



HAROLD BAELE – MICROSOFT CLOUD TECHNICAL CONSULTANT
- MICROSOFT CERTIFIED TRAINER

Identity as a Service using Azure Active Directory

AAD?

AAD for IdAAS

AAD users & passwords

AAD Multi Factor Authentication

AAD Conditional Access

AAD Privileged Identity Management

Azure Application Proxy

HAROLD BAELE – MICROSOFT CLOUD TECHNICAL CONSULTANT AND MICROSOFT CERTIFIED TRAINER @REALDOLMEN IN BELGIUM

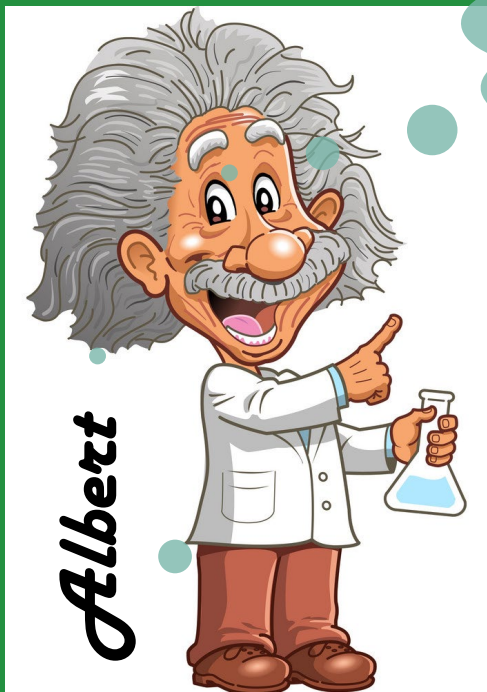
- Harold.baele@realdolmen.com - @hbaele
- Trainer since 2000 on
 - Operating Systems, Networking, AD, PowerShell
 - Exchange → Office 365
 - Azure IAAS
- Consultant since 2016
 - Azure IAAS & Identity
 - Office 365 ...in a Hybrid Cloud context
- Speaker @MicrosoftBE since 2015
 - ModernBiz - PPE's – CSP Workshops ...
- Microsoft Preferred Partner Solutions Expert for Office 365



Microsoft
Cloud
Technical
Consultant

Microsoft
Certified
Trainer





docent@rdeducation.be

Azure2019

UserName + password

Mail

ShortUserName+ password

FileShare

ONLY INTERNAL using HTTP

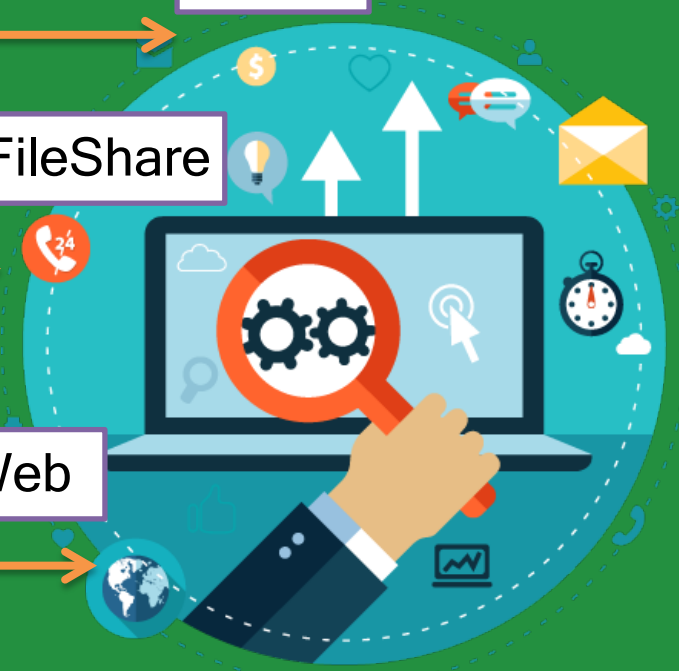
PanoWeb

UserName 2 + password

admin@rdeducation.be

Azure2019

ADMIN

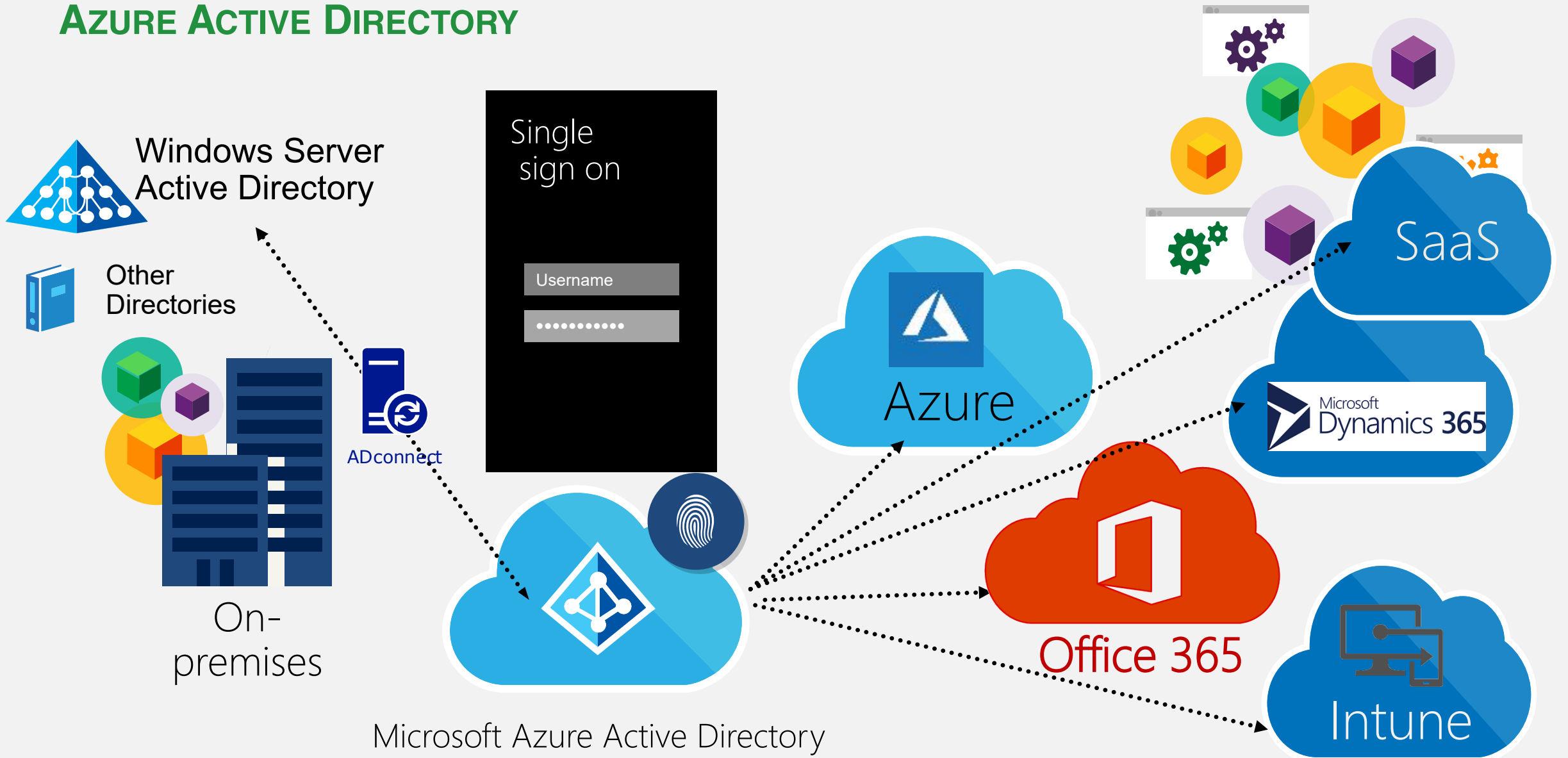




AZURE ACTIVE DIRECTORY ?



