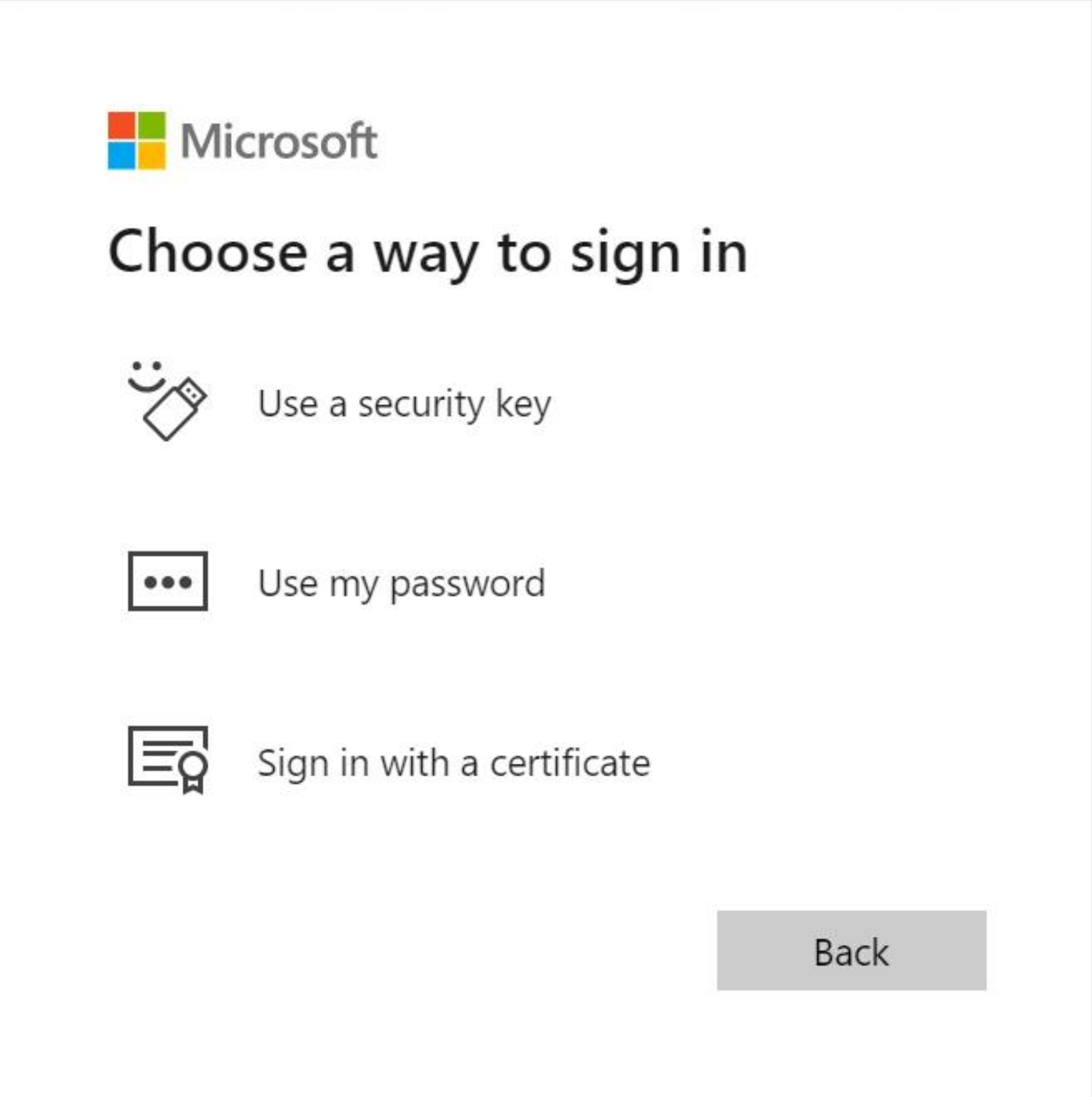
Azure AD native Cert Based Auth

Stefan van der Wiele
Senior Product Manager
@wiele

Identity & Network Access Division



Choose a way to sign in

Use a security key

Use my password

Sign in with a certificate

Who uses CBA today?

- Smartcard / certificate authentication required

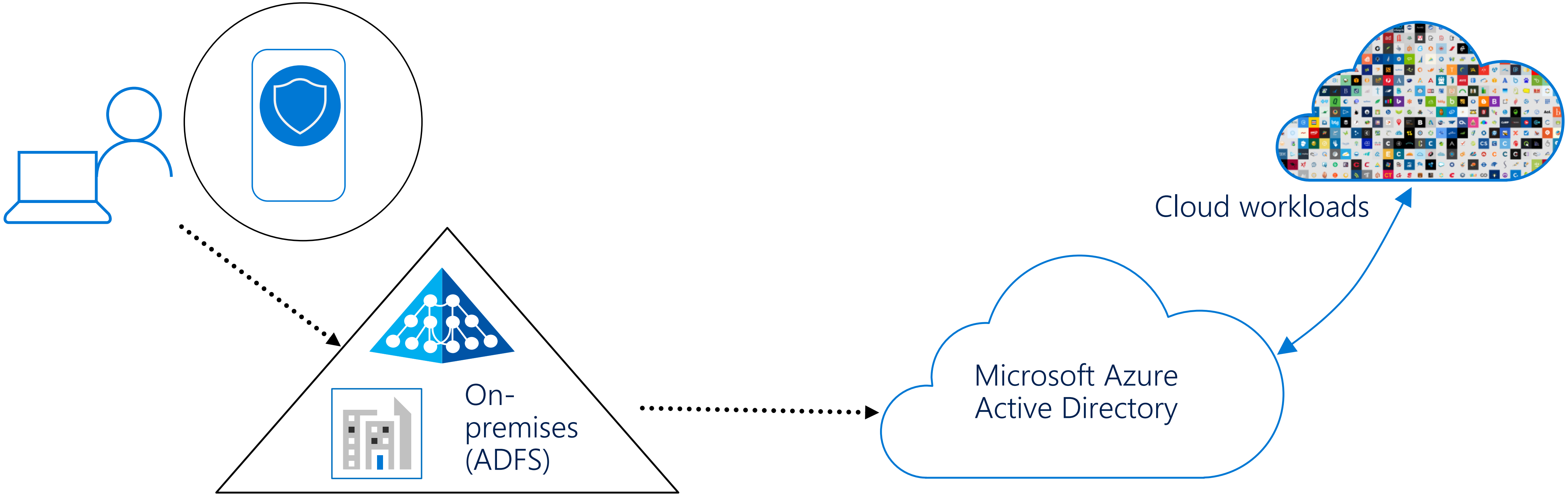
- SSO scenarios on mobile devices

- 3rd party MDM scenarios

Other scenarios?

Azure AD Certificate Based Authentication

Today CBA / SmartCard (CAC/PIV) authentication for Azure AD requires federated ADFS



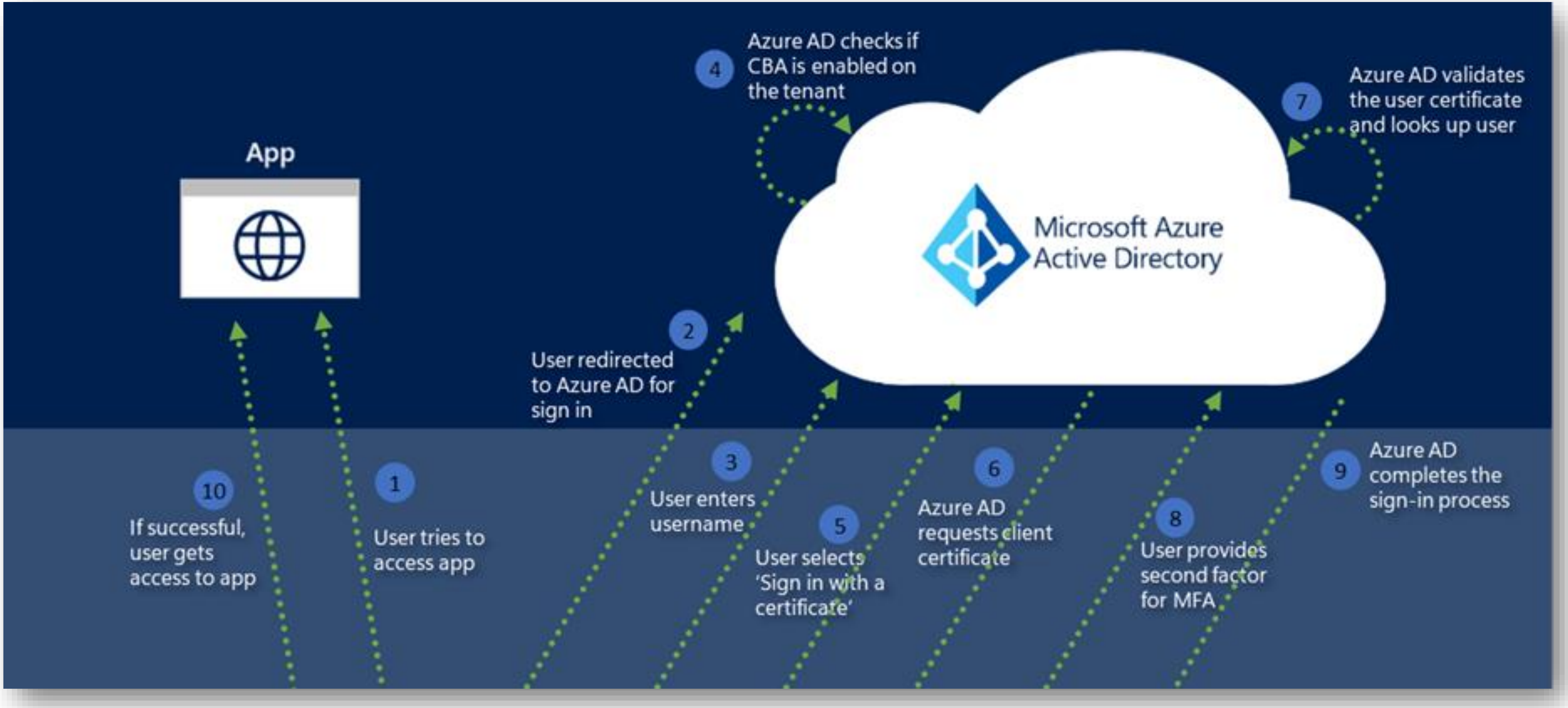
How is cloud native CBA helping?

