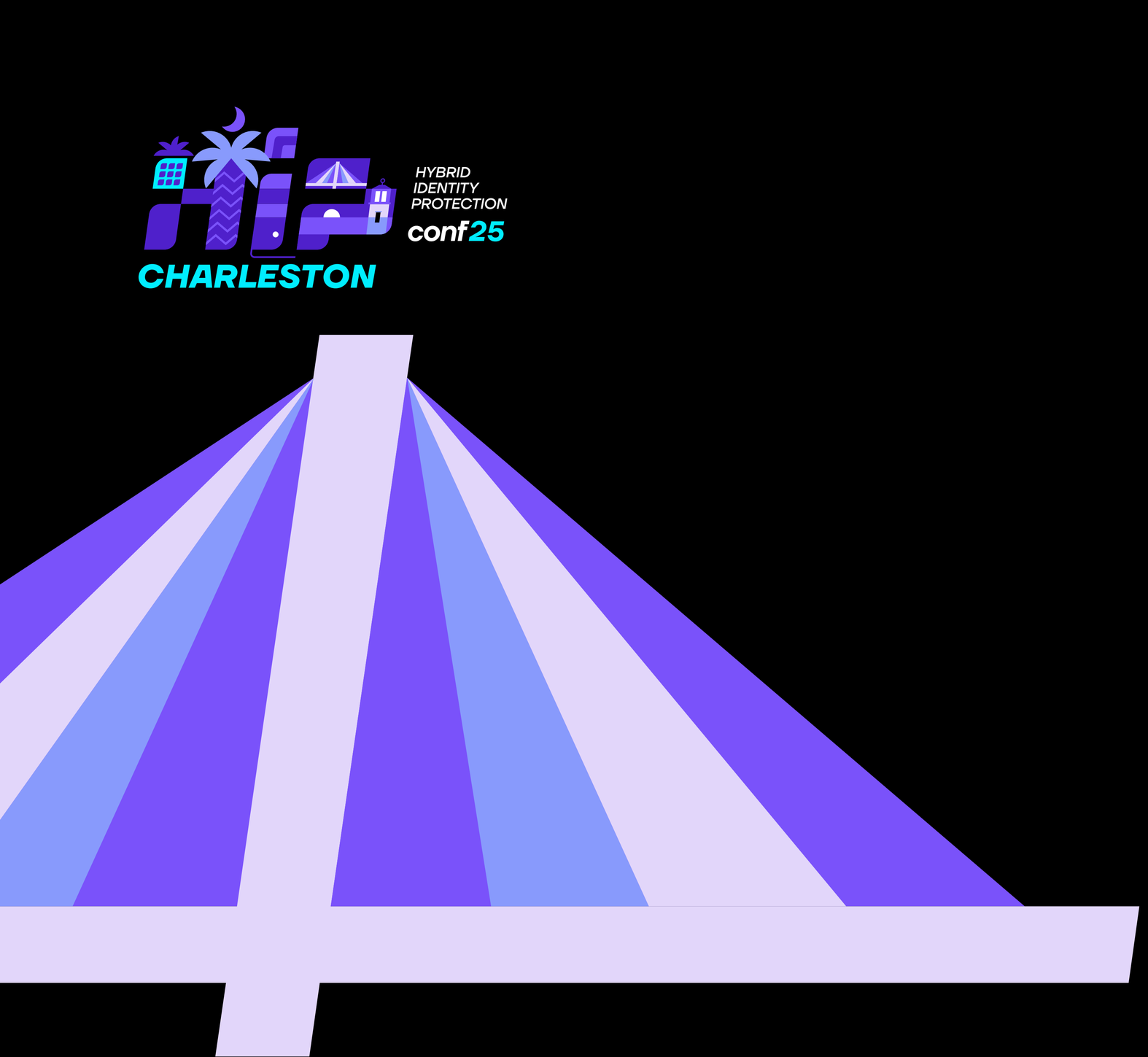
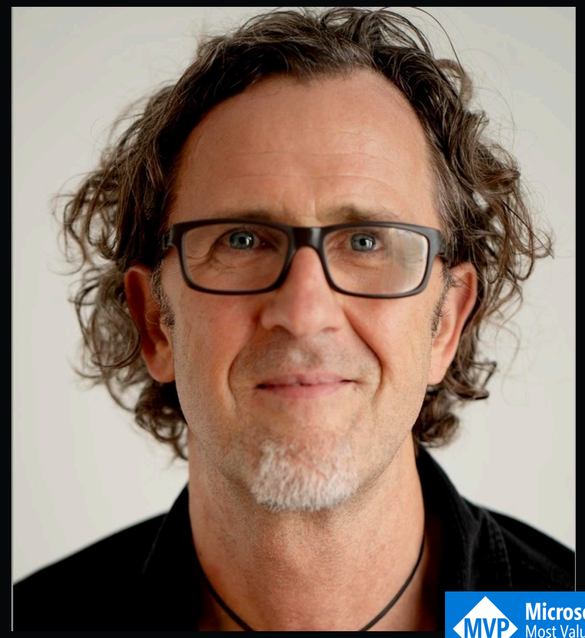


