Beyond Passwords; The Power and potential of Certificate Based Authentication

Oktay Sari

Thank you sponsors!

Gold

liquidware™

PINK

2Pint

PATCH MY PC

Technical Partners

CONSULTEQ

PROXSYS*

Daalmans consulting

Secure At Work

About “Oktay Sari”

Focus

Microsoft Intune and all things security

From

Netherlands

My Blog

https://allthingscloud.blog

Awards

MVP Microsoft® Most Valuable Professional

Hobbies

Hiking, woodworking, RC planes & heli

Contact

@oktay_sari

https://www.linkedin.com/in/oktaysari

Agenda

Key takeaways:

- Goal 1
- Goal 2

Certificate Based Authentication

Intro to Entra CBA, Overview, and Benefits

Configuration

Configuring CBA

Deepdive or just starting…

Use cases and Platform specific implementation

From the field

Limitations and Common Challenges

Next

What comes next and Questions

Certificate Based Authentication

Intro to Entra CBA, Overview, and Benefits

Introduction to CBA

Passwordless

Uses digital certificates instead of passwords for secure access

Use Cases

Ideal for remote work and secure access across iOS, Android, and Windows devices.

Key Bennefits

Provides a seamless, password-free experience, improves security, and meets compliance requirements

Microsoft Entra Integration

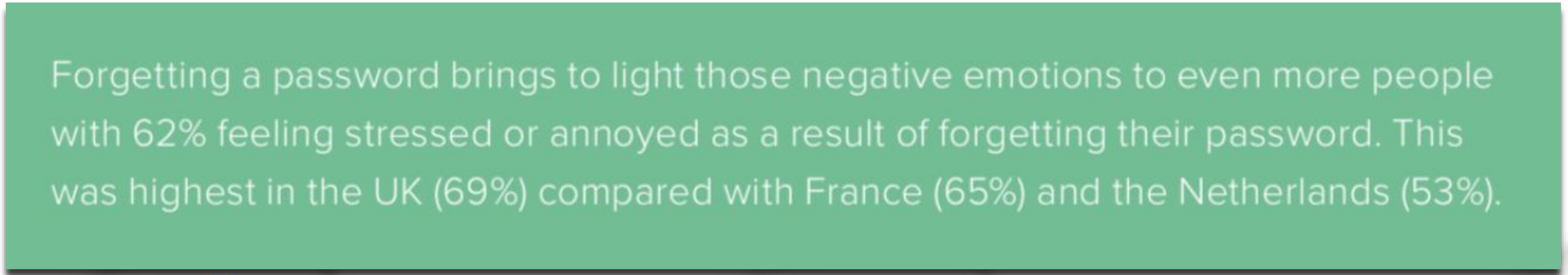
Enables easy deployment and management of CBA

Go for the best!

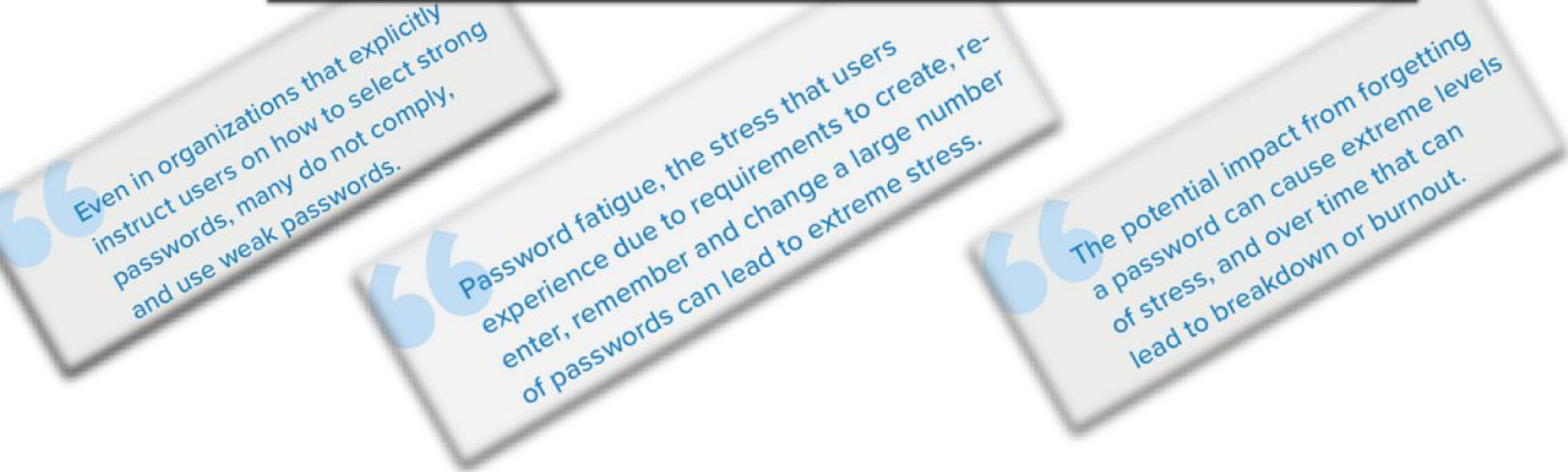
Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
qwerty			Window Hello
password		Software Tokens OTP	FIDO2 security key
iloveyou	Voice		
Password1		Hardware Tokens OTP (Preview)	Certificates

Passkeys !!

(other..) Password Facts…



Forgetting a password brings to light those negative emotions to even more people with 62% feeling stressed or annoyed as a result of forgetting their password. This was highest in the UK (69%) compared with France (65%) and the Netherlands (53%).



> Even in organizations that explicitly instruct users on how to select strong passwords, many do not comply, and use weak passwords.

> Password fatigue, the stress that users experience due to requirements to create, re-enter, remember and change a large number of passwords can lead to extreme stress.

> The potential impact from forgetting a password can cause extreme levels of stress, and over time that can lead to breakdown or burnout.

Source: https://www.okta.com/uk/resources/whitepaper-passwordless-future/

Password Facts…

Configuring CBA - Prerequisites

- A PKI environment
- Configure at least one certificate authority (CA) and any intermediate CAs in Microsoft Entra ID.
- User certificates are issued from the PKI.
- An internet accessible Certificate Revocation List (CRL) for each CA.