Unblock new & existing customers with CBA requirements

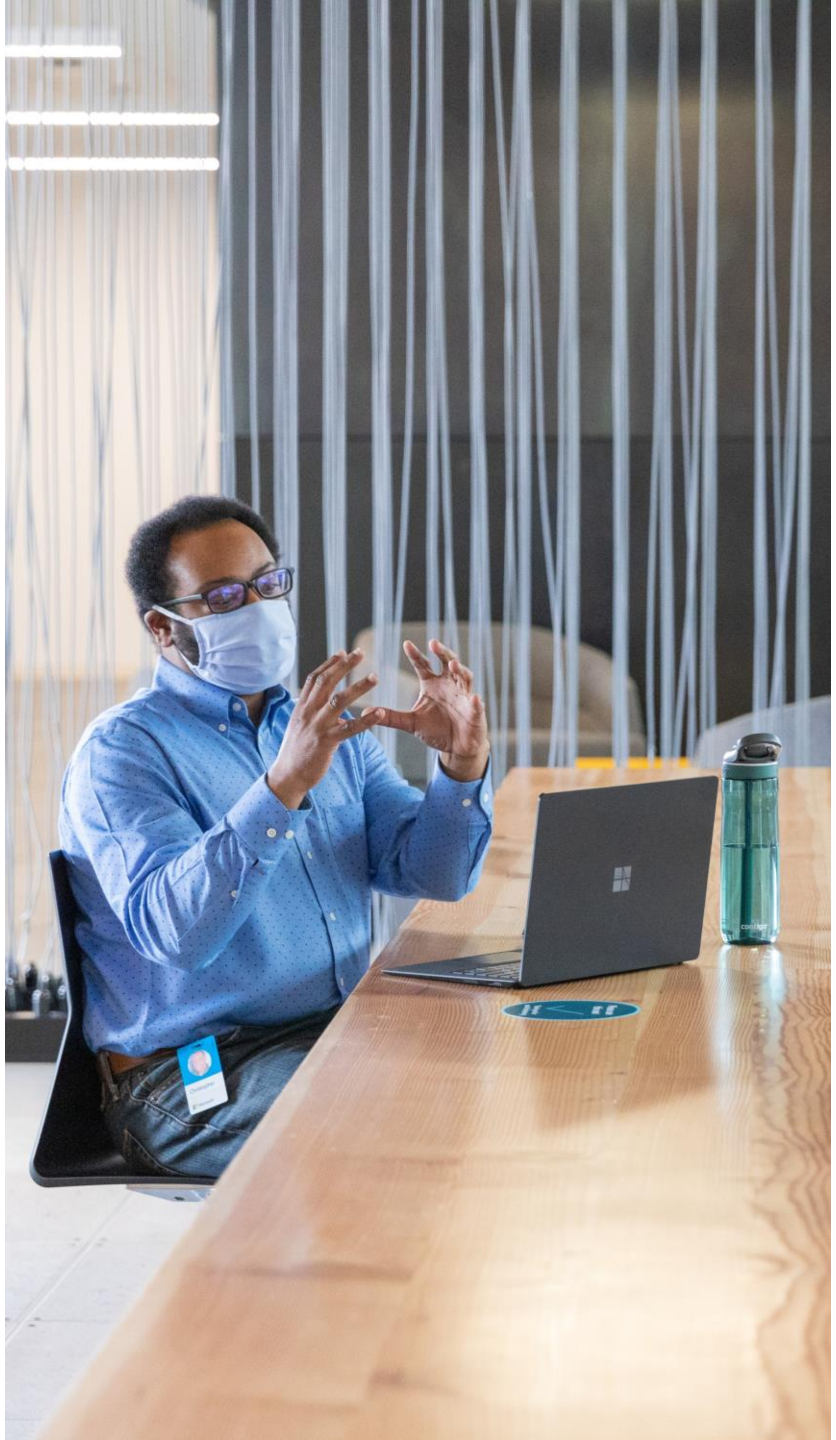
Reduce cost and on prem footprint for customers

Extending Azure AD to support CBA for all accounts

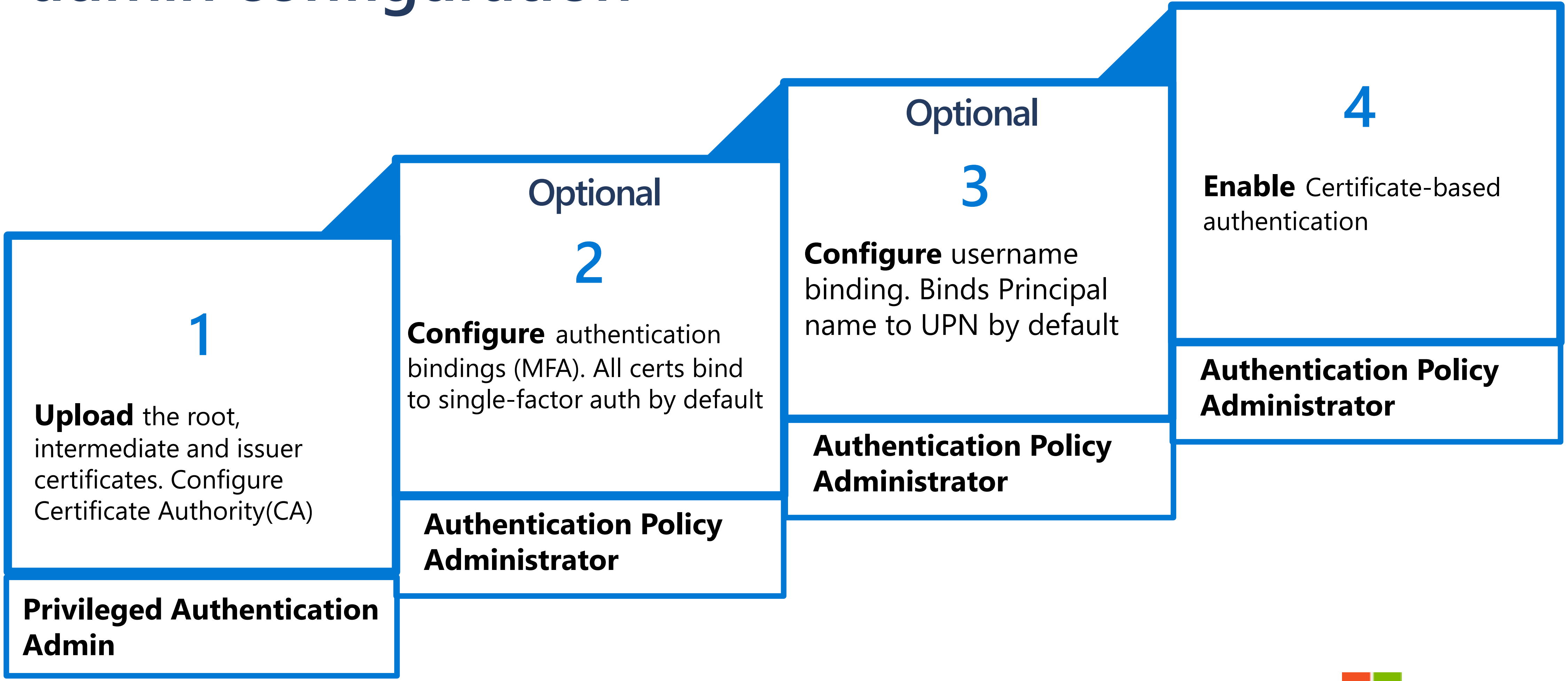
How does Azure AD CBA work?


App
Microsoft Azure Active Directory
1 User tries to access app
2 User redirected to Azure AD for sign in
3 User enters username
4 Azure AD checks if CBA is enabled on the tenant
5 User selects 'Sign in with a certificate'
6 Azure AD requests client certificate
7 Azure AD validates the user certificate and looks up user
8 User provides second factor for MFA
9 Azure AD completes the sign-in process
10 If successful, user gets access to app

How to configure CBA in Azure AD?



