CAPABILITY BRIEF · 01 / 04

acsense

Backup & Recovery

Continuous backup and granular recovery for your IAM tenant. Restore any change to any point in time, regardless of which IDP you run.

Identity is Tier-0 infrastructure. Every employee, application, partner, and AI agent authenticates through it. When configurations break, drift, or get deleted, the consequences cascade. Authentication outages. Ransomware propagation. Audit failures. Regulatory exposure.

Identity providers guarantee their own uptime. They do not guarantee your ability to recover your tenant. Native rollback is limited to specific objects, short retention windows, and offers no full-tenant restore.

Acsense Backup & Recovery closes the gap. Continuous capture of every IAM object, configuration, and relationship, restorable to any point in time, in minutes.

One platform. Any IDP. Tenant-level recovery from a single object to a full rollback, without per-IDP runbooks or one-off restore tooling.

Minutes
RTO for full-tenant recovery

~10 min
RPO with continuous capture

IDP-Agnostic
Tenant-level recovery, any IDP

> *"Identity providers guarantee their own uptime, not your ability to recover your tenant. The recoverability gap is the single most overlooked risk in enterprise IAM."*
>
> Reflecting the AWS Shared Responsibility Model

22% of breaches start with stolen credentials. Credential-based breaches take **246 days** on average to identify and contain. Identity attacks rose **32%** in H1 2025.

SOURCES: VERIZON DBIR 2025 · IBM COST OF A DATA BREACH 2025 · MICROSOFT DIGITAL DEFENSE REPORT 2025

The recovery gap is real, and getting wider

Your company depends on identity for every login, every app, every workflow. IAM environments change constantly: admins onboard apps, rotate roles, update policies, push workflows. AI agents and service principals add thousands of non-human identities, each with its own bindings and tokens. A single mis-applied conditional access policy, a deleted group, or a compromised admin can disrupt authentication for the entire enterprise.

Identity providers are built to deliver authentication. You own the recovery. Recycle bins and soft-delete windows exist for convenience, not for disaster recovery: they do not provide full-tenant restore, point-in-time investigation, or tested recovery runbooks. When something breaks, IAM teams improvise under pressure, often without a known-good baseline to restore from.

How Acsense Backup & Recovery works

STAGE 1

Continuous Capture

Every IAM change captured automatically. Users, groups, apps, policies, workflows, NHIs.

→

STAGE 2

Time Machine + Change Log

Browse the full change history. Inspect any object at any past point in time.

→

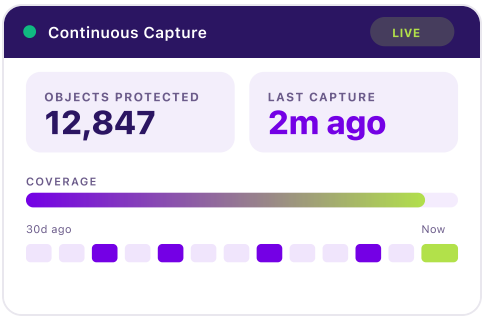
STAGE 3

Granular Restore

Roll back a single object, a bulk set, a policy, or the full tenant. In minutes.

Recover at every level, from a single object to a full tenant

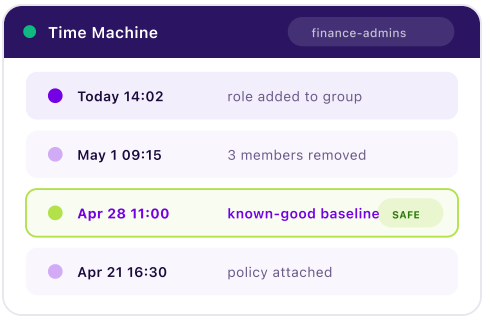
Acsense Backup & Recovery operates at the granularity the incident actually requires. Restore one user. One policy. A workflow. A bulk change. The whole tenant. Each restore is dependency-aware so the relationships between objects come back intact.



Continuous Data Protection

Every IAM change is captured the moment it happens. No scheduled backups, no missed windows, no gaps. Configurations, relationships, and metadata flow into a tamper-resistant change history that reflects your tenant's true state at every moment.

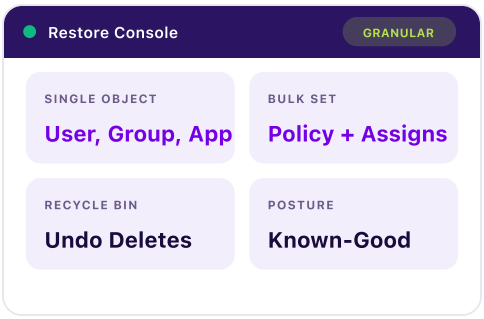
Real-time capture · Tamper-resistant · Tenant onboarding



Time Machine + Object Investigation

Browse the full change log. Compare any IAM object across any two points in time. Trace exactly what changed, when, and by whom, without piecing it together from raw audit logs. Built for incident response and audit evidence.