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/>



Demistify

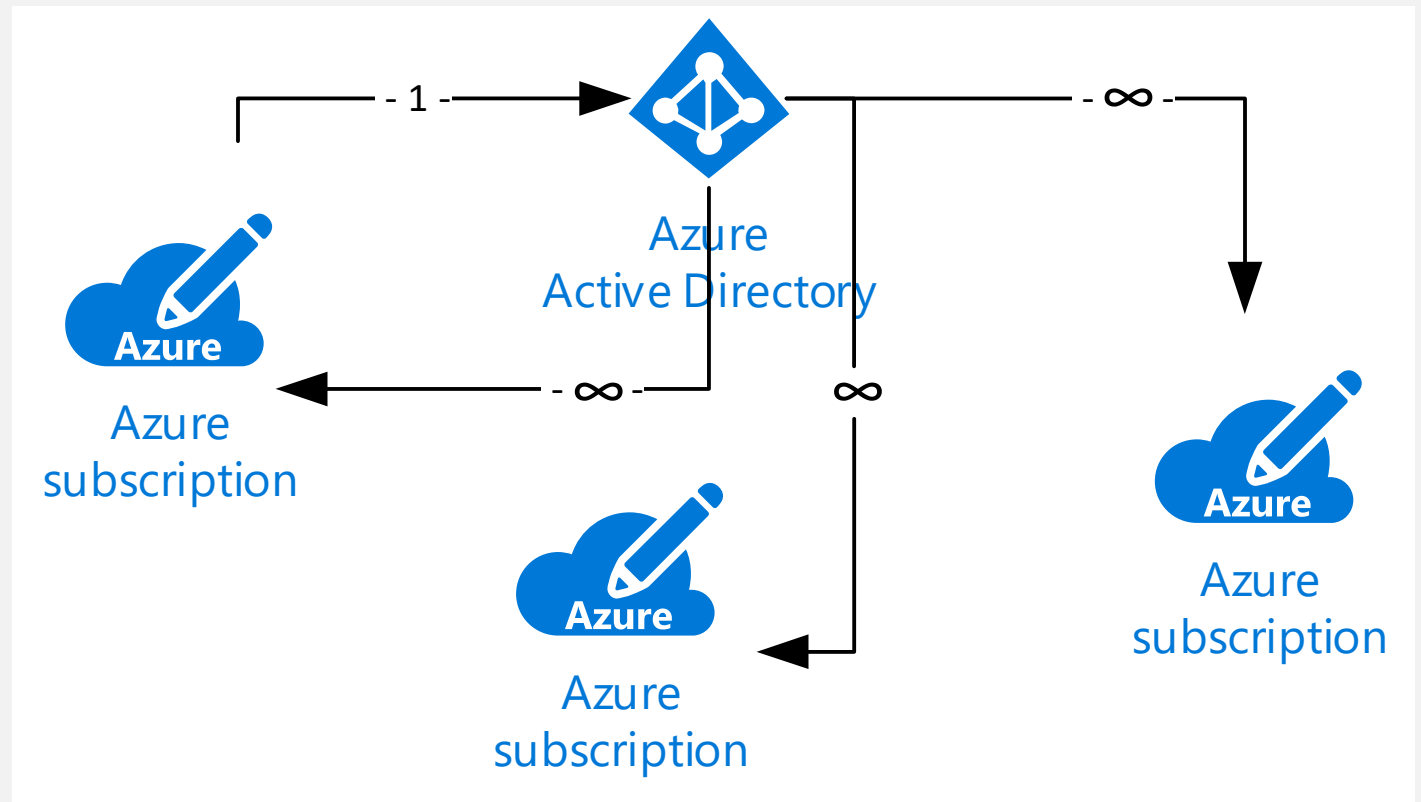
How many AADs can be used by an Azure Subscription?

AAD FUELS THE IDENTITY SOURCE OF AN AZURE SUBSCRIPTION

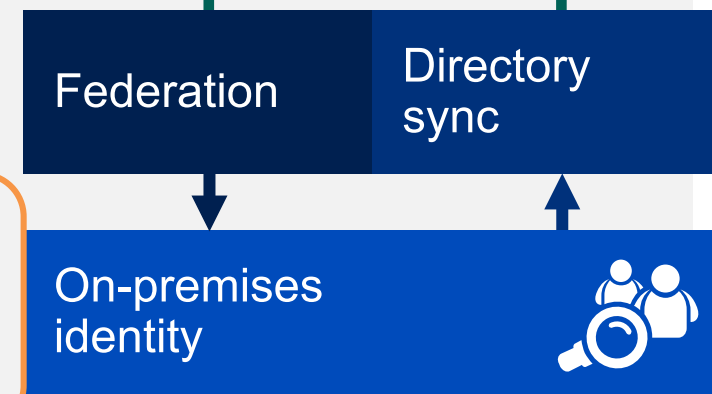
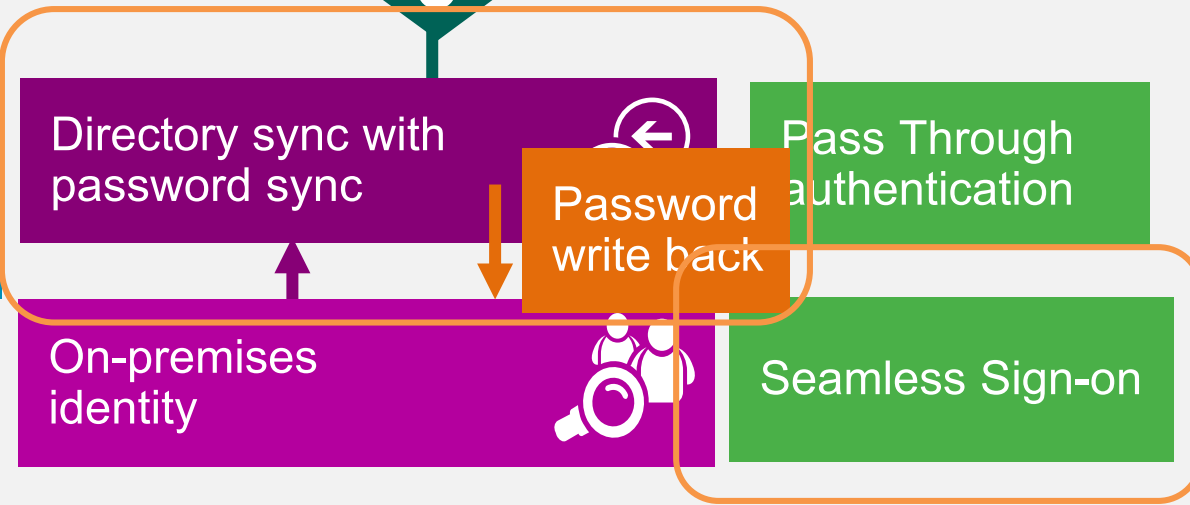
- First user assigned the Service Administrator role
- Other admins: co-administrators