IT admin configuration



1

Upload the root, intermediate and issuer certificates. Configure Certificate Authority(CA)

Privileged Authentication Admin

Optional

2

Configure authentication bindings (MFA). All certs bind to single-factor auth by default

Authentication Policy Administrator

Optional

3

Configure username binding. Binds Principal name to UPN by default

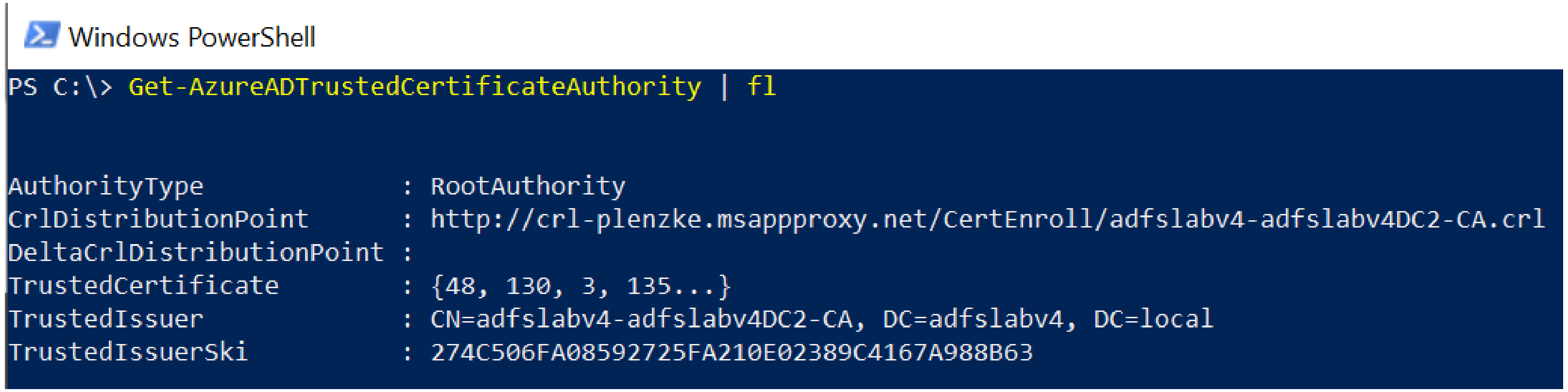
Authentication Policy Administrator

4

Enable Certificate-based authentication

Authentication Policy Administrator

Configure trusted CAs via PowerShell



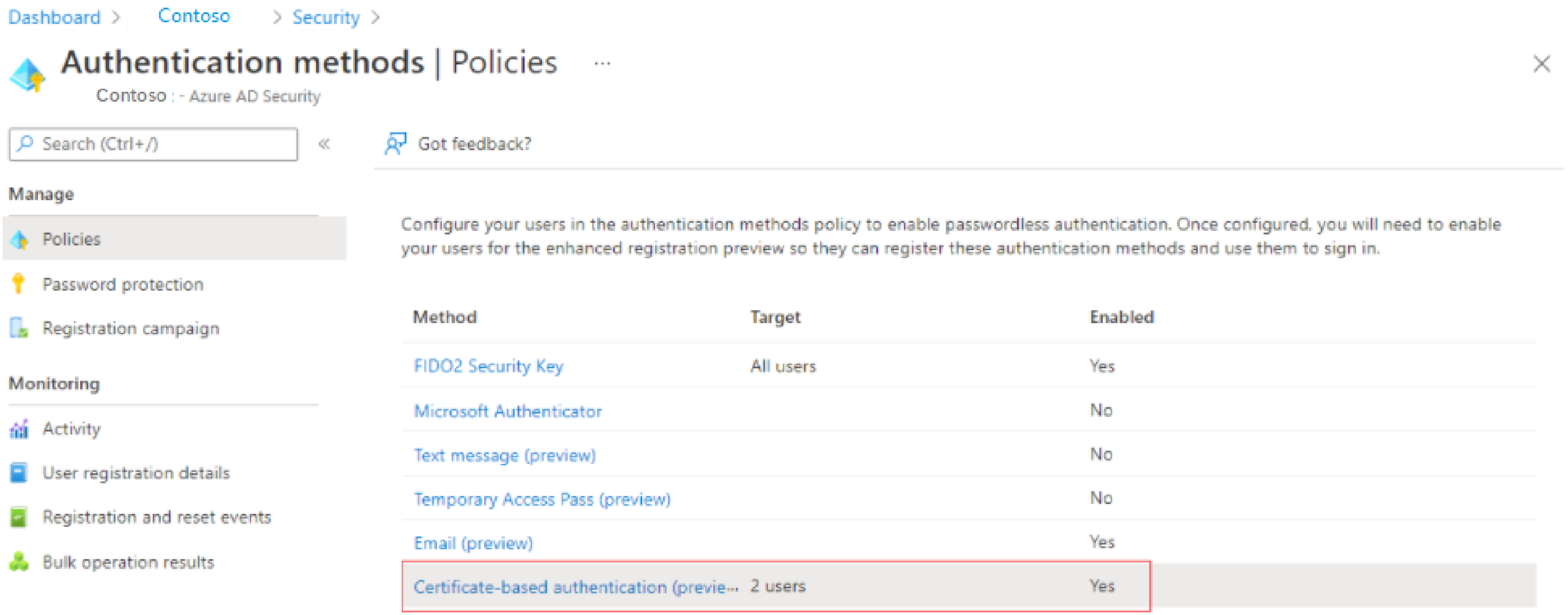
```
PS C:\> Get-AzureADTrustedCertificateAuthority | fl


AuthorityType             : RootAuthority
CrlDistributionPoint      : http://crl-plenzke.msappproxy.net/CertEnroll/adfslabv4-adfslabv4DC2-CA.crl
DeltaCrlDistributionPoint :
TrustedCertificate        : {48, 130, 3, 135...}
TrustedIssuer             : CN=adfslabv4-adfslabv4DC2-CA, DC=adfslabv4, DC=local
TrustedIssuerSki          : 274C506FA08592725FA210E02389C4167A988B63
```

Important

The maximum size of a CRL for Azure Active Directory to successfully download and cache, and the time required to download the CRL are limited. If Azure Active Directory can't download a CRL, the authentication will fail.

Maximum number of CA added to Azure AD is limited to ~50

Authentication Methods Policy



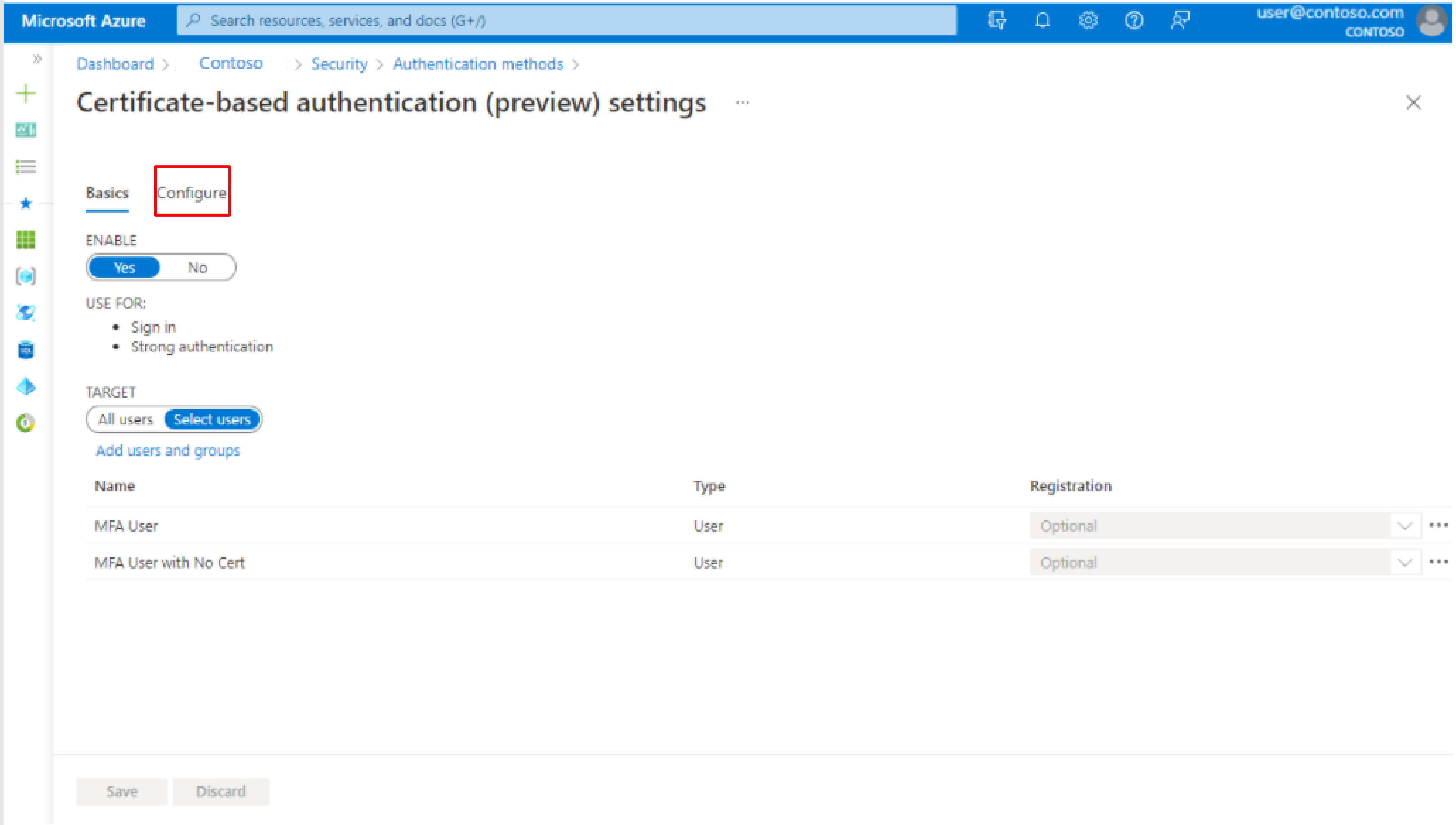
Authentication methods | Policies

Contoso : - Azure AD Security

Configure your users in the authentication methods policy to enable passwordless authentication. Once configured, you will need to enable your users for the enhanced registration preview so they can register these authentication methods and use them to sign in.