Think You Have Entra Backup? Think Again!

Klaus Bierschenk
Director Consulting Expert,
CGI Germany

HYBRID IDENTITY PROTECTION conf25
CHARLESTON



Microsoft Most Valuable Professional

Meet the Speaker

Klaus Bierschenk

Director Consulting Expert / CGI Germany

- Based in Murnau in Bavaria
- With my Family, two cats and two snakes
- Mountain lover, Ultrarunner

linkedin.com/in/klabier/

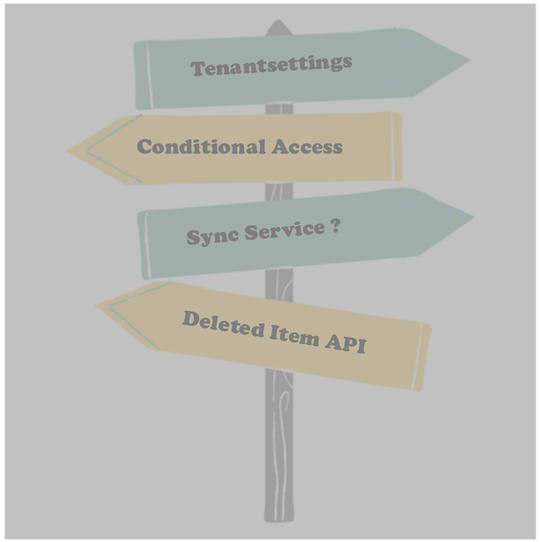
Klaus@nothingbutcloud.net

https://nothingbutcloud.net

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Trust is good, backup is better…
… so what's our topic today?

- ➜ What is Microsoft's standpoint 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 ?

