



# Conditional Access in Zeiten von Global Secure Access

Christopher Brumm



# Christopher Brumm

Cloud Security Architect @glueckkanja

## Focus

Identity + Security  
in Microsoft Cloud

## From

Hamburg, Germany

## My Blog

[chris-brumm.com](http://chris-brumm.com)



## Certs and Titles

CISSP, MVP Identity & Access,  
various MS certs

## Hobbies

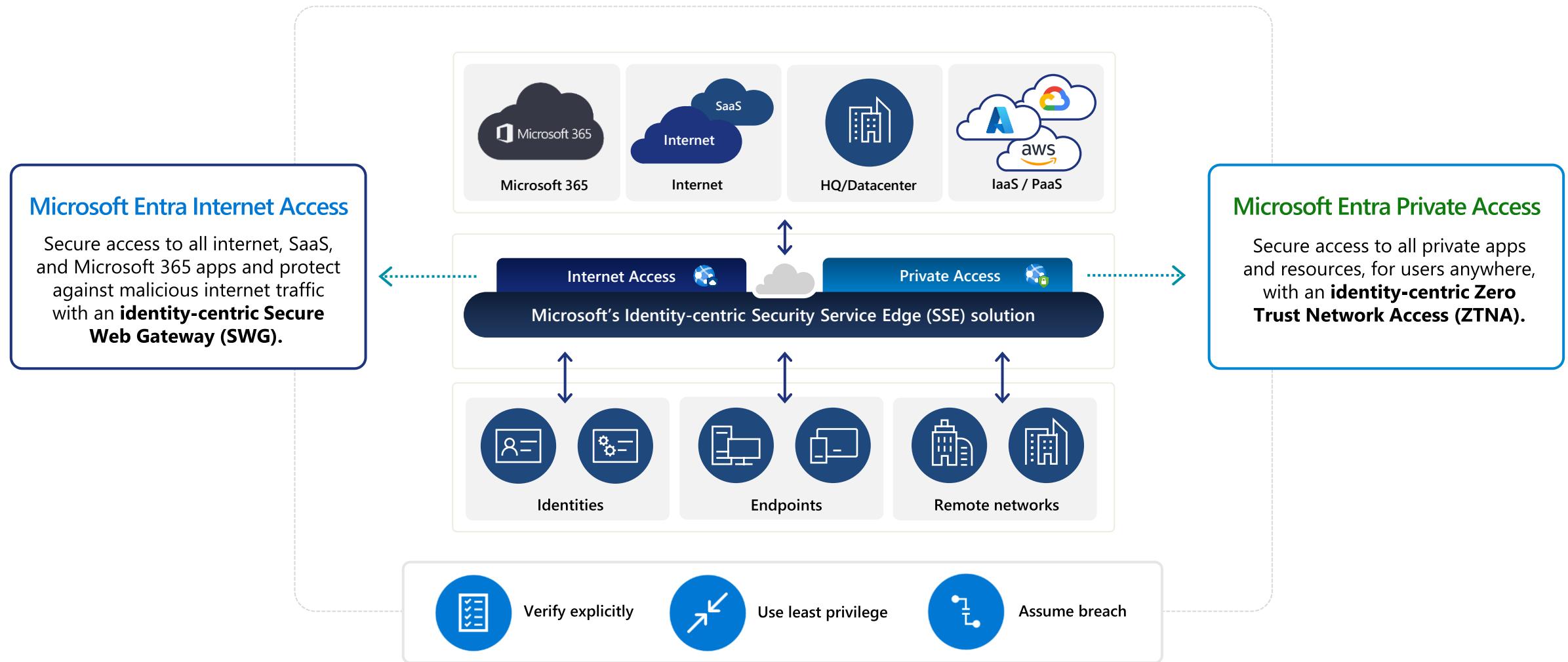
Family, Traveling, Pen & Paper  
RPG

## Contact

[/christopherbrumm](#)



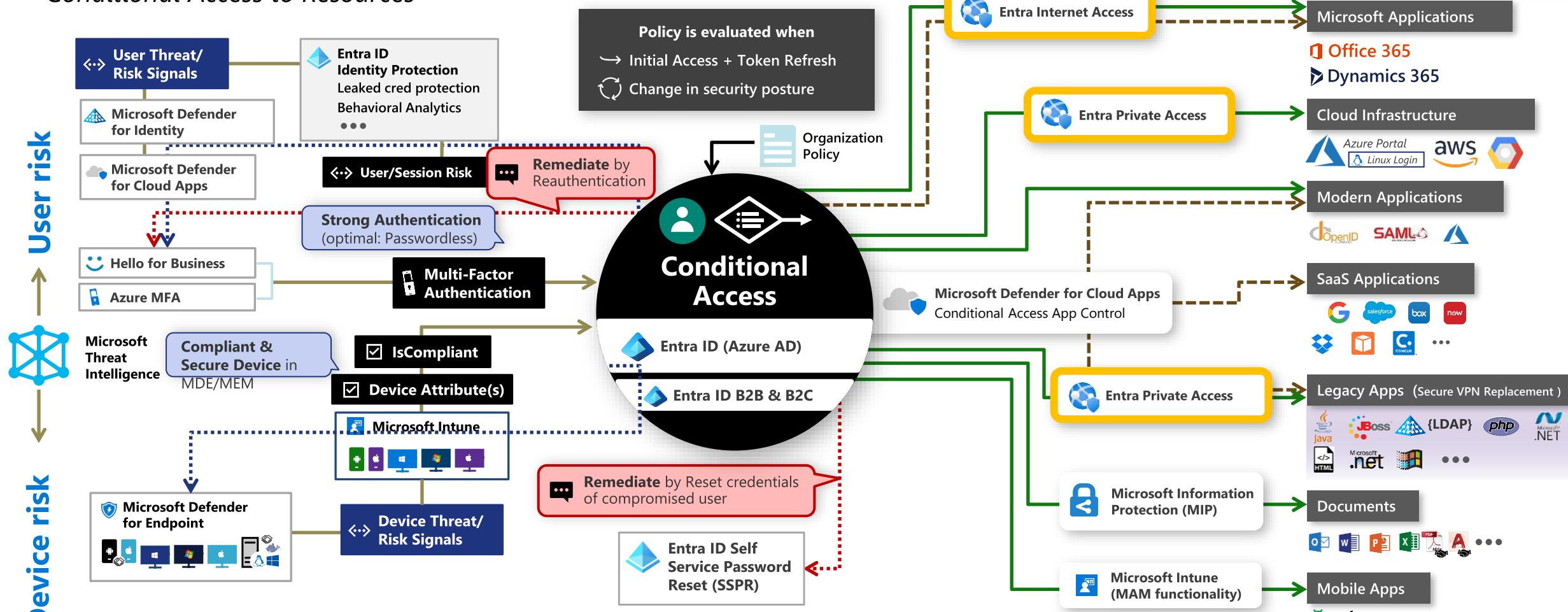
# Microsoft's Identity-centric SSE solution





# Zero Trust Policy Engine

## Conditional Access to Resources



## Legend

- |                 |                  |
|-----------------|------------------|
| Full access     | Limited access   |
| Risk Mitigation | Remediation Path |