Method	Target	Enabled
FIDO2 Security Key	All users	Yes
Microsoft Authenticator		No
Text message (preview)		No
Temporary Access Pass (preview)		No
Email (preview)		Yes
Certificate-based authentication (previe...	2 users	Yes

Configure Authentication Policy



Microsoft Azure
Search resources, services, and docs (G+/)
user@contoso.com
CONTOSO
Dashboard > Contoso > Security > Authentication methods >

Certificate-based authentication (preview) settings

ENABLE

Yes [✓] No

USE FOR:

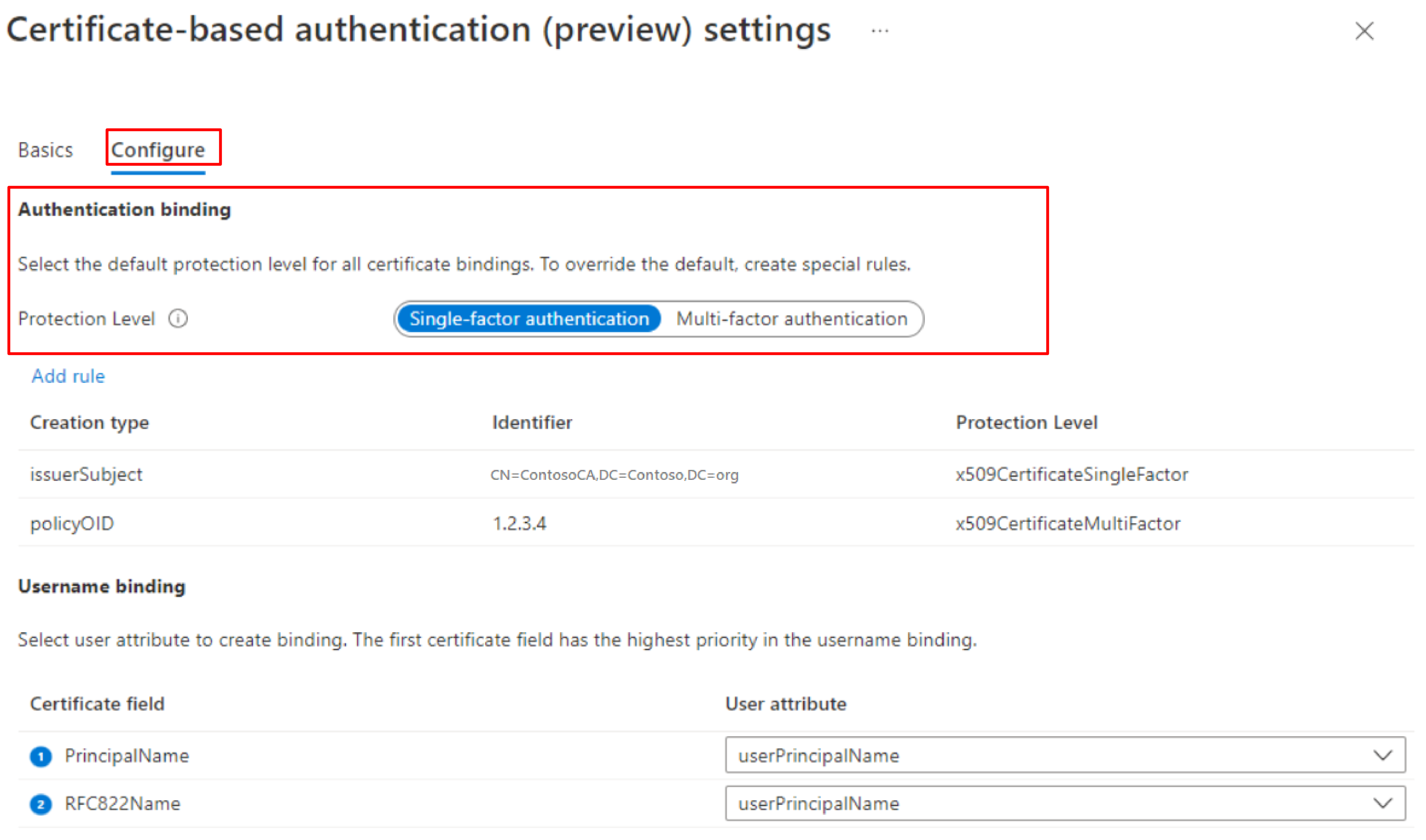
- Sign in
- Strong authentication

TARGET

All users [✓ Select users]

Name	Type	Registration
MFA User	User	Optional
MFA User with No Cert	User	Optional

Configure Authentication binding



Certificate-based authentication (preview) settings

Basics | Configure

Authentication binding

Select the default protection level for all certificate bindings. To override the default, create special rules.

Protection Level ⓘ [✓ Single-factor authentication] Multi-factor authentication

Add rule

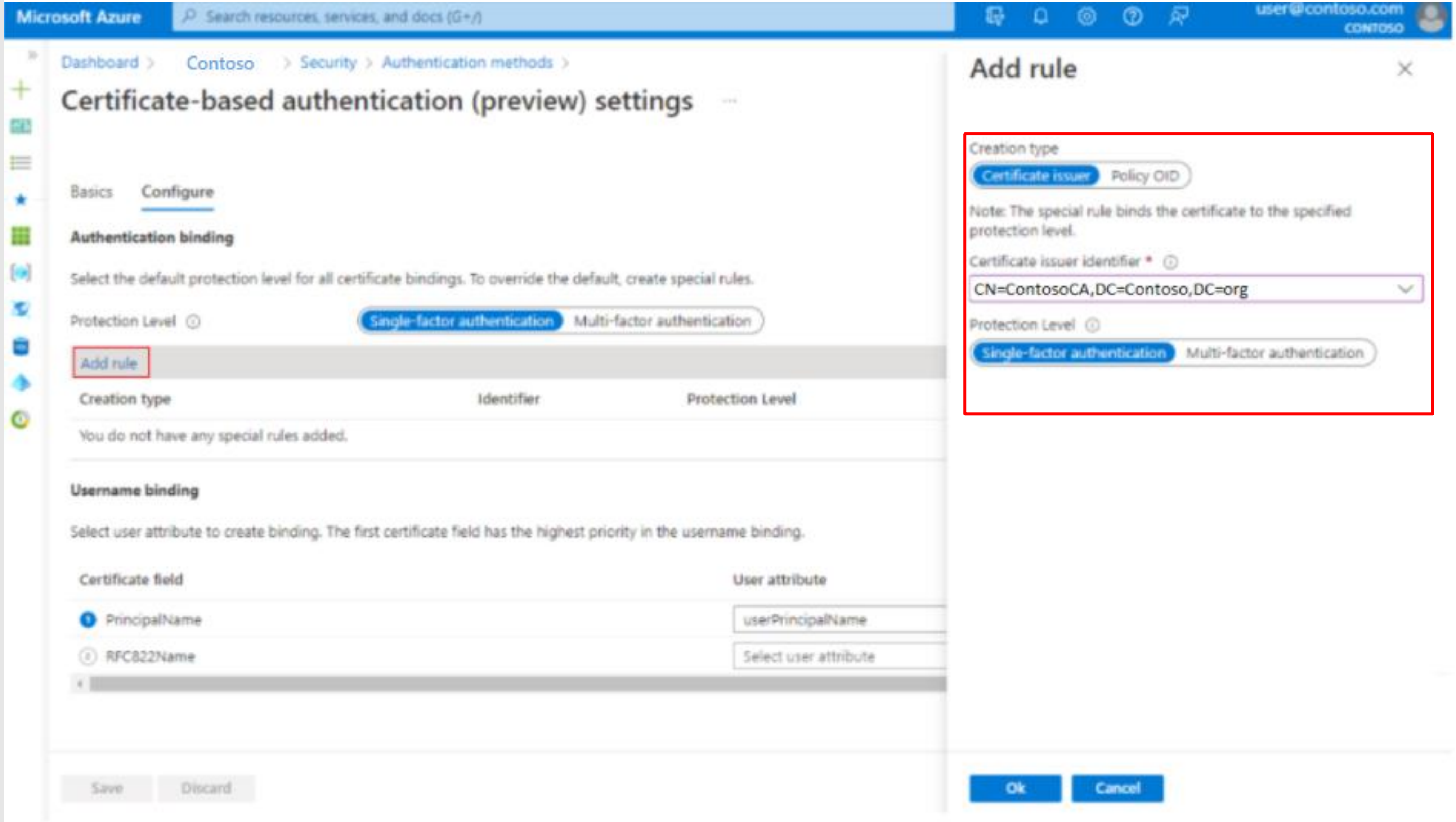
Creation type	Identifier	Protection Level
issuerSubject	CN=ContosoCA,DC=Contoso,DC=org	x509CertificateSingleFactor
policyOID	1.2.3.4	x509CertificateMultiFactor

Username binding

Select user attribute to create binding. The first certificate field has the highest priority in the username binding.

