HAROLD BAELE – MICROSOFT CLOUD TECHNICAL CONSULTANT
- MICROSOFT CERTIFIED TRAINER

Security & Identity

REALDOLMEN
a Gfi Group company

Office 365™
For the ICT administrator

Azure Active Directory ?

Identity types in AAD ?

To get there, together

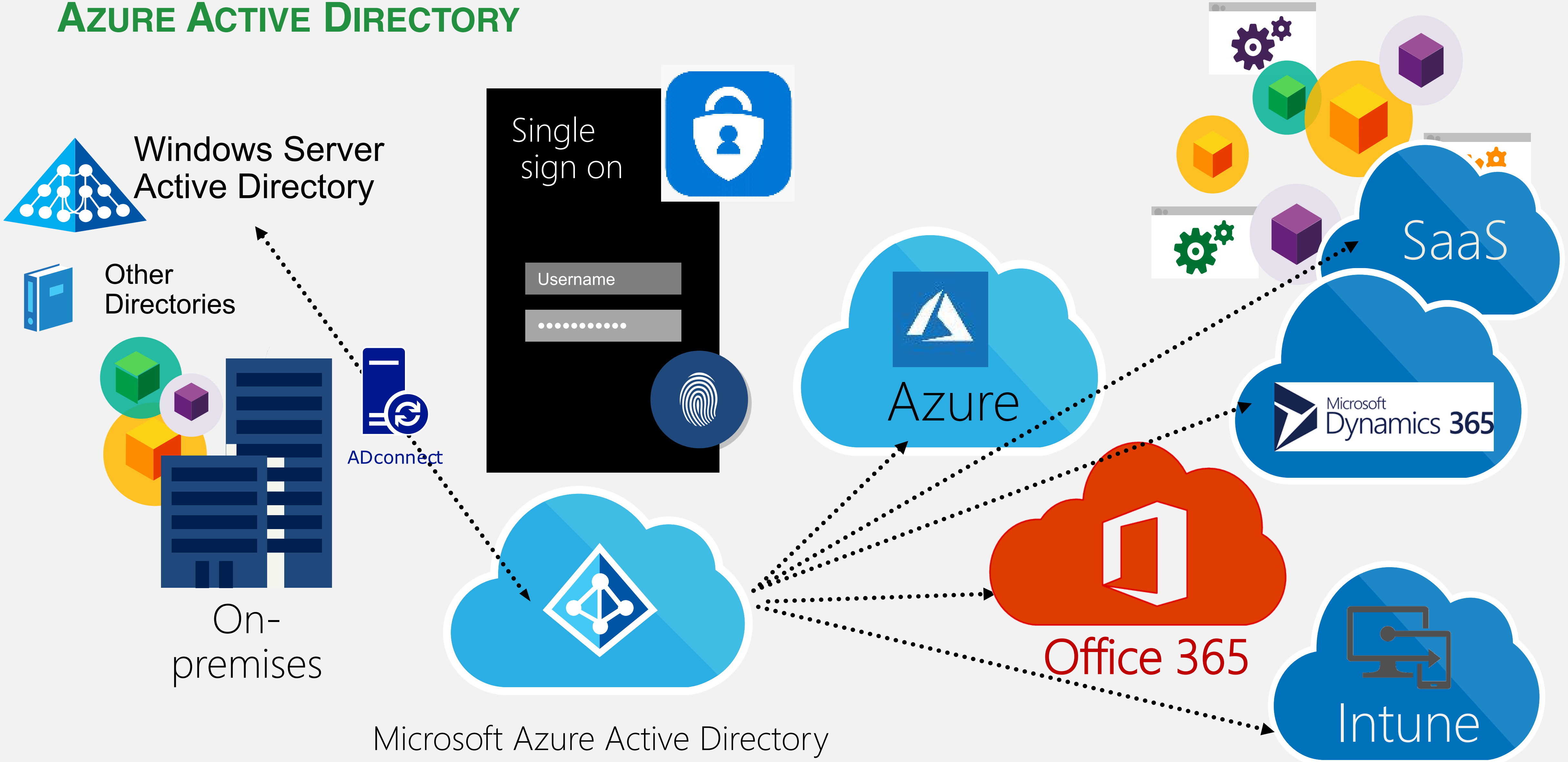
AAD Multi Factor Authentication

Self Service Password Reset
& Password write back

REALDOLMEN
a Gfi Group company

Azure Active Directory ?

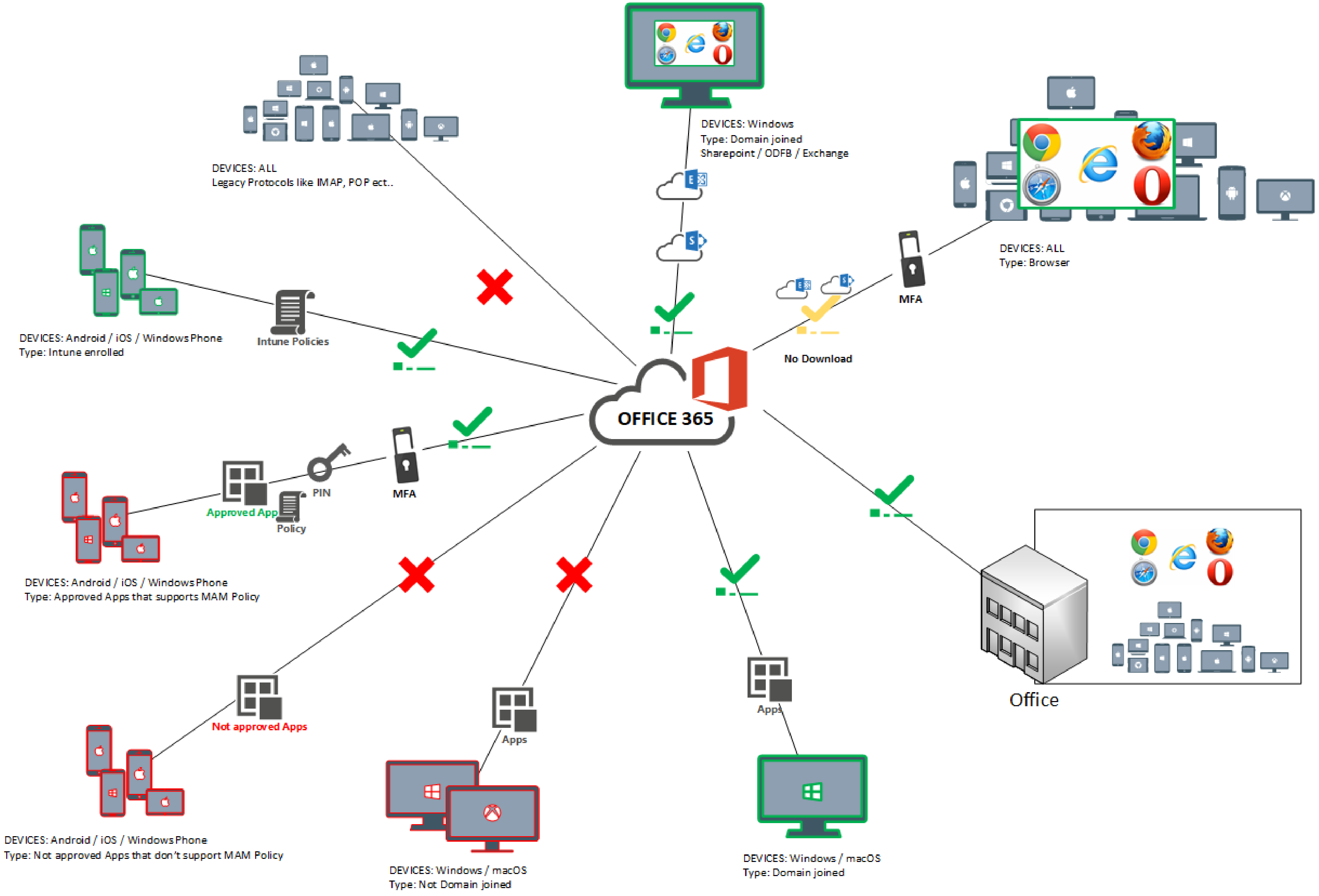
Azure Active Directory



Azure Tenants, Azure Subscriptions & Accounts

- Creating an Azure/O365/Intune subscription means creating/using a Tenant
- A tenant is defined by something.onmicrosoft.com
- Can contain one or more accepted domains like contoso.com
- Defines the users who have access to the resources of the subscription
- Can contain Guest Accounts or AAD accounts

https://azure.microsoft.com/en-us/documentation/articles/active-directory-howto-tenant/
https://azure.microsoft.com/en-us/documentation/articles/active-directory-how-subscriptions-associated-directory/



DEVICES: ALL
Legacy Protocols like IMAP, POP ect..

DEVICES: Windows
Type: Domain joined
Sharepoint / ODFB / Exchange

DEVICES: ALL
Type: Browser

MFA

No Download

DEVICES: Android / iOS / Windows Phone
Type: Intune enrolled

Intune Policies

OFFICE 365

Approved App

Policy

PIN

MFA

DEVICES: Android / iOS / Windows Phone
Type: Approved Apps that supports MAM Policy

Office

Not approved Apps

Apps

Apps

DEVICES: Android / iOS / Windows Phone
Type: Not approved Apps that don't support MAM Policy

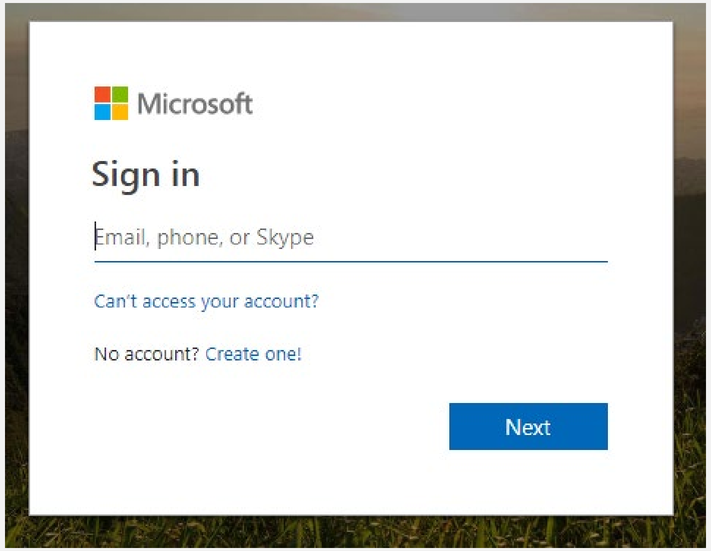
DEVICES: Windows / macOS
Type: Not Domain joined

DEVICES: Windows / macOS
Type: Domain joined

https://www.linkedin.com/in/daniel-nitz-943a50112 /

Identity types in AAD ?

