Loaded: 10 / Total: 10 View: Standard

Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup	Plan	Actions
Host	192.168.217.171	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>#CyberFit Score</span>
VM	192.168.217.171-VA-F179	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>Protect</span>
Host	Skylake	Amos Dong (ad.tech)	625/850	Not protected	Never	Not scheduled		<span>Disaster recovery</span>
VM	VM Replica	Amos Dong (ad.tech)	Not supported	Activity failed	Never	Not scheduled	Replicate to 192.168.2...	<span>Recovery</span>
Host	Win10 Ent 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>Cyber Protection Desktop</span>
VM	WIN10ENT02	Amos Dong (ad.tech)	625/850	OK	May 04 03:13:32 PM	Not scheduled	Backup Desktop 2; Bac...	<span>Patch</span>
VM	WIN2K19DC01	Amos Dong (ad.tech)	625/850	OK	May 04 01:48:08 PM	Not scheduled	Backup Server 1 to Clo...	<span>Details</span>
Host	Win2k19 DC 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>Inventory</span>
VM	WIN2K19DC02	Amos Dong (ad.tech)	625/850	Suspicious activity ...	Apr 19 09:45:16 AM	Not scheduled	Backup Server 2 to Sh...	<span>Activities</span>
Host	Win2k19 DC 02	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>Alerts</span>

Add to group

# Cyber Protection Service Console

Acronis Cyber Cloud

Manage account

DASHBOARD

DEVICES

All devices

Machines with agents

VMware

Hyper-V

AD Cloud Tech 19-APR-2021

Unmanaged machines

Data protection map

PLANS

DISASTER RECOVERY

Powered by Acronis AnyData Engine

All devices

Search

Add Agents, Switch View, Switch Consoles, Help, Account

+ Add

Selected: 1 / Loaded: 10 / Total: 10 View: Standard

Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup	Plan	Actions
PC	192.168.217.171	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		#CyberFit Score
VM	192.168.217.171-VA-F179	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Protect
PC	Skylake	Amos Dong (ad.tech)	625/850	Not protected	Never	Not scheduled		Disaster recovery
VM	VM Replica	Amos Dong (ad.tech)	Not supported	Activity failed	Never	Not scheduled	Replicate to 192.168.2...	Recovery
VM	Win10 Ent 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Cyber Protection Desktop
VM	WIN10ENT02	Amos Dong (ad.tech)	625/850	OK	May 04 03:13:32 PM	Not scheduled	Backup Desktop 2; Bac...	Patch
VM	WIN2K19DC01	Amos Dong (ad.tech)	625/850	OK	May 04 01:48:08 PM	Not scheduled	Backup Server 1 to Clo...	Details
VM	Win2k19 DC 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Inventory
VM	WIN2K19DC02	Amos Dong (ad.tech)	625/850	Suspicious activity ...	Apr 19 09:45:16 AM	Not scheduled	Backup Server 2 to Sh...	Activities
VM	Win2k19 DC 02	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Alerts

Add to group

# Cyber Protection Service Console

Acronis Cyber Cloud

Manage account

DASHBOARD

DEVICES

All devices

Machines with agents

VMware

Hyper-V

AD Cloud Tech 19-APR-2021

Unmanaged machines

Data protection map

PLANS

DISASTER RECOVERY

Powered by Acronis AnyData Engine

### All devices

Search box

Selected: 1 / Loaded: 10 / Total: 10 View: Standard

Type	Name	Owner	CyberFit Score	Status	Last backup	Next backup	Plan	Actions
Host	192.168.217.171	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		#CyberFit Score
VM	192.168.217.171-VA-F179	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Protect
Host	Skylake	Amos Dong (ad.tech)	625/850	Not protected	Never	Not scheduled		Disaster recovery
VM	VM Replica	Amos Dong (ad.tech)	Not supported	Activity failed	Never	Not scheduled	Replicate to 192.168.2...	Recovery
Host	Win10 Ent 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Cyber Protection Desktop
VM	WIN10ENT02	Amos Dong (ad.tech)	625/850	OK	May 04 03:13:32 PM	Not scheduled	Backup Desktop 2; Bac...	Patch
VM	WIN2K19DC01	Amos Dong (ad.tech)	625/850	OK	May 04 01:48:08 PM	Not scheduled	Backup Server 1 to Clo...	Details
Host	Win2k19 DC 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Inventory
VM	WIN2K19DC02	Amos Dong (ad.tech)	625/850	Suspicious activity ...	Apr 19 09:45:16 AM	Not scheduled	Backup Server 2 to Sh...	Activities
Host	Win2k19 DC 02	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Alerts

+ Add    grid icon    list icon    help icon    refresh icon

Add to group

# Cyber Protection Service Console

Acronis Cyber Cloud

Manage account

DASHBOARD

DEVICES

All devices

Machines with agents

VMware

Hyper-V

AD Cloud Tech 19-APR-2021

Unmanaged machines

Data protection map

PLANS

DISASTER RECOVERY

Powered by Acronis AnyData Engine

All devices

+ Add

Actions

Search

Type Name ↑ Account #CyberFit Score Status Last backup Next backup Plan Actions

Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup	Plan	Actions
Host	192.168.217.171	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		#CyberFit Score
VM	192.168.217.171-VA-F179	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Protect
Host	Skylake	Amos Dong (ad.tech)	625/850	Not protected	Never	Not scheduled		Disaster recovery
VM	VM Replica	Amos Dong (ad.tech)	Not supported	Activity failed	Never	Not scheduled	Replicate to 192.168.2...	Recovery
Host	W	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Cyber Protection Desktop
VM	W	Amos Dong (ad.tech)	625/850	OK	May 04 03:13:32 PM	Not scheduled	Backup Desktop 2; Bac...	Patch
VM	WIN2K19DC01	Amos Dong (ad.tech)	625/850	OK	May 04 01:48:08 PM	Not scheduled	Backup Server 1 to Clo...	Details
Host	Win2k19 DC 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Inventory
VM	WIN2K19DC02	Amos Dong (ad.tech)	625/850	Suspicious activity ...	Apr 19 09:45:16 AM	Not scheduled	Backup Server 2 to Sh...	Activities
Host	Win2k19 DC 02	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		Alerts

Main Menus

Add to group

# Cyber Protection Service Console

Acronis Cyber Cloud

- Manage account
- DASHBOARD
- DEVICES
- All devices
- Machines with agents
- VMware
- Hyper-V
- AD Cloud Tech 19-APR-2021
- Unmanaged machines
- Data protection map
- PLANS
- DISASTER RECOVERY

Powered by Acronis AnyData Engine

## All devices

+ Add    ≡    grid    ?    ?

Selected: 1 / Loaded: 10 / Total: 10   View: Standard

Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup	Plan	Actions
PC	192.168.217.171	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>#CyberFit Score</span>
VM	192.168.217.171-VA-F179	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>Protect</span>
PC	Skylake	Amos Dong (ad.tech)	625/850	Not protected	Never	Not scheduled		<span>Disaster recovery</span>
VM	VM Replica	Amos Dong (ad.tech)	Not supported	Activity failed	Never	Not scheduled	Replicate to 192.168.2...	<span>Recovery</span>
VM	Win10 Ent 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>Cyber Protection Desktop</span>
VM	WIN10ENT02	Amos Dong (ad.tech)	625/850	OK	May 04 03:13:32 PM	Not scheduled	Backup Desktop 2; Bac...	<span>Patch</span>
VM	WIN2K19DC01	Amos Dong (ad.tech)	625/850	OK	May 04 01:48:08 PM	Not scheduled	Backup Server 1 to Clo...	<span>Details</span>
VM	Win2k19 DC 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		<span>Inventory</span>
VM	WIN2K19DC02	Amos Dong (ad.tech)	625/850	Suspicious activity ...	Apr 19 09:45:16 AM	Not scheduled	Backup Server 2 to Sh...	<span>Activities</span>
VM	Win2k19 DC 02	Amos Dong (ad.tech)				Not scheduled		<span>Alerts</span>

Selected machine

# Cyber Protection Service Console

Acronis Cyber Cloud

Manage account

DASHBOARD

DEVICES

All devices

Machines with agents

VMware

Hyper-V

AD Cloud Tech 19-APR-2021

Unmanaged machines

Data protection map

PLANS

DISASTER RECOVERY

Powered by Acronis AnyData Engine

All devices

+ Add

Selected: 1 / Loaded: 10 / Total: 10 View: Standard

Actions

#CyberFit Score

Protect

Disaster recovery

Recovery

Cyber Protection Desktop

Patch

Details

Inventory

Activities

Alerts

Add to group

Actions available for selected machine

Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup	Plan	Actions
Host	192.168.217.171	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		
VM	192.168.217.171-VA-F179	Amos Dong (ad.tech)	Not supported	Activity failed	Never	Not scheduled	Replicate to 192.168.2...	
Host	Skylake	Amos Dong (ad.tech)	625/850	Not protected	Never	Not scheduled		
VM	VM Replica	Amos Dong (ad.tech)	Not supported	Activity failed	Never	Not scheduled		
Host	Win10 Ent 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		
VM	WIN10ENT02	Amos Dong (ad.tech)	625/850	OK	May 04 03:13:32 PM	Not scheduled	Backup Desktop 2; Bac...	
VM	WIN2K19DC01	Amos Dong (ad.tech)	625/850	OK	May 04 01:48:08 PM	Not scheduled	Backup Server 1 to Clo...	
Host	Win2k19 DC 01	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		
VM	WIN2K19DC02	Amos Dong (ad.tech)	625/850	Suspicious activity ...	Apr 19 09:45:16 AM	Not scheduled	Backup Server 2 to Sh...	
Host	Win2k19 DC 02	Amos Dong (ad.tech)	Not supported	Not protected	Never	Not scheduled		

# File Sync & Share Administration Mode

The screenshot shows the 'File Sync & Share' administration interface. The left sidebar has a dark theme with white icons and text. The 'Sync & Share' section is selected, showing sub-options: General Restrictions, Sharing Restrictions, File Purging Policies, User Expiration Policies, Audit Log, Devices, and General Settings. The main content area is titled 'General Restrictions' and contains the following information:

These restrictions apply to the usage of Sync & Share storage for all internal and external users

Maximum allowed file size 1024 MB

Blacklisted file types

Specify file types not allowed, by file extension (e.g. mp3, exe).

A list box for file extensions is shown with a '+' Add button and a '-' Remove button. The list box is currently empty.

**Save**

# File Sync & Share Administration Mode

The screenshot shows the 'File Sync & Share' administration interface. On the left, a sidebar lists various settings: Sync & Share, General Restrictions (selected), Sharing Restrictions, File Purging Policies, User Expiration Policies, Audit Log, Devices, and General Settings. The main pane is titled 'General Restrictions' and contains the following sections:

- Maximum allowed file size:** A field set to 1024 MB.
- Blacklisted file types:** A section with a text input placeholder 'Specify file types not allowed, by file extension (e.g. mp3, exe).'. Below it is a list area with a '+' Add button and a '-' Remove button.

A large green arrow points from the bottom right towards the bottom center of the main pane, indicating the 'Settings Pane'.

# File Sync & Share Administration Mode

The screenshot shows the 'File Sync & Share' administration interface. On the left, a sidebar menu lists several options: 'Sync & Share', 'General Restrictions' (which is currently selected), 'Sharing Restrictions', 'File Purging Policies', 'User Expiration Policies', 'Audit Log', 'Devices', and 'General Settings'. A green callout box labeled 'Tabs/Menus' points to the sidebar area. The main content area is titled 'General Restrictions' and contains a sub-section titled 'Blacklisted file types' with a note: 'Specify file types not allowed, by file extension (e.g. mp3, exe)'. It features a list input field with a '+' Add button and a '-' Remove button.

# File Sync & Share User Mode

The screenshot shows the Microsoft File Sync & Share User Mode interface. The left sidebar has a dark blue background with the title "File Sync & Share". The main content area has a white background with a header "Sync & Share" and a search bar. The main content area displays a list of items under the heading "Documents". The list includes a "Sync" icon, a "Type" column showing "Documents", a "Name" column with an upward arrow, and columns for "Size", "Modified", and "Link". On the right side, there is a vertical sidebar with three options: "Create Folder", "Upload Files", and "Show Deleted".

Sync & Share

Search

Sync & Share

Links

Log

Sync Type Name ▲

Size Modified Link

Documents

Create Folder

Upload Files

Show Deleted

# File Sync & Share User Mode

The screenshot shows the Microsoft File Sync & Share user interface. On the left is a sidebar with three items: "Sync & Share" (selected), "Links", and "Log". The main area is titled "Sync & Share" and contains a search bar with the placeholder "Search" and a magnifying glass icon. Below the search bar are filter options: "Sync", "Type", and "Name ▲". A list of files is displayed, with the first item being "Documents". To the right of the main area is a vertical sidebar with four options: "Create Folder", "Upload Files", and "Show Deleted". A large green box highlights the "Search" bar and its associated search icon. An arrow points from the text "Search, Switch Service, Account Settings" to the green box.

Search, Switch Service,  
Account Settings

# File Sync & Share User Mode

The screenshot shows the 'Sync & Share' user interface. On the left, there's a vertical sidebar with three tabs: 'Sync & Share' (selected), 'Links', and 'Log'. A green callout box labeled 'Tabs/Menus' points to the sidebar area. The main content area has a header 'Sync & Share' with a search bar and a settings gear icon. Below the header, there are filters for 'Sync', 'Type', and 'Name' (sorted by Name). The main list displays a single item: 'Documents'. To the right of the list are columns for 'Size', 'Modified', and 'Link'. On the far right, there's a sidebar with three options: 'Create Folder', 'Upload Files', and 'Show Deleted'.

# File Sync & Share User Mode

The screenshot shows the Microsoft File Sync & Share user interface. On the left, a sidebar has three items: 'Sync & Share' (selected), 'Links', and 'Log'. The main area is titled 'Sync & Share' and contains a table with columns: Sync, Type, Name (sorted by Name), Size, Modified, and Link. One row is visible, showing a sync icon, a folder icon, 'Documents', and other details. To the right of the table is a vertical sidebar with options: 'Create Folder', 'Upload Files', and 'Show Deleted'. A large green box labeled 'Synced folder' with a downward arrow points to the 'Documents' entry in the table.

Sync	Type	Name ▲	Size	Modified	Link
		Documents			

Synced folder

# File Sync & Share User Mode

The screenshot shows the Microsoft File Sync & Share application in user mode. On the left is a dark sidebar with three items: "Sync & Share" (selected), "Links", and "Log". The main content area has a header "Sync & Share" with a search bar and a settings icon. Below the header is a table with columns: Sync, Type, Name (sorted), Size, Modified, and Link. A single row is visible, showing "Documents" under "Type". To the right of the table is a vertical sidebar with actions: "Create Folder", "Upload Files", and "Show Deleted". A green callout box with the text "Actions available" is positioned over the "Upload Files" item. An arrow points from the text to the "Upload Files" button.

Sync & Share

Search

Sync & Share

Links

Log

Actions available

Create Folder

Upload Files

Show Deleted

# Notary Service Console

Acronis Cyber Cloud

NOTARIZED FILES

SIGNED FILES

API KEYS

VERIFICATION

Notarized files

Drag and drop files to notarize, or click 'Browse'

The files will not be stored in the cloud.

Browse



A screenshot of the Notary Service Console interface. The top navigation bar includes the Acronis Cyber Cloud logo, a search icon, a grid icon, a help icon, and a user profile icon. On the left, a sidebar lists five categories: NOTARIZED FILES (selected), SIGNED FILES, API KEYS, and VERIFICATION. The main content area is titled "Notarized files" and features a large central upload area with a blue arrow icon and instructions to drag and drop files or click "Browse". Below this, a note states that files will not be stored in the cloud. A "Browse" button is located at the bottom of the upload area.

# Notary Service Console

Acronis Cyber Cloud Notarized files

Search, Switch Console, Help & Account Settings

NOTARIZED FILES

SIGNED FILES

API KEYS

VERIFICATION

Drag and drop files to notarize, or click 'Browse'  
The files will not be stored in the cloud.

Browse

# Notary Service Console

Acronis Cyber Cloud

Notarized files

NOTARIZED FILES

SIGNED FILES

API KEYS

VERIFICATION

Tabs/Menus

Drag and drop files to notarize, or click 'Browse'

The files will not be stored in the cloud.

Browse

# Notary Service Console

Acronis Cyber Cloud

NOTARIZED FILES

SIGNED FILES

API KEYS

VERIFICATION

Notarized files

Drag and drop files to notarize, or click 'Browse'  
The files will not be stored in the cloud.

Browse

Drag & drop or browse for files to upload for notarization

Search icon

Grid icon

Help icon

User profile icon

#CyberFit Academy

# Section Summary



- Acronis provides a consistent interface across all products
- Left hand navigation that has tabs and subtabs
- Persistent top navigation that has breadcrumbs and user details
- Central work areas that often have right hand popouts that reveal more detail
- There are several different interfaces depending on whether you are in the management console or one of the service consoles

# Acronis

## Onboarding Cyber Protect Cloud

### Getting Started with Tenants and Accounts



# Section Modules - Part 3

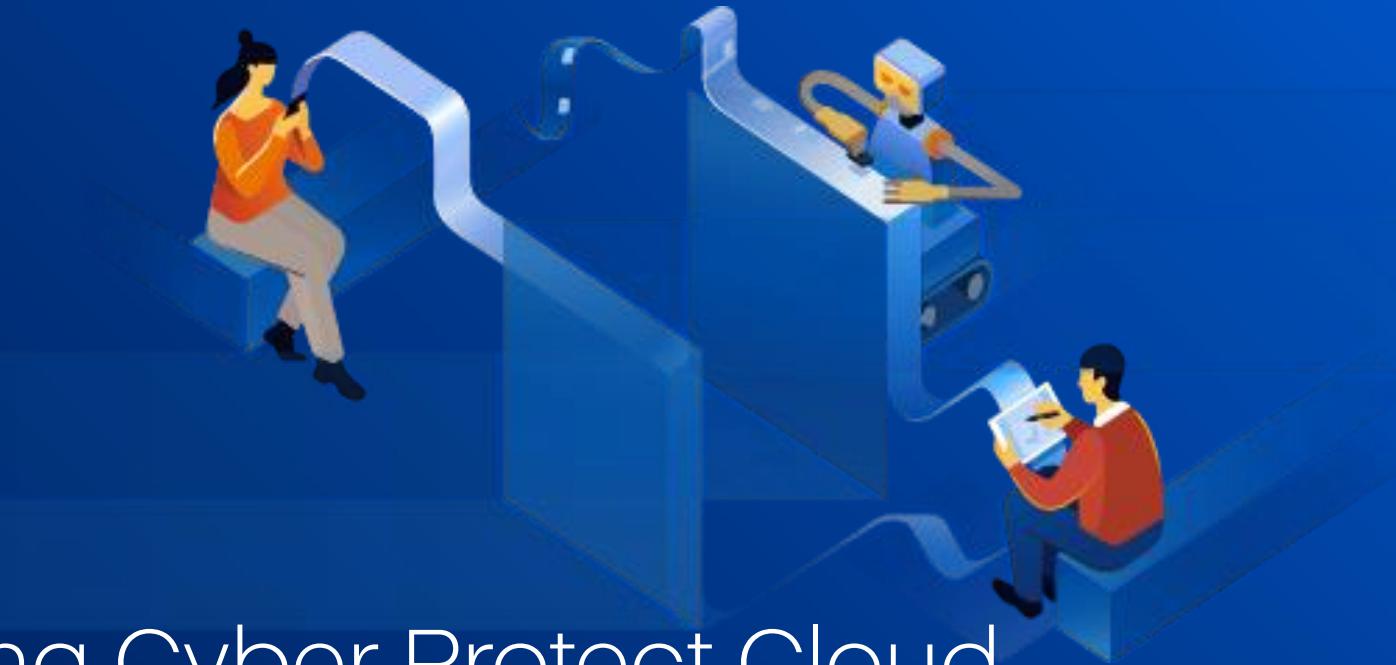


- 1. Onboarding Steps**
- 2. Installing Agents**
  - Supported Environments
  - Installation
  - Auto-Discovery for Windows
- 3. Tenants & Accounts**
- 4. Tenant & Account Operations**
- 5. Managing Tenants**

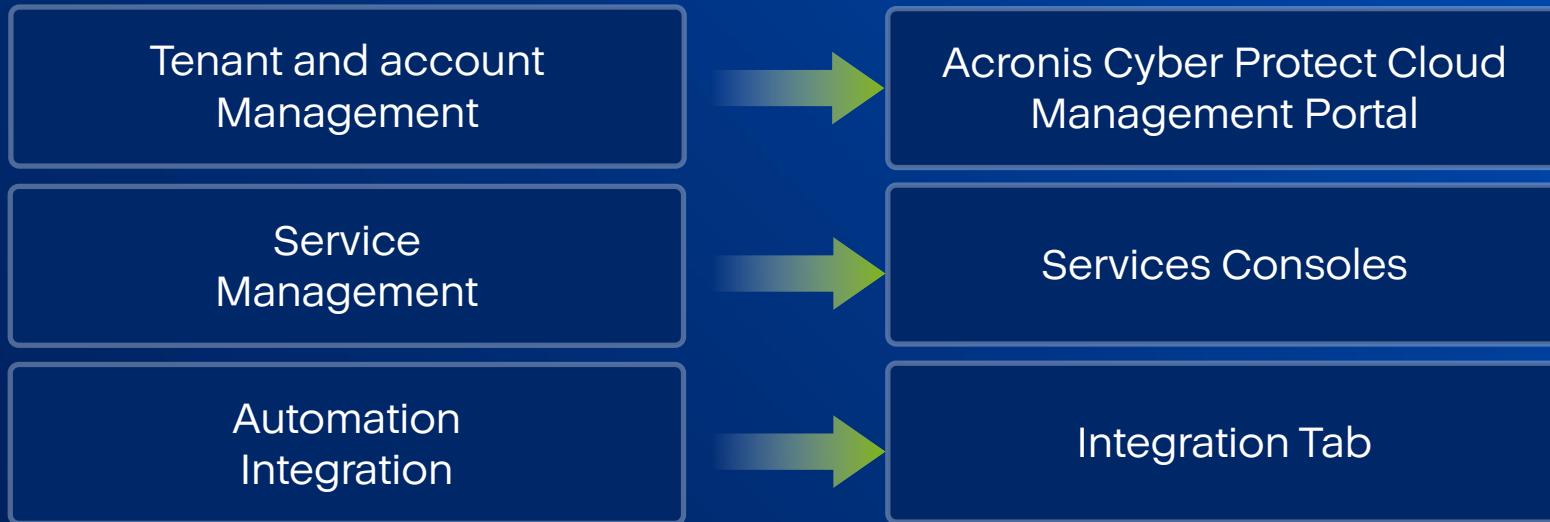
# Acronis

## Onboarding Cyber Protect Cloud

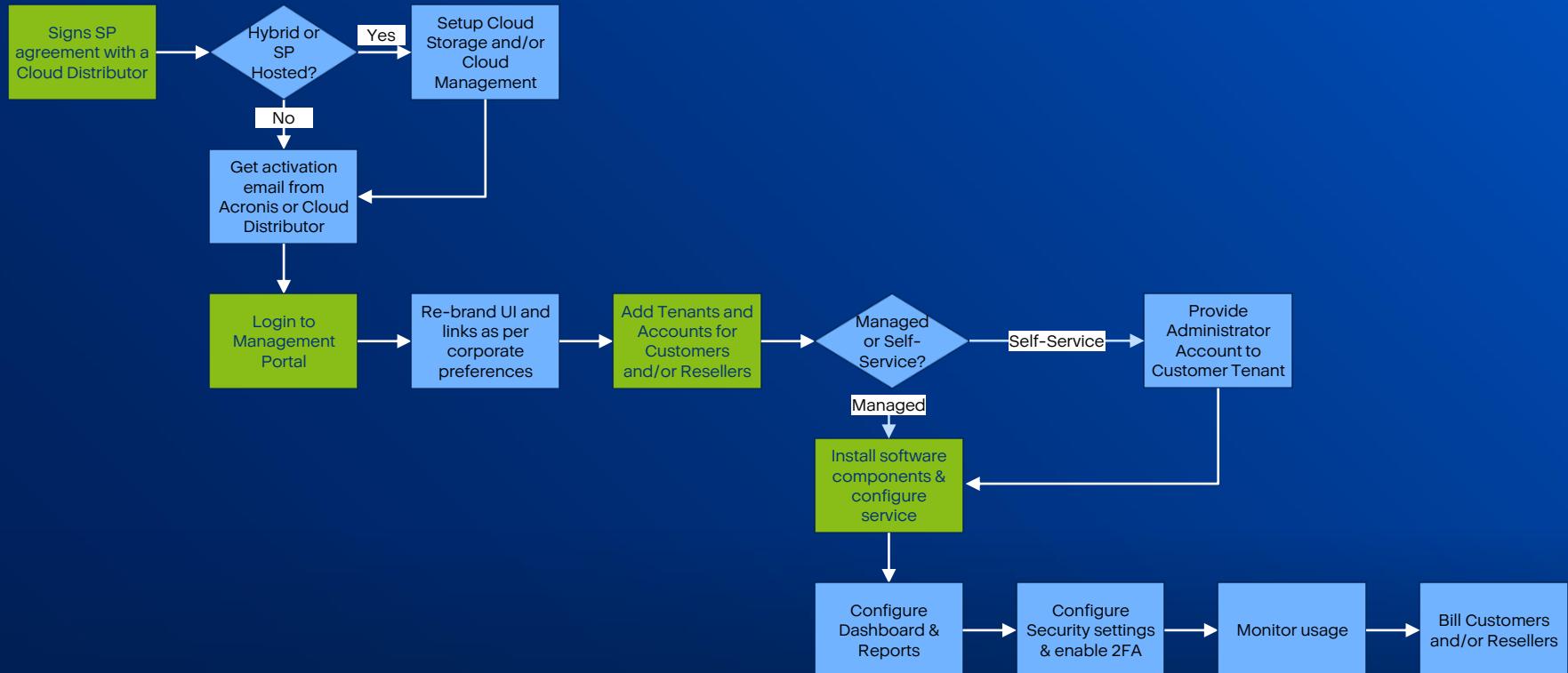
### **Initial steps to get started**



# Getting Started

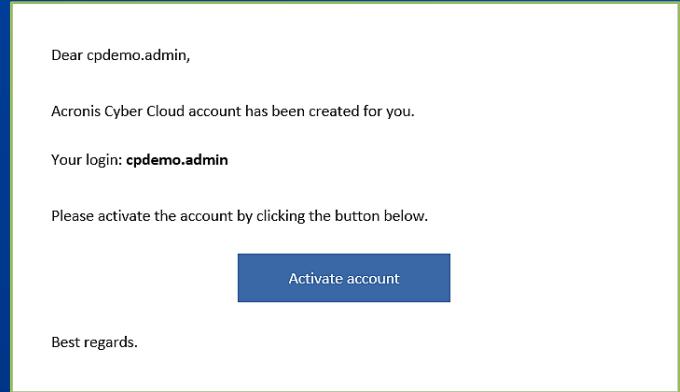


# Acronis Cyber Protect Cloud Onboarding Steps



# Acronis Cyber Protect Cloud Login

1. Acronis will send an activation email to new Service Providers to activate their **Administrator** account
2. Click on the link in the email to go to the account activation page where the administrator will have to set a **new password** for the Administrator account
3. After setting the password, the administrator will be redirected to the Acronis Cyber Protect Cloud **Management Portal**
4. Take note that 1<sup>st</sup> time login will always be from the account activation link in an activation email
5. Subsequent logins can be made from the URL:  
<https://cloud.acronis.com>



# Acronis

## Onboarding Cyber Protect Cloud

### **Installing Agents - Supported Environments**

### **Requirements for installing software components**



# Supported Environments

Component	Supported Environment
Agent for Windows	Windows OS from Windows Server 2003 SP1, Windows XP Pro SP1 and above, x86 and x64, except for RT editions and Nano Server installations
Agent for Linux	Linux OS with kernel 2.6.9 and above, glibc 2.3.4 and above, x86 and x64 including Red Hat Enterprise Linux, Ubuntu, Fedora, SUSE Linux Enterprise Server, Debian, CentOS, Oracle Linux, CloudLinux, ClearOS and ALT Linux
Agent for Mac	OS X 10.9 and above, macOS 10.12 and above
Agent for VMware (Virtual Appliance)	VMware ESXi 4.1 and above
Agent for VMware (Windows)	Windows OS supported by Agent for Windows except for 32-bit Windows OS, Windows XP, Windows Server 2003/2003 R2 and Windows Small Business Server 2003/2003 R2
Agent for Hyper-V	Windows Server 2008 (x64), Windows 8/8.1 and above with Hyper-V
Agent for Virtuozzo	Virtuozzo 6.0.10 and above
Agent for Exchange	Microsoft Exchange Server 2007 and above (Advanced Backup Pack)

