2/18/2020

Security Training

Windows Hello for Business, Conditional Access & MFA

ADEB VBA

ELEVATING CONSTRUCTION TOGETHER

Xylos

AGENDA

Opening and Introduction

Windows Hello for Business

Azure Multi-Factor Authentication

Conditional Access

Q&A

Introduction

- Sebastian Mellebeek
- Sr. IT Consultant @ Xylos
- 10 years of experience in IT

Contact information:

- Email: Sebastian.mellebeek@xylos.com
- Linkedin

Windows Hello for Business

Overview

Xylos

Security Threats with Passwords

- Strong passwords can be difficult to remember, and users often reuse passwords on multiple sites.
- Server breaches can expose symmetric network credentials (passwords).
- Passwords are subject to replay attacks.
- Users can inadvertently expose their passwords due to phishing attacks.

Windows Hello

- Biometric logon
  - Face Recognition
  - Fingerprint
- PIN configuration
- FIDO2 support
- Supporting Hello for Business
  - Password-less Authentication
  - Based on certificates

Difference between Windows Hello and Windows Hello for Business

- Individuals can create a PIN or biometric gesture on their personal devices for convenient sign-in. This use of Windows Hello is unique to the device on which it is set up, however it is not backed by asymmetric (public/private key) or certificate-based authentication.

- Windows Hello for Business, which is configured by Group Policy or mobile device management (MDM) policy, uses key-based or certificate-based authentication.

What and Why do you need a PIN to use biometrics?

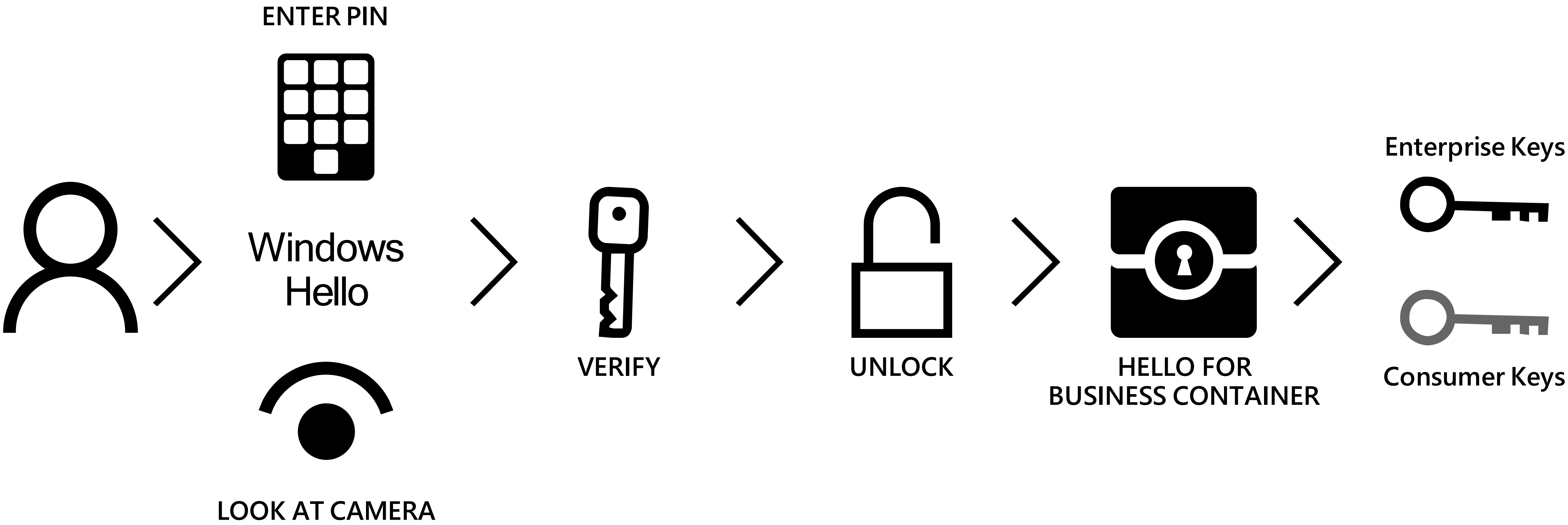
- A PIN can be compared to a Password but is better
- A PIN is more secure because it is:
  - Tied to the device
  - Local to the device
  - Backed by the device hardware (TPM)

- If Biometrics sign-in doesn’t work (i.e. sensor failure)
- Without the PIN, a user would need to login again with Username & Password

How Hello for Business Works?

- Windows Hello Credentials are based on certificates (Assymetric)
- Credentials & tokens are bound to the device
- Keys are stored in TPM hardware (If available) or via software encryption
- Two-factor authentication
  - Device + PIN
  - Device + Biometric
- PIN or Biometric trigger the private key to:
  - Sign authentication data
  - Send to the Identity Provider (AD or AzureAD)
- Identity Provider use public dkey to verify and authenticate the user