4 steps to configuring CBA

Configure the certificate authorities with PKI-based trust store (Preview)

Enable CBA on the tenant

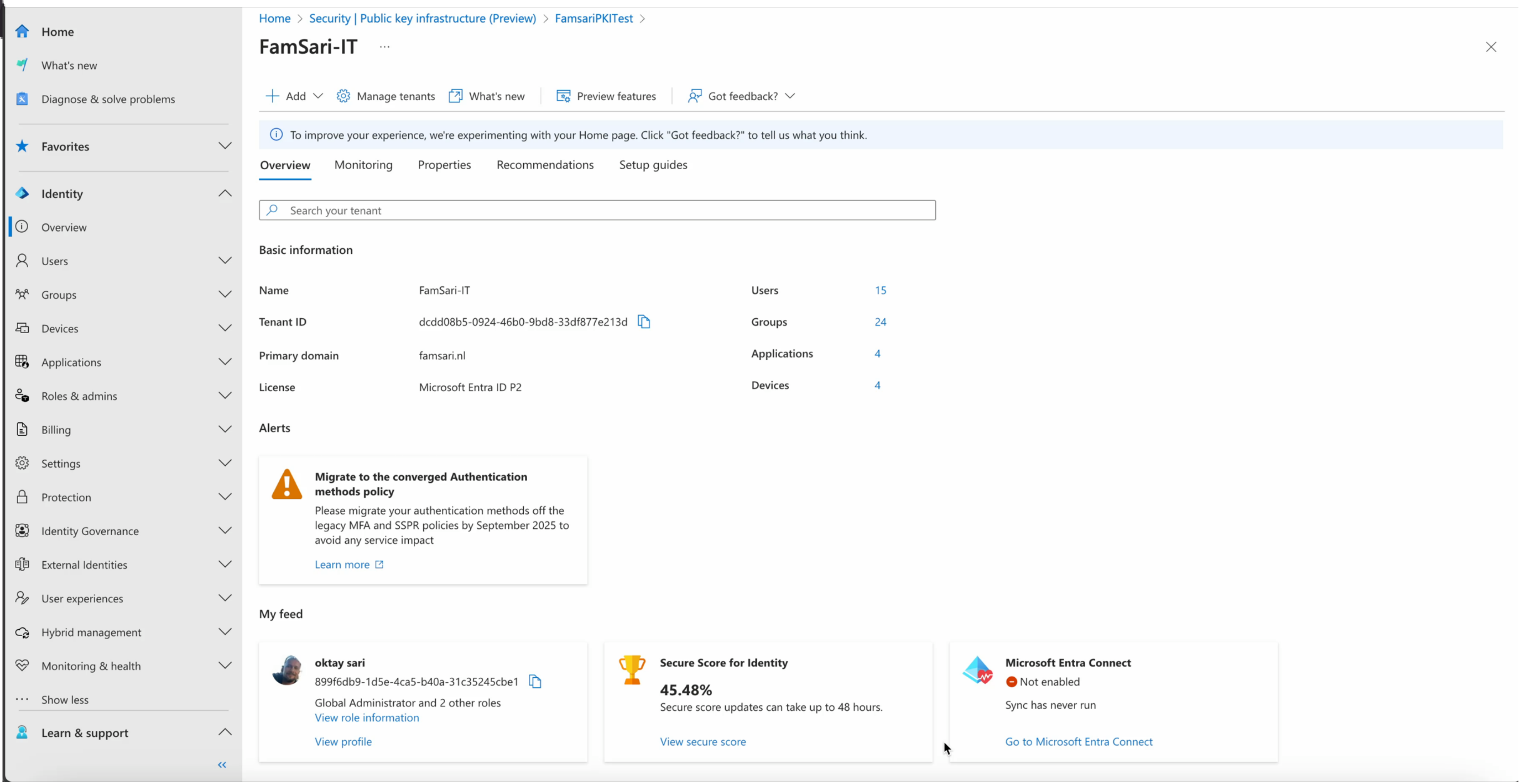
Configure authentication binding policy

Configure username binding policy

Demo

Let’s configure CBA

Demo: Configuring CBA



Home > Security | Public key infrastructure (Preview) > FamsariPKITest >

FamSari-IT

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Basic information

Name	FamSari-IT	Users	15
Tenant ID	dcdd08b5-0924-46b0-9bd8-33df877e213d	Groups	24
Primary domain	famsari.nl	Applications	4
License	Microsoft Entra ID P2	Devices	4

Alerts

Migrate to the converged Authentication methods policy

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact

Learn more

My feed

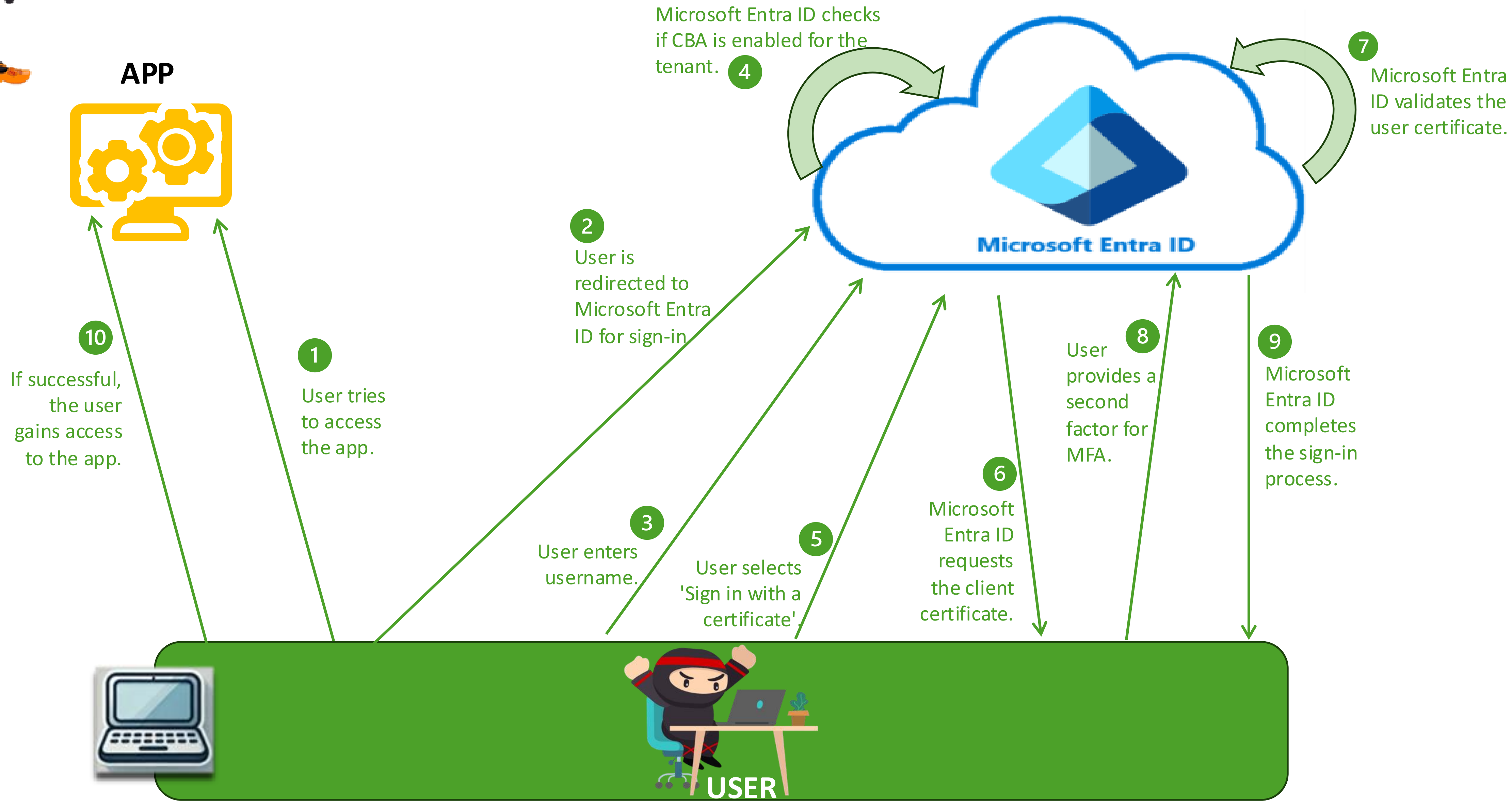
oktay sari
899f6db9-1d5e-4ca5-b40a-31c35245cbe1
Global Administrator and 2 other roles
View role information
View profile