### Signal

to make an informed decision



### Decision

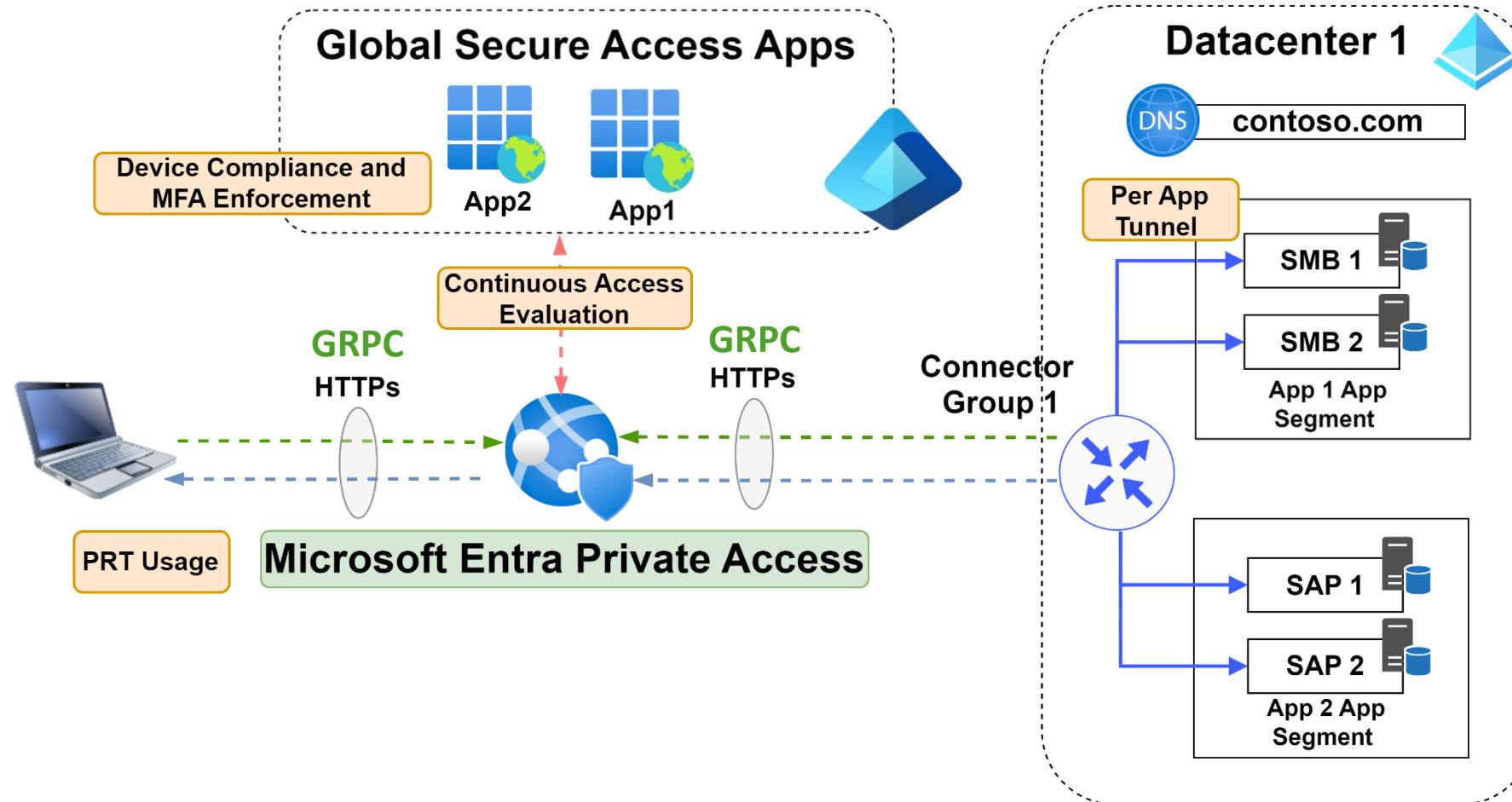
based on organizational policy



Enforcement  
of policy across resources



# Entra Private Access



# Entra Private Access App – Portal View

The diagram illustrates the integration of Conditional Access policies with user/group assignments and network access configurations.

**Conditional Access Policy:** EPA 1 - Require YubiKey for Admin Access

- Target resources:** Network (1 resource included)
- Conditions:** 0 conditions selected
- Access controls:** Grant (1 control selected)
- Session:** Sign-in frequency - Every time

**User Assignment:** Assign users and groups to app-roles for your application here. To create new app-roles for this application, click Add user/group.

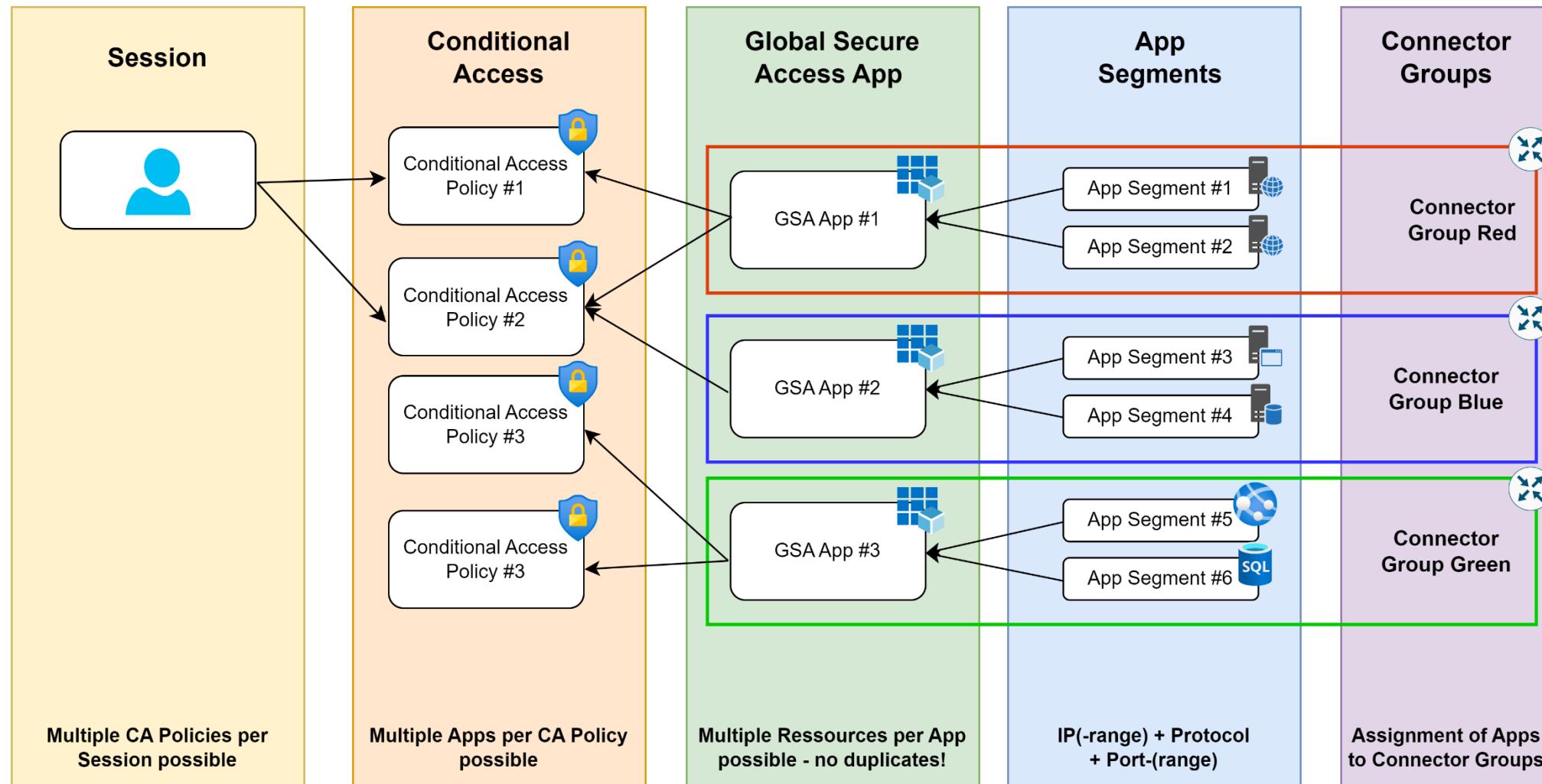
Display Name	Object Type
Bert	User
Big Bird	User

**Network Access Properties:** Private Access - GKFelucia File Service | Network access properties

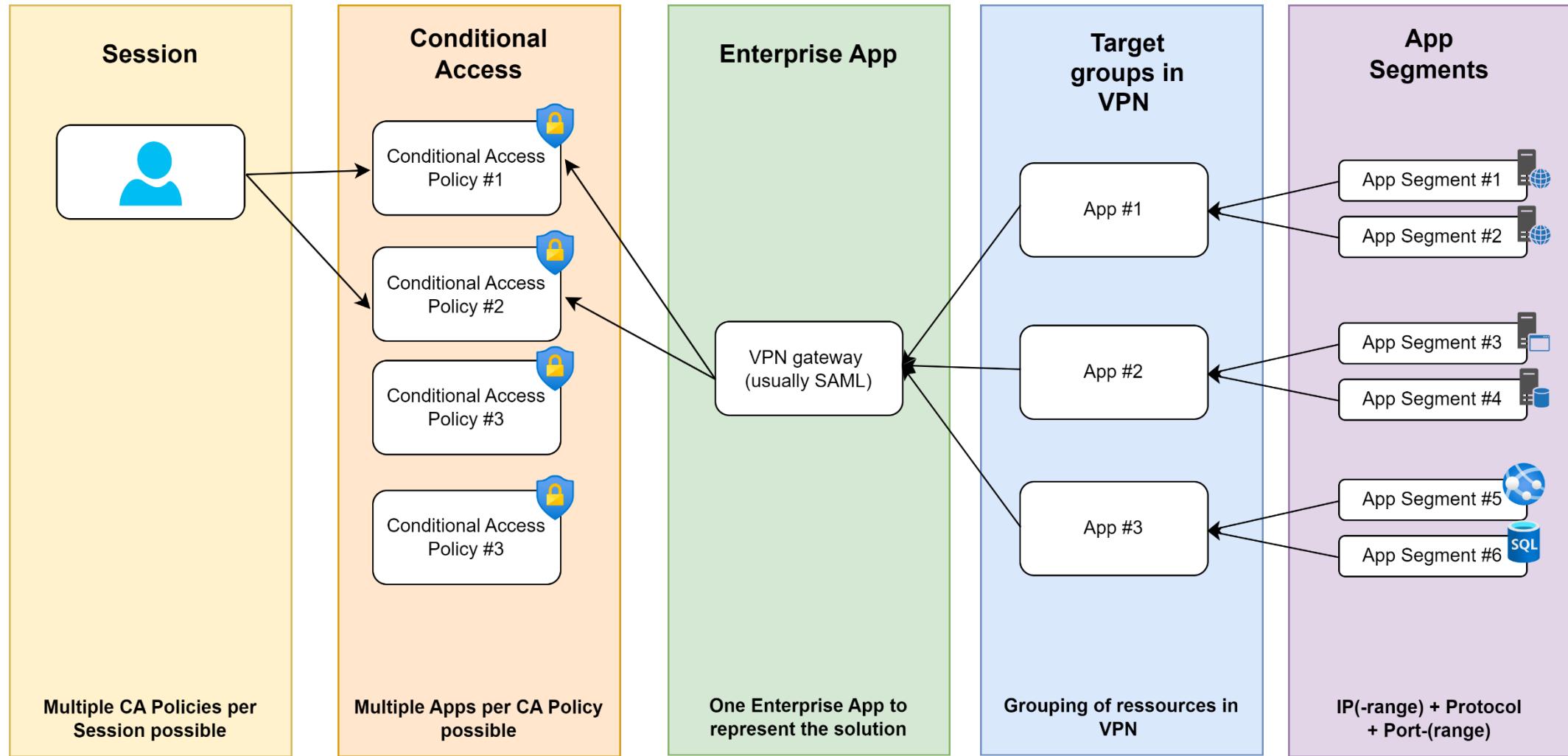
- Connector Group:** ZTNA
- Custom Security Attributes:** We recommend at least two active connectors in selected group 'ZTNA'. Click here to download a connector or manage your connector groups.
- Enable access with Global Secure Access client:** Checked
- Application Segment:** Add application segment
- Destinations:** IP address 192.168.0.21, Port 445, Protocol TCP, UDP, Status Success