Windows Hello and Biometrics



ENTER PIN

Windows Hello

LOOK AT CAMERA

VERIFY

UNLOCK

HELLO FOR BUSINESS CONTAINER

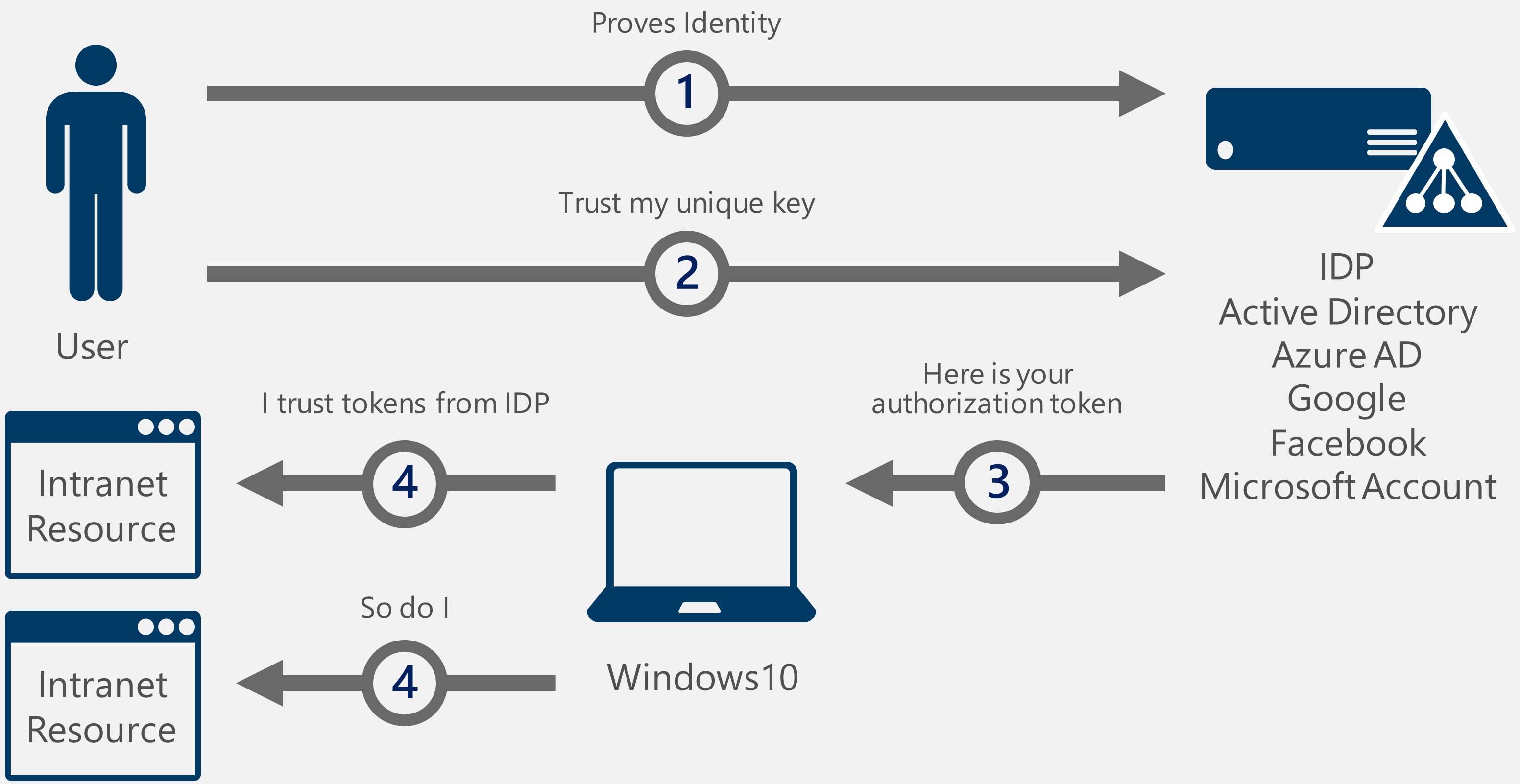
Enterprise Keys

Consumer Keys

Xylos

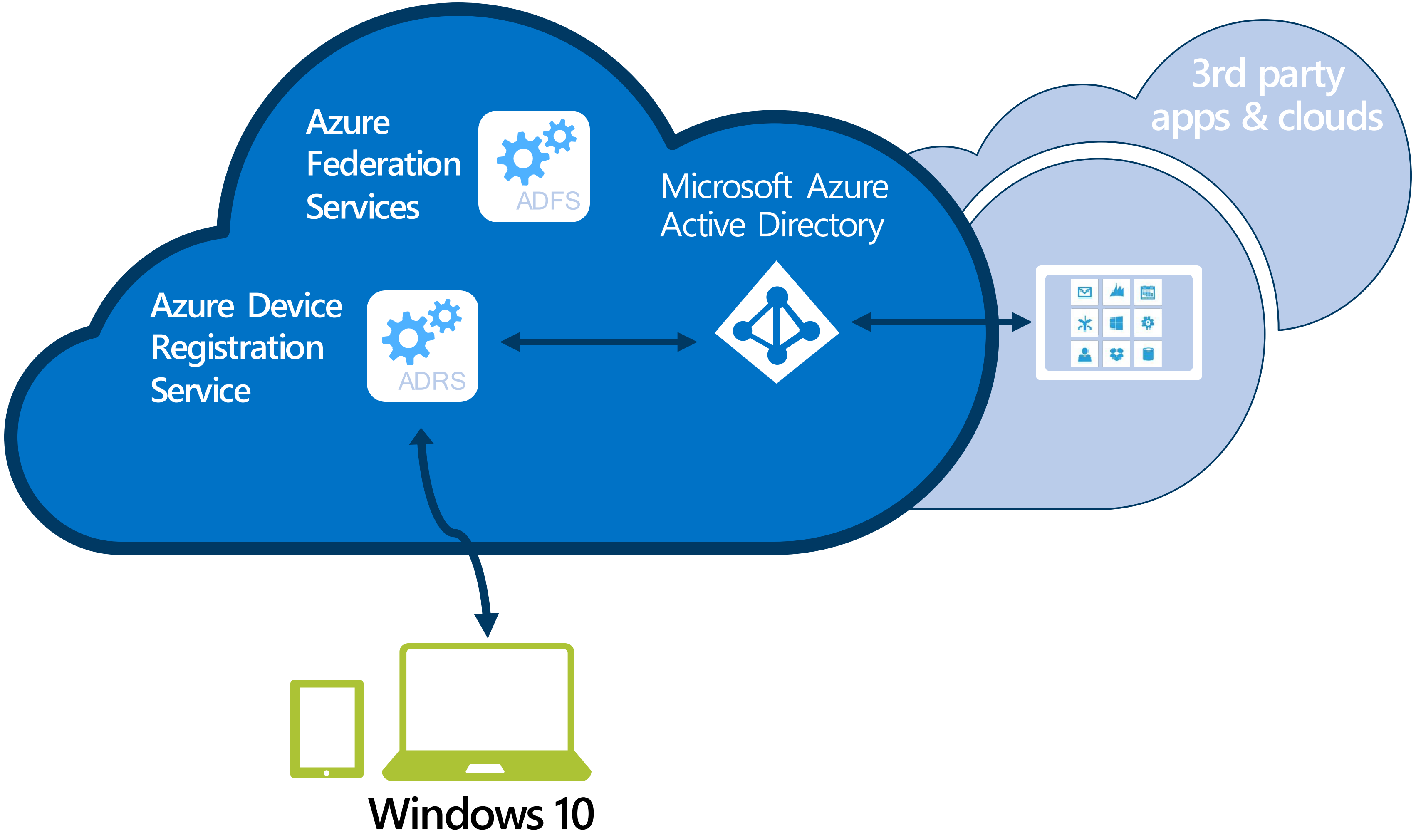
Authentication and Access flow

Workflow



Xylos

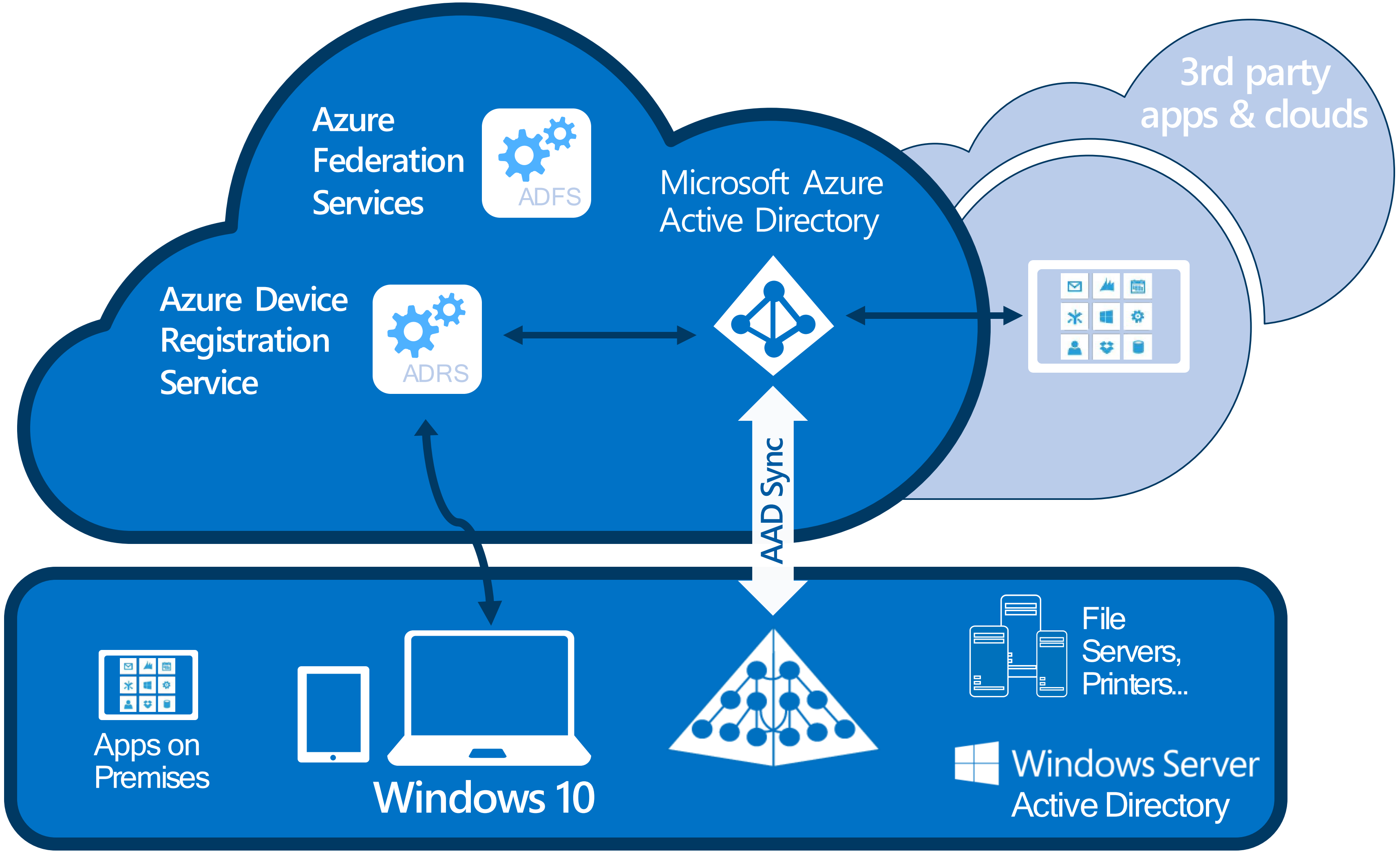
Azure Active Directory only



Azure Federation Services
ADFS
Microsoft Azure Active Directory
3rd party apps & clouds
Azure Device Registration Service
ADRS
Windows 10

Xylos

Azure Active Directory + Active Directory AD Hybrid



Xylos

Bootstrapping the Trust process

User-proofing Enrollment

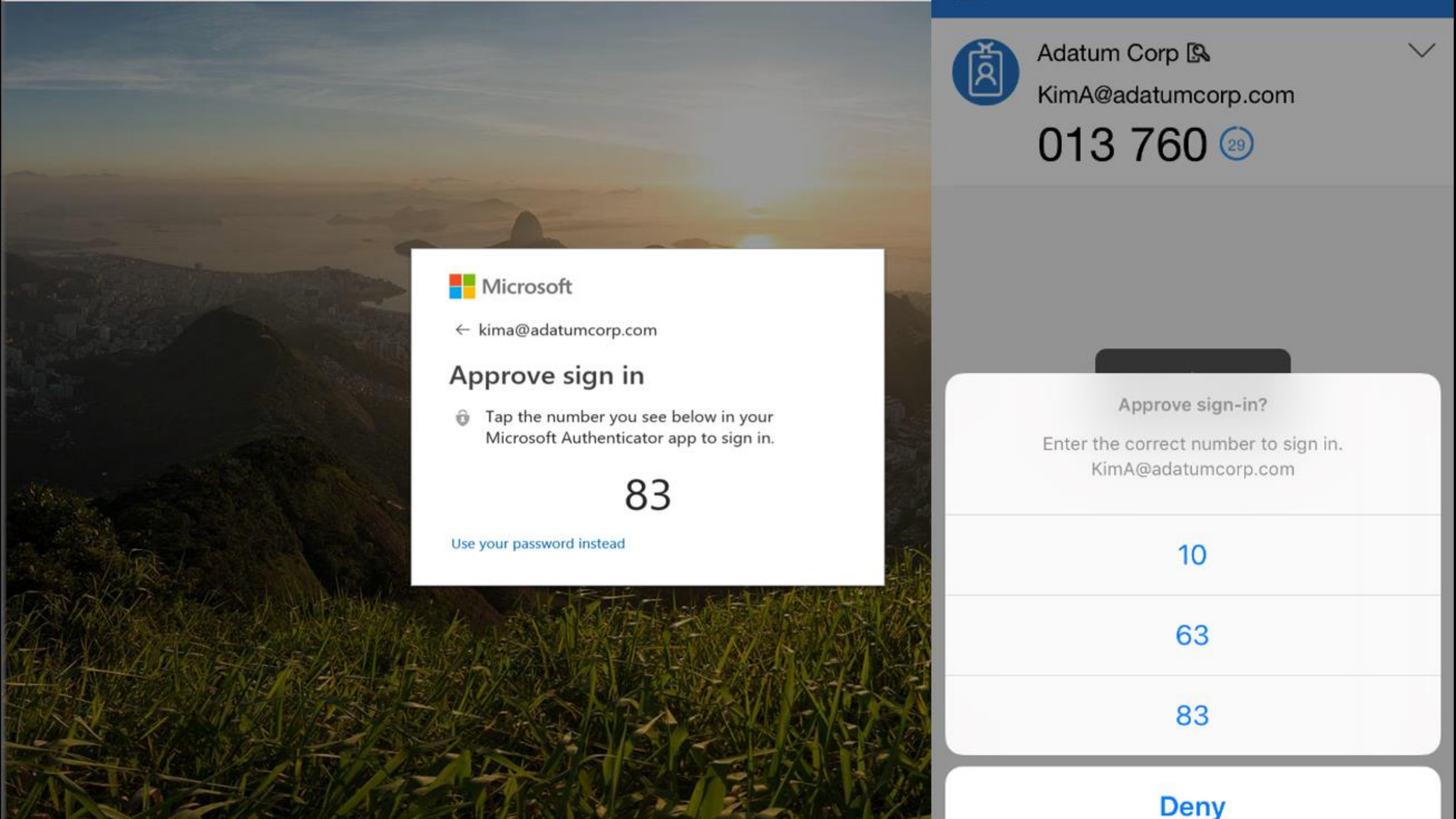
Users will enroll using:

→ Existing password

→ OTP

→ Code (e.g.: SMS)

→ ...



Microsoft

← kima@adatumcorp.com

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

83

Adatum Corp

KimA@adatumcorp.com

013 760

Approve sign-in?

Enter the correct number to sign in.
KimA@adatumcorp.com

Deployment and Management

Windows Hello for Business

Deployment type

- Three deployment models:
  - Cloud Only
  - Hybrid
    - Key trust deployment
    - Certificate trust deployment
  - On-premises
    - Key trust deployment
    - Certificate trust deployment

- The model to choose depends on your current infrastructure
- Requirements depend on the deployment model that suits your organization

Cloud Only Deployment

- Windows 10, version 1511 or later
- Microsoft Azure Account
- Azure Active Directory
- Azure Multi-factor authentication
- Modern Management (Intune or supported third-party MDM), optional
- Azure AD Premium subscription - optional, needed for automatic MDM enrollment when the device joins Azure Active Directory

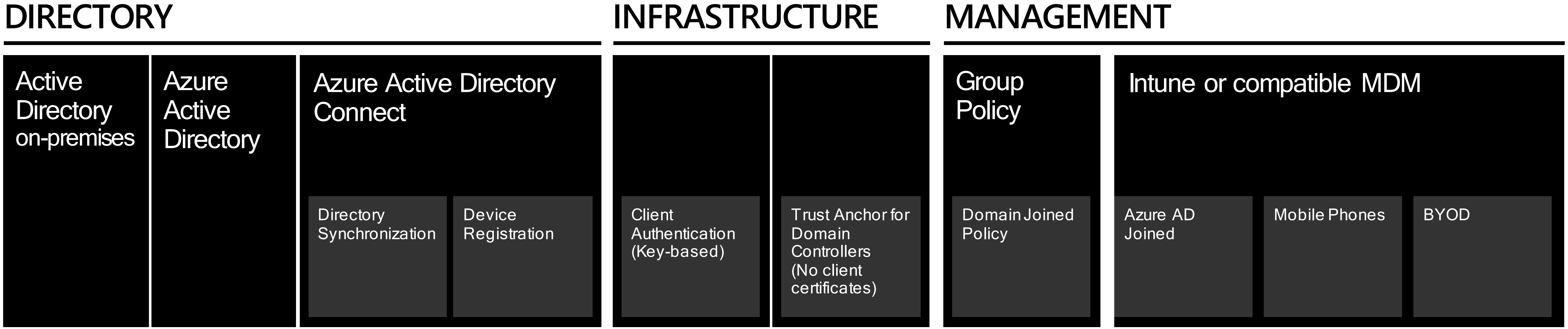
Hybrid Deployment

Key trust **Group Policy managed**	**Certificate trust** **Mixed managed**	**Key trust** **Modern managed**	**Certificate trust** **Modern managed**
Windows 10, version 1511 or later	**Hybrid Azure AD Joined:** *Minimum:* Windows 10, version 1703 *Best experience:* Windows 10, version 1709 or later (supports synchronous certificate enrollment). **Azure AD Joined:** Windows 10, version 1511 or later	Windows 10, version 1511 or later	Windows 10, version 1511 or later
Windows Server 2016 Schema	Windows Server 2016 Schema	Windows Server 2016 Schema	Windows Server 2016 Schema
Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level
Windows Server 2016 or later Domain Controllers	Windows Server 2008 R2 or later Domain Controllers	Windows Server 2016 or later Domain Controllers	Windows Server 2008 R2 or later Domain Controllers
Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority

Hybrid Deployment

Key trust **Group Policy managed**	**Certificate trust** **Mixed managed**	**Key trust** **Modern managed**	**Certificate trust** **Modern managed**
N/A	Windows Server 2016 AD FS with KB4088889 update (hybrid Azure AD joined clients), and Windows Server 2012 or later Network Device Enrollment Service (Azure AD joined)	N/A	Windows Server 2012 or later Network Device Enrollment Service
Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter	Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter	Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter	Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter
Azure Account	Azure Account	Azure Account	Azure Account
Azure Active Directory	Azure Active Directory	Azure Active Directory	Azure Active Directory
Azure AD Connect	Azure AD Connect	Azure AD Connect	Azure AD Connect
Azure AD Premium, optional	Azure AD Premium, needed for device write-back	Azure AD Premium, optional for automatic MDM enrollment	Azure AD Premium, optional for automatic MDM enrollment

Key-Trust (Hybrid)



DIRECTORY

- Active Directory on-premises
- Azure Active Directory
- Azure Active Directory Connect
  - Directory Synchronization
  - Device Registration