Secure Score for Identity
45.48%
Secure score updates can take up to 48 hours.
View secure score

Microsoft Entra Connect
Not enabled
Sync has never run
Go to Microsoft Entra Connect

Going R… Technical Deep-dive or just starting?

How Microsoft CBA works



APP

Microsoft Entra ID

USER

1 User tries to access the app.

2 User is redirected to Microsoft Entra ID for sign-in.

3 User enters username.

4 Microsoft Entra ID checks if CBA is enabled for the tenant.

5 User selects 'Sign in with a certificate'.

6 Microsoft Entra ID requests the client certificate.

7 Microsoft Entra ID validates the user certificate.

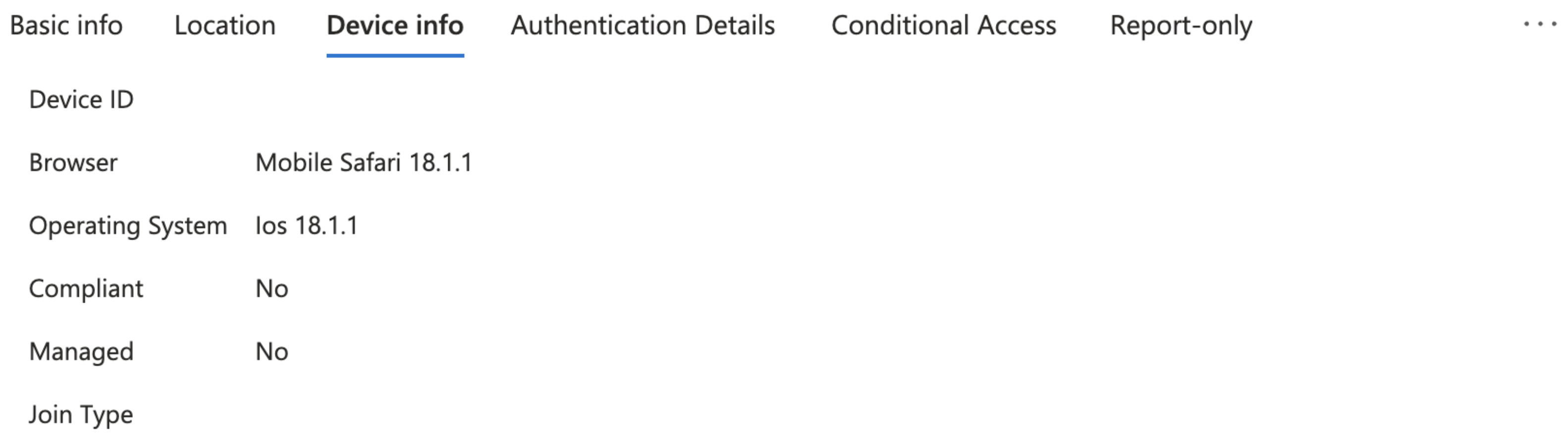
8 User provides a second factor for MFA.

9 Microsoft Entra ID completes the sign-in process.

10 If successful, the user gains access to the app.

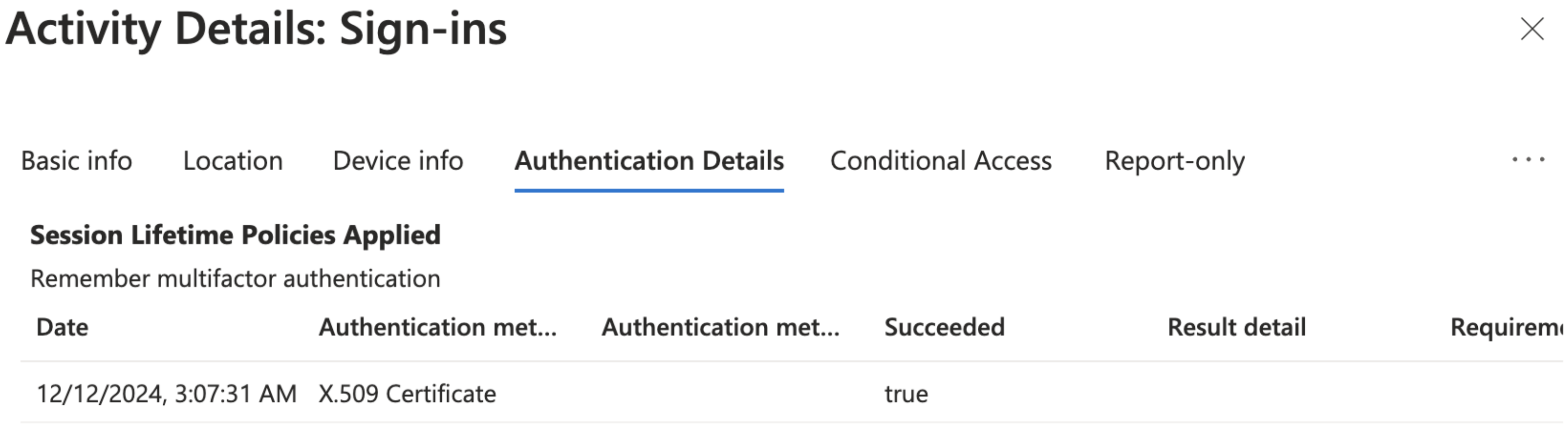
User Experience: iOS

Sign-in logs



Basic info | Location | **Device info** | Authentication Details | Conditional Access | Report-only | ...

