Protect your Tokens!
FIDO won’t help you!


FIDO2
SECURITY

AGENDA

01 What can (and can’t) FIDO2 do?

02 How do Tokens in Entra ID work?

03 How can Tokens be abused?

04 What can we do to protect Tokens?

whoami - Marco

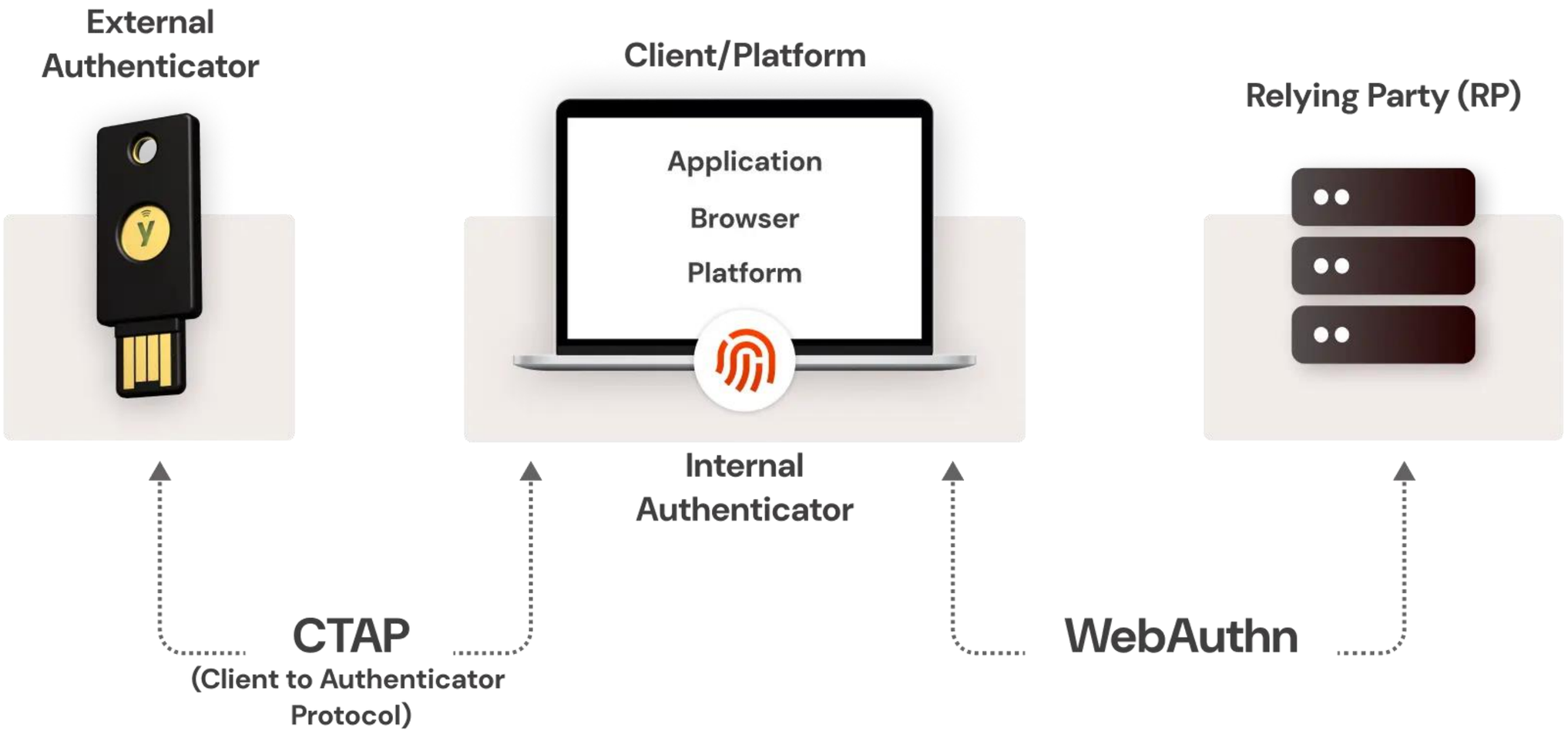
Security Engineer @ GrabX Solutions

Working with customers to protect their cloud environments

Bern, Switzerland

thesecurityguy.ch

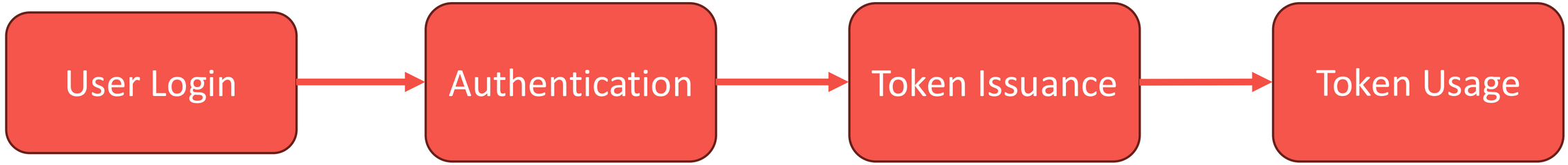
What is FIDO2?

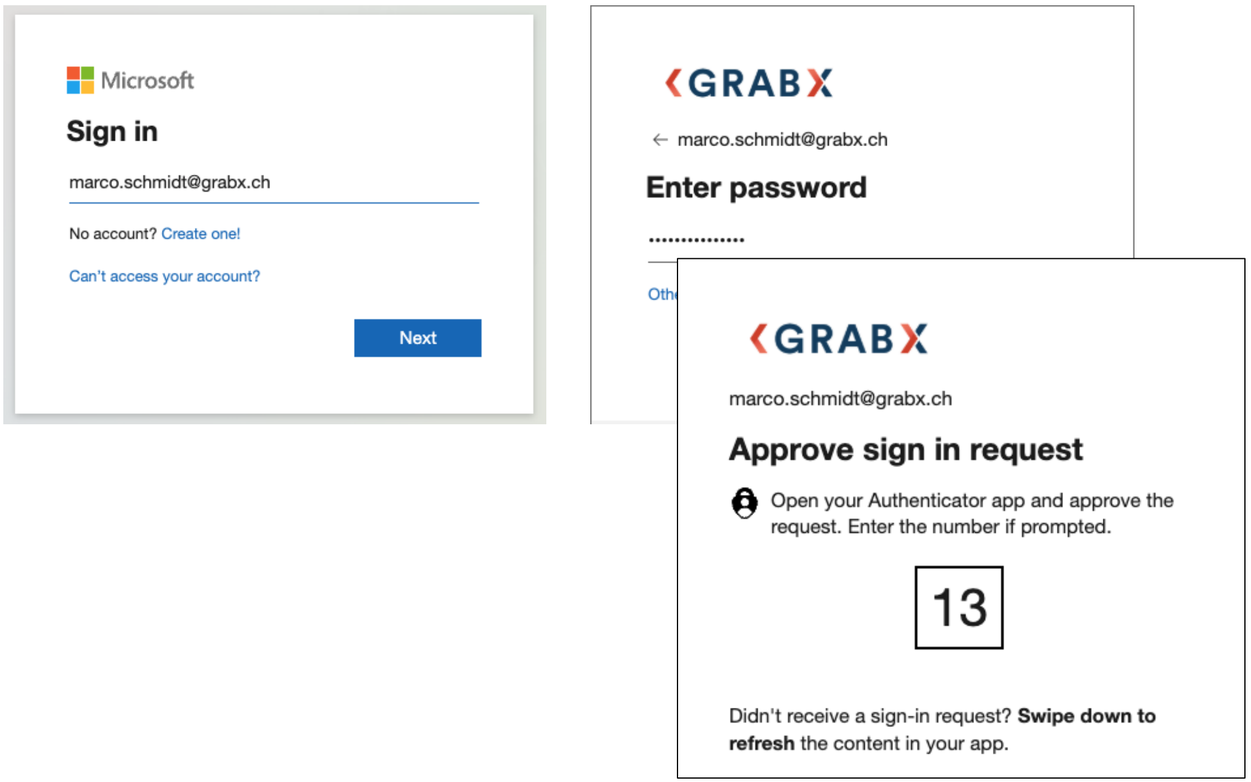


FIDO2 advantages

- Passwordless
- Phishing resistance
- Ease of use
- Public-key Authentication based