Certificate field	User attribute
1 PrincipalName	userPrincipalName
2 RFC822Name	userPrincipalName

Configure Authentication binding



Dashboard > Contoso > Security > Authentication methods >

Certificate-based authentication (preview) settings ...

Basics Configure

Authentication binding

Select the default protection level for all certificate bindings. To override the default, create special rules.

Protection Level ⓘ [✓ Single-factor authentication] Multi-factor authentication

Add rule

Creation type	Identifier	Protection Level
You do not have any special rules added.		

Username binding

Select user attribute to create binding. The first certificate field has the highest priority in the username binding.

Certificate field	User attribute
● PrincipalName	userPrincipalName
○ RFC822Name	Select user attribute

Save Discard

Add rule

Creation type

[✓ Certificate issuer] Policy OID

Note: The special rule binds the certificate to the specified protection level.

Certificate issuer identifier * ⓘ

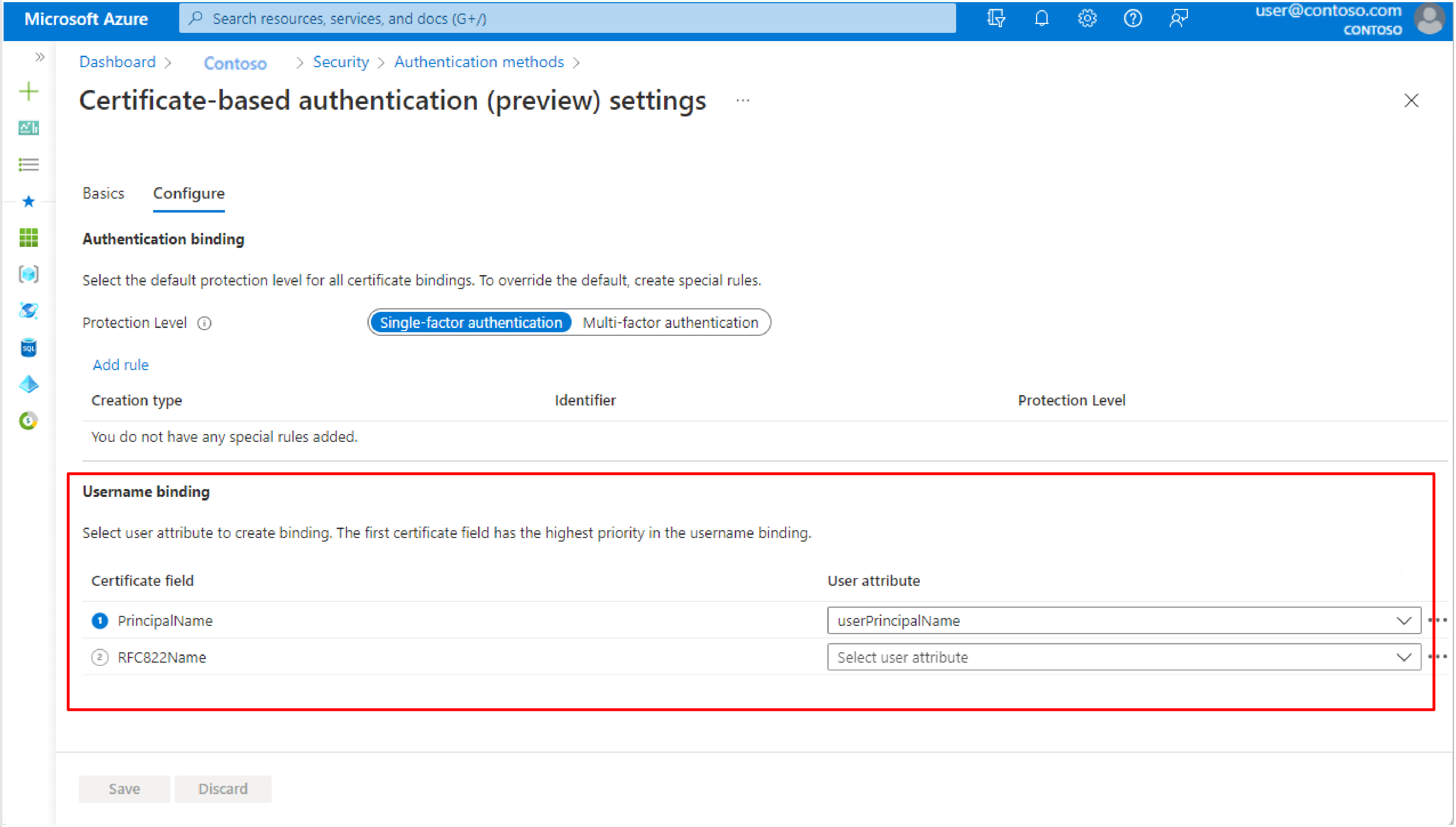
CN=ContosoCA,DC=Contoso,DC=org

Protection Level ⓘ

[✓ Single-factor authentication] Multi-factor authentication

Ok Cancel

Configure Username binding



Microsoft Azure
Search resources, services, and docs (G+/)
user@contoso.com
CONTOSO
Dashboard > Contoso > Security > Authentication methods >
Basics
Configure
Add rule
Save
Discard

Certificate-based authentication (preview) settings

Authentication binding

Select the default protection level for all certificate bindings. To override the default, create special rules.

Protection Level: [✓ Single-factor authentication] Multi-factor authentication

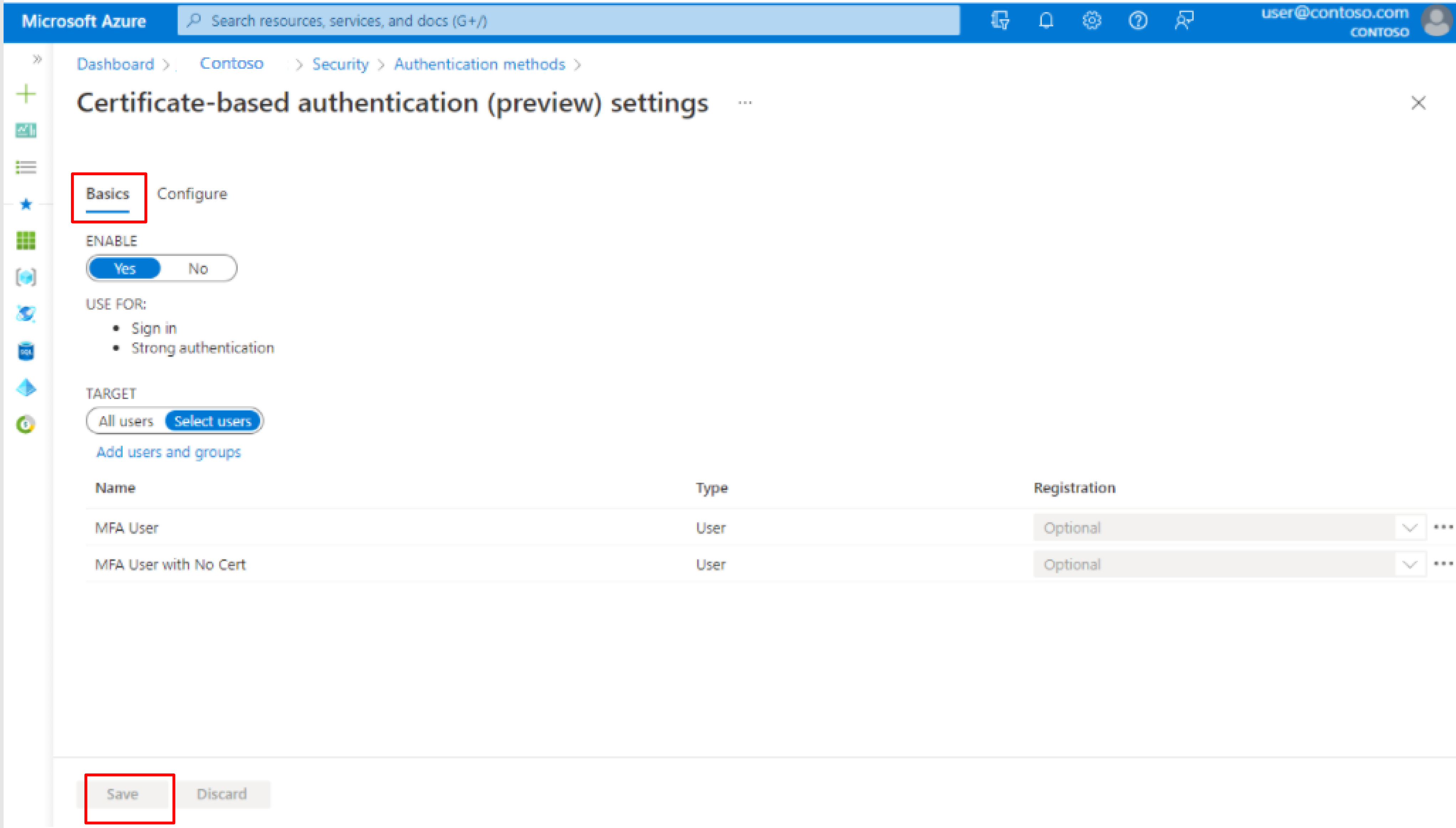
Creation type	Identifier	Protection Level
You do not have any special rules added.		