# Supported Environments

Component	Supported Environment
Agent for SQL	Microsoft SQL Server 2005 and above (Advanced Backup Pack)
Agent for Active Directory	Windows Server 2003 and above with Active Directory Domain Services
Agent for Oracle	Windows Server 2008/2012 R2 Linux kernel and distributions supported by Agent for Linux
Agent for Office 365	Windows Server 2008 (x64), Windows 8/8.1 and above except for RT editions and Nano Server installations
SharePoint Explorer	Microsoft Windows SharePoint Services 3.0 SP2, Microsoft Office SharePoint Server 2007 SP2 and above
Oracle Database	Oracle Database 11g and 12c (single-instance configuration only) (Advanced Backup Pack)
SAP HANA	SAP HANA 2.0 SPS 03 installed on RHEL 7.6 running on a physical machine or VMware ESXi VM (Advanced Backup Pack)

# Supported Environments

Platform	Supported Environment
VMware	VMware vSphere 4.1 and above, vSphere Hypervisor (Free ESXi), VMware Server, Workstation, ACE, Player
Windows	Windows Server 2008 (x64) with Hyper-V and above, Windows 8/8.1 with Hyper-V and above except for Windows Server 2016 Nano Server, Microsoft Virtual PC 2004 and above, Windows Virtual PC, Microsoft Virtual Server 2005
Virtuozzo	Virtuozzo 6.0.10 and above
Citrix	Citrix XenServer 4.1 and above (fully virtualized a.k.a HVM guests only)
Red Hat and Linux	RHEV 2.2 and above, KVM
Parallels	Parallels Workstation, Parallels Server 4 Bare Metal
Oracle	Oracle VM Server 3.0 and above, Oracle VM VirtualBox 4.x (Advanced Backup Pack)
Nutanix	Nutanix Acropolis Hypervisor (AHV) 20160925.x and above
Cloud instances	Amazon EC2 instances and Microsoft Azure virtual machines

# Supported Environments

Category	Details
Network Ports (Inbound and Outbound)	<ul style="list-style-type: none"><li>– <b>443</b> and <b>8443</b>: Accessing service console, registering agents, downloading files from cloud storage</li><li>– <b>5905</b> and <b>7770 – 7800</b>: Communications between components</li><li>– <b>9850</b> for command line (acrocmd) commands</li><li>– <b>445</b> and <b>25001</b> for remote installation</li><li>– <b>443</b> and <b>902</b> for access to vCenter Server and ESXi hosts</li><li>– <b>44445</b> and <b>55556</b>: For backup and recovery from Acronis Cloud Storage</li><li>– <b>6109</b> for Active Protection</li></ul>
Web Browsers	<ul style="list-style-type: none"><li>– Google Chrome <b>29</b> or above   Mozilla Firefox <b>23</b> or above   Opera <b>16</b> or above   Windows Internet Explorer <b>11</b> or above, Microsoft Edge <b>25</b> or above   Safari <b>8</b> or above</li></ul>
Encryption Software	<ul style="list-style-type: none"><li>– Microsoft BitLocker Drive Encryption   McAfee Endpoint Encryption   PGP Whole Disk Encryption</li></ul>

# Component Installation Cheat Sheet

What to back up	What to install	Where to install	Disk Space
<b>Physical machines</b>			
Disk, volumes and files on physical machines running Windows	Agent for Windows	On the machine that will be backed up	550 MB
Disk, volumes and files on physical machines running Linux	Agent for Linux		500 MB
Disk, volumes and files on physical machines running OS X	Agent for Mac		450 MB
<b>Applications</b>			
SQL databases (Advanced Backup Pack)	Agent for Windows + Agent for SQL	On the machine running Microsoft SQL Server	600 MB
Exchange databases (Advanced Backup Pack)	Agent for Windows + Agent for Exchange	On the machine running the Mailbox role of Microsoft Exchange Server	750 MB
Machines running Active Directory Domain Services	Agent for Windows + Agent for Active Directory	On the domain controller	600 MB

# Component Installation Cheat Sheet

What to back up	What to install	Where to install	Disk Space
Microsoft Office 365 mailboxes	Agent for Office 365	On a Windows machine that is connected to the Internet	550 MB
Machines running Oracle Database (Advanced Backup Pack)	Agent for Oracle	On the machine running Oracle Databases	450 MB
<b>Virtual machines</b>			
VMware ESXi VMs	Agent for Windows + Agent for VMware (Windows)	On a Windows machine that has network access to vCenter Server and to the virtual machine storage	700 MB
	Agent for VMware (Virtual Appliance)	On the ESXi host	6 GB
Hyper-V VMs	Agent for Windows + Agent for Hyper-V	On the Hyper-V host	600 MB
Virtuozzo VMs and containers	Agent for Virtuozzo	On the Virtuozzo host	500 MB
VMs hosted on Amazon EC2	The same as physical machines	On the machine that will be backed up	Same as physical machines
VMs hosted on Microsoft Azure			
KVMs			

# Component Installation Cheat Sheet

What to back up	What to install	Where to install	Disk Space
Citrix XenServer VMs	The same as physical machines	On the machine that will be backed up	Same as physical machines
Red Hat Virtualization VMs			
Oracle VMs			
Nutanix AHV VMs			

# Required Linux Packages



## **Adding** modules to Linux Kernel, needed packages

- Package with kernel headers or sources, package version must match kernel version
- GNU Compiler Collection (GCC) compiler system, GCC version must be the one with which the kernel was compiled
- Make tool
- Perl interpreter
- libelf-dev, libelf-devel, or elfutils-libelf-devel libraries for building kernels starting with 4.15 and configured with CONFIG\_UNWINDER\_ORC=y
- Names of the packages vary depending on the Linux distribution used

# Required Linux Packages



## **Adding** modules to Linux Kernel, needed packages

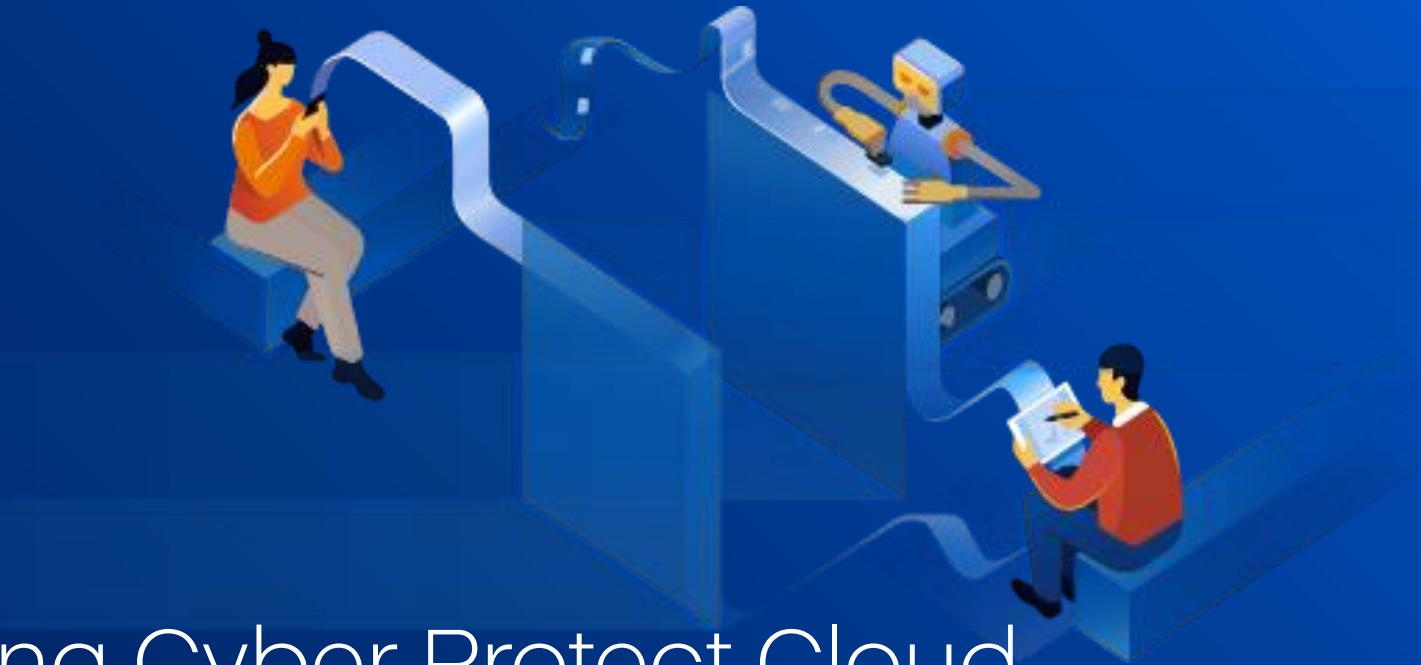
- In Red Hat Enterprise Linux, CentOS and Fedora, these packages normally will be installed by the setup program \*
- In other distributions, they need to be manually installed
- For distributions that does not use RPM Package Manager such as Ubuntu, it needs to be manually installed prior to running the setup program

\*Required packages may need to be manually installed if the machine does not have an active Red Hat subscription or Internet connection

# Acronis

## Onboarding Cyber Protect Cloud

### **Adding machines & Installing agents**



# Adding Machines

Acronis Cyber Cloud

Manage account

DASHBOARD

DEVICES

All devices

Machines with agents

Customer 2

Unmanaged machines

Data protection map

PLANS

DISASTER RECOVERY

Powered by Acronis AnyData Engine

All devices

+ Add

Search

Selected: 1 / Loaded: 1 / Total: 1

Type	Name ↑	Account	Status	Last backup	Next backup
VM	Win2012R2-Demo	demo.admin	Not protected	Apr 13 04:10:57 PM	Apr 14 05:20:22 AM

Protect

Disaster recovery

Recovery

Connect via RDP client

Connect via HTML5 client

Patch

Details

Activities

Alerts

# Adding Machines

Acronis Cyber Cloud

Manage account

DASHBOARD

DEVICES

All devices

Machines with agents

Customer 2

Unmanaged machines

Data protection map

PLANS

DISASTER RECOVERY

Powered by Acronis AnyData Engine

All devices

Search

Selected: 1 / Loaded: 1 / Total: 1

Type Name ↑ Account Status Last backup Next backup

VM	Win2012R2-Demo	demo.admin	Not protected	Apr 13 04:10:57 PM	Apr 14 05:20:22 AM
----	----------------	------------	---------------	--------------------	--------------------

Click to add machines

+ Add

Protect

Disaster recovery

Recovery

Connect via RDP client

Connect via HTML5 client

Patch

Details

Activities

Alerts

# Adding Machines

Acronis Cyber Cloud

Manage account

DASHBOARD

DEVICES

All devices

Machines with agents

Customer 1

Unmanaged machines

PLANS

DISASTER RECOVERY

SOFTWARE MANAGEMENT

Powered by Acronis AnyData Engine

All devices

Search

Type	Name	Account
VM	Win2012R2-Demo2	cust.admin01

Select type of Agent to download

X Add devices

MULTIPLE DEVICES

Windows only

WORKSTATIONS

Windows Mac

SERVERS

Windows Linux

MOBILE DEVICES

# Adding Machines

Acronis Cyber Cloud

Manage account

DASHBOARD

Overview

Alerts

Activities

DEVICES

PLANS

DISASTER RECOVERY

SOFTWARE MANAGEMENT

Powered by Acronis AnyData Engine

Dashboard

No devices added

This dashboard will provide a number of customizable, dynamic widgets that give an overview of your protection infrastructure and protected devices. Because no devices have been added so far, the dashboard is empty. Click below to add the devices.

Add devices

SP Demo Admin

Change language

Downloads

Log out

The screenshot shows the Acronis Cyber Cloud interface. On the left is a dark sidebar with navigation links: Manage account, DASHBOARD (which is highlighted in blue), Overview, Alerts, Activities, DEVICES, PLANS, DISASTER RECOVERY, and SOFTWARE MANAGEMENT. At the bottom of the sidebar is the text 'Powered by Acronis AnyData Engine'. The main area is titled 'Dashboard' and features a large placeholder icon of a clock with a gear. Below it, the text reads: 'No devices added' followed by a descriptive paragraph about the dashboard's purpose. A prominent blue button labeled 'Add devices' is centered in this area. In the top right corner, there is a user menu with options: SP Demo Admin, Change language, Downloads, and Log out. The top right also includes icons for a grid view, help, and user profile.

# Adding Machines

Acronis Cyber Cloud

Manage account

DASHBOARD

Overview

Alerts

Activities

DEVICES

PLANS

DISASTER RECOVERY

SOFTWARE MANAGEMENT

Powered by Acronis AnyData Engine

Dashboard

No devices added

This dashboard will provide a number of customizable, dynamic widgets that give an overview of your protection infrastructure and protected devices. Because no devices have been added so far, the dashboard is empty. Click below to add the devices.

Add devices

Click on Account button to show account menu

SP Demo Admin

Change language

Downloads

Log out

A screenshot of the Acronis Cyber Cloud web interface. On the left is a vertical navigation bar with icons and text for DASHBOARD, Overview, Alerts, Activities, DEVICES, PLANS, DISASTER RECOVERY, and SOFTWARE MANAGEMENT. The 'Overview' item is currently selected and highlighted in blue. The main content area is titled 'Dashboard' and displays a message stating 'No devices added'. Below this message is a paragraph explaining the purpose of the dashboard and a blue 'Add devices' button. In the top right corner, there is a user account dropdown menu with options for 'SP Demo Admin', 'Change language', 'Downloads', and 'Log out'. A green callout box with the text 'Click on Account button to show account menu' points to the account icon in the top right corner of the dashboard header. The bottom left corner of the page footer contains the text 'Powered by Acronis AnyData Engine'. The overall theme is dark blue with light blue highlights for selected items.

# Adding Machines

The screenshot shows the Acronis Cyber Cloud dashboard. On the left, a sidebar lists navigation options: Manage account, DASHBOARD (selected), Overview, Alerts, Activities, DEVICES, PLANS, DISASTER RECOVERY, and SOFTWARE MANAGEMENT. The main area is titled 'Dashboard' and displays the message 'No devices added'. A call-to-action button says 'Add devices'. A green callout box points to the 'Account' button in the top right corner of the dashboard header, with the text 'Click on Account button to show account menu'. Another green callout box points to the 'Downloads' option in the account menu, with the text 'Click to download agents'.

Acronis Cyber Cloud

Manage account

DASHBOARD

Overview

Alerts

Activities

DEVICES

PLANS

DISASTER RECOVERY

SOFTWARE MANAGEMENT

Powered by Acronis AnyData Engine

Dashboard

No devices added

Add devices

Click on Account button to show account menu

SP Demo Admin

Change language

Downloads

Log out

Click to download agents

# Adding Machines

The screenshot shows the Acronis Cyber Cloud interface. On the left, there's a sidebar with various navigation items: Manage account, DASHBOARD (selected), Overview, Alerts, Activities, DEVICES, PLANS, DISASTER RECOVERY, and SOFTWARE MANAGEMENT. The main area is titled 'Dashboard' and contains a 'Downloads' modal. The modal has a header 'Downloads' with a close button 'X'. Below it is a section 'Documentation: User's guide'. Under 'Installers', there are five entries:

Icon	File Name	Size	Action
cube icon	All agents for Windows (32-bit)	527 MB	download
cube icon	All agents for Windows (64-bit)	664 MB	download
Windows icon	Agent for Windows	13.8 MB	download
bell icon	Agent for Linux (32-bit)	410 MB	download
bell icon	Agent for Linux (64-bit)	470 MB	download

A large green button at the bottom of the modal says 'Select agent to download' with a downward arrow pointing to it. To the right of the modal, there's some descriptive text: 'Agents that give an overview of your environment', 'No devices have been added yet.', and 'Add devices.'.

# Adding Machines



## To add machines

Login to the Cyber Protection service console and do either of the following:

1. **Go to Devices tab**, click on the **ADD** button and select the Agent installer to download
2. Click on **Account** button > **Downloads** and select the Agent installer to download

After downloading the installer, perform local installation by running the installer on the machine to be protected

# Local Installation

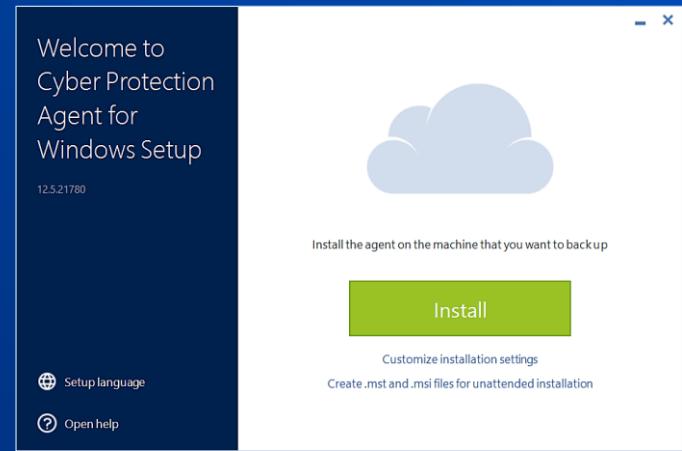


**Ensure that the following requirements are met:**

- Internet connectivity for target machines
- Microsoft Visual C++ Redistributable is installed on Windows machines (required by Cyber Protect features)
- Allow inbound and outbound connections through firewalls and other network security system such as proxy servers for TCP ports 443, 8443, 7770...7800, 44445 and 55556
- For Agent for VMware, allow TCP ports 443, 902 and 333
- Verify that the following local ports are open for inbound communication:
  - 127.0.0.1:9999
  - 127.0.0.1:43234
  - 127.0.0.1:9850

# Local Installation Example – Agent for Windows

1. Log on as an administrator and run the installer
2. [Optional] To change the language, click **Setup language**
3. Click on **Install** to install with default settings or **Customize installation settings** to change installation settings
4. Start the installation
5. After installation, click on **Register now** and enter your Acronis Cyber Cloud credentials in the opened web browser window



# Registering machines



Agents can be registered to an Acronis Cyber Cloud account after agent installation is complete

1. Click **Register the machine** to open a browser window, **login** using the credentials of the account that the machine is to be registered under and confirm the registration
2. Alternatively, click **Show registration info** to show the registration link and **registration code** which is **valid for 1 hour**, copy them then login to Acronis Cyber Cloud using the account that the machine is to be registered under, go to **Devices** and click on the **Add** button to enter the code in the **Register via code** section
3. For mass deployment, a **registration token** can be used instead to register multiple agents to an account – go to **Devices**, click on the **Add** button, scroll down to the **Registration token** section and click **Generate** to generate a registration token

# Registering machines



Agents can be registered to an Acronis Cyber Cloud account after agent installation is complete

1. Click **Register the machine** to open a browser window,
2. **Login** using the credentials of the account that the machine is to be registered under and confirm the registration
3. Alternatively, click **Show registration** info to show the registration link and registration code which is valid for **1 hour**
4. **Copy** registration link and registration code then **login** to Acronis Cyber Cloud using the account that the machine is to be registered under
5. Go to **Devices** and click on the **Add** button to enter the code in the **Register via code** section

# Registering machines



**Run the following command in Linux:**

1. `sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service address> -u <user name> -p <password>`
  
2. Example: `sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword`

Account credential used must not be a partner administrator

# Registering machines



**Run the following command in Mac:**

1. 

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

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

Account credential used must not be a partner administrator

# Agent for VMware (Virtual Appliance)



**Agent for VMware (Virtual Appliance) is available as an OVF template a  
to be deployed to an ESXi host:**

- By default, the virtual appliance is assigned 4GB of RAM and 2vCPUs and can be increased to 8GB of RAM and 4vCPUs if backup traffic bandwidth is expected to exceed 100MB per second such as when using 10GbE networks
- Virtual disks of the appliance will occupy no more than 6GB and thin or thick provisioning does not matter, choosing either will not affect appliance performance

# Agent for VMware (Virtual Appliance)



**Agent for VMware (Virtual Appliance) is available as an OVF template a  
to be deployed to an ESXi host:**

- Virtual appliance is sufficient to protect an entire vSphere environment but best practice is to have 1 virtual appliance per cluster or per host if there are no clusters
- Having both virtual appliance and Agent for VMware (Windows) is possible as long as they are connected to the same vCenter Server or to different standalone ESXi hosts\*

\*Avoid cases when 1 agent is connected to an ESXi host directly and another agent is connected to the vCenter Server managing the same ESXi host

# Other Installation Methods



Agent for Linux and Mac can be installed using local installation,  
refer to the **Help** file for more details

- Besides local installation, the following installation methods can also be used:
  - Unattended installation/uninstallation for Agent for Windows and Linux
  - Using Group Policy in an AD domain for installing Agent for Windows

# Updating Agents



Agents starting with the following versions can be updated online:

- Agent for Windows, Agent for Vmware (Windows), Agent for Hyper-V: 11.9.191 or later
  - Agent for Linux: 11.9.179
  - Other Agents: any version can be updated
- To update agents from earlier version, download and install the newest agent
- Agents are updated using peer-to-peer technology to minimize network traffic:
  - 1st agent to be installed will be assigned the Update role and will be checking the Internet for available updates and distributing them to other agents
  - More agents<sup>1</sup> can be assigned this role in **Settings > Agents > Details**

# Uninstalling Agents



**Agents have to be uninstalled manually from machines:**

- If the machine has an Internet connection, the machine will be unregistered and removed from the service console of the account used for registering the agent
- Otherwise, manually remove the machine from the service console

# Uninstalling Agents



**During agent uninstallation, options for removing logs and configuration settings will be available:**

- Select to remove if there is no intention to re-install the Agent
- Do not remove them if the intention is to install the Agent again otherwise, if an Agent is reinstalled, the machine may be duplicated in the service console and old backups may not be associated with the new machine

# Supported Platforms

Odin



APS STANDARD

RESTful API  
GET PUT POST DELETE

plesk

**Autotask®**

**cPanel**

The logo features a blue five-pointed star-like shape with a white 'x' through it.

flexiant™  
your cloud simplified

**HostBill**

 **iPortalis**

The logo consists of a cluster of purple hexagonal shapes.

resello

The logo features the classic Windows four-pane window icon.

Windows Azure Pack™

The logo features the letters 'WHMCS' in a dark blue sans-serif font, with a green gear icon integrated into the letter 'C'.

WHMCS

The logo features a green square icon with a white silhouette of a person wearing a hard hat.

ConnectWise  
**AUTOMATE™**  
formerly LabTech

The logo features a blue square icon with a white silhouette of a person wearing a hard hat.

ConnectWise  
**MANAGE™**

The logo features a blue cloud icon with a white 'i' inside.

interworks.cloud

# Section Summary



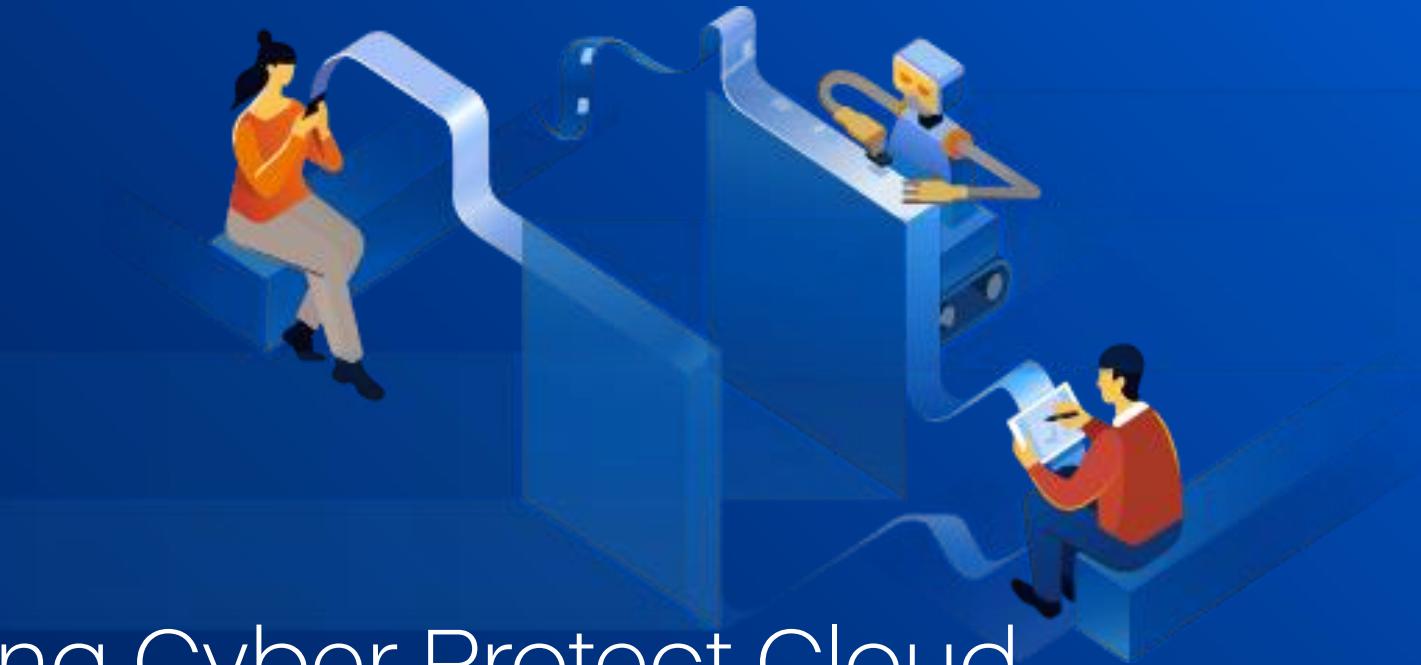
- Acronis Cyber Protect Cloud supports a wide range of operating systems with lots of backward compatibility
- Be sure that your target machine meets the minimum requirements
- Be sure that all necessary ports are available
- When installing agents, you will need to register the agent to the service console
- When uninstalling agents, be sure to both uninstall the agent and remove the device from the service console

# Acronis

## Onboarding Cyber Protect Cloud

### **Auto-Discovery for Windows**

### **Discovering machines for agent installation**



# Autodiscovery for Windows

Acronis Cyber Cloud All devices X Add devices

Manage account

Customer 1

Unmanaged machines

PLANS

DISASTER RECOVERY

SOFTWARE MANAGEMENT

BACKUP STORAGE

REPORTS

SETTINGS

Add machines

Select discovery method

Discovery agent  
Win2012R2-Demo2

Search Active Directory  
The machine where the discovery agent is installed must be a domain member.

Scan local network  
The discovery agent will obtain the neighbor IP addresses by using NetBIOS discovery, Web Service Discovery (WSD), and Address Resolution Protocol (ARP) table.

Specify manually or import from file  
Provide hostnames or IP addresses manually or in a text file.

Cancel Next

MOBILE DEVICES

Mac

Linux

Configure Autodiscovery

# Autodiscovery for Windows

- To start, click on **Add** button and select **Multiple Devices > Windows only**
- Works by automatically detecting machines in an AD domain or local network and machines discovered will be categorized in the service console as follows:
  - **Discovered**: machines that were discovered but no agent is installed
  - **Managed**: machines with agent installed
  - **Unprotected**: machines with no Protection Plan (includes both Discovered and Managed machines)
  - **Protected**: machines with Protection Plan

# Autodiscovery for Windows

- Requires at least 1 installed **Agent for Windows** (discovery agent)
- For **network discovery**, the following technologies will be used:
  - NETBIOS discovery, Web Service Discovery (WSD) and Address Resolution Protocol (ARP) table
- For **AD discovery**, the discovery agent must be installed on a domain machine<sup>1</sup>
- Machines can also be manually specified using a text file that contains either the IP address or hostname of the machines, one per line, to be added<sup>2</sup>
- After discovery, choose to **install and register machines**, **register machines with installed agents** or **add as unmanaged machines**

1. This feature is available starting with Agent version 2.2.0.0. Remote management tools such as WinRM and PowerShell remoting must be installed for successful remote installation of an Agent.