Both can be either Microsoft accounts or work or school accounts from the AAD linked to the Azure subscription

- An Azure subscription trusts 1 AAD
- 1 AAD can trust multiple subscriptions
- Subscription management is part of <https://portal.azure.com>



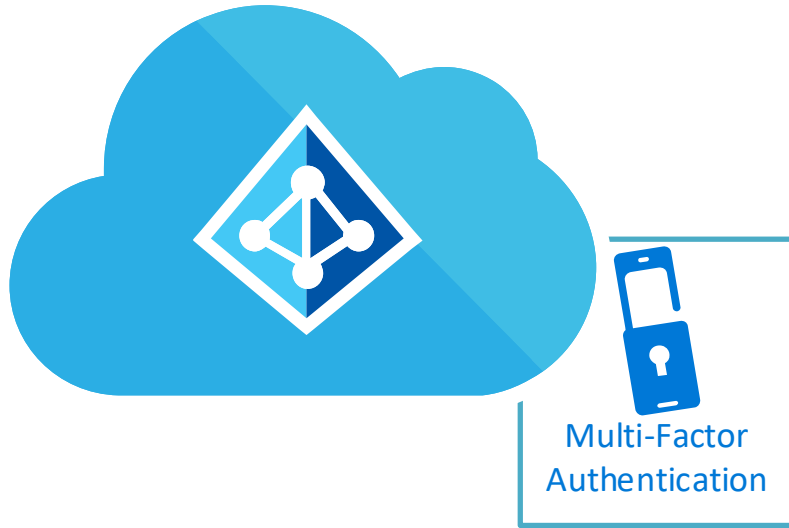
AZURE ACTIVE DIRECTORY IDENTITY MODELS



EXTENDING FEATURES WITH AAD BASIC, PREMIUM 1, PREMIUM 2, OFFICE 365

	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	✓	✓	✓	✓	✓
Single Sign-On (SSO)	10 apps per user ² (pre-integrated SaaS and developer-integrated apps)	10 apps per user ² (free tier + Application proxy apps)	No Limit (free, Basic tiers + Self-Service App Integration templates ⁴)	No Limit (free, Basic tiers + Self-Service App Integration templates ⁴)	10 apps per user ² (pre-integrated SaaS and developer-integrated apps)
B2B Collaboration ⁶	✓	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓	✓
Connect (Sync engine that extends on-premises directories to Azure Active Directory)	https://azure.microsoft.com/en-us/pricing/details/active-directory/				
Security/Usage Reports	Basic Reports	Basic Reports	Advanced Reports	Advanced Reports	Basic Reports





AAD MULTI FACTOR AUTHENTICATION





Demistify

MFA requires a smart
phone with internet access?

AZURE MFA OPTIONS



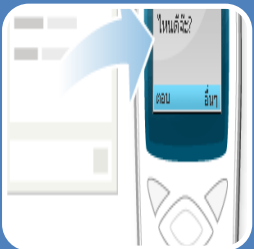
Microsoft Authenticator app

- App which generates a code
- App ask for approval



Phone call

- Phone call asking confirmation with a #



SMS

- Small sms message with code



docent@rdeducation.be

Verify your identity



Approve a request on my Microsoft Authenticator app



Use a verification code from my mobile app



Text +XX XXXXXXXX61



Call +XX XXXXXXXX61

[More information](#)

Cancel

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





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](#)

<input checked="" type="checkbox"/> Authentication phone	<input type="text" value="Belgium (+32)"/>	<input type="text" value="499947440"/>
<input checked="" type="checkbox"/> Office phone	<input type="text" value="Belgium (+32)"/>	<input type="text" value="28014356"/>
		Extension <input type="text"/>
<input checked="" type="checkbox"/> Alternate authentication phone	<input type="text" value="Belgium (+32)"/>	<input type="text" value="497404761"/>

Authenticator app or Token

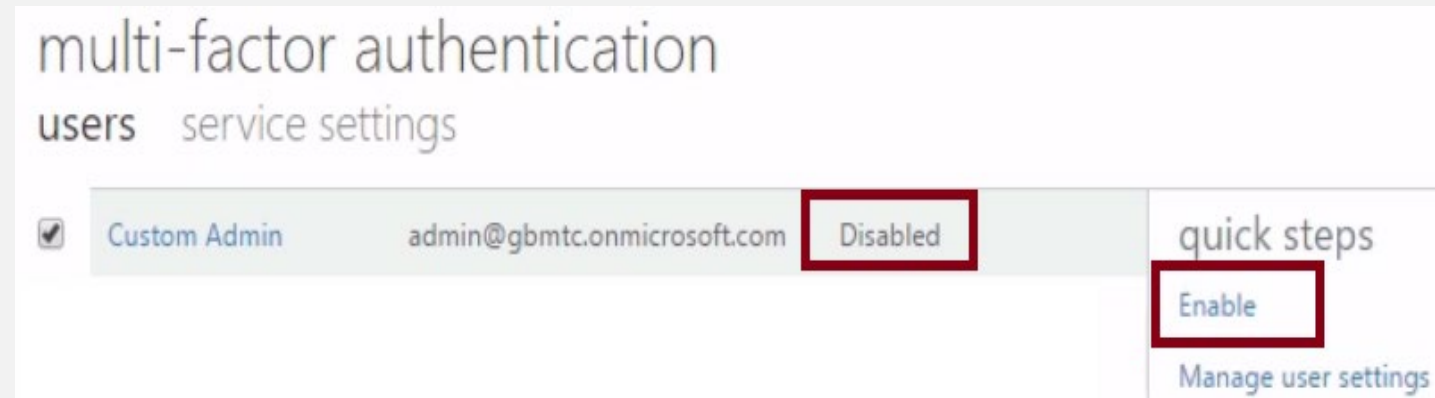
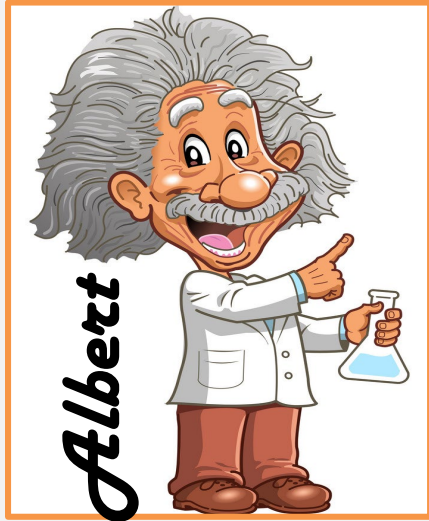
Authenticator app - ONEPLUS A5000

Authenticator app - XT1052

Contact your admin if you need to update your office number. Do not use a Lync phone.