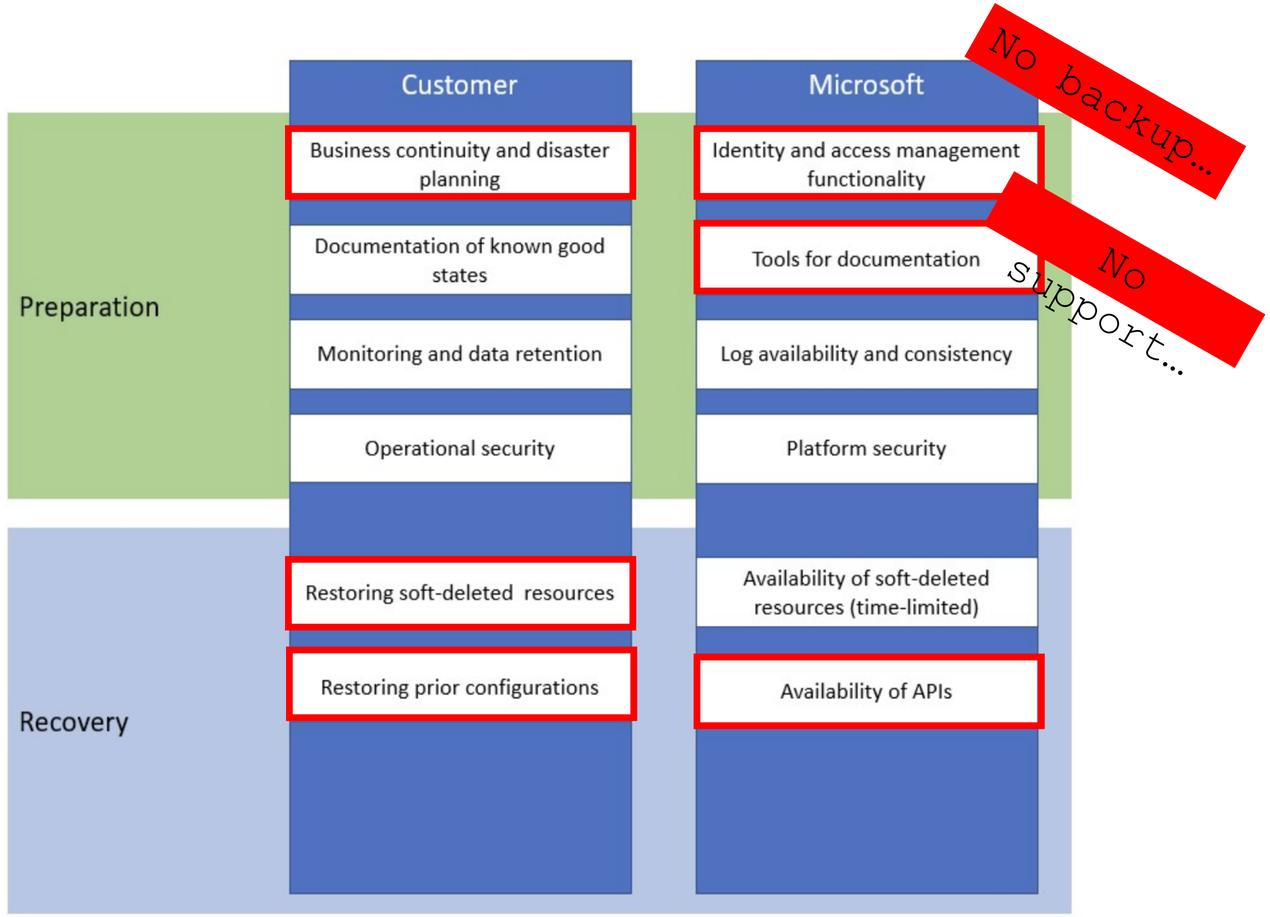


HYBRID IDENTITY PROTECTION conf25 CHARLESTON

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

Microsoft provides platform & APIs

Customer responsible for planning & restoring



Source: Microsoft Learn

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Prioritize your crown jewels

- ➜ *Knowing **„What is really important?“*** otherwise a recovery concept becomes difficult

- ➜ Sometimes proper documentation is enough, sometimes a backup procedure is the better choice
  (… with a tenant of >50 CA policies, documentation alone is not helpful)

- ➜ Every company is different, every Entra ID tenant is different – not everything is always equally critical
  (… when a tenant has Security Defaults enabled, backing up CAs is not the major topic)

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

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
Access for network connections
network segments
apps
Zero Trust Network
Web content filtering
DNS security policies
Logging & monitoring for network access

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

Sync & Synchronization Settings
Hybrid synchronization
Hash Sync)
SCIM synchronization with third-party providers
On-premises directory synchronization (Azure AD Connect)
Custom synchronization rules

Conditional Access & Acces
Policies for users & gro
Device state &
Sessio
apps & services
risk-based rules
access
Security levels for external identities
Terms of use pages

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

Ide Governance & Compliance
Regu
Auto ive accounts
Cor ment
Automa
Entitlement mana
Access control workflows

Device Management & Microsoft Entra Cloud
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)

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

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

Global Secure Access (GSA)