# Autodiscovery for Windows

- For installation, credentials of one or more users with **Administrator** rights, depending on individual machines will have to be provided:
  - Remote installation without any preparation only works if the **built-in Administrator** account is specified for a machine
  - If another Administrator account is used, then the target machine has to be prepared prior to performing Autodiscovery and remote installation, refer to the Help file for details
  - Alternatively, add the following record in the registry:
    - HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: DWORD (32-bit)  
LocalAccountTokenFilterPolicy = 1

# Section Summary

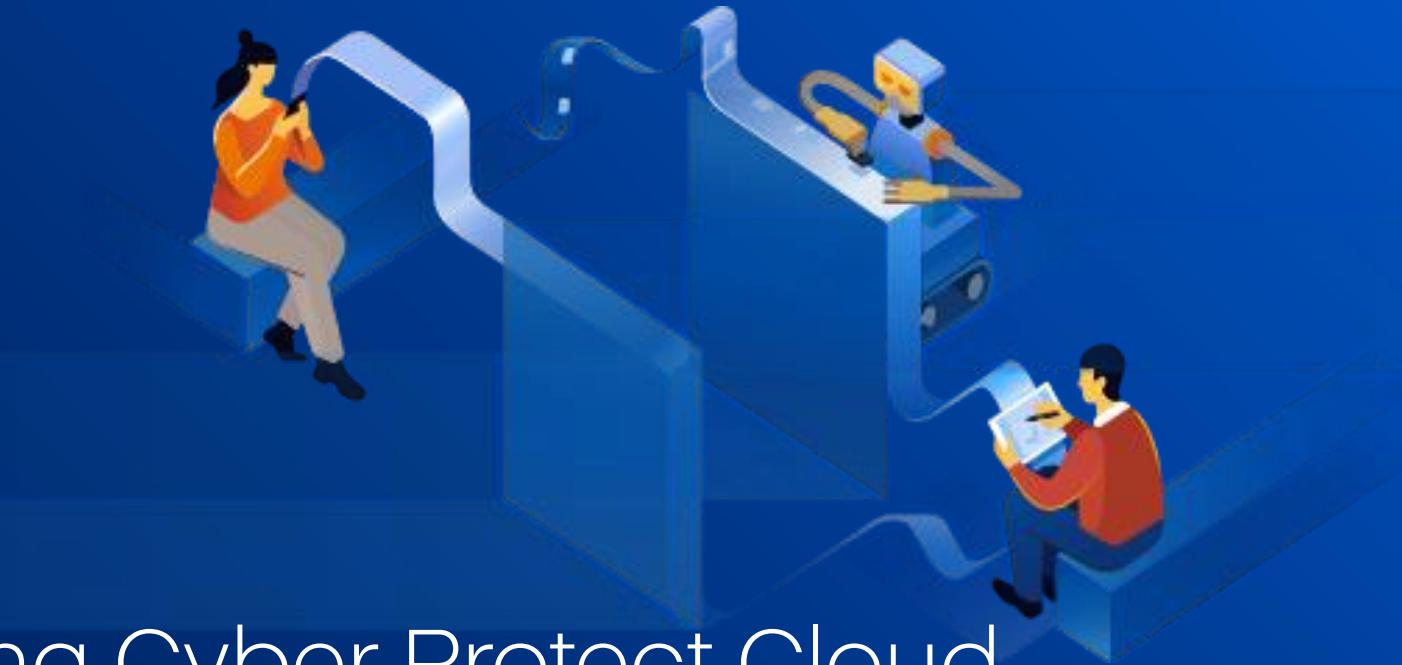


- Autodiscovery for Windows will allow you to onboard customers quickly and easily as you can add all of their machines at once
- Autodiscovery has several modes including network discovery, AD Discovery and manual input through a file
- Autodiscovery can be used to install the agents as well

# Acronis

## Onboarding Cyber Protect Cloud

### **Setting up tenants & user accounts**



# Acronis Cyber Protect Cloud Tenants & Accounts

## Tenants

- Entities that have a relationship with the Service Provider (such as a reseller or end-customer)
- Managed from the Clients tab



**1 Tenant** can have 1 or more user accounts

All Tenant types (except of Customer) can be **nested** according the org. structure

# Acronis Cyber Protect Cloud Types of Accounts

## Administrator

- Access to Management Portal and have administrator role in all configured services



## User

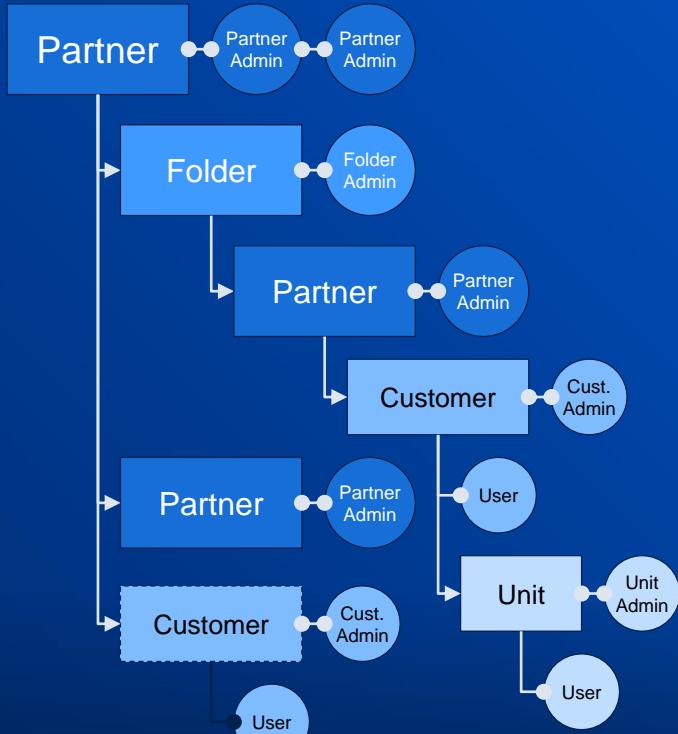
- No access to Management Portal, access to services and role in services defined by an Administrator



# Acronis Cyber Protect Cloud Types of Accounts

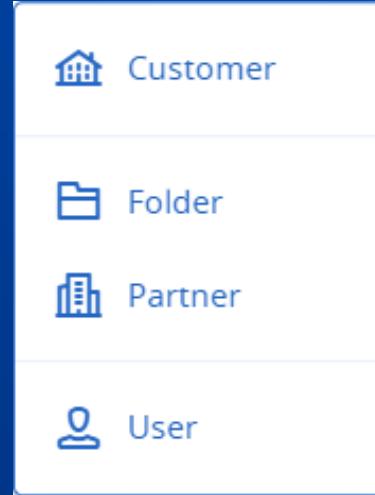
Accounts are created within a tenant:

- Each Customer tenant must have at least 1 Administrator account for service configuration and software installation purposes
- Administrators can create and manage tenants and accounts at or below their level in the tenant hierarchy
- Administrators at Customer and higher levels can limit access to their tenant by toggling off the Allow administrators from parent tenants to manage this tenant setting in **Settings > Security tab**



# Acronis Cyber Protect Cloud Types of Tenants

- **Customer:** Represents an end-customer company or organization that uses services, can create and have one or more Unit tenants under it
- **Folder:** Special tenant type used for grouping similar child tenants together, can also be used as a “template” since child tenants created within a Folder will “inherit” the Services settings of the folder
- **Partner:** Represents a service provider that resells services, can create and have one or more Partner, Customer and Folder tenants under it
- **User:** Each user belongs to a tenant. User does not have access to the management portal. Their access to the services and their roles in the services are defined by an administrator.



# Acronis Cyber Protect Cloud Tenants & Accounts

Operations that can be performed by Administrator and User accounts:

Operation	Users	Customer and Unit Administrator	Partner and Folder Administrator
Create tenants	✗	✓	✓
Create accounts	✗	✓	✓
Download and install the software <sup>1</sup>	✓	✓	✗
Manage and Use services	✓	✓	✓
Create reports about the service usage	✗	✓	✓
Configure branding	✗	✗	✓

<sup>1</sup> Partner Administrator account cannot be used for installing software components. If needed, Partner Administrators can create a Customer Administrator account as a surrogate

# Acronis Cyber Protect Cloud Tenants & Accounts

The screenshot shows the Acronis Cyber Protect Cloud interface. On the left, a sidebar menu includes: Overview (selected), Clients (highlighted in blue), Users, Reports, Audit Log, and Settings. The main content area has tabs for Cyber Protect and Cyber Infrastructure, with Cyber Protect selected. Below these tabs is a navigation bar with Protection, File Sync & Share, Physical Data Shipping, and Notary. The main table displays tenant information:

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB 0 GB 0 0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	-	0 GB 0 GB 0 0 GB
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider	-	0 GB 0 GB 0 0 GB

A context menu is open over the first row, listing options: Customer, Folder, Partner, and User. The bottom right corner of the interface shows the text "Acronis Cyber Cloud".

# Acronis Cyber Protect Cloud Tenants & Accounts

The screenshot shows the Acronis Cyber Protect Cloud interface. On the left, a sidebar includes links for Overview, Clients, Users, Reports, Audit Log, and Settings. The main area is titled 'Cyber Protect' and shows a table of 'Tenants'. The table columns are: Name, Tenant status, Billing mode, 2FA status, Management mode, and 7-day history. The data rows are:

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history
Customer 1	Active	Per workload	Disabled	By service provider	No Data
Group 1	Active	Per workload, Per gigabyte	-	-	0 GB
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider	0 GB

A modal window titled '+ New' is open on the right, listing four options: Customer, Folder, Partner, and User. An arrow points from this modal to a green callout box containing the text 'Adding new Tenants and Accounts'.

# Account Activation

- An activation email will be sent to the email address specified during user account creation
- Click on the **Activate account** button to go to the account activation page and enter a password for the new account
- Thereafter, the user will be able to access the respective service consoles and Management Portal if the account is an Administrator account
- User forgets or losses password, they can request to reset their password on their own or parent tenant administrator

# Section Summary



- Partners, Customers, Folders and Units can be added by clicking the +New button and then selecting the correct option
- 2 kinds of roles can be added to the system- Users and Administrators
- +New button is context sensitive to the level of the system
- Services and quotas can be added when creating new tenants

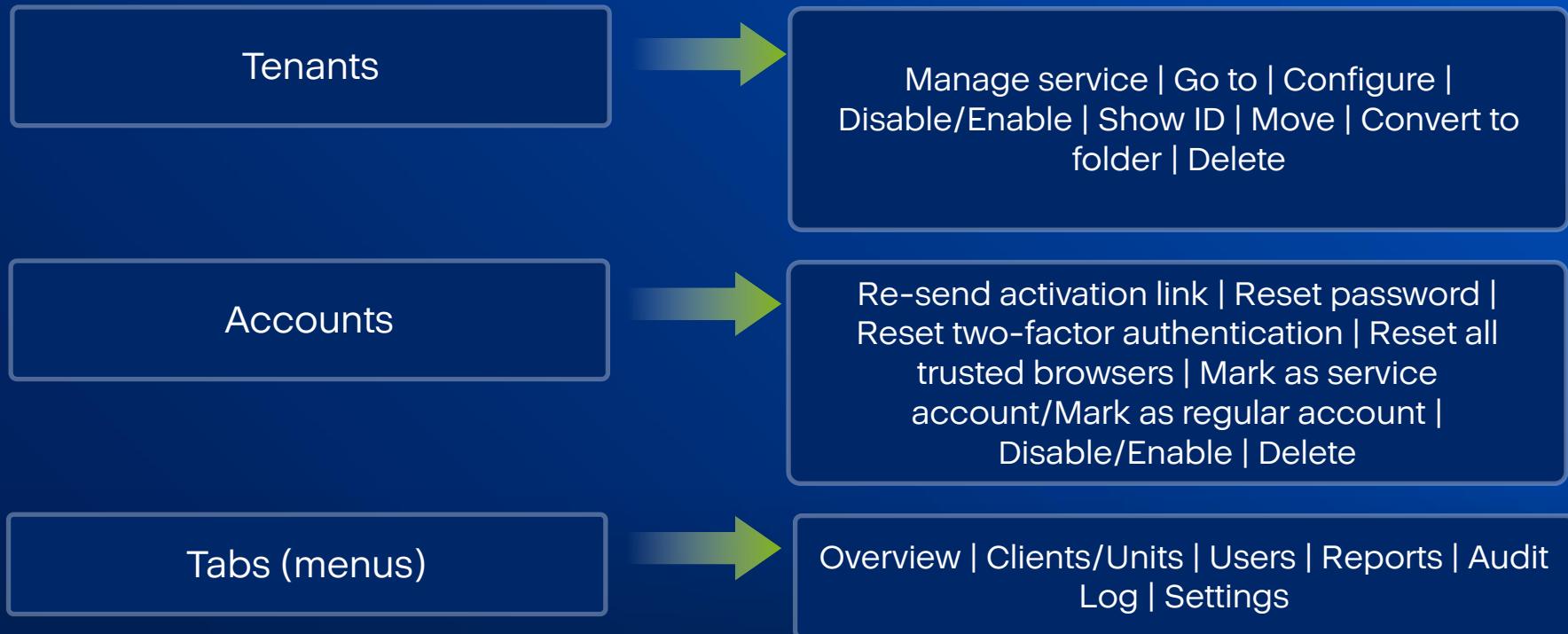
# Acronis

## Tenant & Account Operations

### **Actions Available for tenants and users accounts**



# Tenant & Account Operations



# Tenant Operations

**Manage service:**

Switch to the service console for selected service, e.g., Cyber Protection

**Go to a tenant:**

Switch to the selected tenant

**Configure:**

Show the **Select services** and Configure services menus for enabling/disabling services/editions and/or offering items for a tenant

# Tenant Operations

SGLAB.Demo.Provider > ~Training > ~Service Provider

+ New Search Help Logout

**OVERVIEW** Cyber Protect Cyber Infrastructure Settings

**CLIENTS** Protection File Sync & Share Physical Data Shipping Notary

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Name	Tenant status	Billing mode	2FA status	Management mode	7-day history	Totals	Local backup
Customer 1	Active	Per workload	Disabled	By service provider	No Data	0 GB	0 GB
Group 1	Active	Per workload, Per gigabyte	-	-	-	0 GB	0 GB
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider	-	0 GB	0 GB

Manage service >

- Go to
- Configure
- Disable
- Show ID
- Move
- Convert to partner

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

# Tenant Operations

The screenshot shows the Acronis Cyber Cloud interface with the following details:

- Header:** SGLAB.Demo.Provider > ~Training > ~Service Provider
- Top Navigation:** + New, Search icon, User icons.
- Sidebar:** OVERVIEW, CLIENTS (selected), USERS, REPORTS, AUDIT LOG, SETTINGS.
- Main Content:** Protection tab selected. Sub-tabs: Protection, File Sync & Share, Physical Data Shipping, Notary.
- Table Headers:** Name (sorted up), Tenant status, Billing mode, 2FA status, Management mode, 7-day history, Totals, Local backup.
- Data Rows:**
  - Customer 1: Active, Per workload, Disabled, By service provider, No Data, 0 GB, 0 GB, 0, 0 GB.
  - Group 1: Active, Per workload, Per gigabyte, -, -, 0 GB, 0 GB, 0, 0 GB.
  - Partner 1: Active, Per workload, Per gigabyte, Disabled, By service provider, 0 GB, 0 GB, 0, 0 GB.
- Context Menu (for Customer 1):**
  - Manage service (highlighted)
  - Go to
  - Configure
  - Disable
  - Show ID
  - Move
  - Convert to partner
- Callout:** Operations for child tenant (points to the Manage service option in the context menu).

# Enabling Upsell Scenarios

The screenshot shows the Acronis Cyber Cloud interface. On the left, a sidebar menu includes 'OVERVIEW', 'CLIENTS' (selected), 'USERS', 'REPORTS', 'AUDIT LOG', and 'SETTINGS'. The main area displays 'CYBER PROTECTION' with a table of clients: Customer 1 (Trial, No Data), Group 1 (Active), and Reseller 1 (Active). A modal window titled 'Customer 1' is open, showing configuration options. The 'Notary' feature is enabled with a description: 'Enables users to notarize and verify files by using the Blockchain technology, and sign files electronically.' The 'Upsell' section contains a toggle switch for 'Promote more advanced editions' (which is turned on) and sections for 'General information' (Name: Cyber Protect Customer, Language: English) and 'Contact information'.

Service Provider

Customer 1

Trial ... X

OVERVIEW

CLIENTS

USERS

REPORTS

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

CYBER PROTECTION

Name Tenant status 7-day history

Customer 1 Trial No Data

Group 1 Active

Reseller 1 Active

Notary

Enables users to notarize and verify files by using the Blockchain technology, and sign files electronically.

Upsell

Promote more advanced editions

General information

Name: Cyber Protect Customer

Language: English

Contact information

# Enabling Upsell Scenarios

The screenshot shows the Acronis Cyber Cloud interface. On the left, a sidebar menu includes Service Provider, OVERVIEW, CLIENTS (selected), USERS, REPORTS, AUDIT LOG, and SETTINGS. Below the sidebar is the text "Acronis Cyber Cloud" and "Powered by Acronis AnyData Engine". The main area is titled "CYBER PROTECTION" and shows a table with columns: Name (sorted by name), Tenant status, and 7-day history. One row is visible for "Customer 1" (Trial status, No Data). To the right of the table is a "Customer 1" panel with tabs: Overview, Notary, Upsell, General information, Language, and Contact information. The "Upsell" tab is currently active, displaying the sub-section "Promote more advanced editions" with a toggle switch set to "On". A large green callout box with the text "Enabling Upsell for a Customer tenant" points to the "Upsell" section.

Service Provider

OVERVIEW

CLIENTS

USERS

REPORTS

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

CYBER PROTECTION

Name ↓ Tenant status 7-day history

Customer 1 Trial No Data

Notary

Enables users to notarize and verify files by using the Blockchain technology, and sign files electronically.

Upsell

Promote more advanced editions

General information

Name: Cyber Protect Customer

Language: English

Contact information

Customer 1

Trial ... X

Configure

Enabling Upsell for a Customer tenant

# Enabling Upsell Scenarios

The screenshot displays the Acronis Cyber Cloud web interface. On the left, a dark sidebar lists navigation options: Acronis Cyber Cloud, SGLAB Demo Provider (Manage), AD Cloud Sales 12-A..., DASHBOARD (with a red notification badge), DEVICES (selected), All devices, Machines with agents, AD Cloud Sales 12-APR-2021, Unmanaged machines, PLANS, DISASTER RECOVERY, ANTI-MALWARE PROTECTION, and SOFTWARE. At the bottom of the sidebar, it says "Powered by Acronis AnyData Engine".

The main content area shows a table titled "All devices" with one entry: WIN2K19DC01, which is a VM owned by Amos Dong (ad.sales) with a #CyberFit Score of 625/850 and an OK status. To the right of the table is a detailed view for WIN2K19DC01, showing various protection plan settings:

- New protection plan (Create button)
- Upgrade cyber protection to the next level by using advanced functionality. Contact your administrator to enable it. (Find out more)
- Backup: Enabled (green switch)
- Disaster recovery: Enabled (green switch)
- Antivirus & Antimalware protection: Enabled (green switch)
- URL filtering: Enabled (green switch)
- Windows Defender Antivirus: Enabled (green switch)
- Vulnerability assessment: Enabled (green switch)

# Tenant Operations



## Delete a tenant

- Removes the tenant from Acronis Cyber Protect Cloud (must be disabled prior to deleting), operation is irreversible and takes effect immediately:
- All sub-tenants will be deleted
- All users with this tenant and all its sub-tenants will be deleted
- All services enabled within this tenant and all its sub-tenant will stop operating
- All service-related data (e.g., backups, synced files) of this tenant and all its sub-tenants will be deleted

# Tenant Operations



## Convert to folder/partner:

- Used for converting a Partner type tenant to a Folder type tenant and vice versa
- Previously before Folder tenant type was available, Service Providers had to use Partner tenant type for grouping purposes, this operation allows Service Providers to change those Partner tenants to Folder tenants for proper organization
- Used purely for grouping purposes and doesn't affect the users within the tenant and any service-related data such as backups

# Tenant Operations



## Move a tenant:

Move a child tenant to a different parent, e.g., transfer a customer to a different partner:

- Partner/Folder type tenants can only be moved to other Partner/Folder type tenants
- Customer type tenants can only be moved to other Partner/Folder type tenants
- Tenants cannot be moved to its child tenant and Unit tenants cannot be moved
- Tenants can only be moved if target parent tenant has the same or larger set of service and offering as the original parent
- When moving a Customer tenant, all storages assigned to the Customer tenant in the original parent must exist in the target parent tenant as Customer-related data cannot be moved from one storage to another

# Tenant Operations

1. To move a tenant, select the target tenant and click on **Show ID** to view the **Internal ID** string
2. Copy the ID string and then select the tenant to be moved and click on **Move**
3. Paste the ID string in the **Move...to** field and click **Move**

Tenant ID

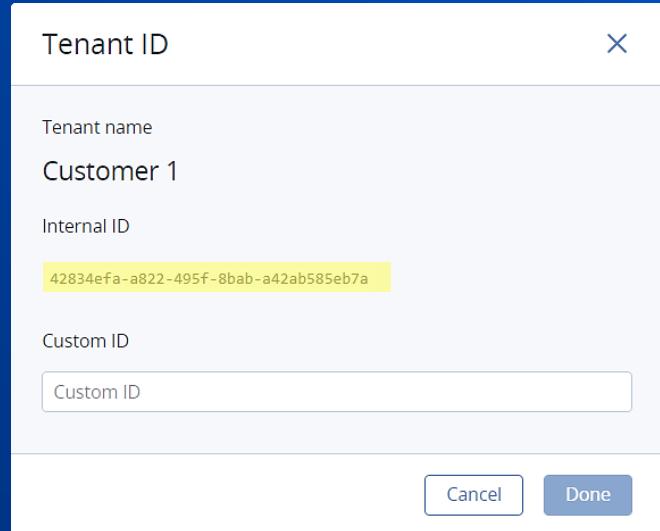
X

Tenant name  
Customer 1

Internal ID  
`42834efa-a822-495f-8bab-a42ab585eb7a`

Custom ID

Cancel Done

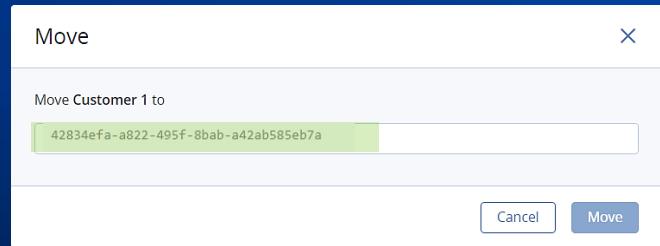


Move

X

Move Customer 1 to  
`42834efa-a822-495f-8bab-a42ab585eb7a`

Cancel Move



# Account Operations

Cyber Protect Customer

+ New ? grid refresh user

Overview CYBER PROTECTION

Units

Users

Reports

Audit Log

Settings

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

**OVERVIEW**

**UNITS**

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

**CYBER PROTECTION**

Name	Status	2FA status	Login	Roles	Totals
cpdemo.admin01	Active	Setup required	cpdemo.admin...	Company Admi...	6.97 GB
cpdemo.admin <span>Me</span>	Active	Configured	cpdemo.admin	Company Admi...	0 GB

...

Reset password

Reset two-factor authentication

Reset all trusted browsers

Mark as service account

# Account Operations

The screenshot shows the Acronis Cyber Cloud interface. The left sidebar has navigation links: OVERVIEW, UNITS, USERS (selected), REPORTS, AUDIT LOG, and SETTINGS. The main area is titled 'CYBER PROTECTION' and shows a table of users under the 'USERS' tab. One user, 'cpdemo.admin01', is active and has 'Setup required'. Another user, 'cpdemo.admin' (marked as 'Me'), is also active and has 'Configured'. A context menu is open for the 'Me' user, listing options: Reset password, Reset two-factor authentication, Reset all trusted browsers, and Mark as service account. A green callout box points to this menu with the text 'Enabling Upsell for a Customer tenant'.

Name	Status	2FA status	Login	Roles	Totals
cpdemo.admin01	Active	Setup required	cpdemo.admin...	Company Admin...	6.97 GB
cpdemo.admin	Active	Configured	cpdemo.admin	Company Admin...	0 GB

Enabling Upsell for a Customer tenant

# Account Operations

## Resend activation link for an account:

- Resend the activation email for a newly created account that has not been activated

## Reset password for an account:

- Send a password reset email to the email address specified for the account

## Disable or Enable an account:

- Temporarily disable/enable selected account, disabled account will not be able to login to Acronis Cyber Protect Cloud

# Account Operations

## Delete an account:

Removes the account from the tenant (must be disabled prior to deleting), operation is irreversible and takes effect immediately:

- All data of machines associated with this user will be deleted
- All machines associated with this user will be unregistered
- All protection plans will be revoked from all machines associated with this user

# Account Operations

## Reset two-factor authentication (2FA) for an account

- Only shown when 2FA is configured for a tenant, resets the user's current 2FA setup and allows the user to setup a new 2FA. Time-Based One Time Password (TOTP) of user initiating the reset will be required

## Reset all trusted browsers for an account:

- Only shown when 2FA is configured for a tenant, resets all trusted browsers for a user. TOTP of user initiating the reset will be required

# Account Operations

## Mark as service/regular account for an account:

Mark as service account will disable 2FA for a user account and is needed for an account that is used for API access<sup>1</sup>. TOTP of user making the change will be required. Mark as regular account will enable 2FA for the account again

*Do not switch normal users to service users in order to disable 2FA, otherwise the user may not be able to log in*

# Section Summary



- Tenants can be managed and modified after creation
- The actions that can be performed on tenants or users is context sensitive and the options change as you modify other features
- Tenants and Users must first be disabled before they can be deleted and delete either with extreme caution noting the warnings
- Folders and Units can be used to address hierarchy issues and partner can be converted to folders and vice versa



# Acronis

## Tenant & Account Operations

### **Managing Tenants using the Management Portal**

# Managing Tenants – Overview > Usage Tab

The screenshot shows the Acronis Cyber Cloud tenant management interface. The top navigation bar includes 'Service Provider' and 'Customer 1'. The main menu on the left has sections: OVERVIEW (selected), Usage (highlighted in blue), Operations, UNITS, USERS, REPORTS, AUDIT LOG, and SETTINGS. The Acronis Cyber Cloud logo is at the bottom left, and a note at the bottom center says 'Powered by Acronis AnyData Engine'.

The central area has tabs: CYBER PROTECTION, FILE SYNC & SHARE, PHYSICAL DATA SHIPPING, and NOTARY. A 'Manage service' button is visible. Below it, under 'Usage', there's a 'Totals' section showing 'Total cloud storage size' as 0 GB. The 'Data sources' section lists 'Cyber Backup - Standard Edition' with detailed counts for various resources:

Category	Count
Workstations	0
Servers	0
Virtual machines	0
Mobile devices	0
Office 365 seats	0
G Suite seats	0
Web hosting servers	0
Websites	0

# Managing Tenants – Overview > Usage Tab

The screenshot shows the Acronis Cyber Cloud tenant management interface. The top navigation bar includes 'Service Provider' and 'Customer 1'. On the right are buttons for '+ New', search, and help. The left sidebar has icons for Overview, Usage (selected), Operations, Units, Users, Reports, Audit Log, and Settings. The main content area is titled 'OVERVIEW' and shows tabs for CYBER PROTECTION, FILE SYNC & SHARE, PHYSICAL DATA SHIPPING, and NOTARY. A 'Manage service' button is highlighted with a red arrow pointing to a green callout box that says 'Click to go to service console'. Below this are sections for 'Totals' (Total cloud storage size: 0 GB) and 'Data sources' (Cyber Backup - Standard Edition). The 'Data sources' section contains tables for Workstations, Servers, Virtual machines, Mobile devices, Office 365 seats, G Suite seats, Web hosting servers, and Websites.

Service Provider > Customer 1

+ New

?

?

OVERVIEW

CYBER PROTECTION FILE SYNC & SHARE PHYSICAL DATA SHIPPING NOTARY

Manage service

Click to go to service console

Usage

Operations

UNITS

USERS

REPORTS

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Workstations	Servers	Virtual machines
0	0	0

Mobile devices	Office 365 seats	G Suite seats
0	0	0

Web hosting servers	Websites
0	0

Total cloud storage size  
0 GB

Totals

Data sources

Cyber Backup - Standard Edition

Workstations 0

Servers 0

Virtual machines 0

Mobile devices 0

Office 365 seats 0

G Suite seats 0

Web hosting servers 0

Websites 0

# Managing Tenants – Overview > Operations Tab

Acronis (14) > Customer 2

+ New

**OVERVIEW**

**Operations**

**UNITS**

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

**Protection status**

1 Resources

- Protected 1
- Unprotected 0
- Managed 1
- Discovered 0

**Active alerts summary**

There are no items to show in this view

**Activities**

8  
7  
6  
5  
4  
3  
2  
1  
0

6 Apr 8 Apr 10 Apr 12 Apr

**Patch installation status**

1 Resources

- Installed 0
- Reboot required 1
- Failed 0

**Missing updates by categories**

24 Updates

- Other 14
- Critical updates 0
- Security updates 10

**Disk health status**

There are no items to show in this view

# Managing Tenants – Overview > Operations Tab

Acronis (14) > Customer 2

+ New

Add widget, Download dashboard, Send as email

**OVERVIEW**

Usage

**Operations**

UNITS

USERS

REPORTS

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

**Protection status**

1 Resources

- Protected 1
- Unprotected 0
- Managed 1
- Discovered 0

There are no items to show in this view

**Patch installation status**

1 Resources

- Installed 0
- Reboot required 1
- Failed 0

**Missing updates by categories**

24 Updates

- Other 14
- Critical updates 0
- Security updates 10

Activities

8  
7  
6  
5  
4  
3  
2  
1  
0

6 Apr 8 Apr 10 Apr 12 Apr

Disk health status

There are no items to show in this view

# Managing Tenants – Overview > Operations Tab

The screenshot shows the Acronis Cyber Cloud interface. On the left, there's a sidebar with various navigation items like Alerts, Activities, Threat feed, DEVICES, PLANS, DISASTER RECOVERY, and FILE SYNC & SHARE. In the center, there's a summary card with metrics such as 'Backed up today' (93.56 GB), 'overall compressed size' (101.12 GB), and 'Patch installation status'. A large green box labeled 'Available widgets' is highlighted with a white arrow pointing to a modal window titled 'Add widget'. The modal contains a search bar, a category dropdown set to 'All widgets', and a list of available widgets categorized under 'Activities'. The list includes 'Activities' (Shows results of activities for the last seven days), 'Activity list' (Shows results of activities performed during a specified time period), 'Alerts', 'Anti-malware protection', and '#CyberFit Score'.