Device ID	
Browser	Mobile Safari 18.1.1
Operating System	Ios 18.1.1
Compliant	No
Managed	No
Join Type	



Activity Details: Sign-ins

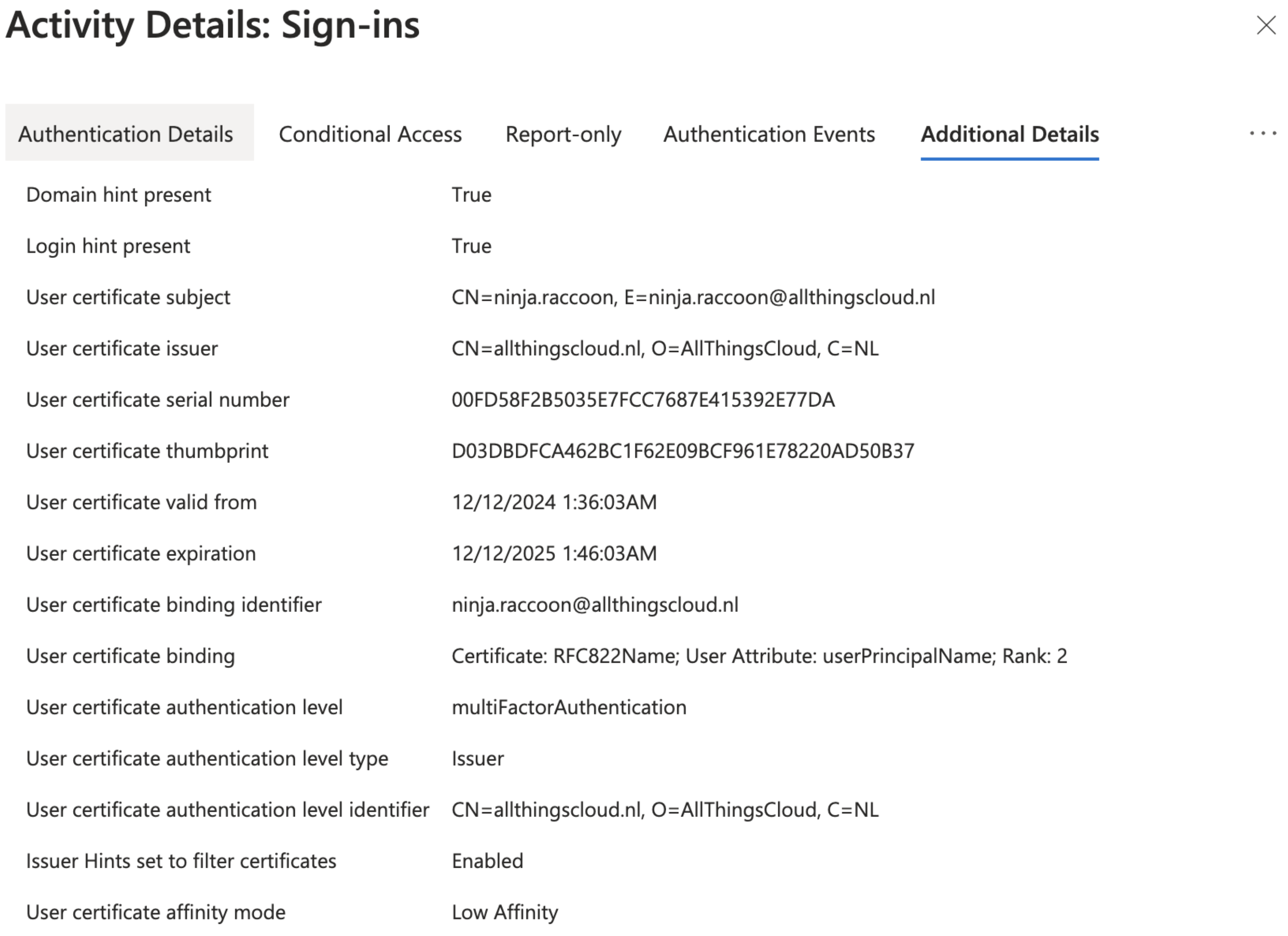
Basic info | Location | Device info | **Authentication Details** | Conditional Access | Report-only | ...

Session Lifetime Policies Applied

Remember multifactor authentication

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requirem
12/12/2024, 3:07:31 AM	X.509 Certificate		true		