Sign-In Flow


User Login
Authentication
Token Issuance
Token Usage


Microsoft
Sign in
marco.schmidt@grabx.ch
No account? Create one!
Can't access your account?
Next
GRABX
marco.schmidt@grabx.ch
Enter password
GRABX
marco.schmidt@grabx.ch
Approve sign in request
Open your Authenticator app and approve the request. Enter the number if prompted.
13
Didn't receive a sign-in request? Swipe down to refresh the content in your app.

Tokens – JSON Web Token (JWT)

eyJ0eXAiOiJKV1QiLCJub25jZSI6IjFWWVR1RWQ2UHlaYlMyOGdScWVKWDB4dmVQU0JrMVotX0syRnRya1MyZFEiLCJhbGciOiJSUzI1NiIsIng1dCI6IkpZaEFjVFBNWl9MWDZEQmxPV1E3SG4wTmVYRSIsImtpZCI6IkpZaEFjVFBNWl9MWDZEQmxPV1E3SG4wTmVYRSJ9.eyJhdWQiOiIwMDAwMDAwMy0wMDAwLTAwMDAtYzAwMC0wMDAwMDAwMDAwMDAiLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9hMmZhOTE1OC02NTY3LTQ5N2MtYTgwNS1mNTNjZmY5OTM3YjMvIiwiaWF0IjoxNzU3MDcyNjcxLCJuYmYiOjE3NTcwNzI2NzEsImV4cCI6MTc1NzA3NzY4MCwiYWNjdCI6MCwiYWNyIjoiMSIsImFjcnMiOlsicDEiLCJ1cm46dXNlcjpyZWdpc3RlcnNlY3VyaXR5aW5mbyJdLCJhaW8iOiJBY1FBTy84WkFBQUF2bS9lelRvK1dKNEUzQ1RhOWQ1SDF5NGg2TlhrQy9BNFJLSGEyWFMyZkZxbUFEMzVodENHUGRVVzdOYTNjTURmK2FEdnBvMURremNYS0IwUHJ4ZzVSaUhveTdkZitrc0lER1k1cmZpWG9YbWJhR25Yd0o0a1BHVmdUdnU5RUtFWkJyeDc0VUs1Z1R3SEdqaUtXMngyOXQwL2Q3NjRXRkxwRDhOK1FUS3JGdWV5Vys0R3RNQkxIV3Z4MFlTMzMrYllRektmV0VSdVBnOVZXNkxWU0Y1a3REc1g2N09DRzk4TGxHZUI4RERCaGQzSG44UGRYc0xzbklvMnVIVWFjNWFqIiwiYW1yIjpbInJzYSIsIm1mYSJdLCJhcHBfZGlzcGxheW5hbWUiOiJHcmFwaCBFeHBsb3JlciIsImFwcGlkIjoiZGU4YmM4YjUtZDlmOS00OGIxLWE4YWQtYjc0OGRhNzI1MDY0IiwiYXBwaWRhY3IiOiIwIiwiaXBhZGlzcGxheW5hbWUiOiJHcmFwaCBFeHBsb3JlciIsImFwcGlkIjoiZGU4YmM4YjUtZDlmOS00OGIxLWE4YWQtYjc0OGRhNzI1MDY0IiwiYXBwaWRhY3IiOiIwIiwiY29udHJvbHMiOlsiYXBwX3JlcyJdLCJhcHBfZGlzcGxheW5hbWUiOiJHcmFwaCBFeHBsb3JlciIsImFwcGlkIjoiZGU4YmM4YjUtZDlmOS00OGIxLWE4YWQtYjc0OGRhNzI1MDY0IiwiYXBwaWRhY3IiOiIwIiwiY29udHJvbHMiOlsiYXBwX3JlcyJdLCJhcHBpZCI6IjcxNDQxMzNmLTcyNjAtNDAzNi1iMTA4LTIwODMxZjgzZTQ0NSIsImZhbWlseV9uYW1lIjoiU2NobWlkdCIsImdpdmVuX25hbWUiOiJNYXJjbyIsImlkdHlwIjoidXNlciIsImlwYWRkciI6IjgzLjc4LjE4OC4xMjAiLCJuYW1lIjoiTWFyY28gU2NobWlkdCIsIm9pZCI6IjhmODlmZjAxLTc2ZTMtNDM5Mi1hMzQ5LWYzNmJhNWMwOTZmNCIsInBsYXRmIjoiNSIsInB1aWQiOiIxMDAzMjAwMjRDQjNBM0NFIiwicmgiOiIxLkFUQUFXSkg2b21kbGZFbW9CZlU4XzVrM3N3TUFBQUFBQUFBQXdBQUFBQUFBQUFCREFVNHdBQS4iLCJzY3AiOiJDYWxlbmRhcnMuUmVhZFdyaXRlIENvbnRhY3RzLlJlYWRXcml0ZSBGaWxlcy5SZWFkV3JpdGUuQWxsIEdyb3VwLlJlYWRXcml0ZS5BbGwgTWFpbC5SZWFkV3JpdGUgTm90ZXMuUmVhZFdyaXRlLkFsbCBvcGVuaWQgUGVvcGxlLlJlYWRXcml0ZSBaXRlcy5SZWFkV3JpdGUuQWxsIFRhc2tzLlJlYWRXcml0ZSBUZWFtd29ya0FwcFNldHRpbmdzLlJlYWRXcml0ZS5BbGwgVXNlci5SZWFkV3JpdGUgQWxsIFFvZXIuUmVhZEJhc2lljLkFsbCBVc2VyLlJlYWRXcml0ZSBlbWFpbCIsInNpZCI6IjAwNmYxZDY5LTRjOWQtMTE5YS05OTg4LTdlZTIyYmQ5OGM3NSIsInNpZ25pbl9zdGF0ZSI6WyJkdmNfbW5nZCIsImR2Y19jbXAiLCJrbXNpIl0sInN1YiI6IlpveHpfeERVTUlxRzh6bS10Z0ZQWmxUQlFXTHVQVmFjTmw0VmFEc0c4dFUiLCJ0ZW5hbnRfcmVnaW9uX3Njb3BlIjoiRVUiLCJ0aWQiOiJhMmZhOTE1OC02NTY3LTQ5N2MtYTgwNS1mNTNjZmY5OTM3YjMiLCJ1bmlxdWVfbmFtZSI6Im1hcmNvLnNjaG1pZHRAZ3JhYnguY2giLCJ1cG4iOiJtYXJjby5zY2htaWR0QGdyYWJ4LmNoIiwidXRpIjoib085RVVPT2pkMEc1REFQX3I2SWpBUSIsInZlciI6IjEuMCIsIndpZHMiOlsiYjc5ZmJmNGQtM2VmOS00Njg5LTgxNDMtNzZiMTk0ZTg1NTA5Il0sInhtc19jYyI6WyJDUDEiXSwieG1zX2Z0ZCI6Im16OWMxSkhZU3RmNVlMQ2FZWmxUS0Q5T29adzhVall6OVoxS3g5bjE4R1FCYzNkbFpHVnVZeTFrYzIxeiIsInhtc19pZHJlbCI6IjEgOCIsInhtc19zdCI6eyJzdWIiOiIzckMtdUhtcDFYM1dlVXZuRDV3WDVPQ0pvQXVrdU9icHhvV1ZnNW9jZlhBIn0sInhtc190Y2R0IjoxNTM3ODEzNDQ0LCJ4bXNfdGRiciI6IkVVIn0.RTId1Dwczr-4ot6LzX9DzeOrRJJN13lNvOMQsP5roTNEfg9d6Zng7SfwLV5LJTu06Spyd-aYf65UmH6HgtJsC_E0_0xvknCh-WErW-HvO1FMkyNvDI8p0s4jPAo4fi1gNddLriPC-Pt-cm8no6z6xq5aXibgF8s4L0bRAhHt7akeVyNMHup-ZJgllR4Fe7xNDREjVW3Z8pXT30be3gLDut0Xu3OTk2U48s6MSpyNvHc0MfH-Q9EwTiiRmi4Ewlkd81haixv9X8c4tAK9dYNXKCjhuK5yURVKYrnOhQZsui-il-aO48QH1Axez37Ok2uF3LDIFBzNox6i7j0zRSryow