# Managing Tenants – Overview > Operations Tab

Acronis (14) > Customer 2

+ New

**OVERVIEW**

**Operations** (selected)

**UNITS**

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

**Protection status**

1 Resources

- Protected 1
- Unprotected 0
- Managed 1
- Discovered 0

**Active alerts summary**

There are no items to show in this view

**Activities**

Date	Activity Count
6 Apr	0
7 Apr	0
8 Apr	0
9 Apr	0
10 Apr	0
11 Apr	14
12 Apr	1

**Patch installation status**

1 Resources

- Installed 0
- Reboot required 1
- Failed 0

**Missing updates by categories**

24 Updates

- Other 14
- Critical updates 0
- Security updates 10

**Disk health status**

There are no items to show in this view

**Add widget**

Excel and PDF

Excel

PDF

# Managing Tenants – Overview > Operations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Customer 2' tenant selected. The left sidebar includes links for Overview, Usage, Operations (which is highlighted), Units, Users, Reports, Audit Log, and Settings. The main area displays several widgets:

- Protection status:** Shows 1 Resource. Data: Protected 1, Unprotected 0, Managed 1, Discovered 0.
- Active alerts summary:** Shows 0 alerts. Message: "There are no items to show in this view".
- Patch installation status:** Shows 1 Resource. Data: Installed 0, Reboot required 1, Failed 0.
- Missing updates by categories:** Shows 24 Updates. Data: Other 14, Critical updates 0, Security updates 10.
- Disk health status:** Shows 0 disk health issues. Message: "There are no items to show in this view".

A green callout box in the center-right area says "Download as Excel, PDF or both". A dropdown menu next to it offers "Download" options: "Add widget", "Download" (selected), "Send", "Excel and PDF", "Excel", and "PDF".

# Managing Tenants – Client/Unit Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Clients' tab selected. The left sidebar has icons for Overview, Clients (selected), Users, Reports, Audit Log, and Settings. The main area has tabs for Cyber Protection, File Sync & Share, and Notary. The Clients table lists three tenants: Customer 1, Customer 2, and MSSP Partner, all marked as Active.

Name	Tenant status	7-day history	Totals
Customer 1	Active	6.97 GB	0 GB
Customer 2	Active	0 GB	0 GB
MSSP Partner	Active	0 GB	0 GB

Acronis Cyber Cloud  
Powered by Acronis AnyData Engine

# Managing Tenants – Client/Unit Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'CLIENTS' tab selected. The main area displays a table of tenants with columns for Name, Tenant status, 7-day history, and Totals. Three rows are visible: 'Customer 1' (Active, 6.97 GB, 0 GB), 'Customer 2' (Active, 0 GB, 0 GB), and 'MSSP Partner' (Active, 0 GB, 0 GB). A green callout box with the text 'Click on the row to show tenant properties' has an arrow pointing to the 'MSSP Partner' row.

Name	Tenant status	7-day history	Totals
Customer 1	Active	6.97 GB	0 GB
Customer 2	Active	0 GB	0 GB
MSSP Partner	Active	0 GB	0 GB

Click on the row to show tenant properties

# Managing Tenants – Client/Unit Tab

The screenshot shows the Acronis Cyber Cloud interface with the following details:

**Header:** SGLAB.Demo.Provider > ~Training > ~Service Provider

**Page Title:** Customer 1

**Left Sidebar:**

- OVERVIEW
- CLIENTS** (selected)
- USERS
- REPORTS
- AUDIT LOG
- SETTINGS

**Client List:**

Name	Tenant status	Billing mode	2FA status	Management
Customer 1	Active	Per workload	Disabled	By service pro
Group 1	Active	Per workload, Per gigabyte	-	-
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service pro

**Right Panel:**

**Services**

**Cyber Protect**  
All-in-one cyber protection solution that integrates data protection, malware prevention, security controls, remote assistance, monitoring, reporting, file sharing, file notarization, and e-signing of files.  Protection

Select a billing mode

**Per workload**  
Provides cyber protection, monitoring, management, backup, and disaster recovery that satisfy most users' needs. The billing is according to the number of protected workloads, and cloud storage is charged separately.

Add advanced protection:  
 Advanced Backup (i)  
 Advanced Management (i)  
 Advanced Security (i)  
 Advanced Disaster Recovery (i)

**Per gigabyte**  
Provides cyber protection, monitoring, management, backup, and disaster recovery that satisfy

# Managing Tenants – Client/Unit Tab

The screenshot shows the Acronis Cyber Cloud interface for managing tenants. On the left, a sidebar includes links for Overview, Clients, Users, Reports, Audit Log, and Settings. The main area displays a list of tenants: Customer 1 (Active, Per workload, 2FA disabled), Group 1 (Active, Per workload, Per gigabyte, 2FA disabled), and Partner 1 (Active, Per workload, Per gigabyte, 2FA disabled). A green callout box labeled "Tenant properties" points to the "Customer 1" row. To the right, a detailed configuration panel for "Customer 1" is open, titled "Customer 1". It shows the "Cyber Protect" service is enabled (green toggle switch) and "Protection" is selected. It also lists "Select a billing mode" options: "Per workload" (selected, described as providing protection, monitoring, management, backup, and disaster recovery), "Advanced protection" (checkboxes for Advanced Backup, Advanced Management, Advanced Security, and Advanced Disaster Recovery are checked), and "Per gigabyte" (described as providing cyber protection, monitoring, management, and disaster recovery based on file size).

Name	Tenant status	Billing mode	2FA status	Management
Customer 1	Active	Per workload	Disabled	By service provider
Group 1	Active	Per workload, Per gigabyte	-	-
Partner 1	Active	Per workload, Per gigabyte	Disabled	By service provider

**Cyber Protect**  
All-in-one cyber protection solution that integrates data protection, malware prevention, security controls, remote assistance, monitoring, reporting, file sharing, file notarization, and e-signing of files.

Protection

Select a billing mode

Per workload  
Provides cyber protection, monitoring, management, backup, and disaster recovery that satisfy most users' needs. The billing is according to the number of protected workloads, and cloud storage is charged separately.

Add advanced protection:

Advanced Backup ⓘ  
 Advanced Management ⓘ  
 Advanced Security ⓘ  
 Advanced Disaster Recovery ⓘ

Per gigabyte  
Provides cyber protection, monitoring, management, and disaster recovery based on file size.

# Managing Tenants – Users Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'OVERVIEW' tab selected in the sidebar. The main area displays a table of users with one row visible:

Name	Status	Login	Roles
spdemo.admin <span style="background-color: #0072BD; color: white; border-radius: 50%; padding: 2px 5px;">Me</span>	Active	spdemo.admin	Administrator

At the top right, there are buttons for '+ New', search, help, and notifications. The sidebar also includes links for 'CLIENTS', 'REPORTS', 'AUDIT LOG', and 'SETTINGS'. The bottom left corner features the 'Acronis Cyber Cloud' logo and the text 'Powered by Acronis AnyData Engine'.

# Managing Tenants – Users Tab

Service Provider

+ New ? !

OVERVIEW

CLIENTS

USERS

REPORTS

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Name	Status	Login	Roles
spdemo.admin <span>Me</span>	Active	spdemo.admin	Administrator

Click on the row to show account properties

# Managing Tenants – Users Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Service Provider' tenant selected. The left sidebar includes navigation links for Overview, Clients, Users (selected), Reports, Audit Log, and Settings. The main area displays a table of users under the 'OVERVIEW' tab, with one row selected for 'spdemo.admin'. A detailed modal window on the right provides information about this user, including General information, Services and roles, and Settings.

**General information**

Login	spdemo.admin
Email	ron.eo@acronis.com
Language	English

**Services and roles**

Management Portal	Administrator
Cyber Infrastructure	Administrator

**Settings**

Quota overuse notifications	Enabled
-----------------------------	---------

# Managing Tenants – Users Tab

The screenshot shows the Acronis Cyber Cloud interface. On the left, a sidebar menu includes 'OVERVIEW', 'CLIENTS', 'USERS' (which is selected and highlighted in blue), 'REPORTS', 'AUDIT LOG', and 'SETTINGS'. Below the sidebar, it says 'Acronis Cyber Cloud' and 'Powered by Acronis AnyData Engine'. The main content area has a header 'spdemo.admin Service Provider'. A table lists users: 'Name' (spdemo.admin), 'Status' (Active), 'Login' (spdemo.admin), and 'Roles' (Admins). A green callout box labeled 'Account properties' points to the user row for spdemo.admin. To the right, a detailed view of the user 'spdemo.admin' is shown in a modal window. The modal has tabs for 'General information', 'Services and roles', and 'Settings'. Under 'General information', details are listed: Login (spdemo.admin), Email (ron.eo@acronis.com), and Language (English). Under 'Services and roles', roles are assigned to Management Portal (Administrator) and Cyber Infrastructure (Administrator). Under 'Settings', 'Quota overuse notifications' is set to Enabled.

Name	Status	Login	Roles
spdemo.admin	Active	spdemo.admin	Admins

General information

Login	spdemo.admin
Email	ron.eo@acronis.com
Language	English

Services and roles

Management Portal	Administrator
Cyber Infrastructure	Administrator

Settings

Quota overuse notifications	Enabled
-----------------------------	---------

# Managing Tenants – Reports> Usage Tab

The screenshot shows the Acronis Cyber Cloud tenant management interface. The left sidebar has a dark blue background with white icons and text:

- OVERVIEW** (with a bar chart icon)
- CLIENTS** (with a user group icon)
- USERS** (with a person icon)
- REPORTS** (with a document icon)
- Usage** (with a bar chart icon, highlighted in blue)
- Operations** (with a gear icon)
- AUDIT LOG** (with a log icon)
- SETTINGS** (with a gear icon)

Below the sidebar, the text "Acronis Cyber Cloud" and "Powered by Acronis AnyData Engine" are displayed.

The main content area has a white background with a dark blue header bar at the top containing:

- Service Provider icon
- + New button
- Search icon
- Help icon
- User icon

The main content area shows the "Usage" tab settings:

- Scheduled** tab is selected (highlighted in blue).
- Ad hoc** tab is also present.
- Send a monthly summary report** checkbox is checked.
- Description:** A scheduled report covers service usage metrics for the last full calendar month. The report is generated at 23:59:59 by UTC time on the first day of a month and sent on the second day of that month to administrators of your tenant who have the "Scheduled usage reports" option enabled.
- Level of detail:** A dropdown menu set to "Direct customers and partners".
- Buttons:** Save and Cancel.

# Managing Tenants – Reports> Usage Tab

The screenshot shows the Acronis Cyber Cloud tenant management interface. On the left, a sidebar lists navigation options: Overview, Clients, Users, Reports (which is selected), Usage (highlighted in blue), Operations, Audit Log, and Settings. The main content area is titled "Usage". At the top right of this area are buttons for "+ New", search, help, and user profile. Below these are two tabs: "Scheduled" (selected) and "Ad hoc". A green callout box with the text "Select type of Report: Scheduled" points to the "Scheduled" tab. Underneath the tabs, there is a checkbox labeled "Send a monthly summary report" which is checked. To the right of the checkbox is a detailed description of what a scheduled report covers. Further down, there is a "Level of detail" dropdown set to "Direct customers and partners", and "Save" and "Cancel" buttons at the bottom.

Service Provider

Scheduled Ad hoc

Select type of Report: Scheduled

Send a monthly summary report

A scheduled report covers service usage metrics for the last full calendar month. The report is generated at 23:59:59 by UTC time on the first day of a month and sent on the second day of that month to administrators of your tenant who have the "Scheduled usage reports" option enabled.

Level of detail

Direct customers and partners

Save Cancel

OVERVIEW

CLIENTS

USERS

REPORTS

Usage

Operations

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

# Managing Tenants – Reports> Usage Tab

The screenshot shows the Acronis Cyber Cloud tenant management interface. On the left, a sidebar lists navigation options: Overview, Clients, Users, Reports (which is selected), Usage (highlighted in blue), Operations, Audit Log, and Settings. The main content area is titled "Service Provider". It displays two tabs: "Scheduled" (selected) and "Ad hoc". A green callout box points to the "Scheduled" tab with the text "Select type of Report: Scheduled". Below this, there is a checkbox labeled "Send a monthly summary report" which is checked. A detailed description follows: "A scheduled report covers service usage metrics for the last full calendar month. The report is generated at 23:59:59 by UTC time on the first day of a month and sent on the second day of that month to administrators of your tenant who have the "Scheduled usage reports" option enabled." A green callout box points to the "Level of detail" dropdown with the text "Select Level of detail". The dropdown menu is open, showing the option "Direct customers and partners". At the bottom of the form are "Save" and "Cancel" buttons.

Service Provider

+ New ? !

**Scheduled** Ad hoc

Send a monthly summary report

A scheduled report covers service usage metrics for the last full calendar month. The report is generated at 23:59:59 by UTC time on the first day of a month and sent on the second day of that month to administrators of your tenant who have the "Scheduled usage reports" option enabled.

Level of detail

Direct customers and partners

Save Cancel

Select type of Report: Scheduled

Select Level of detail

# Managing Tenants – Reports> Usage Tab

The screenshot shows the Acronis Cyber Cloud interface with a dark blue header and sidebar. The header includes a 'Service Provider' icon, a search bar, and navigation icons for '+ New', '?', and '@'. The sidebar on the left has icons for Overview, Clients, Users, Reports (which is selected), Usage, Operations, Audit Log, and Settings. The main content area is titled 'OVERVIEW' and shows three report options under 'Ad hoc': 'Current usage' (selected), 'Summary for period', and 'Day-by-day for period'. Each option has a description. Below these is a 'Level of detail' dropdown set to 'Direct customers and partners' and a 'Generate and send' button.

Service Provider

+ New ? @

**OVERVIEW**

**CLIENTS**

**USERS**

**REPORTS**

**Usage**

**Operations**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Scheduled Ad hoc

Current usage  
The report contains the current service usage metrics.

Summary for period  
The report contains the service usage metrics for the end of the specified period, and the difference between the metrics in the beginning and at the end of the specified period.

Day-by-day for period  
The report contains the service usage metrics and their changes for each day of the specified period.

Level of detail

Direct customers and partners

Generate and send

# Managing Tenants – Reports> Usage Tab

The screenshot shows the Acronis Cyber Cloud tenant management interface. On the left, a sidebar lists navigation options: Overview, Clients, Users, Reports (which is selected), Usage (highlighted in blue), Operations, Audit Log, and Settings. The main content area is titled "Select type of Report: Ad hoc". It includes three report options: "Current usage" (selected), "Summary for period", and "Day-by-day for period". Below these is a "Level of detail" dropdown set to "Direct customers and partners", and a "Generate and send" button.

Service Provider

Scheduled Ad hoc

Select type of Report:  
Ad hoc

Current usage  
The report contains the current service usage metrics.

Summary for period  
The report contains the service usage metrics for the end of the specified period, and the difference between the metrics in the beginning and at the end of the specified period.

Day-by-day for period  
The report contains the service usage metrics and their changes for each day of the specified period.

Level of detail

Direct customers and partners

Generate and send

OVERVIEW

CLIENTS

USERS

REPORTS

Usage

Operations

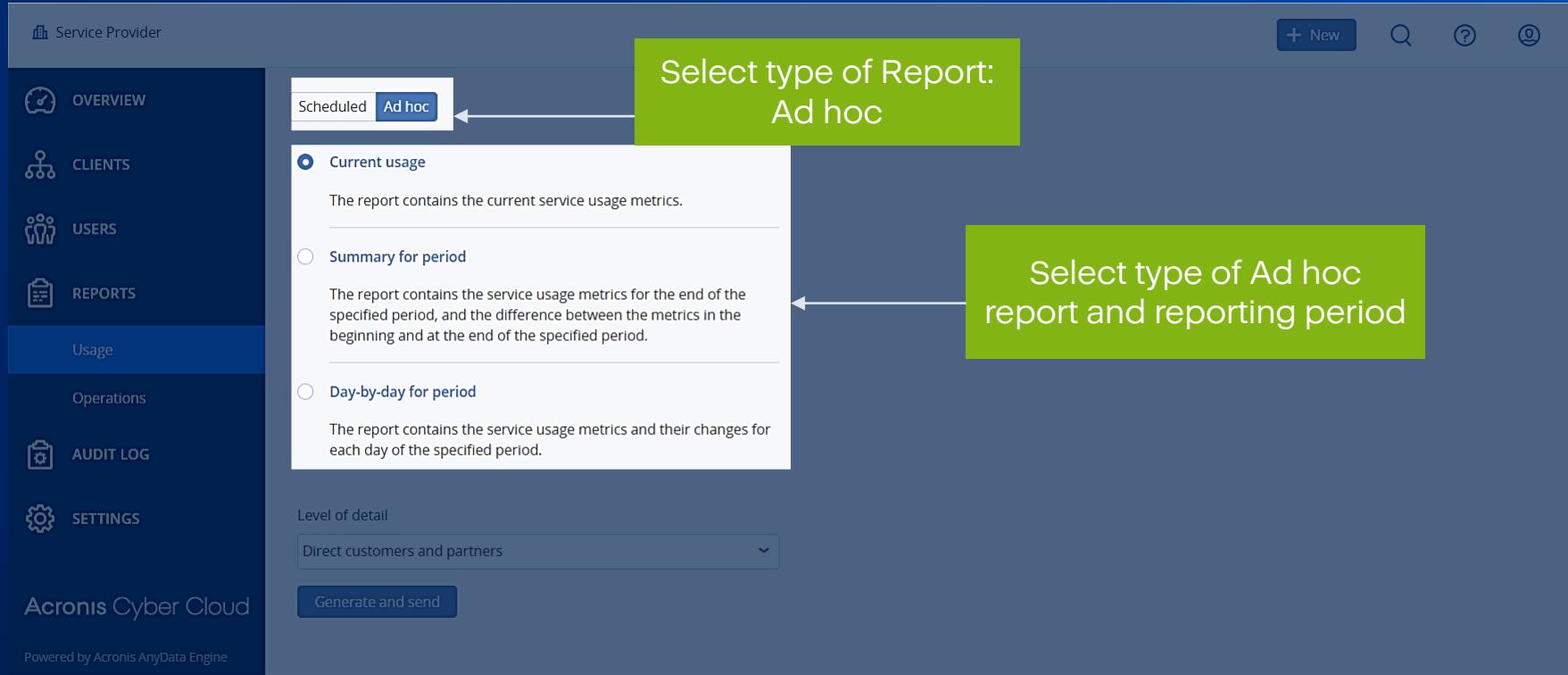
AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

# Managing Tenants – Reports> Usage Tab



The screenshot shows the 'Usage' tab in the Acronis Cyber Cloud tenant management interface. On the left, a sidebar lists navigation options: Overview, Clients, Users, Reports (selected), Usage (selected), Operations, Audit Log, and Settings. The main content area displays a 'Select type of Report' section. At the top of this section, there are two buttons: 'Scheduled' and 'Ad hoc' (which is highlighted with a green box). Below these buttons is a heading 'Select type of Report: Ad hoc'. The 'Ad hoc' section contains three options: 'Current usage' (selected, indicated by a blue dot), 'Summary for period', and 'Day-by-day for period'. Each option has a brief description. At the bottom of the 'Ad hoc' section, there is a 'Level of detail' dropdown set to 'Direct customers and partners' and a 'Generate and send' button.

Service Provider

+ New ? !

OVERVIEW

CLIENTS

USERS

REPORTS

Usage

Operations

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Select type of Report:  
Ad hoc

Current usage  
The report contains the current service usage metrics.

Summary for period  
The report contains the service usage metrics for the end of the specified period, and the difference between the metrics in the beginning and at the end of the specified period.

Day-by-day for period  
The report contains the service usage metrics and their changes for each day of the specified period.

Level of detail

Direct customers and partners

Generate and send

Select type of Ad hoc report and reporting period

# Managing Tenants – Reports> Usage Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Usage' tab selected in the sidebar. The main area displays options for generating reports:

- Select type of Report:** Ad hoc (highlighted in green)
- Select type of Ad hoc report and reporting period:** Options include "Current usage", "Summary for period", and "Day-by-day for period" (highlighted in green).
- Select Level of detail:** Direct customers and partners (highlighted in green)

Other visible elements include the Service Provider header, a navigation bar with '+ New', search, and help icons, and a sidebar with links for Overview, Clients, Users, Reports, Operations, Audit Log, Settings, and Acronis Cyber Cloud.

# Managing Tenants – Reports> Operations Tab

SGLAB.Demo.Provider > ~Training > ~Amos Project Igloo 21.03 > AD Cloud Tech 19-APR-2021

+ New

**OVERVIEW**

Search < Summary

Add widget Download Settings ...

**UNITS**

Alerts

- Backup scanning details
- Daily activities
- Data protection map
- Detected threats
- Discovered machines
- Disk health prediction
- Existing vulnerabilities
- Hardware inventory
- Patch management summary
- Software inventory
- Summary
- Weekly activities

**REPORTS**

Usage

**Operations**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

**Active alerts summary**

24 Total

- Suspicious activity is de... 15
- Activity failed 1
- VPN connection error 1
- A malicious process is ... 1
- Windows Defender Ant... 3
- Windows Defender Ant... 2
- Malware is detected an... 1

**Activities**

Time	Count
18 PM	1
12 May	2
06 AM	1
12 PM	4
06 PM	1
10 PM	1
02 AM	1
06 AM	1
10 AM	1
02 PM	1
06 PM	1

**Vulnerable machines**

6 Resources

- Secured 3
- Critical 0
- High 2
- Medium 1
- Low 0
- None 0

**Locations summary**

Location name	Location type	Current free space	Current size of backups	Current number of backups	Number of orphaned backu...	...
\\\192.168.217.192\Share 2\	Network share	92.67 GB	7.21 GB	1	0	
Online storage at Acronis ...	Cloud Storage	-	-	0	0	
\\192.168.217.191\Share 1\	Network share	92.48 GB	87.55 GB	2	0	
ad.tech	Cloud Storage	-	6.35 GB	1	0	

**Backup status**

Device name	Plan name	Last result	Device state	Last successful backup	Total caps	Number of successful ...	...

# Managing Tenants – Reports> Operations Tab

SGLAB.Demo.Provider > ~Training > ~Amos Project Igloo 21.03 > AD Cloud Tech 19-APR-2021

**OVERVIEW**

Search  Summary

**Alerts**

- Backup scanning details
- Daily activities
- Data protection map
- Detected threats
- Discovered machines
- Disk health prediction
- Existing vulnerabilities
- Hardware inventory
- Patch management summary
- Software inventory
- Summary
- Weekly activities

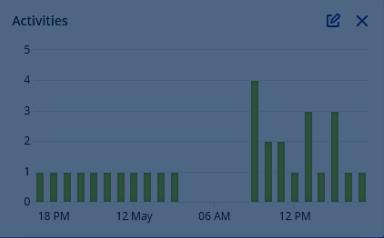
**Add report**

**Activities**

Active alerts summary

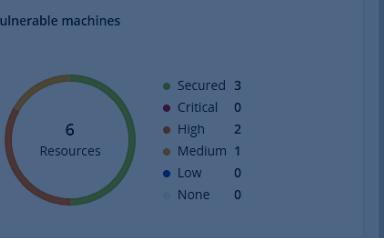
- Suspicious activity is detected 15
- Activity failed 1
- VPN connection error 1
- A malicious process is running 1
- Windows Defender Antivirus scan 3
- Windows Defender Antivirus scan 2
- Malware is detected and removed 1

Activities



Time	Activities
18 PM	1
19 PM	2
20 PM	2
21 PM	3
22 PM	2
23 PM	1
00 AM	4
01 AM	2
02 AM	3
03 AM	2
04 AM	1
05 AM	1
06 AM	1

Vulnerable machines



Severity Level	Count
Secured	3
Critical	0
High	2
Medium	1
Low	0
None	0

**Locations summary**

Location name	Location type	Current free space	Current size of backups	Current number of backups	Number of orphaned backups	Actions
\\\192.168.217.192\Share 2\	Network share	92.67 GB	7.21 GB	1	0	
Online storage at Acronis ...	Cloud Storage	-	-	0	0	
\\192.168.217.191\Share 1\	Network share	92.48 GB	87.55 GB	2	0	
ad.tech	Cloud Storage	-	6.35 GB	1	0	

**Backup status**

Device name	Plan name	Last result	Device state	Last successful backup	Total caps.	Number of successful caps.	Actions
							

**Add widget** **Download** **Settings** **Send** **...**

Search box

# Managing Tenants – Reports> Operations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Operations' tab selected in the sidebar. The main area displays several reports and metrics:

- Search box:** Located at the top left, with a green callout pointing to it.
- Types of reports:** A green callout pointing to a section containing a donut chart labeled '24 Total' and a bar chart showing activities over time.
- Active alerts summary:** Shows 24 total alerts, with a breakdown: Windows Defender Ant... 2 and Malware is detected an... 1.
- Activities:** A bar chart showing activity counts at 18 PM, 12 May, 06 AM, and 12 PM.
- Vulnerable machines:** A donut chart showing 6 resources with a breakdown: Secured 3, Critical 0, High 2, Medium 1, Low 0, and None 0.
- Locations summary:** A table showing storage locations with their types, free space, backup sizes, and backup counts.
- Backup status:** A table showing device names, plan names, last results, device states, last successful backups, total runs, and number of successful runs.

The sidebar also includes links for Overview, Units, Users, Reports, Usage, Audit Log, and Settings, along with a summary of existing vulnerabilities and hardware inventory.

# Managing Tenants – Reports> Operations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Operations' tab selected. On the left, a sidebar lists navigation items: Overview, Units, Users, Reports, Usage, Operations (selected), Audit Log, and Settings. Below the sidebar, it says 'Acronis Cyber Cloud' and 'Powered by Acronis AnyData Engine'. The main area is titled 'Search' and contains several report sections:

- Summary**: A circular gauge chart showing '24 Total' alerts.
- Active alerts summary**: A bar chart showing alert counts over time.
- Activities**: A list of recent activities.
- Locations summary**: A table showing storage locations and their metrics.
- Backup status**: A table showing backup device status.
- Vulnerable machines**: A chart showing the number of secured and vulnerable machines.

Annotations highlight specific features:

- A green box labeled 'Search box' points to the search bar at the top of the page.
- A green box labeled 'Types of reports' points to the list of report categories on the left.
- A large green box on the right contains the text: 'Add widget, Download report, Settings, Send as email, More actions'.

# Managing Tenants – Reports> Operations Tab

The screenshot shows the Acronis Cyber Protect interface with a dark blue header and sidebar. The sidebar on the left includes sections for Overview, Units, Users, Reports, Operations, Audit Log, and Settings. The main area displays various monitoring metrics like 'Vulnerable machines' and 'Backup status'. A green callout box labeled 'Add Report' points to a modal window titled 'Create report'. This modal lists several report templates:

- #CyberFit Score by machine: Shows summary of #CyberFit Score in the organization.
- 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: Report about unprotected locations.

At the bottom of the modal is a 'Create' button.

# Managing Tenants – Reports> Operations Tab

SGLAB.Demo.Provider > ~Training > ~Amos Project Igloo 21.03 > AD Cloud Tech 19-APR-2021

+ New

**OVERVIEW**

Search < Summary

**Alerts**

- Backup scanning details
- Daily activities
- Data protection map
- Detected threats
- Discovered machines
- Disk health prediction
- Existing vulnerabilities
- Hardware inventory
- Patch management summary
- Software inventory
- Summary
- Weekly activities

**Activities**

**Vulnerable machines**

**Locations summary**

Location name	Location type	Current free space	Current size of backups	Current number of backups	Number of orphaned backups	...
\192.168.217.192\Share 2\	Network share	92.67 GB	7.21 GB	1	0	
Online storage at Acronis ...	Cloud Storage	-	-	0	0	
//192.168.217.191\Share 1\	Network share	92.48 GB	87.55 GB	2	0	
ad.tech	Cloud Storage	-	6.35 GB	1	0	

**Backup status**

Device name	Plan name	Last result	Device state	Last successful backup	Total runs	Number of successful runs	...

