CTTT

★ Est.2023 ★

Entra Backup?
Think You Have One?
Think Again!

Klaus Bierschenk

Klaus Bierschenk

Director Consulting Expert @ CGI Germany

- Based in Murnau am Staffelsee in Germany
- With my Family, two cats, two snakes
- Mountain lover, Ultra Runner

✉ Klaus@nothingbutcloud.net

https://nothingbutcloud.net

@klabier.bsky.social

www.linkedin.com/in/klabier

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

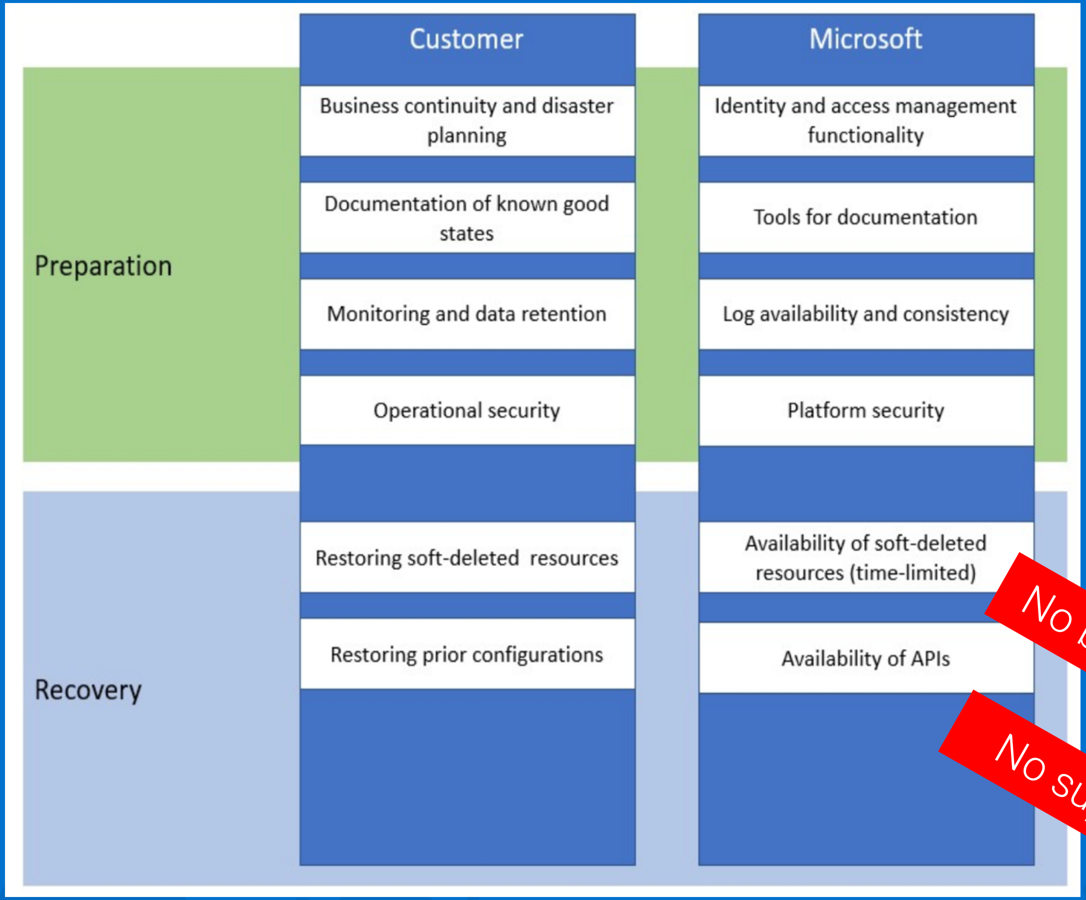
No commercials

- ❖ What is 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?
- ❖ Operational prerequisites: How can we prevent object or configuration loss in Entra ID?

What is Microsoft’s standpoint on backup and restore in Entra ID ?