Username binding

Select user attribute to create binding. The first certificate field has the highest priority in the username binding.

Certificate field	User attribute
1 PrincipalName	userPrincipalName
2 RFC822Name	Select user attribute

Assign authentication method



Microsoft Azure
Search resources, services, and docs (G+/)
user@contoso.com
CONTOSO
Dashboard > Contoso > Security > Authentication methods >

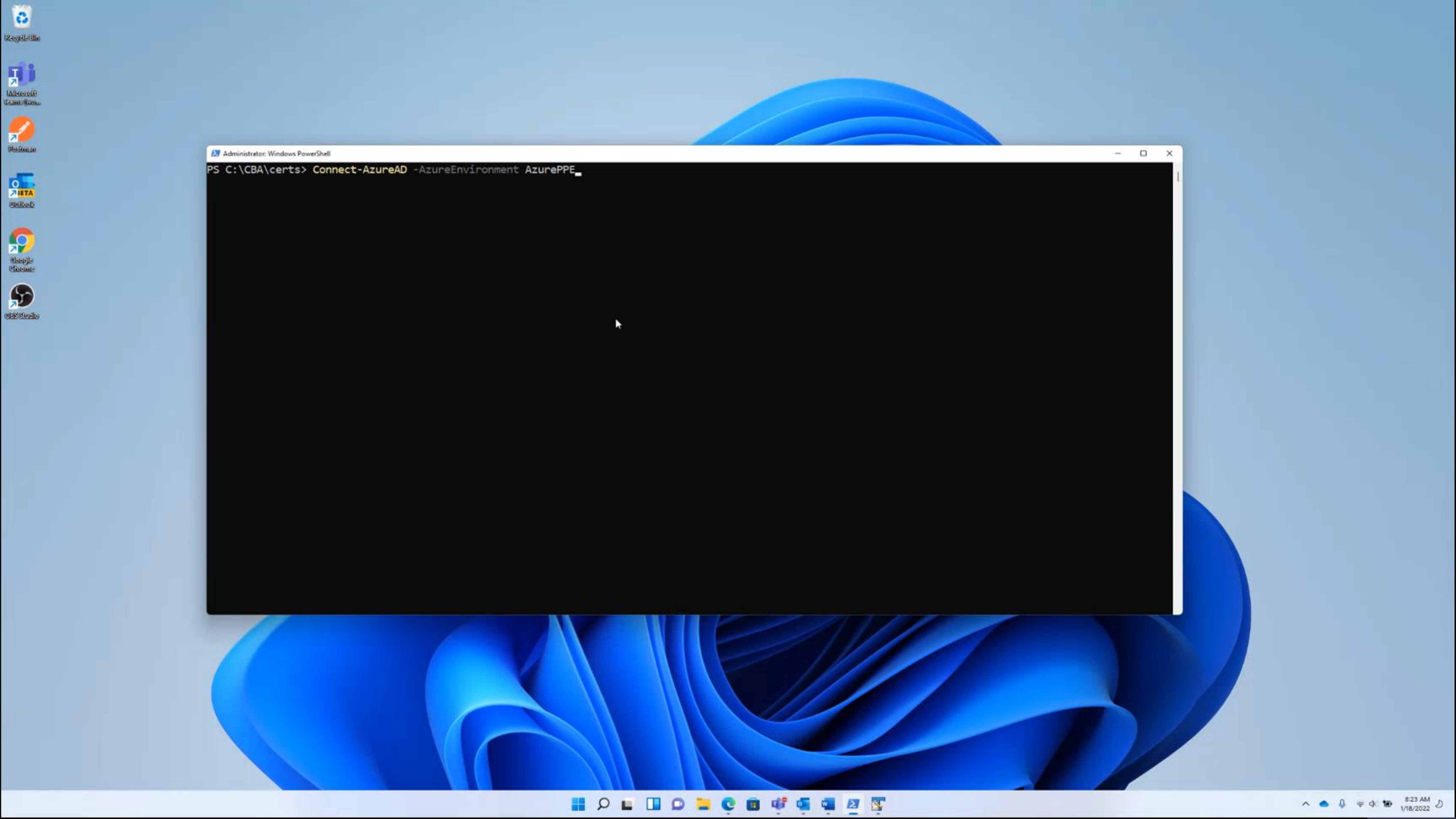
Certificate-based authentication (preview) settings

ENABLE
● Yes ○ No

USE FOR:
- Sign in
- Strong authentication

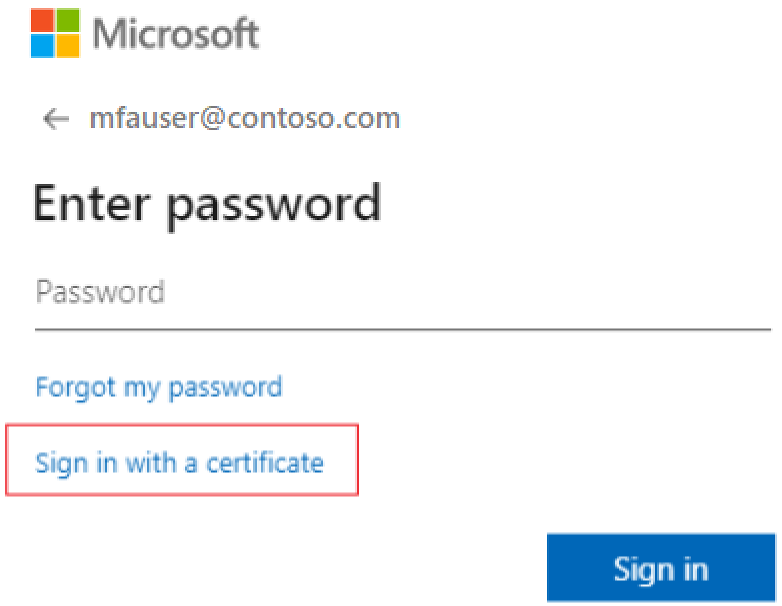
TARGET
○ All users ● Select users

Name	Type	Registration
MFA User	User	Optional
MFA User with No Cert	User	Optional



```
PS C:\CBA\certs> Connect-AzureAD -AzureEnvironment AzurePPE
```

