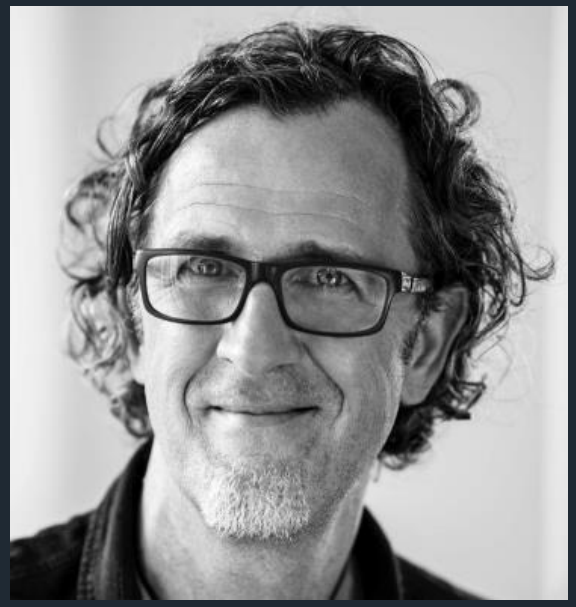
Delete Is Easy – Recovery Is Not

The Reality of Entra ID Backup & Restore

Speaker: Klaus Bierschenk

TROOPERS
JUNE 22ND TO JUNE 26th

Delete Is Easy – Recovery Is Not: The Reality of Entra ID Backup & Restore



Klaus Bierschenk
Director Consulting Expert @ CGI Germany

Based in Murnau am Staffelsee, Bavaria

Living with my family, two snakes, two cats – and lots of other animals my cats bring home from time to time

@klabier.bsky.social

http://www.linkedin.com/in/klabier

Klaus@NothingButCloud.net

https://nothingbutcloud.net/

Microsoft® MVP Most Valuable Professional

Azure Infra & Entra ID SÜDDEUTSCHLAND

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?