Microsoft provides platform & APIs

Customer responsible for planning & restoring



	Customer	Microsoft
Preparation	Business continuity and disaster planning	Identity and access management functionality
	Documentation of known good states	Tools for documentation
	Monitoring and data retention	Log availability and consistency
	Operational security	Platform security
Recovery	Restoring soft-deleted resources	Availability of soft-deleted resources (time-limited)
	Restoring prior configurations	Availability of APIs

No backup...

No support...

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

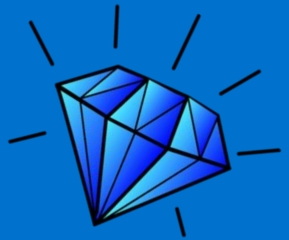
Prioritize your crown jewels

- → *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 lockout 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)
…ccess policies
…twork connections
…ments
Assignment…
Zero Trust Network Acces…
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

…Cloud Sync & Synchronization Settings
E… …figuration
A…
(…
Hybrid sy… …Auth,
Password Hash Sync)
SCIM synchronization with third-party prov…s
On-premises directory synchronization (Azure AD Connect)
Custom synchronization rules

Entra Cloud Sync & settings

Conditional Access & Access Control
Policies for users & groups
Device state & compliance-b…
Session policies & t…
Adaptive ac…
Co…
A…
C…
Se… …xternal identities
Te… …se pages

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 & Co…
Regular access re…
Automati…
(…
A… …apps
E… …policies
Ac… …orkflows

Identity-Governance & Compliance

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 U…
Administrati…
Assig…
…y for AUs
…specific AUs

Administrative Units (AUs)

Tenant Settings & Organizational Policies
Manage tenant name 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)

Entra object restore – reality check

Objekttyp	Soft delete	Restore?
User object	✓	🗑 30d Recycle Bin -> Hard deleted
Security group	✓	~~🚫 No restore ⚠~~ new since Nov 2025 Recycle Bin (Public Preview)
M365 group	✓	🗑 30d Recycle Bin -> Hard deleted
Device object	✗	🚫 No restore -> New registration (dsregcmd.exe)
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	✓	🔄 Previously: Deleted Items API only -> new since Sept 2025 Recycle Bin 🗑

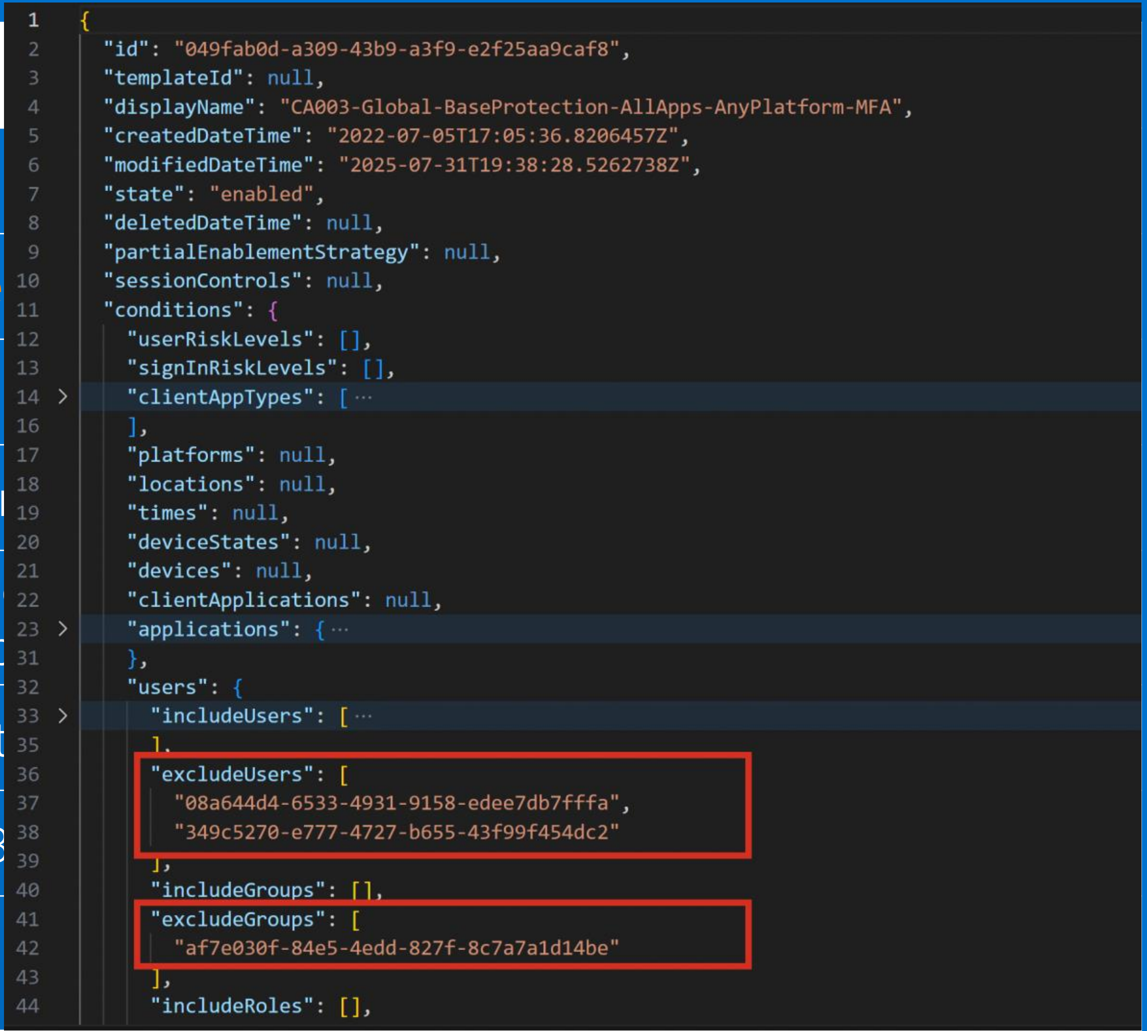
🗑 Restore via Recycle Bin, 🚫 no Restore at all, 🔄 Restore via API