Microsoft Cloud Identity Models



Microsoft

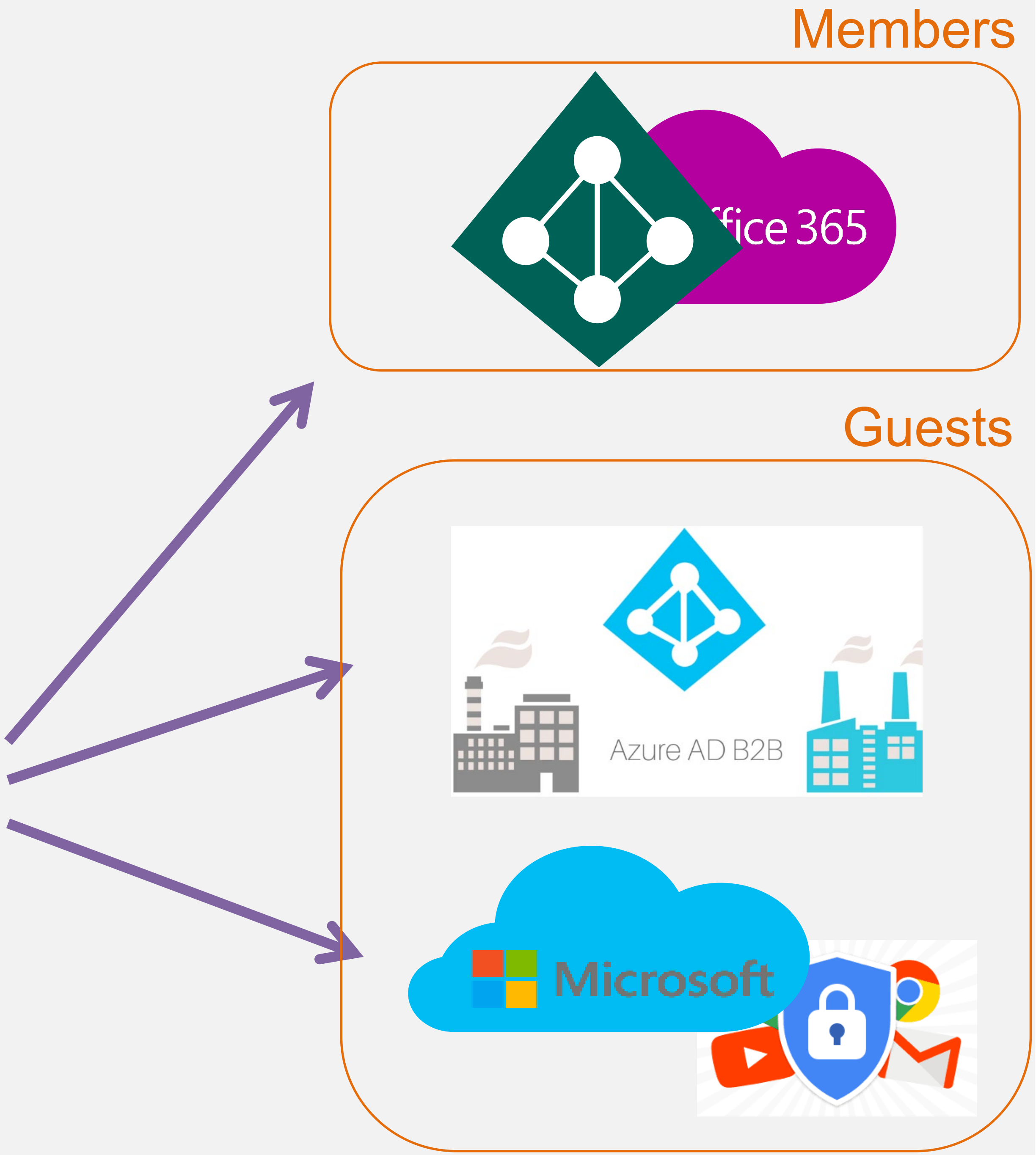
Sign in

Email, phone, or Skype

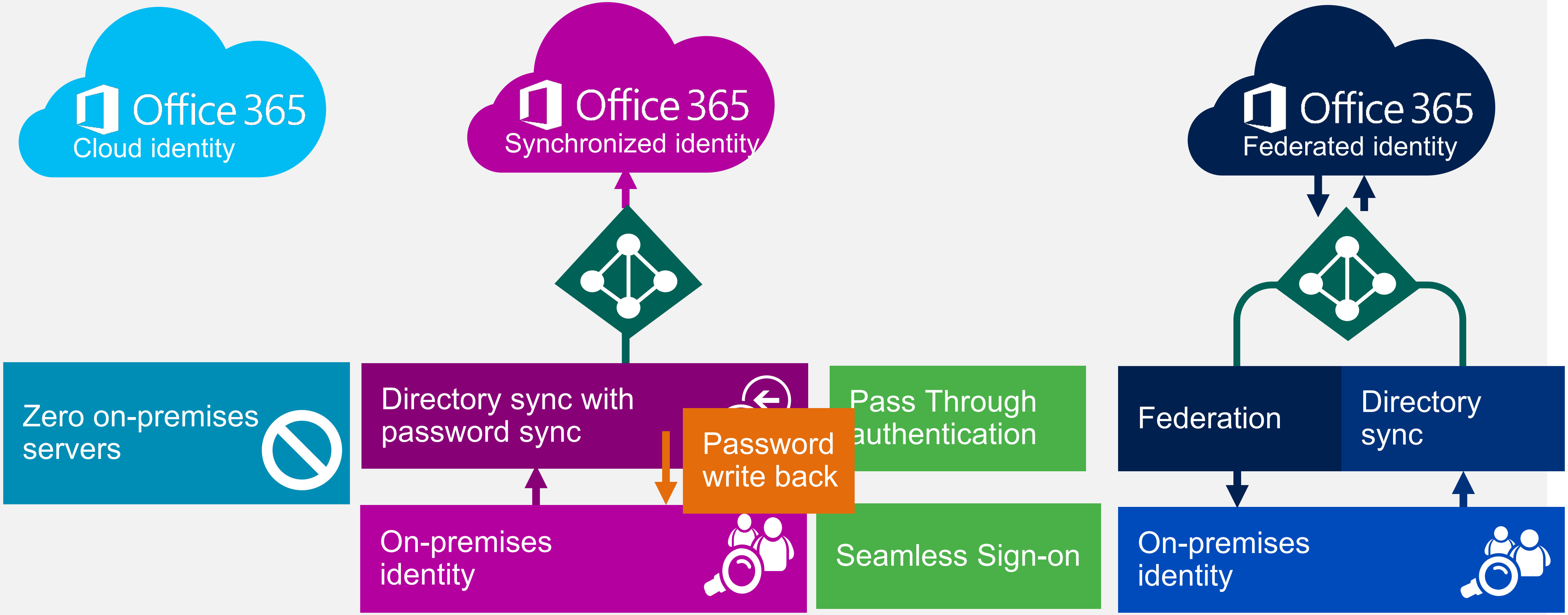
Can't access your account?

No account? Create one!