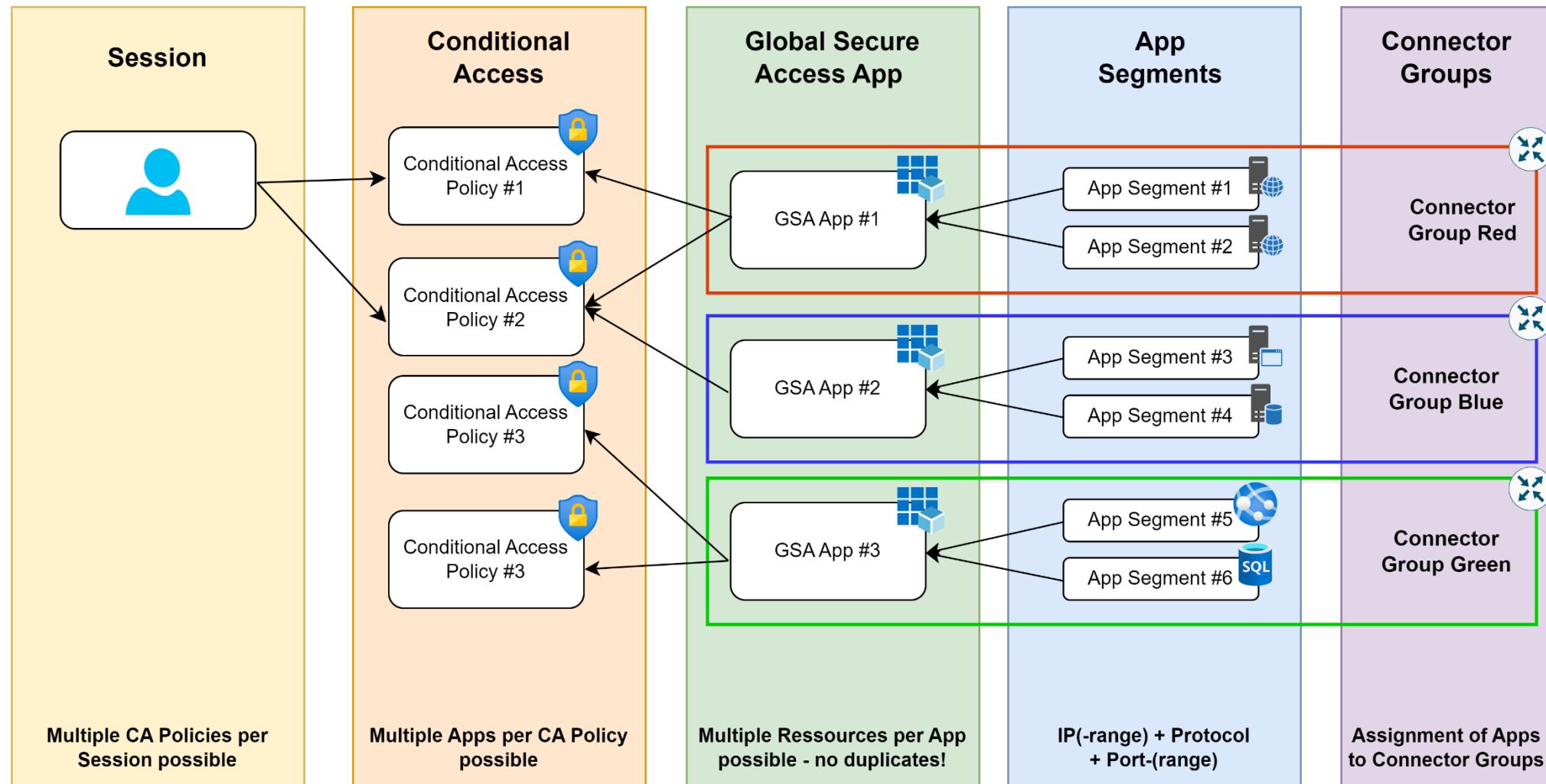
# EPA Conditional Access Integration



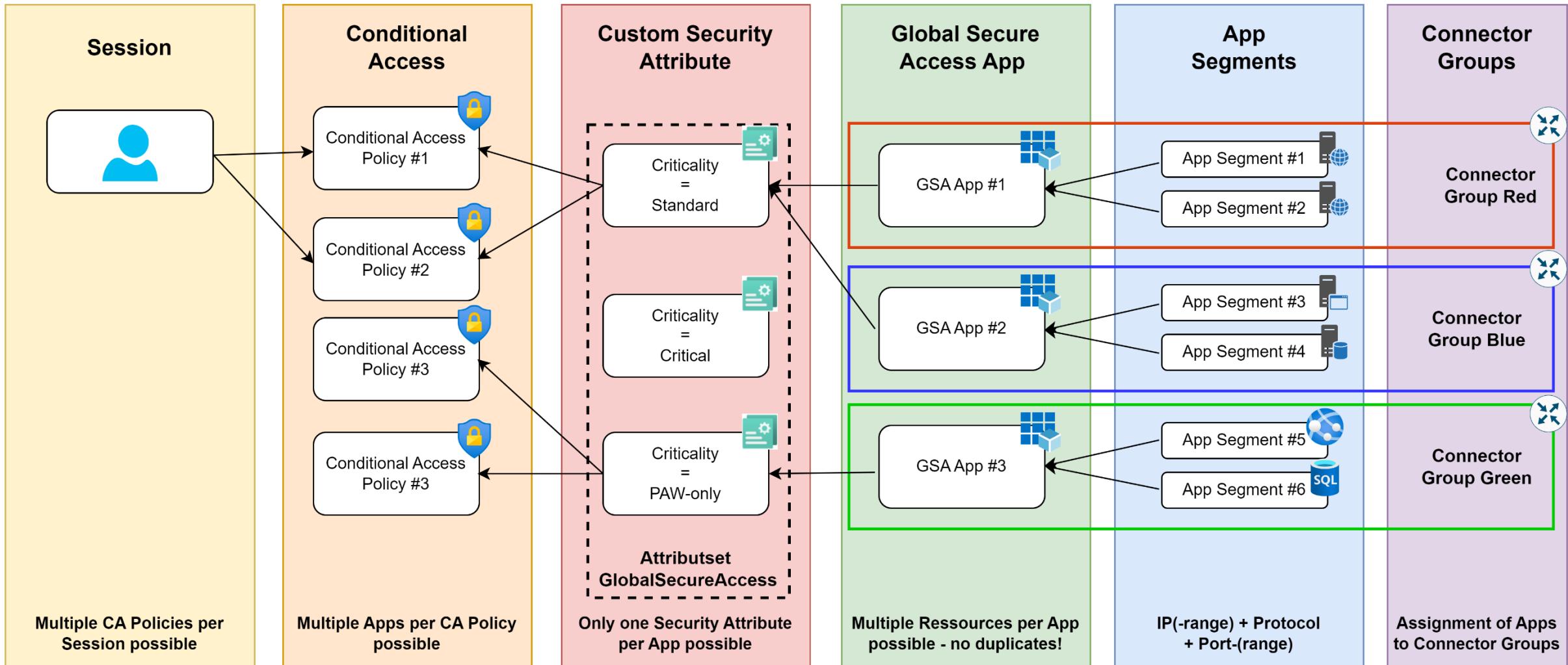
# Conditional Access Integration for VPN