Token Terminology

- Primary Refresh Token (PRT)
- Refresh Token (RT)
- Access Token (AT)

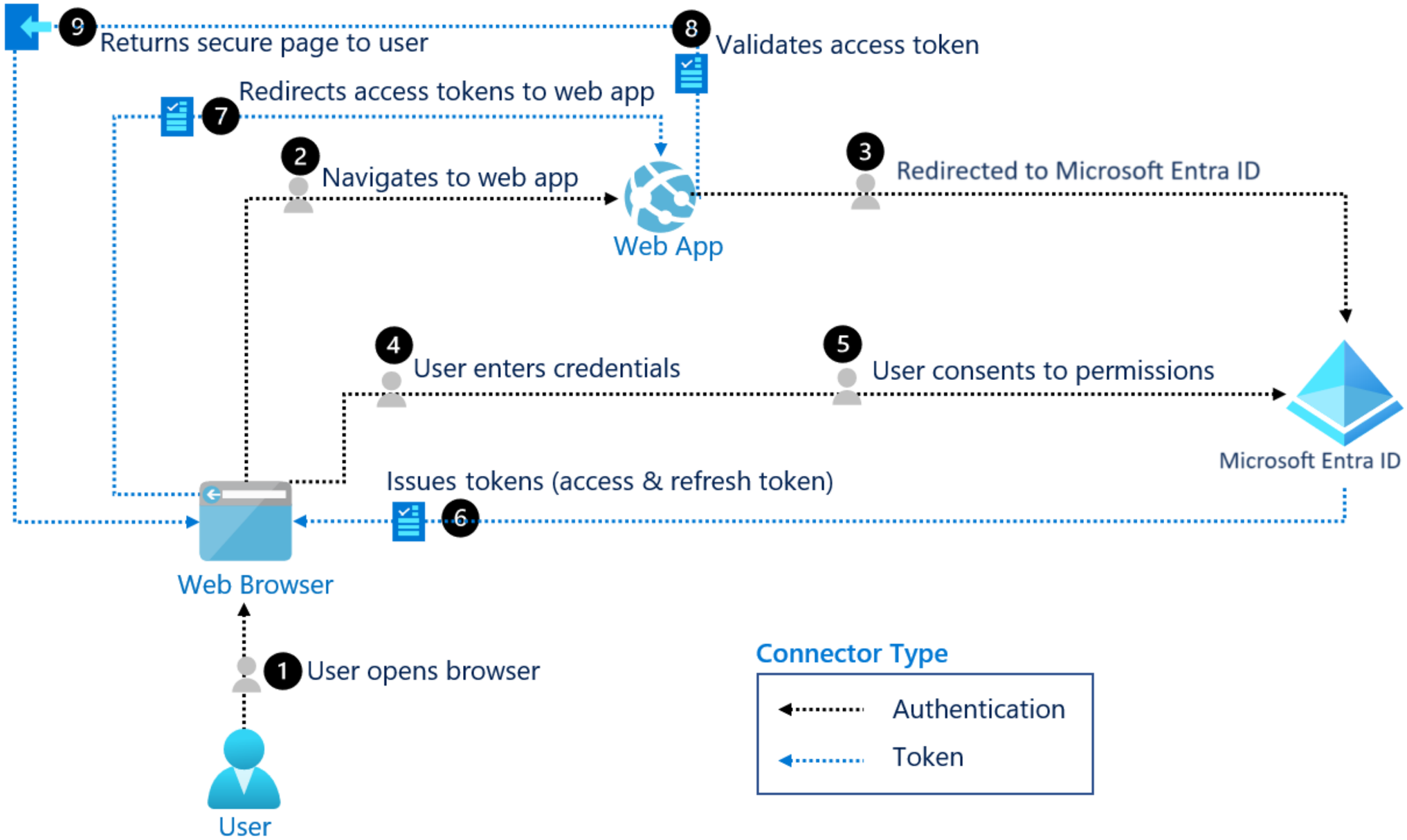
- Entra ID Continuous Access Evaluation (CAE)
- Entra ID Token Protection

GRABX

The Rules

1. Tickets always have to be signed by the counter to be valid
2. Each Ticket has a Lifetime
3. To enter a tent, you need a separate ticket
4. No communication between counter and Security

OIDC Authentication Flow




TOKENS
ENTRA ID
SECURITY
SECURITY
SECURITY
SECURITY

Token Lifetimes

Token Type	Lifetime	Comment
Primary Refresh Token	14 days	
Refresh Tokens	90 days	There is also a special type called “Familiy Refresh Tokens” which is not documented by MS
Access Tokens	1 hour	
Access Tokens (CAE)	24 hours	Access Tokens that are issued to CAE compatible Apps

CA Policies PRT

https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token

> ⓘ **Note**
>
> Microsoft Entra Conditional Access policies aren't evaluated when PRTs are issued.

How is the PRT protected?