INFRASTRUCTURE

- Client Authentication (Key-based)
- Trust Anchor for Domain Controllers (No client certificates)

MANAGEMENT

- Group Policy
  - Domain Joined Policy
- Intune or compatible MDM
  - Azure AD Joined
  - Mobile Phones
  - BYOD

Certificate-Trust (Hybrid)

DIRECTORY

- Active Directory on-premises
- Azure Active Directory
- Azure Active Directory Connect
  - Directory Synchronization
  - Device Registration

INFRASTRUCTURE

- Domain Controller Certificates
- Client Certificates

MANAGEMENT

- Active Directory on-premises
  - Domain Joined Policy
- SCCM (Current Branch)
  - Domain Joined Certificate Enrollment
- Intune or compatible MDM
  - Mobile Phones
  - BYOD

On-premises Deployment

Key trust **Group Policy managed**	**Certificate trust** **Group Policy managed**
Windows 10, version 1703 or later	Windows 10, version 1703 or later
Windows Server 2016 Schema	Windows Server 2016 Schema
Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level
Windows Server 2016 or later Domain Controllers	Windows Server 2008 R2 or later Domain Controllers
Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority
Windows Server 2016 AD FS with KB4088889 update	Windows Server 2016 AD FS with KB4088889 update
AD FS with Azure MFA Server, or AD FS with 3rd Party MFA Adapter	AD FS with Azure MFA Server, or AD FS with 3rd Party MFA Adapter
Azure Account, optional for Azure MFA billing	Azure Account, optional for Azure MFA billing

Key-Trust (On-premises)

DIRECTORY

Active Directory
on-premises

Azure Active Federation Services 2016

- Domain Registration
- Key Registration

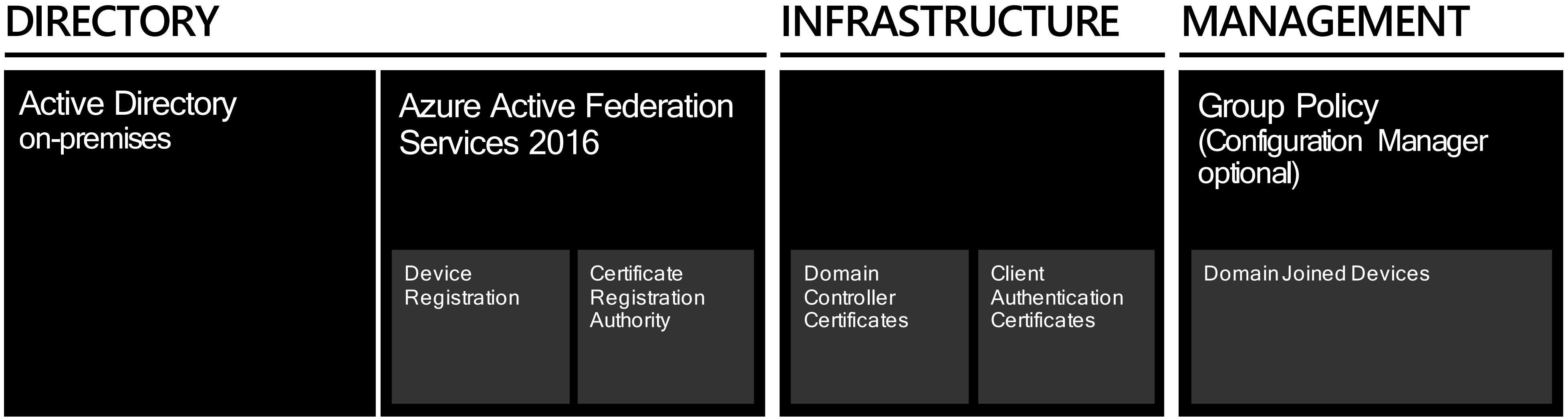
INFRASTRUCTURE

- Client Authentication
(Key-based)
- Trust Anchor for Domain Controllers
(No client certificates)

MANAGEMENT

Group Policy or Configuration Manager

Certificate-Trust (On-premises)



DIRECTORY

Active Directory
on-premises

Azure Active Federation Services 2016

Device Registration

Certificate Registration Authority

INFRASTRUCTURE

Domain Controller Certificates

Client Authentication Certificates

MANAGEMENT

Group Policy
(Configuration Manager optional)

Domain Joined Devices

Xylos

Windows Hello for Business

Features

WHFB features

- Conditional access
- Dynamic lock
- PIN reset
- Dual Enrollment
- Remote Desktop with Biometrics

Conditional Access

To:

- Empower the end users to be productive wherever and whenever
- Protect the corporate assets at any time

Requirements:

- Azure Active Directory
- Hybrid Windows Hello for Business deployment

Dynamic Lock

Automatic lock of your device if your paired device is it out of range

Example: Smartphone that is paired to your Windows device via bluetooth

Requirements:

- Windows 10, version 1703

PIN reset

Users will be able to reset their PIN if forgotten

Requirements:

- Azure Active Directory
- Hybrid Windows Hello for Business deployment
- Azure AD registered, Azure AD joined, and Hybrid Azure AD joined
- Windows 10, version 1709 or later, Enterprise Edition

Dual Enrollment

Dual enrollment enables administrators to perform elevated, administrative functions by enrolling both their non-privileged and privileged credentials on their device.

Requirements

- Hybrid and On-premises Windows Hello for Business deployments
- Enterprise Joined or Hybrid Azure joined devices
- Windows 10, version 1709

Remote Desktop with Biometrics

Using Windows Hello for Business to Remote desktop to your Windows device.

Requirements

- Hybrid and On-premises Windows Hello for Business deployments
- Azure AD joined, Hybrid Azure AD joined, and Enterprise joined devices
- Certificate trust deployments
- Biometric enrollments
- Windows 10, version 1809

Only works with Certificate trust models

DEMO

10:36

Friday, September 14

Azure Multi-Factor Authentication

What is Azure Multi-Factor Authentication

What it is

- A standalone Azure identity and access management service, also included in Azure Active Directory Premium
- Prevents unauthorized access to both on-premises and cloud applications by providing an additional level of authentication
- Trusted by thousands of enterprises to authenticate employee, customer, and partner access

Per-User MFA versus Conditional Access

Per-User MFA

- Require MFA always, for all applications
- Free of charge for all Azure AD admins and all Azure admins

Conditional Access

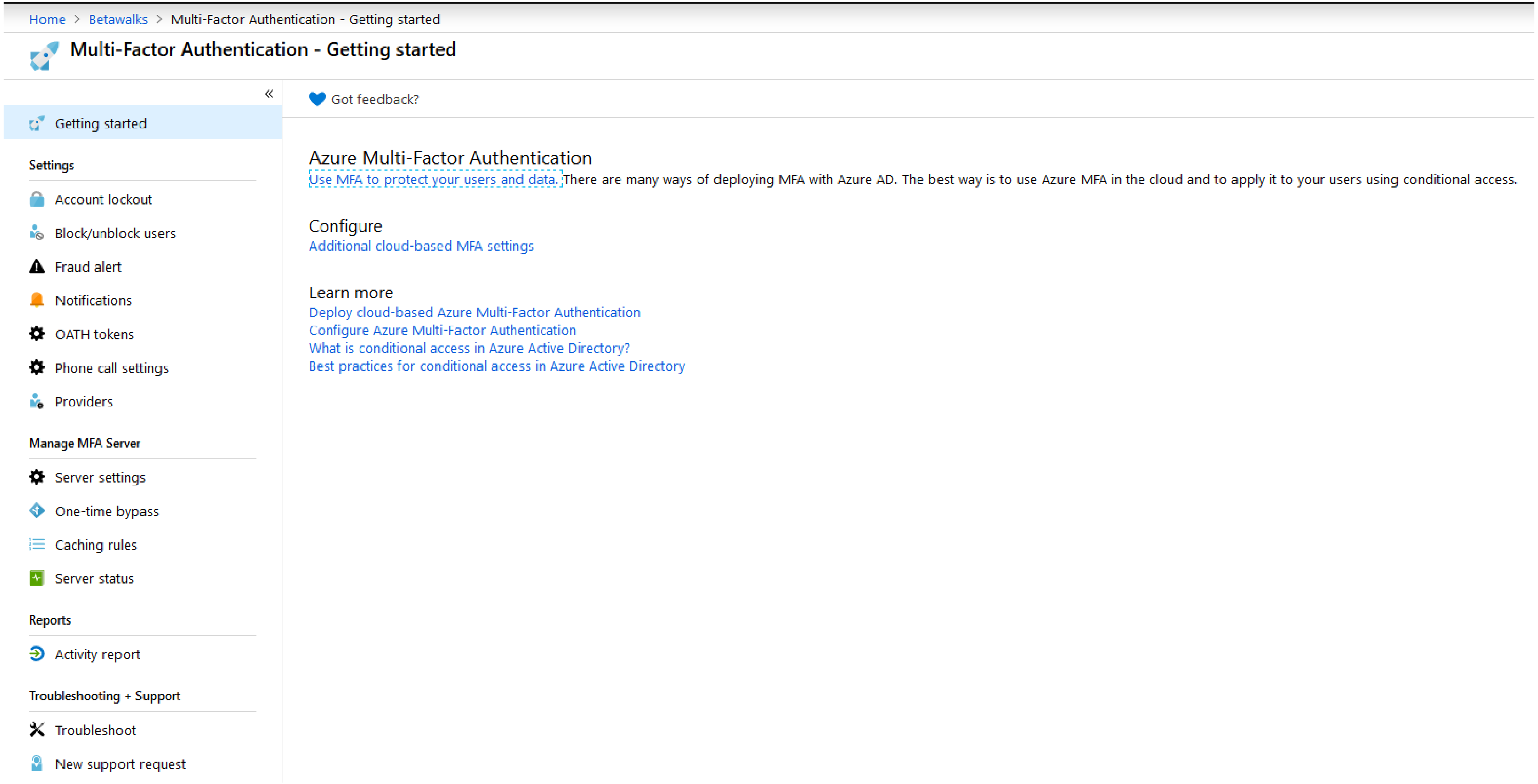
- Require MFA under specific conditions
- For a specific app e.g. Azure Admin Portal
- When not on work network
- When sign-in considered high risk

Azure AD Premium feature

- Licenses needed for users who are affected by policy

Prerequisites

Scenario	Prerequisite
Cloud-only identity environment with modern authentication	**No additional prerequisite tasks**
Hybrid identity scenarios	Azure AD Connect is deployed and user identities are synchronized or federated with the on-premises Active Directory Domain Services with Azure Active Directory.
On-premises legacy applications published for cloud access	Azure AD Application Proxy is deployed.
Using Azure MFA with RADIUS Authentication	A Network Policy Server (NPS) is deployed.
Users have Microsoft Office 2010 or earlier, or Apple Mail for iOS 11 or earlier	Upgrade to Microsoft Office 2013 or later and Apple mail for iOS 12 or later. Conditional Access is not supported by legacy authentication protocols.



Multi-Factor Authentication - Getting started

Azure Multi-Factor Authentication

Use MFA to protect your users and data. There are many ways of deploying MFA with Azure AD. The best way is to use Azure MFA in the cloud and to apply it to your users using conditional access.