**Add report**

# Managing Tenants – Reports> Operations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Operations' tab selected in the sidebar. The main area displays several widgets:

- Active alerts summary:** A donut chart showing 24 total alerts. A green callout box with the text "Edit Widget, Close Widget" points to the close button in the top right corner of this widget.
- Locations summary:** A table showing storage locations with their details:

Location name	Location type	Current free space	Current size of backups	Current number of backups	Number of orphaned backups
\\\192.168.217.192\Share 2\	Network share	92.67 GB	7.21 GB	1	0
Online storage at Acronis ...	Cloud Storage	-	-	0	0
\\\192.168.217.191\Share 1\	Network share	92.48 GB	87.55 GB	2	0
ad.tech	Cloud Storage	-	6.35 GB	1	0

- Backup status:** A table showing backup status for various devices:

Device name	Plan name	Last result	Device state	Last successful backup	Total runs	Number of successful r...
Device 1	Plan 1	Success	Up	2021-05-12 12:00	10	10
Device 2	Plan 2	Success	Up	2021-05-12 12:00	10	10
Device 3	Plan 3	Success	Up	2021-05-12 12:00	10	10

# Managing Tenants – Reports> Operations Tab

Report settings

OVERVIEW

CLIENTS

USERS

REPORTS

Usage

Operations

AUDIT LOG

SETTINGS

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

+ New

SEARCH

SAVE

CLOSE

Patch management

Patch installation status

1 Resources

Insta  
Rebo  
Faile

Name  
Patch management summary

Set one tenant for all widgets

Range  
30 days

General

Scheduled

Report settings and scheduling for Send as email

Add widget

Download

Settings

Send

...

Patch installation summary

Installation status Total number of patches

Installed 1

High severity Medium severity Low severity No severity

0 0 0 0

# Managing Tenants – Reports> Operations Tab

The screenshot shows the Acronis tenant management interface. On the left, there's a sidebar with icons for Overview, Clients, Users, Reports, Usage, Operations (which is selected), Audit Log, and Settings. The main area is titled "Patch management summary" and shows a circular icon with "1 Resources". Below it, there are sections for "Patch installation status" and "Missing updates by categories". A modal window titled "Send report" is open, prompting for "Recipients" (with "user1@example.com; user2@example.com" entered) and "File format" (set to "Excel and PDF"). At the bottom of the modal are "Cancel" and "Send" buttons. In the background, there's a green button with the text "Send as email immediately" and an upward arrow pointing towards the modal.

Acronis (14)

+ New ? !

OVERVIEW

← Patch management summary

CLIENTS

USERS

REPORTS

Usage

Operations

AUDIT LOG

SETTINGS

Patch installation status

Missing updates by categories

1 Resources

Insta  
Rebo  
Faile

Send report

Recipients  
user1@example.com; user2@example.com

File format  
Excel and PDF

C Cancel Send

High severity 0 Medium sev... 0 Low severity 0 No severity 0

Send as email immediately

# Managing Tenants – Reports> Operations Tab

SGLAB.Demo.Provider > ~Training > ~Amos Project Igloo 21.03 > AD Cloud Tech 19-APR-2021

+ New

**OVERVIEW**

Search

**Alerts**

- Backup scanning details
- Daily activities
- Data protection map
- Detected threats
- Discovered machines
- Disk health prediction
- Existing vulnerabilities
- Hardware inventory
- Patch management summary
- Software inventory
- Summary
- Weekly activities

**Activities**

Active alerts summary

24 Total

- Suspicious activity is de... 15
- VPN connection error 1
- Activity failed 1
- A malicious process is ... 1
- Malware is detected an... 1
- Windows Defender Ant... 3
- Windows Defender Ant... 2

Activities

Vulnerable machines

6 Resources

Locations summary

Location name	Location type	Current free space	Current size of backups	Current number of backups	Number of orphaned backu...	...
\\\192.168.217.192\Share 2\	Network share	92.67 GB	7.21 GB	1	0	
Online storage at Acronis ...	Cloud Storage	-	-	0	0	
\\192.168.217.191\Share 1\	Network share	92.48 GB	87.55 GB	2	0	
ad.tech	Cloud Storage	-	6.35 GB	1	0	

Backup status

Device name	Plan name	Last result	Device state	Last successful backup	Total runs	Number of successful r...	...

Add widget Download Settings Send

**Clone**  
**Export**  
**Dump data**  
**Delete report**

Sec...  
Cri...  
High...  
Medium 1  
Low 0  
None 0

# Managing Tenants – Reports> Operations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Operations' tab selected in the sidebar. The main area displays several dashboards and reports:

- Active alerts summary:** A circular chart showing 24 total alerts. The legend includes:
  - Suspicious activity is de... 15
  - VPN connection error 1
  - Activity failed 1
  - A malicious process is ... 1
  - Malware is detected an... 1
  - Windows Defender Ant... 3
  - Windows Defender Ant... 2
- Activities:** A bar chart showing activity counts over time (18 PM, 12 May, 06 AM, 12 PM). The counts fluctuate between 1 and 5.
- Resources:** A circular chart showing 6 resources. The legend indicates:
  - Secure 1
  - Critical 1
  - High 1
  - Medium 1
  - Low 0
  - None 0
- Locations summary:** A table listing storage locations with details like free space, backup size, and backup count. One entry is highlighted in yellow.
- Backup status:** A table showing backup progress for various devices.

A green callout box labeled "More actions" points to a context menu that appears when hovering over the three-dot ellipsis icon in the top right corner. The menu includes options: Clone, Export, Dump data, Delete report, and a separator line.

# Managing Tenants – Audit Log Tab

The screenshot shows the Acronis Cyber Cloud interface with the Audit Log tab selected. The left sidebar includes navigation links for Overview, Clients, Users, Reports, Audit Log (which is highlighted in blue), and Settings. The main area features a table of audit log entries with columns for Event, Severity, Date, Object name, Tenant, Initiator, Initiator's tenant, and IP. A search bar and filter results button are at the top of the table.

Event	Severity	Date	Object name	Tenant	Initiator	Initiator's tenant	IP
User signed in to the service	Informational	04/12/2020 6:06 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
User signed in to the service	Informational	04/12/2020 6:06 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
User signed in to the service	Informational	04/12/2020 3:35 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
User signed out from the service	Informational	04/12/2020 3:35 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
User signed in to the service	Informational	04/12/2020 2:56 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	185.151.16
User signed in to the service	Informational	04/12/2020 2:09 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
User signed out from the service	Informational	04/12/2020 2:09 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
User signed in to the service	Informational	04/12/2020 2:06 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
User signed in to the service	Informational	04/12/2020 2:06 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
User signed in to the service	Informational	04/12/2020 2:02 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
User signed out from the service	Informational	04/12/2020 1:57 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	MSSP Partner	MSSP	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	MSSP	MSSP	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	Customer 2	Cyber Protect Customer	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	Cyber Protect Customer	Cyber Protect Customer	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152

# Managing Tenants – Audit Log Tab

Acronis (14)

+ New ? o

**OVERVIEW**

**CLIENTS**

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Filter results  ?

Event Severity Date Object name Initiator Initiator unit IP

Event	Severity	Date	Object name	Initiator	Initiator unit	IP	
User signed in to the service	Informational	04/12/2020 6:06 PM UTC	Ron Eo (ron.eo@acronis.r...	Ron Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16	
User signed in to the service	Informational	04/12/2020 6:06 PM UTC	Ron Eo (ron.eo@acronis.r...	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152	
User signed in to the service	Informational	04/12/2020 3:35 PM UTC	Ron Eo (ron.eo@acronis.r...	Acronis (14)	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
User signed out from the service	Informational	04/12/2020 3:35 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
User signed in to the service	Informational	04/12/2020 2:56 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	185.151.16
User signed in to the service	Informational	04/12/2020 2:09 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
User signed out from the service	Informational	04/12/2020 2:09 PM UTC	Ron Eo (ron.eo@acronis.r...	Acronis (14)	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
User signed in to the service	Informational	04/12/2020 2:06 PM UTC	Ron Eo (ron.eo@acronis.r...	Acronis (14)	Ron Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
User signed in to the service	Informational	04/12/2020 2:06 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
User signed in to the service	Informational	04/12/2020 2:02 PM UTC	Ron Eo (ron.eo@acronis.r...	Acronis (14)	Ron Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
User signed out from the service	Informational	04/12/2020 1:57 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	MSSP Partner	MSSP	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	MSSP	MSSP	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	Customer 2	Cyber Protect Customer	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
Tenant was updated	Notice	04/12/2020 1:56 PM UTC	Cyber Protect Customer	Cyber Protect Customer	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152

Search by object, unit, initiator, initiator unit

# Managing Tenants – Audit Log Tab

The screenshot shows the Acronis Cyber Cloud interface with the Audit Log tab selected. The left sidebar includes links for Overview, Clients, Users, Reports, Audit Log (selected), and Settings. The main area displays an audit log table with the following columns: Date, Object name, Tenant, Initiator, Initiator's tenant, and IP. The table lists various events such as user sign-ins, tenant updates, and administrative actions across different tenants and initiators. A filter sidebar on the left allows users to refine results by Event type (Not selected), Severity (Any), and Date (Before 04/12/2020). A search bar and a 'Clear filters' button are also present.

Date	Object name	Tenant	Initiator	Initiator's tenant	IP
2020-04-12 20:06 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
2020-04-12 20:06 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 20:35 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 20:35 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
2020-04-12 20:56 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	185.151.16
2020-04-12 20:09 PM UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
2020-04-12 20:09 PM UTC	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 20:06 PM UTC	User signed in to the service	Informational	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
2020-04-12 20:06 PM UTC	User signed in to the service	Informational	demo.admin	Customer 2	39.109.152
2020-04-12 20:02 PM UTC	User signed in to the service	Informational	Ron.Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
2020-04-12 19:57 PM UTC	User signed out from the service	Informational	demo.admin	Customer 2	39.109.152
2020-04-12 19:56 PM UTC	Tenant was updated	Notice	MSSP Partner	MSSP	39.109.152
2020-04-12 19:56 PM UTC	Tenant was updated	Notice	MSSP	MSSP	39.109.152
2020-04-12 19:56 PM UTC	Tenant was updated	Notice	Customer 2	Cyber Protect Customer	39.109.152
2020-04-12 19:56 PM UTC	Tenant was updated	Notice	Cyber Protect Customer	Cyber Protect Customer	39.109.152

# Managing Tenants – Audit Log Tab

The screenshot shows the Acronis Cyber Cloud interface with the Audit Log tab selected. The left sidebar includes links for Overview, Clients, Users, Reports, Audit Log (selected), and Settings. The main area displays an audit log table with columns: Date, Object name, Tenant, Initiator, Initiator's tenant, and IP. A green rectangular box highlights the 'Filter results' sidebar, which contains fields for Event type (Not selected), Severity (Any), and a date range (Before 04/12/2020). An 'Apply' button is at the bottom of the sidebar. The table lists several audit events, such as users signing in and out and tenants being updated.

Date	Object name	Tenant	Initiator	Initiator's tenant	IP
2020-04-12 20:06 UTC	Ron Ed...	Acronis (14)	Ed (ron.eo@acronis.r...	Acronis (14)	185.151.16
2020-04-12 20:06 UTC	Ron Ed...	Acronis (14)	Ed (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 20:35 UTC	Ron Ed...	Acronis (14)	Ed (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 20:35 UTC	demo...	Customer 2	demo.admin	Customer 2	39.109.152
2020-04-12 20:56 UTC	demo.admin	Customer 2	demo.admin	Customer 2	185.151.16
2020-04-12 20:09 UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
2020-04-12 20:09 UTC	Ron Eo (ron.eo@acronis.r...	Acronis (14)	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 20:06 UTC	Ron Eo (ron.eo@acronis.r...	Acronis (14)	Ron Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
2020-04-12 20:02 UTC	Ron Eo (ron.eo@acronis.r...	Acronis (14)	Ron Eo (ron.eo@acronis.r...	Acronis (14)	185.151.16
2020-04-12 19:57 UTC	demo.admin	Customer 2	demo.admin	Customer 2	39.109.152
2020-04-12 19:56 UTC	MSSP Partner	MSSP	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 19:56 UTC	MSSP	MSSP	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 19:56 UTC	Customer 2	Cyber Protect Customer	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152
2020-04-12 19:56 UTC	Cyber Protect Customer	Cyber Protect Customer	Ron Eo (ron.eo@acronis.r...	Acronis (14)	39.109.152

# Managing Tenants – Settings > Locations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Locations' tab selected in the sidebar. The main area displays a table of locations with columns for Name, Service, Inherited, and Occupied space.

Name	Service	Inherited	Occupied space
Acronis Cloud			
baas-fes-sg1.acronis.com	Backup	Yes	0 GB
Disaster Recovery Storage	Disaster Recovery	Yes	0 GB
Acronis Cloud (Files)			
sg2-s3gw.acronis.com	File Sync & Share	Yes	0 GB

Buttons at the top right include '+ New', a magnifying glass for search, and help icons. The sidebar also includes links for Overview, Clients, Users, Reports, Audit Log, and Settings.

# Managing Tenants – Settings > Locations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Locations' tab selected in the sidebar. The main area displays a list of locations with columns for Name, Service, Inherited, and Occupied space.

Name	Service	Inherited	Occupied space
Acronis Cloud			
baas-fes-sg1.acronis.com	Backup	Yes	0 GB
Disaster Recovery Storage	Disaster Recovery	Yes	0 GB
Acronis Cloud (Files)			
sg2-s3gw.acronis.com	File Sync & Share	Yes	0 GB

**Add location** button

**Add backup storage** button

**Service Provider** icon

**+ New** button

**?** icon

**?** icon

**CLIENTS**

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

**Locations** (selected)

**Branding**

**Acronis Cyber Cloud**

Powered by Acronis AnyData Engine

# Managing Tenants – Settings > Locations Tab

The screenshot shows the Acronis Cyber Infrastructure tenant management interface. The left sidebar has a 'Service Provider' icon at the top, followed by a green 'Add location' button, and then a list of categories: CLIENTS, USERS, REPORTS, AUDIT LOG, SETTINGS, Locations (which is highlighted in blue), and Branding. Below these is a section titled 'Acronis Cyber Cloud' with the subtext 'Powered by Acronis AnyData Engine'. The main content area has a header with 'Service Provider' and a search bar. It features a large green callout box in the upper right corner with the text 'Download Acronis Cyber Infrastructure ISO'. Below the header are two buttons: '+ New' and a search icon. A row of icons for 'CLIENTS', 'USERS', 'REPORTS', 'AUDIT LOG', and 'SETTINGS' follows. The main table has columns for 'Name', 'Service', 'Inherited', and 'Occupied space'. The data table contains the following rows:

Name	Service	Inherited	Occupied space
Acronis Cloud ↑			
baas-fes-sg1.acronis.com	Backup	Yes	0 GB
Disaster Recovery Storage	Disaster Recovery	Yes	0 GB
Acronis Cloud (Files)			
sg2-s3gw.acronis.com	File Sync & Share	Yes	0 GB

# Managing Tenants – Settings > Locations Tab

The screenshot shows the Acronis Cyber Infrastructure tenant management interface. The left sidebar has a dark blue background with white icons and labels: Service Provider, Add location (highlighted in green), CLIENTS, USERS, REPORTS, AUDIT LOG, SETTINGS (highlighted in green), Locations (selected), Branding, API integrations, and Acronis Cyber Cloud. The main content area has a light blue header with a dark blue background below it. The header includes a 'Service Provider' icon, a search bar with a magnifying glass icon, and three help icons. Below the header is a green button labeled 'Download Acronis Cyber Infrastructure ISO'. The main content area features a table titled 'Locations' with columns: Name, Service, Inherited, and Occupied space. The table lists three entries under 'Acronis Cloud': 'baas-fes-sg1.acronis.com' (Backup, Yes, 0 GB), 'Disaster Recovery Storage' (Disaster Recovery, Yes, 0 GB), and 'sg2-s3gw.acronis.com' (File Sync & Share, Yes, 0 GB). A large green box at the bottom center contains the text 'List of cloud storages' with an upward arrow pointing to the table. A small green box at the top right of the table contains the text 'Add location' and 'Add backup storage'.

Name	Service	Inherited	Occupied space
Acronis Cloud			
baas-fes-sg1.acronis.com	Backup	Yes	0 GB
Disaster Recovery Storage	Disaster Recovery	Yes	0 GB
Acronis Cloud (Files)			
sg2-s3gw.acronis.com	File Sync & Share	Yes	0 GB

# Managing Tenants – Settings > Locations Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Locations' tab selected in the sidebar. The main area displays a table of locations with columns for Name, Service, Inherited, and Occupied space.

Name	Service	Inherited	Occupied space
Acronis Cloud			
baas-fes-sg1.acronis.com	Backup	Yes	0 GB
Disaster Recovery Storage	Disaster Recovery	Yes	0 GB
Acronis Cloud (Files)			
sg2-s3gw.acronis.com	File Sync & Share	Yes	0 GB

Buttons at the top right include '+ New', a magnifying glass for search, and help icons. The sidebar also includes links for Overview, Clients, Users, Reports, Audit Log, and Settings.

# Managing Tenants – Settings > Locations Tab

Acronis (1)

+ New ? ? ?

OVERVIEW

Add location Add backup storage

CLIENTS

USERS

REPORTS

AUDIT LOG

SETTINGS

Locations

Branding

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Name ↓

Acronis Cloud ↑

Cloud icon betacloud\_s3

Cloud icon Default disaster recovery infrastructure

Cloud icon fes-eu3-baas.acronis.com

Occupied space

0 GB

0 GB

7.73 GB

Add location

Specify the location name

Cancel Done

Add custom Location name for grouping 1 or more added storage

# Managing Tenants – Settings > Locations Tab

Acronis (14)

+ New ? Q o

**OVERVIEW**

**CLIENTS**

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Locations

Branding

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Add backup storage X

 Acronis Cyber Infrastructure

Join local nodes into a highly available software-defined storage cluster or use an external NFS or object storage (S3, Azure, Swift) as the storage backend for the backed-up data. At least one physical or virtual machine is required for deployment.

[Download ISO](#)

Quick start guide | Administrator's guide

More deployment options

Deploy Acronis Cyber Infrastructure in a public cloud as a gateway to cloud's object storage. The following platforms are supported: Google Cloud Platform, Amazon AWS, Microsoft Azure, Yandex Cloud, IBM Cloud, and Alibaba Cloud.

 [Amazon Machine Image](#)  
[Quick start guide](#)

 [Microsoft Azure virtual machine image](#)  
[Quick start guide](#)

# Managing Tenants – Settings > Locations Tab

Acronis (14)

+ New

OVERVIEW

CLIENTS

USERS

REPORTS

AUDIT LOG

Click to download the latest Acronis Cyber Infrastructure ISO image

Acronis Cyber Cloud  
Powered by Acronis AnyData Engine

Add backup storage

 Acronis Cyber Infrastructure

Join local nodes into a highly available software-defined storage cluster or use an external NFS or object storage (S3, Azure, Swift) as the storage backend for the backed-up data. At least one physical or virtual machine is required for deployment.

[Download ISO](#)

Quick start guide | Administrator's guide

More deployment options

Deploy Acronis Cyber Infrastructure in a public cloud as a gateway to cloud's object storage. The following platforms are supported: Google Cloud Platform, Amazon AWS, Microsoft Azure, Yandex Cloud, IBM Cloud, and Alibaba Cloud.

 Amazon Machine Image  
[Quick start guide](#)

 Microsoft Azure virtual machine image  
[Quick start guide](#)

# Managing Tenants – Settings > Locations Tab

The screenshot shows the Acronis interface with a sidebar containing 'OVERVIEW', 'CLIENTS', 'USERS', 'REPORTS', and 'AUDIT LOG'. A green callout box on the left says 'Click to download the latest Acronis Cyber Infrastructure ISO image' with an arrow pointing to the 'Download ISO' button in the central dialog. Another green callout box at the bottom right says 'Click to redirect to the respective vendor's webpage' with arrows pointing to the 'Quick start guide' links for AWS and Microsoft Azure.

Acronis (14) + New 🔍 ⓘ

OVERVIEW CLIENTS USERS REPORTS AUDIT LOG

Click to download the latest Acronis Cyber Infrastructure ISO image

Add backup storage

**A** Acronis Cyber Infrastructure

Join local nodes into a highly available software-defined storage cluster or use an external NFS or object storage (S3, Azure, Swift) as the storage backend for the backed-up data. At least one physical or virtual machine is required for deployment.

**Download ISO**

Quick start guide | Administrator's guide

More deployment options

Deploy Acronis Cyber Infrastructure in a public cloud as a gateway to cloud's object storage. The following platforms are supported: Google Cloud Platform, Amazon AWS, Microsoft Azure, Yandex Cloud, IBM Cloud, and Alibaba Cloud.

**aws** Amazon Machine Image Quick start guide

**Microsoft Azure** Microsoft Azure virtual machine image Quick start guide

Click to redirect to the respective vendor's webpage

# Managing Tenants – Settings > Branding Tab

Service Provider

+ New

USERS REPORTS AUDIT LOG SETTINGS Locations **Branding** API clients Security Integration

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

## Branding

White label | Reset to defaults | Disable branding

The branding options will be applied to all direct and indirect child partners/folders and customers of the tenant where the branding is configured.

### Appearance

Service name: Acronis Cyber Cloud

Logo and color scheme:

Branding

# Managing Tenants – Settings > Branding Tab

The screenshot shows the 'Branding' tab in the Acronis Cyber Cloud tenant management interface. The left sidebar includes 'Service Provider', 'USERS', 'REPORTS', 'AUDIT LOG', 'SETTINGS', 'Locations', 'Branding' (which is selected and highlighted in blue), 'API clients', 'Security', and 'Integration'. The main content area has a green header bar with the text 'Branding options'. Below it is a note: 'The branding options will be applied to all direct and indirect child partners/folders and customers of the tenant where the branding is configured.' A button bar at the top right contains '+ New', a magnifying glass icon, a question mark icon, and a help icon. The 'Appearance' section displays the service name 'Acronis Cyber Cloud' and a logo preview labeled '224x64'. Other sections include 'Logo and color scheme' and 'Font and colors'.

# Managing Tenants – Settings > API Clients Tab

Service Provider

+ New   

-  USERS
-  REPORTS
-  AUDIT LOG
-  SETTINGS
- Locations
- Branding
- API clients**
- Security
- Integration

Acronis Cyber Cloud  
Powered by Acronis AnyData Engine



## API clients

API clients are used for accessing the account management and service APIs for integration purposes. You can create and manage the API clients in the current section

[Create API client](#)

# Managing Tenants – Settings > API Clients Tab

Service Provider

USERS

REPORTS

AUDIT LOG

SETTINGS

Locations

Branding

API clients

Security

Integration

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

API clients

API clients are used for accessing the account management and service APIs for integration purposes. You can create and manage the API clients in the current section

Click to create new API Client

Create API client

# Managing Tenants – Settings > Security Tab

The screenshot shows the 'Settings > Security' tab for the tenant 'Steve Brining LLC'. The left sidebar lists various settings categories: USERS, REPORTS, AUDIT LOG, SETTINGS, Locations, Branding, API clients, Security (which is selected and highlighted in blue), Integration, and Agents update. The main content area contains three configuration sections:

- Login control**: A description stating "Specify the IP addresses from which members of this tenant can sign in to the web interface or access API. This setting does not apply to the child tenants of this tenant" with a toggle switch set to off.
- Two-factor authentication**: A description stating "This is a method of identification that provides an effective account protection by requesting authentication data of two different types" with a toggle switch set to off.
- Support access**: A description stating "Grant full access to administrators of the parent tenants: modify properties; manage tenants, users, and services; access backups, and other resources. If it is turned off, administrators from the parent tenant will not be able to access or manage anything inside the child tenant (e.g. tenants, users, services, backups, and other resources)." with a toggle switch set to on.

At the bottom of the page, it says "Powered by Acronis AnyData Engine".

# Managing Tenants – Settings > Security Tab

The screenshot shows the Acronis Cyber Cloud web interface. The top navigation bar includes a logo for 'Steve Brining LLC', a search bar, and a '+ New' button. The left sidebar lists several options: USERS, REPORTS, AUDIT LOG, SETTINGS (which is selected and highlighted in blue), Locations, Branding, API clients, Security (selected), Integration, and Agents update. The main content area is titled 'Security settings'. It contains three sections: 'Login control', 'Two-factor authentication', and 'Support access'. Each section has a description and a toggle switch. The 'Login control' and 'Two-factor authentication' switches are off (grey). The 'Support access' switch is on (green).

Steve Brining LLC

+ New

REPORTS

AUDIT LOG

SETTINGS

Locations

Branding

API clients

Security

Integration

Agents update

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Login control

Specify the IP addresses from which members of this tenant can sign in to the web interface or access API. This setting does not apply to the child tenants of this tenant

Two-factor authentication

This is a method of identification that provides an effective account protection by requesting authentication data of two different types

Support access

Grant full access to administrators of the parent tenants: modify properties; manage tenants, users, and services; access backups, and other resources. If it is turned off, administrators from the parent tenant will not be able to access or manage anything inside the child tenant (e.g. tenants, users, services, backups, and other resources).

Security settings

# Managing Tenants – Settings > Security Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'Service Provider' role selected. The left sidebar includes links for USERS, REPORTS, AUDIT LOG, SETTINGS (which is selected), Locations, Branding, API clients, Security (highlighted in blue), and Integration. The main content area is titled 'Login control' and describes specifying allowed IP addresses for tenant members. A note cautions against using incorrect IP addresses. Below is a text input field for 'Allowed IP addresses' with a placeholder and a note about entering at least one address. A list of examples is provided: IP addresses: 192.0.2.0;192.0.2.1, IP ranges: 192.0.2.0-192.0.2.255, and Subnets: 192.0.2.0/24. At the bottom are 'Cancel' and 'Save' buttons.

Service Provider

+ New ? !

USERS

REPORTS

AUDIT LOG

SETTINGS

Locations

Branding

API clients

Security

Integration

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Login control

Specify the IP addresses from which members of this tenant can sign in to the web interface or access API. This setting does not apply to the child tenants of this tenant

Please pay attention to the examples below

Using incorrect IP addresses will result in the inability to log in for all members of your tenant. Contact your Internet Service Provider to get the external IP addresses for your organization.

Allowed IP addresses

Enter at least one IP address.

- IP addresses: 192.0.2.0;192.0.2.1
- IP ranges: 192.0.2.0-192.0.2.255
- Subnets: 192.0.2.0/24

Cancel Save

Two-factor authentication

# Managing Tenants – Settings > Security Tab

The screenshot shows the Acronis Cyber Cloud web interface. On the left, a sidebar menu includes options like Service Provider, USERS, REPORTS, AUDIT LOG, and a highlighted 'Specify allowed IP addresses' button. Below these are API clients, Security (which is selected), and Integration. At the bottom of the sidebar is the Acronis Cyber Cloud logo and a note about the AnyData Engine.

The main content area is titled 'Login control'. It explains that users can specify IP addresses from which members of the tenant can sign in to the web interface or access the API. A green toggle switch indicates the feature is enabled. A note cautions against entering incorrect IP addresses, stating it will prevent all members from logging in. Below this is a text input field labeled 'Allowed IP addresses' with a placeholder 'Enter at least one IP address.' and a list of examples: IP addresses: 192.0.2.0;192.0.2.1, IP ranges: 192.0.2.0-192.0.2.255, and Subnets: 192.0.2.0/24. At the bottom right are 'Cancel' and 'Save' buttons.

# Managing Tenants – Settings > Security Tab

The screenshot shows the 'Settings > Security' tab in the Acronis Cyber Cloud interface. A large green box highlights the 'Enable 2FA' button in the 'Login control' section. An arrow points from this green box to a modal dialog titled 'Enable two-factor authentication'. The dialog contains the following text: 'All users of the organization will not be able to sign in until they configure two-factor authentication in their accounts.' It features 'Cancel' and 'Enable' buttons. Below the dialog, another section titled 'Support access' is visible, with the sub-instruction 'Allow administrators from parent tenants to manage this tenant' and a toggle switch.

Service Provider

+ New

?

?

USERS

REPORT

AUDIT L

SETTINGS

Locations

Branding

API clients

Security

Integration

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Enable 2FA

Login control

Enable two-factor authentication

All users of the organization will not be able to sign in until they configure two-factor authentication in their accounts

Cancel

Enable

Support access

Allow administrators from parent tenants to manage this tenant

# Managing Tenants – Settings > Integrations Tab

Steve Brining LLC

+ New   

Available integrations

-  Autotask
-  APS STANDARD
-  ConnectWise Automate
-  ConnectWise Command
-  ConnectWise Manage
-  cPanel
-  flexiant™  
your cloud simplified
-  HostBill
-  Kaseya®

USERS

REPORTS

AUDIT LOG

SETTINGS

Locations

Branding

API clients

Security

Integration

Agents update

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

# Managing Tenants – Settings > Integrations Tab

The screenshot shows the Acronis AnyData Engine tenant management interface. On the left, a sidebar lists various settings categories: USERS, REPORTS, Supported PSA & RMM tools (highlighted in green), Branding, API clients, Security, Integration (selected), Agents update, and Acronis Cyber Cloud. At the bottom of the sidebar, it says "Powered by Acronis AnyData Engine". The main area is titled "Available integrations" and displays a grid of nine integration cards:

Autotask	APS STANDARD	ConnectWise CERTIFIED INTEGRATOR
Autotask	APS Cloud Application Standard	ConnectWise Automate
ConnectWise Command	ConnectWise CERTIFIED INTEGRATOR	cPanel
flexiant™ your cloud simplified	HostBill	Kaseya®

A blue arrow points from the "Supported PSA & RMM tools" button in the sidebar to the first row of the integration grid.