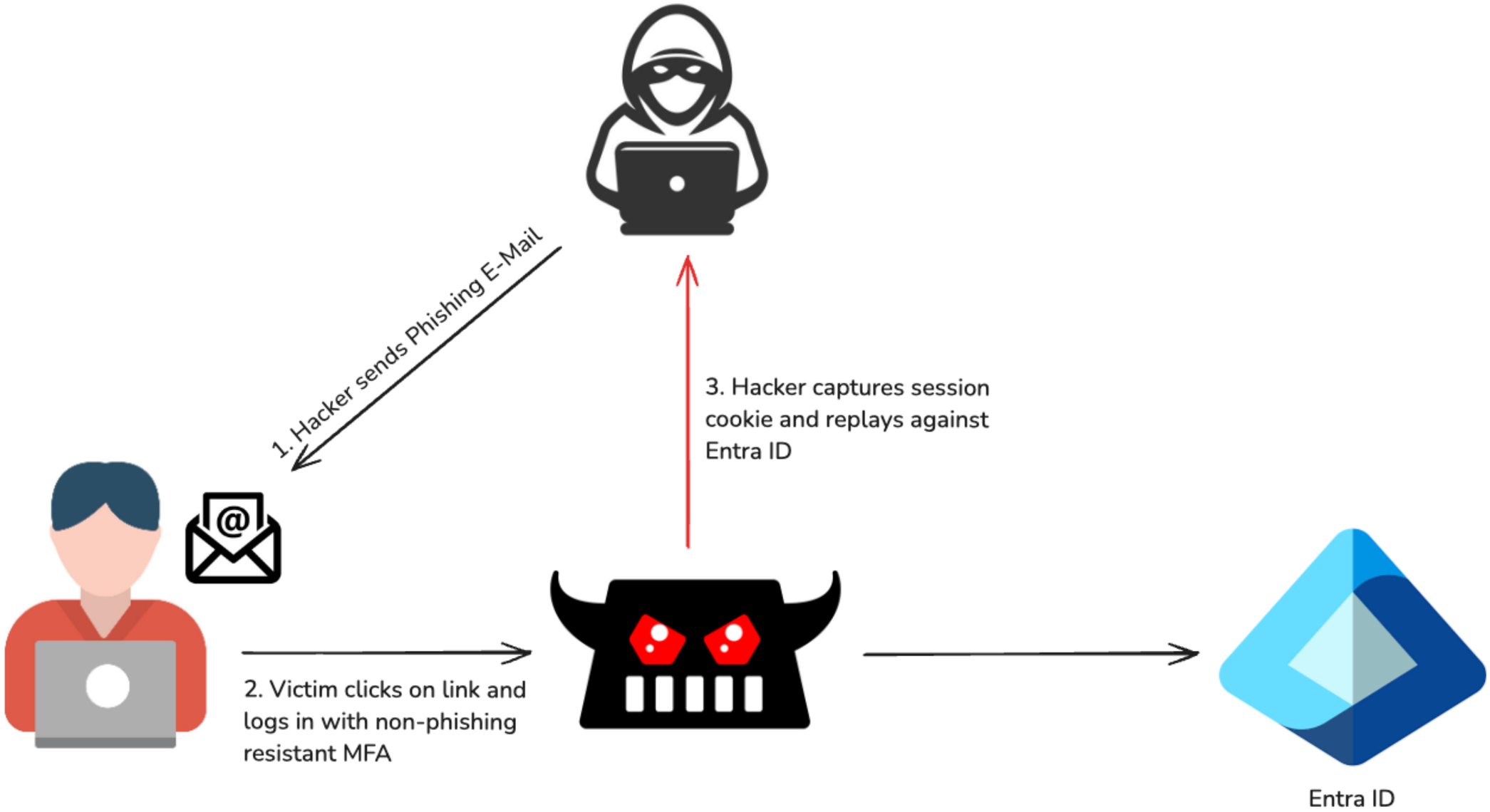
A PRT is protected by binding it to the device the user has signed in to. Microsoft Entra ID and Windows 10 or newer enable PRT protection through the following methods:

GRABX

How do attackers get my tokens?

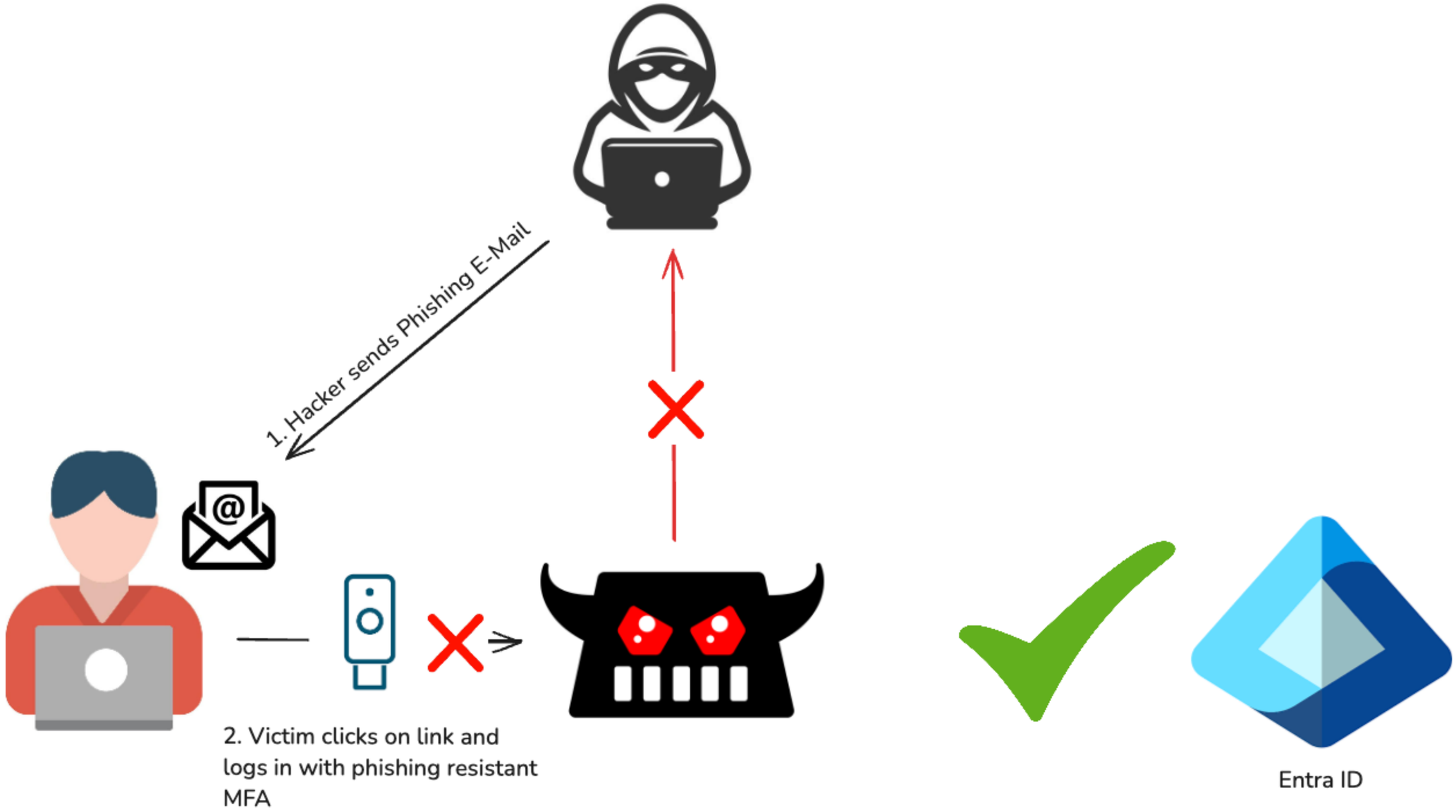
GRABX

AiTM Attack


1. Hacker sends Phishing E-Mail
3. Hacker captures session cookie and replays against Entra ID
2. Victim clicks on link and logs in with non-phishing resistant MFA
Entra ID

DEMO TIME!