Microsoft Learn Article

Entra object restore – reality check

Objekttyp	Soft delete	Restore?
User object	✓	🗑 30d Recycle Bin ->
Security group	✓	~~🚫 No restore ⚠~~ ne
M365 group	✓	🗑 30d Recycle Bin ->
Device object	✗	🚫 No restore -> New
Enterprise Application	✓	🔄 Multi-Tenant -> Del 🔄 Single-Tenant -> Ap
App Registration	✓	🗑 Recycle Bin (Secret
Administrative Unit	✓	🔄 Deleted Item API (3
Conditional Access	✓	🔄 Previously: Deleted 🗑

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



```
{
  "id": "049fab0d-a309-43b9-a3f9-e2f25aa9caf8",
  "templateId": null,
  "displayName": "CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA",
  "createdDateTime": "2022-07-05T17:05:36.8206457Z",
  "modifiedDateTime": "2025-07-31T19:38:28.5262738Z",
  "state": "enabled",
  "deletedDateTime": null,
  "partialEnablementStrategy": null,
  "sessionControls": null,
  "conditions": {
    "userRiskLevels": [],
    "signInRiskLevels": [],
    "clientAppTypes": [ ···
    ],
    "platforms": null,
    "locations": null,
    "times": null,
    "deviceStates": null,
    "devices": null,
    "clientApplications": null,
    "applications": { ···
    },
    "users": {
      "includeUsers": [ ···
      ],
      "excludeUsers": [
        "08a644d4-6533-4931-9158-edee7db7fffa",
        "349c5270-e777-4727-b655-43f99f454dc2"
      ],
      "includeGroups": [],
      "excludeGroups": [
        "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
      ],
      "includeRoles": [],
```

Microsoft Learn Article

Demo:

Restore Administrative Unit 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

Conditional Access Policies
https://graph.microsoft.com/beta/identity/conditionalAccess/deletedItems/policies

JAMES MONTGOMERY FLAGG
I WANT YOU
To protect your
Entra Crown Jewels

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 – read-only attributes e.g.