# GSA Conditional Access Integration



# Custom Security Attribute Extension



# Step-up auth for specific app segments

Home > Conditional Access | Policies >

**EPA 1 - Require YubiKey for Admin Access** Conditional Access policy

[Delete](#) [View policy information](#)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \* **EPA 1 - Require YubiKey for Admin Access**

Assignments

Users or workload identities [①](#)

Specific users included and specific users excluded

Target resources [①](#)

1 app included

Network NEW [①](#)

Not configured

Conditions [①](#)

0 conditions selected

Access controls

Grant [①](#)

1 control selected

Session [①](#)

**Sign-in frequency - Every time** Session

**Grant**

Control access enforcement to block or grant access. [Learn more](#)

Block access  Grant access

Require multifactor authentication

**⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)**

**Require authentication strength** [YubiKey Only](#)

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more](#)

Require device to be marked as compliant

Require Microsoft Entra hybrid joined device

Require approved client app [See list of approved client apps](#)

Require app protection policy [See list of policy protected client apps](#)

Recycle Bin

share

Search share

New Sort View Details

Name	Date modified	Type	Size
New folder	29/07/2024 10:28	File folder	0
Ninja!	28/08/2024 12:33	File folder	0
New Text Document	26/01/2024 11:45	Text Document	0
test	29/07/2024 10:29	Text Document	1

Desktop Downloads Documents Pictures Music Videos share OneDrive

4 items

Thursday, 29 August 2024

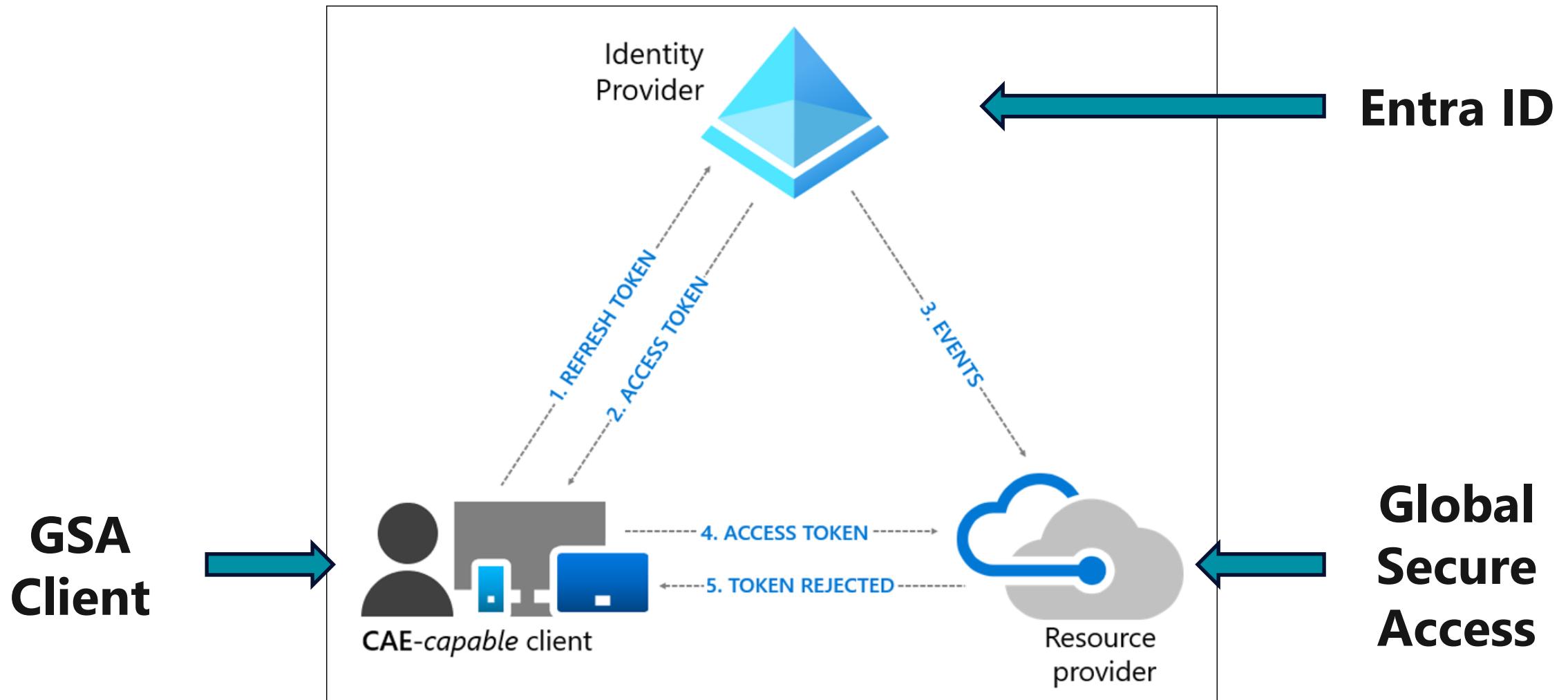
15:20 29/08/2024

 RDCMan

**experts live Germany**



# Universal Continuous Access Evaluation

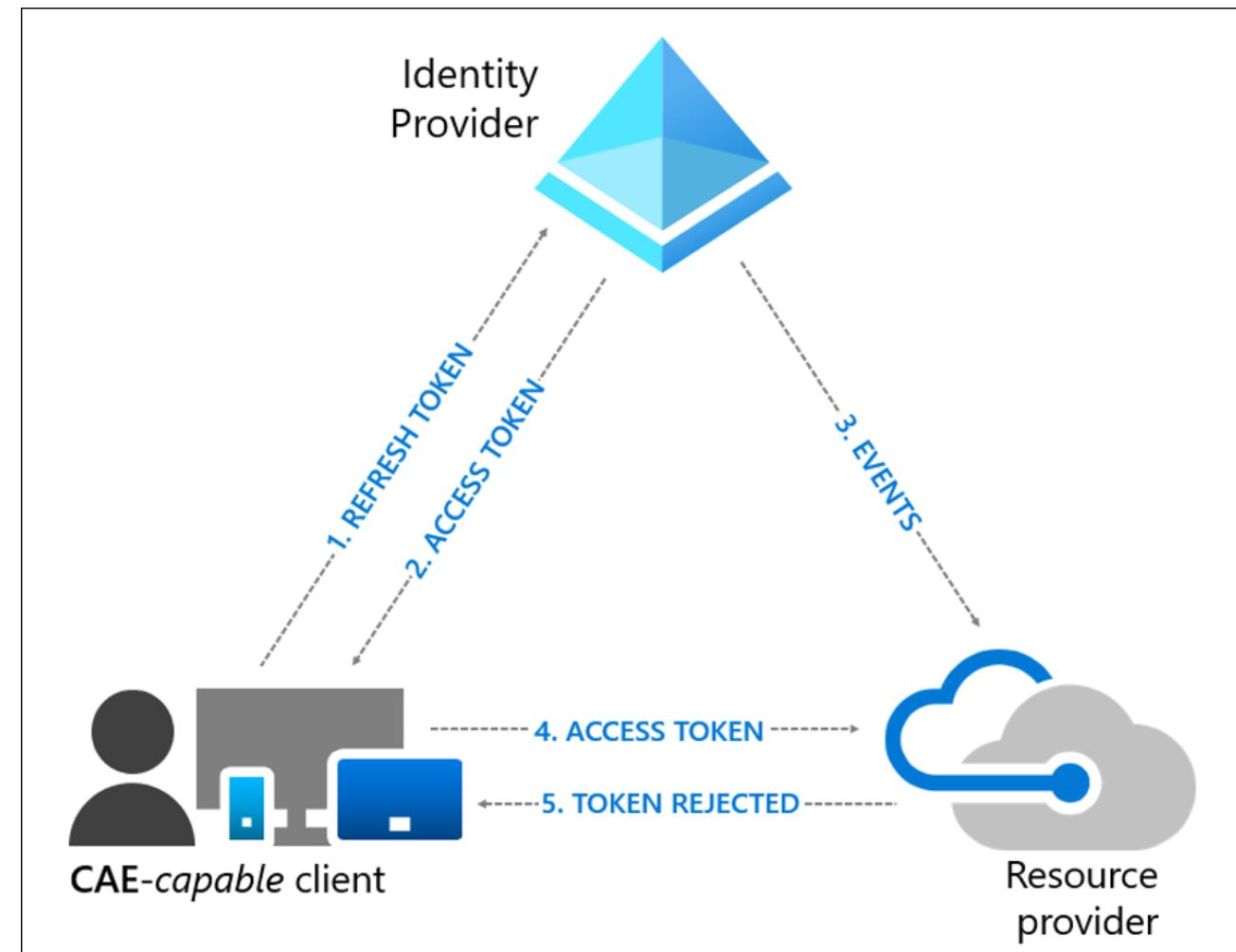




# Universal Continuous Access Evaluation

## Trigger events for Universal CAE:

- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Microsoft Entra ID Protection