Next



Azure Active Directory Identity Models



Office 365
Cloud identity

Office 365
Synchronized identity

Office 365
Federated identity

Zero on-premises servers

Directory sync with password sync

Password write back

Pass Through authentication

Seamless Sign-on

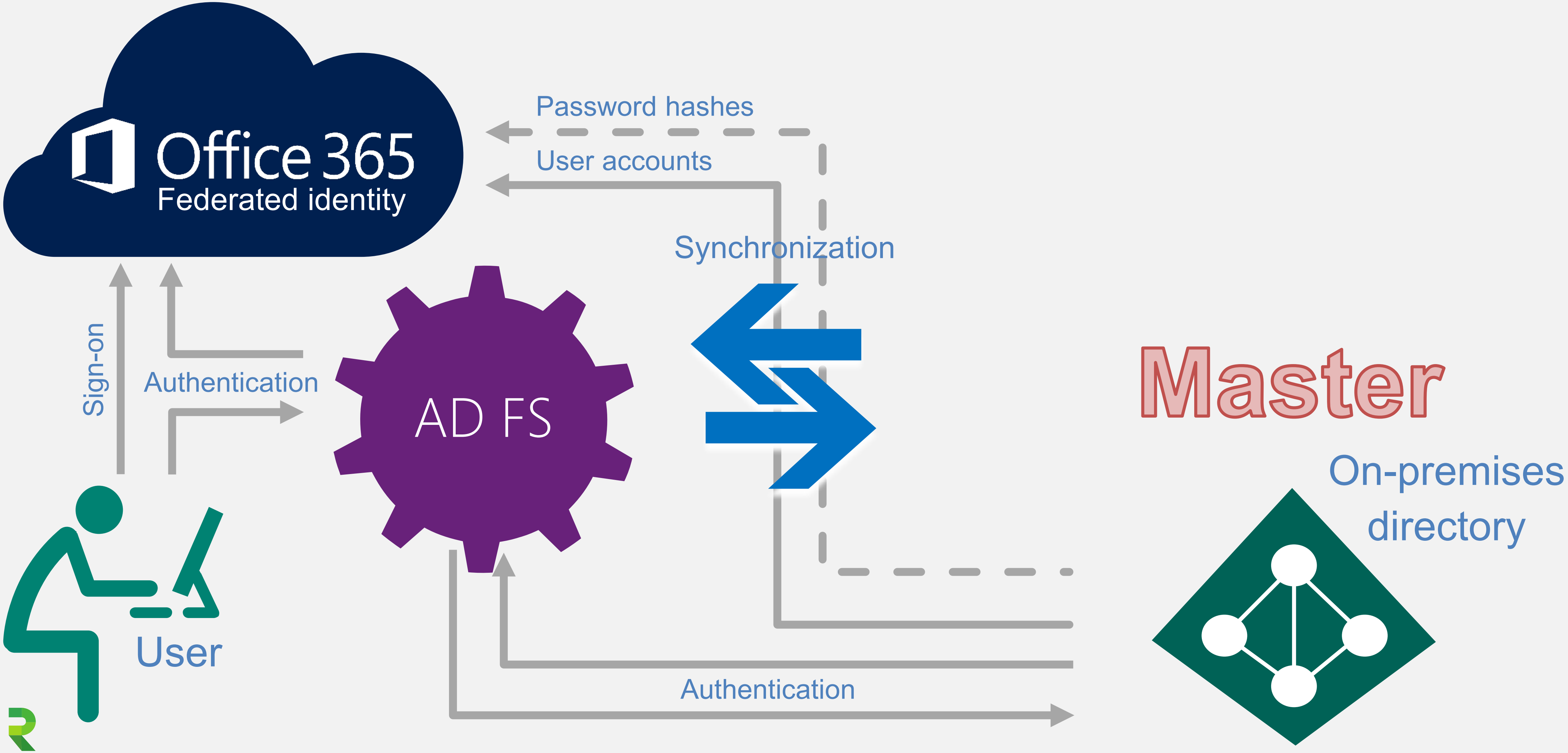
On-premises identity

Federation

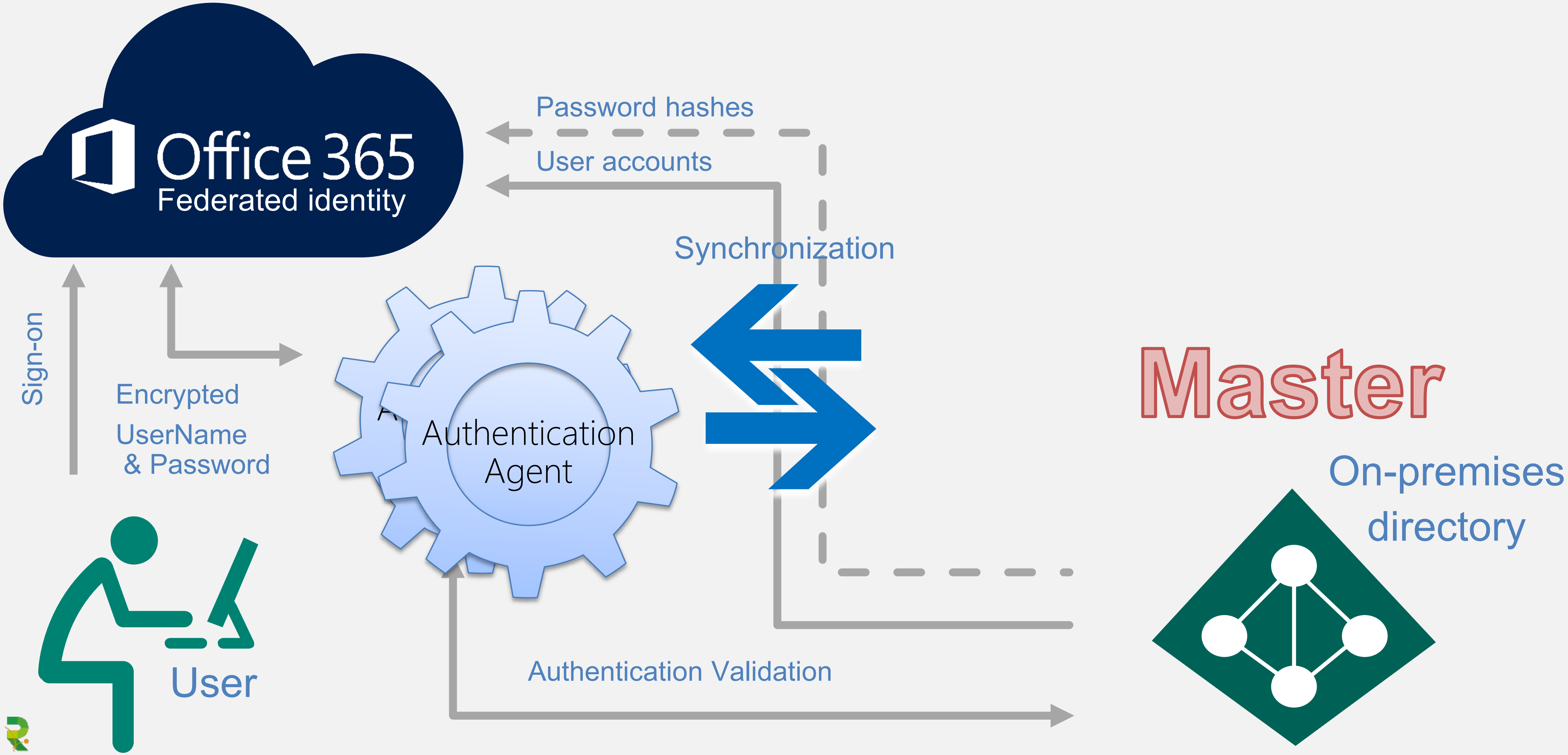
Directory sync

On-premises identity

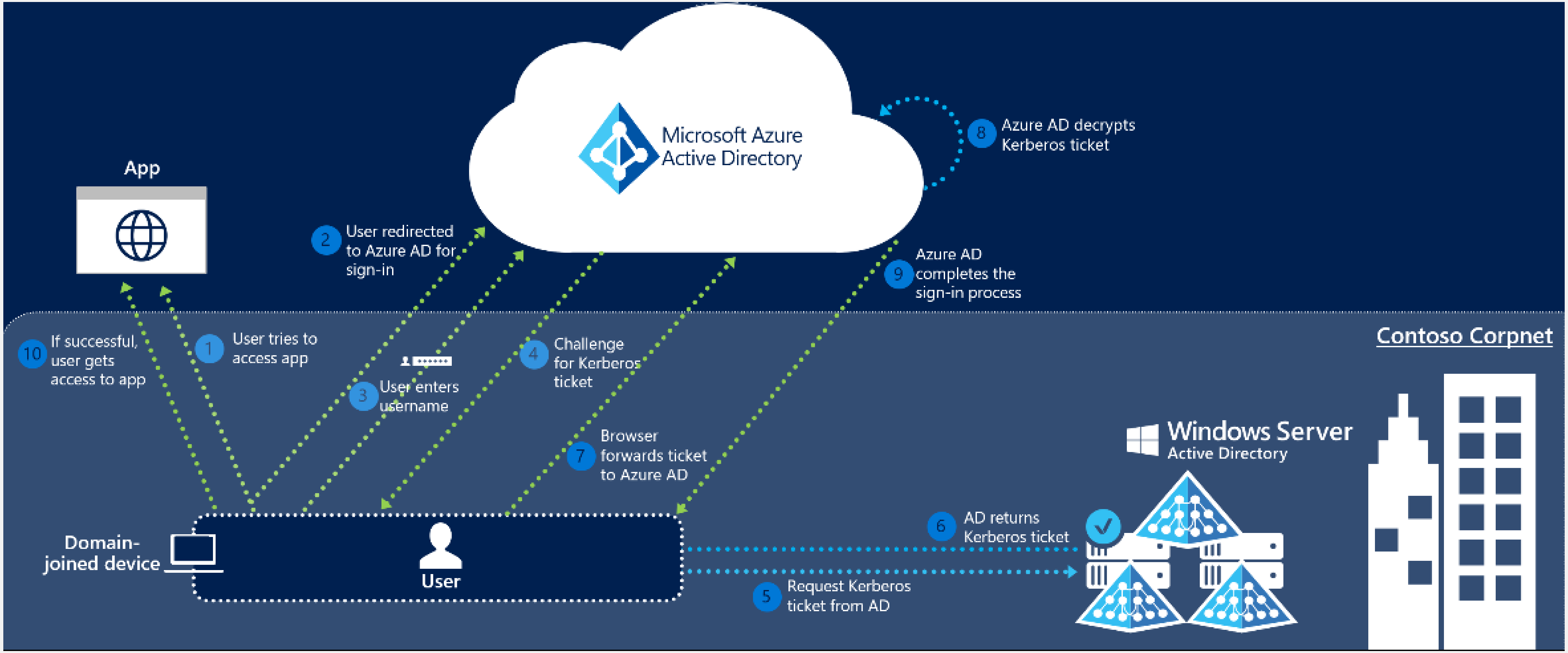
Federated identity model



Pass Through Sign-On identity model

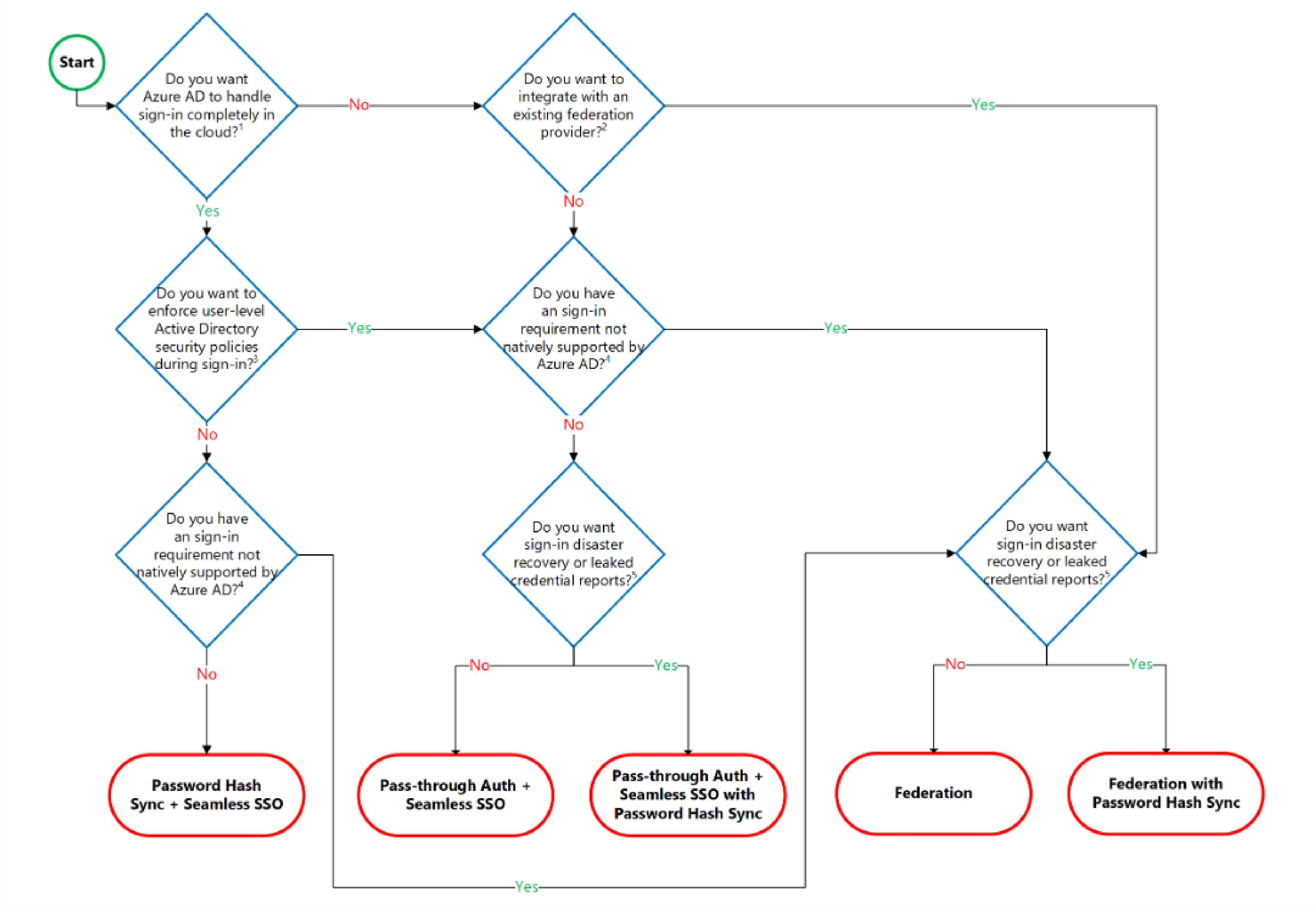


Optional Seamless Sign-On for Domain Joined devices



Microsoft Azure
Active Directory
8 Azure AD decrypts Kerberos ticket
App
2 User redirected to Azure AD for sign-in
9 Azure AD completes the sign-in process
Contoso Corpnet
10 If successful, user gets access to app
1 User tries to access app
3 User enters username
4 Challenge for Kerberos ticket
7 Browser forwards ticket to Azure AD
Windows Server
Active Directory
6 AD returns Kerberos ticket
5 Request Kerberos ticket from AD
Domain-joined device
User

AUTHENTICATION METHODS – DECISION TREE



Start

Do you want Azure AD to handle sign-in completely in the cloud?[1]

Do you want to integrate with an existing federation provider?[2]

Do you want to enforce user-level Active Directory security policies during sign-in?[3]

Do you have an sign-in requirement not natively supported by Azure AD?[4]

Do you have an sign-in requirement not natively supported by Azure AD?[4]

Do you want sign-in disaster recovery or leaked credential reports?[5]

Do you want sign-in disaster recovery or leaked credential reports?[5]