# Managing Tenants – Overview > Usage Tab

The screenshot shows a web-based tenant management interface for Acronis Cyber Cloud. The top navigation bar includes 'Service Provider' and 'Customer 1'. Below the navigation is a toolbar with '+ New', a search icon, a help icon, and a refresh icon. On the left, a sidebar menu lists 'OVERVIEW' (selected), 'Usage' (highlighted in blue), 'Operations', 'UNITS', 'USERS', 'REPORTS', 'AUDIT LOG', and 'SETTINGS'. The main content area has a green background. It contains descriptive text and a bulleted list:

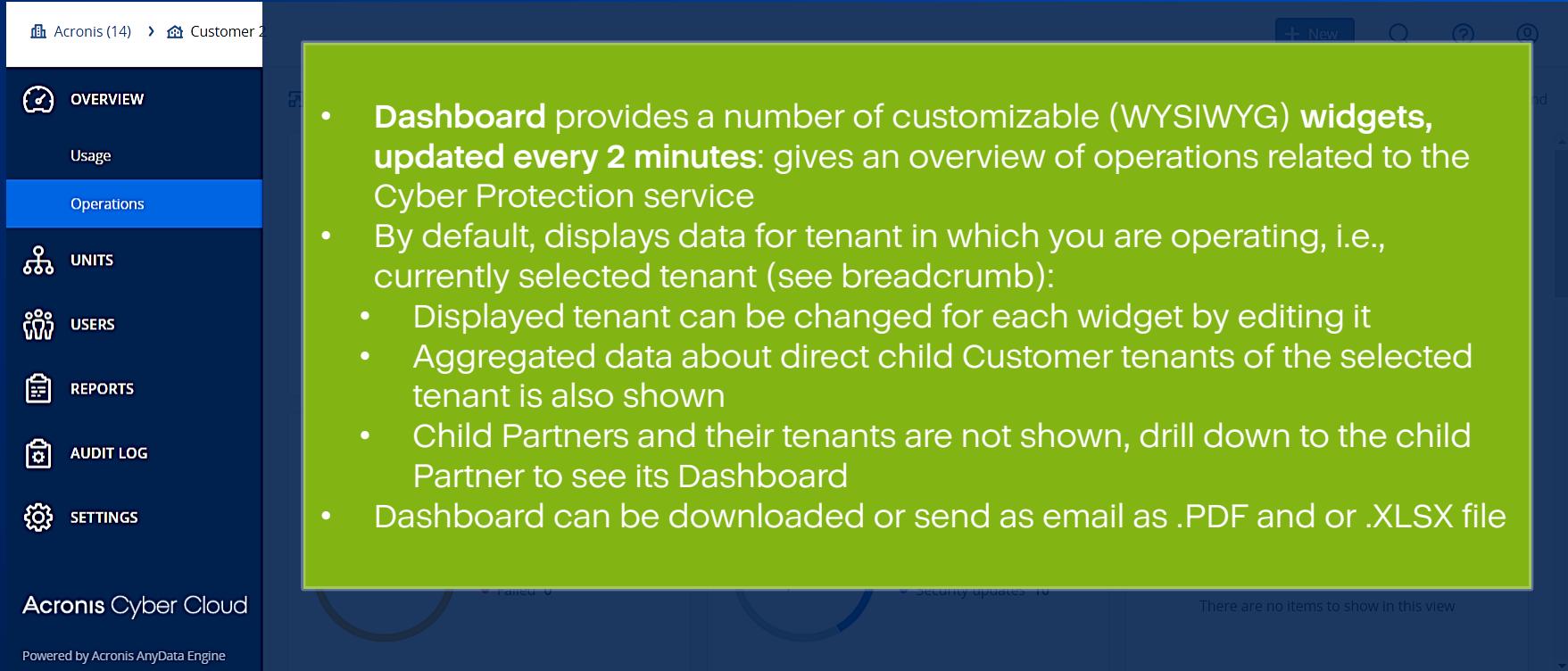
Provides an overview of the service usage and enables access to the respective service consoles:

- **Cyber Protection** User service console
- **File Sync & Share** Administrator and User service consoles
- **Physical Data** Shipping User service console
- **Notary service console**

Depending on the offering configured by parent tenant, certain services may not be available

At the bottom, there's a table with columns for 'Web hosting servers' (0) and 'Websites' (0). The footer indicates 'Acronis Cyber Cloud' and 'Powered by Acronis AnyData Engine'.

# Managing Tenants – Overview > Operations Tab



The screenshot shows the Acronis Cyber Cloud interface. At the top left, there's a breadcrumb navigation: Acronis (14) > Customer 2. The top right features standard UI elements: a '+' New button, a search icon, a help icon, and a user profile icon. On the left, a vertical sidebar menu has several items: OVERVIEW (selected), Usage, Operations (highlighted in blue), UNITS, USERS, REPORTS, AUDIT LOG, and SETTINGS. Below the sidebar is the title "Acronis Cyber Cloud". The main content area has a green header box containing the following bullet points:

- **Dashboard** provides a number of customizable (WYSIWYG) **widgets**, **updated every 2 minutes**: gives an overview of operations related to the Cyber Protection service
- By default, displays data for tenant in which you are operating, i.e., currently selected tenant (see breadcrumb):
  - Displayed tenant can be changed for each widget by editing it
  - Aggregated data about direct child Customer tenants of the selected tenant is also shown
  - Child Partners and their tenants are not shown, drill down to the child Partner to see its Dashboard
  - Dashboard can be downloaded or send as email as .PDF and or .XLSX file

At the bottom of the main content area, there are two status messages: "There are no items to show in this view" and "Security updates 10".

# Managing Tenants – Overview > Users Tab

The screenshot shows the Acronis Cyber Cloud interface with the 'OVERVIEW' tab selected. The 'USERS' tab is highlighted in blue, indicating it is the active tab. A green callout box highlights this tab and provides the following list of features:

- Allows **Partner or Customer Administrators** to view and manage user accounts:
  - View usage of all user accounts belonging to the tenant
  - Click on the row of a user account to view and modify: **General information | Services and roles | Settings (for email notifications)**

# Managing Tenants – Client/Unit Tab

The screenshot shows the Acronis Cyber Cloud web interface. The left sidebar has a dark blue background with white icons and text. The 'CLIENTS' icon is highlighted with a blue background, indicating it is the active tab. The main content area shows a list of tenants under 'Customer 1'. A large green rectangular callout box is overlaid on the right side of the tenant list, containing a bulleted list of features. The bottom of the interface includes a footer with the Acronis logo and some small text.

- Allows **Partner or Customer Administrators** to view and manage all child tenants:
  - View usage of all child tenants
  - Click on the row of a child tenant to view and modify: **Services/Editions and Offering Items | General information | Contact information**
  - Click on the **name** of the child tenant to drill down into the child tenant's hierarchy:
    - **Allow administrators from parent tenants to manage this tenant** setting must be enabled in child tenant's Security settings
    - View and modify settings of entire hierarchy (all tenants and accounts) of child tenant

# Managing Tenants – Reports > Usage Tab

The screenshot shows the Acronis Cyber Cloud interface with a dark blue header and sidebar. The sidebar on the left has icons for Service Provider, Overview, Clients, Users, Reports (which is selected and highlighted in blue), Operations, Audit Log, and Settings. The main content area is titled 'Usage'. It shows three report types: 'Scheduled' (highlighted with a white box and a callout arrow), 'Current usage', and 'Summary for period'. The 'Scheduled' section includes a description and a dropdown for 'Level of detail' set to 'Direct customers and partners'. A large green callout box on the right side contains the following text:

Two types of usage reports available:

- **Scheduled:**
  - Monthly report sent on the 2nd day of each month to all tenant Administrators
  - Contains usage summary for the last full calendar month
  - Level of detail can be selected, from Direct customers and partners to All customers and partners (including account details)

# Managing Tenants – Reports > Usage Tab

Service Provider

**OVERVIEW**

**CLIENTS**

**USERS**

**REPORTS**

**Usage**

**Operations**

**AUDIT LOG**

**SETTINGS**

Acronis Cyber Cloud

Powered by Acronis AnyData Engine

Scheduled    **Ad hoc**

Current usage  
The report contains the current service usage metrics.

Summary for period  
The report contains the service usage metrics for the end of the specified period, and the difference between the metrics in the beginning and at the end of the specified period.

Day-by-day for period  
The report contains the service usage metrics and their changes for each day of the specified period.

Level of detail  
Direct customers and partners

Generate and send

+ New    ?    !

Two types of usage reports available:

- **Ad hoc:**
  - Ad-hoc report generated and sent immediately to the logged in Administrator account
  - Reporting period can be selected, from Current usage to Day-by-day for period where the time period can be customized
  - Level of detail can be selected, from Direct customers and partners to All customers and partners (including account details)

# Managing Tenants – Reports > Usage Tab

The screenshot shows the Acronis Cyber Cloud web interface. On the left, a vertical sidebar menu is visible with the following items:

- Service Provider
- OVERVIEW
- CLIENTS
- USERS
- REPORTS
- Usage** (highlighted in blue)
- Operations
- AUDIT LOG
- SETTINGS

Below the sidebar, the main content area has a dark header bar with icons for 'New', 'Search', 'Help', and 'Logout'. The main body of the page is titled 'Usage' and contains several sections of text and dropdown menus. A large green rectangular callout box highlights the following list of bullet points:

- Reports are sent as email with two attachments (.csv and .html)
- Email body will **include Date of report generation, Reporting period and Level of detail information**
- Attachments will contain the following details:
  - Tenant name and type
  - Service usage metrics

At the bottom of the main content area, there is a blue button labeled 'Generate and send'.

# Managing Tenants – Reports > Operations Tab

The screenshot shows the Acronis Cyber Cloud web interface. The left sidebar has a dark blue background with white icons and text. The 'Operations' tab is highlighted with a blue background. Other tabs include Overview, Units, Users, Reports, Audit Log, and Settings. The main content area has a light gray header with the tenant name 'SGLAB.Demo.Provider'. Below the header is a navigation breadcrumb: 'Training > ~Amos Project Igloo 21.03 > AD Cloud Tech 19-APR-2021'. To the right of the breadcrumb are several small icons: a plus sign for 'New', a magnifying glass for 'Search', a person icon, a question mark, and a gear icon. The main content area contains a large green box with the following bullet points:

- Operations report are widget-based similar to **Dashboard** in **Overview** > Operations tab
- Several pre-defined **Reports** are available and more can be added
- By default, all widgets in a **Report** show the summary information for the tenant in which you are operating:
  - Individual widgets can be configured to show information about a specific tenant instead of a summary by clicking on the **Edit** button for the widget
  - To configure all widgets at once to show information about a specific tenant, go to **Settings** instead

# Managing Tenants – Reports > Operations Tab

The screenshot shows the Acronis Cyber Cloud web interface. The left sidebar has a dark blue background with white icons and text. The 'Operations' tab is highlighted with a blue background. The main content area has a light gray background. At the top, there's a breadcrumb navigation: SGLAB.Demo.Provider > Training > ~Amos Project Igloo 21.03 > AD Cloud Tech 19-APR-2021. To the right of the breadcrumb are several small icons: a plus sign for 'New', a magnifying glass for 'Search', a person icon, a question mark, and a gear icon. Below the breadcrumb, there's a 'Search' input field and a list of report categories. The 'Reports' category is selected, showing sub-options like 'Alerts', 'Backup scanning', 'Daily activities', 'Data protection', 'Detected threats', 'Discovered machines', 'Disk health prediction', 'Existing vulnerabilities', 'Hardware inventory', 'Patch management', 'Software inventory', 'Summary', and 'Weekly activities'. A large green callout box is overlaid on the right side of the screen, containing the following bullet points:

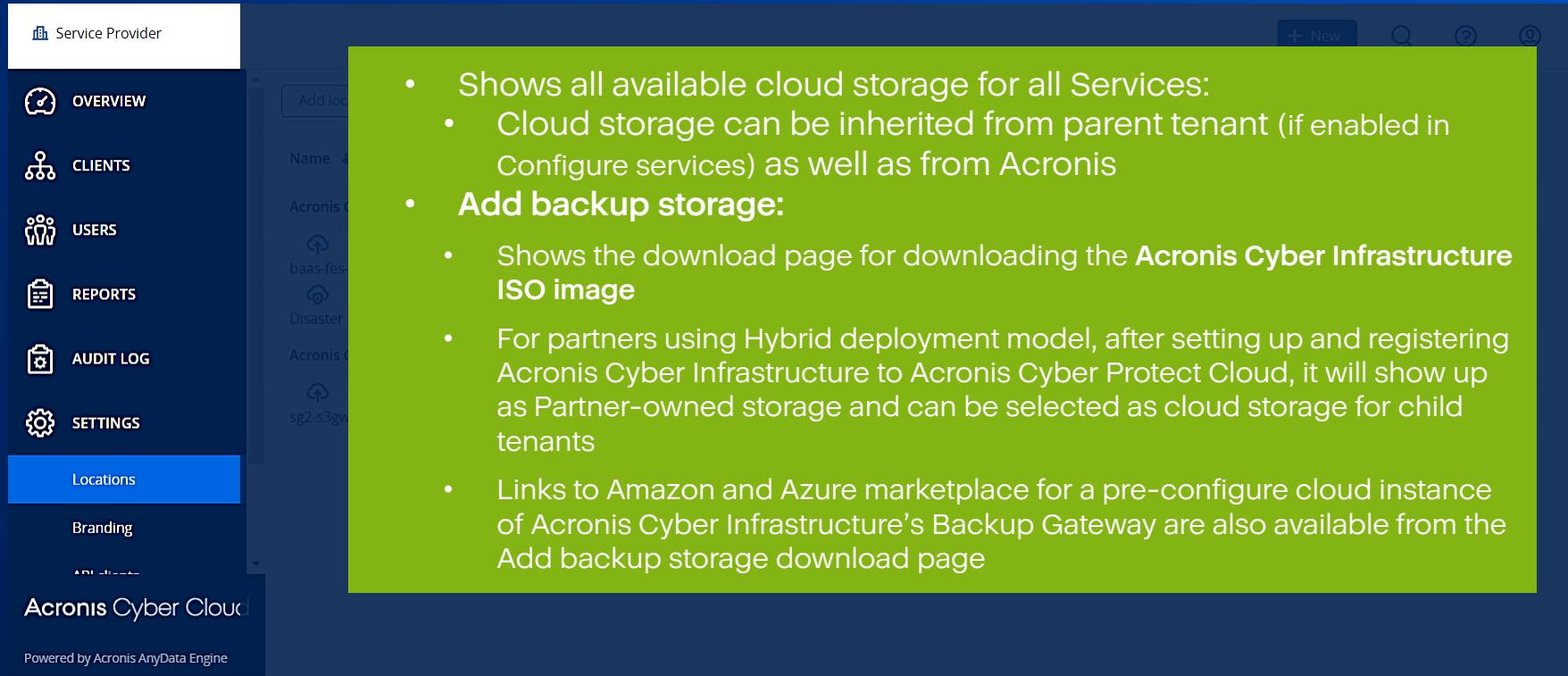
- Reports can be downloaded or send as email immediately as .PDF and/or .XLSX file
- Reports can be scheduled to be sent as email to one or more recipients from **Settings**
- Additionally, clicking on **More actions** enables the following:
  - **Clone**: Create a copy of the Report
  - **Export**: Export the as a .json file to be used subsequently for importing
  - **Dump data**: Export data as .csv file for further manipulation
  - **Delete report**: Delete the selected Report

# Managing Tenants – Audit Log Tab

The screenshot shows the Acronis Cyber Cloud interface. The left sidebar has navigation links: Overview, Clients, Users, Reports, Audit Log (which is highlighted in blue), and Settings. The main content area is titled 'Audit Log' and lists several events. Each event row contains the following columns: Event, Severity, Date, Object name, Tenant, Initiator, and IP address. The 'Event' column lists actions like 'User signed in' and 'Tenant was updated'. The 'Severity' column includes 'Notice' and 'Warning'. The 'Date' column shows dates like '04/12/2020 | 56 PM UTC'. The 'Object name' column shows tenant names. The 'Tenant' column shows the tenant ID. The 'Initiator' column shows user emails. The 'IP address' column shows the IP address.

- **Audit Log** provides a chronological record of the following events:
  - Operations performed by users in the management portal
  - System messages about reached quotas and quota usage
  - Consists of Event name, **Severity**, Date, Object name, Tenant, Initiator, Initiator's tenant, IP address and Method
- Shows events in the tenant in which you are operating as well as child tenants and you can click on an event to view more information
- The log is cleaned up on a daily basis and events are removed after **180 days**
- Events can be filtered by description, severity or date and can be searched by object, unit, initiator and initiator's unit

# Managing Tenants – Settings > Locations Tab



The screenshot shows the Acronis Cyber Cloud interface. On the left, a sidebar menu includes options like Service Provider, Overview, Clients, Users, Reports, Audit Log, Settings, Locations (which is highlighted in blue), and Branding. Below the sidebar is the text "Acronis Cyber Cloud" and "Powered by Acronis AnyData Engine". The main content area has a header with "+ New", a search icon, and a help icon. It displays a table of locations with columns for Name, Status, and Actions. The first location listed is "Acronis Cyber Protect Cloud". A large green callout box is overlaid on the right side of the screen, containing the following bullet points:

- Shows all available cloud storage for all Services:
  - Cloud storage can be inherited from parent tenant (if enabled in Configure services) as well as from Acronis
- **Add backup storage:**
  - Shows the download page for downloading the **Acronis Cyber Infrastructure ISO image**
  - For partners using Hybrid deployment model, after setting up and registering Acronis Cyber Infrastructure to Acronis Cyber Protect Cloud, it will show up as Partner-owned storage and can be selected as cloud storage for child tenants
  - Links to Amazon and Azure marketplace for a pre-configure cloud instance of Acronis Cyber Infrastructure's Backup Gateway are also available from the Add backup storage download page

# Managing Tenants – Settings > Locations Tab



The screenshot shows the Acronis Cyber Cloud Service Provider interface. The left sidebar has a 'Service Provider' header and links for Overview, Clients, Users, Reports, Audit Log, Settings (which is highlighted in blue), and Locations. The main area is titled 'OVERVIEW' and shows a list of locations. At the top right of this area are buttons for '+ New', 'Search', 'Help', and 'Logout'. A callout box highlights the 'Add location' button. Below it, another callout box highlights the 'Add backup storage' button. The list of locations includes:

- Acronis Cloud
- baas-fes-sg1.acronis.com
- Disaster Recovery Storage
- Acronis Cloud (Files)
- sg2-s3gw.acronis.com

A large green callout box on the right side contains the following bullet points:

- **Add location:**
  - Used for creating one or more **Locations**, which are logical containers to group partner-owned storage added by parent or own tenant
  - Locations will show up in child tenants if enabled in **Configure Services** when creating/modifying a child tenant

# Managing Tenants – Settings > Branding Tab

The screenshot shows the Acronis Cyber Cloud web interface. On the left, there is a vertical sidebar with the following menu items:

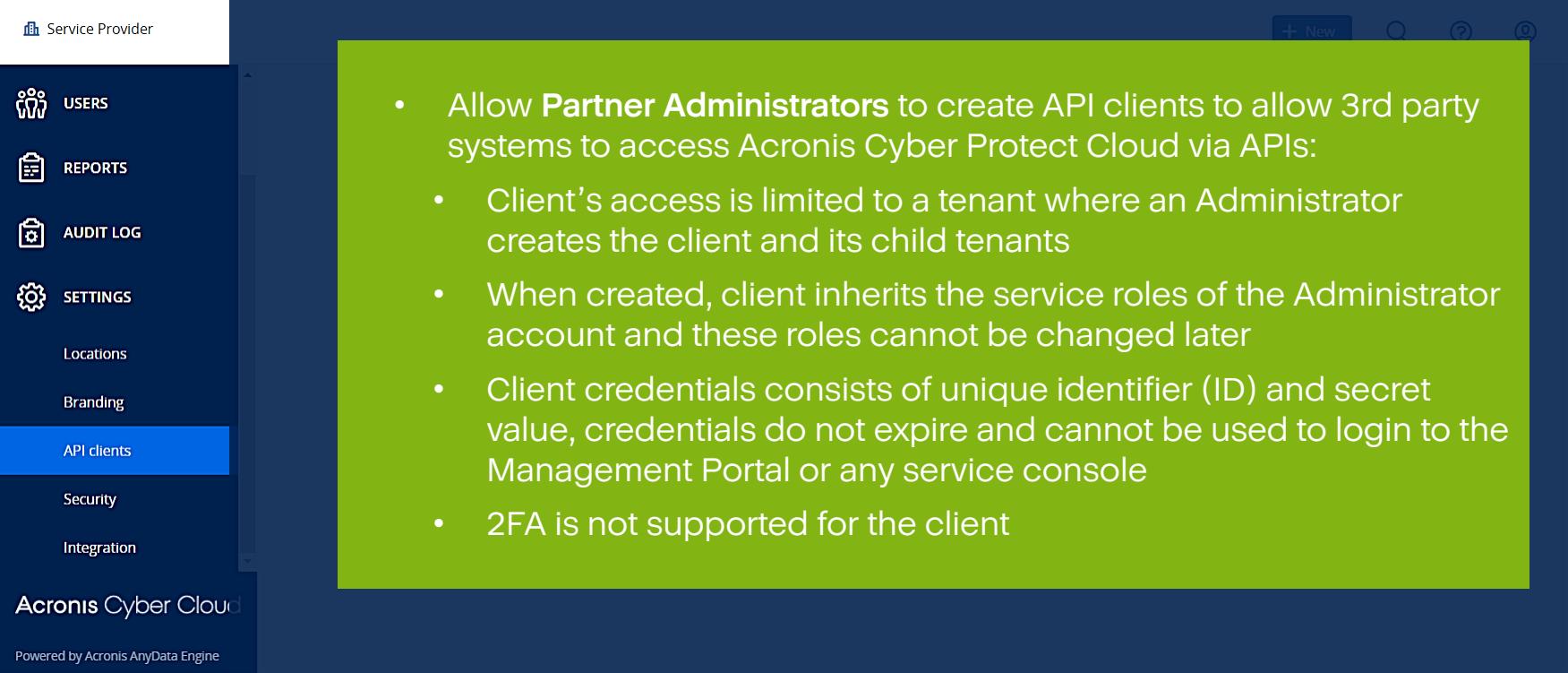
- Service Provider
- USERS
- REPORTS
- AUDIT LOG
- SETTINGS
- Locations
- Branding** (highlighted with a blue background)
- API clients
- Security
- Integration

At the bottom of the sidebar, it says "Acronis Cyber Cloud" and "Powered by Acronis AnyData Engine".

The main content area has a green background and contains the following list:

- Allow **Partner Administrators** to customize interface of management portal and service consoles:
  - Available only for **Partner** and **Folder** tenant types, child tenants will inherit the branding
  - Branding** items includes:
    - Appearance:** Service name, logo and color scheme
    - Documentation and Support:** URLs for Home, Support, KB, Management Portal administrator's guide and help, Support phone number
    - Legal:** URLs for EULA and platform terms
    - Upsell:** URL for buy button
    - Mobile apps:** URLs for Apple and Google app store
    - Email server settings**

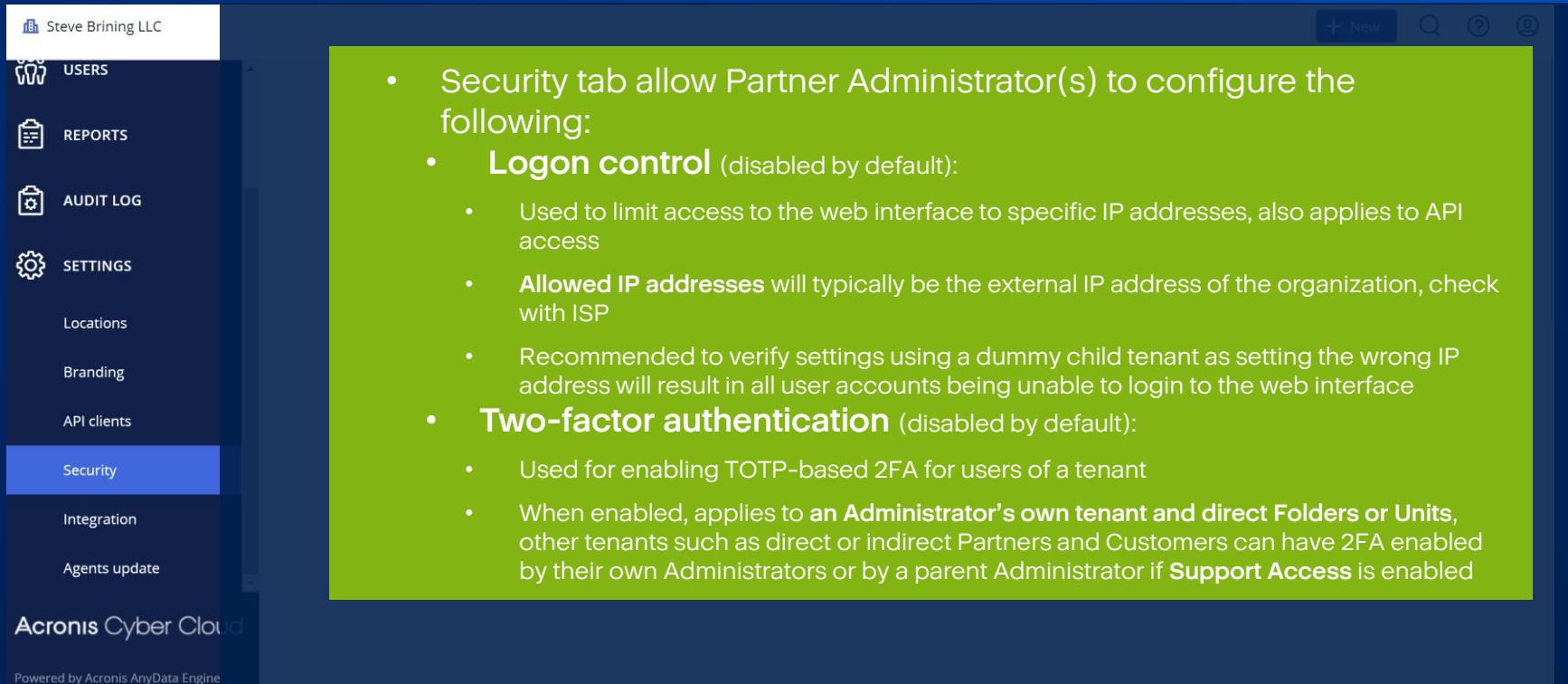
# Managing Tenants – Settings > API Clients Tab



The screenshot shows the Acronis Cyber Protect Cloud Management Portal interface. The left sidebar contains navigation links: Service Provider, USERS, REPORTS, AUDIT LOG, SETTINGS, Locations, Branding, API clients (which is highlighted in blue), Security, and Integration. The main content area has a green background and displays the following bullet points:

- Allow **Partner Administrators** to create API clients to allow 3rd party systems to access Acronis Cyber Protect Cloud via APIs:
  - Client's access is limited to a tenant where an Administrator creates the client and its child tenants
  - When created, client inherits the service roles of the Administrator account and these roles cannot be changed later
  - Client credentials consists of unique identifier (ID) and secret value, credentials do not expire and cannot be used to login to the Management Portal or any service console
  - 2FA is not supported for the client

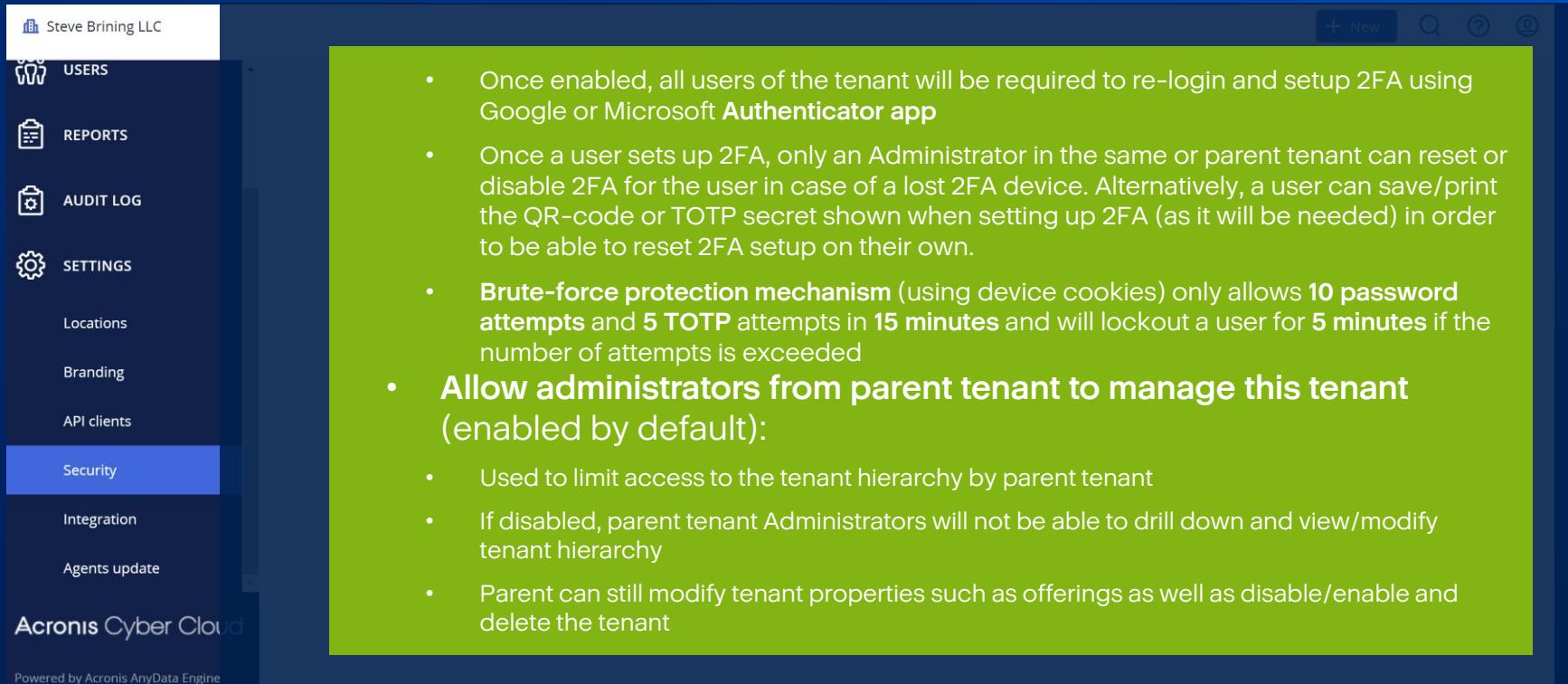
# Managing Tenants – Settings > Security Tab



The screenshot shows the Acronis Cyber Cloud web interface. At the top left is the tenant name "Steve Brining LLC". The left sidebar has a dark blue background with white icons and text. The "SETTINGS" section is expanded, showing "Locations", "Branding", "API clients", "Security" (which is highlighted with a blue background), and "Integration". Below the sidebar is the main content area, which has a light green background. The main content starts with a bullet point: "• Security tab allow Partner Administrator(s) to configure the following:" followed by two nested lists: one for "Logon control" and one for "Two-factor authentication".