AiTM Attack with FIDO2



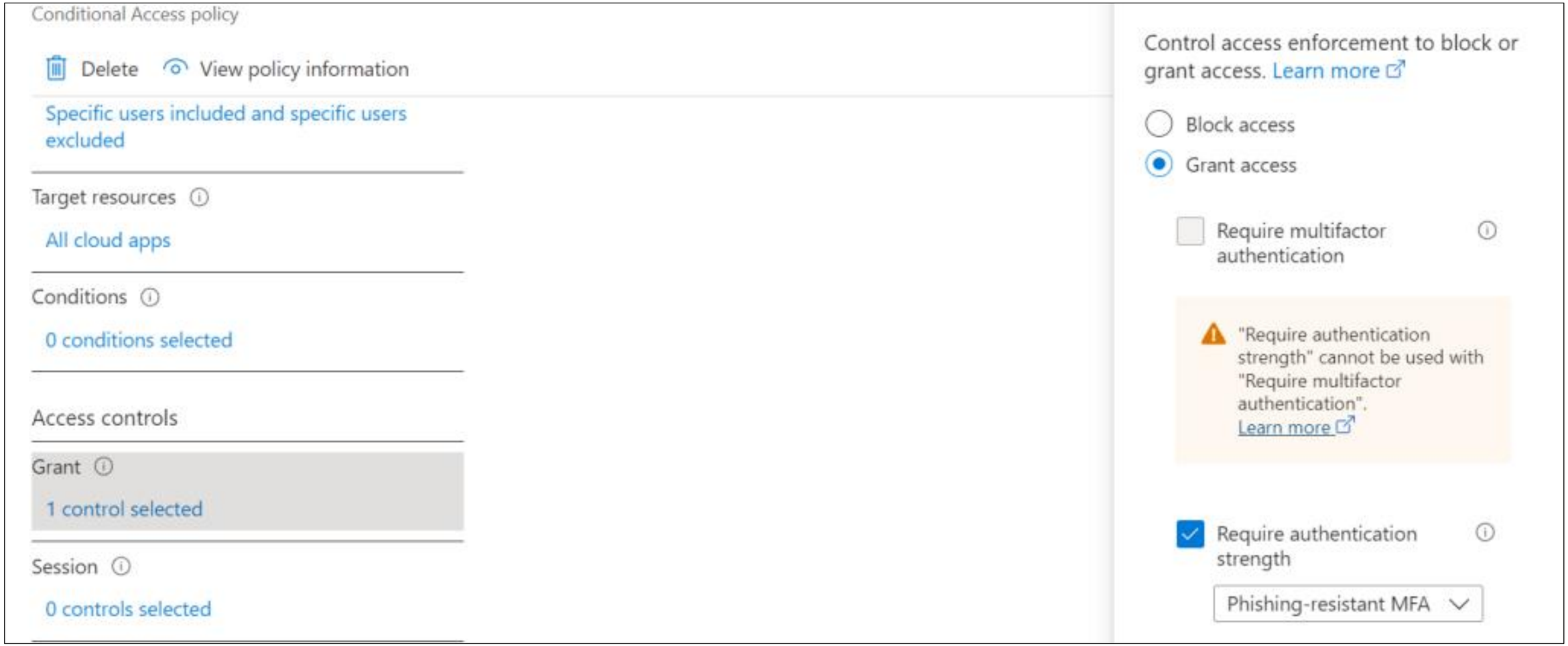
Introduction

- This phishlet is designed for the Evilginx framework, aiming to enhance phishing campaigns against Office 365 (O365) environments.
- It specifically targets the Windows Hello for Business authentication method, enabling an attacker to downgrade this secure authentication to more vulnerable, phishable methods.
- In addition, this phishlet incorporates JavaScript injection techniques to hide the sign-in option for Windows Hello for Business, among other functionalities, to increase the efficacy of phishing attacks.

Disclaimer: This tool is provided for educational purposes only. It is essential to use it ethically and legally. The developers and contributors are not responsible for misuse or for any damage that may be caused.

GRABX

What can I do?


Conditional Access policy
Delete
View policy information
Specific users included and specific users excluded
Target resources
All cloud apps
Conditions
0 conditions selected
Access controls
Grant
1 control selected
Session
0 controls selected
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
Phishing-resistant MFA

What can I do?

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

Name *

GRANT - MFA to register security information

Assignments

Users

Specific users included and specific users excluded

Target resources

1 user action included

Control access based on all or specific app internet resources, actions, or authenticati context. Learn more

Select what this policy applies to

User actions

Select the action this policy will apply to

- [x] Register security information
- [ ] Register or join devices

Grant

Control access enforcement to block or grant access. Learn more

- ( ) Block access
- (•) Grant access

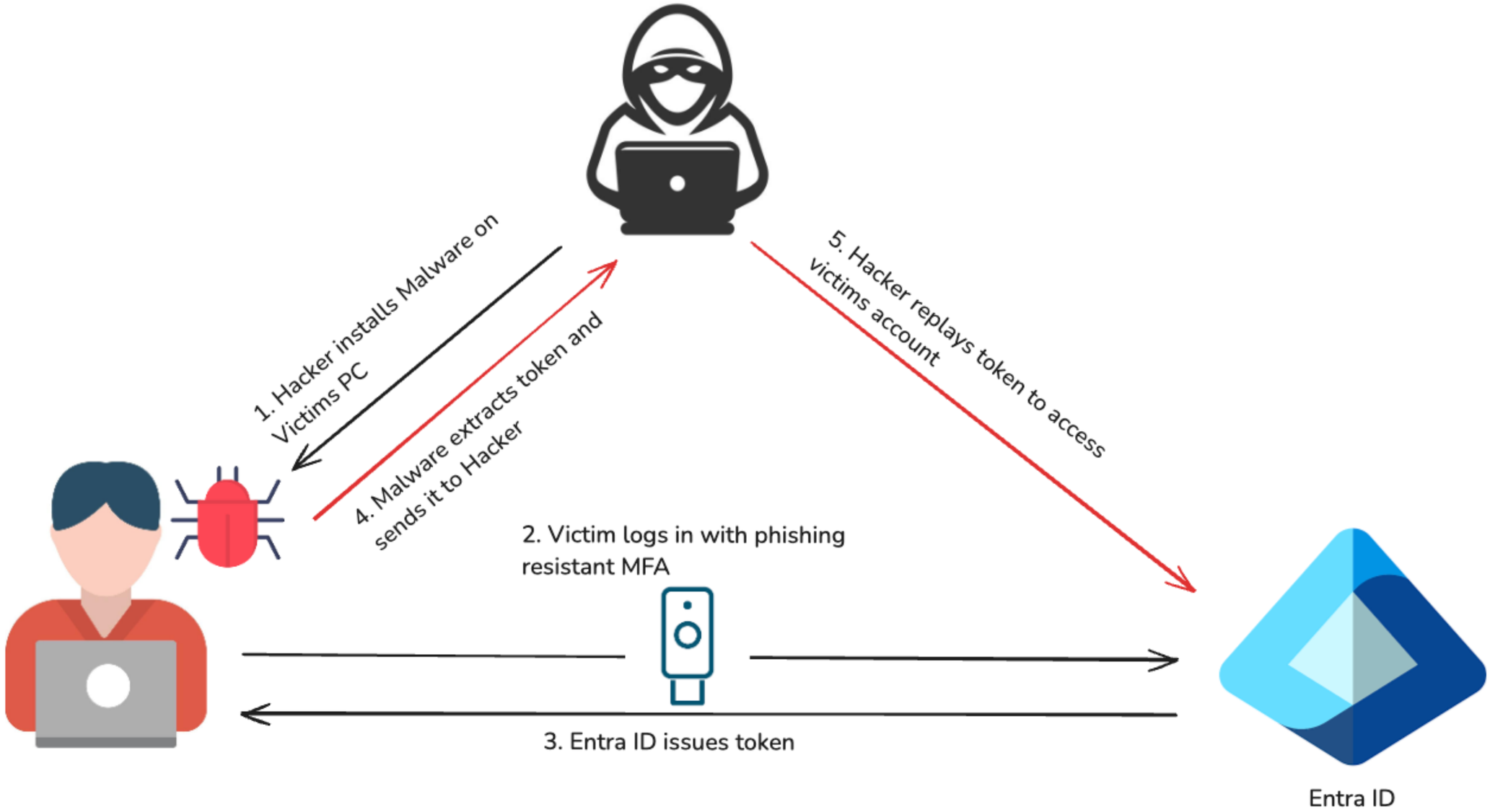
- [ ] Require multifactor authentication