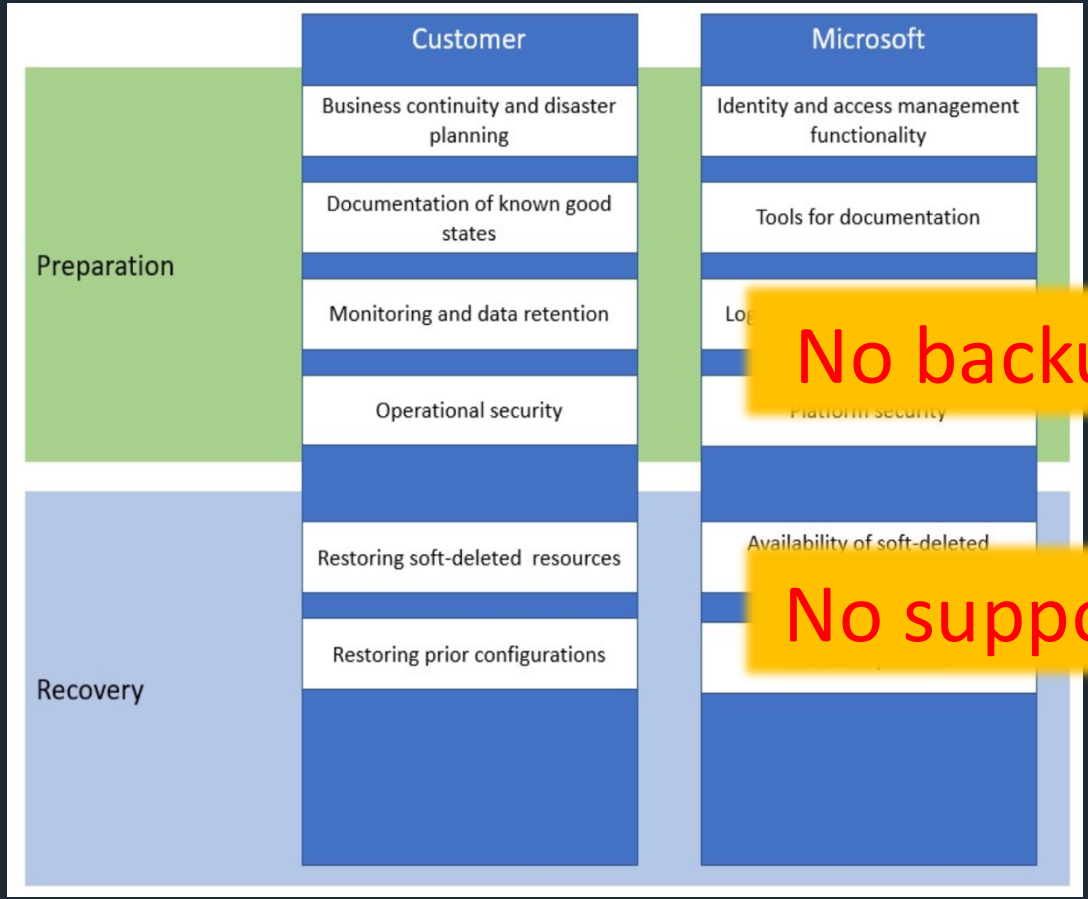
No commercials

Security: How can we prevent object or configuration loss in Entra ID?

Microsoft’s standpoint on backup and restore in Entra ID

Microsoft provides platform & APIs

Customer responsible for planning & restoring



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

TROOPERS

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)
Network access policies
Condition for network connections
Configur segments
Access
Traffic
Assign
Zero Trust Netw
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 Clou Synchronization Settings
Entra Cloud S
Attribute ma
Custom expr
Synchroniza
Hybrid synchronizatio ord
Hash Sync)
SCIM synchronization with third-party providers
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-based policies
Session policies & token lifetimes
Adaptive access policies
Conditional Access for
Anomaly dete
Cross-tenant
Security levels
Terms of use p

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
Compliance re
Auto
Entitle
Access

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)

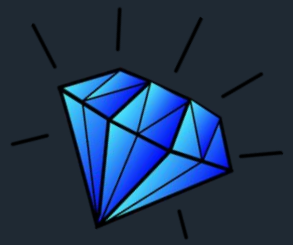
Application Management & Access Controls
Add/remove enterprise applications
Enable Single Sign-On (SSO) for applications
Configure App Proxy for legacy applications
Define OAuth and OpenID Connect policies
Configure third-party identity providers
Manage token lifetimes for applications
Define Conditional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

Administrative Units (AUs)
Administrative Unit objects
Assign users & groups to A
Role-based access
Delegated
Policies for A

Administrative Units (AUs)

Tenant Se izational Policies
Manage tenant 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