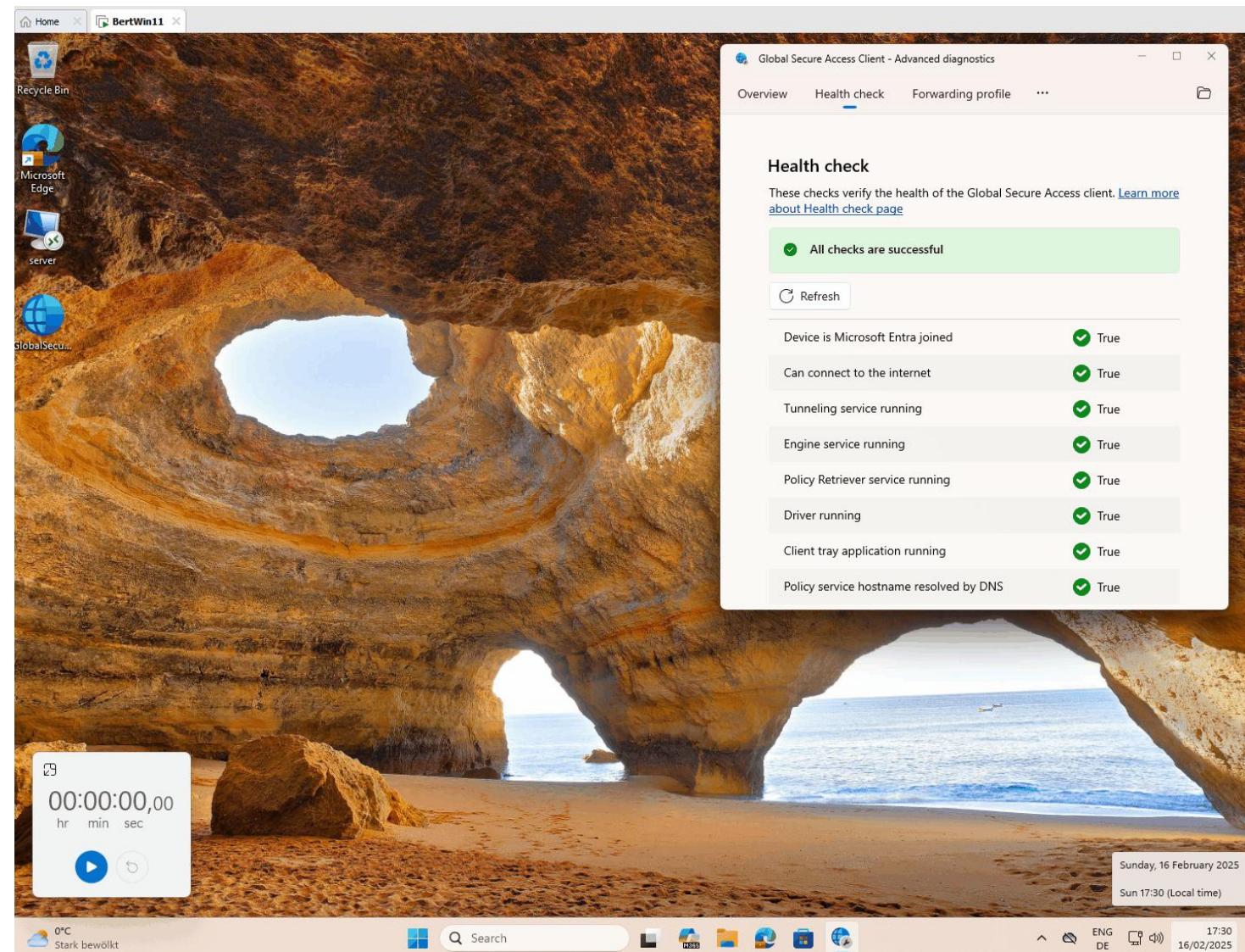




# Universal Continuous Access Evaluation

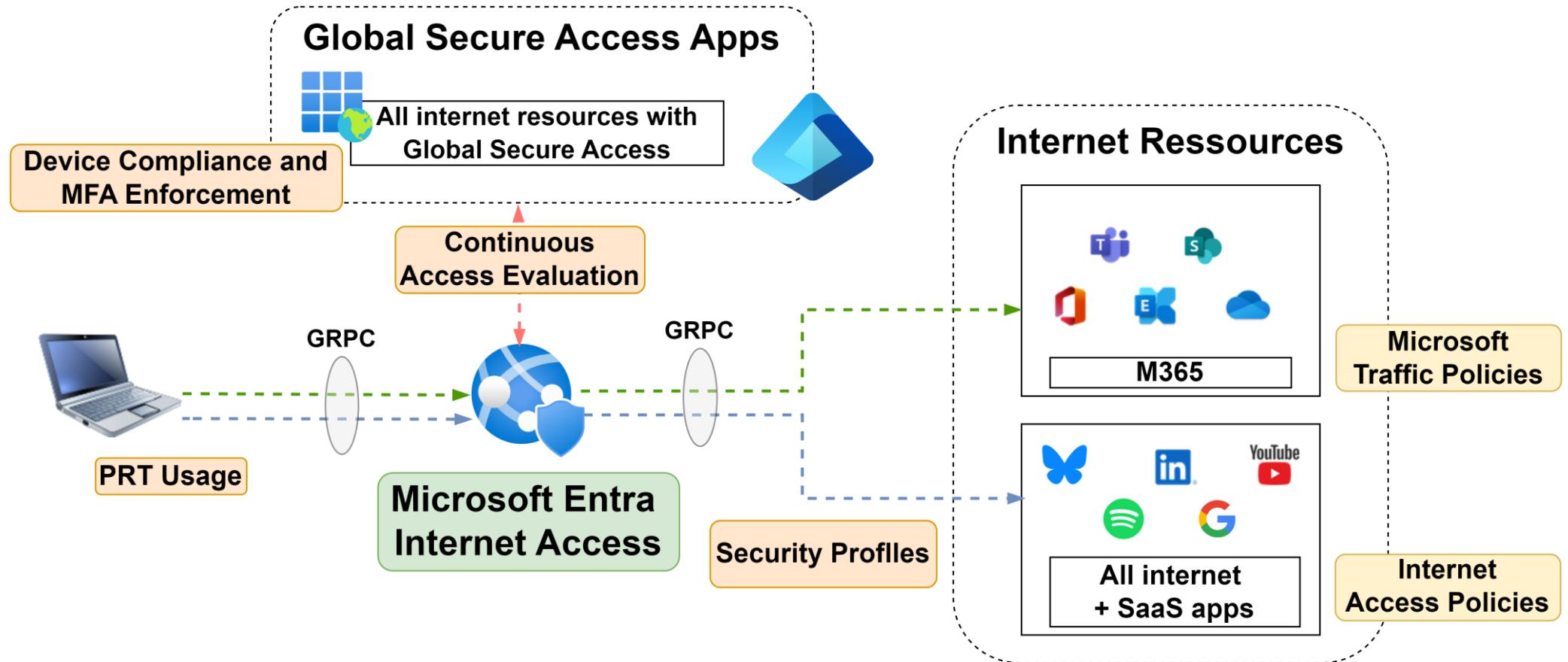
## Trigger events for Universal CAE:

- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Microsoft Entra ID Protection