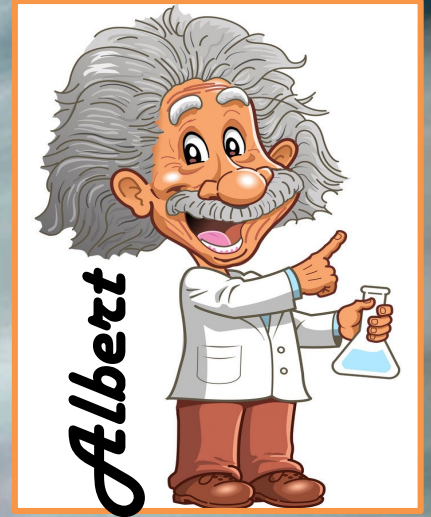


MFA FOR GLOBAL ADMINS



- Free of charge for global administrator security
- Added level of security when managing and creating Azure resources, like virtual machines





Demo (part 1)

- MFA login (company branded demo tenant)
- show the password in edge (it's ok)

multi-factor authentication

users [service settings](#)

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

85.234.194.188/32

192.168.1.0/27

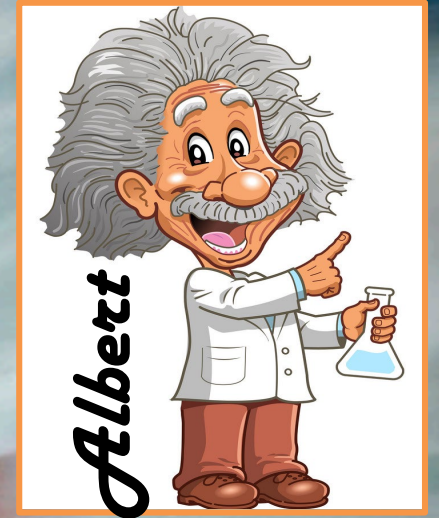
192.168.1.0/27

192.168.1.0/27

verification options [\(learn more\)](#)

Methods available to users:

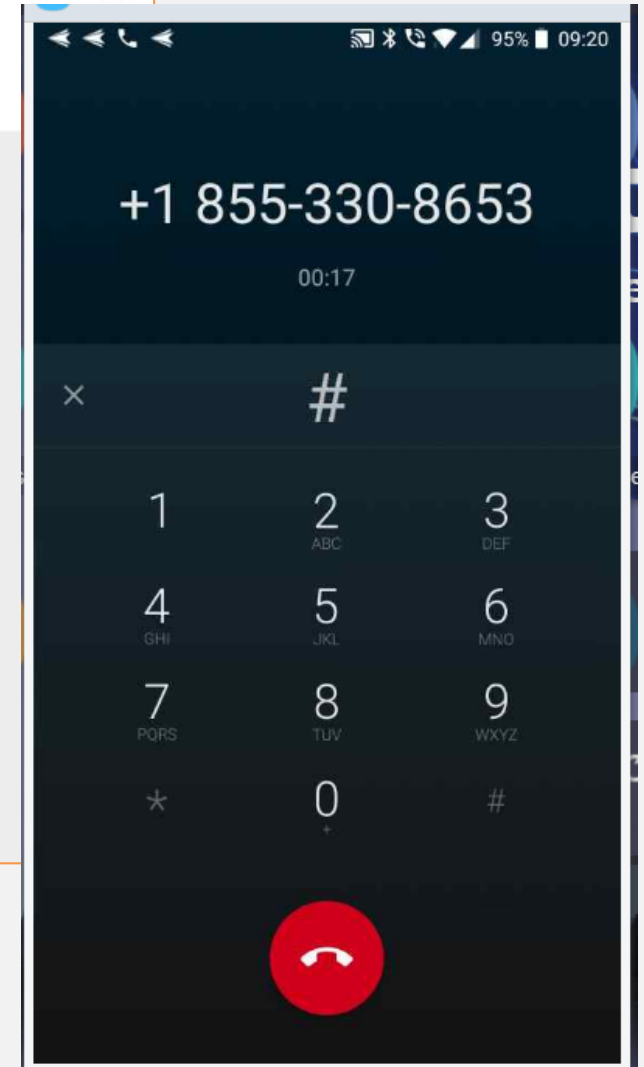
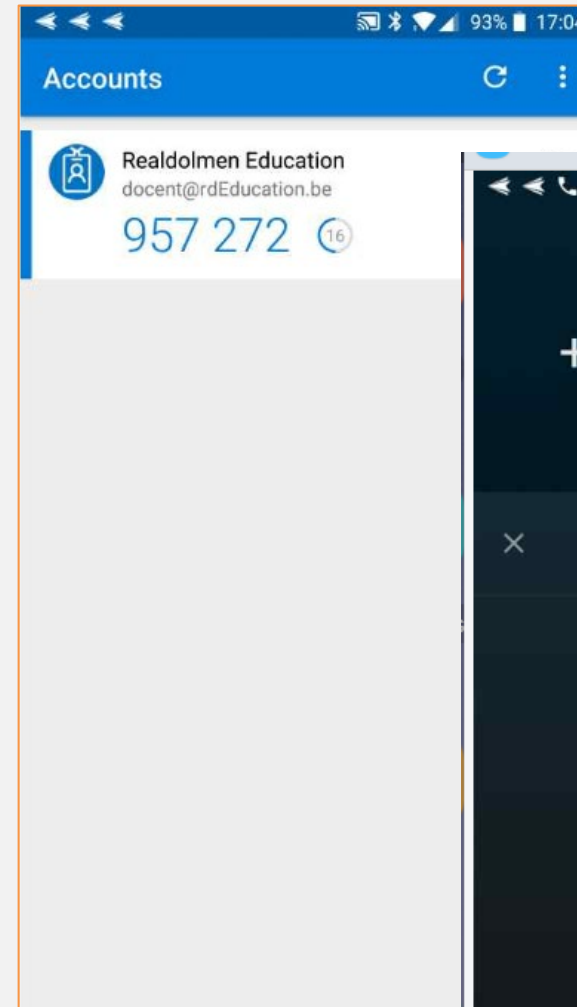
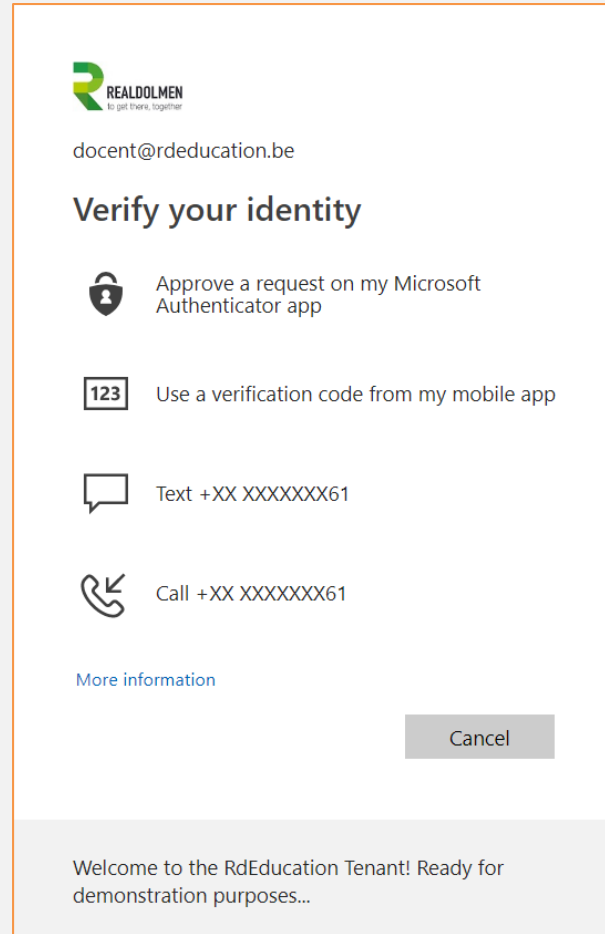
- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token