"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

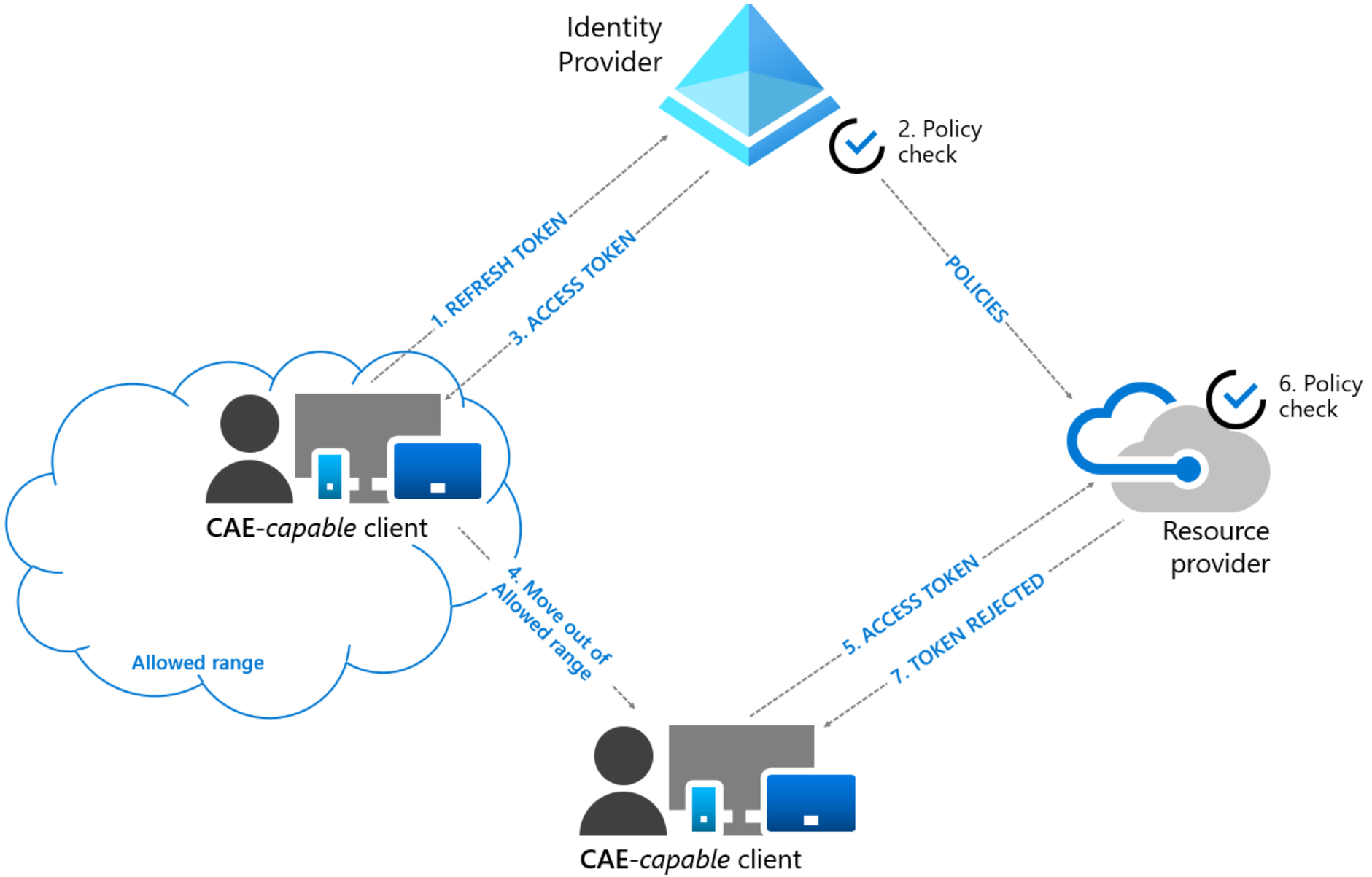
- [x] Require authentication strength

Multifactor authentic...