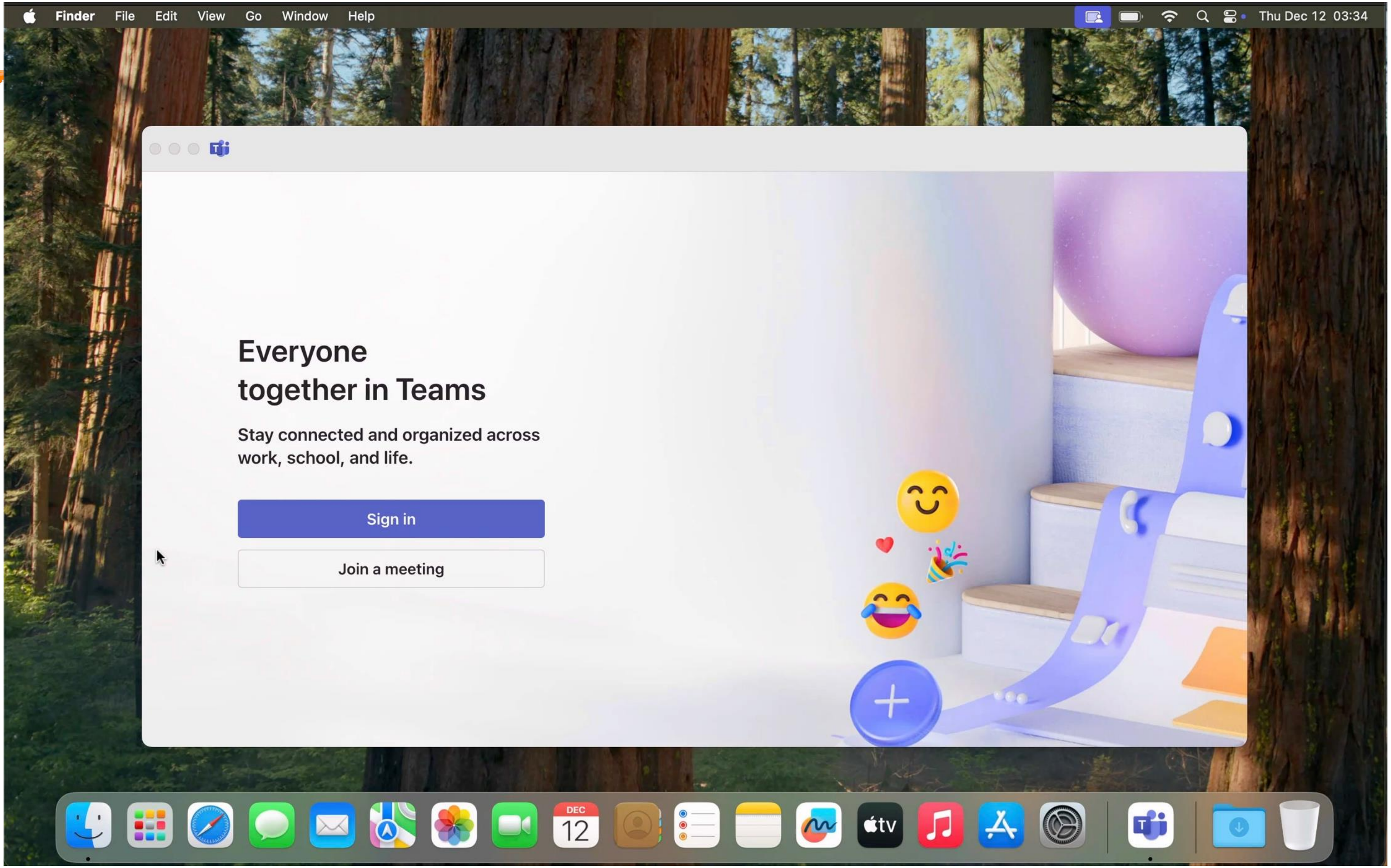
Sign-in logs



Activity Details: Sign-ins

Domain hint present	True
Login hint present	True
User certificate subject	CN=ninja.raccoon, E=ninja.raccoon@allthingscloud.nl
User certificate issuer	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
User certificate serial number	00FD58F2B5035E7FCC7687E415392E77DA
User certificate thumbprint	D03DBDFCA462BC1F62E09BCF961E78220AD50B37
User certificate valid from	12/12/2024 1:36:03AM
User certificate expiration	12/12/2025 1:46:03AM
User certificate binding identifier	ninja.raccoon@allthingscloud.nl
User certificate binding	Certificate: RFC822Name; User Attribute: userPrincipalName; Rank: 2
User certificate authentication level	multiFactorAuthentication
User certificate authentication level type	Issuer
User certificate authentication level identifier	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
Issuer Hints set to filter certificates	Enabled
User certificate affinity mode	Low Affinity

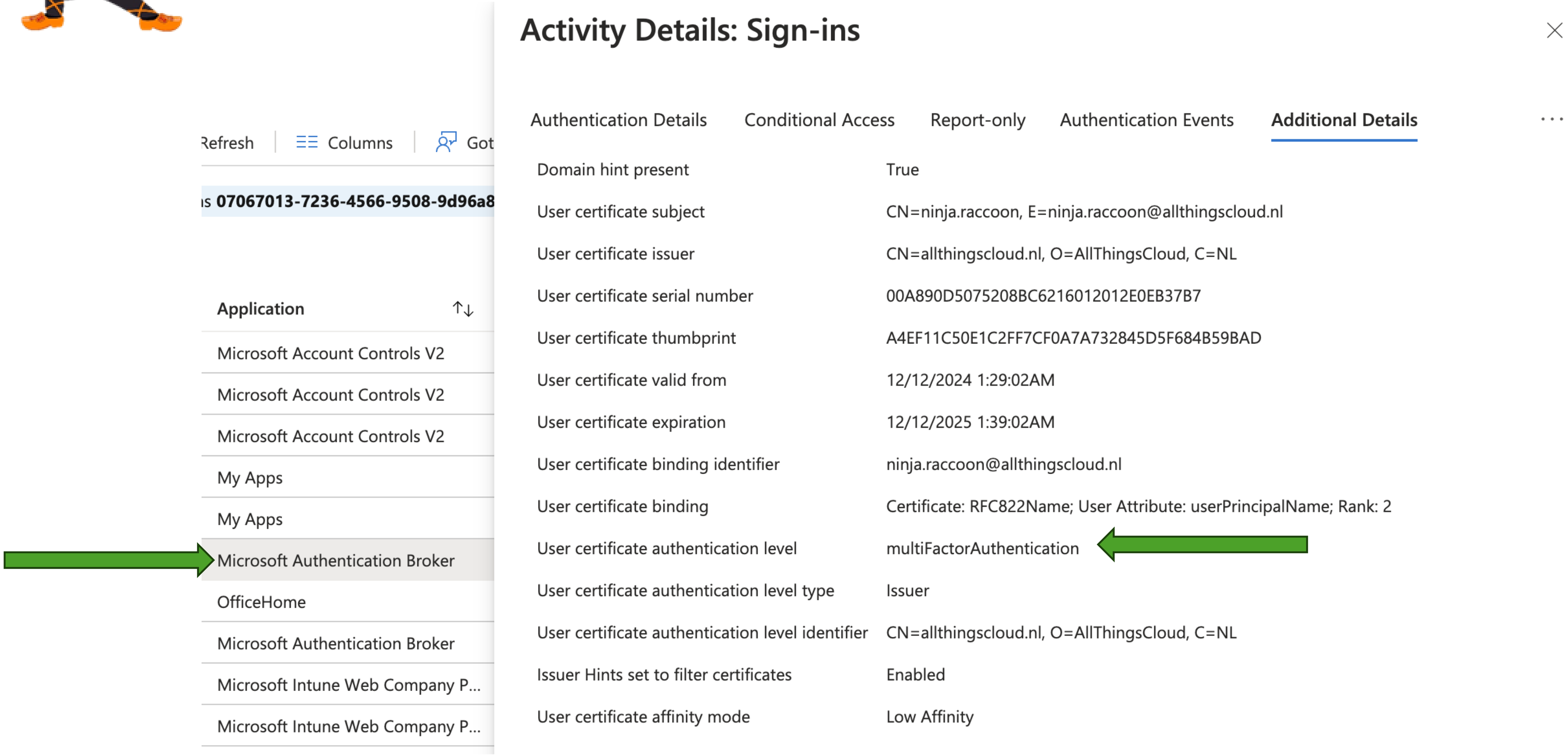
User Experience: macOS



Everyone together in Teams

Stay connected and organized across work, school, and life.