End user experience



Microsoft

← mfauser@contoso.com

Enter password

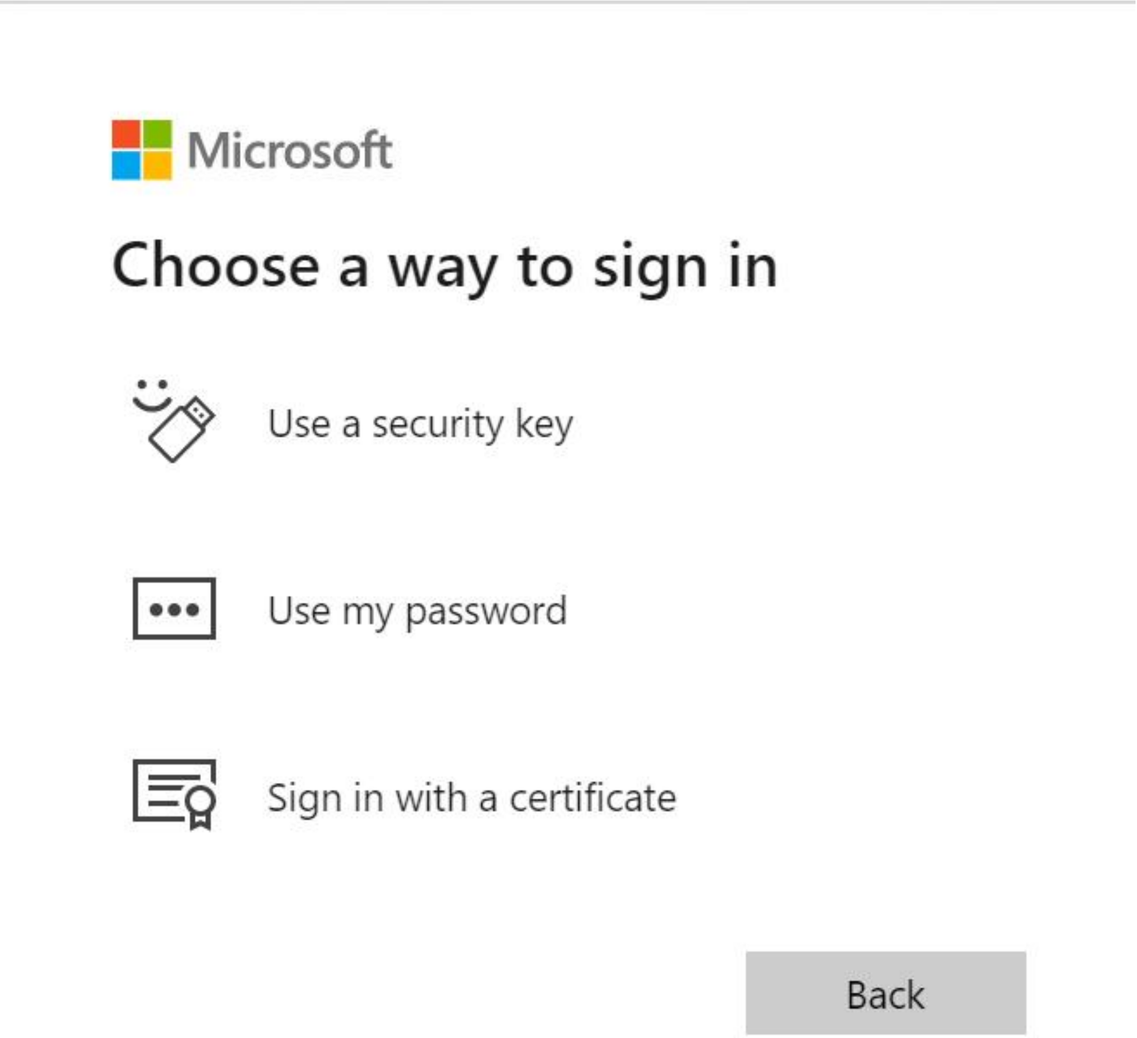
Password

Forgot my password

Sign in with a certificate

Sign in

End user experience



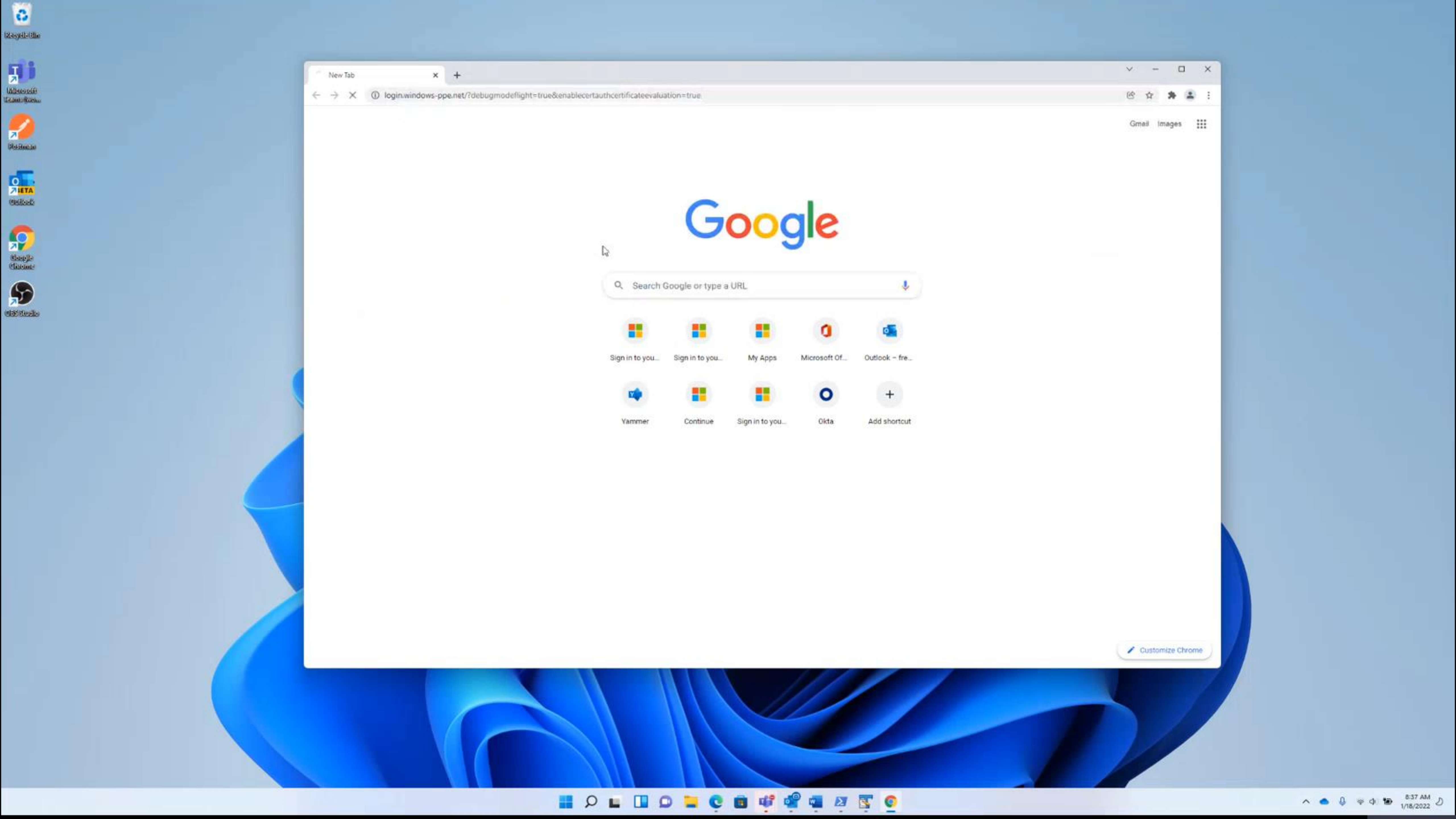
Microsoft

Choose a way to sign in

Use a security key

Use my password

Sign in with a certificate



login.windows-ppe.net/?debugmodeflight=true&enablecertauthcertificateevaluation=true

Revocation

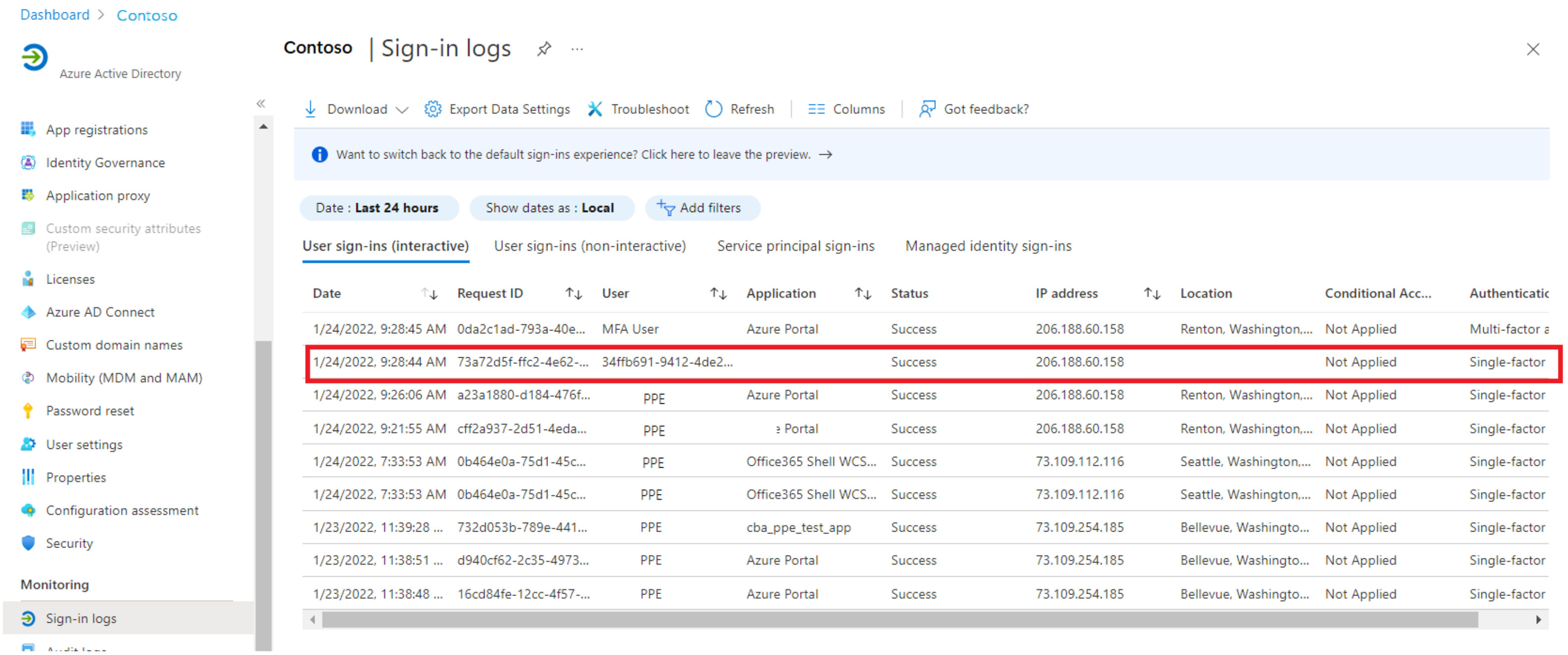
Only CRL is supported

CRL is cached

CRL needs to be downloaded in less then 10 seconds

No check on trust chain (Root compromised)