Token Theft by Malware

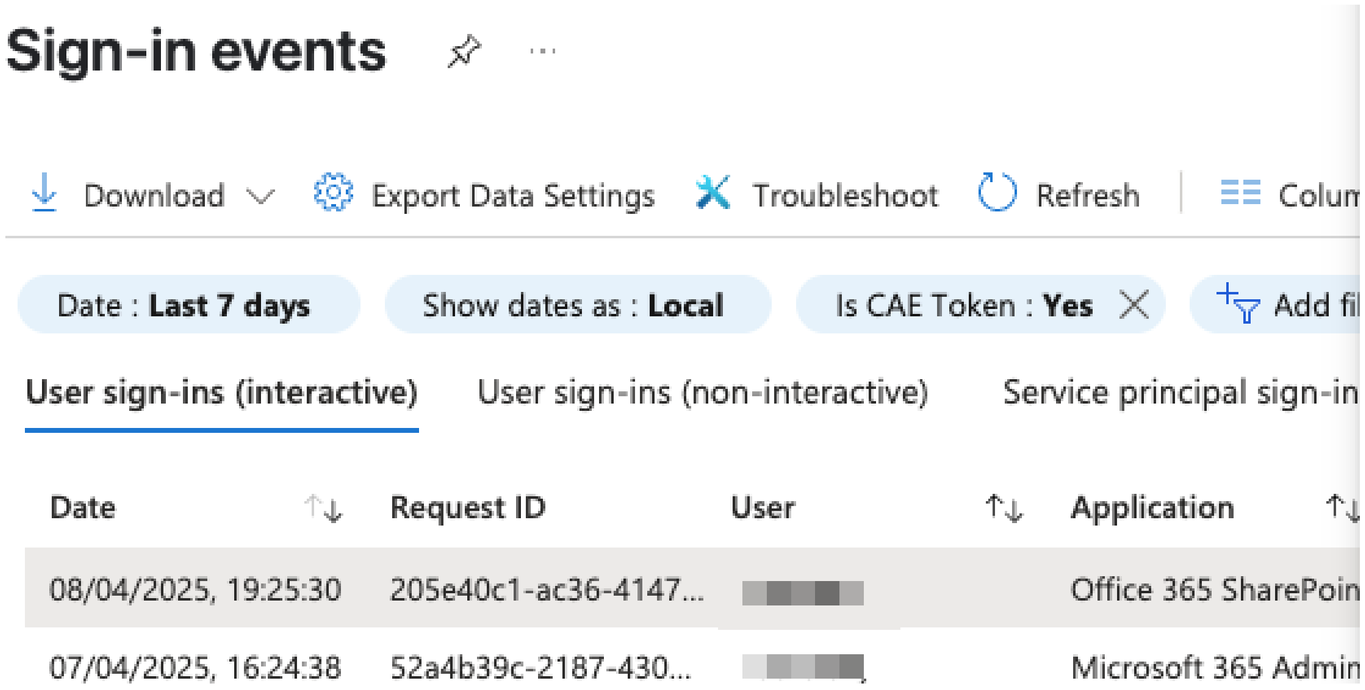


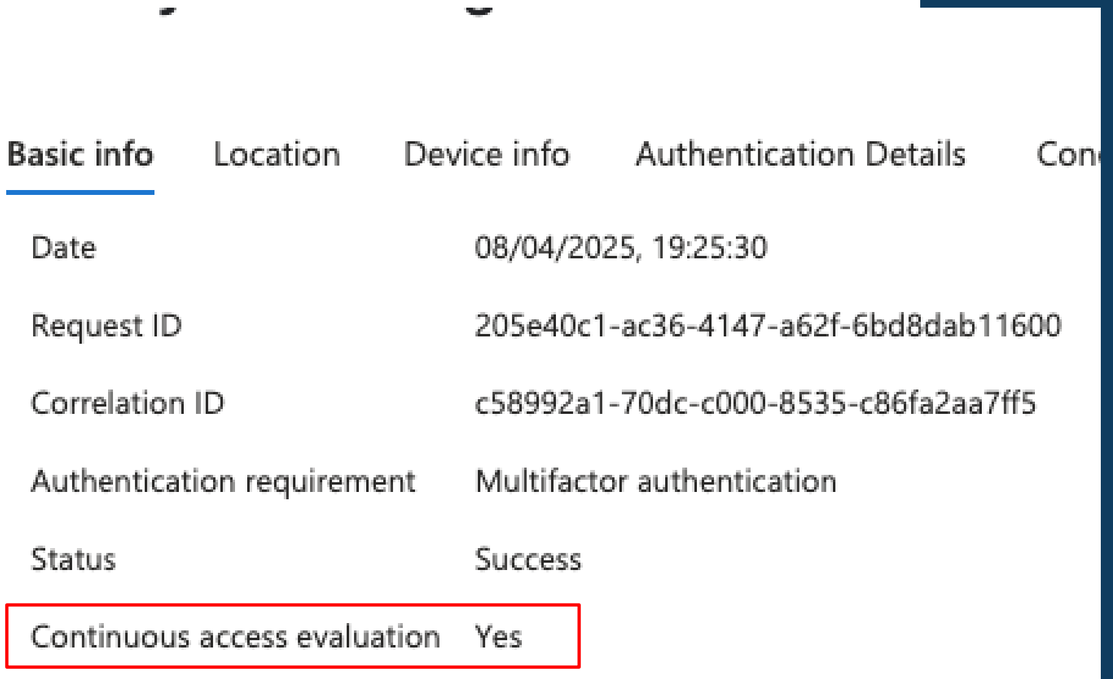
Continuous Access Evaluation




TOKENS
ENTRA ID
SECURITY
SECURITY
SECURITY
SECURITY

Continuous Access Evaluation





Continuous Access Evaluation

Assignments

Users ⓘ

0 users and groups selected

Target resources ⓘ

No target resources selected

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

☐ Use Conditional Access App Control ⓘ

☐ Sign-in frequency ⓘ

☐ Persistent browser session ⓘ

☑ Customize continuous access evaluation ⓘ

- ○ Disable
- ◉ Strictly enforce location policies (Preview) ⓘ

See list of supported clients and resource providers

☐ Disable resilience defaults ⓘ

Continuous Access Evaluation
Benefits / Downsides

- **Benefits**
  - Longer living Access Tokens (24h instead of 1h)
  - (Nearly) instant token revocation
- **Downsides**
  - Limited compatibility -> Application has to support it

	Outlook Web	Outlook Win32	Outlook iOS	Outlook Android	Outlook Mac
SharePoint Online	Supported	Supported	Supported	Supported	Supported
Exchange Online	Supported	Supported	Supported	Supported	Supported

Expand table

	Office web apps	Office Win32 apps	Office for iOS	Office for Android	Office for Mac
SharePoint Online	Not Supported *	Supported	Supported	Supported	Supported
Exchange Online	Not Supported	Supported	Supported	Supported	Supported

Expand table

	OneDrive web	OneDrive Win32	OneDrive iOS	OneDrive Android	OneDrive Mac
SharePoint Online	Supported	Not Supported	Supported	Supported	Not Supported

Expand table

	Teams web	Teams Win32	Teams iOS	Teams Android	Teams Mac
Teams Service	Partially supported	Partially supported	Partially supported	Partially supported	Partially supported
SharePoint Online	Partially supported	Partially supported	Partially supported	Partially supported	Partially supported
Exchange Online	Partially supported	Partially supported	Partially supported	Partially supported	Partially supported

Continuous Access Evaluation
Critical Events

- 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 is detected by Entra ID Protection

Entra ID Token Protection

- Cryptographically bind tokens to enrolled or registered devices
- Token can only be used by device that it was issued for
- Prevents Token Theft

GRABX

Entra ID Token Protection

Supported devices

- Windows 10 or newer devices that are Microsoft Entra joined, Microsoft Entra hybrid joined, or Microsoft Entra registered. See the known limitations section for unsupported device types.
- Windows Server 2019 or newer that are hybrid Microsoft Entra joined.