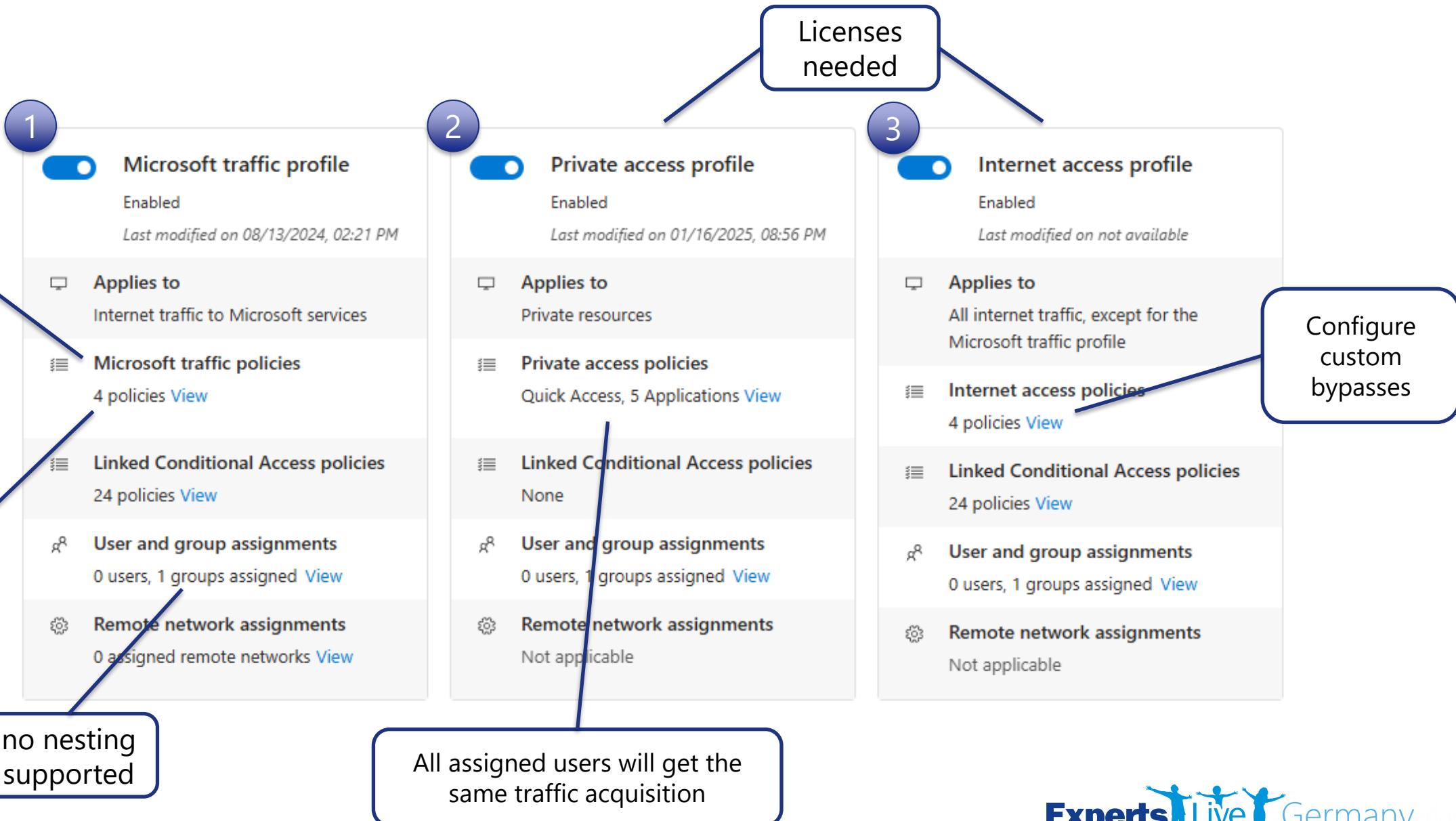




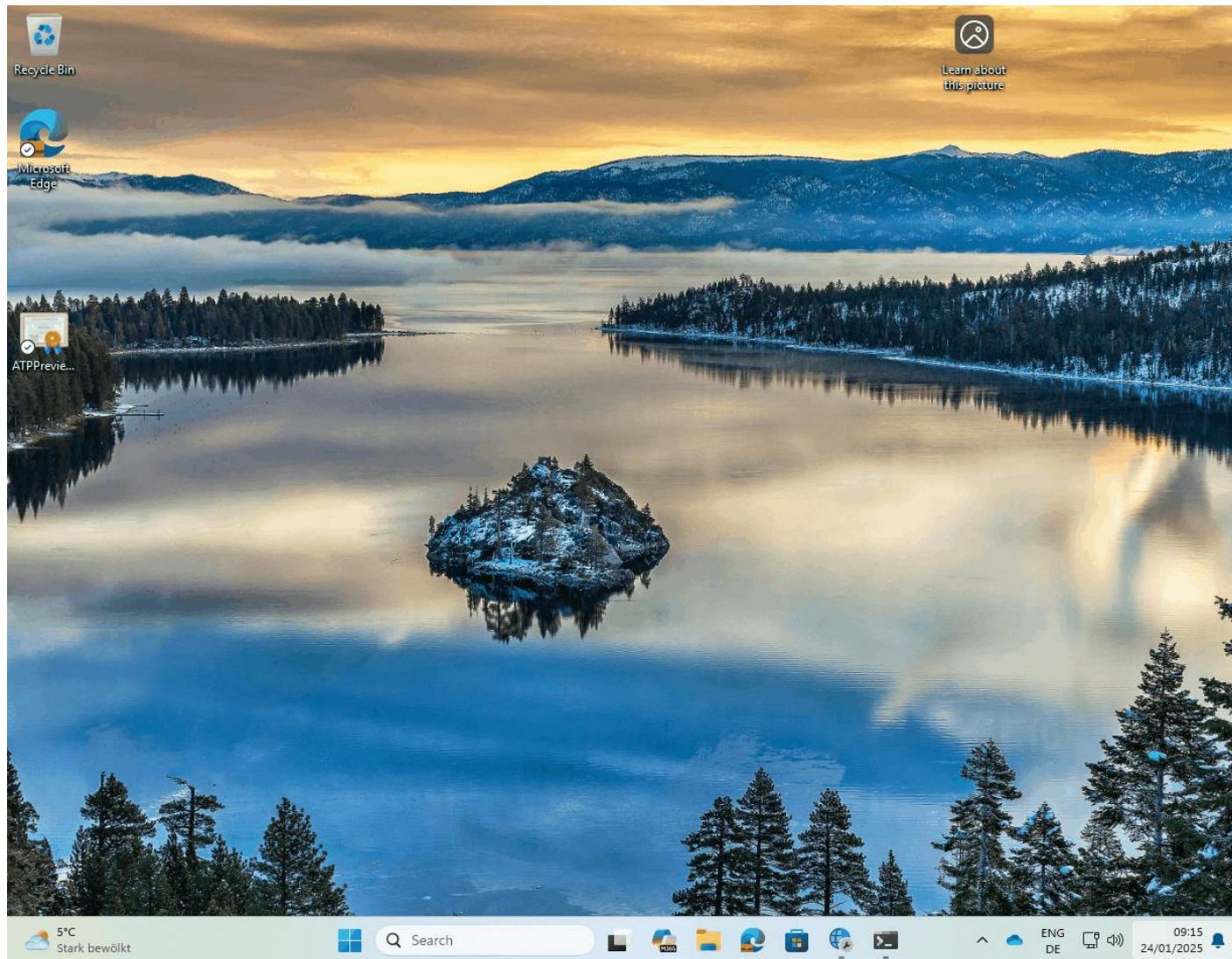
# Entra Internet Access



# Side note: traffic acquisition



# Using the Webfilter in Entra Internet Access



Name \*  
EIA 1 - Apply Basic Employee Web Filtering

Assignments

Users or workload identities (i)

Specific users included

Target resources (i)

All internet resources with Global Secure Access

Network NEW (i)

Not configured

Conditions (i)

0 conditions selected

Access controls

Grant (i)

0 controls selected

Session (i)

Conditional Access Network Control selected

Select what this policy applies to  
Resources (formerly cloud apps) (i)

**Include**   **Exclude**

None

All internet resources with Global Secure Access

All resources (formerly 'All cloud apps')

Select resources

Use Global Secure Access security profile (i)

Basic Employee Profile

IT Guys Profile

Basic Employee Profile

# Using the Webfilter in Entra Internet Access

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot Admin-Chris@c4a8feluc... GK FELICIA DEMO ENVIRONME...

Home > Charles Waldorf

## Charles Waldorf | Sign-in logs

User

Search

Date : Last 24 hours Show dates as : Local User contains adf2e754-b0d1-4794-9fe4-3a4ce0458365 Time aggregate : 24 hours

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Resource contains Internet resources with Global Secure Access Add filters