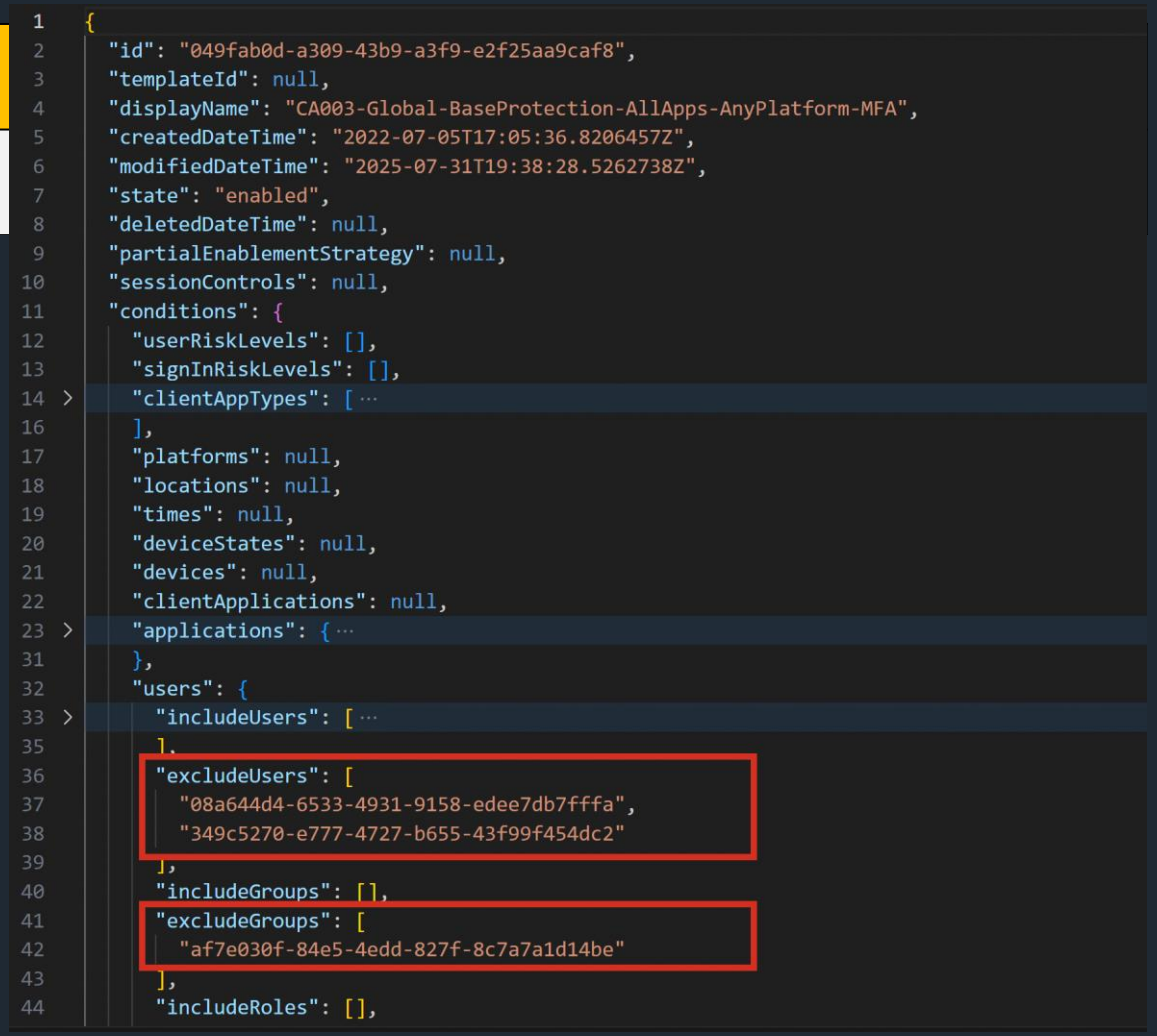


(just the big picture – not for detailed reading)

TROOPERS

Entra object restore – reality check

Object typ	Soft delete	Restore?
User object	✓	30d Recycle Bin ->



```
{
  "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": [],
```

Restore via Recycle Bin, no Restore at all, Restore via API Microsoft Learn Article

TROOPERS

Entra object restore – reality check

Object typ	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 Microsoft Learn Article

TROOPERS

Demo:

Restore Administrative Unit via Microsoft Graph API

CLASS_8a_Objects | Users

Main Identity LAB

Search

Manage

- Properties
- Users
- Groups
- Devices
- Roles and administrators
- Dynamic membership rules

Activity

- Bulk operation results

Membership rules | Add member | Download users | Bulk operations | Refresh | Manage view

Azure Active Directory is now Microsoft Entra ID.

Search users | Add filter

5 users found

Display name	User principal name	User type	Last interactive sign-in time	Identities
S8 Student1 8a	Student1_8a@kbr...	Member		kbcorp2021.onmicrosoft.c
S8 Student2 8a	Student2_8a@kbr...	Member		kbcorp2021.onmicrosoft.c
S8 Student3 8a	Student3_8a@kbr...	Member		kbcorp2021.onmicrosoft.c
S8 Student4 8a	Student4_8a@kbr...	Member		kbcorp2021.onmicrosoft.c
S8 Student5 8a Protected	Student5_8a_Prot...	Member		kbcorp2021.onmicrosoft.c

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

TROOPERS

How to create a smart and easy backup?