- Security tab allow Partner Administrator(s) to configure the following:
  - **Logon control** (disabled by default):
    - Used to limit access to the web interface to specific IP addresses, also applies to API access
    - **Allowed IP addresses** will typically be the external IP address of the organization, check with ISP
    - Recommended to verify settings using a dummy child tenant as setting the wrong IP address will result in all user accounts being unable to login to the web interface
  - **Two-factor authentication** (disabled by default):
    - Used for enabling TOTP-based 2FA for users of a tenant
    - When enabled, applies to **an Administrator's own tenant and direct Folders or Units**, other tenants such as direct or indirect Partners and Customers can have 2FA enabled by their own Administrators or by a parent Administrator if **Support Access** is enabled

# Managing Tenants – Settings > Security Tab



The screenshot shows the Acronis Cyber Cloud web interface. The left sidebar has a dark blue background with white icons and text. The 'Security' option is highlighted with a blue background. Other options include 'Users', 'Reports', 'Audit Log', 'Settings', 'Locations', 'Branding', 'API clients', and 'Integration'. At the bottom of the sidebar, it says 'Powered by Acronis AnyData Engine'. The main content area has a light green background. It displays a bulleted list of features under the 'Security' tab:

- Once enabled, all users of the tenant will be required to re-login and setup 2FA using Google or Microsoft **Authenticator app**
- Once a user sets up 2FA, only an Administrator in the same or parent tenant can reset or disable 2FA for the user in case of a lost 2FA device. Alternatively, a user can save/print the QR-code or TOTP secret shown when setting up 2FA (as it will be needed) in order to be able to reset 2FA setup on their own.
- Brute-force protection mechanism** (using device cookies) only allows **10 password attempts** and **5 TOTP attempts** in **15 minutes** and will lockout a user for **5 minutes** if the number of attempts is exceeded
- Allow administrators from parent tenant to manage this tenant** (enabled by default):
  - Used to limit access to the tenant hierarchy by parent tenant
  - If disabled, parent tenant Administrators will not be able to drill down and view/modify tenant hierarchy
  - Parent can still modify tenant properties such as offerings as well as disable/enable and delete the tenant

# Managing Tenants – Settings > Integrations Tab



The screenshot shows the Acronis Cyber Cloud web interface. The left sidebar has a dark blue background with white icons and text. The 'Integration' tab is highlighted with a blue background. Other visible tabs include 'Users', 'Reports', 'Audit Log', 'Settings', 'Locations', 'Branding', 'API clients', 'Security', and 'Agents update'. At the bottom of the sidebar, it says 'Acronis Cyber Cloud' and 'Powered by Acronis AnyData Engine'. The main content area has a green background and contains a bulleted list of features:

- Allow **Partner Administrators** to configure integration with a variety of 3rd party **Professional Services Automation** (PSA) and Remote Monitoring and Management (RMM) systems
- Depending on the 3rd party system selected, the user may be redirected to download the required packages (for installation in the PSA or RMM system) or configure integration settings from within the Integration tab
- Acronis Cyber Protect Cloud **RESTful API documentation** is also available on this page

In the bottom right corner of the main content area, there are logos for 'TIEKLANT', 'HOSTBELL', and 'Kaseya®'.

# Section Summary



- Dashboards can be used to review system health and identify problems that need to be addressed quickly
- Reports can be used to demonstrate value to customers and keep managers informed on system health
- Integrations with 3<sup>rd</sup> party vendors allow for automating many tasks through our APIs
- Branding provides the ability make the system match corporate branding or white labeling

# Acronis

## Acronis Cyber Protect Cloud

### Troubleshooting



# Section Modules - Part 4



- 1. Basic Troubleshooting Steps and Resources**
- 2. Most Common Issues**
- 3. Escalating Issue to Acronis Support**

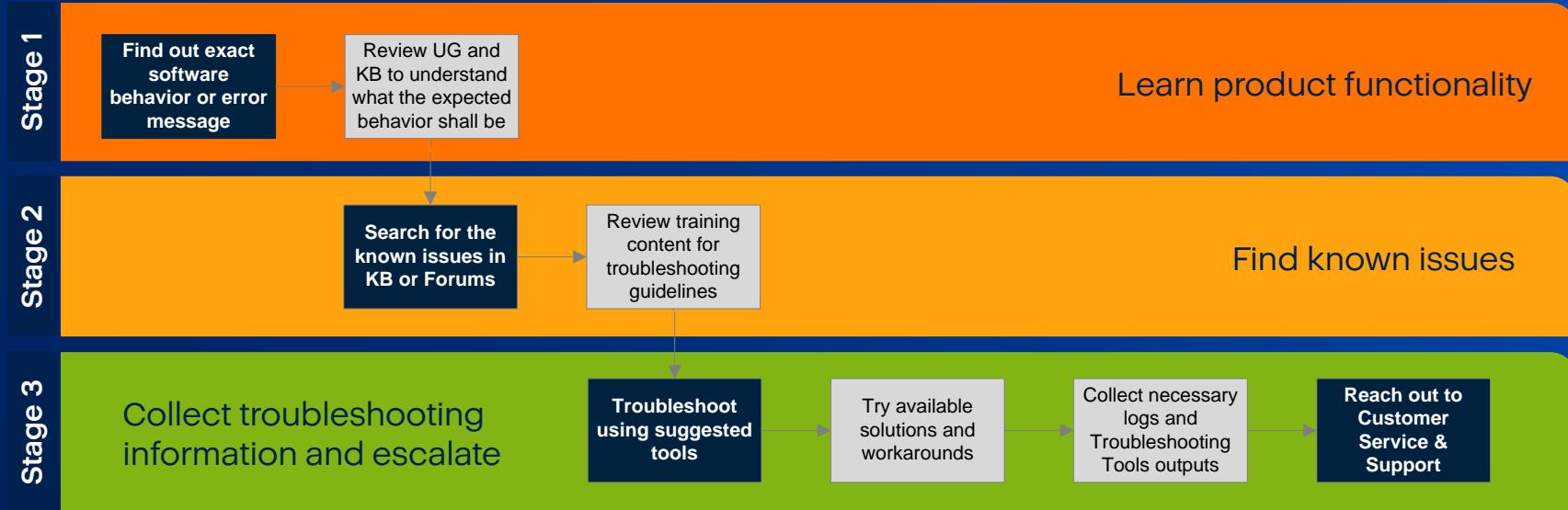
# Acronis

## Acronis Cyber Protect Cloud

### Basic Troubleshooting Steps and Resources



# Basic Troubleshooting Steps



# Searching through user guide

The screenshot shows a user guide interface for the Backup and Disaster Recovery service. At the top, there's a dark blue header bar with the title "Backup and Disaster Recovery service". Below the header, there's a navigation bar with icons for home, up, and down, followed by "Contents" and "Index" buttons. To the right is a search bar with a magnifying glass icon.

The main content area starts with a "Welcome to Backup and Disaster Recovery service" message. Below it, there's a section titled "Getting started" with two bullet points: "About the Backup service" and "About the Disaster Recovery service".

On the left side, there's a sidebar menu with the following items:

- Welcome to Backup and Disaster Recovery service
- Backup
  - About the backup service
  - Software requirements
  - Supported file systems
  - Activating the account
  - Accessing the backup service
  - Installing the software
    - Backup console views
  - Backup
  - Recovery
  - Operations with backups
  - Operations with backup plans

Below the sidebar, there's a section titled "Backup & Disaster Recovery functionality" with two columns: "Backup" and "Disaster Recovery", each containing a list of bullet points.

Backup	Disaster Recovery
<ul style="list-style-type: none"><li>Software requirements</li><li>Backup</li><li>Recovery</li><li>Operations with backups</li><li>Protecting Microsoft applications</li></ul>	<ul style="list-style-type: none"><li>Software requirements</li><li>Setting up connectivity to cloud recovery site</li><li>Setting up recovery servers</li><li>Setting up primary servers</li></ul>

# Searching through user guide

The screenshot shows a user guide for the Backup and Disaster Recovery service. At the top, there's a navigation bar with icons for home, back, forward, and search, along with a search input field. Below the bar, the title "Backup and Disaster Recovery service" is displayed. On the left, a sidebar menu lists various topics under "Backup" and "Disaster Recovery". A green box highlights the "Navigation tree" section, which contains a list of items: "About the Backup service", "Software requirements", "Supported file systems", "Activating the account", "Accessing the backup service", "Installing the software", "Backup console views", "Backup", "Recovery", "Operations with backups", and "Operations with backup plans". To the right of the sidebar, the main content area has a heading "Getting started" followed by two bullet points: "About the Backup service" and "About the Disaster Recovery service". Below this is a section titled "Backup & Disaster Recovery functionality" with two columns: "Backup" and "Disaster Recovery", each containing a list of items.

Backup and Disaster Recovery service

Contents Index

Welcome to Backup and Disaster Recovery service

Getting started

- About the Backup service
- About the Disaster Recovery service

Backup & Disaster Recovery functionality

Backup

- Backup
- Recovery
- Operations with backups
- Operations with backup plans

Disaster Recovery

- Software requirements
- Setting up connectivity to cloud recovery site
- Setting up recovery servers
- Setting up primary servers

Navigation tree

# Searching through user guide

The screenshot shows a user guide for the Backup and Disaster Recovery service. At the top, there's a dark blue header with the title "Backup and Disaster Recovery service". Below the header is a navigation bar with icons for home, back, forward, contents, and index. A search bar is located in the top right corner.

The main content area has a title "Welcome to Backup and Disaster Recovery service". Below it, a "Getting started" section lists two items:

- About the Backup service
- About the Disaster Recovery service

Further down, there's a section titled "Backup & Disaster Recovery functionality" which is divided into "Backup" and "Disaster Recovery".

A green box highlights the "Navigation tree" section, which contains a list of topics under "Backup":

- [Backup](#)
- [Recovery](#)
- [Operations with backups](#)
- [Operations with backup plans](#)

An arrow points from the "Navigation tree" label to the "Backup" heading in the list. Another green box highlights the "Search bar" at the top right of the page.

# Searching through user guide

The screenshot shows the 'Backup and Disaster Recovery service' user guide. At the top left is the title bar. Below it is a header with icons for home, back, forward, and search. A navigation bar has 'Contents' and 'Index' tabs; 'Index' is highlighted and has a green callout labeled 'Alphabetical index'. To the right is a search bar with a magnifying glass icon, also labeled 'Search bar' with a green callout. The main content area includes a 'Welcome to Backup and Disaster Recovery service' banner, a 'Getting started' section with two bullet points, a 'Backup & Disaster Recovery functionality' section, and a 'Navigation tree' section. The 'Navigation tree' section is highlighted with a green callout and contains a diagram showing a central node connected to 'Backup' and 'Disaster Recovery', which further connect to various sub-points.

Backup and Disaster Recovery service

Alphabetical index

Search bar

Getting started

- About the Backup service
- About the Disaster Recovery service

Backup & Disaster Recovery functionality

Navigation tree

Backup

- Configuration
- Backup
- Recovery
- Operations with backups
- Protecting Microsoft applications

Disaster Recovery

- Software requirements
- Setting up connectivity to cloud recovery site
- Setting up recovery servers
- Setting up primary servers

# Knowledge base

- Acronis Knowledge Base ([kb.acronis.com](https://kb.acronis.com)) is a main resource for official information about:
  - product functionality
  - product limitations
  - known issues
  - troubleshooting techniques
  - support tools and usage
  - other relevant support information
- Acronis Cyber Protect Cloud articles are all listed and grouped by topics at <https://kb.acronis.com/acronis-cyber-protect-cloud>

The screenshot shows the Acronis Knowledge Base homepage. At the top, there's a search bar with placeholder text "Enter your keywords", a search button labeled "SEARCH", and a dropdown menu set to "Any". To the right, there are links for "Forums", "Support", and "English". Below the header, there's a section titled "Browse in sections" with three categories: "Acronis Cyber Protect Cloud" (represented by a blue cube icon), "Acronis Cyber Infrastructure" (represented by a blue hexagon icon with a white letter "A"), and "Acronis Cyber Files Cloud" (represented by a blue square icon). The main content area is divided into several sections: "FAQs & Hot Topics" (with a link to "Acronis Backup Cloud: FAQ"), "Licensing, Requirements, Features & More" (listing topics like "Acronis Products: Windows 10 Support" and "Acronis Backup Archive Compatibility Across Different Product Versions"), "How-tos" (with a link to "Viewing Build Number in Acronis Products"), and a "Show all articles" button.

# KB search best practices

- Few simple rules to enhance search results in the Knowledge Base:
- Use product filter**
  - After typing search request and before running search, select product to show only relevant results
- Search wisely**
  - It makes sense to search for the most non-generic error message while searching through KB
- Verify if the particular KB is applicable**

58006: Acronis software: NVMe drives in RAID mode are not detected by Linux-based bootable media and Acronis startup recovery manager

Also read in: 日本語 or use Google Translate Select Language ▾

Applies to: [Acronis True Image 2021](#) [Acronis Cyber Backup 12.5](#) [Acronis Snap Deploy 5](#) [Acronis Disk Director 12.5](#)  
[Acronis Cyber Protect Cloud](#) [Acronis Cyber Backup Cloud](#) [Acronis Backup 12](#) [Acronis Backup 11.7](#) [Acronis Backup 11.5](#)  
[Acronis True Image 2020](#) [Acronis True Image 2019](#) [Acronis True Image 2018](#) [Acronis True Image 2017](#)



Acronis | Knowledge Base

Search

Invalid handle  in Any

Acronis Cyber Protect

Browse in sections

Acronis Cyber Protect Cloud (highlighted with a green box)

Acronis Cyber Backup Cloud

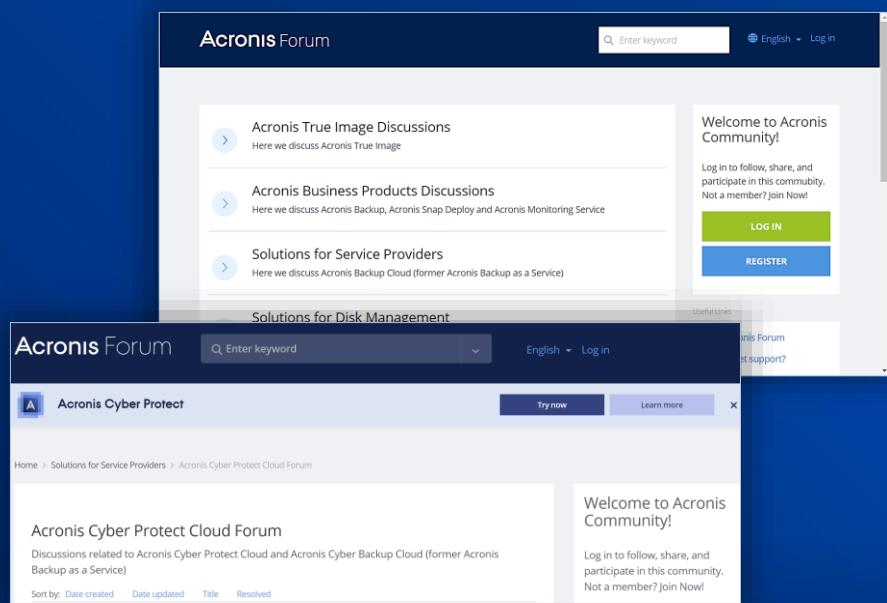
Acronis Cyber Cloud Integration with WHMCS

Acronis Cyber Disaster Recovery Cloud

Acronis True Image 2021 Acronis True Image 2020

# Acronis Forums

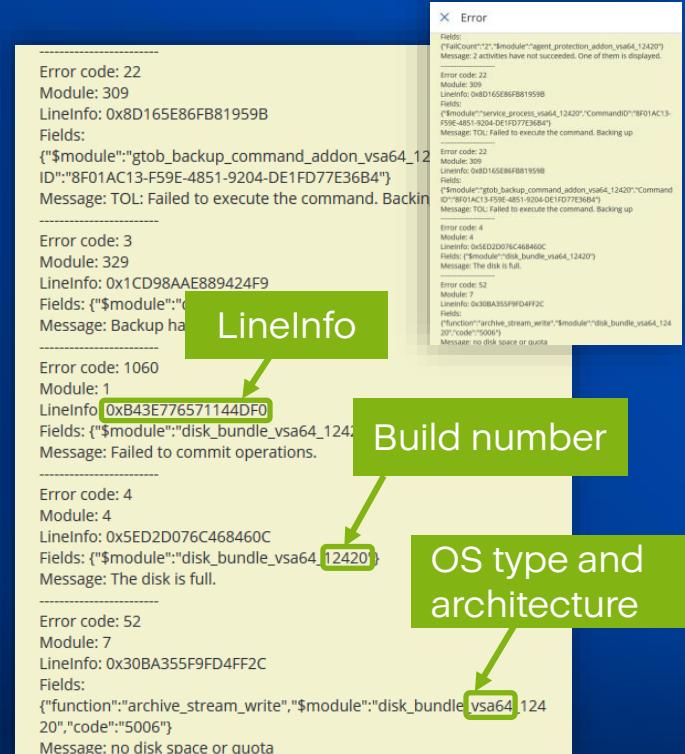
- Acronis Support Forums is an open community where you can get in touch with:
  - Acronis Customer Service & Support Team
  - Acronis Development Team
  - Acronis Forum MVPs and other Service Providers
- Requires Acronis web account in order to post in the discussion boards
- For Acronis Cyber Protect Cloud-related discussions:  
<https://forum.acronis.com/forum/solutions-service-providers/acronis-cyber-protect-cloud-forum>



# Reading the error message

- Error message consist of several field sets of error information, stacked in one message. Each field set corresponds to a particular software module which gave the error
- How to process the error message:
  - Start reading the error message from bottom field set to top, since the corresponding failed module gives the most user-relevant error message
  - Always read several field sets to have a complete understanding of the message
- KB search-relevant information in each field set:
  - Message: User-readable description of the error
  - LineInfo: unique ID for the error message
- Troubleshooting-relevant information:
  - Fields: contains the process name, OS details and the build number

Last field set



# Error lookup in knowledge base

- Open the warning or error message and click on **Support**:
  - If KB contains a similar error message, follow instructions of the article to confirm and solve the issue
  - Alternatively use KB search to look for similar issues following general KB search rules

The diagram illustrates the process of looking up errors in a knowledge base. It starts with a screenshot of a software interface showing an 'Activity details' window for a backup plan. A red error message at the bottom of the window says 'Backup failed' with the sub-message 'None of the items selected for backup were found.' A green arrow points from this window to a screenshot of the Acronis Knowledge Base website. The website shows a search result for the error code 58030, which corresponds to 'Backup Fails with "All items specified for backup do not exist."'. The article includes sections for 'Symptoms' and 'Cause', providing detailed information about the error and how to resolve it.

**Activity details**

10:04 PM — 10:04 PM  
Backup plan 'Files/folders to Cloud Storage' (abc-agent)

Status: Error  
Device: abc-agent  
Plan: Files/folders to Cloud Storage  
Started by: On schedule

Start time: Jul 06, 2017, 10:04:01 PM  
Finish time: Jul 06, 2017, 10:04:01 PM  
Duration: 0 sec

Details Support

**Error**

Backup failed  
None of the items selected for backup were found.

Details Support

**Acronis | Knowledge Base**

Search Enter your keywords  in Any

We found a KB article about an [error which is similar to your error](#).

58030: Acronis Backup 12: Backup Fails with "All items specified for backup do not exist."

Also read in: 日本語 Translate to: Выбрать язык Applies to: Acronis Backup 12

### Symptoms

Your backup fails a few seconds after start with the following error message:  
"All items specified for backup do not exist."

In the details view, you will find an error message like this:

Error code: 58  
Module: 307  
Lineinfo: 0xC3471CEFFA18278  
Message: No backup items were resolved: ('avfs:/local?P:/UserFiles/User43','mms::file:dir';('4B2A7A93-A44F-4155-BDE3-A023C57C9431';'gct:files')) The specified file does not exist. The system cannot find the file specified

### Cause

This error happens when every single item in the "Items to back up" of your backup plan can no longer be found by Acronis Backup. Since Acronis Backup cannot find any of the items selected for backup, the backup fails.

# Section Summary



Use the Acronis basic troubleshooting steps and recourses to:

- Learn product functionality
- Find known issues
- Collect troubleshooting information and escalate

There are several Acronis help recourses available

- User guides
- Knowledge Base
- Acronis Forum

# Acronis

## Acronis Cyber Protect Cloud

### Most Common Issues



# Quotas are automatically reset

## Problem



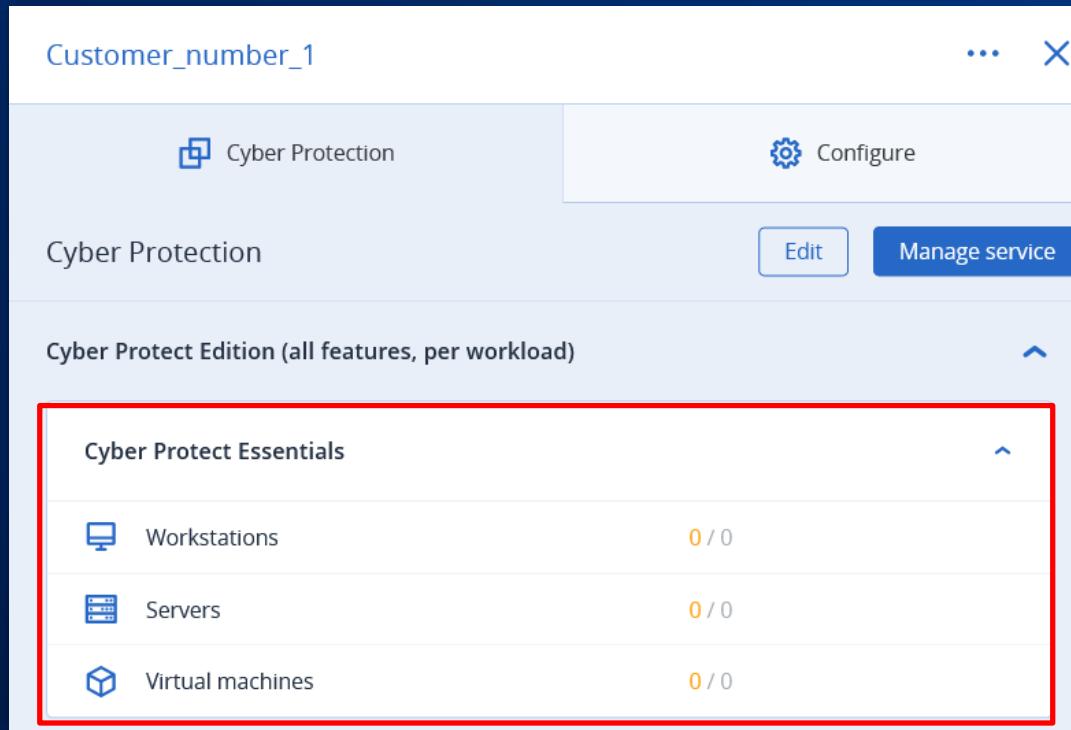
1. You change some quotas for any offering items within Acronis Cyber Protect Cloud's management console.
2. After short period of time the quotas are reset to original value ("0", "unlimited", etc.).



## Solution

1. Check the management portal's Audit logs. It will show explicitly who has initiated the quota's reset.
2. In most of the cases the issue is caused by integration set up between Acronis Cyber Protect Cloud and a 3rd party business platform.
3. Verify if integration settings are configured properly.
4. If integration is enabled, do not modify quotas from Acronis Cyber Protect Cloud's management console.

# Quotas are automatically reset



The screenshot shows the Azure portal interface for managing a service named "Customer\_number\_1". The "Cyber Protection" blade is open, displaying the "Cyber Protect Edition (all features, per workload)" configuration. A red box highlights the "Cyber Protect Essentials" section, which contains three quota items: Workstations, Servers, and Virtual machines, all showing 0/0 usage.

Category	Resource Type	Quota
Cyber Protect Essentials	Workstations	0 / 0
	Servers	0 / 0
	Virtual machines	0 / 0

# Emails from the platform are not received

## Problem



1. You don't receive some notification from Acronis Cyber Protect Cloud platform's side, e.g.
  - account activation email, scheduled reports, backup notification etc.



## Solution

1. Check your mailbox's *Junk/Spam* folders.
2. If custom email server settings were applied under **Branding**, verify if a test message successfully delivered using *Send test email message* button.
3. For backup status notifications: check [Backup notifications level](#) and make sure the type of the notifications you have been expecting is enabled.
4. Details: <https://kb.acronis.com/content/49778>

# Emails from the platform are not received

The screenshot displays two main windows of the Acronis Cyber Cloud interface.

**Top Window:** A modal titled "Settings" for the user "msp-lab-eu3". It lists several notification types with checkboxes:

- Quota overuse notifications (unchecked)
- Scheduled usage reports (unchecked)
- Failure notifications** (checked)
- Warning notifications** (checked)
- Success notifications** (checked)
- Daily recap about active alerts (unchecked)
- Device Control notifications (unchecked)

**Bottom Window:** A "Email server settings" section. It includes a note: "These email server settings will be used by all direct and indirect child partners/folders and customers by default." Below this is a "Customize" button and a red-bordered "Send test email message" button.

# Unexpected group/user deletion

## Problem



1. Some Customer/Partner group has disappeared from Acronis Cyber Protect Cloud's management portal.
2. Settings of a particular group have been modified by an unknown person.
3. Service/offering for some group have been disabled.

## Solution



1. Search **Audit logs** for the event of your interest.
2. Open the event's settings and check its details.

# Unexpected group/user deletion

The screenshot shows the Acronis Cyber Cloud interface with the Audit Log tab selected. A specific event in the log is highlighted: "User was deleted". A modal window titled "User was deleted" provides detailed information about this event.