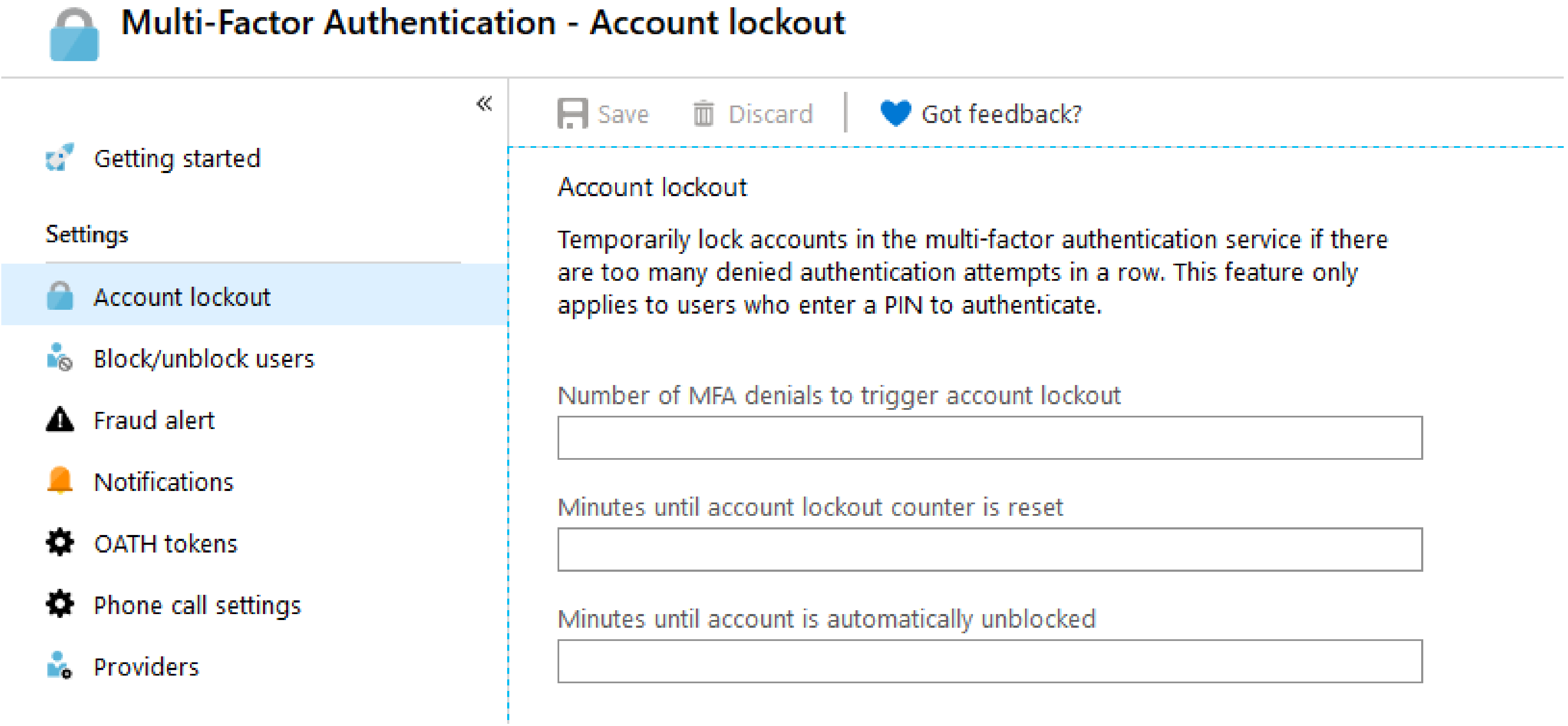
Configure

Additional cloud-based MFA settings

Learn more

Deploy cloud-based Azure Multi-Factor Authentication
Configure Azure Multi-Factor Authentication
What is conditional access in Azure Active Directory?
Best practices for conditional access in Azure Active Directory

Account lockout



Multi-Factor Authentication - Account lockout

Account lockout

Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.

Number of MFA denials to trigger account lockout

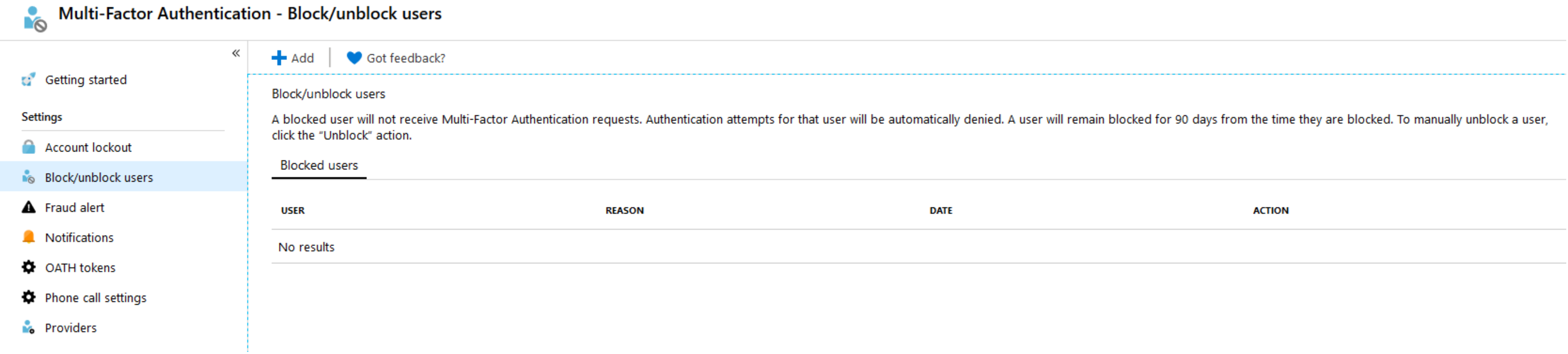
Minutes until account lockout counter is reset

Minutes until account is automatically unblocked

Xylos

Block/Unblock Users

- User won’t receive an MFA request
- Request is automatically denied
- Users remain blocked for 90 days from the time they are blocked



Multi-Factor Authentication - Block/unblock users

Block/unblock users

A blocked user will not receive Multi-Factor Authentication requests. Authentication attempts for that user will be automatically denied. A user will remain blocked for 90 days from the time they are blocked. To manually unblock a user, click the “Unblock” action.

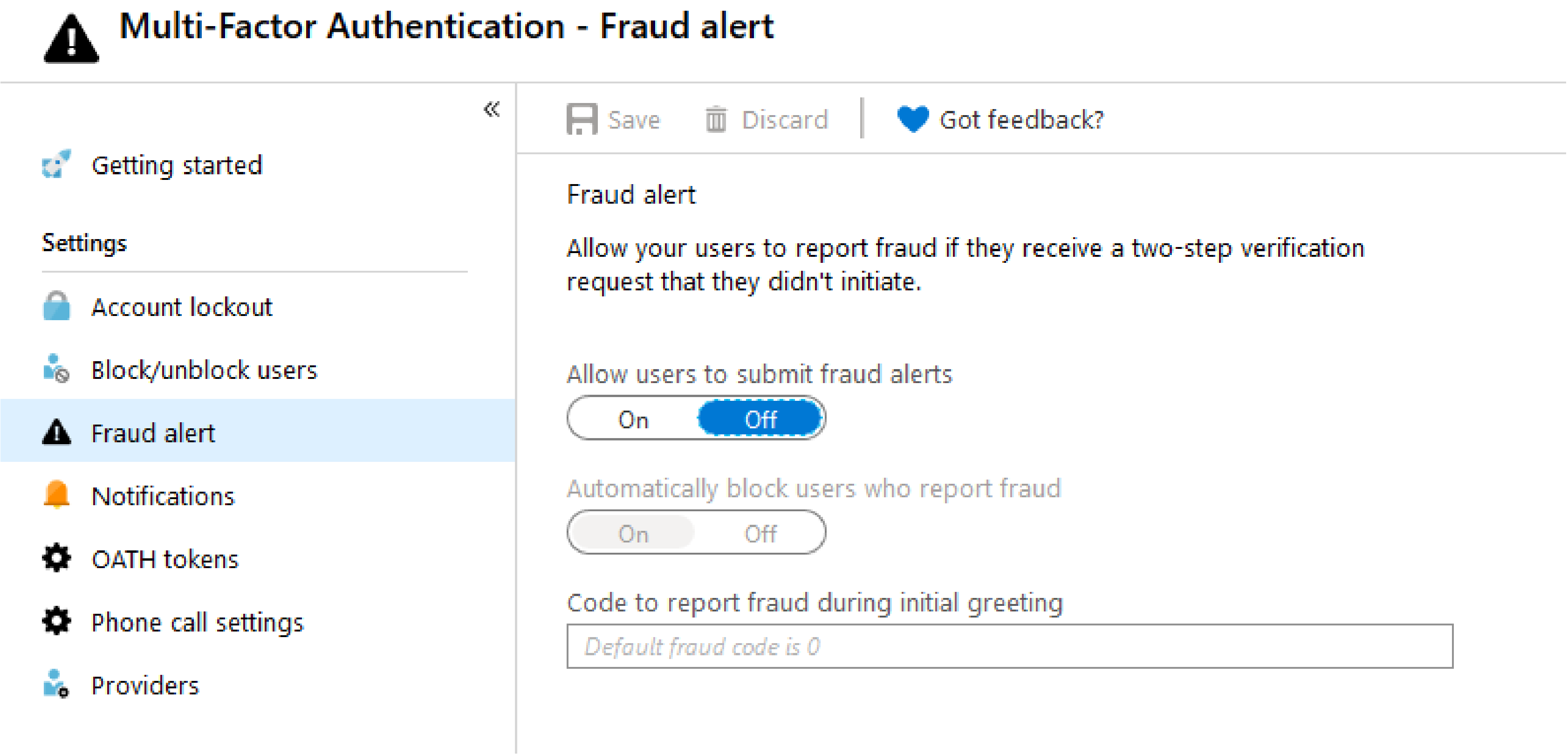
Blocked users

USER	REASON	DATE	ACTION
No results			

Xylos

Fraud alerts

For users to alert fraudulent attemps to access their resources



Multi-Factor Authentication - Fraud alert

Fraud alert

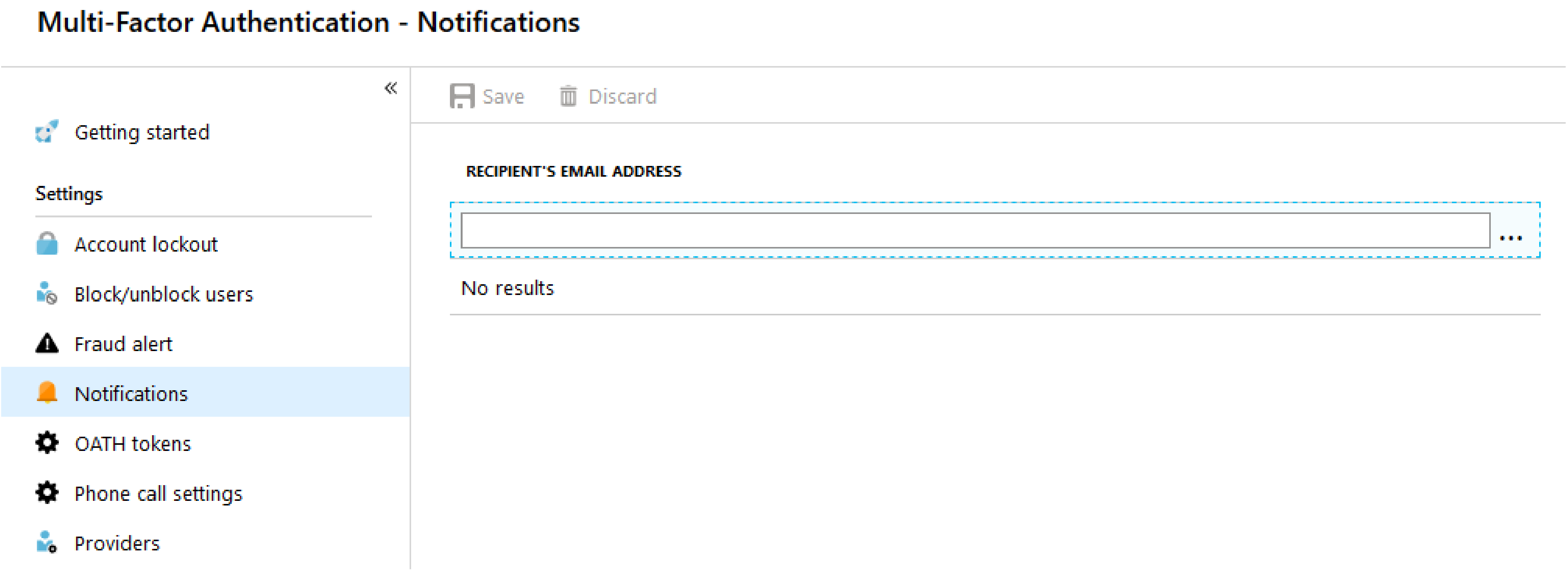
Allow your users to report fraud if they receive a two-step verification request that they didn't initiate.