Yes

No

Password Hash Sync + Seamless SSO

Pass-through Auth + Seamless SSO

Pass-through Auth + Seamless SSO with Password Hash Sync

Federation

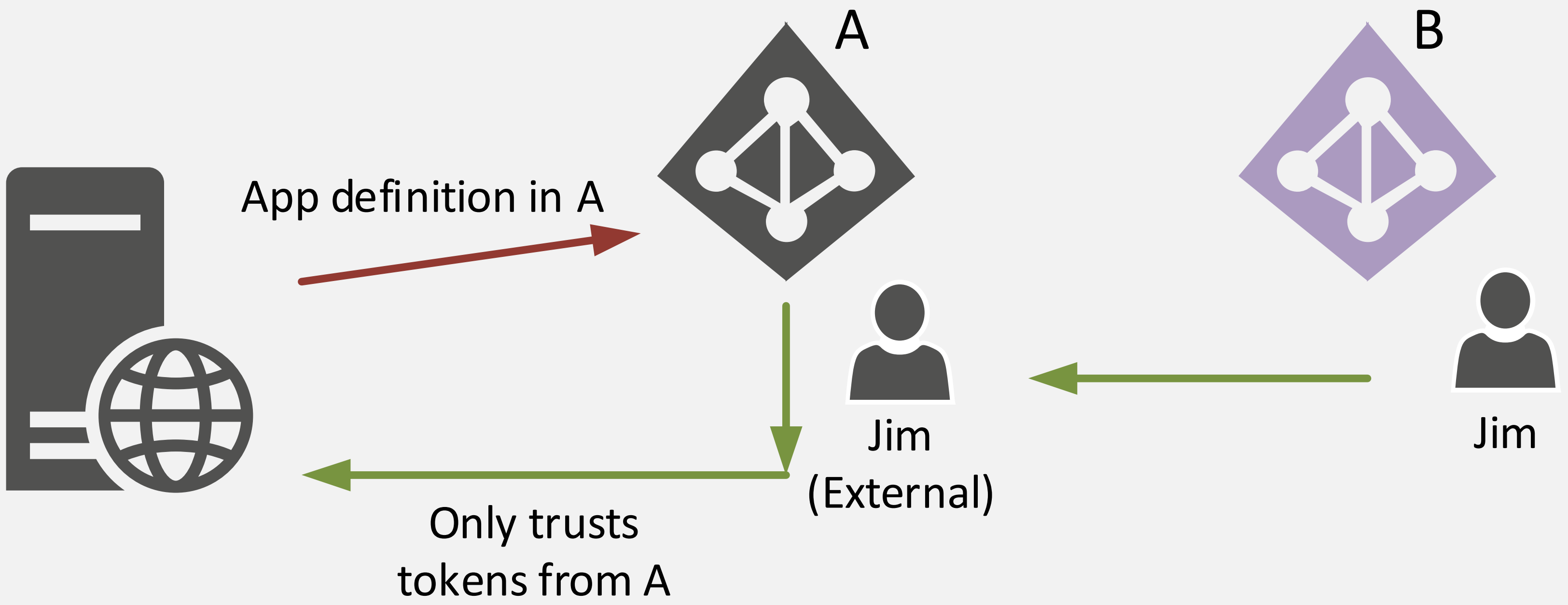
Federation with Password Hash Sync

Azure AD B2B – Guest Access

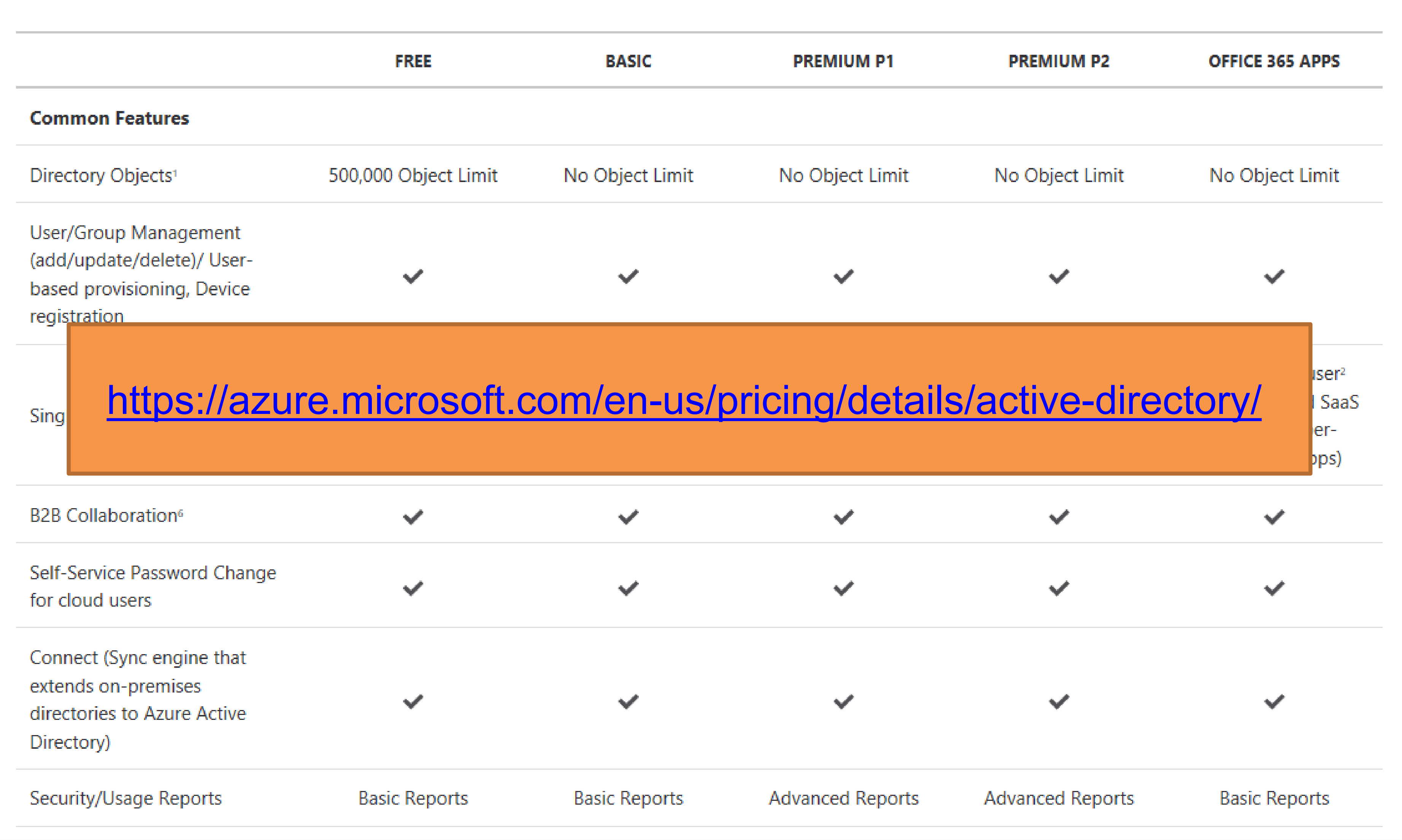
- Extension on Azure Active Directory
- Allowing authorizing external users on any Microsoft Cloud services

- General licensing principal 1:5 ratio

- User of tenant B is represented as **guest user** in tenant A
- User profile, group membership and application assignment is done in tenant A



Extending Features with AAD premium



	FREE	BASIC	PREMIUM P1	PREMIUM P2	OFFICE 365 APPS
Common Features					
Directory Objects[1]	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit	No Object Limit
User/Group Management (add/update/delete)/ User-based provisioning, Device registration	✓	✓	✓	✓	✓
Sing					ser[2] SaaS er- ps)
B2B Collaboration[6]	✓	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓	✓
Connect (Sync engine that extends on-premises directories to Azure Active Directory)	✓	✓	✓	✓	✓
Security/Usage Reports	Basic Reports	Basic Reports	Advanced Reports	Advanced Reports	Basic Reports

https://azure.microsoft.com/en-us/pricing/details/active-directory/

AAD Multi Factor Authentication

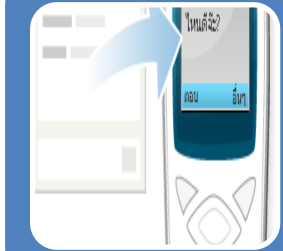
AZURE MFA OPTIONS

Microsoft Authenticator app

- App which generates a code
- App ask for approval

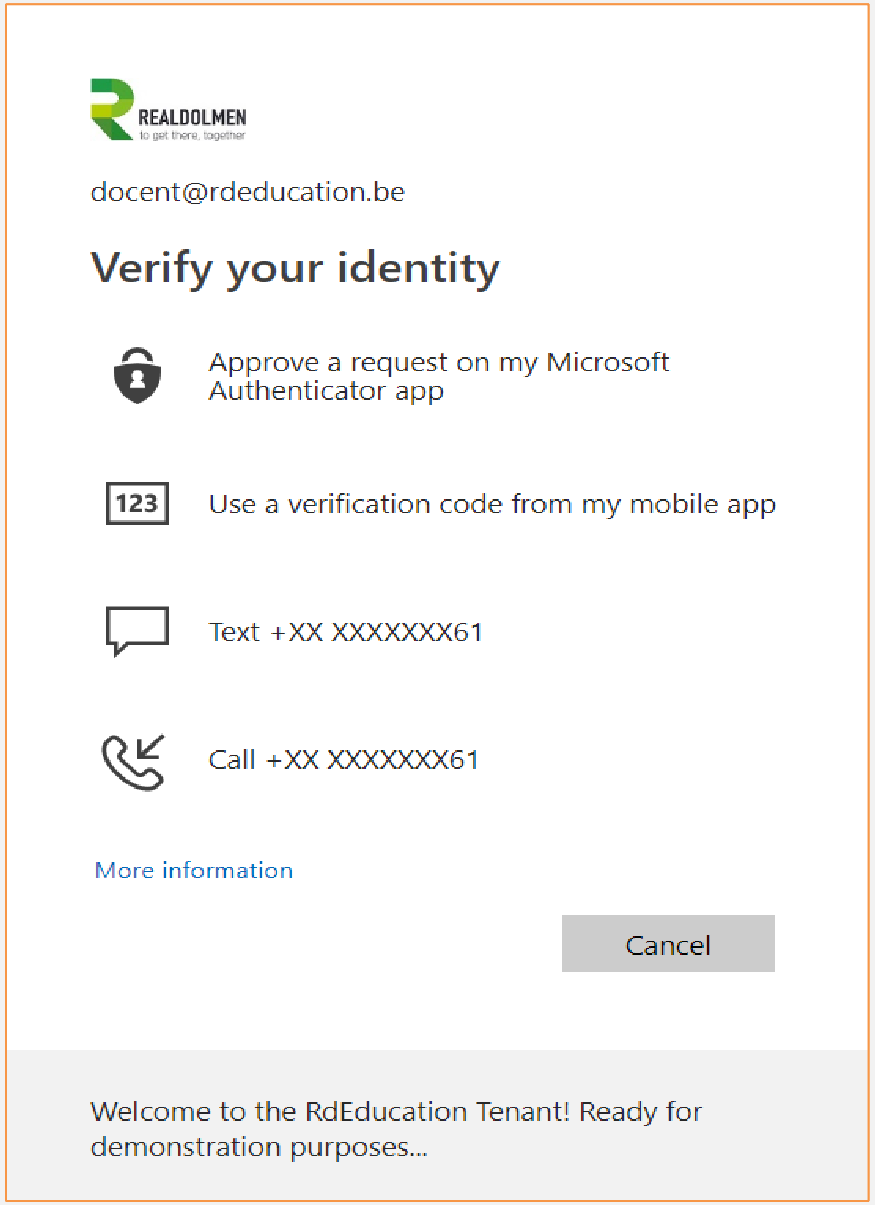
Phone call

- Phone call asking confirmation with a #



SMS

- Small sms message with code



REALDOLMEN
to get there, together

docent@rdeducation.be

Verify your identity

Approve a request on my Microsoft Authenticator app

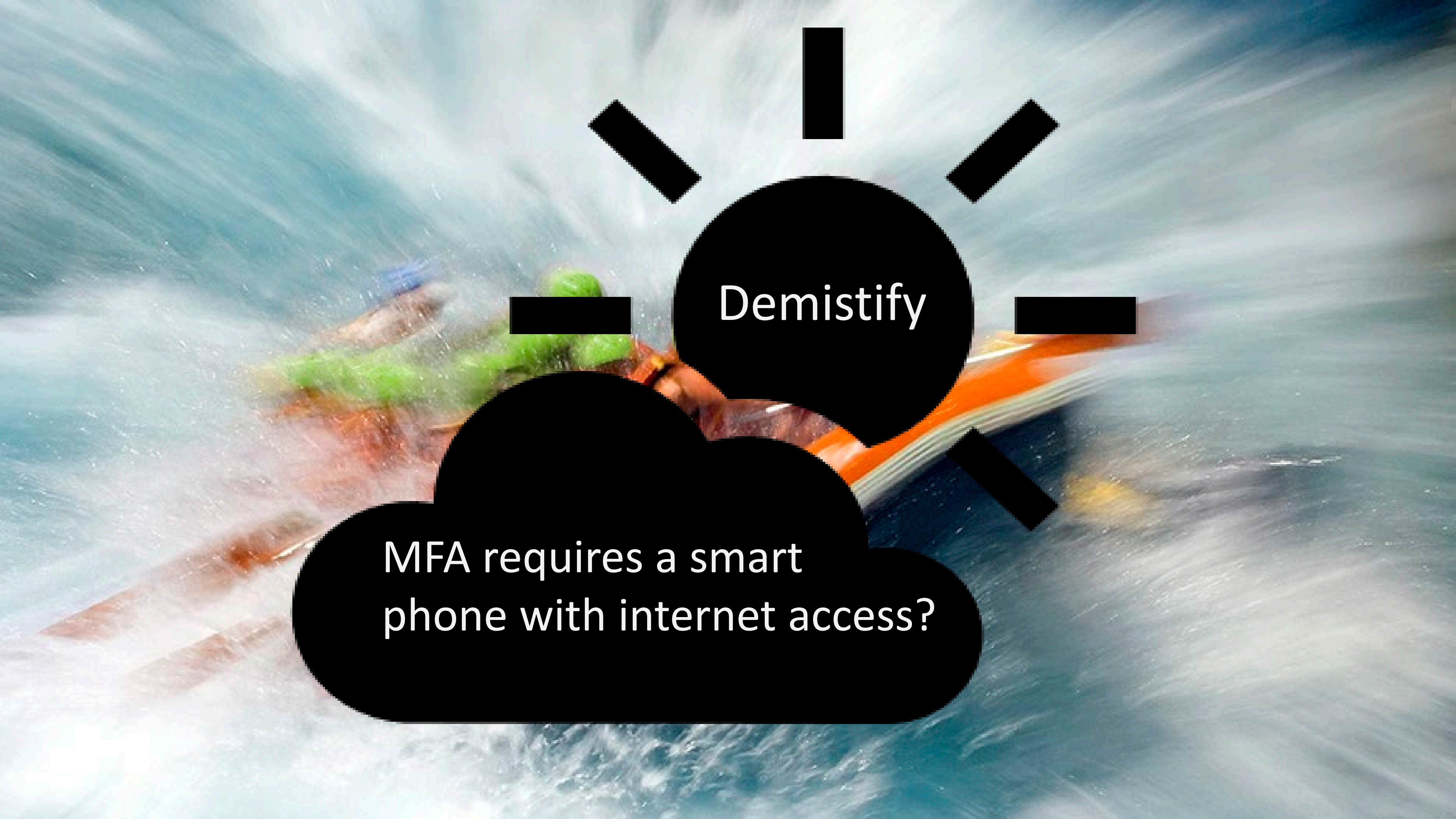
Use a verification code from my mobile app