Sign-in logs: PSSO registration



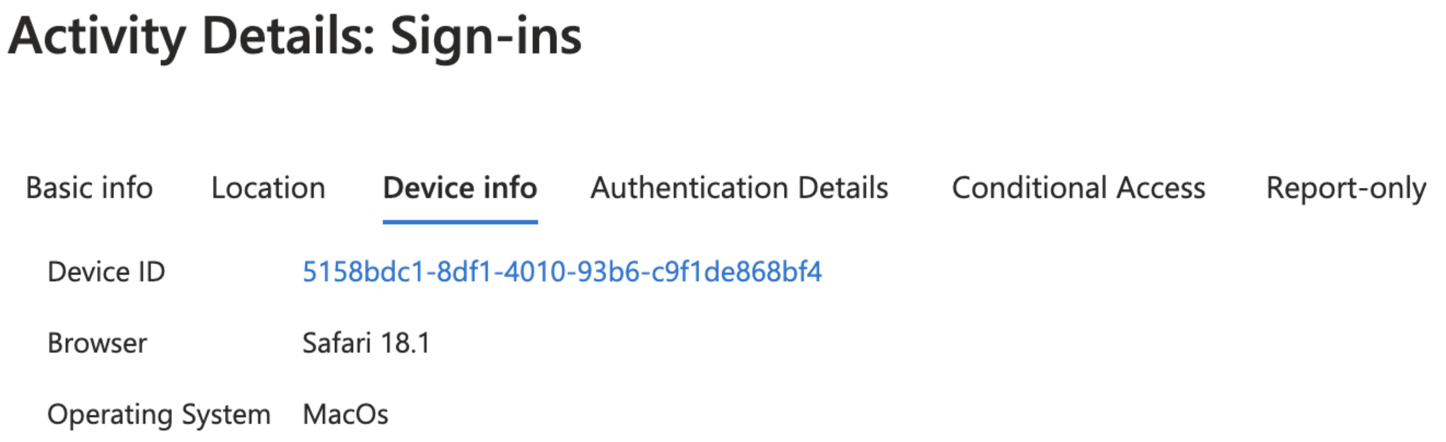
ıs 07067013-7236-4566-9508-9d96a8

Application
Microsoft Account Controls V2
Microsoft Account Controls V2
Microsoft Account Controls V2
My Apps
My Apps
Microsoft Authentication Broker
OfficeHome
Microsoft Authentication Broker
Microsoft Intune Web Company P...
Microsoft Intune Web Company P...

Activity Details: Sign-ins

Domain hint present	True
User certificate subject	CN=ninja.raccoon, E=ninja.raccoon@allthingscloud.nl
User certificate issuer	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
User certificate serial number	00A890D5075208BC6216012012E0EB37B7
User certificate thumbprint	A4EF11C50E1C2FF7CF0A7A732845D5F684B59BAD
User certificate valid from	12/12/2024 1:29:02AM
User certificate expiration	12/12/2025 1:39:02AM
User certificate binding identifier	ninja.raccoon@allthingscloud.nl
User certificate binding	Certificate: RFC822Name; User Attribute: userPrincipalName; Rank: 2
User certificate authentication level	multiFactorAuthentication
User certificate authentication level type	Issuer
User certificate authentication level identifier	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
Issuer Hints set to filter certificates	Enabled
User certificate affinity mode	Low Affinity