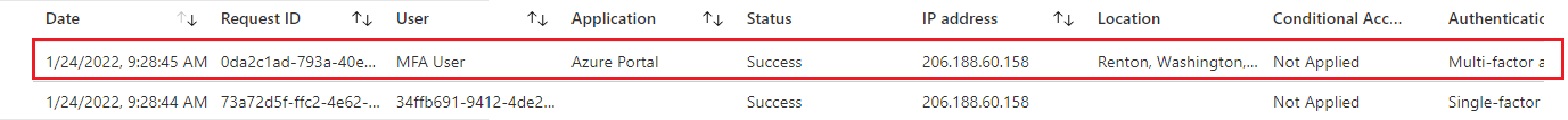
Logging: Single Factor



Contoso | Sign-in logs

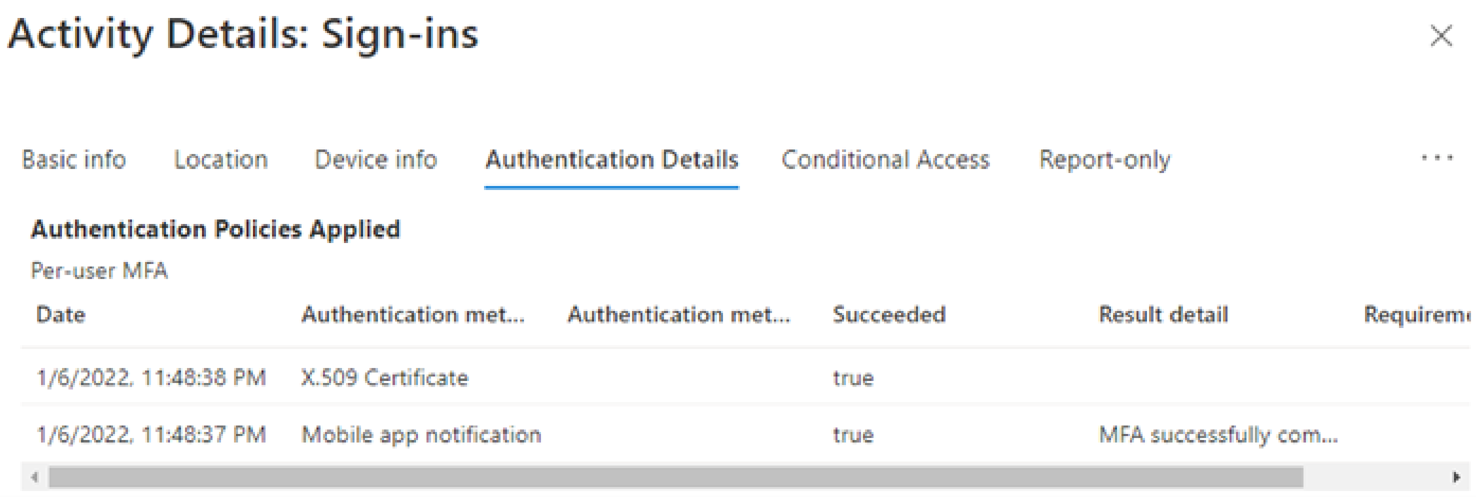
Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...	Authenticatic
1/24/2022, 9:28:45 AM	0da2c1ad-793a-40e...	MFA User	Azure Portal	Success	206.188.60.158	Renton, Washington,...	Not Applied	Multi-factor a
1/24/2022, 9:28:44 AM	73a72d5f-ffc2-4e62-...	34ffb691-9412-4de2...		Success	206.188.60.158		Not Applied	Single-factor
1/24/2022, 9:26:06 AM	a23a1880-d184-476f...	PPE	Azure Portal	Success	206.188.60.158	Renton, Washington,...	Not Applied	Single-factor
1/24/2022, 9:21:55 AM	cff2a937-2d51-4eda...	PPE	ɐ Portal	Success	206.188.60.158	Renton, Washington,...	Not Applied	Single-factor
1/24/2022, 7:33:53 AM	0b464e0a-75d1-45c...	PPE	Office365 Shell WCS...	Success	73.109.112.116	Seattle, Washington,...	Not Applied	Single-factor
1/24/2022, 7:33:53 AM	0b464e0a-75d1-45c...	PPE	Office365 Shell WCS...	Success	73.109.112.116	Seattle, Washington,...	Not Applied	Single-factor
1/23/2022, 11:39:28 ...	732d053b-789e-441...	PPE	cba_ppe_test_app	Success	73.109.254.185	Bellevue, Washingto...	Not Applied	Single-factor
1/23/2022, 11:38:51 ...	d940cf62-2c35-4973...	PPE	Azure Portal	Success	73.109.254.185	Bellevue, Washingto...	Not Applied	Single-factor
1/23/2022, 11:38:48 ...	16cd84fe-12cc-4f57-...	PPE	Azure Portal	Success	73.109.254.185	Bellevue, Washingto...	Not Applied	Single-factor



Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...	Authenticatic
1/24/2022, 9:28:45 AM	0da2c1ad-793a-40e...	MFA User	Azure Portal	Success	206.188.60.158	Renton, Washington,...	Not Applied	Multi-factor a
1/24/2022, 9:28:44 AM	73a72d5f-ffc2-4e62-...	34ffb691-9412-4de2...		Success	206.188.60.158		Not Applied	Single-factor

Logging: MFA requested

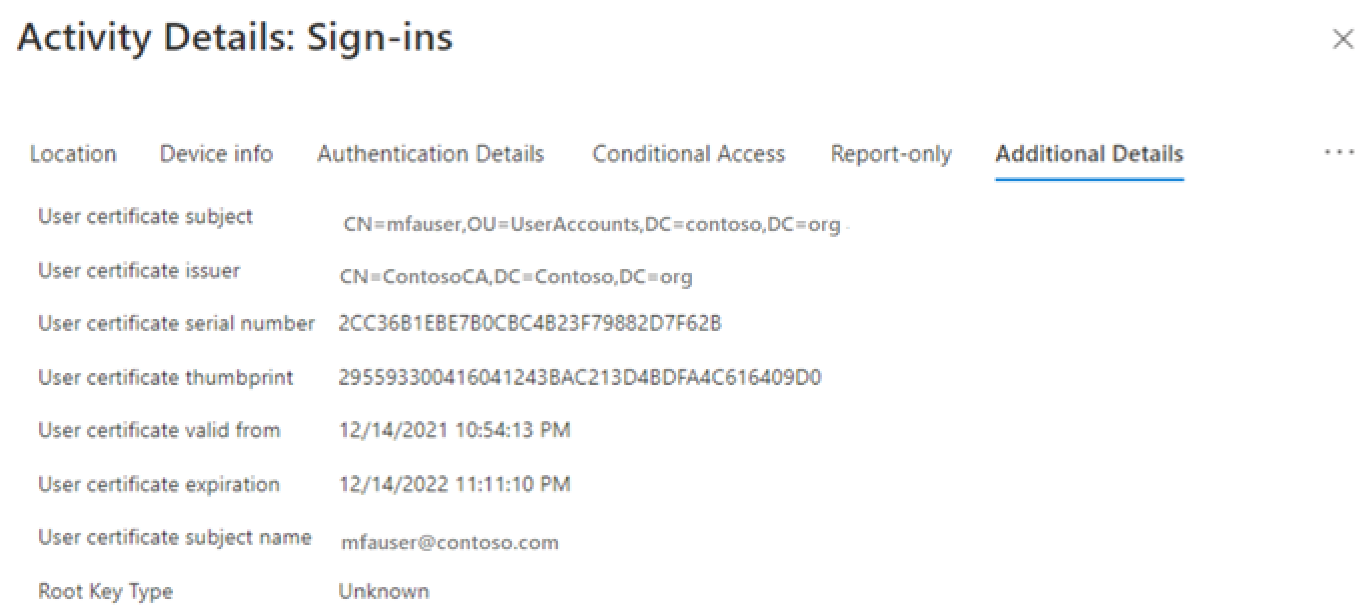


Authentication Policies Applied

Per-user MFA

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requirem
1/6/2022, 11:48:38 PM	X.509 Certificate		true		
1/6/2022, 11:48:37 PM	Mobile app notification		true	MFA successfully com...	

Logging: Additional Information



Activity Details: Sign-ins

User certificate subject	CN=mfauser,OU=UserAccounts,DC=contoso,DC=org
User certificate issuer	CN=ContosoCA,DC=Contoso,DC=org
User certificate serial number	2CC36B1EBE7B0CBC4B23F79882D7F62B
User certificate thumbprint	295593300416041243BAC213D4BDFA4C616409D0
User certificate valid from	12/14/2021 10:54:13 PM
User certificate expiration	12/14/2022 11:11:10 PM
User certificate subject name	mfauser@contoso.com
Root Key Type	Unknown

Supported Scenarios

- User sign-ins to web browser-based applications on all platforms.
- User sign-ins on mobile native browsers.
- Support for granular authentication rules for multifactor authentication by using the certificate issuer Subject and policy OIDs.
- Configuring certificate-to-user account bindings by using the certificate Subject Alternate Name (SAN) principal name and SAN RFC822 name.

Q&A

Microsoft

Thank you!

Twitter: @azuread / @wiele