Text +XX XXXXXXX61

Call +XX XXXXXXX61

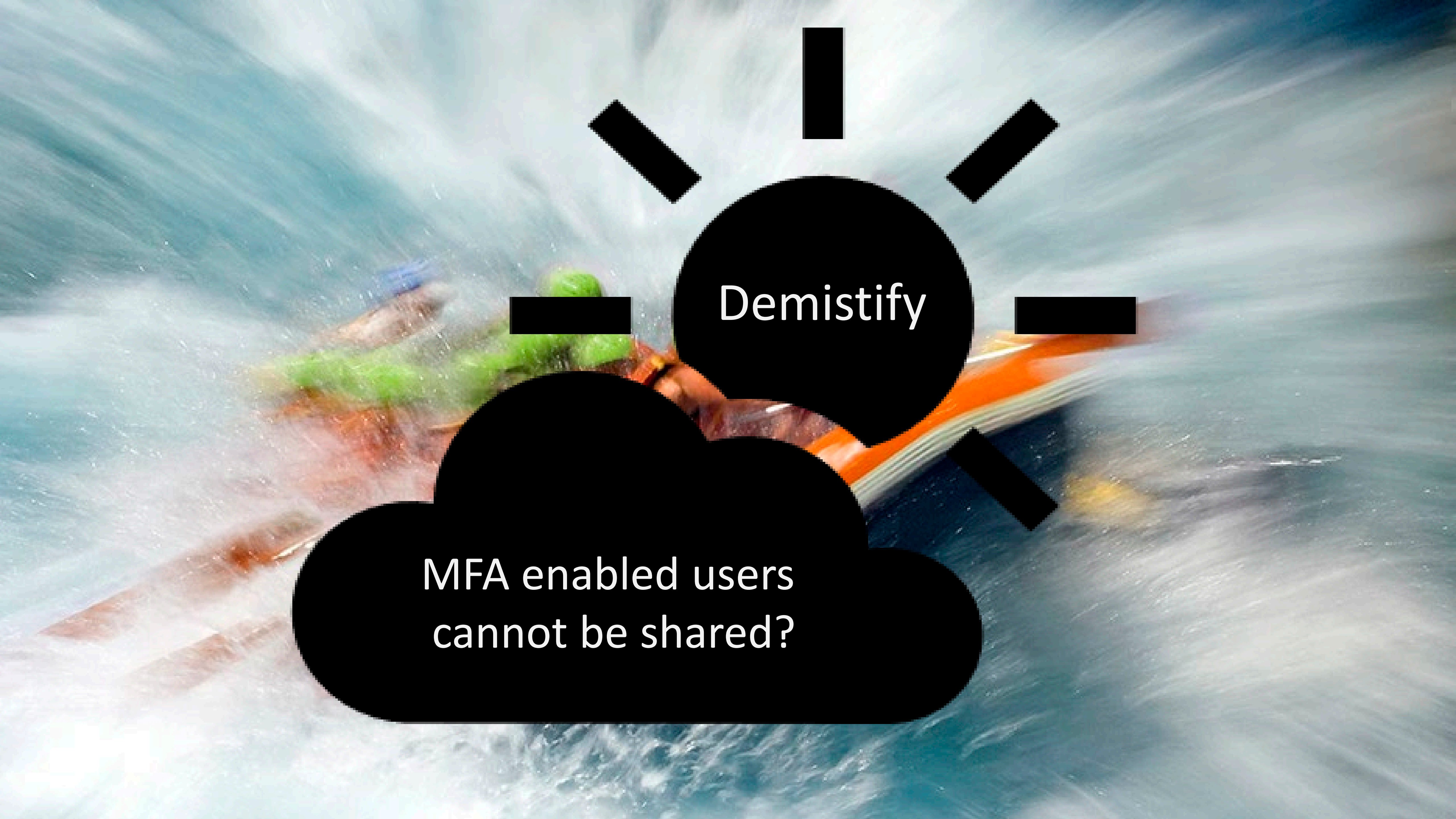
More information

Welcome to the RdEducation Tenant! Ready for demonstration purposes...



Demistify

MFA requires a smart phone with internet access?

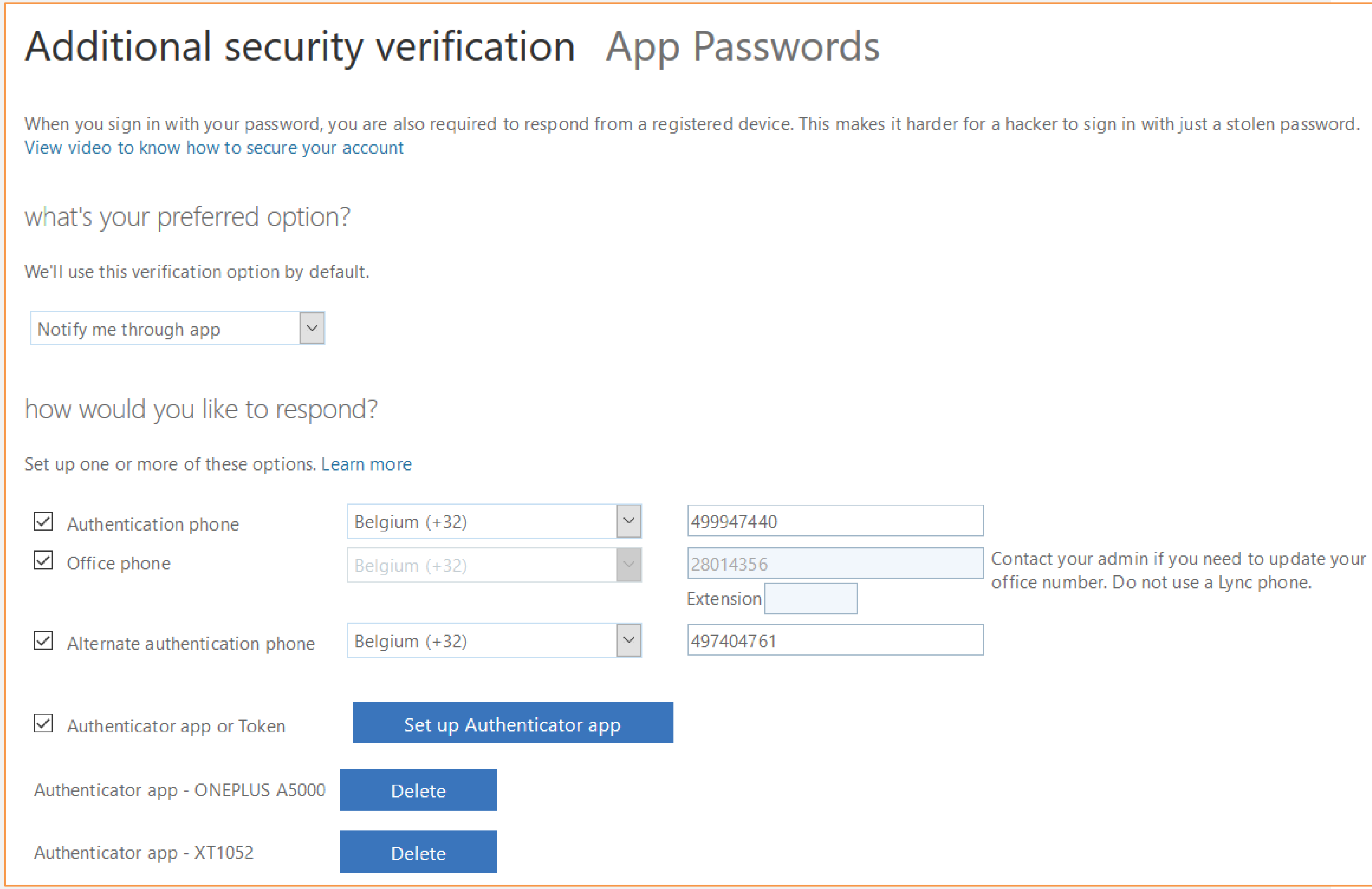


Demistify

MFA enabled users cannot be shared?

SECURITY VERIFICATION OPTIONS

- User can add one (or more) authentication apps
- User will add an authentication phone
- User can add his Office Phone
  It’s number is managed using the ‘Office Phone attribute’



Additional security verification App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
View video to know how to secure your account

what's your preferred option?

We'll use this verification option by default.

Notify me through app

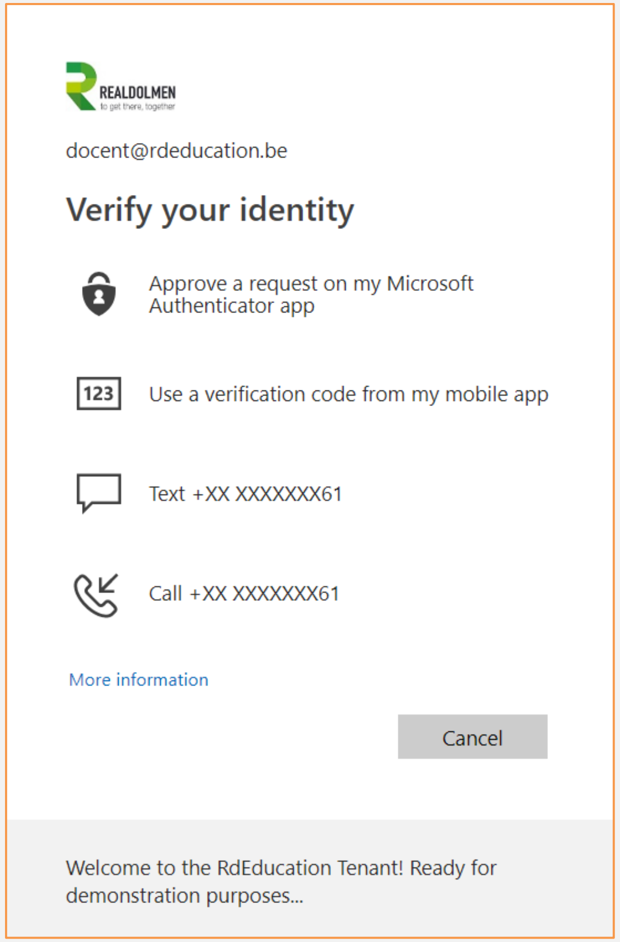
how would you like to respond?