Entra Cloud Sync & settings

Conditional Access & Access Control

Identity-Governance & Compliance

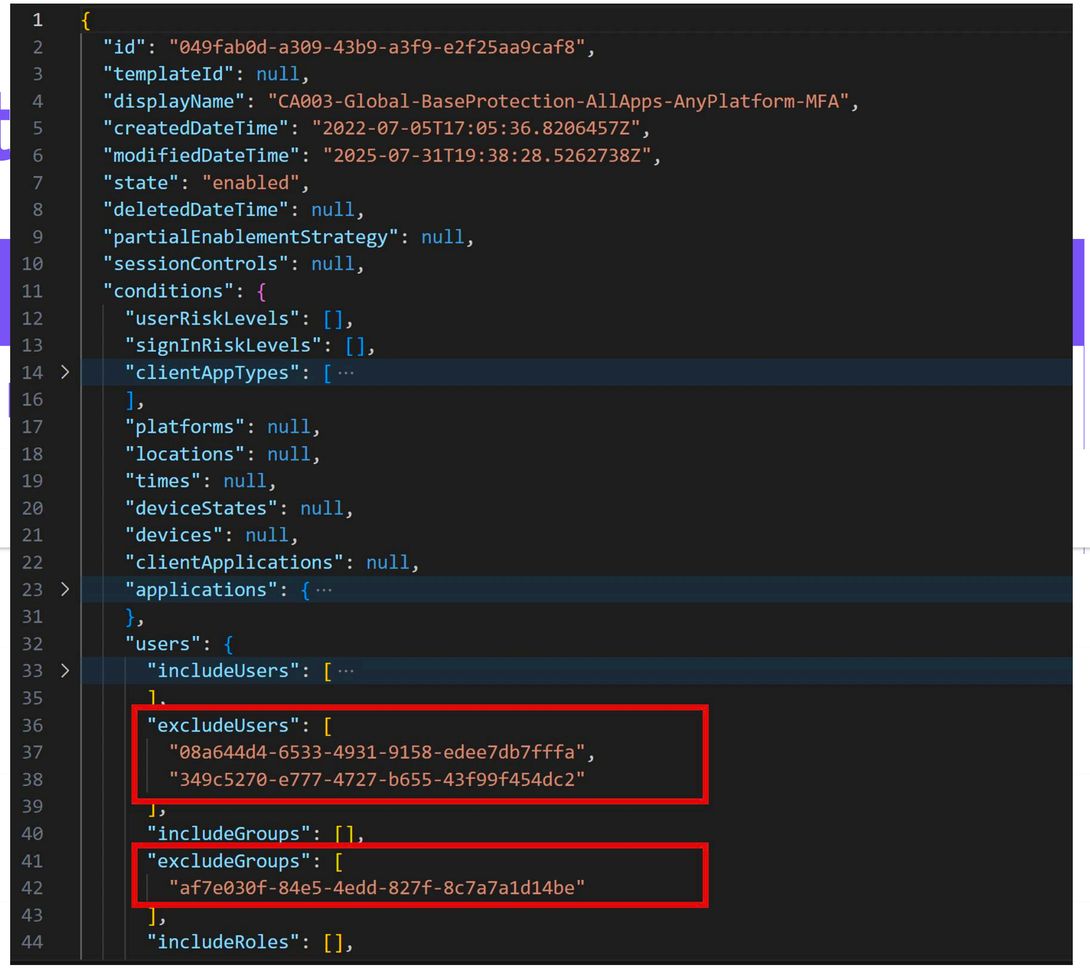
Administrative Units (AUs)

Just the big picture – not for detailed reading

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Entra object

Objekttyp	Soft delete	Restore?
User object	✓	🗑️ 30d Recycle



```
{
  "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

Additional read: Microsoft Learn

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Entra object restore – reality check

Objekttyp	Soft delete	Restore?
User object	✓	🗑 30d Recycle Bin -> Hard deleted
Security group	✗	🚫 No restore ⚠
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	✓	🔄 Deleted Item API (30d) -> JSON export / import

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

Additional read: Microsoft Learn

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Recover via deletedItems API

GET | beta | https://graph.microsoft.com/beta/identity/conditionalAccess/deletedItems/policies | Run query

Request Body | Request Headers | Modify Permissions | Access token

OK - 200 - 242 ms

Response preview | Response headers | Code snippets | Toolkit component | Adaptive cards