**Audit Log Details:**

Event	Severity	Date
Tenant was deleted	Warning	03/16/2021
Service was disabled	Warning	03/16/2021
<b>User was deleted</b>	Warning	03/16/2021
Tenant was disabled	Warning	03/16/2021
User was disabled	Warning	03/16/2021
User signed in to the service	Informational	03/16/2021
User signed in to the service	Informational	03/16/2021
User signed out from the service	Informational	03/16/2021
Legal document was signed	Informational	03/16/2021
Legal document was signed	Informational	03/16/2021
User signed in to the service	Informational	03/16/2021
User was updated	Notice	03/16/2021
User's password was changed	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021
Offering item was turned on	Informational	03/16/2021

**Event Details:**

Event	User was deleted
Severity	Warning
Date	03/16/2021 11:43 AM UTC
Object name	testdelete
Tenant	Customer E
Initiator	bentest2
Initiator's tenant	Customer E
IP	154.160.14.119
Method	Web interface

**Description:**

User 'testdelete' was deleted:  
Status: 'disabled'  
ID: '0a0d982f-9e3c-4e10-a2d3-d5a8ca02f8b8'  
Type: 'default'

# Miscellaneous GUI errors

## Problem



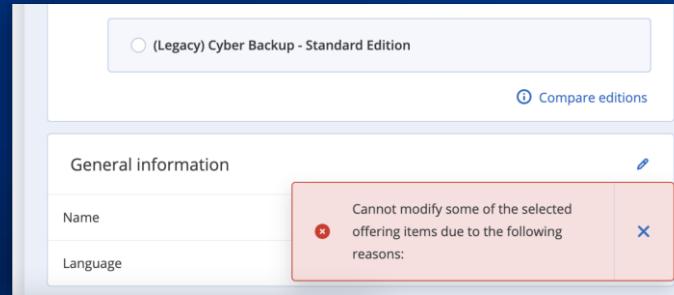
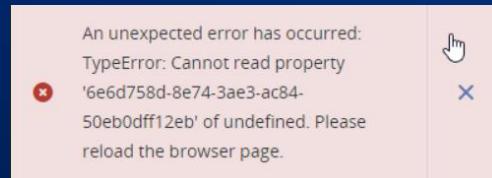
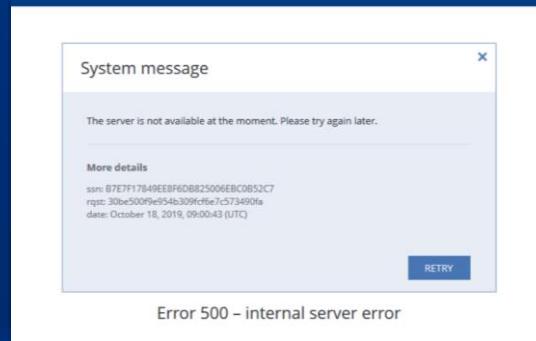
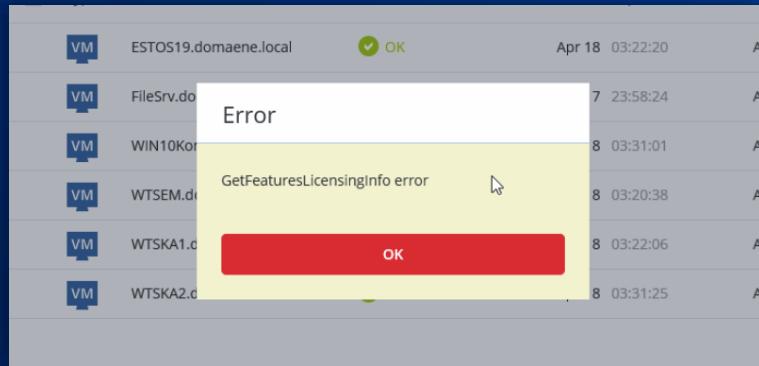
1. Upon making some actions web console shows errors, e.g.:
  - Modifying tenant's settings
  - Saving changes to protection plan

## Solution



1. Collect HAR (HTTP Archive format) log – a log of a web browser's interaction with a site.
2. This information is required for troubleshooting web console issues in Acronis products. Should be collected from the machine you are trying to connect to web console.
3. Details: <https://kb.acronis.com/content/58514>

# Miscellaneous GUI errors



# User-level vs group-level quotas

## Problem



1. You receive a notification saying Cloud storage (or any other) quota is exceeded.
2. You verify quota value for the affected customer at it appears to be sufficient.

## Solution



1. Check if customer user who owns a device also has a quota set for the same offering item.
2. In case **user's** quota is exceeded – increase it.

# User-level vs group-level quotas

The screenshot shows the Acronis Cyber Cloud interface. On the left, a sidebar has tabs for Overview, Usage (which is selected and highlighted in blue), Operations, and Audit Log. The main content area is titled "Cyber Protect" under "Protection". It shows "Location: Cape Town Storage" and a table with a single row: "Backup storage (storage1-cpt.dataake...)" with a status of "74.99 GB / 200 GB". A red arrow points from the text "Quotas on group level" to the storage quota entry.

Quotas on group level

Acronis Cyber Cloud

Cyber Protect

Protection

Manage service

Location: Cape Town Storage

Backup storage (storage1-cpt.dataake...)

74.99 GB / 200 GB

Quotas on user level

Name ↓

Name	Data sources
LK_backup	Workstations 0 / Unlimited
	Servers 0 / Unlimited
	Virtual machines 0 / Unlimited
Cape Town Storage	
Backup storage	74.99 GB / 200 GB

# Incorrect cloud storage usage

## Problem

- 1. You've made a backup of a workload, but Cloud storage consumption shown at management console didn't increase.
- 2. You've deleted some archives for Customer group, but Cloud storage consumption shown at management console didn't decrease.
- 3. The total size of Cloud backups shown under Cyber Protection console differs from the value under management console.



## Solution

- 1. Statistics in Acronis Cyber Protect Cloud is recalculated every 4-6 hours; then the new values are displayed in the management console.
- 2. In case the value under management console is not updated within 24 hrs, this issue needs to be reported to Acronis Support.
- 3. Details: <https://kb.acronis.com/content/59979>

# Incorrect cloud storage usage

The screenshot shows the Acronis Cyber Protect interface. The navigation bar at the top includes 'Support-RU', 'VB\_subpartner', 'FOR WEBINAR', and 'WEB\_CUSTOMER'. On the left, a sidebar has tabs for 'OVERVIEW' (selected), 'Usage' (highlighted in blue), 'Operations', 'UNITS', 'USERS', and 'REPORTS'. The main content area is titled 'Cyber Protect' and shows 'Protection' settings. It displays 'Location: Default location', 'Backup storage (baas-fes-ru2.acronis.co...)', and a progress bar indicating '50.66 GB / Unlimited GB'. The 'Usage' tab is highlighted.

The screenshot shows the Acronis Cyber Cloud interface. The navigation bar at the top includes 'Acronis Cyber Cloud' (selected), 'DASHBOARD' (with a red notification badge '16'), 'DEVICES', 'SOFTWARE MANAGEMENT', and 'BACKUP STORAGE'. The main content area is titled 'Locations' and shows a search bar and a table of locations. One row is selected, showing 'ru2\_webinar\_user' under 'Cloud storage' with the status 'Occupied space: 142 GB'. A large red arrow points from the 'Occupied space' text in the screenshot above down to the 'Occupied space: 142 GB' text in this screenshot.

# Installer missing from the service console

## Problem

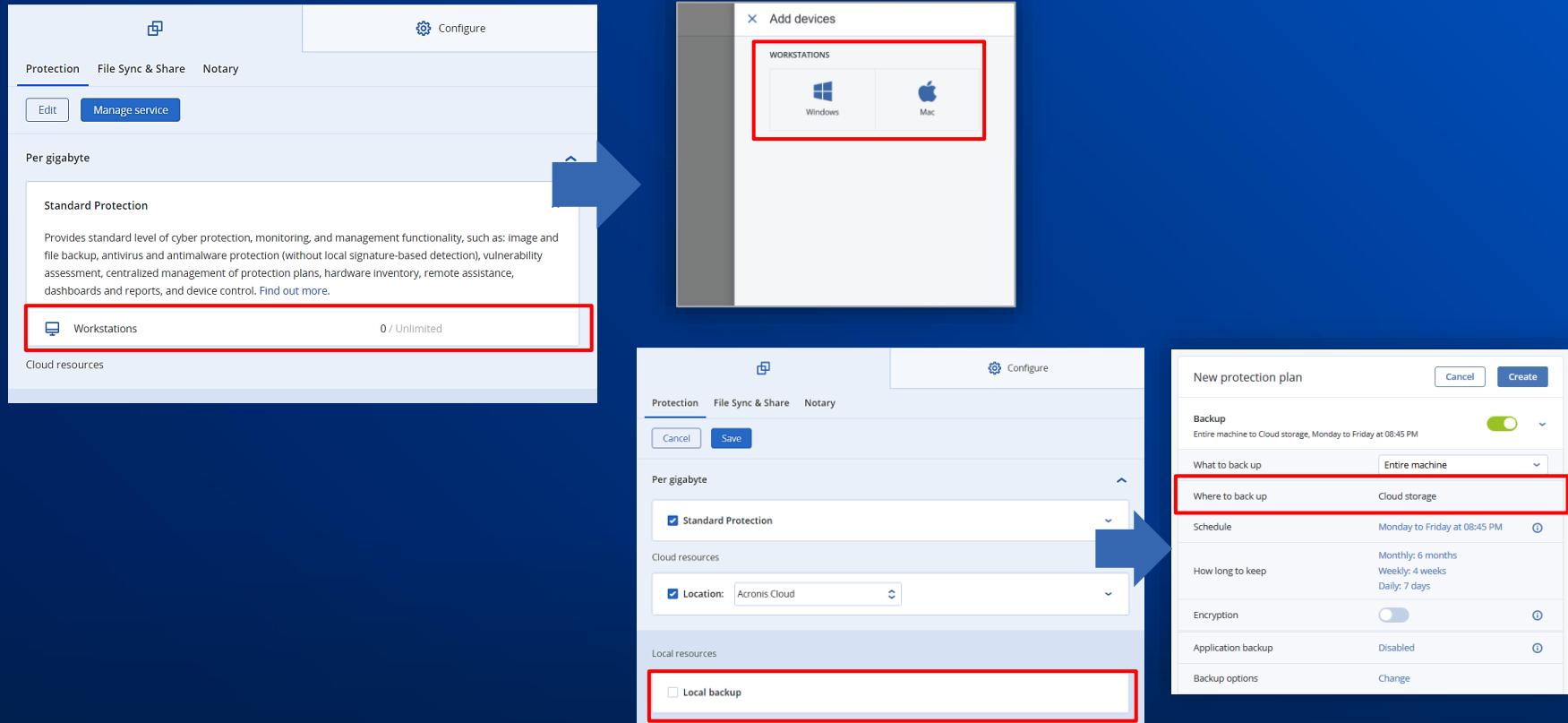
- 1. You are looking for a specific installer to download (e.g. Agent for Linux, Agent for O365 etc.) but you cannot find it under the protect console



## Solution

- 1. Check the offering items enabled for the Customer group.
- 2. Disabling the offering hides respective item in the service console. If the desired offering is disabled – turn it on.
- 3. E.g., when offering is disabled for physical servers and virtual machines, only agents for physical workstations are available.
- 4. Disabling **local backup** offering fixes selection of backup destination on Cloud Storage.
- 5. If some offering is not disabled but completely missing at the Customer group, check the group's Parent preferences. It might be disabled there.

# Installer missing from the service console



# Impossible to change cloud storage for a customer

## Problem

- 1. You are editing Customer group's settings to change the Cloud storage from currently used to a new one.
- 2. The UI does not allow you to change the Cloud storage or
- 3. The new Cloud storage is missing from the list



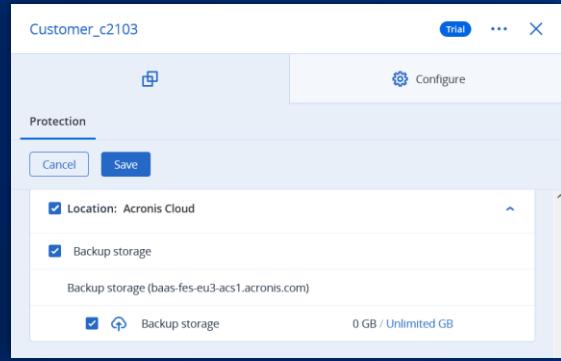
## Solution

- 1. To change Cloud storage for a Customer group, you need to make sure that current Cloud location has no backups (Cloud storage's usage should be = 0).
- 2. Once Cloud storage is freed, you also need to verify that the new Cloud storage is enabled on the Parent group's level.

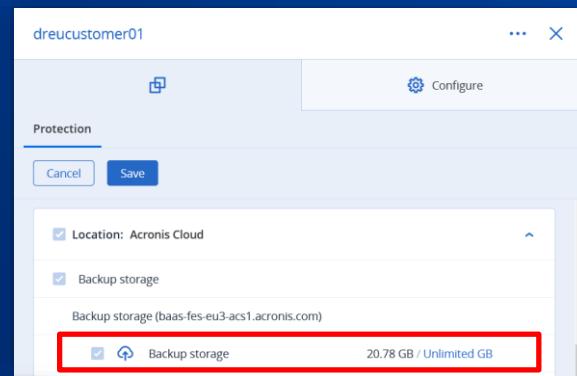


# Impossible to change cloud storage for a customer

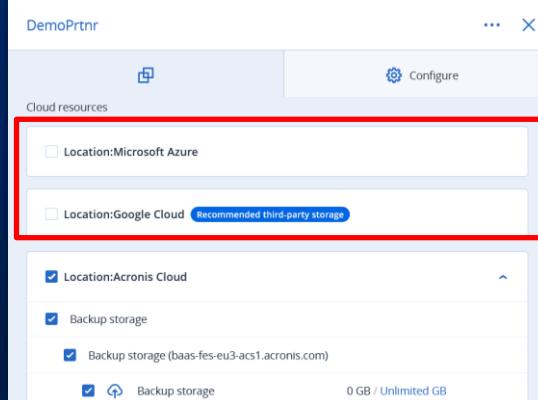
1



2



3



# No support access

## Problem

- 1. Some group has **No access** sign, and you are unable to navigate inside it



## Solution

- 1. The group was created in Self-service mode, therefore parent groups administrators cannot go inside this group (cannot see its children).
- 2. To allow access for parent accounts, an administrator of the group should turn on Support access option under the group's Security settings

# No support access

The screenshot shows a list of tenants in a management interface:

Name	Tenant status	2FA status	Management mode	
Krasnov	Active	Disabled	By service provider	
MacTest	Active	Disabled	By service provider	
MSPtraining	No access	Trial	Disabled	Self-service
NAZ-Partner-RU2	Active	Disabled	By service provider	

A red box highlights the row for 'MSPtraining'. A red arrow points to the 'Support access' toggle switch in the 'Settings' panel, which is currently turned off (green).

**CLients**

**USERS**

**REPORTS**

**AUDIT LOG**

**SETTINGS**

Locations

Branding

API clients

Security

**Login control**  
Specify the IP addresses from which members of this tenant can sign in to the web interface or access API. This setting does not apply to the child tenants of this tenant.

**Two-factor authentication**  
This is a method of identification that provides an effective account protection by requesting authentication data of two different types.

**Support access**  
Grant full access to administrators of the parent tenants: modify properties; manage tenants, users, and services; access backups, and other resources. If it is turned off, administrators from the parent tenant will not be able to access or manage anything inside the child tenant (e.g. tenants, users, services, backups, and other resources).

# Wrong device count

## Problem

- 1. You as a partner placed a quota for Workstations equal to 5, with an overage equal to 0.
- 2. Despite that, customer user has managed to add 10 machines



## Solution

- 1. As soon as at least a single protection plan is applied to a device, it is considered as **protected**.
- 2. Only protected devices consume quotas. In case a device is registered under Cyber Protection console, but does not have any protection plans applied, it does not consume quotas.
- 3. Whenever all protection plans are revoked from a device, the quota occupied by that device is freed.



# Wrong device count

The screenshot illustrates a discrepancy in the number of protected machines between the Cyber Protection service and the main device list.

**Cyber Protection Service (Top Right):**

Category	Count	Limit
Workstations	1	Unlimited
Servers	0	Unlimited
Virtual machines	1	Unlimited

**All devices List (Bottom Left):**

Type	Name	Account	Status	Last backup	Next backup
Windows	vbykov-nb.corp.acronis.com	kdgdkdgd@gmail.com-2	OK	Mar 04	05:01:00 PM
Windows	ru-06478024.corp.acronis.c...	kdgdkdgd@gmail.com-2	OK	Mar 20	04:51:51 PM
VM	blablabla	kdgdkdgd@gmail.com-2	Not protected	Never	Not scheduled
Windows	Centos 7	kdgdkdgd@gmail.com-2	Not protected	Never	Scheduled
Windows	Centos_static	kdgdkdgd@gmail.com-2	Not protected	Never	Scheduled
Windows	WIn2016-shared	kdgdkdgd@gmail.com-2	Not protected	Never	Scheduled
Windows	ApplicationBackupLab	kdgdkdgd@gmail.com-2	Not protected	Never	Not scheduled

A green bracket groups the first two entries (protected) under the heading "Protected machines". A red bracket groups the remaining six entries (non-protected) under the heading "Non-protected machines".

# Section Summary



- Hold on to this section to help with common issues
- Use the knowledgebase at <https://kb.Acronis.com> to find all of these same articles with a quick search

# Acronis

## Escalating Issue to Acronis Support

### How to contact Acronis Support



# Acronis customer service & support

- **24x7 Support in English**
- End Users have to contact their Service Provider for any assistance. Service Providers in their turn may reach out to Acronis Customer Service & Support 24x7. Service is provided according to the following guidelines in English only:  
<http://www.acronis.com/en-us/support/serviceproviderguidelines/>
- **Customer Service & Support Portal**
- Acronis maintains a Customer Service & Support portal for Service Providers to contact Support:  
<http://www.acronis.com/en-us/support/>

The screenshot displays two main sections of the Acronis Customer Support website:

- Service Provider Support Guidelines:** A page titled "Customer Support" featuring the "Acronis Service Provider Support Guidelines". It states that Acronis is committed to providing world-class customer service and support, available via email and telephone seven days a week, 24 hours a day. The Service Provider is responsible for Tier 1 support directly to its Resellers, Subresellers and/or End Users. The page also mentions "Certification" and includes a note about reporting and support.
- Customer Service and Support:** The main customer support portal. It features a navigation bar with links for Home, United Kingdom, Renewals, Contacts, Careers, Search, FOR HOME, BUSINESS, PARTNERS, COMPANY, SUPPORT, and MY ACCOUNT. Below the navigation is a section titled "Customer Service and Support" with a message about support availability in multiple languages. A "Select Category" dropdown is shown, followed by three service categories: "Services for Providers" (Backup, Recovery, Storage for Service Providers), "Acronis Backup" (Backup for Business Needs), and "Acronis Access" (Secure Data Access Sync and Share).

# Acronis customer service & support

## Contacting Customer Service & Support:

- In order to access the Acronis Customer Service & Support portal, Service Provider has to log in to their account on Acronis website, click on the tab labeled “Support”, press the “Contact Support” button and go through the special support wizard:

<https://support.acronis.com/msp>

- The support wizard will ask what type of the issue Service Provider experiences, what type of the product and exact product name they use. Based on the answers provided it will offer best support contact options available, including e-mail and phone.

# Acronis customer service & support

- **Emergency Contacts:**
  - Service Providers may also use direct contacts to reach out to Acronis in case of emergency, e.g. critical issues, problems accessing Customer Service & Support portal, etc:
- **E-mail:** [mspsupport@acronis.com](mailto:mspsupport@acronis.com)
- **Phone:**

Country	Number	Country	Number
US	+1 (888) 223-4587	Australia	+61 (1800) 354 401
Canada	+1 (888) 864-4381	UK	+44 203 514 70 44
Russia	+7 (499) 969-8031	Hong Kong	+852 5803 2291
Japan	+81 (3) 45102313	Argentina	+54 (11) 50789771
Germany	+49 (89) 21093361	South Africa	+27 (0)87 550-2262
Singapore	+65 3158-9823		

*- If you choose to call us, the best way to proceed is to first submit a ticket with details by e-mail and then provide the ticket number to support engineer on the phone.*

# Information required for escalation

Split different issues in separate requests  
(you will get a support case number for each request)

## Description:

- Explain the issue and the symptoms
- Provide steps to reproduce the issue
- Describe the desired outcome you expect from the product

## Logs:

- Provide full error message and screenshots associated with the issue (if any)

## Additional information

- Provide user account login
- Provide device name
- Provide environment details (OS, network configuration etc.)



# Section Summary



- Reach out to your cloud distributor first and follow their rules for contacting support
- Use emergency contact information in a crisis
- Gather all of the needed information so we can provide resolution as quickly as possible

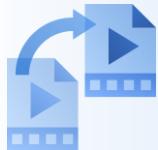
# What's Next?



# Review the Materials



Download and review  
the course materials



Re-watch the videos as  
many times as you'd like

# Take your test



20 MCQ questions



60 Minutes working time



70% Passing Grade



Two Attempts given

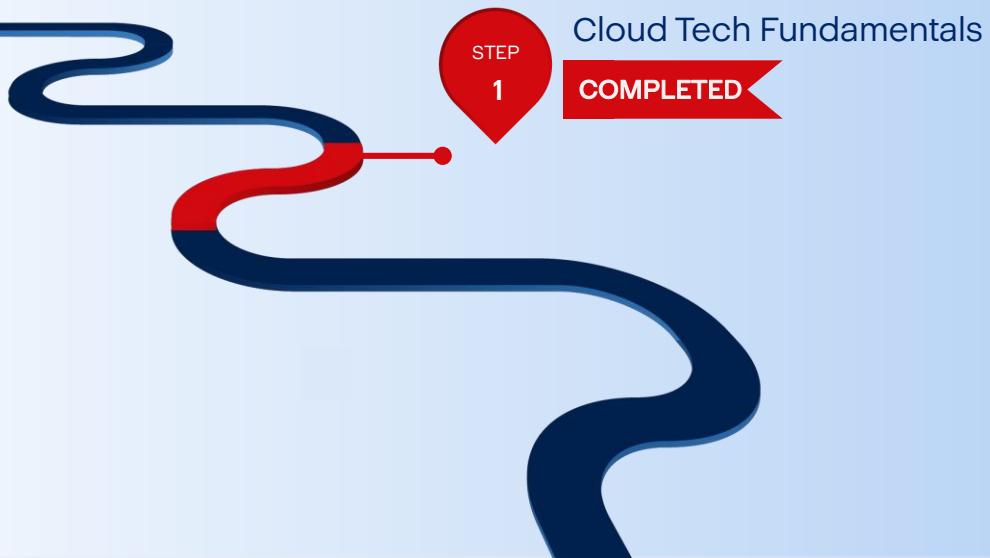


Open Book

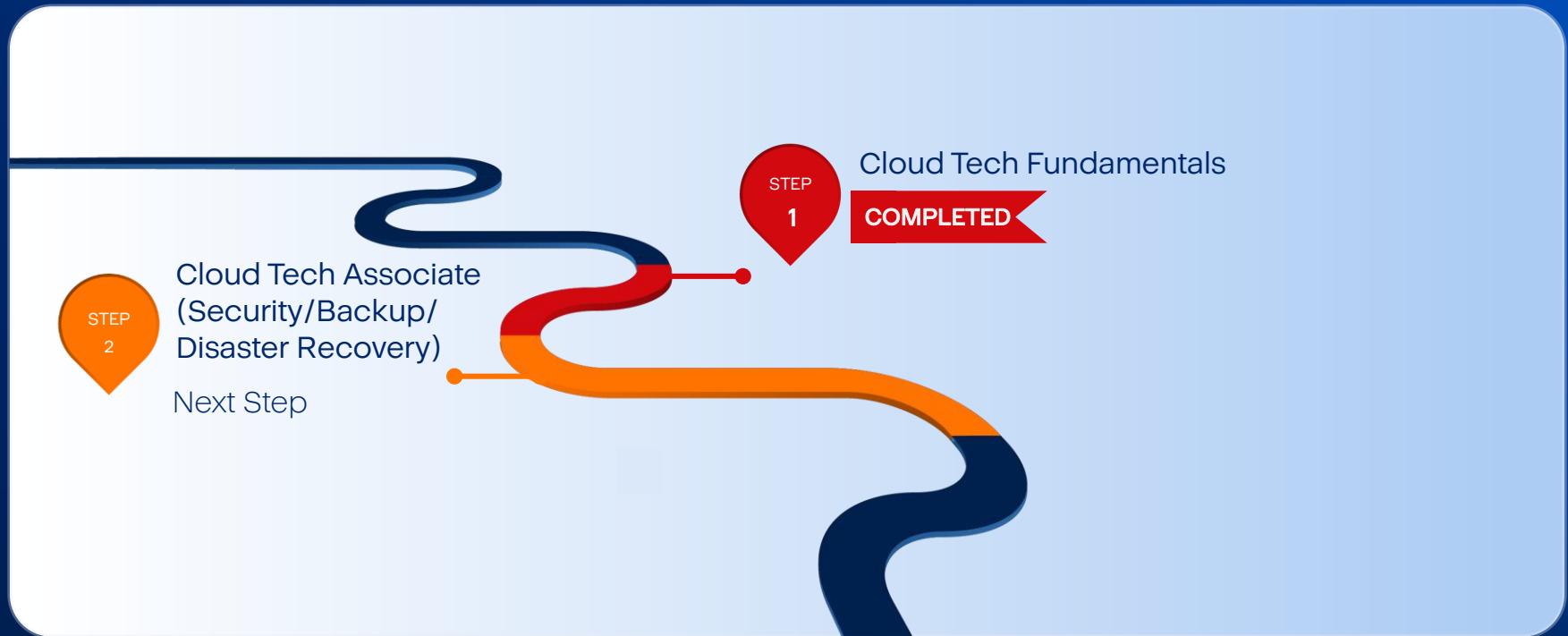
# Certification Track



# Certification Track



# Certification Track



# Certification Track



## Acronis #CyberFit Cloud Tech Associate Certifications

Consists of the following courses (specializations)



+



+



+



+



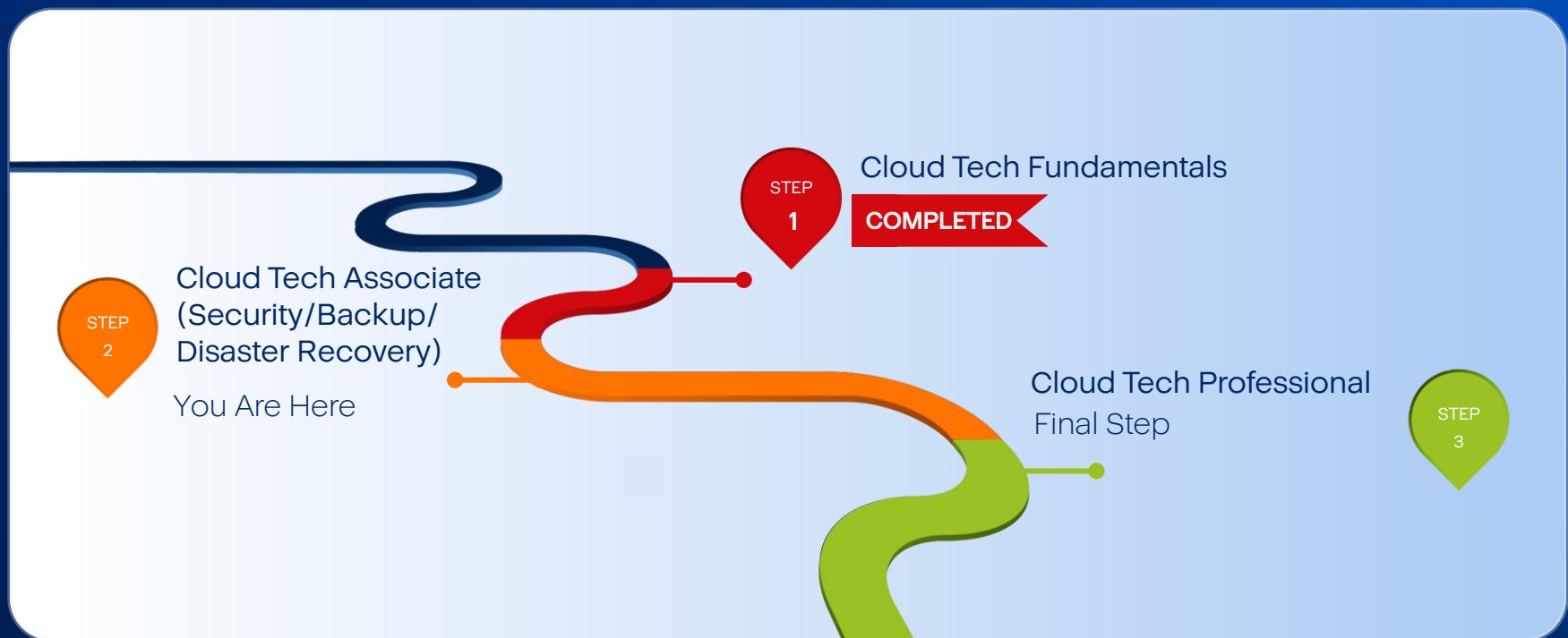
=



Optional:



# Certification Track



# Other Acronis Resources

- Inside Sales
- Field Sales
- Partner Success Managers
- Solution Engineers
- Sales Enablement Team
- Partner Portal for More #CyberFit Academy Training Courses

# Supplemental Materials

The Evangelism Team at Acronis will be periodically releasing new content

Please check back often

Check email for #CyberFit Academy Updates

<https://kb.acronis.com/academy>

## Social Media Accounts

- Instagram: <https://www.instagram.com/acronis>
- Facebook: <https://www.facebook.com/acronis>
- Twitter: <https://twitter.com/Acronis>
- Reddit: <https://www.reddit.com/r/acronis>
- YouTube: <https://www.youtube.com/user/Acronis>

# Acronis Cyber Foundation

Building a More  
Knowledgeable Future

**Create, Spread and Protect  
Knowledge with Us!**

[www.acronis.org](http://www.acronis.org)

Building New Schools  
Publishing Education Programs  
Publishing Books