Set up one or more of these options. Learn more

☑ Authentication phone	Belgium (+32)	499947440	
☑ Office phone	Belgium (+32)	28014356 Extension	Contact your admin if you need to update your office number. Do not use a Lync phone.
☑ Alternate authentication phone	Belgium (+32)	497404761	
☑ Authenticator app or Token	Set up Authenticator app		
Authenticator app - ONEPLUS A5000	Delete		
Authenticator app - XT1052	Delete		

MFA – User Login

- MFA used with a code generated in the authenticator app (with a cycle of 1 code per minute)
- MFA with SMS code
- MFA with telephone call



docent@rdeducation.be

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

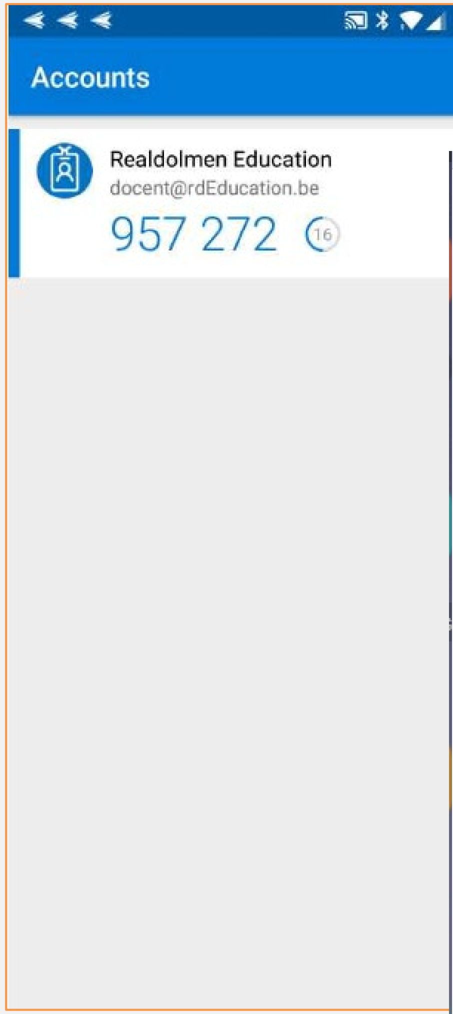
Text +XX XXXXXXX61

Call +XX XXXXXXX61

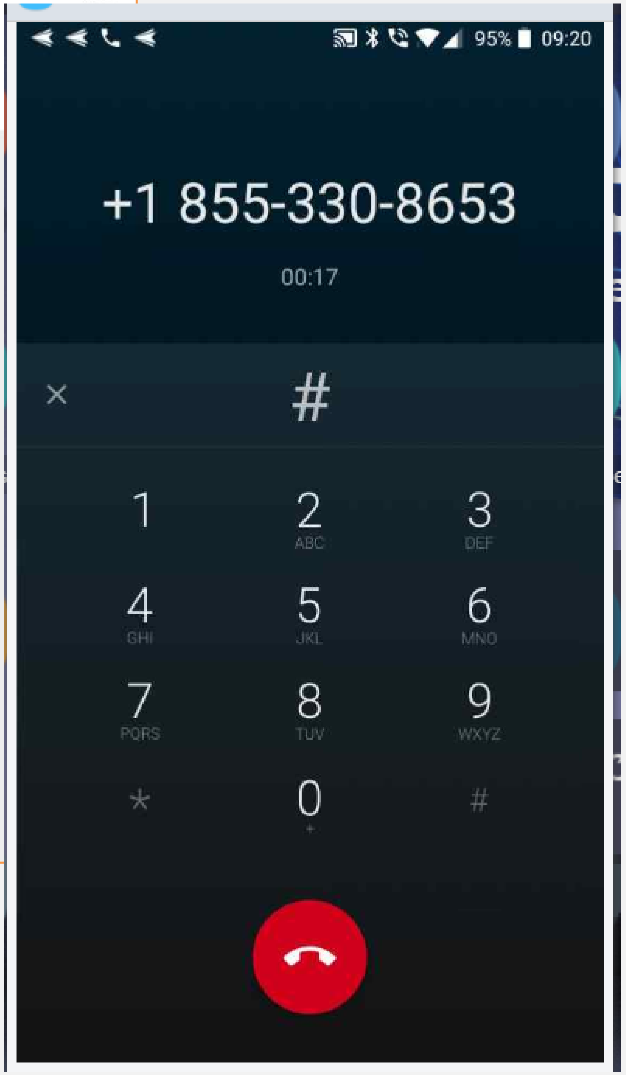
More information

Cancel

Welcome to the RdEducation Tenant! Ready for demonstration purposes...



Realdolmen Education
docent@rdEducation.be
957 272 16

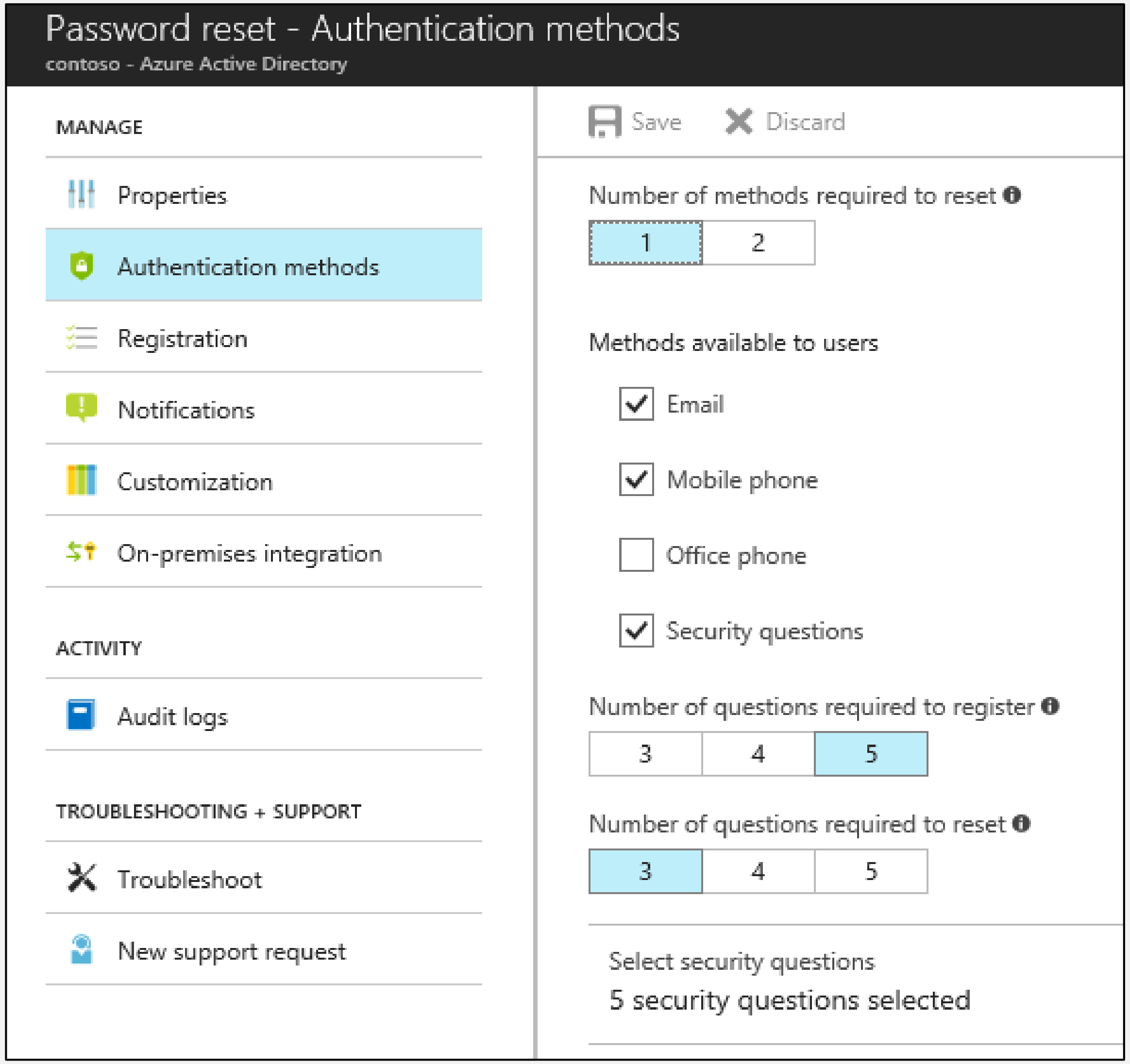


SELF SERVICE PASSWORD RESET

& PASSWORD WRITE BACK

Authentication Methods for Password Reset

- Choose the:
  - Number of authentication methods required to reset a password
  - Number of authentication methods available to users
- Authentication methods include:
  - Email notification
  - Text or code sent to phone
  - Number of security questions to be registered and how many must be correctly answered



Password reset - Authentication methods

contoso - Azure Active Directory

Number of methods required to reset: [✓ 1] 2

Methods available to users

☑ Email

☑ Mobile phone

□ Office phone

☑ Security questions

Number of questions required to register: 3 4 [✓ 5]

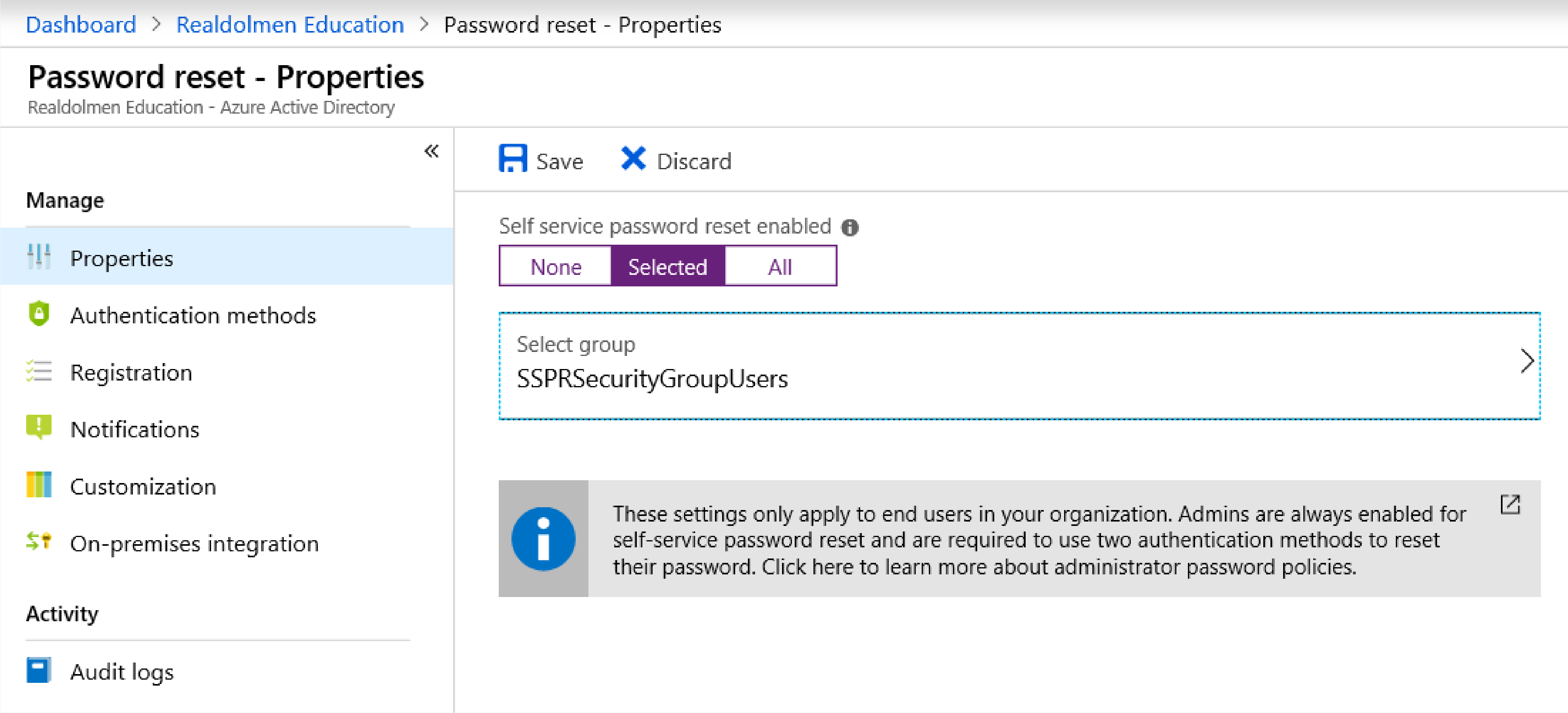
Number of questions required to reset: [✓ 3] 4 5

Select security questions

5 security questions selected

CONFIGURING SELF-SERVICE PASSWORD RESET

- Determine who will be enabled to use self-service password reset
- Narrow your selection to specific groups