```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#identity/conditionalAccess/deletedItems/policies",
    "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For
    example: GET identity/conditionalAccess/deletedItems/policies?$select=conditions,createdDateTime",
    "value": [
        {
            "id": "7bedcea6-9403-450a-8cdb-7e73ee937552",
            "templateId": null,
            "displayName": "CA116-TESTAdmins-ProtectedAction-DeleteCAPolicies-Grant-OnlyGA",
            "createdDateTime": "2025-04-05T11:06:56.8869666Z",
            "modifiedDateTime": "2025-07-31T20:05:11.4691406Z",
            "state": "disabled",
            "deletedDateTime": "2025-09-16T15:18:04Z",
```


Supported resources:

- → Administrative unit
- → Application
- → M365 Group
- → ServicePrincipal
- → User
- → CA Policy **NEW**

https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.serviceprincipal
https://graph.microsoft.com/v1.0/directory/deletedItems/microsoft.graph.administrativeUnit
https://graph.microsoft.com/beta/identity/conditionalAccess/deletedItems/policies

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Recover via deletedItems API

POST v1.0 https://graph.microsoft.com/v1.0/directory/deletedItems/49807c30-fa32-4f17-92ed-d95666262d83/restore Run query

No resource was found matching this query

Request body | Request headers | Modify permissions | Access token

Permissions

One of the following permissions is required to run the query. If possible, consent to the least privileged permission.

OK - 200 - 799 ms

Response preview | Response headers | Code snippets | Toolkit component | Adaptive cards | Expand


```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#directoryObjects/$entity",
    "@odata.type": "#microsoft.graph.servicePrincipal",
    "id": "49807c30-fa32-4f17-92ed-d95666262d83",
    "deletedDateTime": null,
    "accountEnabled": true,
    "alternativeNames": [],
    "appDisplayName": "Microsoft Graph Command Line Tools",
```


Permissions and additional reading at Microsoft Learn

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

How to create a smart and easy Backup?

→ Manually

Code-base

→ PowerSh

Some mani