- Manually difficult (Entra Admin Center, CSV etc.)
  Code-based approaches are mu
- PowerShell is your frier
  Some manual tweaking… JSON
- EntraExporter 3.01 is y
  Download here: Open-Source C

```powershell
$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
```

TROOPERS

How to create a smart and easy backup?

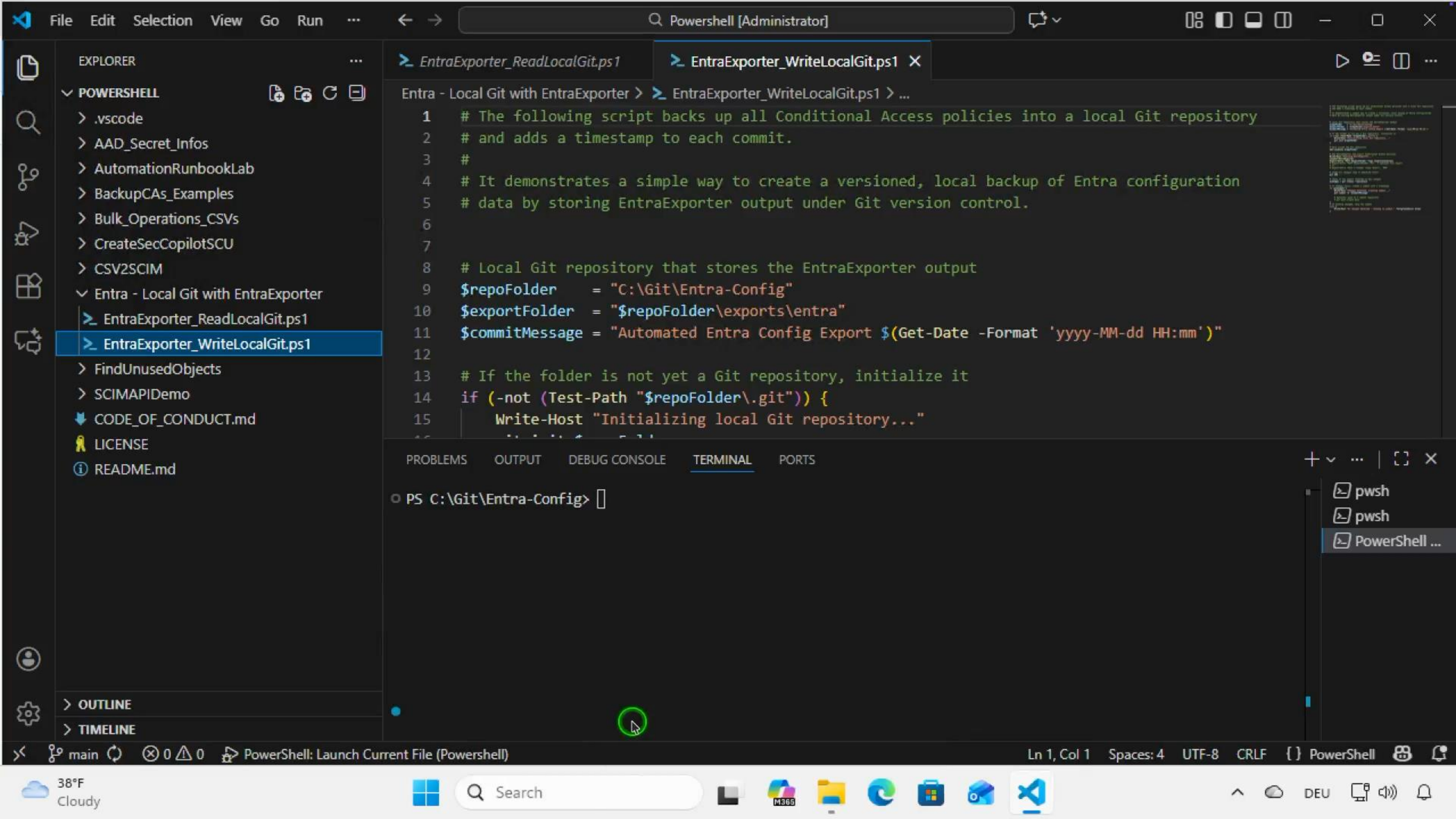
- → Manually difficult (Entra Admin C
  Code-based approaches are mu
- → PowerShell is your frier
  Some manual tweaking… JSON
- → EntraExporter 3.01 is y
  Download here: Open-Source C

```
$AllPolicies =

foreach ($Poli
        # Get
        $Polic

        # Conv
        $Polic

        # Writ
        $Polic

        # Prir
        Write-
    }

Write-host "`r
```


```
{
  "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 …

TROOPERS


File Edit Selection View Go Run
Powershell [Administrator]
EXPLORER
POWERSHELL
.vscode
AAD_Secret_Infos
AutomationRunbookLab
BackupCAs_Examples
Bulk_Operations_CSVs
CreateSecCopilotSCU
CSV2SCIM
Entra - Local Git with EntraExporter
EntraExporter_ReadLocalGit.ps1
EntraExporter_WriteLocalGit.ps1
FindUnusedObjects
SCIMAPIDemo
CODE_OF_CONDUCT.md
LICENSE
README.md
EntraExporter_ReadLocalGit.ps1
EntraExporter_WriteLocalGit.ps1
Entra - Local Git with EntraExporter > EntraExporter_WriteLocalGit.ps1 > ...
1 # The following script backs up all Conditional Access policies into a local Git repository
2 # and adds a timestamp to each commit.
3 #
4 # It demonstrates a simple way to create a versioned, local backup of Entra configuration
