

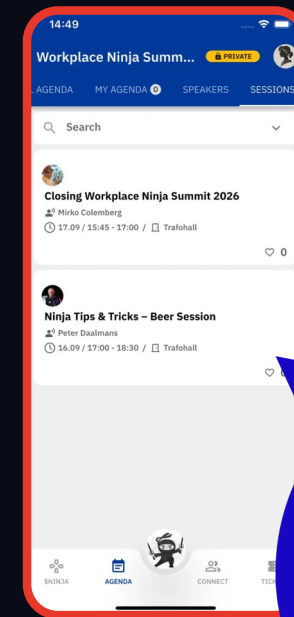
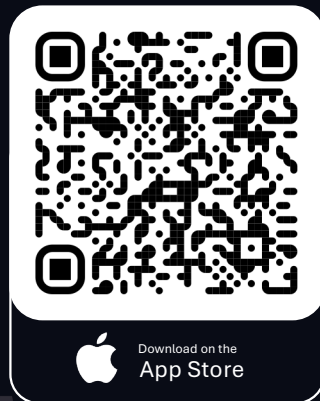
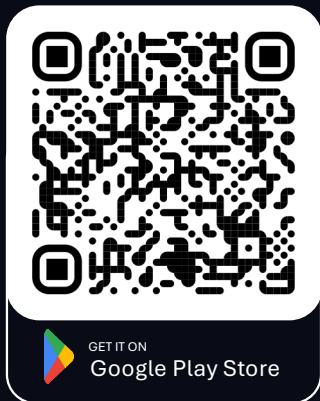
**SHARING KNOWLEDGE.
TOGETHER.**

**WORKPLACE
NINJA**

**SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT**



Check in and rate this session in the Workplace Ninja Summit 2026 app



We appreciate
your feedback!

Welcome on stage



Session

Deletion Happens –
Are you Ready for Recovery in Entra ID?

Community Stage
room check-in



Speaker

Klaus Bierschenk
CGI Germany, Microsoft Security MVP

#wpninjas

Thank you to our sponsors!



PLATINUM SPONSORS

glueck  kanja

 PATCH MY PC

Recast

 2Pint

 Microsoft

GOLD SPONSORS

control  UP

 Admin
By Request
ZERO TRUST PLATFORM

eido

THREATLOCKER®
ZERO TRUST PLATFORM

inforcer 

baseVISION
Trusted Swiss Cybersecurity


robopack

 EPIC FUSION
BRING IT ALL TOGETHER


nerdio

SILVER SPONSORS

 systemcenterdudes

Apento

water 
IT Security & Defense

 ugurlabs

About Klaus Bierschenk



Focus

Identity / Security

From

Murnau / Germany (1h south of Munich)

My Blog

<https://Nothingbutcloud.net>



Certifications



Hobbies

Sports, Mountains

Contact

[linkedin.com/in/klabier/](https://www.linkedin.com/in/klabier/)

Klaus@nothingbutcloud.net /

Trust is good, backup is better!
So, what's our topic today?



- Microsoft's position on backup and restore in Entra ID?
- How can we back up Entra ID? Or should we rather ask: what can actually be restored?
- Security: How can we prevent object or configuration loss in Entra ID?