Demo (part 2) – Seamless Sign On
without MFA using an internal client

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





AAD AS A SSO





Same

Seamless

Single

WHAT ABOUT APPLICATIONS OUTSIDE OF OFFICE 365

- Do we still need ADFS for Single Sign On? **No, we don't!**
- Azure AD is also a Security Token Service supporting SAML, OpenID, OAuth..
- Move applications to Azure AD
- +10 or SAML Requires Premium P1 licenses on Azure AD
- Customers without P1 licenses can still rely on ADFS

The screenshot displays the Azure AD application gallery interface. It is divided into two main sections:

- Add from the gallery:** This section contains a sub-section titled "Featured applications" (highlighted with a red box). Below this, there are four application tiles: "Box" (with a hand cursor over the logo), "Concur", "DocuSign", and "Dropbox for Business".
- Add your own app:** This section contains three numbered options:
 - 1 Application you're developing:** Register an app you're working on to integrate it with Azure AD.
 - 2 On-premises application:** Configure Azure AD Application Proxy to enable secure remote access.
 - 3 Non-gallery application:** Integrate any other application that you don't find in the gallery.




END USER EXPERIENCE

Using Office 365 App Launcher


•  To-Do

•  Video


•  Word


 Yammer

Other

 Booking.com

 Box


 EducationRD

 PanoramixWEB


 SAMLweb


Using MyApps.microsoft.com



docent
REALDOLMEN EDUCATION 

Apps


 Add-In


 Calendar

 Excel

 MyAnalytics

 Outlook

 Planner

 PowerPoint

 Booking.com

 Delve

 Flow

 OneDrive

 PanoramixWEB


 Power BI

 SAMLweb

 Box

 Dynamics 365

 Forms

 OneNote

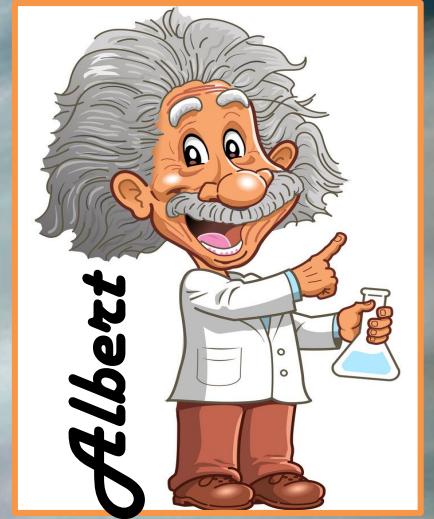
 People

 PowerApps

 SharePoint

 Groups

 Access reviews



Demo - Login SAMLweb



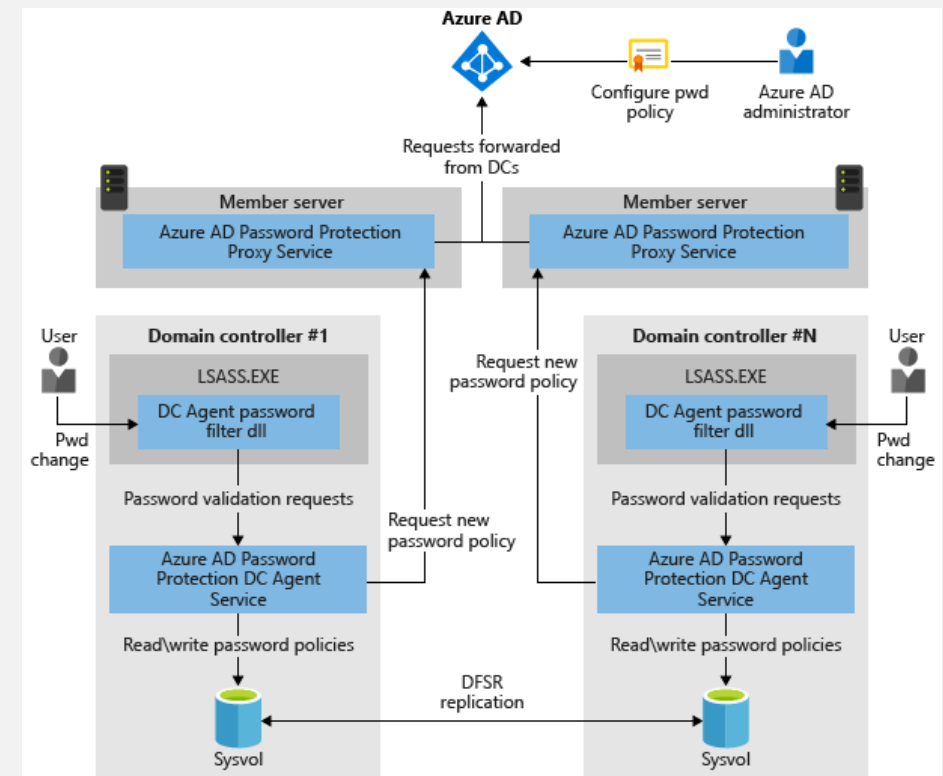
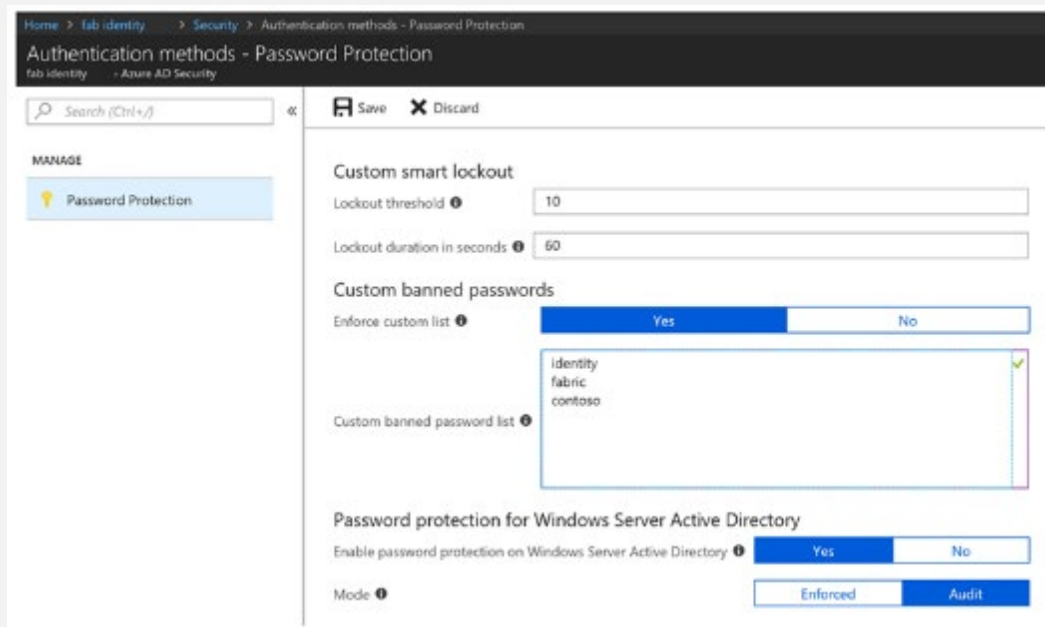
SECURE PASSWORDS