Dashboard > Realdolmen Education > Password reset - Properties

Password reset - Properties

Realdolmen Education - Azure Active Directory

Self service password reset enabled

None [✓ Selected] All

Select group

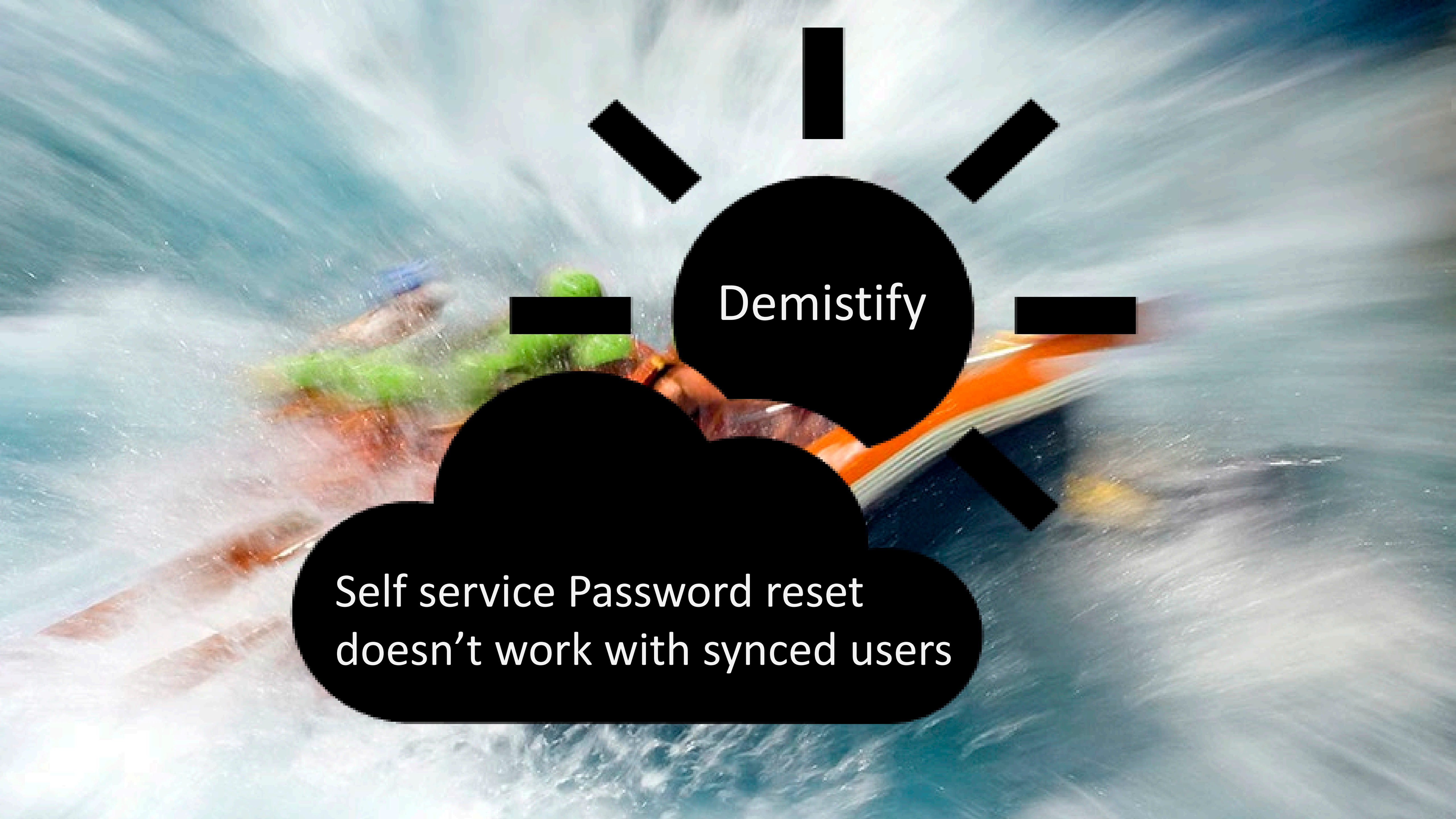
SSPRSecurityGroupUsers

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Custom Password portal links

If you want to provide the links to the different portals for password reset, registration and changing the password

Function	URL
Azure AD password reset registration portal	https://aka.ms/ssprsetup
Azure AD password reset portal	https://aka.ms/sspr
Azure AD password change portal	https://account.activedirectory.windowsazure.com/ChangePassword.aspx

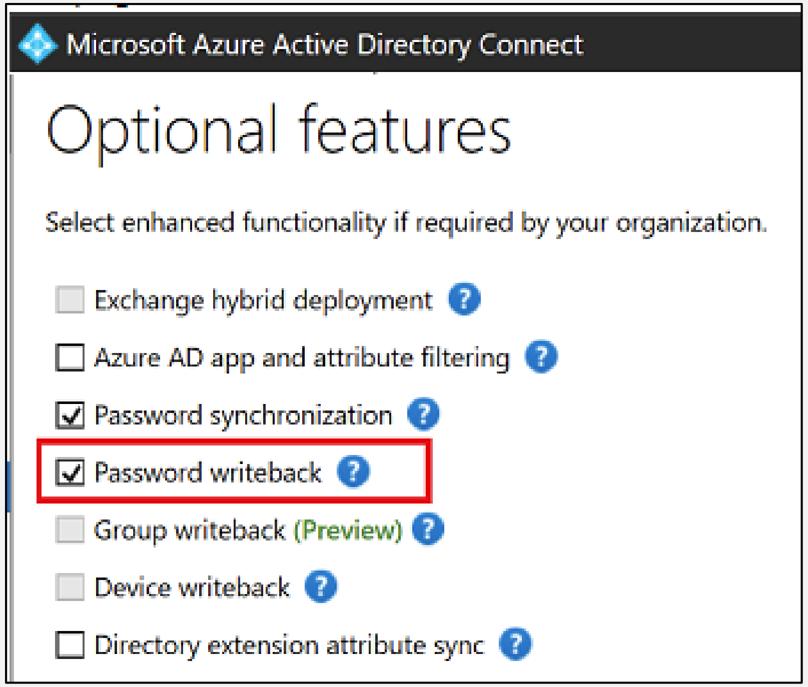


Demistify

Self service Password reset doesn’t work with synced users

Password Write back

- Use Password Write back to configure Azure AD to write passwords back to your on-premises Active Directory
- A component of Azure AD Connect
- Available to subscribers of Premium Azure Active Directory editions
- Removes the need to set up and manage an on-premises SSPR solution



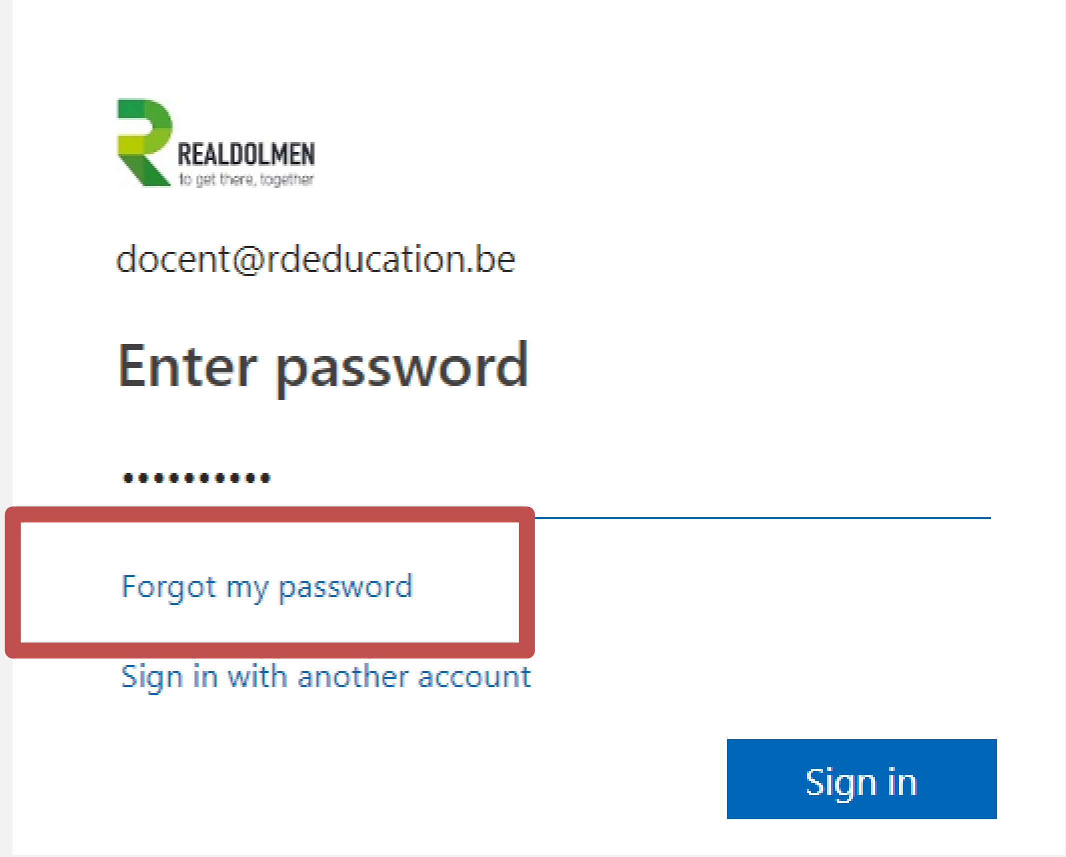
Microsoft Azure Active Directory Connect

Optional features

Select enhanced functionality if required by your organization.

- □ Exchange hybrid deployment
- □ Azure AD app and attribute filtering
- ☑ Password synchronization
- ☑ Password writeback
- □ Group writeback (Preview)
- □ Device writeback
- □ Directory extension attribute sync

Using Self Service Password Reset



docent@rdeducation.be

Enter password

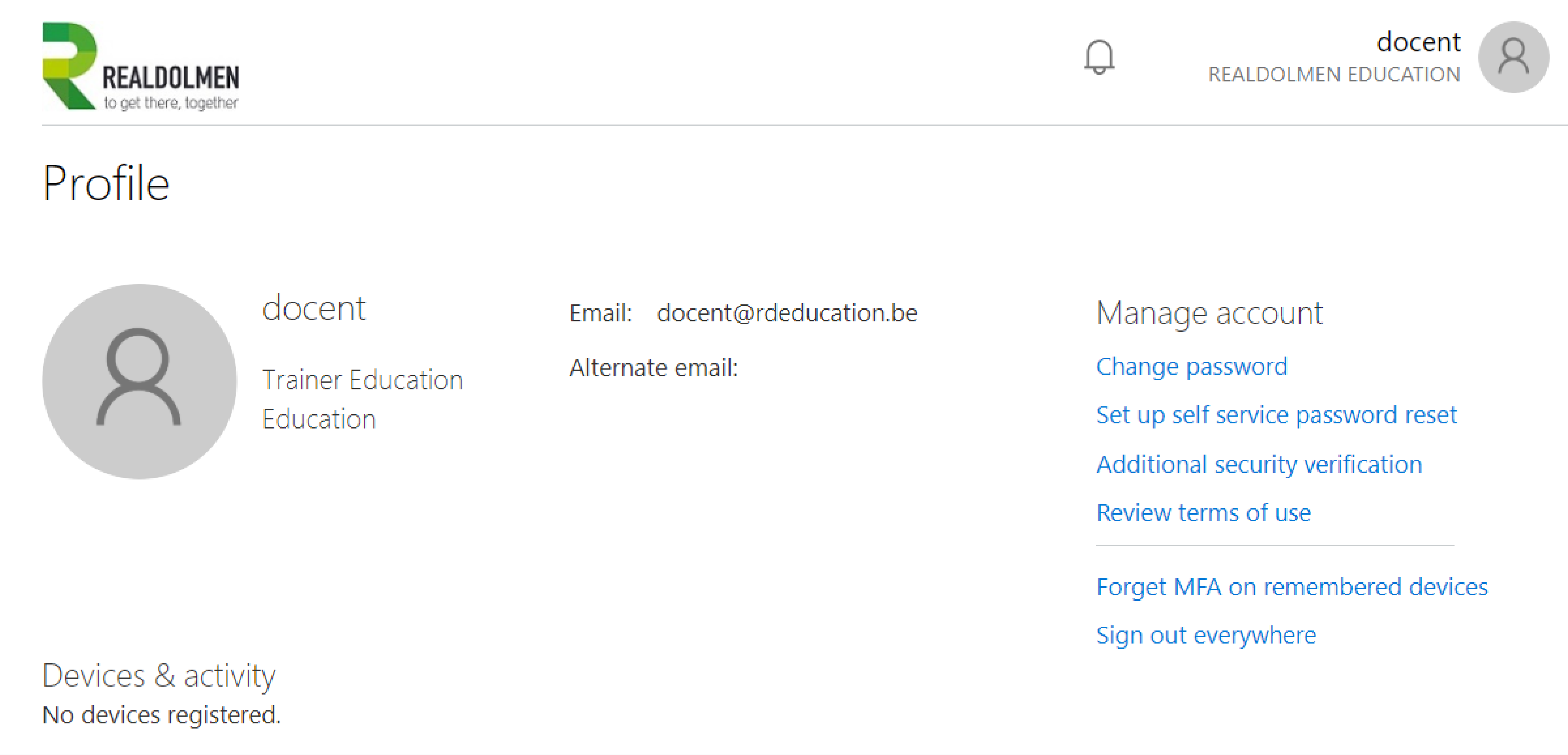
••••••••••••

Forgot my password

Sign in with another account

AAD USER ACCOUNT PROFILE MANAGEMENT

https://account.activedirectory.windowsazure.com



Profile

docent

Trainer Education

Education

Email: docent@rdeducation.be

Alternate email:

Manage account

Change password

Set up self service password reset

Additional security verification

Review terms of use

Forget MFA on remembered devices

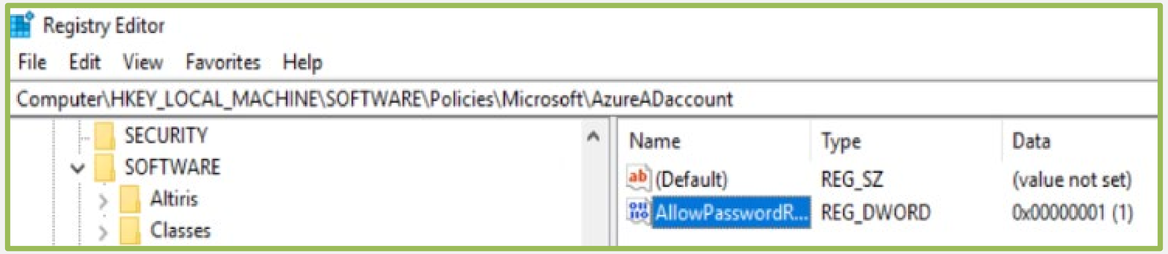
Sign out everywhere

Devices & activity

No devices registered.