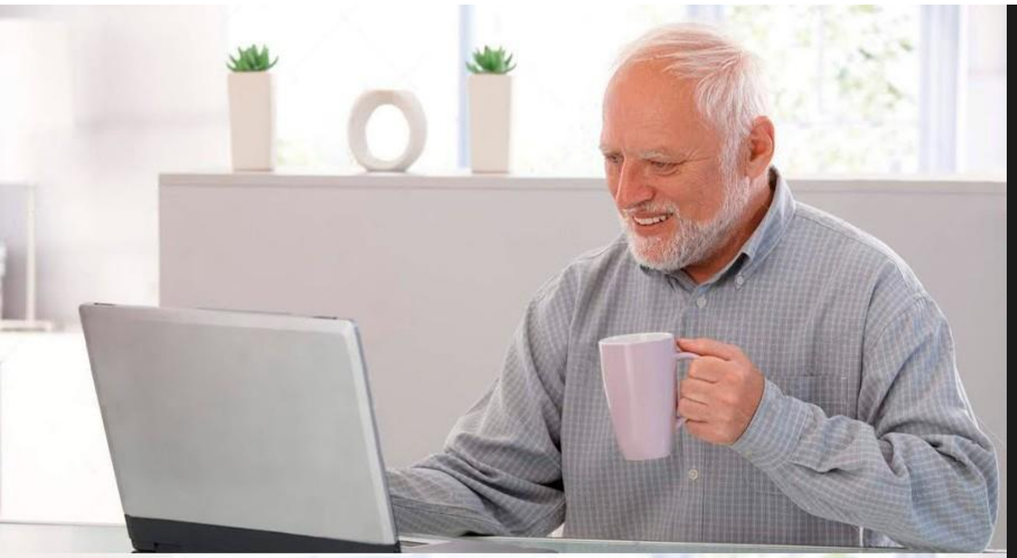
Supported applications

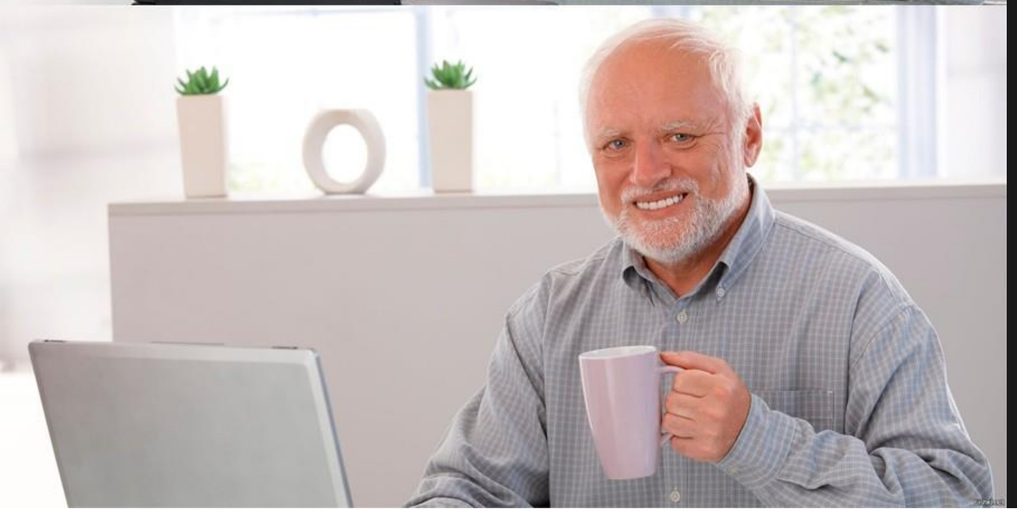
- OneDrive sync client version 22.217 or newer
- Teams native client version 1.6.00.1331 or newer
- Power BI desktop version 2.117.841.0 (May 2023) or newer
- Exchange PowerShell module version 3.7.0 or newer
- Microsoft Graph PowerShell version 2.0.0 or newer with EnableLoginByWAM option
- Visual Studio 2022 or newer when using the 'Windows authentication broker' Sign-in option
- Windows App version 2.0.379.0 or newer

The following resources support Token Protection:

- Office 365 Exchange Online
- Office 365 SharePoint Online
- Microsoft Teams Services
- Azure Virtual Desktop
- Windows 365

Entra ID Token Protection Limitations

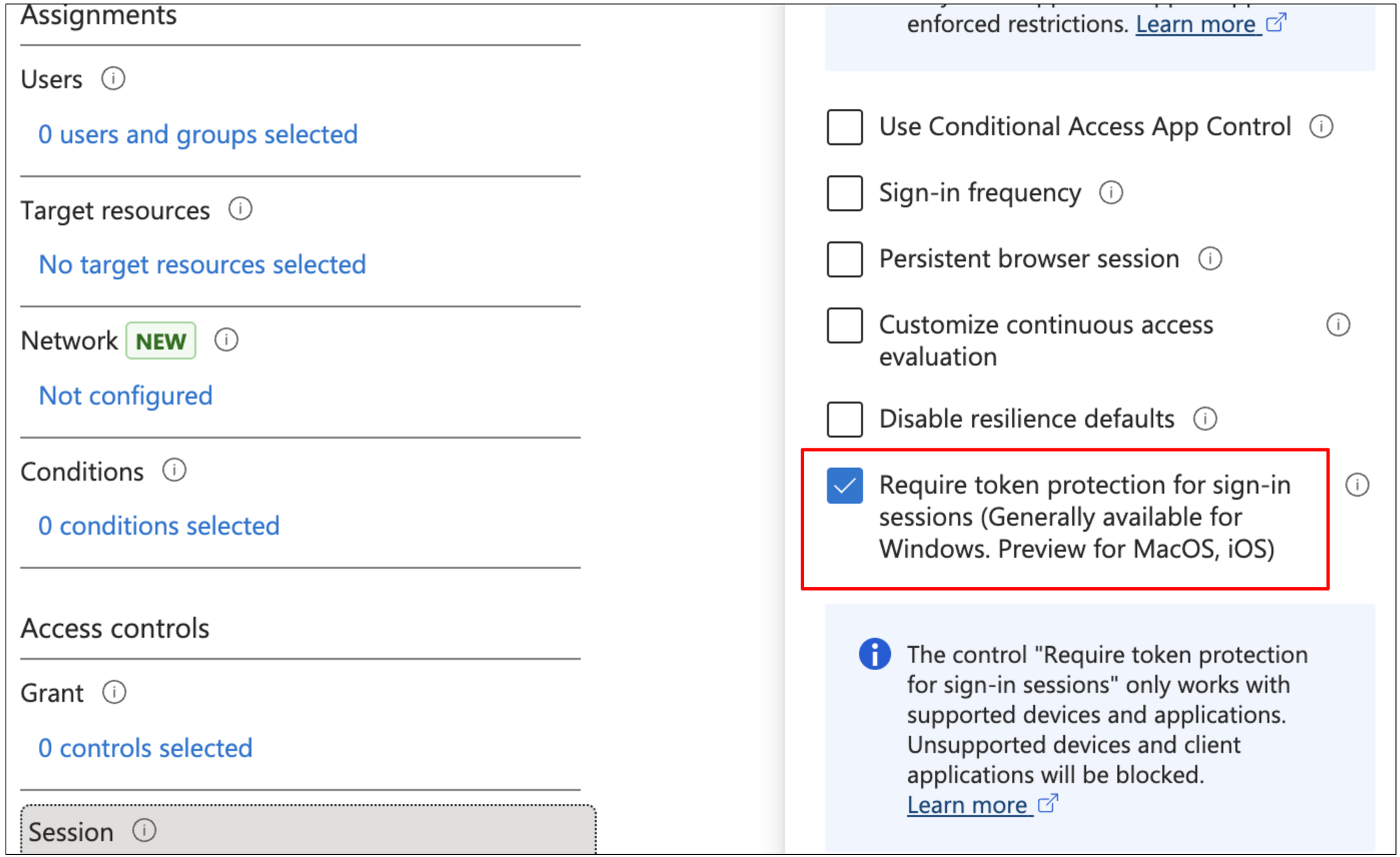




Known limitations

- Office perpetual clients aren't supported.
- The following applications don't support signing in using protected token flows and users are blocked when accessing Exchange and SharePoint:
  - PowerShell modules accessing SharePoint
  - PowerQuery extension for Excel
  - Extensions to Visual Studio Code which access Exchange or SharePoint
- The following Windows client devices aren't supported:
  - Surface Hub
  - Windows-based Microsoft Teams Rooms (MTR) systems
- External users who meet the token protection device registration requirements in their home tenant are supported. However, users who don't meet these requirements see an unclear error message with no indication of the root cause.
- Devices registered with Microsoft Entra ID using the following methods are unsupported:
  - Microsoft Entra joined Azure Virtual Desktop session hosts.
  - Windows devices deployed using bulk enrollment.
  - Cloud PCs deployed by Windows 365 that are Microsoft Entra joined.
  - Power Automate hosted machine groups that are Microsoft Entra joined.
  - Windows Autopilot devices deployed using self-deploying mode.
  - Windows virtual machines deployed in Azure using the virtual machine (VM) extension that are enabled for Microsoft Entra ID authentication.
- New Microsoft Entra registered devices on Windows versions before 24H2 might be blocked if users don't perform a fresh sign-in during registration. If blocked, users must re-register the device.

Entra ID Token Protection



Conclusion

- Some things are being automatically done for us
- We have to close the gaps that are still open
- Use FIDO2 Authentication
- Make sure no weak MFA can be used
- Create CA Policy to require MFA for security info registration
- Check if CAE is used -> if not, try to find out why
- Use Entra ID Token Protection where possible

Description	Link
FIDO2	https://fidoalliance.org/passkeys/
Entra Token Protection	https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection
Continuous Access Evaluation (CAE)	https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation
FOCI (Familiy Refresh Tokens) Research	https://github.com/secureworks/family-of-client-ids-research
Area41: Phishing The Resistant: Phishing For Primary Refresh Tokens In Microsoft Entra	https://www.youtube.com/watch?v=tNh_sYkmurI
DEFCON33: Turning Microsoft's Login Page into our Phishing Infrastructure	https://www.youtube.com/watch?v=z6GJqrkL0S0

Marco Schmidt
thesecurityguy.ch