SECURING PASSWORDS

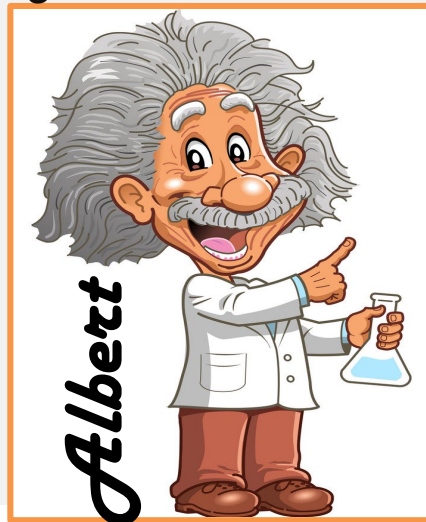
PASSWORD PROTECTION & SMART LOCKOUT (GA!)

- Prevent users from using most commonly used passwords, plus over 1 million character substitution variations of those passwords
- Can be leveraged in both Azure AD as on premises AD
- Create own banned password list with company specific keywords
- Audit and enforcement mode



SELF SERVICE 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

MANAGE

- Properties
- Authentication methods**
- Registration
- Notifications
- Customization
- On-premises integration

ACTIVITY

- Audit logs

TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

Save Discard

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



USING SELF SERVICE PASSWORD RESET



docent@rducation.be

Enter password

.....

[Forgot my password](#)

[Sign in with another account](#)