Allow users to submit fraud alerts
On [✓ Off]

Automatically block users who report fraud
On Off

Code to report fraud during initial greeting
Default fraud code is 0

Notifications



Multi-Factor Authentication - Notifications

RECIPIENT'S EMAIL ADDRESS

No results

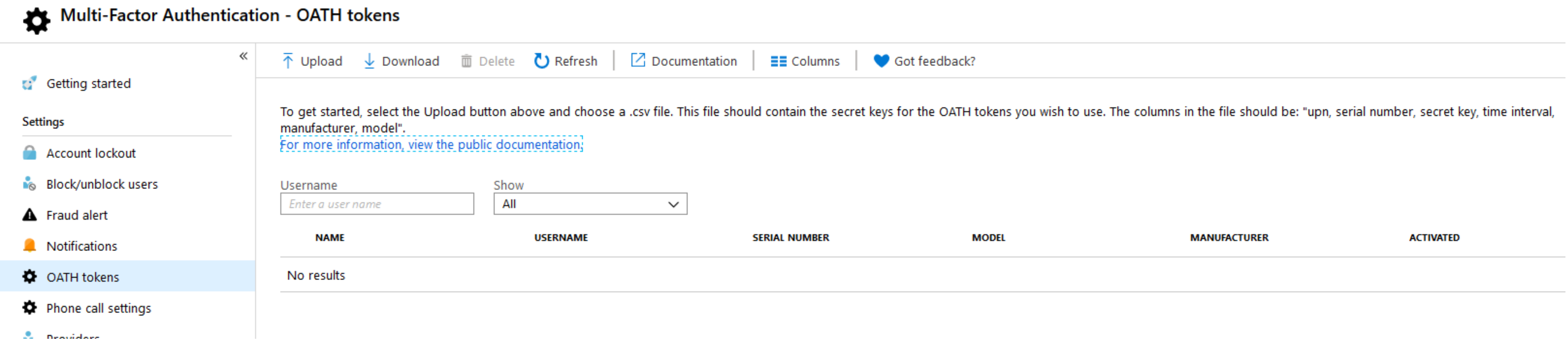
Xylos

Authentication methods available

Authentication Method	Usage
Password	MFA and SSPR
Security questions	SSPR Only
Email address	SSPR Only
Microsoft Authenticator app	MFA and SSPR
OATH Hardware token	Public preview for MFA and SSPR
SMS	MFA and SSPR
Voice call	MFA and SSPR
App passwords	MFA only in certain cases

Register OATH tokens

- OATH-TOTP SHA-1 tokens of the 30-second variety
- OATH-TOTP SHA-1 tokens of the 60-second variety
- Vendor of choice
- Secret keys are limited to 128 characters and need to be encoded in base32



To get started, select the Upload button above and choose a .csv file. This file should contain the secret keys for the OATH tokens you wish to use. The columns in the file should be: "upn, serial number, secret key, time interval, manufacturer, model".

For more information, view the public documentation.

Username: Enter a user name

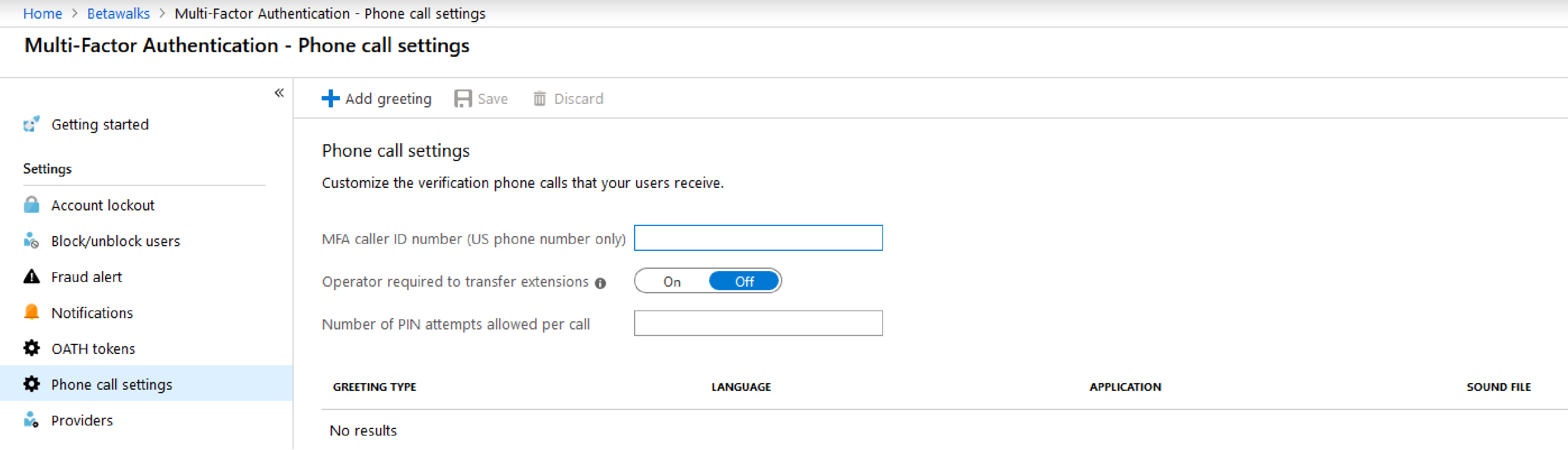
Show: All

NAME	USERNAME	SERIAL NUMBER	MODEL	MANUFACTURER	ACTIVATED
No results					

Xylos

Phone call settings

- Use custom voice messages
- User receive message in language depending on configured language for that user



Multi-Factor Authentication - Phone call settings

Phone call settings

Customize the verification phone calls that your users receive.

MFA caller ID number (US phone number only)

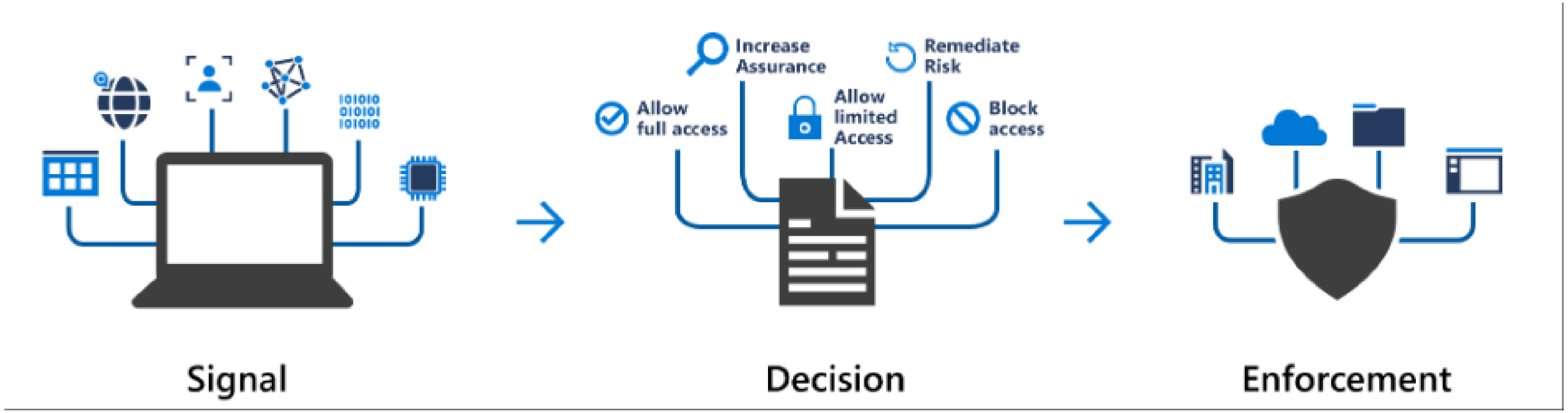
Operator required to transfer extensions: On [✓ Off]

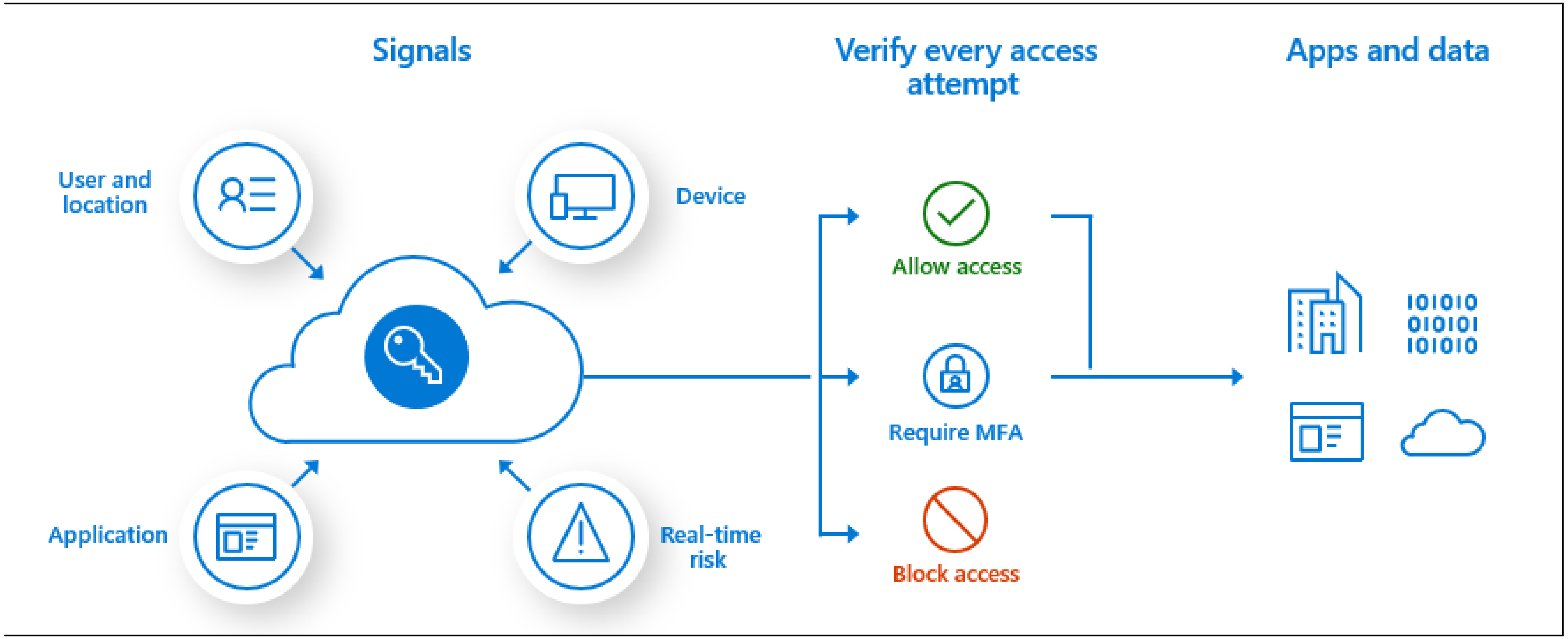
Number of PIN attempts allowed per call

GREETING TYPE	LANGUAGE	APPLICATION	SOUND FILE
No results			

Conditional Access

Conditional Access




Signals
Verify every access attempt
Apps and data
User and location
Device
Application
Real-time risk
Allow access
Require MFA
Block access
101010
010101
101010

Xylos

Common signals

- User or group membership
  - Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
- IP Location information
  - Organizations can create trusted IP address ranges that can be used when making policy decisions.
  - Administrators can specify entire countries IP ranges to block or allow traffic from.
- Device
  - Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Common signals

- Application
  - Users attempting to access specific applications can trigger different Conditional Access policies.
- Real-time and calculated risk detection
  - Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to perform password changes or multi-factor authentication to reduce their risk level or be blocked from access until an administrator takes manual action.
- Microsoft Cloud App Security (MCAS)
  - Enables user application access and sessions to be monitored and controlled in real time, increasing visibility and control over access to and activities performed within your cloud environment.