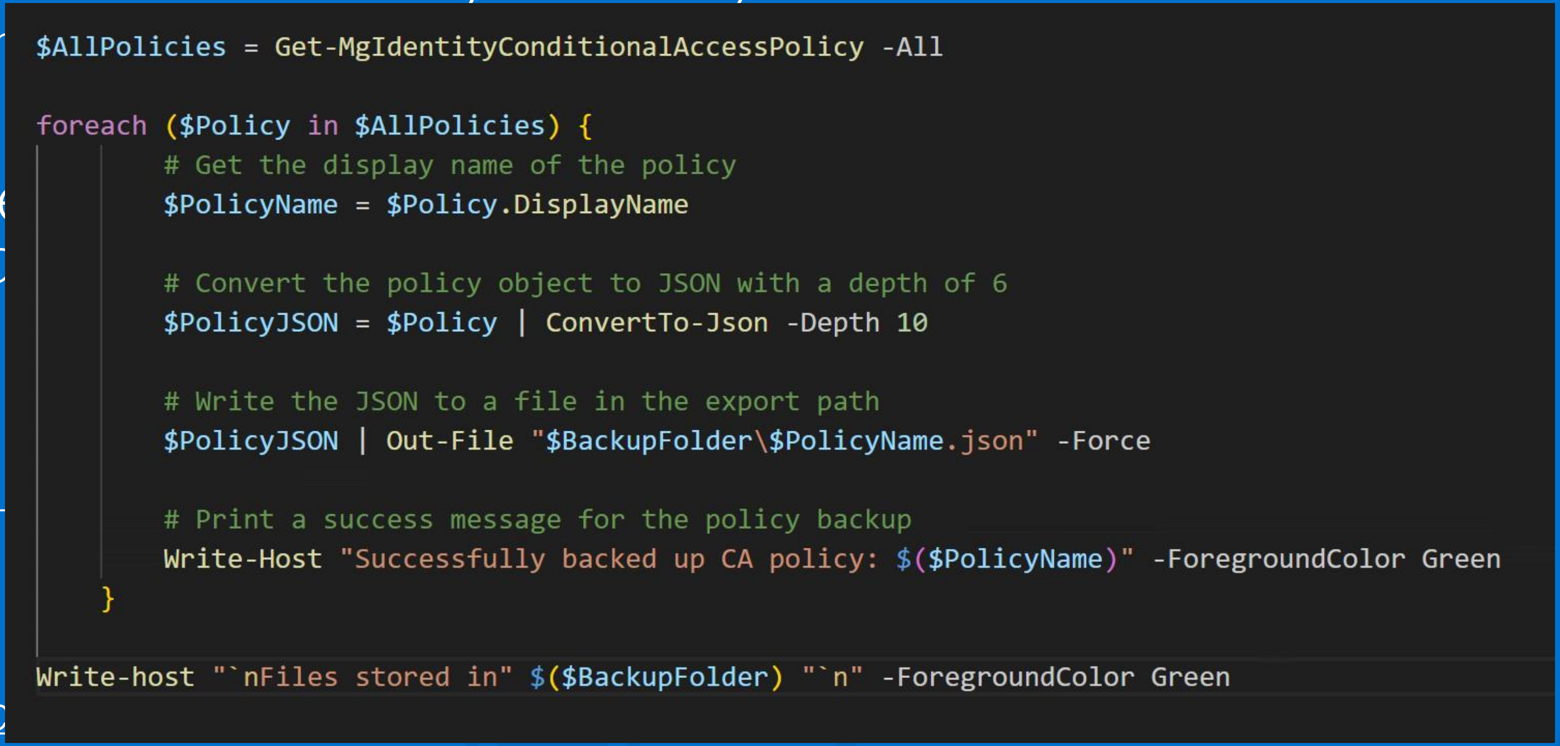
→ EntraExporter is your better friend 🤓
Download here: Open-Source Github

→ M365DSC is another great friend 🤓
Download here: Open-Source Github

Related Microsoft announcement from this week:
Configuration management APIs in Microsoft Graph – Link is in the appendix

How to create a smart and easy backup?