Sign in



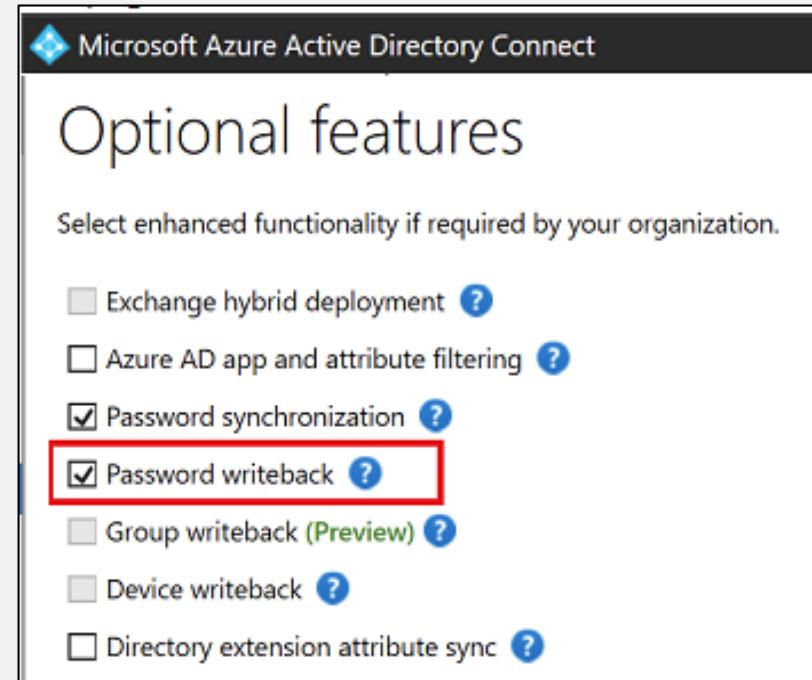


Demistify

Self service Password reset
doesn't work with synced users

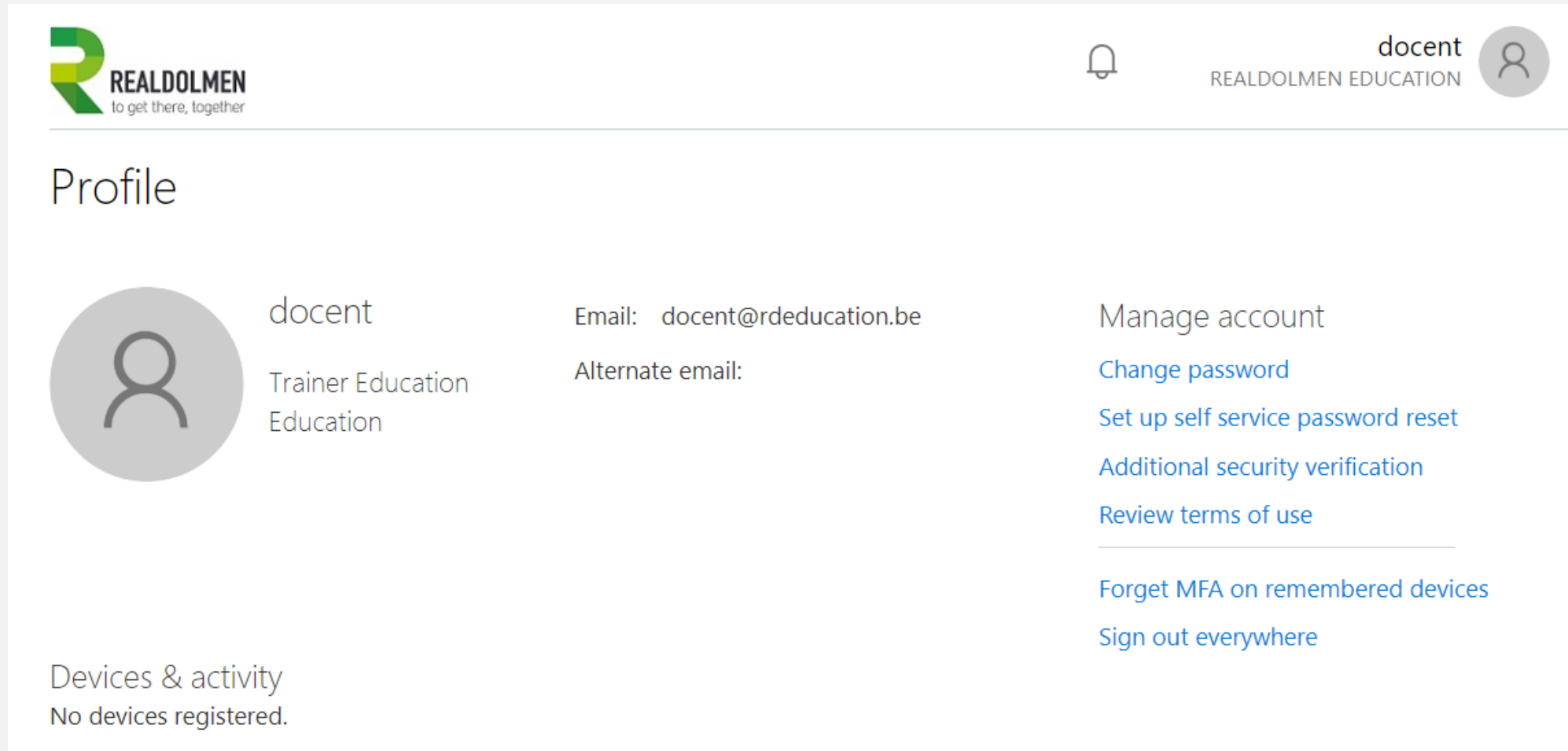
PASSWORD WRITE BACK

- 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



AAD USER ACCOUNT PROFILE MANAGEMENT

<https://account.activedirectory.windowsazure.com>



The screenshot shows the user account profile management interface. At the top left is the REALDOLMEN logo with the tagline 'to get there, together'. At the top right, there is a notification bell icon, the user name 'docent', the organization 'REALDOLMEN EDUCATION', and a profile picture icon. The main heading is 'Profile'. Below this, there is a large grey circle containing a person icon. To the right of this icon, the user name 'docent' is displayed, followed by the role 'Trainer Education' and 'Education'. Below the name, the email address 'Email: docent@rdeducation.be' and 'Alternate email:' are shown. On the right side of the profile, there is a list of management options: 'Manage account', 'Change password', 'Set up self service password reset', 'Additional security verification', 'Review terms of use', 'Forget MFA on remembered devices', and 'Sign out everywhere'. At the bottom left, there is a section for 'Devices & activity' which states 'No devices registered.'.

REALDOLMEN
to get there, together

docent
REALDOLMEN EDUCATION

Profile

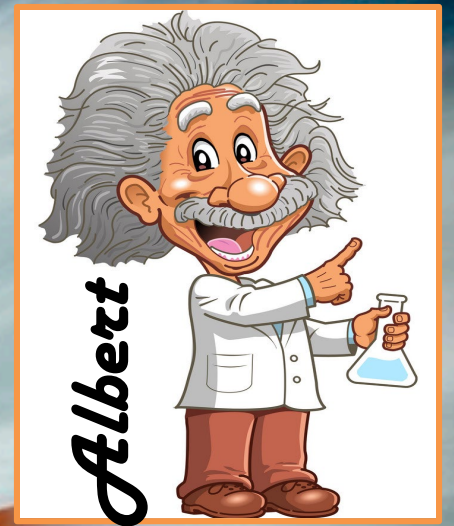
docent
Trainer Education
Education

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.





- Demo - Change password
- Password Self Service Reset config

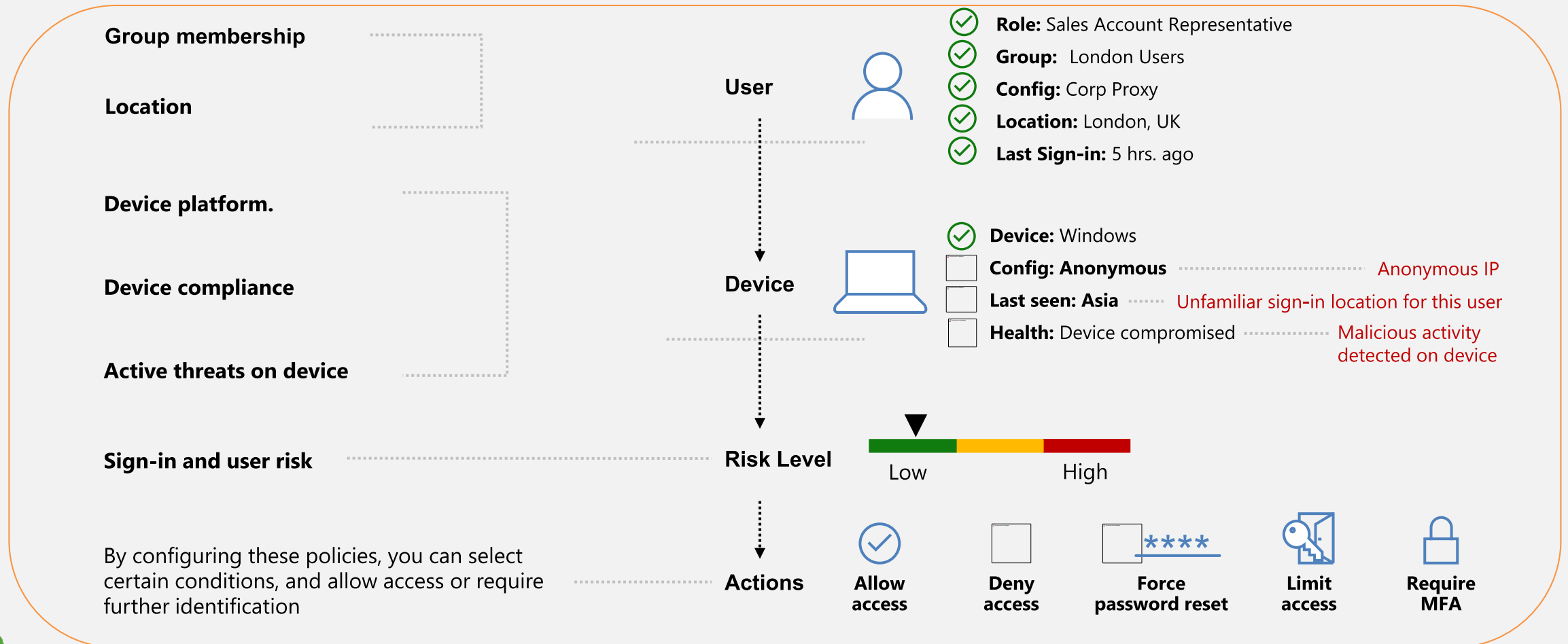


AAD CONDITIONAL ACCESS



CONDITIONAL ACCESS POLICIES EXPLAINED

Conditional access policies can be applied based on device state, application sensitivity, location and user rules



CONDITIONAL ACCESS BASELINE POLICY

- Does not require Premium AAD license
- Currently in preview (verified 2019-03-26)
- You can opt out
- You can exclude users, for break glass account



Baseline policy: Require...

Policies

i This policy will automatically be enabled in the future. Click here to learn more. [→](#)

Name

Baseline policy: Require MFA for admins (Pr...