Sign-in logs

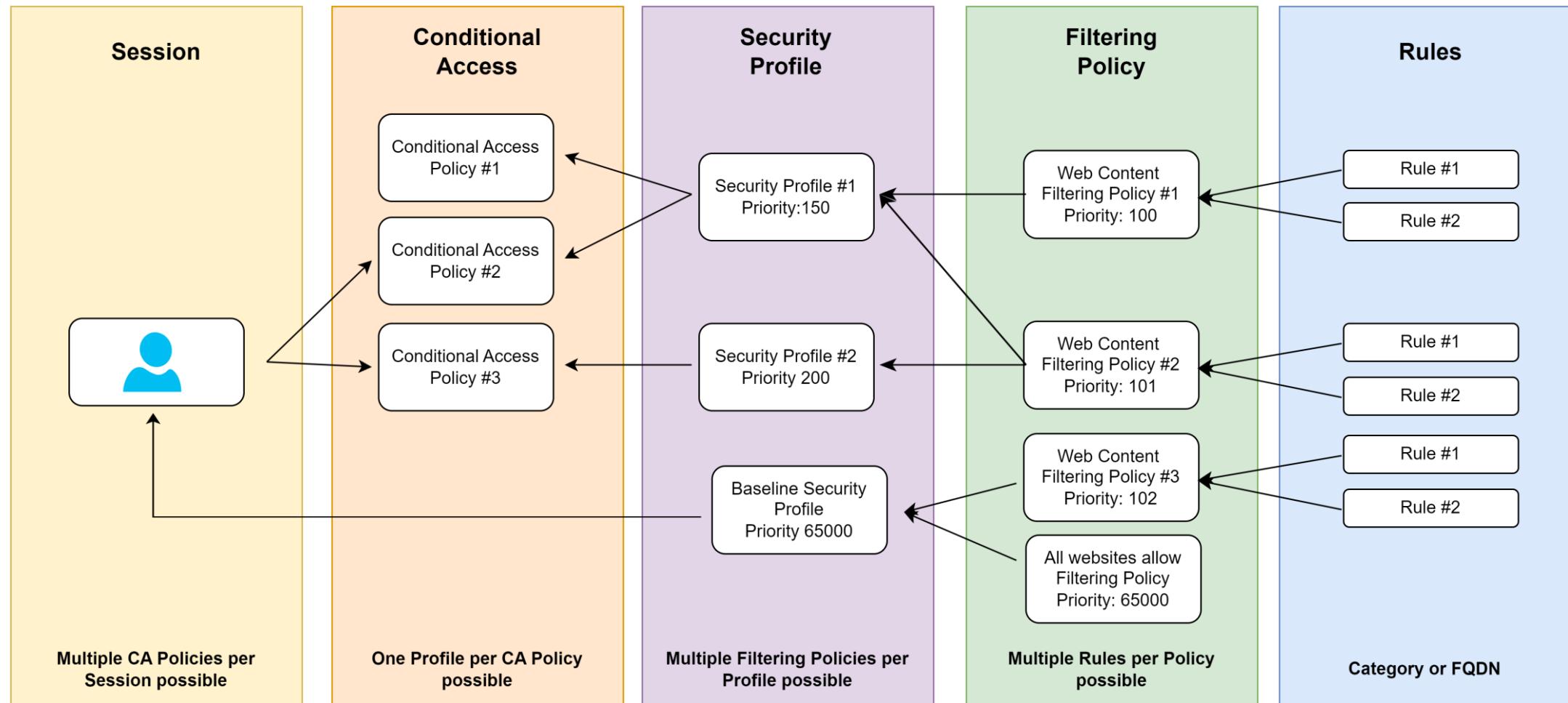
Overview Audit logs Diagnose and solve problems Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods

User sign-ins (interactive) User sign-ins (non-interactive)

Sign-ins in the table below are grouped by user and resource. Click on a row to see all the sign-ins for a user and resource on that date and time.

Date	Request ID	Username	Application	Status	IP address	Resource	Resource ID	Condition	
1/24/2025, 1:00:00	Aggregate	waldorf@gkfelicia.net	Global Secure Acces...	Success	84.46.12.242	Internet resources wi...	5dc48733-b5df-475c...	Success	
1/24/2025, 9:1	0f60614a-9c51-4261-b	waldorf@gkfelicia.net	Global Secure Acces...	Success	84.46.12.242	Internet resources wi...	5dc48733-b5df-475c...	Success	
1/24/2025, 8:5	16a08f1b-9c0c-4e3a-9	waldorf@gkfelicia.net	Global Secure Acces...	Success	84.46.12.242	Internet resources wi...	5dc48733-b5df-475c...	Success	
>	1/23/2025, 1:00:00	Aggregate	waldorf@gkfelicia.net	Global Secure Acces...	Success	87.179.10.1	Internet resources wi...	5dc48733-b5df-475c...	Success

# EIA Conditional Access Integration



# "Compliant Network" Condition

- Reasonable policy:
  - "Require Compliant Network to access Cloud Apps"
- Incompatible with
  - Require app protection policy
  - Require approved client app
  - Use Global Secure Access security profile

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more ↗](#)

Name \*

GSA - Require Compliant Network to access...

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Target resources ⓘ

1 app included

Network NEW ⓘ

Any network or location and 1 excluded

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Control user access based on their network or physical location. [Learn more ↗](#)

Configure ⓘ

Yes

No

Include Exclude

Select the locations to exempt from the policy

- All trusted networks and locations
- All Compliant Network locations (Preview)
- Selected networks and locations

⚠ All Compliant Network locations" does not work with "Require app protection policy" or "Require approved client app" grant controls. [Learn more ↗](#)

ℹ 'Locations' condition is moving! Locations will become the 'Network' assignment with a new Global Secure Access capability of 'All Compliant network locations'. No action required. [Learn more ↗](#)

# The Compliant Network Condition

**Name \***  
EIA 3 - Require Compliant Network to access...

**Assignments**

Users or workload identities ⓘ  
Specific users included and specific users excluded

**Target resources ⓘ**  
All resources (formerly 'All cloud apps') included and 2 resources excluded

**Network NEW ⓘ**  
Any network or location and 1 excluded

**Conditions ⓘ**  
1 condition selected

**Access controls**

Grant ⓘ  
Block access

**Session ⓘ**  
0 controls selected

**Include Exclude**  
Select the resources to exempt from the policy

None  
 All internet resources with Global Secure Access  
 Select resources

**Edit filter**  
None

**Select**  
Microsoft Intune Enrollment and 1 more

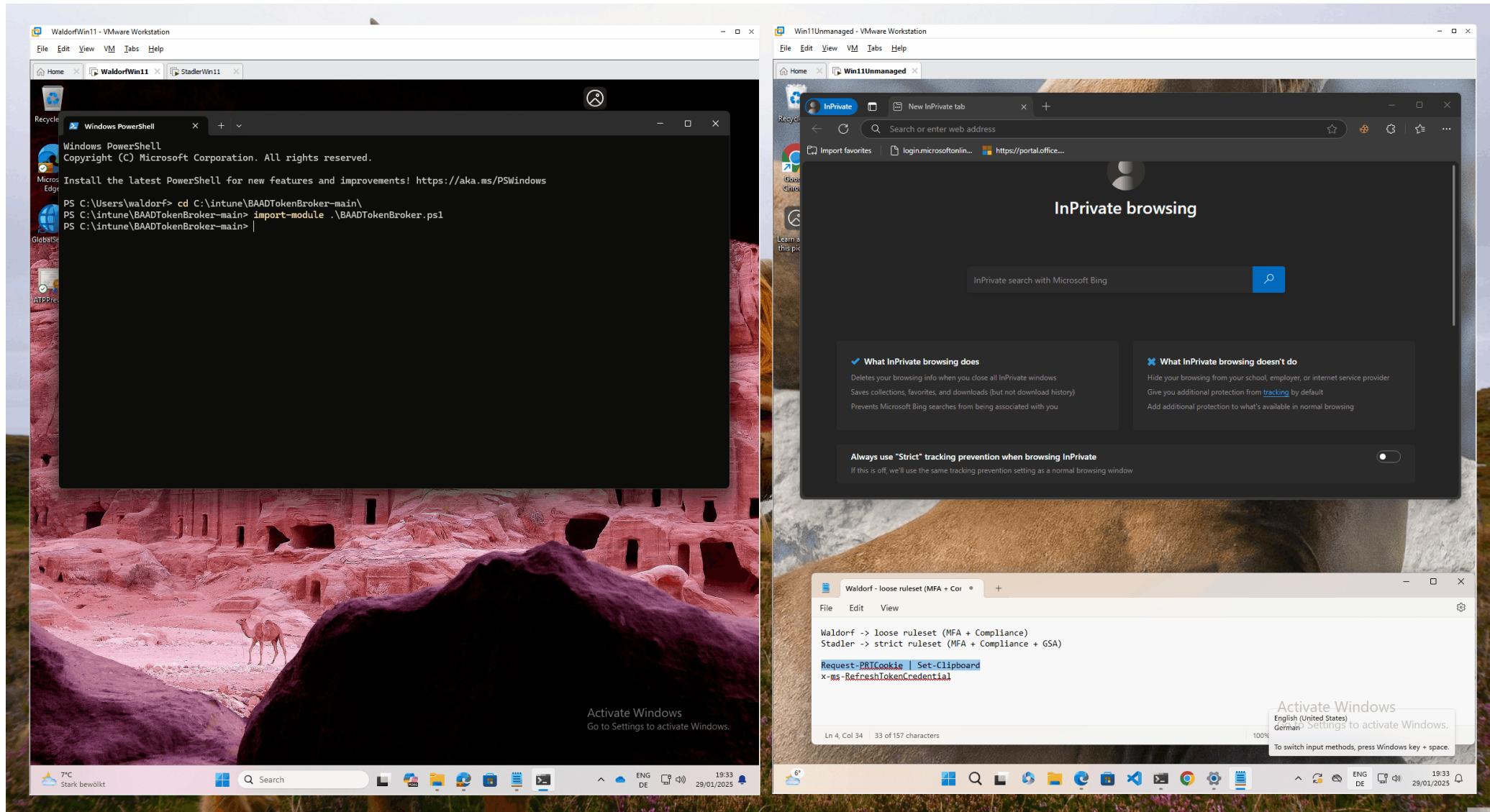
MI Microsoft Intune 0000000a-0000-0000-c000-000000000000 ...  
MI Microsoft Intune Enrollment d4ebce55-015a-49b5-a083-c84d1797ae...