```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
```

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

How to create a smart and easy Backup?

→ Manually difficult

Code-based approaches are much better

→ PowerShell is your friend

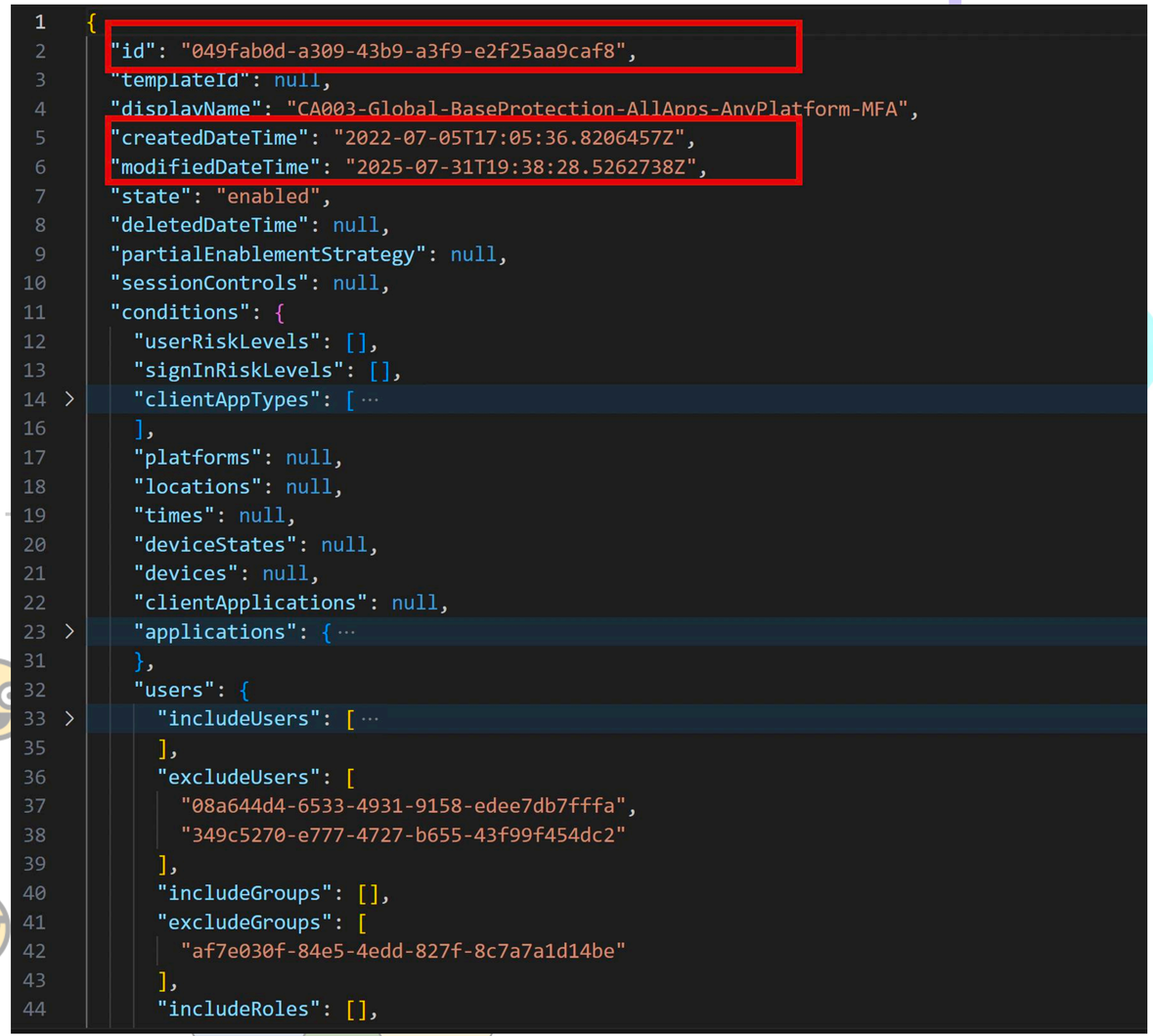
Some manual tweaking… JSON must be precise

→ EntraExporter is your better friend

Download here: Open-Source Github

→ M365DSC is another great friend

Download here: Open-Source Github

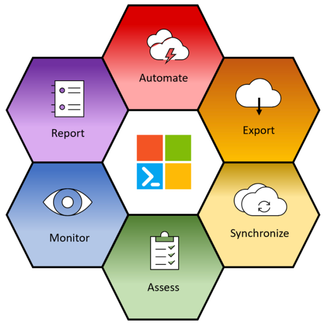


How to create a smart and easy Backup?

- → Manually difficult
  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

Demo …

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