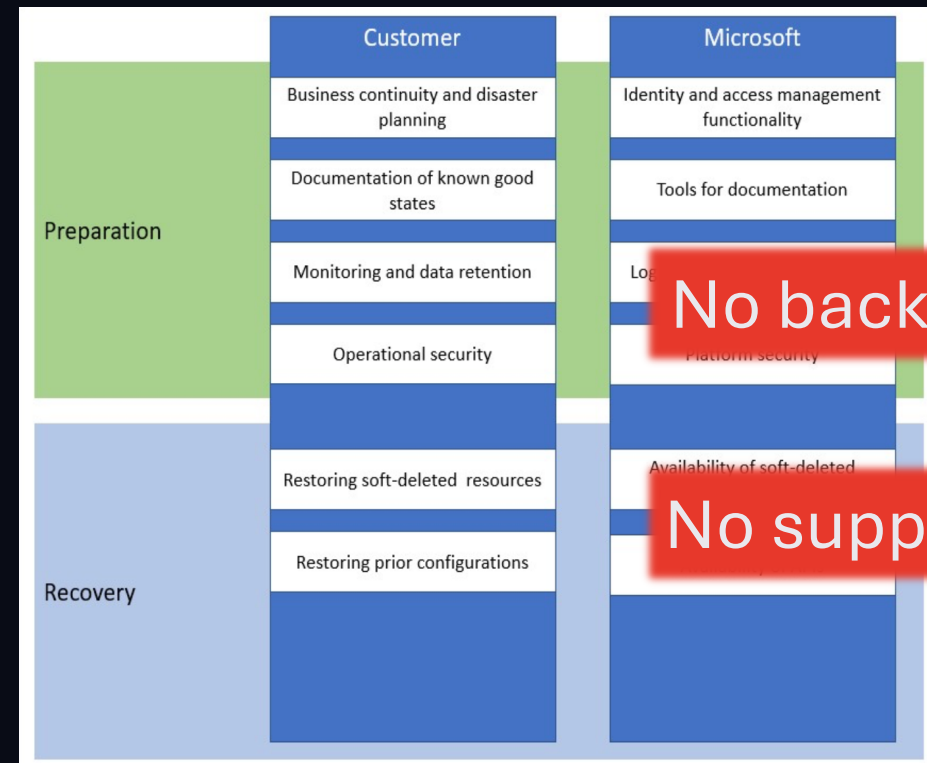
No commercials inside

MS standpoint on backup / restore in Entra ID



Microsoft provides platform & APIs

Customer responsible for planning & restoring



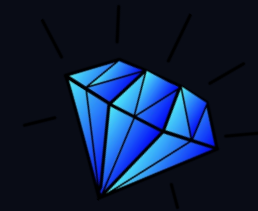
<https://learn.microsoft.com/en-us/entra/architecture/recoverability-overview>

#wpninja

Prioritize your crown jewels



- **Knowing what is really important** - otherwise a recovery concept becomes difficult
- Every company is different, every Entra ID Tenant is different – not everything is always equally critical
(e.g. when a Tenant has Security Defaults enabled, backing up CAs is not the major topic)
- Sometimes proper documentation is enough. Sometimes a backup procedure is the better choice
(e.g. with +50 CA policies, documentation alone is not sufficient)



Many settings. Which ones really matter?



User Management & Settings

- User roles & permissions
- Default sign-in options for users
- User lifecycle policies
- Locked account policies
- User sign-in & session policies
- Policies for secondary email addresses
- User sign-in logs & auditing
- Management of authentication methods
- Self-service user registration

Authentication & Security

- Multi-Factor Authentication (MFA) policies
- Passwordless authentication (FIDO2, Windows Hello)
- Certificate-based authentication
- Token lifetimes & session configuration
- Continuous Access Evaluation (CAE)
- Risk-based authentication
- Identity risk policies
- Authentication strengths for external users
- Adaptive authentication policies

Password Policies & Password Protection

- Password length & complexity requirements
- Password expiration period
- Banned password policy (custom deny list)
- Smart logout policy (failed sign-in attempts)
- Self-Service Password Reset (SSPR) policies
- Security questions for SSPR
- Temporary Access Pass policies
- Advanced password protection policies for on-premises AD

Global Secure Access (GSA)

- Network access policies
- Conditional access for network connections
- Configuration of network segments
- Access to corporate resources
- Traffic filtering for mobile apps
- Assignment of network resources
- Zero Trust Network Access
- Web content filtering
- DNS security policies
- Logging & monitoring for network access

Global Secure Access (GSA)

Group Management

- Dynamic group policies
- Group-based license assignment
- Self-service group management policies
- Automatic group membership based on attributes

Guest Users & External Collaboration (B2B/B2C)

