

ACRONIS-POWERED. SOTERIA CLOUD DELIVERED.

How to set up least-privilege platform access

Protect the management plane with role design, admin ownership, MFA visibility, and audit evidence that buyers can understand.

Buyer-ready

Operational evidence

Total Data Protection

BEST FIT

MSPs, resellers, customer IT leaders, security owners, and compliance teams governing administrative access.

The buyer needs to reduce admin risk and show that access to protection systems is controlled and traceable.

Acronis

Powered by Acronis



Soteria Cloud delivered

Soteria Cloud

+ New

Acronis AI

Q

?

@

CLIENTS

MONITORING

MY INBOX23

REPORTS

MY COMPANY

Name ↑	Status	2FA status	Login	Roles	Company contacts ⚙
Admin SVC	Active	Disabled	redacted@exa...	Company administrator	Billing, Business, Technical
Soteria Admin ME	Active	Disabled	redacted@exa...	Company administrator	Billing, Business, Technical
Thomas Honiball	Active	Configured	thomas-nfr	Company administrator	Business, Technical

Review users and access ownership



BUYER NEED

Make the commercial requirement operational.

Governance and incident response guidance increasingly treats roles, access, and accountability as part of cyber resilience.

BUYER TRIGGER

The buyer needs to reduce admin risk and show that access to protection systems is controlled and traceable.

PRODUCTS INVOLVED

Cyber Protect Cloud, Advanced Backup, EDR, DLP, Microsoft 365 Protection

CONSOLE SURFACES

Users, Roles and permissions, Security, Audit log

01

The backup and security console is a high-value system; admin access needs the same discipline as other critical platforms.

02

Create role templates for sales, support, billing, technical admin, and security escalation.

03

Separate day-to-day support access from destructive or policy-changing permissions.

04

Use MFA and audit evidence in the monthly review when the buyer has compliance pressure.

05

Remove stale users before reviewing service performance, not after an incident.

06

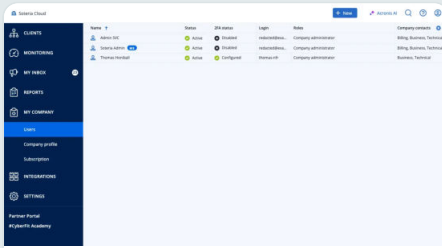
Keep emergency access explicit, named, and reviewed.

PRACTICAL PATH

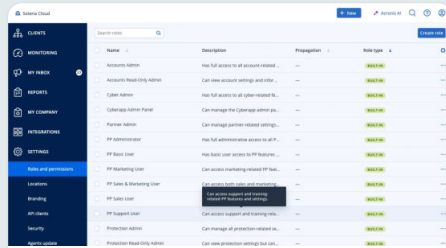
Turn the offer into a repeatable service motion.

Soteria Cloud positions Acronis technology around buyer outcomes, support ownership, recurring review, and evidence that can be explained without product jargon.

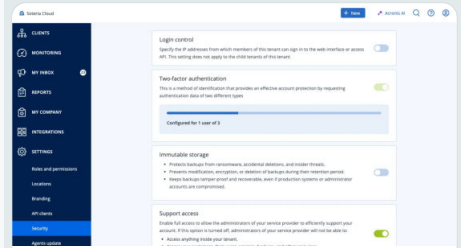
LIST ACCESS ROLES	Identify who needs customer admin, technical support, reporting, billing, security, API, or emergency access.
ASSIGN LEAST PRIVILEGE	Use Roles and permissions to align each user with the smallest role that supports their work.
HARDEN SIGN-IN	Use Security settings and MFA visibility to reduce the risk of account takeover or unmanaged admin access.
REVIEW USER HYGIENE	Check Users for stale accounts, role drift, departed staff, shared accounts, and incomplete ownership.
AUDIT CHANGES	Use Audit log to show role changes, admin activity, and sensitive operations during governance reviews.



Review users and access ownership



Assign roles with clear permissions



Check platform security settings

BUYER OUTCOME

Protect the management plane with role design, admin ownership, MFA visibility, and audit evidence that buyers can understand.



EVIDENCE

Show the proof buyers expect to see.

Soteria Cloud service reviews give buyers visible status, known exceptions, agreed actions, and a reviewable record of protection activity.

Evidence to keep

- Role matrix
- MFA or security setting status
- User access review
- Privileged action audit trail
- Access exceptions

Measures to review

- Privileged users reviewed
- MFA coverage
- Stale accounts removed
- Role exceptions approved
- Privileged actions traceable

01

Privileged users reviewed

02

MFA coverage

03

Stale accounts removed

04

Role matrix

05

MFA or security setting status

06

User access review

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Acronis-powered protection packaged with Soteria Cloud onboarding, service ownership, reporting, and recurring buyer-ready review.