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Hard deleted? And now what?

- ✓ Object must be recreated
- ✓ Previews 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 -> Read Article

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

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 (samples at the end of the slide deck)

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Summary: back to the „Agenda-Questions

- ✓ Microsoft’s standpoint is clear
- ✓ It is up to the Tenant Admin 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

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

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.

MS Learn: Restore CA Policy Public Preview (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

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?

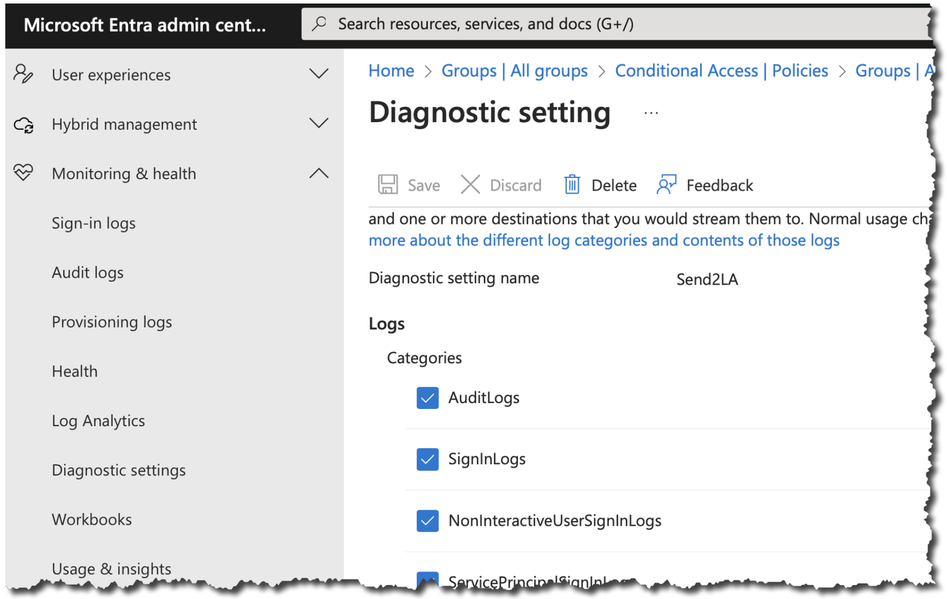
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Backup slides!

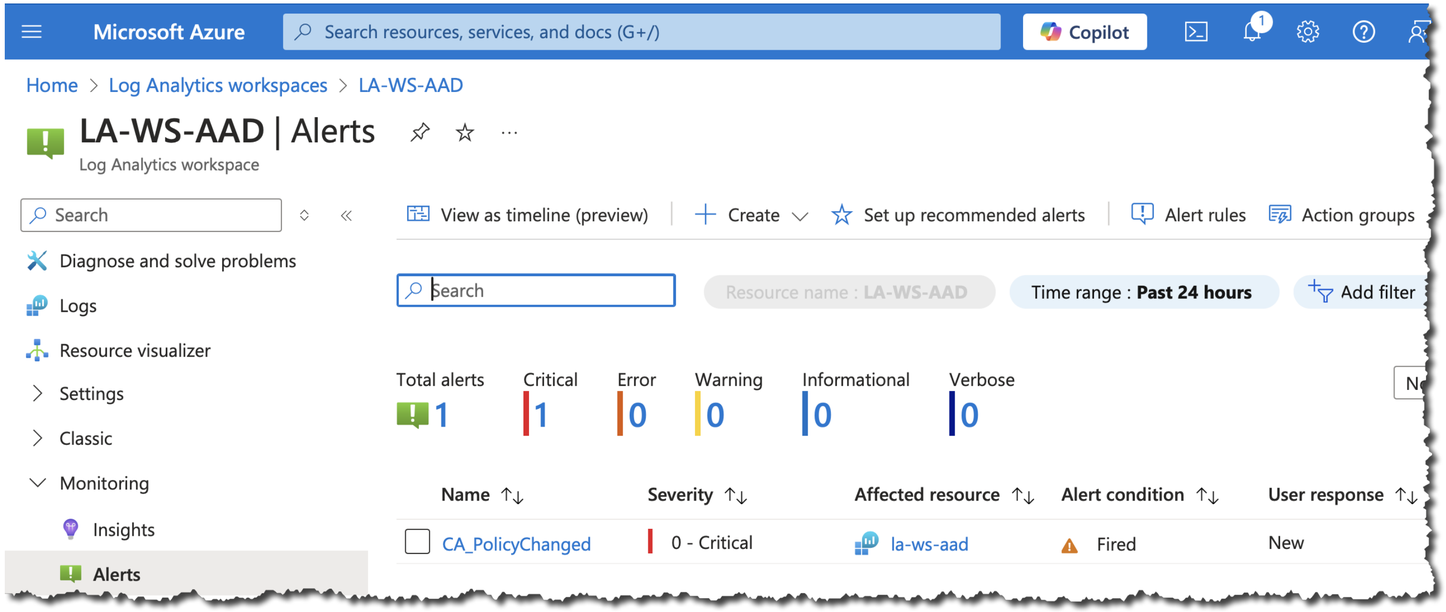
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

The simple way to alerting (1/2)

Configure diagnostic settings in Entra ID



Configure response in Azure Portal

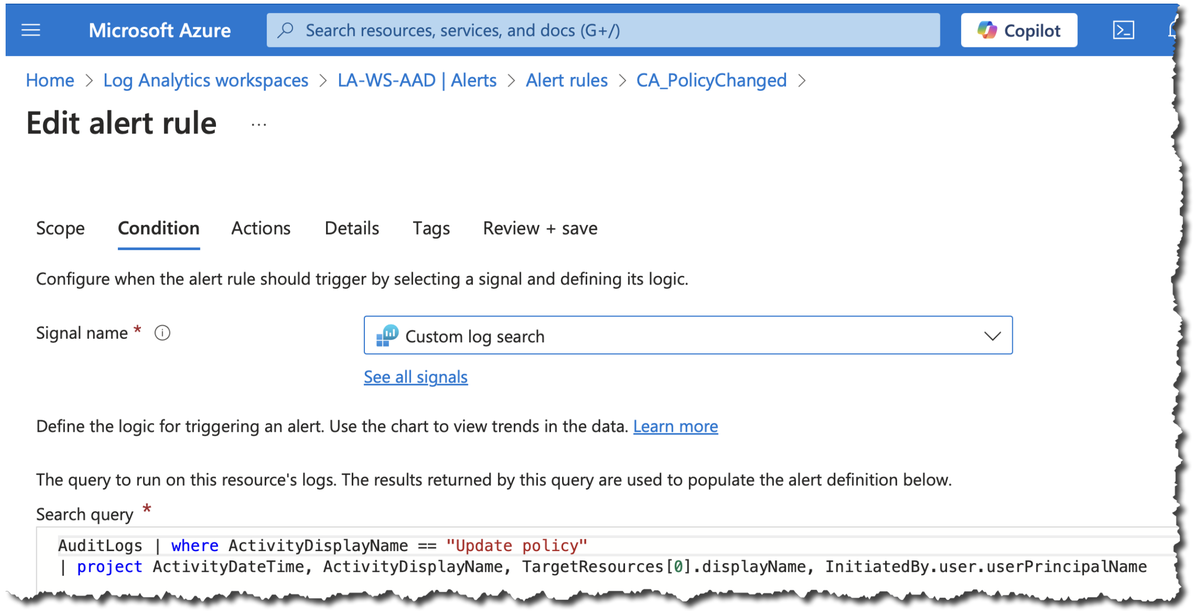


Logs will be sent to Repository

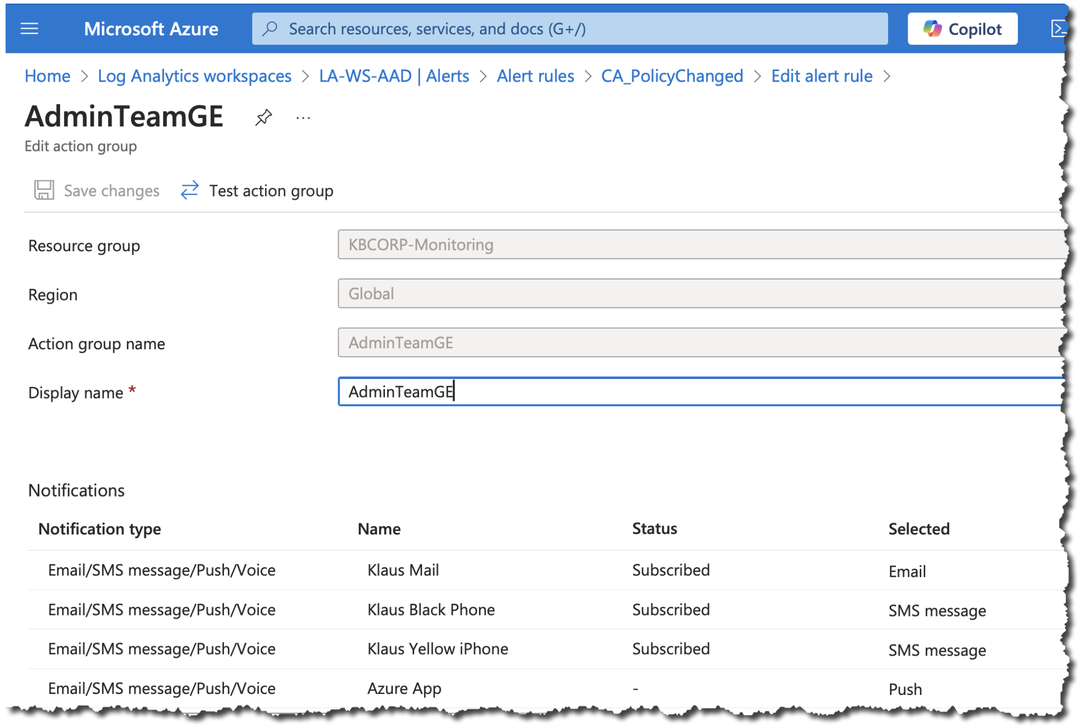
Then set up „Alert Rule“ and „Action Group“ →

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

The simple way to alerting (2/2)



Set up Alert Rule



… then set up Action Group