5 # data by storing EntraExporter output under Git version control.
6
7
8 # Local Git repository that stores the EntraExporter output
9 $repoFolder = "C:\Git\Entra-Config"
10 $exportFolder = "$repoFolder\exports\entra"
11 $commitMessage = "Automated Entra Config Export $(Get-Date -Format 'yyyy-MM-dd HH:mm')"
12
13 # If the folder is not yet a Git repository, initialize it
14 if (-not (Test-Path "$repoFolder\.git")) {
15 Write-Host "Initializing local Git repository..."
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS C:\Git\Entra-Config>
pwsh
pwsh
PowerShell ...
OUTLINE
TIMELINE
main
0 0
PowerShell: Launch Current File (Powershell)
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF { } PowerShell
38°F
Cloudy
Search
DEU

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 …

- ➜ Once upon a time there was M365DSC as another great friend 🤓
  But now we have Tenant Configuration Management (GA since May `26) – API Only

Demo …

- ➜ Check out Backup and Recovery (Preview since Mar `26 and P1/P2 required)
  Easy built-in functionality (keep in mind: one backup per day and five days history max.!)

TROOPERS

Demo:

→ *Conditional Access Policy Recovery*

Recycle-Bin or JSON-Import?

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

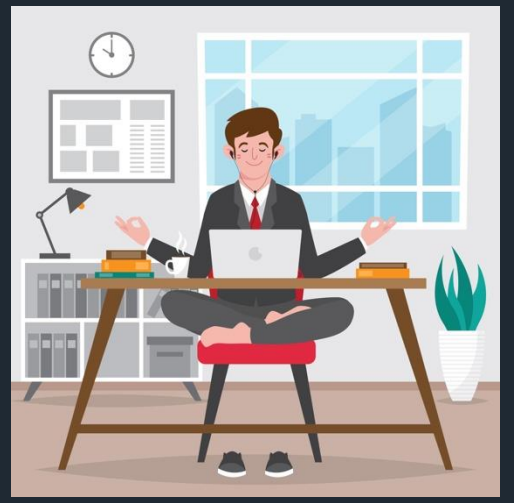
Demo …

- ✓ Protected Actions for hard deletions

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)**

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

TROOPERS

Thank You

TROOPERS