- → Manually difficult (Entra Admin Center, CSV etc.)
  Code-based approaches are r
- → PowerShell is your frie
  Some manual tweaking... JSO
- → EntraExporter is your
  Download here: Open-Source
- → M365DSC is another
  Download here: Open-Sourc



```
$AllPolicies = Get-MgIdentityConditionalAccessPolicy -All

foreach ($Policy in $AllPolicies) {
        # Get the display name of the policy
        $PolicyName = $Policy.DisplayName

        # Convert the policy object to JSON with a depth of 6
        $PolicyJSON = $Policy | ConvertTo-Json -Depth 10

        # Write the JSON to a file in the export path
        $PolicyJSON | Out-File "$BackupFolder\$PolicyName.json" -Force

        # Print a success message for the policy backup
        Write-Host "Successfully backed up CA policy: $($PolicyName)" -ForegroundColor Green
    }
Write-host "`nFiles stored in" $($BackupFolder) "`n" -ForegroundColor Green
```

Related Microsoft announcement from this week:
Configuration management APIs in Microsoft Graph – Link is in the appendix

How to create a smart and easy backup?

→ Manually difficult (Entra Admir

Code-based approaches are much better

→ PowerShell is your friend

Some manual tweaking… JSON must be p

→ EntraExporter is your better fri

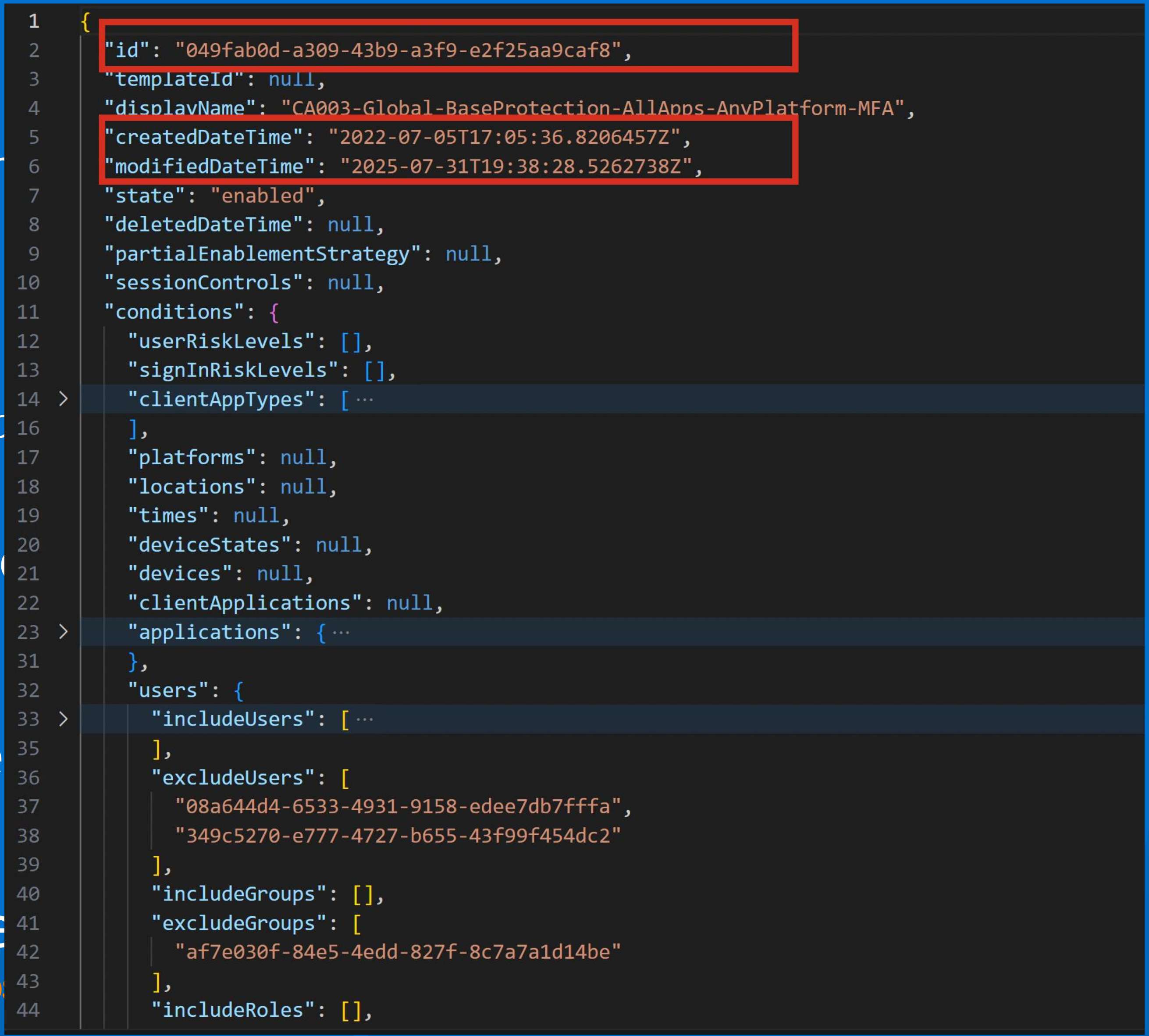
Download here: Open-Source Github

→ M365DSC is another great frie

Download here: Open-Source Github

Related Microsoft announceme

Configuration management APIs in Micro



```
{
  "id": "049fab0d-a309-43b9-a3f9-e2f25aa9caf8",
  "templateId": null,
  "displayName": "CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA",
  "createdDateTime": "2022-07-05T17:05:36.8206457Z",
  "modifiedDateTime": "2025-07-31T19:38:28.5262738Z",
  "state": "enabled",
  "deletedDateTime": null,
  "partialEnablementStrategy": null,
  "sessionControls": null,
  "conditions": {
    "userRiskLevels": [],
    "signInRiskLevels": [],
    "clientAppTypes": [ ···
    ],
    "platforms": null,
    "locations": null,
    "times": null,
    "deviceStates": null,