Common decisions

- Block access
  - Most restrictive decision
- Grant access
  - Least restrictive decision, can still require one or more of the following options:
    - Require multi-factor authentication
    - Require device to be marked as compliant
    - Require Hybrid Azure AD joined device
    - Require approved client app
    - Require app protection policy (preview)

Typical policies deployed by organizations

- Requiring multi-factor authentication for users with administrative roles
- Requiring multi-factor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Risk-based Conditional Access (Requires Azure AD Premium P2)
- Require trusted location for MFA registration
- Blocking or granting access from specific locations
- Require compliant device
- Requiring organization-managed devices for specific applications

Licensing

Built conditional access policies

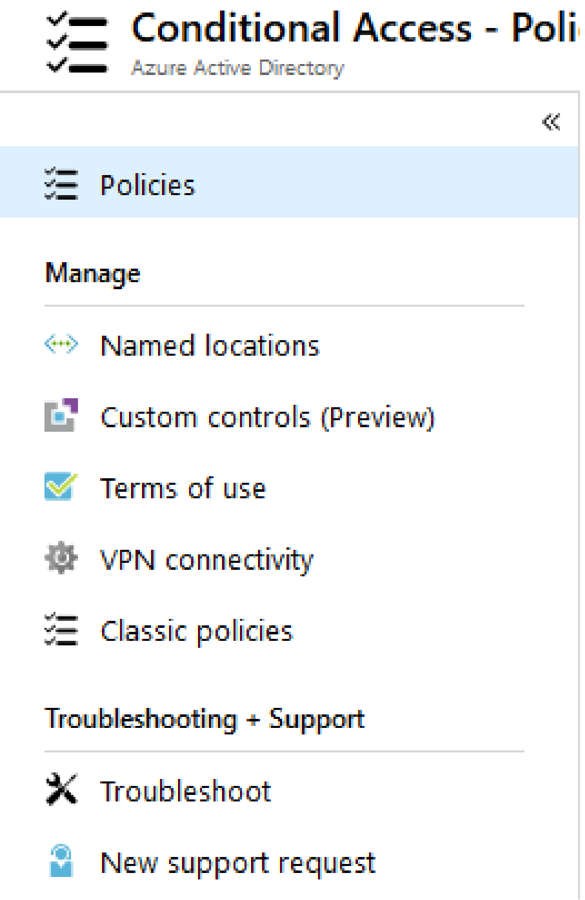
- Policies are made up of:
  - Assignments
  - Conditions
  - Controls

Policy minimum configuration requirements

- Name of the policy.
- Assignments
  - Users and/or groups to apply the policy to.
  - Cloud apps or actions to apply the policy to.
- Access controls
  - Grant or Block controls

Configuration navigation menu

- Named Locations – info in following slide
- Custom Controls - redirect authentication requests to a third party for additional Identity Management
- Terms of Use – info in following slide
- VPN Connectivity – Windows 10 feature that installs a VPN certificate provided by Azure
- Classic Policies – any remaining policies from the previous Azure Portal



Conditional Access - Poli

Azure Active Directory

«

Policies

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Classic policies

Troubleshooting + Support

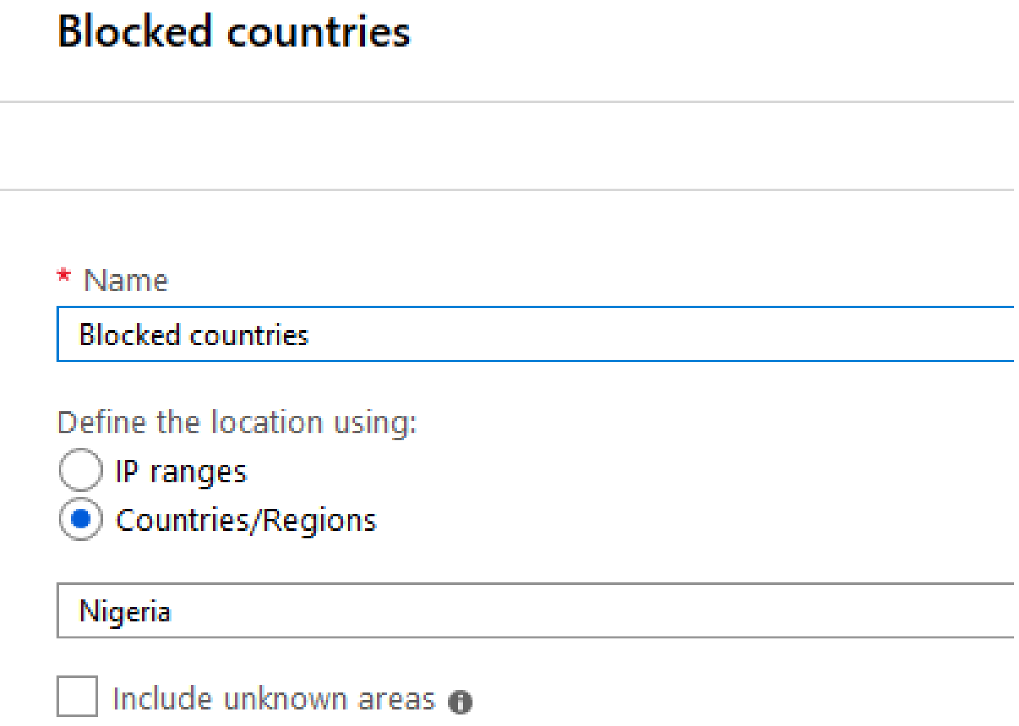
Troubleshoot

New support request

Xylos

Named locations

- Upload/Download a text file of IP ranges
- Location Name
- Use IP Ranges or Countries of Origin
- Mark as trusted to use with the All Trusted Locations setting in the Policy
- Enter IP ranges
- If Country is selected, a checkbox for unknown areas is available - IP Addresses that cannot be mapped to a country or region



Blocked countries

* Name

Blocked countries

Define the location using:

○ IP ranges

● Countries/Regions

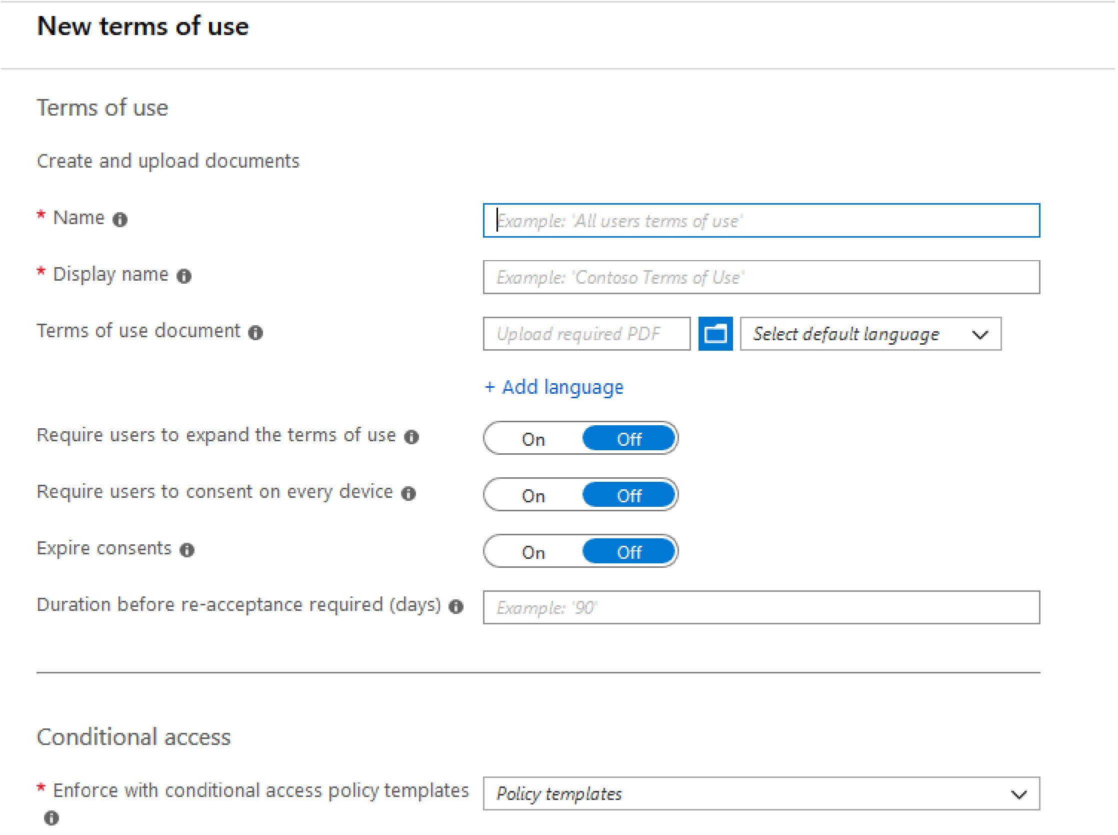
Nigeria

□ Include unknown areas

Xylos

Terms of use

- Name/Display Name
- PDF Upload
- Require users to scroll through it all
- Enforce with policy templates*
- Selected templates



New terms of use

Terms of use

Create and upload documents

* Name	Example: 'All users terms of use'
* Display name	Example: 'Contoso Terms of Use'
Terms of use document	Upload required PDF · Select default language
	+ Add language
Require users to expand the terms of use	On [✓ Off]
Require users to consent on every device	On [✓ Off]
Expire consents	On [✓ Off]
Duration before re-acceptance required (days)	Example: '90'

Conditional access

* Enforce with conditional access policy templates	Policy templates

*Selecting Create a policy and Access to cloud apps enforces the terms of use for all users and all cloud apps

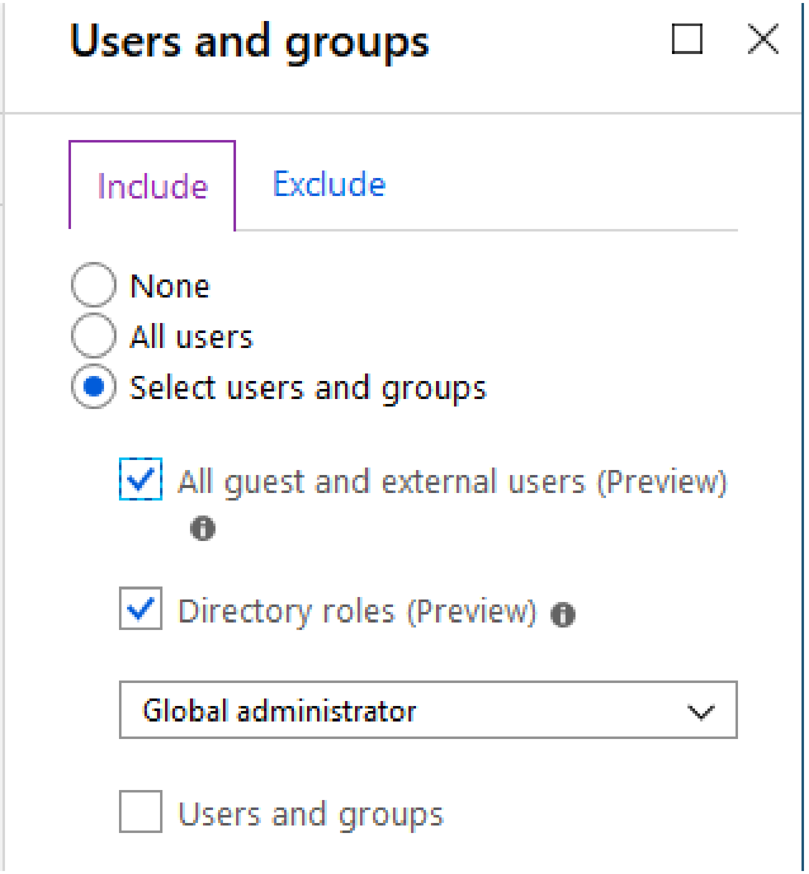
Assignments

The assignments portion controls the who, what, and where of the Conditional Access policy

Xylos

Users & Groups

- Include or Exclude
- All Users
- Selection of
  - All guest users
  - Directory roles
  - Users and/or groups



Users and groups

Include | Exclude

○ None
○ All users
● Select users and groups

☑ All guest and external users (Preview)

☑ Directory roles (Preview)

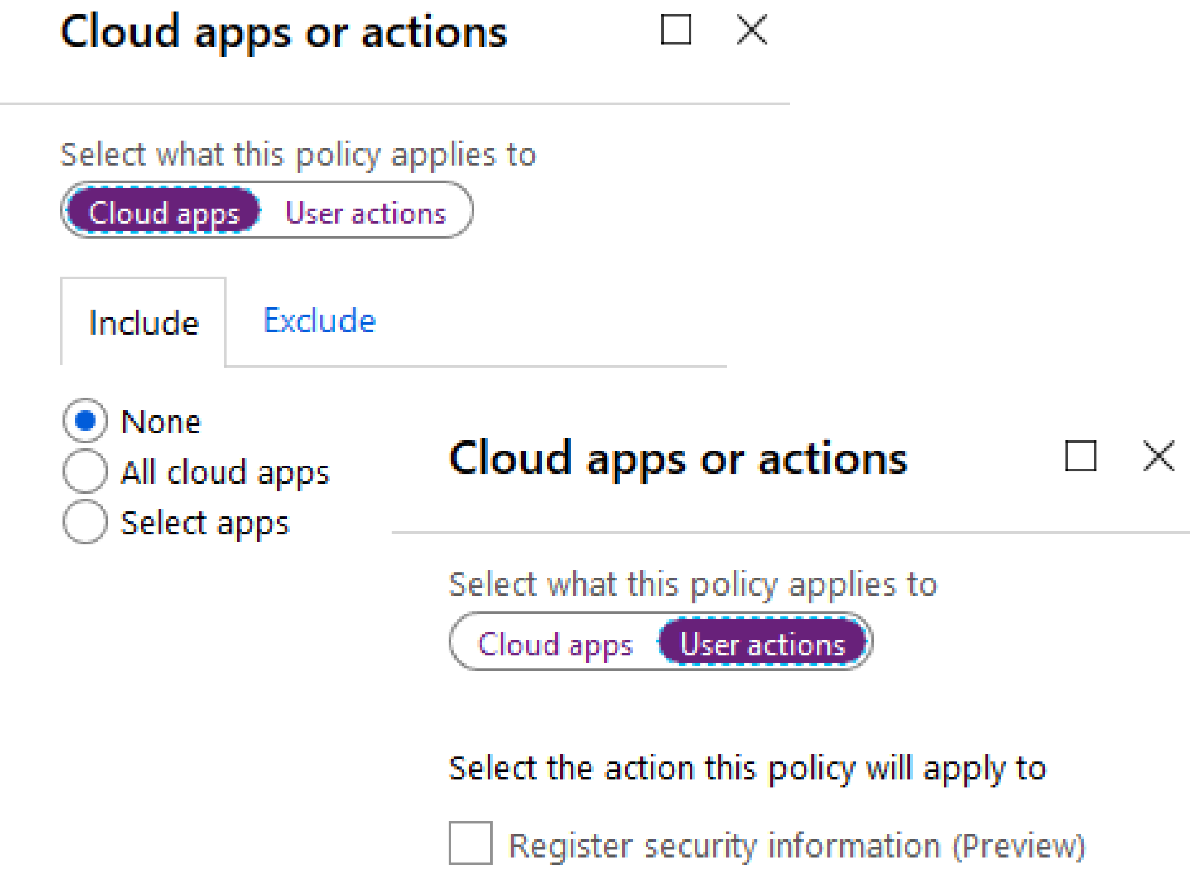
Global administrator

□ Users and groups

Xylos

Cloud apps or User actions

- Include or Exclude
- All cloud apps (Includes Default, Intune and Azure Gallery Apps)
- Select individual apps
- User actions