Self Service Password reset from logon

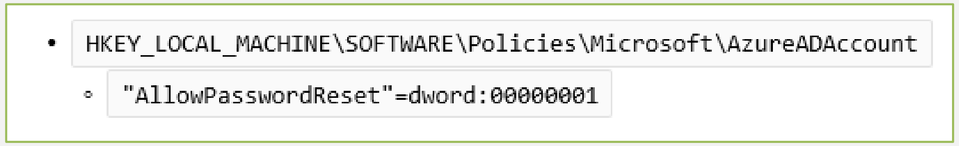
- Needs AAD join or Hybrid AAD Join
- Activate using registry key or Intune rule



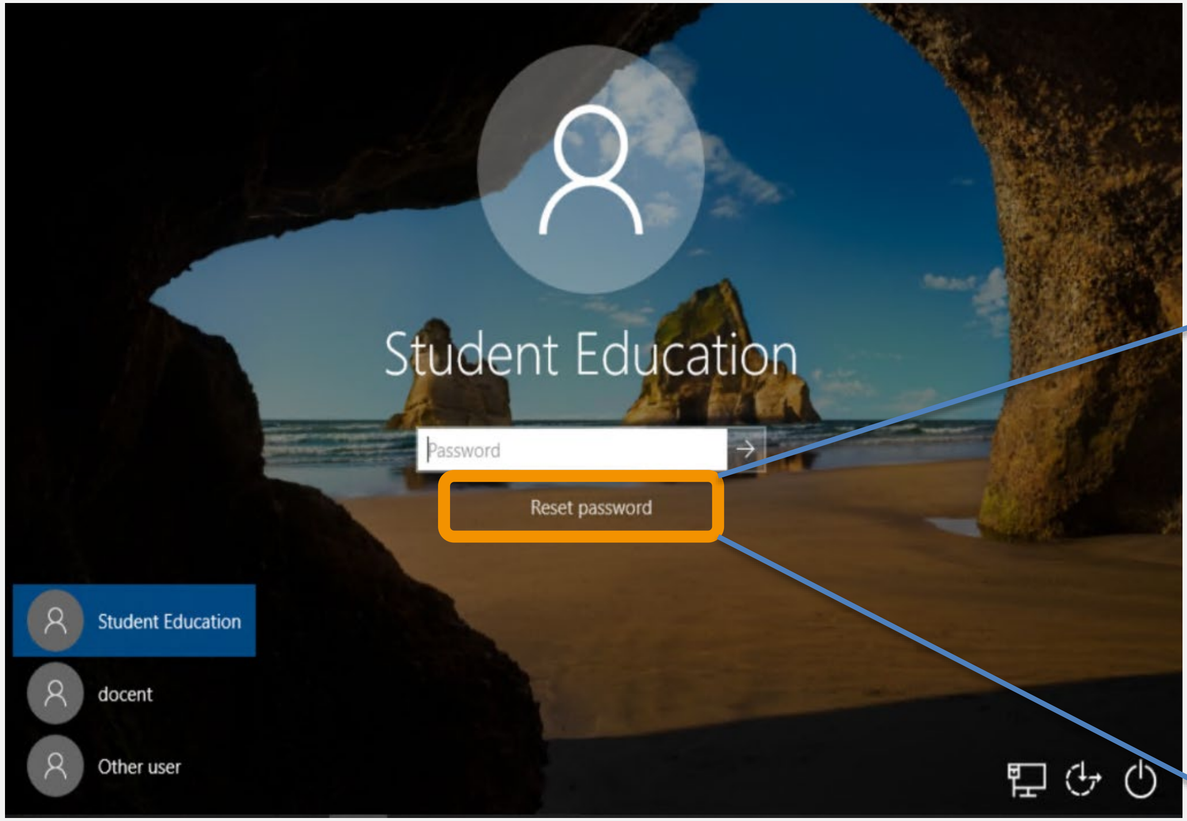
Registry Editor

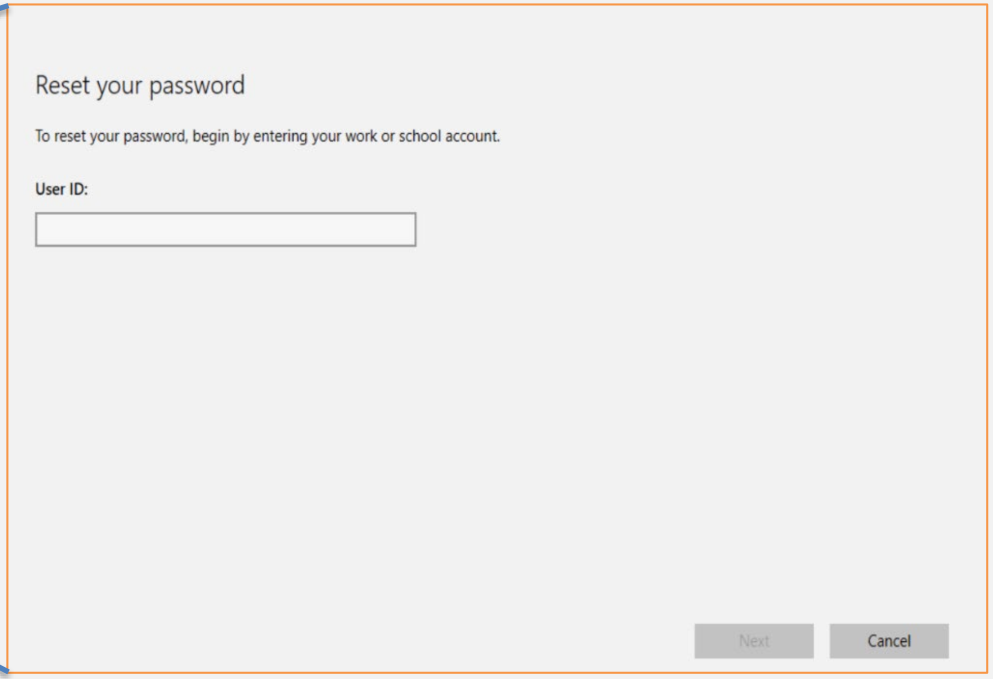
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AzureADaccount

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowPasswordR...	REG_DWORD	0x00000001 (1)



```
• HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AzureADAccount
  ◦ "AllowPasswordReset"=dword:00000001
```

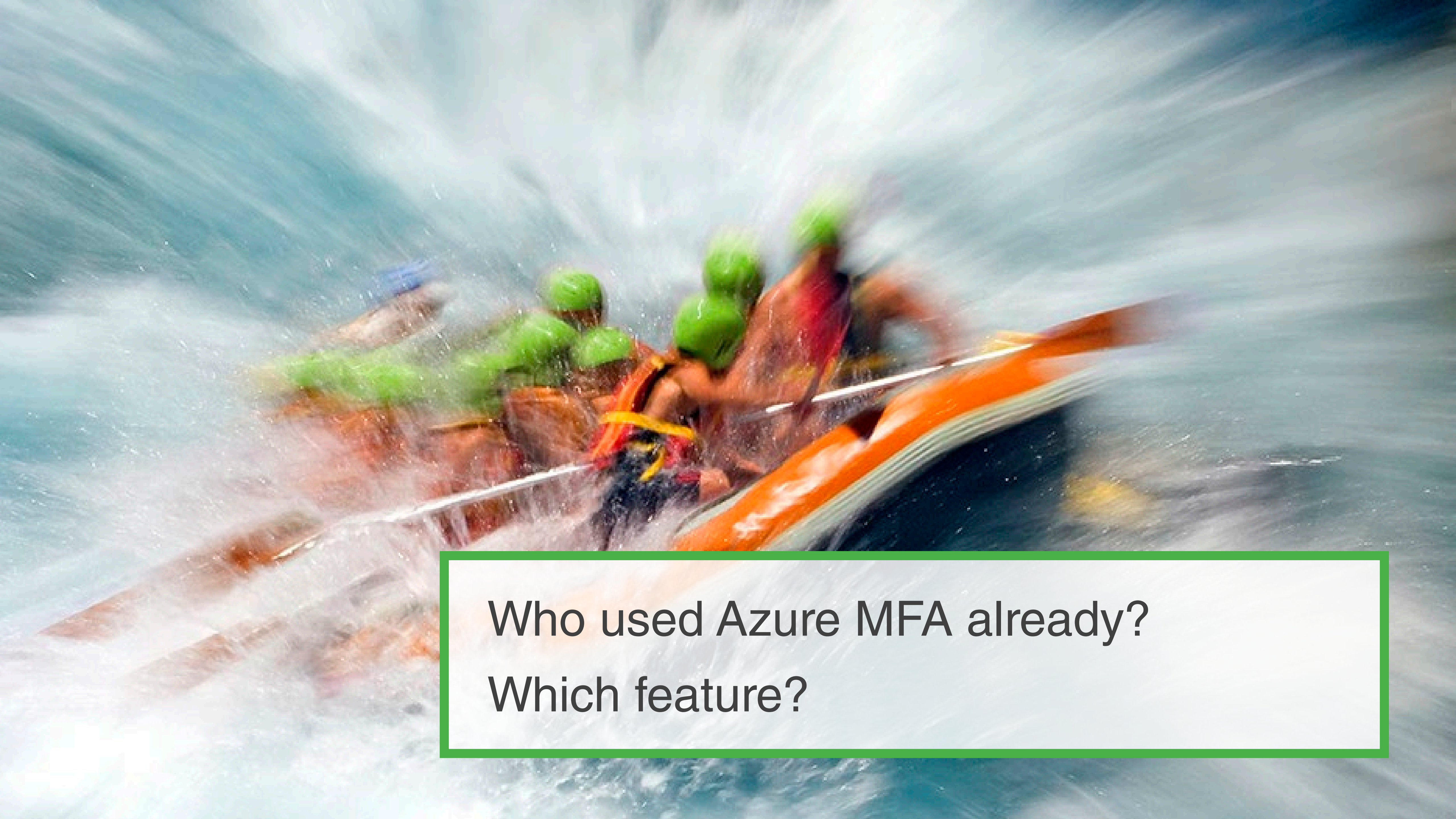




Reset your password

To reset your password, begin by entering your work or school account.

User ID:



Who used Azure MFA already?

Which feature?

Demonstration:

1. Using MFA

Configuring Self-Service Password Reset

1. Enable SSPR for everyone
2. Select the authentication methods, security questions
3. Configure notifications, users and administrators
4. First time user logins must answer the security questions
5. Try out password reset

To get there, together

REALDOLMEN

HQ Realdolmen Huizingen
A. Vaucampslaan 42
B-1654 Huizingen
+32 2 801 55 55

www.realdolmen.com