- Guest invitation settings
- External identity providers (Google, Facebook, SAML, OpenID)
- B2B collaboration policies
- Guest user permission policies
- Automate external user deletion
- Session policies for guest users

Entra Cloud Sync Settings

- Entra Cloud Sync
- Attribute mapping
- Custom export rules
- Synchronization of user profiles
- Hybrid synchronization options (password sync)
- Password Hash Sync
- SCIM synchronization with third-party providers
- On-premises directory synchronization (Azure AD Connect)
- Custom synchronization rules

Conditional Access & Access Control

- Policies for users & groups
- Device state & compliance-based policies
- Session policies & token lifetimes
- Adaptive access policies
- Conditional Access
- Anomaly detection
- Cross-tenant access
- Security levels
- Terms of use policies

Conditional Access & Access Control

Security & Monitoring Policies

- Security alerts & Identity Protection
- Identity protection and risk detection settings
- Audit logging for identity activities
- Anomaly detection for sign-in attempts
- Security assessments & recommendations

Roles & Permissions (RBAC & PIM)

- Custom roles & permissions
- Least privilege access policies
- Time-bound role assignments (Just-In-Time)
- Approval workflows for admin roles
- Audit logs for privileged roles
- Security reviews for highly privileged accounts

Identity Governance & Compliance

- Regular access reviews
- Automatic deactivation of access
- Compliance reporting
- Automated access requests
- Entitlement management
- Access reviews

Device Management & Microsoft Entra Cloud Sync

- Register devices in Entra ID (Hybrid Azure AD Join, Azure AD Join)
- Device tagging and compliance
- Device management for Windows, macOS, iOS, and Android
- Enable/disable devices in Entra ID
- Device lifecycle management
- Configure and manage Entra ID Cloud Sync
- Define synchronization filters for groups and users
- SCIM synchronization with third-party services
- Manage on-premises directory synchronization (Azure AD Connect, Cloud Sync)

Application Management & Access Controls

- Add/remove enterprise applications
- Enable Single Sign-On (SSO) for applications
- Configure App Proxy for legacy applications
- Define OAuth and OpenID Connect policies
- Configure third-party identity providers
- Manage token lifetimes for applications
- Define Conditional Access policies for applications
- Configure user and group permissions for apps
- Set up managed identities for services

Administrative Units (AUs)

- Administrative Unit objects
- Assign users & groups to AUs
- Role-based access control
- Delegated administration
- Policies for AUs

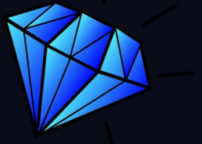
Administrative Units (AUs)

Tenant Settings & Organizational Policies

- Manage tenant settings and domains
- Configure organizational branding
- Define privacy policies for identities
- Restrictions for multi-tenant organizations
- Enable Microsoft Entra ID Governance
- Manage Adaptive Application Controls
- Conditional Access for tenant-level policies
- Control self-service group management

Microsoft Entra Cross-Tenant Access

- Policies for cross-tenant collaboration
- Manage external access to organizational resources
- Define tenant-based authentication rules
- Adaptive authentication mechanisms for external users



(just the big picture – not for detailed reading)