Sign-in logs: myapps with Safari

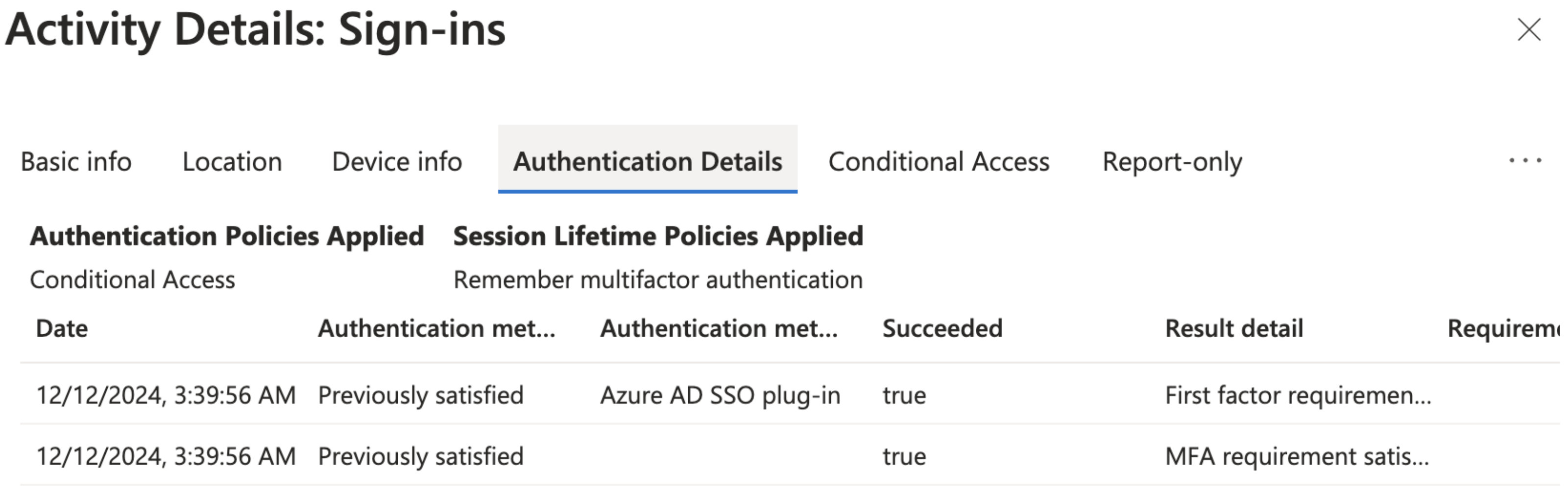


Activity Details: Sign-ins

Device ID 5158bdc1-8df1-4010-93b6-c9f1de868bf4

Browser Safari 18.1

Operating System MacOs

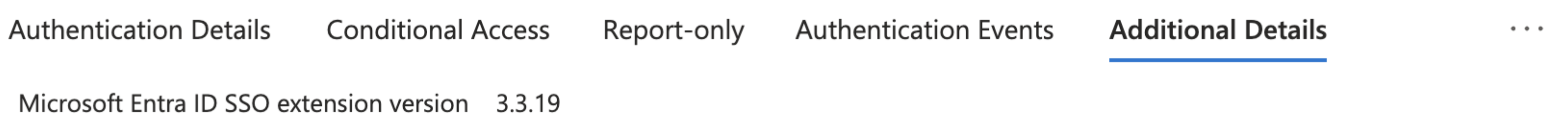


Activity Details: Sign-ins

Authentication Policies Applied
Conditional Access

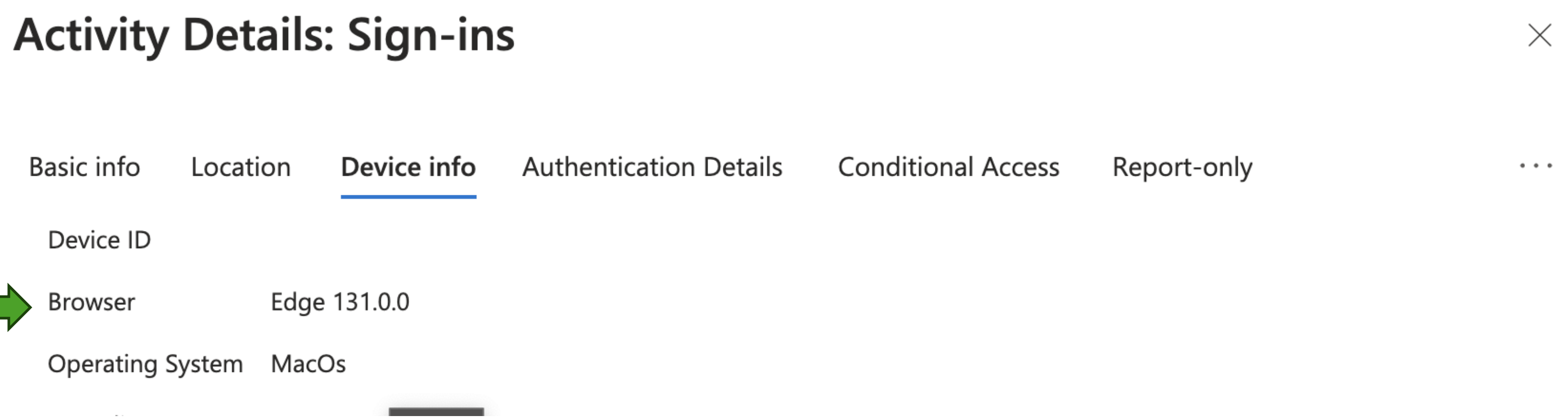
Session Lifetime Policies Applied
Remember multifactor authentication

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requirem
12/12/2024, 3:39:56 AM	Previously satisfied	Azure AD SSO plug-in	true	First factor requiremen...	
12/12/2024, 3:39:56 AM	Previously satisfied		true	MFA requirement satis...	



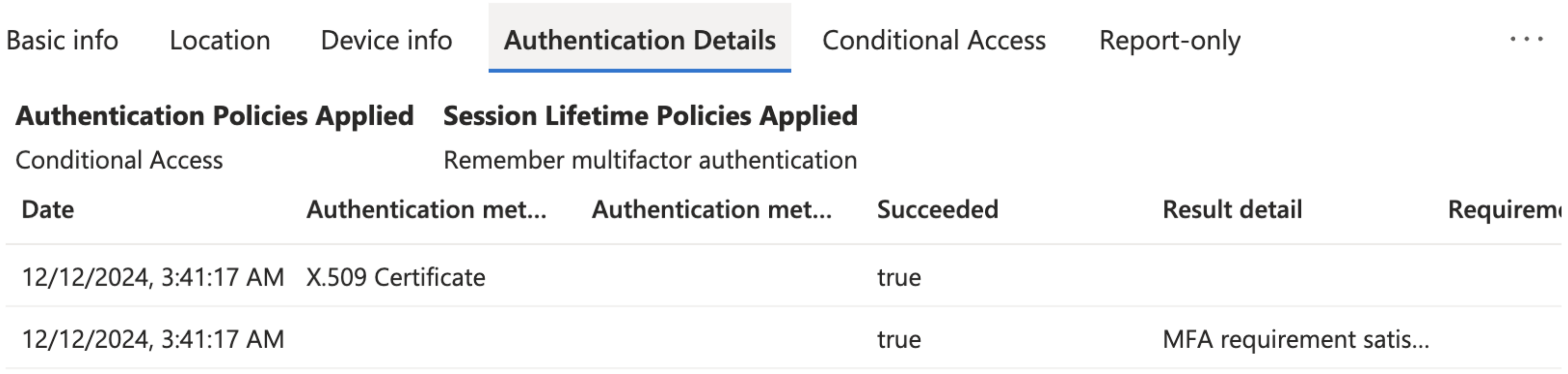
Microsoft Entra ID SSO extension version 3.3.19

Sign-in logs: myapps with Edge



Activity Details: Sign-ins

Device ID	
Browser	Edge 131.0.0
Operating System	MacOs

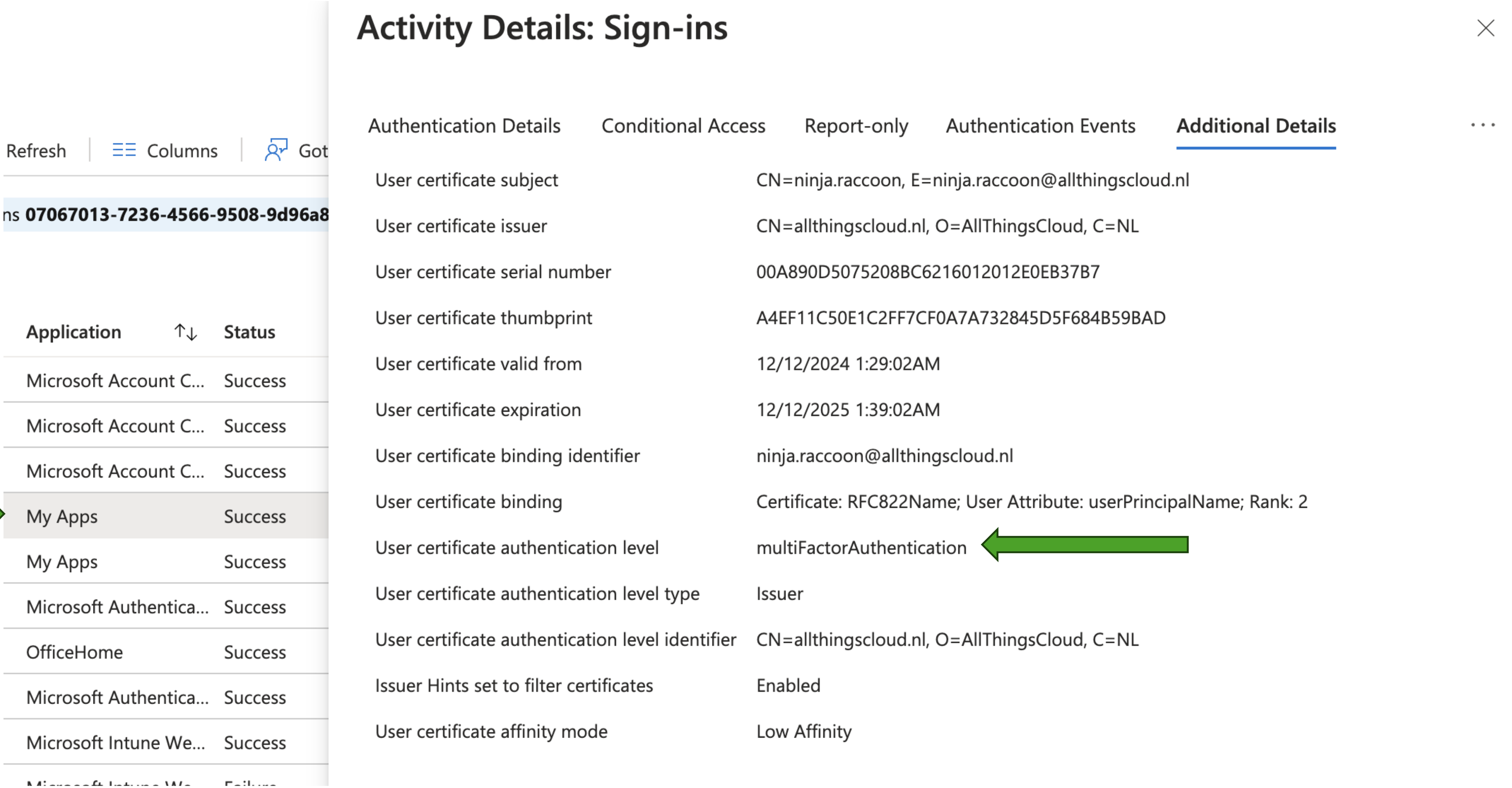


Authentication Policies Applied
Conditional Access

Session Lifetime Policies Applied
Remember multifactor authentication

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requireme
12/12/2024, 3:41:17 AM	X.509 Certificate		true		
12/12/2024, 3:41:17 AM			true	MFA requirement satis...	