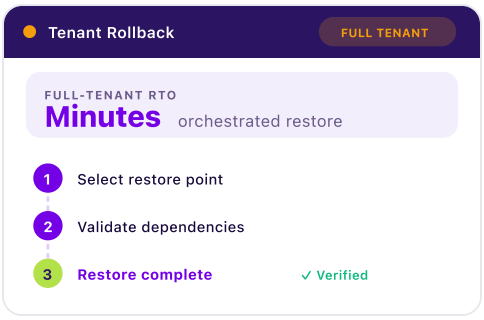
Point-in-time view · Diff & compare · Audit-ready evidence



Granular Recovery: single object to bulk set

Restore one user, one group, a policy and all its assignments, or a configuration baseline, without touching the rest of the tenant. Undo from the recycle bin in one click. Bulk-restore a workflow change that broke production. Posture recovery returns the tenant to a known-good state.

Single-object restore · Bulk recovery · Recycle bin undo · Posture recovery



Tenant Rollback + Tenant Investigation

For the largest blast radius (full tenant compromise, ransomware, mass mis-configuration), roll the entire tenant back to any prior point in time. Tenant Investigation lets you analyze tenant state at any past moment to understand what happened before you restore. Workflow Backup ensures even orchestrated identity flows survive.

Full-tenant rollback · Tenant investigation · Workflow backup

Real scenarios. Real recovery.

Backup & Recovery operates at the granularity the incident actually requires. Four scenarios from real IAM environments. Each at the tenant level, regardless of which IDP is running underneath.

WHEN THIS HAPPENS

Admin deletes a critical policy by mistake

Acsense: Time Machine + Single Object Recovery restore the policy and its assignments in under 5 minutes.

Authentication never went down. No P1, no escalation.

WHEN THIS HAPPENS

Compromised admin pushes mass mis-config

Acsense: Tenant Rollback to last known-good baseline; Tenant Investigation freezes a forensic snapshot in parallel.

Clean tenant restored. IR gets a full evidence trail.

WHEN THIS HAPPENS

Migration breaks 200+ user app assignments

Acsense: Bulk Recovery restores app assignments with dependencies intact (workflows, group rules, profile mappings).

Zero re-provisioning. Users never noticed.

WHEN THIS HAPPENS

Auditor asks "what changed in IAM last quarter"

Acsense: Object Investigation produces a full change history at any past point in time, by user, object, or scope.

Audit-ready evidence on demand. The change log is the evidence.

Why Acsense for Backup & Recovery

Purpose-built for cloud IAM

Not an AD tool retrofitted. Not a generic SaaS backup. Architected for the configuration complexity of cloud-native identity.

Recover in minutes, not days

Full-tenant RTO and RPO measured in minutes. Granular restore for every level, from single object to full tenant.

Time Machine for IAM

Full change history with point-in-time investigation. Trace exactly what changed, when, and by whom, across every object.

Dependency-aware restore

Objects are restored with their relationships intact. Policies with their assignments, workflows with their bindings.

IDP-agnostic by design

Acsense protects your tenant the same way regardless of which IDP runs it. Switch IDPs, add a second one, run hybrid. Your runbook stays the same.

NHI & AI agent coverage

Service principals, API tokens, and agent bindings are first-class objects: captured, restorable, and tracked alongside human identities.

Ready to recover any identity change in minutes?

See Acsense Backup & Recovery in action on your IAM tenant.

Request a demo

Built for the IAM admin, and everyone who depends on identity

Backup & Recovery is the operational foundation. The platform serves the people who keep IAM running every day, and the leaders who carry the risk when it doesn't.

IAM Administrators

Your job is to keep IAM running. Recover any identity change in minutes, from single object to bulk set to full tenant. Time Machine answers "what changed, when, and by whom" without piecing it together from raw audit logs.

IT & Operations Leaders

Defined RTO and RPO for identity infrastructure, measured in minutes, not days. One runbook, one console, one set of restore primitives, regardless of which IDP runs your tenant.

Security & CISO

Tamper-resistant change history and dependency-aware restore as the foundation for identity incident response. The recoverability evidence regulators ask for, produced automatically, not assembled in a fire drill.

AI & ML Leaders

Service principals, API tokens, and agent bindings are first-class objects in Acsense: captured, restorable, and tracked alongside human identities. As your NHI surface grows, recovery scales with it.

CERTIFIED & AUDITED

- **FedRAMP High** Authorized
- **SOC 2 Type II** Audited by EY
- **ISO 27001** Information Security
- **ISO 27017** Cloud Security
- **ISO 27018** Cloud Privacy

ABOUT ACSENSE

Acsense is the IAM Resilience Platform that protects, recovers, and continuously validates enterprise identity infrastructure at scale. The platform delivers Backup & Recovery, Configuration Management, Disaster Recovery, and Compliance & Assurance across Okta and Microsoft Entra ID, from a single purpose-built product. Acsense serves security-first enterprises and federal agencies across financial services, healthcare, critical infrastructure, public sector, and technology globally. Learn more at acsense.com.