#wpninjas

Entra object restore – reality check



Object type	Soft delete	Restore?
User object	✓	🗑️ 30d Recycle Bin -> Preview from Nov `22
Security group	✓	🗑️ 30d Recycle Bin -> Preview from Nov `22
M365 group	✓	🗑️ 30d Recycle Bin -> Preview since Jun `22
Device object	✓	🗑️ 30d Recycle Bin -> Preview since Jun `22
Enterprise Application	✓	🔄 Multi-Tenant -> Deleted Item API (30d)
App Registration	✓	🗑️ Recycle Bin (Secrets)
Administrative Unit	✓	🔄 Deleted Item API (30d)
Conditional Access	✓	🗑️ New since Sept 2022

```

1  {
2    "id": "049fab0d-a309-43b9-a3f9-e2f25aa9caf8",
3    "templateId": null,
4    "displayName": "CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA",
5    "createdDateTime": "2022-07-05T17:05:36.8206457Z",
6    "modifiedDateTime": "2025-07-31T19:38:28.5262738Z",
7    "state": "enabled",
8    "deletedDateTime": null,
9    "partialEnablementStrategy": null,
10   "sessionControls": null,
11   "conditions": {
12     "userRiskLevels": [],
13     "signInRiskLevels": [],
14     "clientAppTypes": [ ...
15   ],
16   "platforms": null,
17   "locations": null,
18   "times": null,
19   "deviceStates": null,
20   "devices": null,
21   "clientApplications": null,
22   "applications": { ...
23 },
24 "users": {
25   "includeUsers": [ ...
26 ],
27   "excludeUsers": [
28     "08a644d4-6533-4931-9158-edee7db7fffa",
29     "349c5270-e777-4727-b655-43f99f454dc2"
30   ],
31   "includeGroups": [],
32   "excludeGroups": [
33     "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
34   ],
35   "includeRoles": [],
36 }
37 }
38 }
39 }
40 }
41 }
42 }
43 }
44 }
```

🗑️ Restore via Recycle Bin, 🚫 no Restore at all, 🔄 Restore via API

Entra object restore – reality check



Object type	Soft delete	Restore?
User object	✓	30d Recycle Bin -> Hard deleted
Security group	✓	30d Recycle Bin -> Hard deleted Preview from Nov `25 and GA since Feb. `26 - Previously: No restore
M365 group	✓	30d Recycle Bin -> Hard deleted
Device object	✓	30d Recycle Bin -> Hard deleted Preview since Jun `26 – Previously No restore
Enterprise Application	✓	Multi-Tenant -> Deleted Item API Single-Tenant -> App Reg Recycle Bin
App Registration	✓	Recycle Bin (Secrets & Certs ✓)
Administrative Unit	✓	Deleted Item API (30d) -> Hard deleted
Conditional Access	✓	New since Sept 2025 Recycle Bin - Previously: Deleted Items API only

Restore via Recycle Bin, no Restore at all, Restore via API

#wpninjas



**MARTY, WE HAVE TO GO
BACK**

Demo



Administrative Unit
restore via
Microsoft Graph API



Recover via deletedItems API



URLs:

Enterprise Applications

<https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.serviceprincipal>

Administrative Units

<https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.administrativeUnit>

(Post) <https://graph.microsoft.com/v1.0/directory/deletedItems/Object-ID/restore>

Conditional Access Policies

<https://graph.microsoft.com/beta/identity/conditionalAccess/deletedItems/policies>



How to create a smart and easy backup?



→ Manually difficult (Entra Admin Center, CSV etc.)

Code-based approaches are much better

→ PowerShell is your friend

Some manual tweaking... JSON must be precise – e.g. read-only attributes

→ EntraExporter 3.01 is your better friend 🧐

Download here: [Open-Source GitHub](#)

Demo ...

→ Check out Backup and Recovery (Preview since Mar `26 and P1/P2 req)

Easy built-in functionality (keep in mind: one backup per day and seven days history max.!)

Demo ...

→ Once upon a time there was M365DSC as another great friend 🧐

But now we have [Tenant Configuration Management](#) (API GA since May `26) – Entra Admin Center in Preview

Demo



Tenant Configuration

Snapshot Managament



How ready is Configuration Management



→ Snapshots

This is my tenant right now

- Retained for 7 days
- Can be downloaded for long-term retention
- Can be used as a starting point for a baseline

→ Baseline

This is my desired configuration

- Declarative JSON representation of the desired state
- Can be created from a snapshot and then edited
- Contains only the resources/properties you want to monitor

→ Monitor

Tell me when it no longer matches

- **Compares Actual State vs. Desired State every 6 hours**
- No built-in notifications or remediation
- Need *who / when / how?* → check Audit Logs

→ Configuration drift

Something changed

- Resource no longer matches the baseline
- Shows Current vs. Desired
- After remediation, the next run marks the drift as Fixed

Hard deleted? And now what?



