Barracuda Entra ID Backup

Easy-to-use, cloud-first backup for your Entra ID data

Microsoft recommends utilizing a third-party backup solution for safeguarding your Entra ID data. In the event of a cyberattack or accidental deletion, having a reliable backup with quick recovery capabilities is crucial. Restoring any user information can be a labor-intensive, manual process. Entra ID data is vital to your operations and downtime can be expensive.

Barracuda Entra ID Backup offers a user-friendly, cloud-based solution managed in the same Barracuda Cloud-to-Cloud Backup application that customers use today to manage their Microsoft 365 backup data. Entra ID Backup delivers comprehensive and cost-efficient backup and recovery services for your Entra ID data. This includes backing up 13 Entra ID components that can be safeguarded and recovered at any time.

Recover from errors and malicious attacks

Attackers may target your Entra ID data as they know you rely on it to keep track of who has access to applications in your organization. Without Entra ID data, your workforce will not be able to log in and do their work — which increases the chance that attackers will receive a ransomware payment. Microsoft only retains your Entra ID data for 30 days and recommends backing up your data — including Entra ID.

With Entra ID Backup, organizations can go back as far as needed to reverse accidental changes, well beyond the 30-day max retention period Microsoft provides.

Even in the case of accidental data loss, you need to have a secure backup of your most important data — including SaaS data such as Entra ID.

Cost-effective data protection

Entra ID backup provides a comprehensive, cost-effective solution for safeguarding your critical data in the cloud. With seamless cloud-to-cloud backup, advanced encryption and easy recovery options, it ensures the security and availability of your information.

Entra ID Backup offers you simple, per-user pricing for cost predictability if purchased on its own. When you license Cloud to Cloud Backup, you get user backup of Entra ID included at no additional charge.

In addition, Entra ID provides unlimited storage and retention. That means that your organization can go back as far as needed to audit and retrieve the data required.

Easy to use

The user interface is globally accessible, ensuring that you can quickly and effortlessly locate and recover your data. With highly efficient search and filter options, the process of restoring data back to your organization is made as simple as possible.

You can easily monitor the status of your backups, assess the health of your data and access storage statistics. Additionally, an audit log and email alerts keep you well-informed about the details of every action taken, ensuring you stay updated on the backup process.

Quick to deploy, easy to use

- Easy to deploy, manage and use
- All-inclusive, per-user licensing
- From sign up to running first backup in 5 minutes
- Managed in the same intuitive, trusted Cloud-to-Cloud Backup available for backing up your Microsoft 365 data
- Fast and easy to find and recover data
- Point-in-time recovery
- Scheduled or on-demand backup
- Multifactor authentication
- Five levels of role-based access control — you decide who can back up, restore, export, or view reports
- Barracuda Cloud Storage is SSAE Type II certified
- Multi-tenant support
- Available in Japanese, French, Italian, German, Spanish, and English localized versions

Flexible recovery

- Full or granular restore of user, group, role, or administrative unit objects
- Protection for Entra ID components:
  - Users, groups, roles, organizational units
  - App registrations
  - Audit logs
  - Authentication method policies
  - Authentication dtrength policies
  - BitLocker keys
  - Conditional access policies
  - Device management
  - Enterprise applications
  - Named locations
- Unlimited storage and retention — retain all your data for as long as you need
- Flexible recovery
- Restore any data to original location
- Retain data for inactive objects
- Delayed cloud purging for ransomware protection
- Granular reporting
- Detailed reporting for backups and restores
- Audit-log reporting for all actions across your account
- Configurable email notification — monitor your account through customizable email reports

Cloud native

- Full software-as-a-service solution — no hardware, software, or patches to manage
- Instant scalability
- 13 regional storage locations available worldwide to meet data storage and residency requirements
- Independent SOC2 audited and certified annually
- User data is encrypted in transit (TLS) and at rest using industry-standard AES 256* encryption
- Retain multiple external copies of backed up data

Barracuda