    "devices": null,
    "clientApplications": null,
    "applications": { ···
    },
    "users": {
      "includeUsers": [ ···
      ],
      "excludeUsers": [
        "08a644d4-6533-4931-9158-edee7db7fffa",
        "349c5270-e777-4727-b655-43f99f454dc2"
      ],
      "includeGroups": [],
      "excludeGroups": [
        "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
      ],
      "includeRoles": [],
```

Demo:

Export with
Entra Exporter v3.01 and
Conditional Access Policy Recovery

Demo:

Export with
Entra Exporter v3.01 and
Conditional Access Policy Recovery

Hard deleted? And now what?

- → Object must be recreated
- → Previous JSON export required (EntraExporter)
- → Object will become a new ID
- → Microsoft can not help
- → Example article on rebuilding a hard-deleted Administrative Unit on my blog

  https://nothingbutcloud.net/2025-08-30-DeletedEntraObjects/

To make sure it never comes down to a restore …

- ✓ Protect sensitive Groups with „PIM Protected Groups“
  ➜ possible, but should you?
- ✓ AU – Restricted Management (GA since June 2025) Demo …
- ✓ Protected Actions for hard deletions (GA since January 2025) Demo …
- ✓ Smart Alerting for important Resources
  Example implementation on my blog

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)

Best Practices & Community

Jorge de Almeida Pinto on HIPConf: Best Practices for Resync AD and Entra ID

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

HEADLINE

robopack

empowered by SOFTWARE CENTRAL

GOLD

XOPERO Backup&Recovery

Master Packager

Visit Tallinn

NetApp

PATCH MY PC

SILVER

ARROW

PROEKSPERT

ONLINE

QUBIX

ChangePilot by Empowering.Cloud

DYNAMICS MINDS powered by DOCENTRIC

ColorCloud HAMBURG

Klaus Bierschenk

Director Consulting Expert @ CGI Germany

- Based in Murnau am Staffelsee in Germany
- With my Family, two cats, two snakes
- Mountain lover, Ultra Runner

✉ Klaus@nothingbutcloud.net

https://nothingbutcloud.net

@klabier.bsky.social

www.linkedin.com/in/klabier

Thank you!

Please rate this session!

Questions?