



ANYCLOUD BACKUP FOR ENTRA ID

Safeguarding your identity infrastructure

Version 1.0 September 2025

any.cloud

Executive Summary

Microsoft Entra ID is the cornerstone of modern identity and access management. It enables secure authentication and authorization for thousands of applications and services, making it a critical component of business continuity and compliance.

While Microsoft ensures the uptime and availability of the Entra ID platform, the responsibility for protecting identity objects, policies, and configurations lies with the customer. Accidental deletions, misconfigurations, insider threats, and cyberattacks can disrupt business operations and create severe compliance risks.

Anycloud Backup for Entra ID addresses this challenge with a SaaS-based backup and recovery solution that ensures continuity, visibility, and compliance. Delivered through secure IBM Cloud datacenters worldwide, the service offers automated backups, air-gapped storage, and rapid recovery of Entra ID objects – enabling organizations to minimize downtime, meet regulatory requirements, and safeguard their identity infrastructure.

Why protect Entra ID?

Identity is now the most targeted attack surface in enterprise IT. Microsoft registers over 600 million identity-related threats every day. A single deleted policy, a compromised account, or an insider misconfiguration can disrupt critical business processes across the entire Microsoft 365 and SaaS ecosystem.

Key risk scenarios include:



Accidental deletion of users or groups



Misconfigured Conditional Access Policies



Malicious insider attacks



Ransomware or external cyber threats targeting identity data



Compliance violations under GDPR, DORA, and other regulations

Without a dedicated backup solution, recovering lost Entra ID data is time-consuming, incomplete, or in some cases impossible. Anycloud Backup for Entra ID closes this gap.

Key features and capabilities



Backup of users, groups, directory roles, application registrations, enterprise apps, Conditional Access Policies, administrative units, audit logs, and change history.



Rapid object-level restore of users, groups, apps, and policies directly back into Microsoft 365.



One-click restore to minimize downtime.



Comparison between current and previous backups to identify changes.



Backups are kept according to the customer's chosen retention policy, which can range from a day to unlimited.



GDPR-compliant "Right to be Forgotten" with a 72-hour grace period before permanent deletion.



Full logging of all backup and restore activities for audit readiness.



Cloud-to-cloud backup model with full segregation of duties (SoD).



Air-gapped storage in IBM Cloud datacenters with minimum Tier-3 certification.



AES-256 encryption in transit and at rest.



Insider Threat Protection with 30-day retention of deleted identity data.



Multi-role access through Role-Based Access Control (RBAC).



Centralized management portal for scheduling, monitoring, and restoring backups.



Detailed security dashboard with risk score, recommendations, and audit trail.



Configurable notifications and daily backup reports.

Security and governance

Enterprise-grade security

Anycloud Backup for Entra ID is designed with a defense-in-depth approach to protect sensitive identity data against both external and internal threats. Security measures include:

- **AES-256 encryption** applied in transit and at rest, ensuring that no data is readable by third parties.
- **Air-gapped architecture** that isolates backups from the production tenant, preventing ransomware or malware from spreading into backup environments.
- **Immutable storage options** with IBM Object Lock technology, preventing backups from being modified, overwritten, or deleted during the defined retention period.
- **Multi-factor authentication (MFA)** for all administrative access to the management portal.
- **Insider Threat Protection (ITP)**, which retains deleted identity objects for 30 days, safeguarding against accidental or malicious deletion.

ISO 27001
CERTIFIED

ISAE 3000
ASSURANCE REPORT

CLOUD SECURITY
ALLIANCE

Governance and control

Beyond technical protection, the solution provides comprehensive governance features that strengthen security oversight and policy compliance:

- **Full audit logging** of all backup and restore operations, including user activity, timestamps, and object-level details, supporting both internal governance and external audit requirements.
- **Change comparison tools** that allow administrators to review modifications between backups and the live environment, increasing visibility into configuration drift and unauthorized changes.
- **Security dashboard** with consolidated visibility into identity backup status, risk posture, and actionable recommendations for strengthening identity governance.



Compliance assurance

With built-in features for data privacy and governance, Anycloud Backup for Entra ID supports compliance with leading regulations and frameworks, including:

- **GDPR** with support for the “Right to be Forgotten” through controlled and auditable user deletion workflows.
- **DORA (Digital Operational Resilience Act)** by ensuring identity continuity and providing verifiable recovery time objectives (RTO) and recovery point objectives (RPO).
- **ISO 27001 and ISAE 3000** alignment, ensuring robust controls around information security and data management.

Risk management

By combining advanced backup technology with governance features, Anycloud Backup for Entra ID reduces operational, compliance, and security risks across the identity landscape. This enables IT and security leaders to maintain control over one of the most critical assets in modern enterprises – the identity fabric that underpins all access to business systems and data.

Business benefits



Business continuity

Identity-related objects can be restored within minutes, ensuring minimal downtime and continuity of critical services.



Security assurance

Identity data remains fully protected from cyberattacks, insider threats, and administrative errors.



Regulatory compliance

Built-in features such as audit logs, retention flexibility, GDPR deletion, and immutable storage ensure compliance with GDPR, DORA, and ISO standards.



Operational efficiency

Streamlined onboarding, automated backup scheduling, and centralized management reduce administrative workload and complexity.

LET'S STAY CONNECTED

Anycloud A/S
Hedegaardsvej 88
2300 Copenhagen S
Denmark

CVR: DK31161509
E-mail: sales@anycloud.dk

any.cloud