Cloud apps or actions

Select what this policy applies to

● None
○ All cloud apps
○ Select apps

Cloud apps or actions

Select what this policy applies to

Select the action this policy will apply to

□ Register security information (Preview)

Conditions

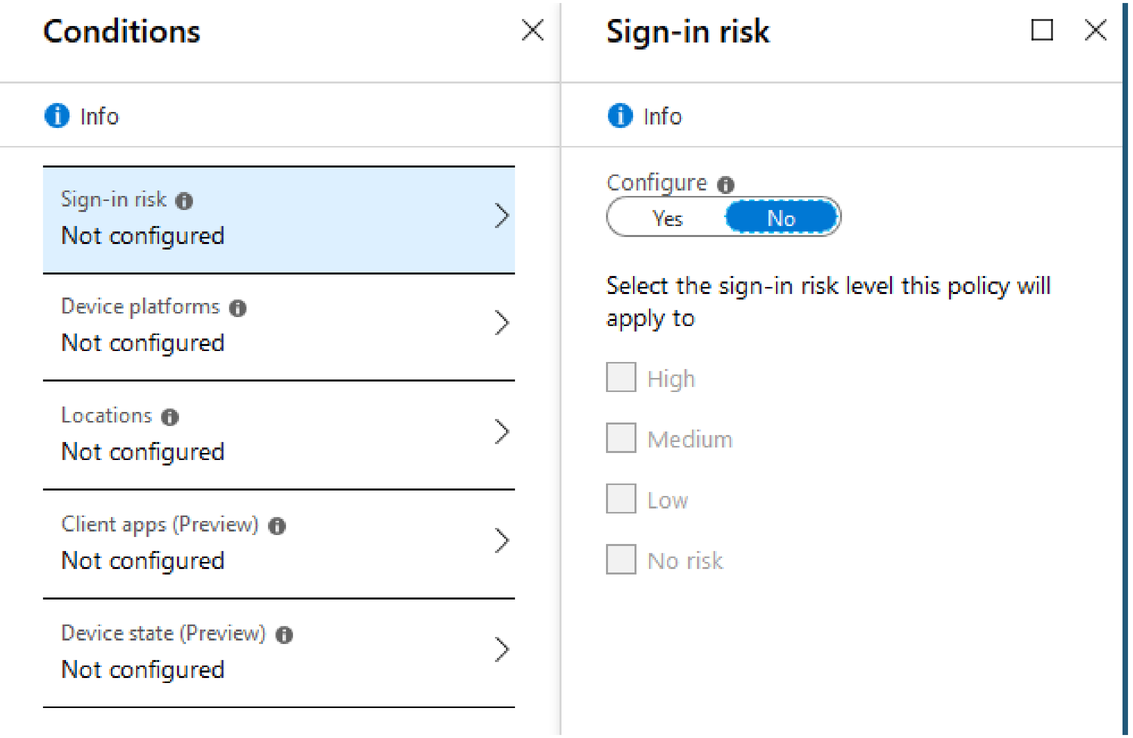
A policy can contain multiple conditions.

Conditions

- Sign-in Risk
- Device Platforms
- Locations
- Client apps
- Device state

Sign-in Risk

- Configure Yes/No
- Select Risk Level (defined on next slide)



Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (Preview)
Not configured

Device state (Preview)
Not configured

Sign-in risk

Info

Configure
Yes [✓ No]

Select the sign-in risk level this policy will apply to

□ High

□ Medium

□ Low

□ No risk

How sign-in risk is determined

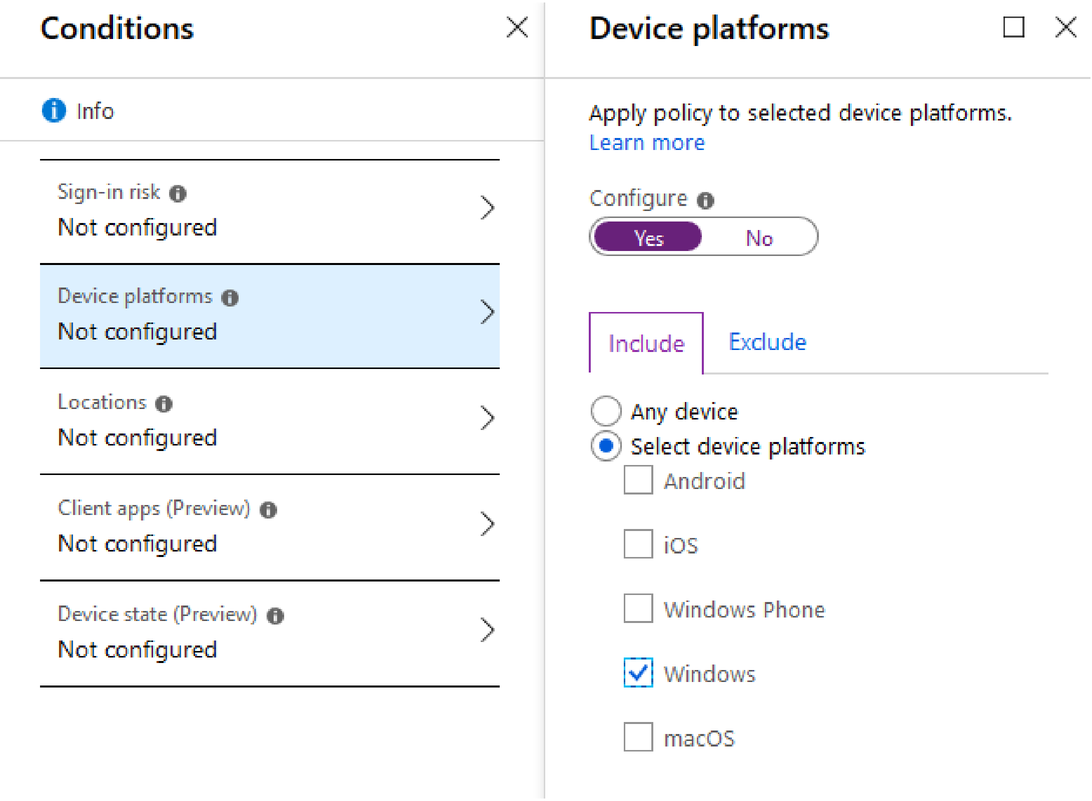
- **High**: High confidence and high severity risk event. These events are strong indicators that the user’s identity has been compromised, and any user accounts impacted should be remediated immediately.
- Medium: High severity, but lower confidence risk event, or vice versa. These events are potentially risky, and any user accounts impacted should be remediated.
- Low: Low confidence and low severity risk event. This event may not require an immediate action, but when combined with other risk events, may provide a strong indication that the identity is compromised.

Examples of Event Levels

- Leaked credentials – High
- Sign-ins from anonymous IP Addresses – Medium
- Impossible Travel to atypical locations – Medium
- Sign-in from unfamiliar locations – Medium
- Sign-ins from infected devices – Low
- Sign-ins from IP addresses with suspicious activity – Medium

Device platforms

- Configure Yes/No
- Include/Exclude
- Any device
- Selection of device platforms



Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (Preview)
Not configured

Device state (Preview)
Not configured

Device platforms

Apply policy to selected device platforms.
Learn more

Configure: [✓ Yes] No

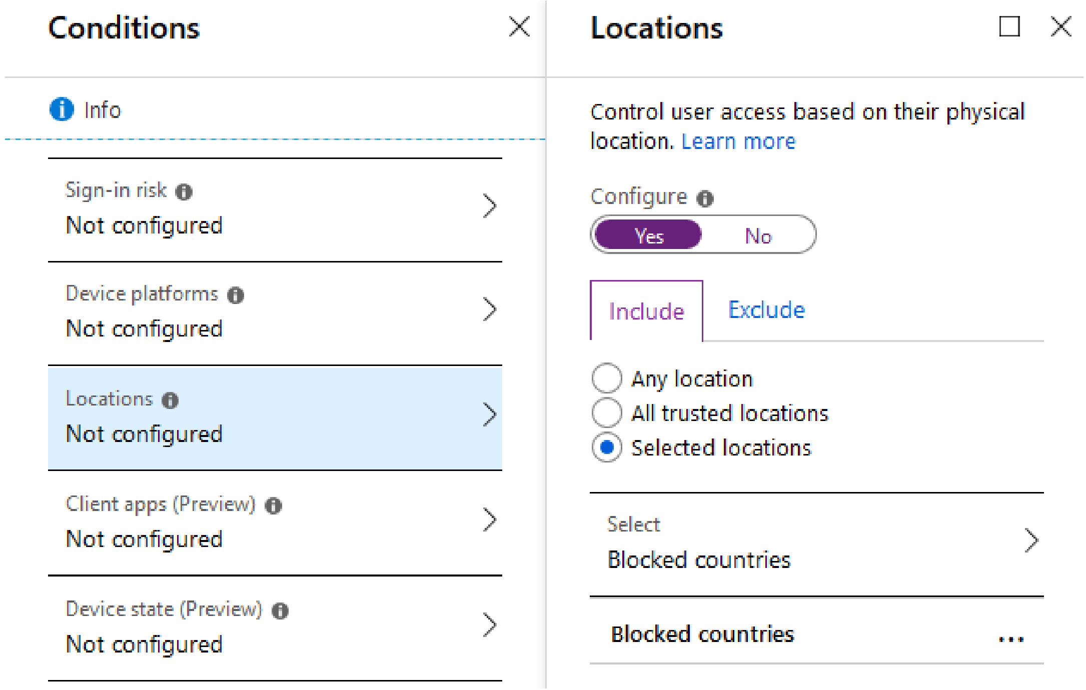
Include | Exclude

○ Any device
● Select device platforms
□ Android
□ iOS
□ Windows Phone
☑ Windows
□ macOS

Xylos

Locations

- Configure Yes/No
- Include/Exclude
- Any location
- All trusted locations
- Selected locations



Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (Preview)
Not configured

Device state (Preview)
Not configured

Locations

Control user access based on their physical location. Learn more

Configure
[✓ Yes] No

[✓ Include] Exclude

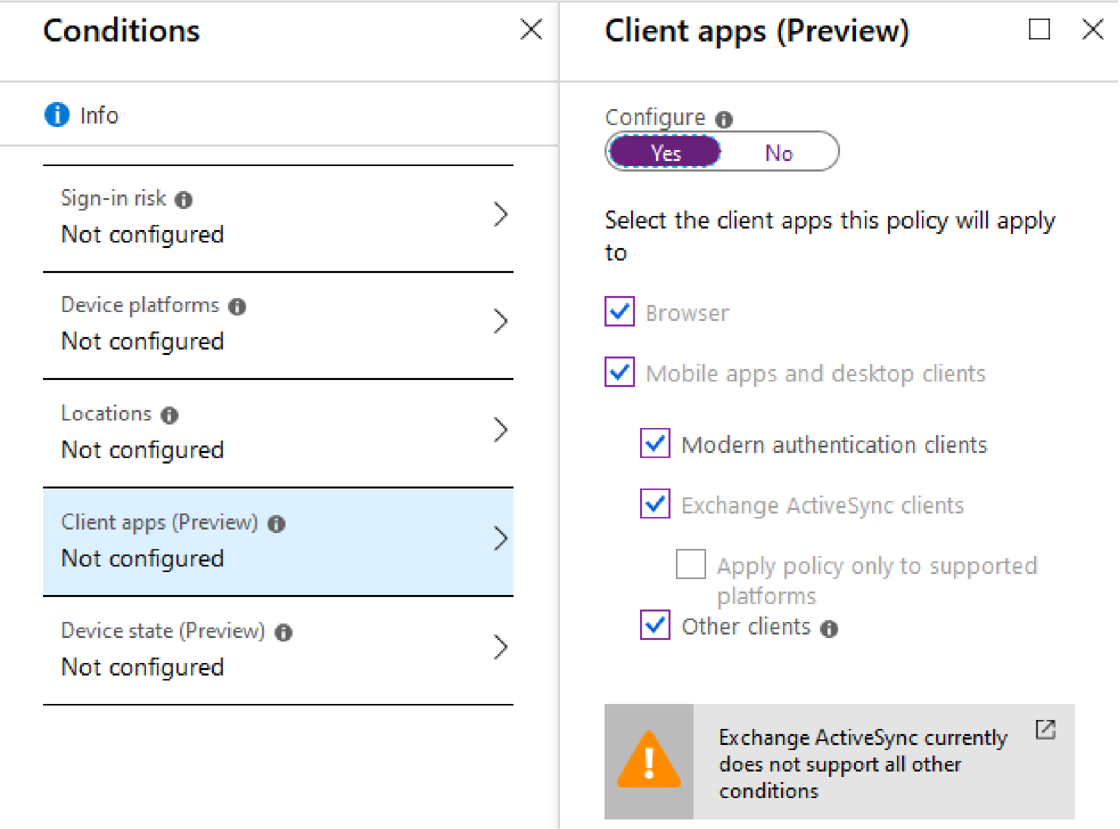
○ Any location
○ All trusted locations
● Selected locations

Select
Blocked countries

Blocked countries ...

Client apps

- Configure Yes/No
- Include/Exclude
- Browser
- Mobile apps and desktop clients
  - Modern authentication
  - Exchange ActiveSync clients
  - Other clients



Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (Preview)
Not configured

Device state (Preview)
Not configured

Client apps (Preview)

Configure
[✓ Yes] No

Select the client apps this policy will apply to

☑ Browser

☑ Mobile apps and desktop clients

☑ Modern authentication clients

☑ Exchange ActiveSync clients

□ Apply policy only to supported platforms

☑ Other clients

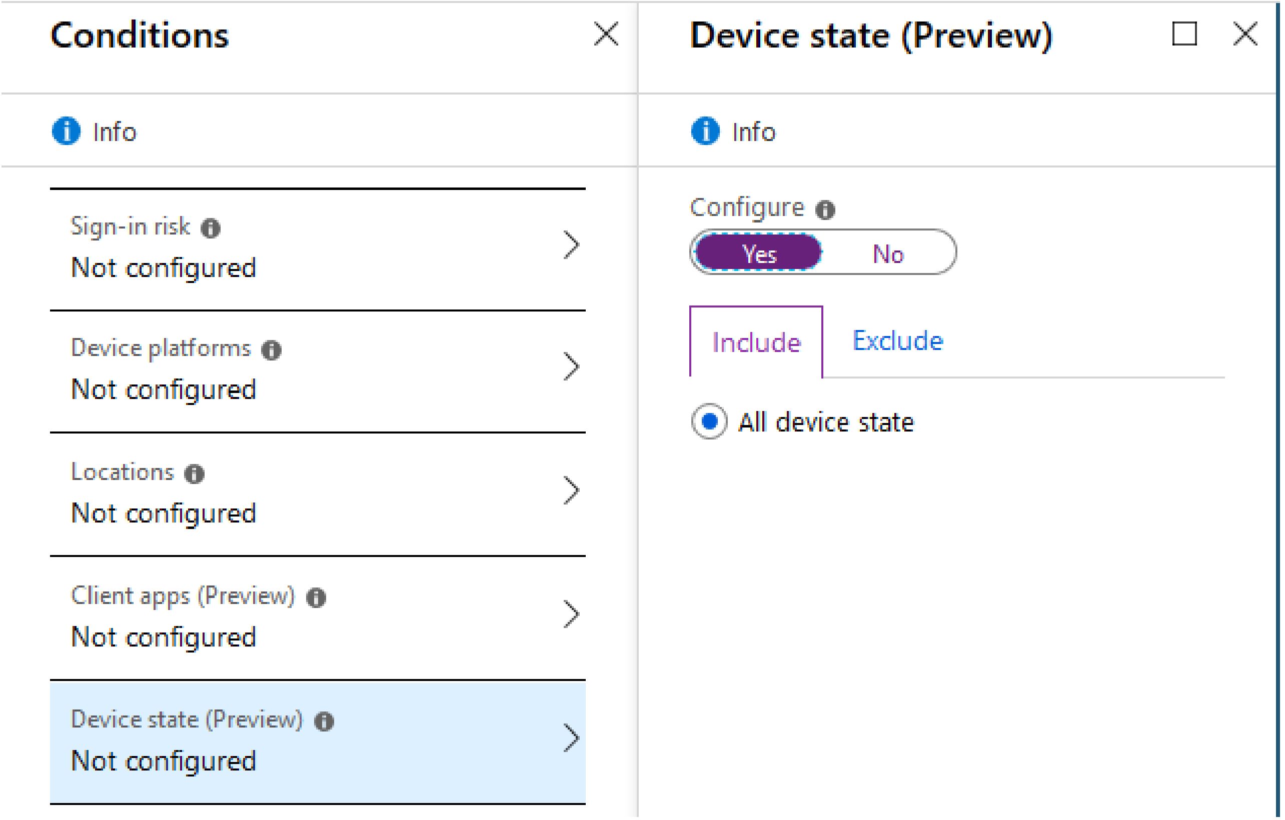
Exchange ActiveSync currently does not support all other conditions

Xylos

Device state

- Configure Yes/No
- Include/Exclude
- All device state

- Exclude
  - Hybrid joined devices
  - Compliant devices



Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (Preview)
Not configured

Device state (Preview)
Not configured

Device state (Preview)

Info

Configure
[✓ Yes] No

Include | Exclude

● All device state

Xylos

Access controls

The access controls portion of the Conditional Access policy controls how a policy is enforced.

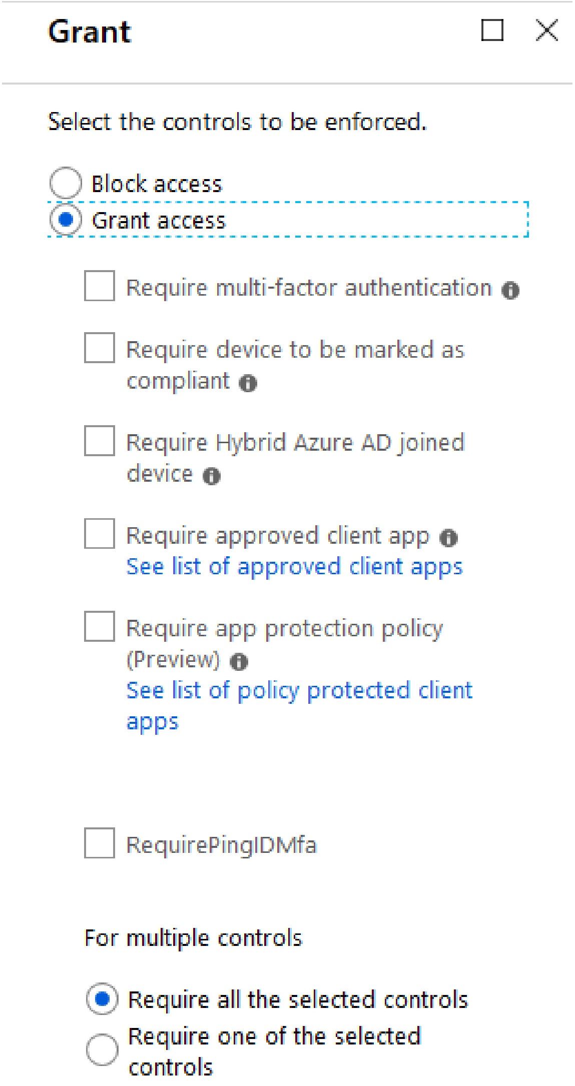
Access controls

- Block access
- Grant access
  - Require multi-factor authentication (Azure Multi-Factor Authentication)
  - Require device to be marked as compliant (Intune)
  - Require Hybrid Azure AD joined device
  - Require approved client app
  - Require app protection policy

- Session
  - Use app enforced restrictions
  - Use Conditional Access App Control
  - Sign-in frequency
  - Persistent browser session

Grant controls

- Grant/Block
- Require MFA
- Require Compliant - an iOS and Android device compliance policy in Intune
  - Specifies password requirements, versions, conditions
- Require Hybrid Azure AD joined - requires additional configuration on Azure AD Connect
- Require approved Client App - currently Microsoft Apps like Office 2016, and apps configured in Intune
- Require app protection policy



Grant

Select the controls to be enforced.

○ Block access
● Grant access

□ Require multi-factor authentication

□ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy (Preview)
See list of policy protected client apps

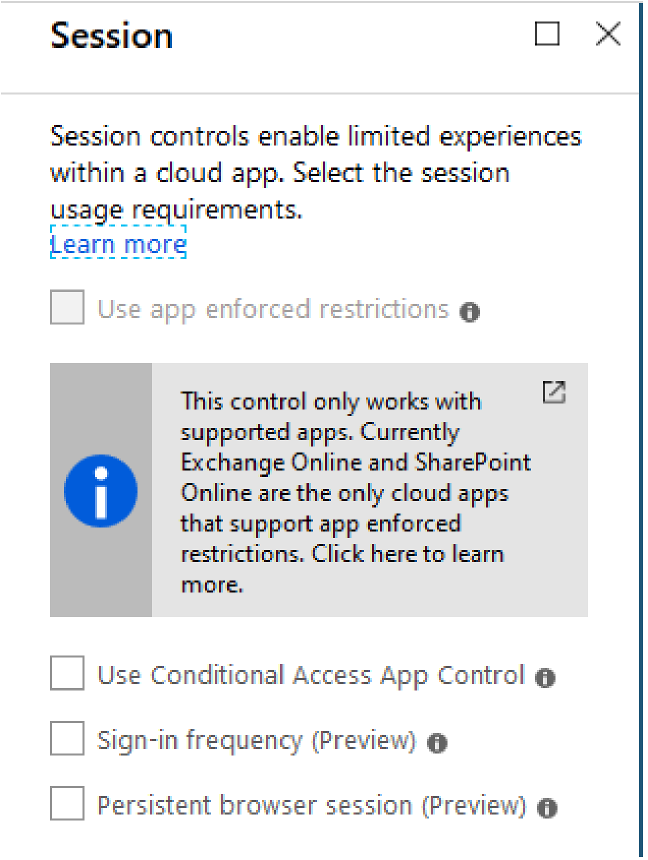
□ RequirePingIDMfa

For multiple controls

● Require all the selected controls
○ Require one of the selected controls

Session controls

- App enforced restrictions
- Use conditional access app control
- Sign-in frequency
- Persistent browser session



Session

Session controls enable limited experiences within a cloud app. Select the session usage requirements.
Learn more

□ Use app enforced restrictions

This control only works with supported apps. Currently Exchange Online and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

□ Use Conditional Access App Control

□ Sign-in frequency (Preview)

□ Persistent browser session (Preview)

Xylos

Best Practices

As a best practice, create a user account that is:

- Dedicated to policy administration
- Excluded from all your policies

Avoid doing

For all users, all cloud apps:

- Block access - This configuration blocks your entire organization, which is definitely not a good idea.
- Require compliant device - For users that have not enrolled their devices yet, this policy blocks all access including access to the Intune portal.
- Require domain join - This policy block access has also the potential to block access for all users in your organization if you don't have a domain-joined device yet.
- Require app protection policy - This policy block access has also the potential to block access for all users in your organization if you don't have an Intune policy.

For all users, all cloud apps, all device platforms:

- Block access - This configuration blocks your entire organization, which is definitely not a good idea.

Troubleshooting

- Simulate sign-in behavior with the conditional access What if tool
- Azure Active Directory user sign-in logs

DEMO

Questions?

Xylos

care.grow.passion.

Xylos