## Examples for additional exclusions:

### Azure Windows VM Sign-In

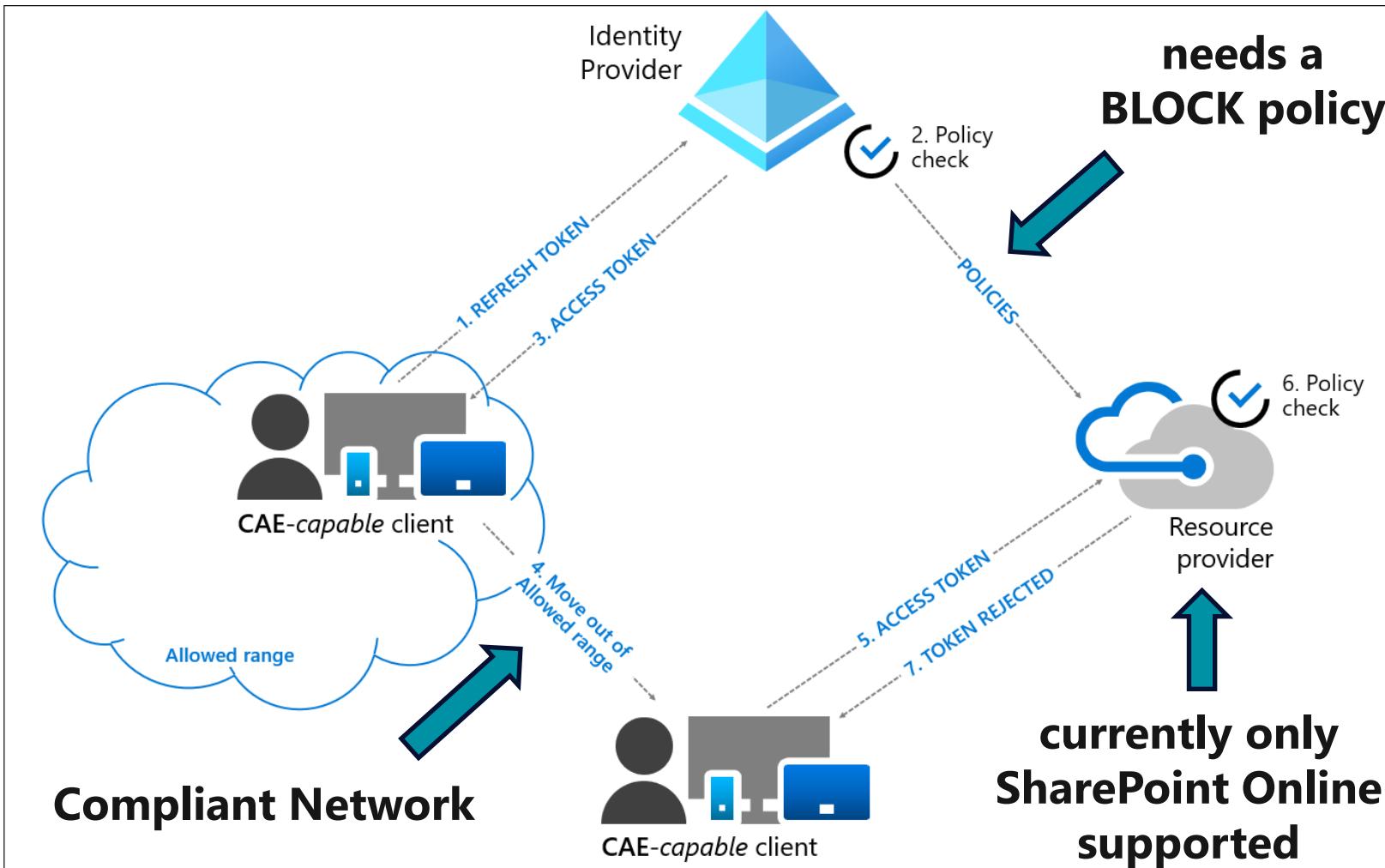
Azure Virtual Desktop  
Windows 365  
Microsoft Remote Desktop  
Windows Cloud Login

# The Compliant Network Condition





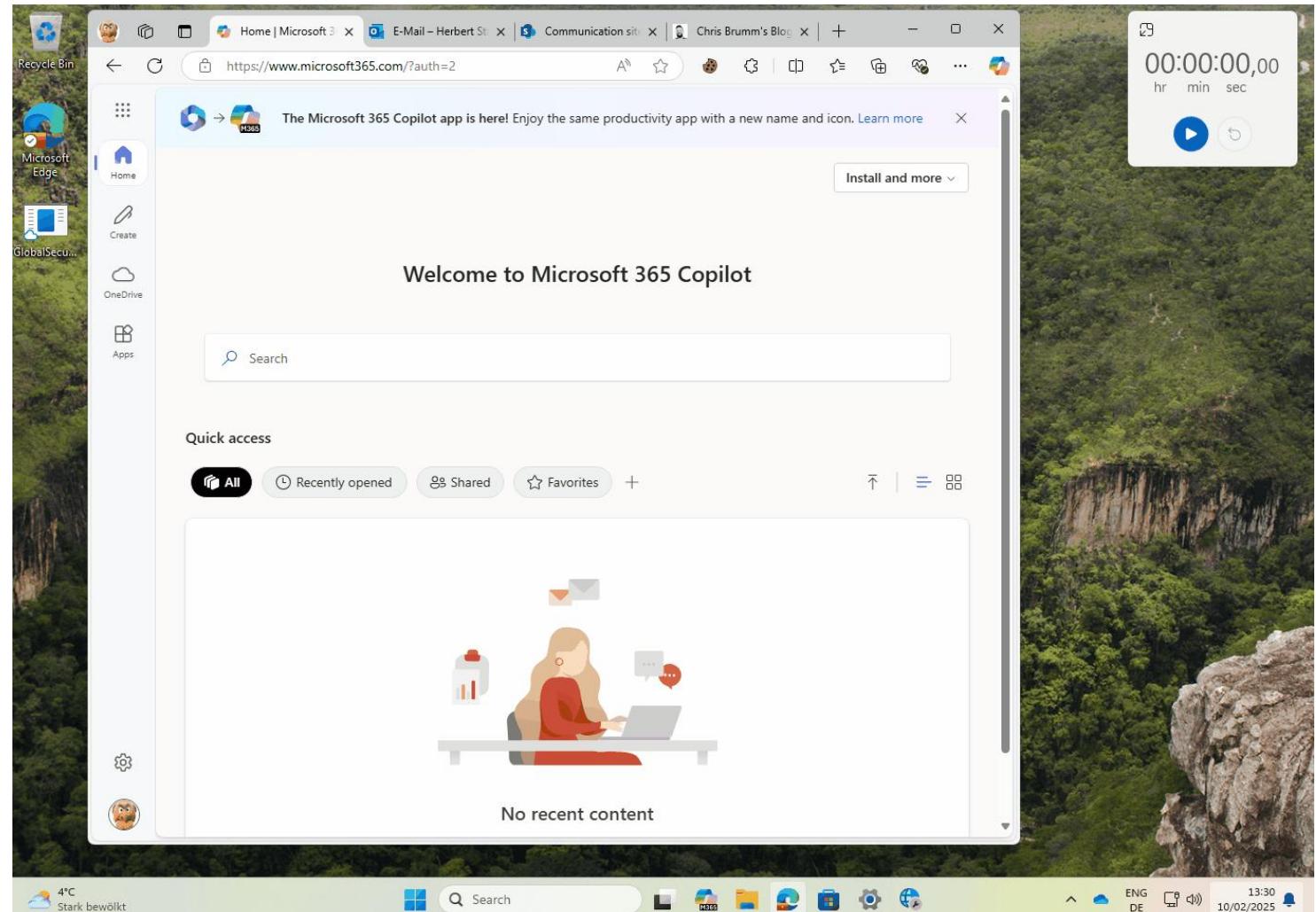
# GSA Compliant Network and CAE





# Leaving the compliant network

- Data plane enforcement works with services that support Continuous Access Evaluation (CAE) - **currently, only SharePoint Online**.
- With apps that support CAE, stolen access tokens that are replayed outside your tenant's compliant network will be rejected by the application **in near-real time**.
- Without CAE, a stolen access token will last up to its full lifetime (default 60-90 minutes).





Vielen Dank an unsere Sponsoren!

---

Diamond



---

Platinum



---

Gold





Bitte gebt uns euer Feedback!

Feedback geben und Geschenk mitnehmen

Vielen Dank!