

Dropsuite Entra Backup

Fortify your data protection and security with Entra Backup

Think of Microsoft Entra ID as your business's central access hub for all Microsoft tools and resources. This cloud-based solution manages employees access, organizes users into groups with tailored permissions, and ensures robust security.

However, mistakes like accidental configuration changes, deleted identities, or malicious activity can cause serious disruptions. With cyber threats on the rise, identity systems are increasingly targeted, potentially resulting in unauthorized access, data breaches, financial losses, or compliance violations.

A reliable backup ensures you can quickly restore critical settings, permissions, and identities if something goes wrong, reducing downtime and protecting your business from costly risks.

Mitigate Risks with Dropsuite Entra Backup

Dropsuite Entra Backup protects Entra ID data from data loss or cyberattacks. Key benefits include:

- **Protect Critical Data Beyond 30 Days:** Safeguard Entra ID records with unlimited retention, ensuring recoverability beyond Microsoft's 30-day limit. Ensure compliance with open-standard data export for thorough change tracking and regulatory requirements.
- **Get Back to Operations:** Revert undesired changes quickly in minutes instead of days.
- **Mitigate Risks:** Identify changes rapidly to prevent misconfigurations and security breaches.

Dropsuite Entra Backup Capabilities

- ✓ Rapid deployment with simple setup
- ✓ Quick snapshot searches for specific attributes
- ✓ Comparison of backup snapshots to live data
- ✓ Full system recovery to a specific point-in-time
- ✓ Restore specific attributes with precision
- ✓ Relationships and object data restore

Why Choose Dropsuite

Contact your reseller today to discover how Dropsuite Entra Backup can safeguard your business. With Dropsuite, you'll enjoy unmatched data protection, seamless scalability, and the peace of mind that your critical configurations are always secure.

Key Risks with Entra ID

- ✓ Many Entra features lack a recycle bin, and where one exists, data is permanently lost after 30 days.
- ✓ Entra ID lacks native backup capabilities, placing the responsibility for data loss protection on the customer.
- ✓ The lack of an "undo" function makes recovery slow and costly from extended downtime.
- ✓ Audit and sign-in logs are limited to 30 days, preventing long-term change tracking.
- ✓ Identity data is a prime target for cybercriminals.

Entra Features	Backup Coverage
Users	✓
Groups	✓
Roles	✓
Custom Roles	✓
App Registrations	Coming soon
Enterprise Applications	Coming soon
Conditional Access Policies	Coming soon
Administrative Units	Coming soon
Sign-in Logs	Coming soon
Audit Logs	Coming soon
Bitlocker Keys	Coming soon
Devices	Coming soon