NinjaOne Entra Backup

Strengthen Your Identity and Access Protection

Microsoft Entra ID is the foundation of identity and access for Microsoft 365. It governs how users, devices, and applications connect securely.

As cyber threats increasingly target identity systems, Microsoft Entra has become a major attack surface.

Misconfigurations and policy drift can lead to lockouts, security gaps, and compliance risks. Protecting the full identity infrastructure, including Conditional Access policies, device configurations, and app service principals, is essential.

Entra Backup helps turn backup into a critical layer of a company's security posture and cyber resilience strategy.

Key risks in failing to back up Entra ID

Built-in protection is not enough

In Microsoft's own words: "Unintended deletions and misconfigurations will happen to your tenant. To minimize the impact of these unintended events, you must prepare for their occurrence."[1]

Security blind spots are leaving gaps

Entra has become a top attack surface. According to the Microsoft Digital Defense Report, approximately 90% of organizations surveyed experienced at least one identity-related security incident in 2024. Misconfigured Conditional Access or device policies can create security gaps and increase breach risk. With audit logs limited to just 30 days, it's difficult to conduct thorough investigations or meet long-term compliance requirements.

Manual recovery means downtime

There's no "undo" in Microsoft Entra. Accidental deletions or misconfigurations can take hours or days to fix, leaving users locked out and businesses exposed in the meantime. Recovery is entirely manual, and the burden falls on the organization.

1. https://learn.microsoft.com/en-us/entra/architecture/recoverability-overview

Protect against risks with Entra Backup

Entra Backup protects Entra ID configurations, minimizes downtime, and enables rapid recovery from data loss or cyberattacks.

Unlimited data retention: Retain long-term historical records of Entra ID data beyond Microsoft's 30-day limit.

Granular recovery: Instantly restore specific security settings or policies to a known-good state. Reduce billable support hours and restore productivity faster.

Tracking of configuration changes: Identify and track configuration changes without digging through limited audit logs. Search by attributes or previous values to pinpoint issues quickly.

Resilience against ransomware & human error: Bounce back from accidental policy deletions, junior admin errors, or targeted identity attacks in seconds instead of weeks.

Support for compliance & governance: Maintain a reliable, long-term record of Entra settings to meet audit requirements and reinforce policy controls.

What could go wrong?

Ransomware attack: A client is hit. Email is safe, but Entra is locked down. With Entra Backup, restore Entra, Intune, and access rules to get users back online fast.

End-user error: A junior admin disables a critical Conditional Access policy. Entra Backup rolls it back in seconds. No downtime, no blame.

Policy oversight: During onboarding, app service principals aren't replicated. Automations break. Entra Backup ensures they're recoverable and secure.

Entra Backup capabilities

Quick setup
Deploy quickly with a simplified onboarding process designed for efficiency. Start protecting Entra environments (including devices) in minutes.

Snapshot search
Search historical snapshots by object type, attribute, or configuration value. Easily locate and resolve issues.

Live comparison
Compare current configurations to backup snapshots to detect unauthorized or accidental changes. Accelerate incident response and policy recovery.

Point-in-time restore (PITR)
Perform a full system recovery to a specific point in time for minimal data loss and a quick return to normal operations.

Attribute-level restore
Restore specific policy elements or object attributes without affecting unrelated settings. Maintain control and avoid unnecessary overwrites.

Relationship-aware recovery
Automatically preserve object relationships like group memberships, role assignments, and app associations, so restores are complete and functional.

Entra ID features included	
Users	✓
Groups	✓
Roles	✓
Custom roles	✓
App registrations	✓
Enterprise applications	✓
Conditional Access policies[1]	✓
Device and Intune policies[2]	✓
BitLocker recovery keys	✓
Devices	✓
Administrative units	Coming soon
Sign-in logs	Coming soon
Audit logs	Coming soon

1. Including named locations, authentication strengths, and authentication contexts
2. Including compliance policies, configuration profiles, and Intune device compliance policies

Entra Backup plans

Features	Entra Backup with SaaS Backup	Entra Backup with Archiver
Entra ID & device backup protection	✓	✓
Incremental backup for continuous protection	✓	✓
Email journaling	✗	✓
Unlimited storage	✓	✓
Advanced search	✓	✓
Search within documents	✗	✓
Granular, point-in-time restore	✓	✓
Role-based access control*	✓	✓
Reporting dashboard	✓	✓
Retention policies	Flexible options	Fully customizable policies
Audit log	✓	✓
eDiscovery & saved searches	✗	✓
Tagging & alerting	✗	✓
Legal hold & data review process	✗	✓

* RBAC unavailable for support or finance roles

Why NinjaOne?

Contact us today to discover how Entra Backup can safeguard your business. With NinjaOne, you will benefit from unmatched data protection, effortless scalability, and peace of mind that your critical configurations are always secure. Start an Entra Backup free trial today!

US (888) 542-8339 / **DE** +49 (0)30-76758700 / **UK** +44 (0)20 3880 9027 / **FR** +33 (0)800 91 09 90 / **AU** +61 1800 490 516 / sales@ninjaone.com