Sign-in logs: myapps with Edge



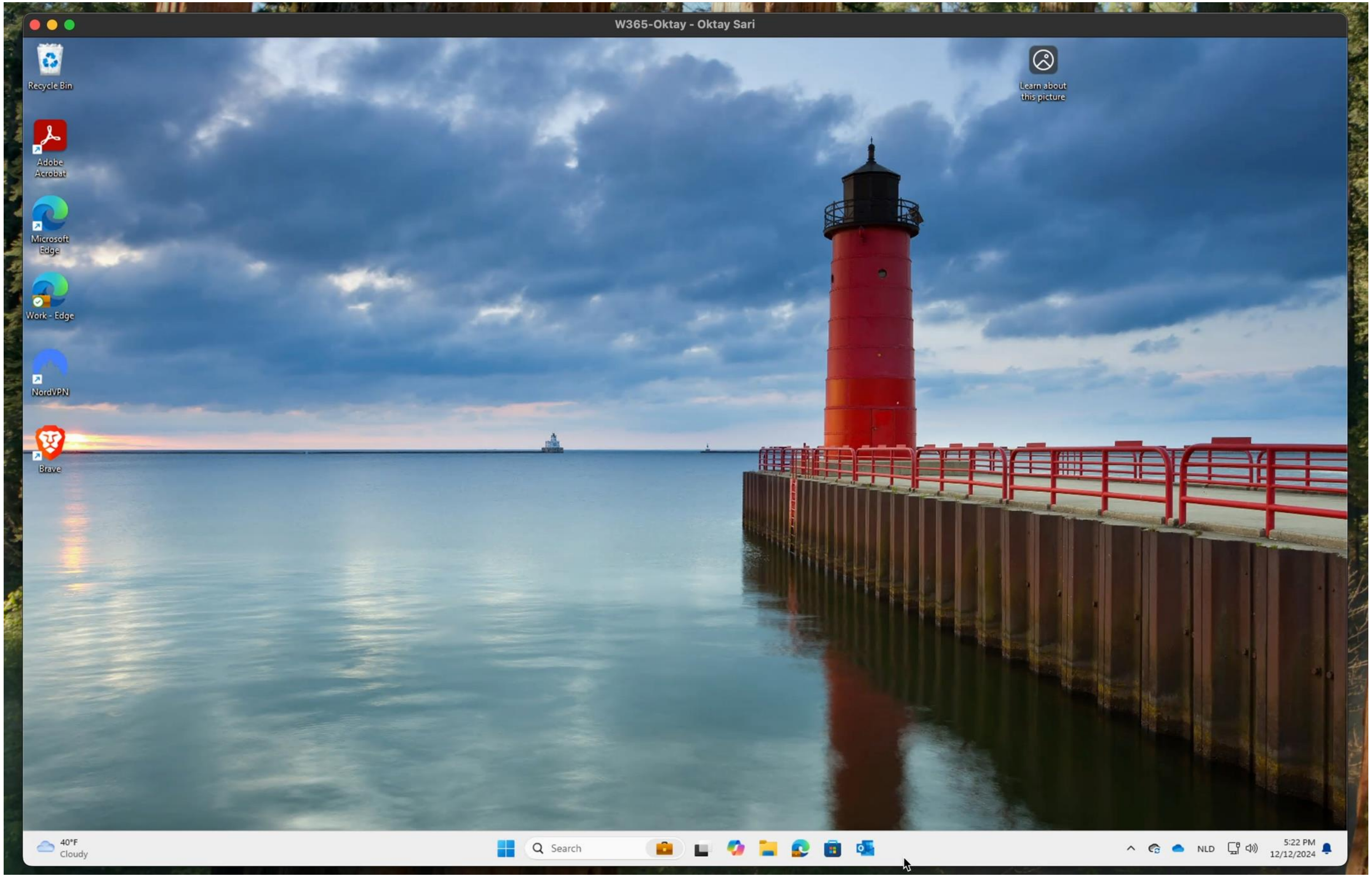
ns **07067013-7236-4566-9508-9d96a8**

Application	Status
Microsoft Account C...	Success
Microsoft Account C...	Success
Microsoft Account C...	Success
My Apps	Success
My Apps	Success
Microsoft Authentica...	Success
OfficeHome	Success
Microsoft Authentica...	Success
Microsoft Intune We...	Success
Microsoft Intune We...	Failure

Activity Details: Sign-ins

User certificate subject	CN=ninja.raccoon, E=ninja.raccoon@allthingscloud.nl
User certificate issuer	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
User certificate serial number	00A890D5075208BC6216012012E0EB37B7
User certificate thumbprint	A4EF11C50E1C2FF7CF0A7A732845D5F684B59BAD
User certificate valid from	12/12/2024 1:29:02AM
User certificate expiration	12/12/2025 1:39:02AM
User certificate binding identifier	ninja.raccoon@allthingscloud.nl
User certificate binding	Certificate: RFC822Name; User Attribute: userPrincipalName; Rank: 2
User certificate authentication level	multiFactorAuthentication
User certificate authentication level type	Issuer
User certificate authentication level identifier	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
Issuer Hints set to filter certificates	Enabled
User certificate affinity mode	Low Affinity

User Experience: Windows



From the field

- Microsoft Entra CBA is a free feature. Play with it in a test tenant
- Other licensing requirements might be in place (Cloud PKI, MFA, M365, Intune)
- Password as an authentication method can't be disabled
- You need to setup a PKI for creating client certificates.
- Sign-in to device is only supported on Windows (using smartcard/fido)
- If CBA is enabled on the tenant, all users see the link to Use a certificate or smart card on the password page.
- Play with Conditional Access and Authentication strength.
- Play with certificates on FIDO2 keys (PIV capable=smartcard)

What’s next: Windows Smartcard login

Thank You

Happy holidays
&
have a great 2025!