- Object must be recreated
- Object will become a new ID
- Previous JSON export required (EntraExporter)
- Example article on rebuilding a hard-deleted Administrative Unit on my blog
<https://nothingbutcloud.net/2025-08-30-DeletedEntraObjects/>
- Microsoft cannot help



To make sure it never comes down to a restore



- ✓ Protect sensitive Groups with „PIM Protected Groups“
→ possible, but should you?
- ✓ Restricted Management AU
- ✓ Protected Actions for hard deletions
- ✓ Smart Alerting for important Resources
Example implementation on my blog

Demo ...

Demo ...

<https://nothingbutcloud.net/2025-12-16-ZeroTrust-Monitoring/>



Summary: back to the “Agenda Questions”



- ✓ Microsoft's standpoint is clear
- ✓ It is up to the Tenant Admins to define what is important
- ✓ Regularly reassess your crown jewels: what is truly important, and choose the right backup approach
- ✓ Protective measures against configuration loss: *Who can do what?*
Being proactive instead of reactive saves time and nerves



Further Resources ...



Microsoft Learn

[Recoverability best practices](#) (covers Microsoft standpoint in shared responsibility)

[MS Learn: Recover from deletions](#)

[MS Learn: List deleted Item API Objects](#)

[MS Learn: Restore deleted Items and permissions](#)

[MS Learn: Application objects, service principals etc.](#)

[Use the unified tenant configuration management APIs in Microsoft Graph \(NEW\)](#)

[Microsoft Entra Backup and Recovery overview \(Preview\)](#)



Best Practices & Community

[Restricted management administrative units in Microsoft Entra ID](#)



NothingButCloud Blog

[Can I restore deleted Entra objects? Yes? No? Maybe?](#)

[Protecting your Conditional Access Policies: Lean Backup Strategies for Entra ID](#)

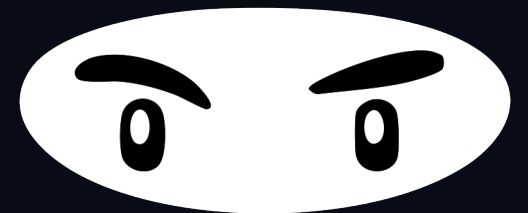
**Thank You,
Ninjas!**



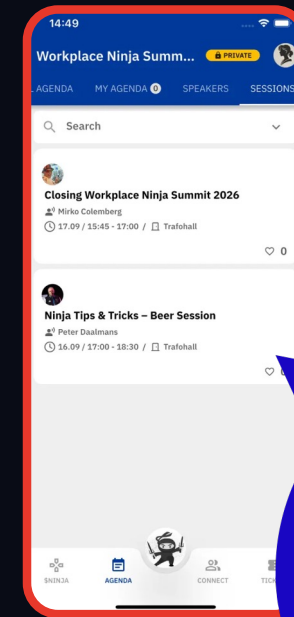
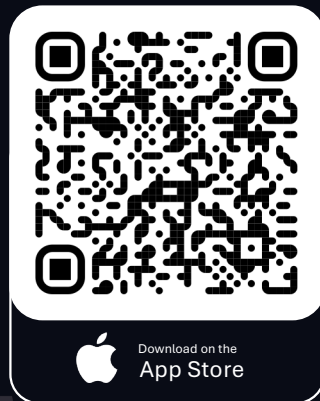
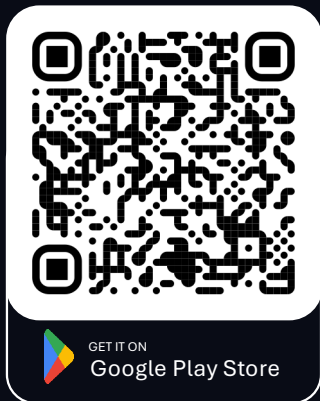
See You
Next Year!



SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT



Download the app and never miss any updates



We appreciate
your feedback!