This policy requires **multi-factor authentication** for the following directory roles:

- Global administrators
- SharePoint administrators
- Exchange administrators
- Conditional Access administrators
- Security administrators

[Learn more](#)

Enable policy

Automatically enable policy in the future

Use policy immediately

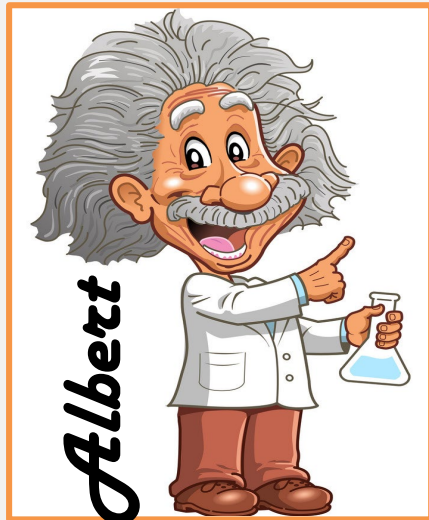
Do not use policy

Exclude users **i** [>](#)

0 users selected



NO ACCESS TO AZURE PORTAL



Dashboard > Conditional Access - Policies > Disable Azure portal > Conditions > Locations

Disable Azure portal

Info Delete

* Name
Disable Azure portal

Assignments

Users and groups
All users included and specific... >

Cloud apps
1 app included >

Conditions
1 condition selected >

Access controls

Grant
Block access >

Session
0 controls selected >

Enable policy

Conditions

Info

Device platforms
Not configured >

Locations
Any location and all trusted locat... >

Client apps (preview)
Not configured >

Device state (preview)
Not configured >

Locations

Control user access based on their physical location. [Learn more](#)

Configure

Select the locations to exempt from the policy

All trusted locations
 Selected locations

Select
None >





docent@rdeducation.be

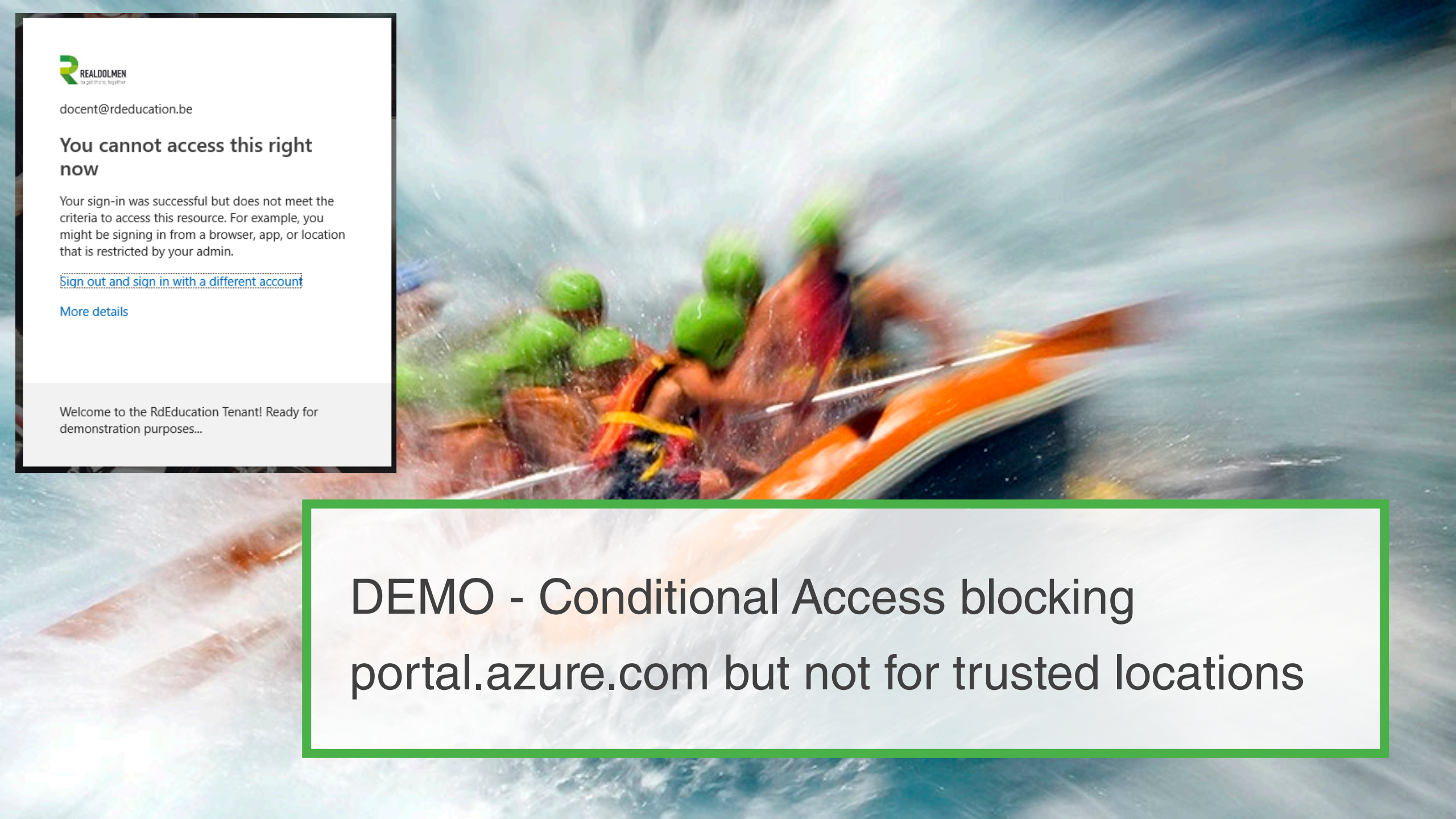
You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

[Sign out and sign in with a different account](#)

[More details](#)

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



DEMO - Conditional Access blocking
portal.azure.com but not for trusted locations

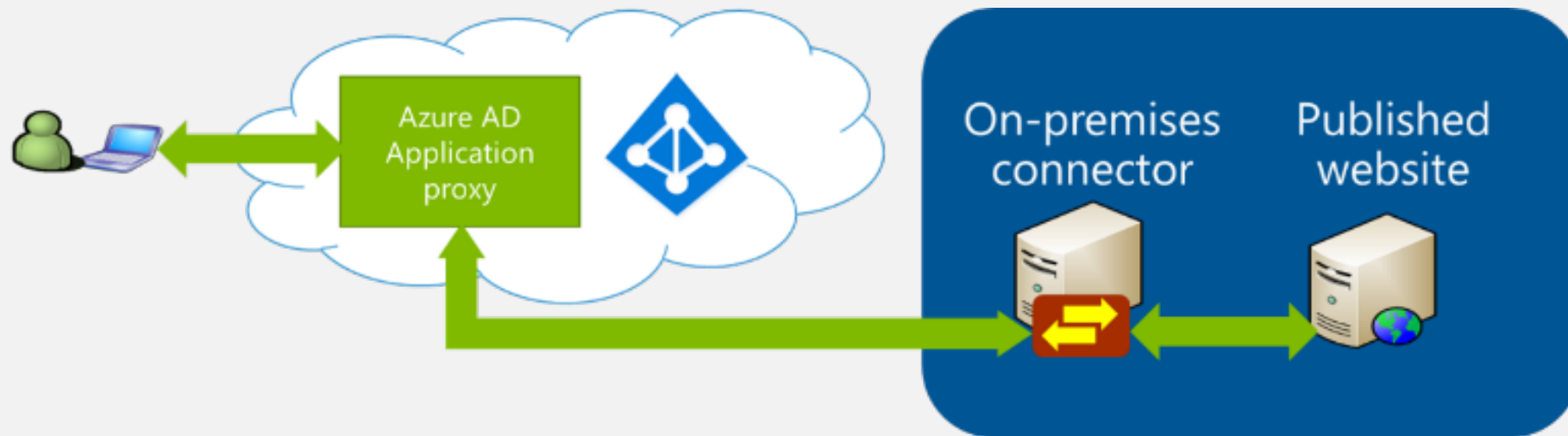


AAD APPLICATION PROXY



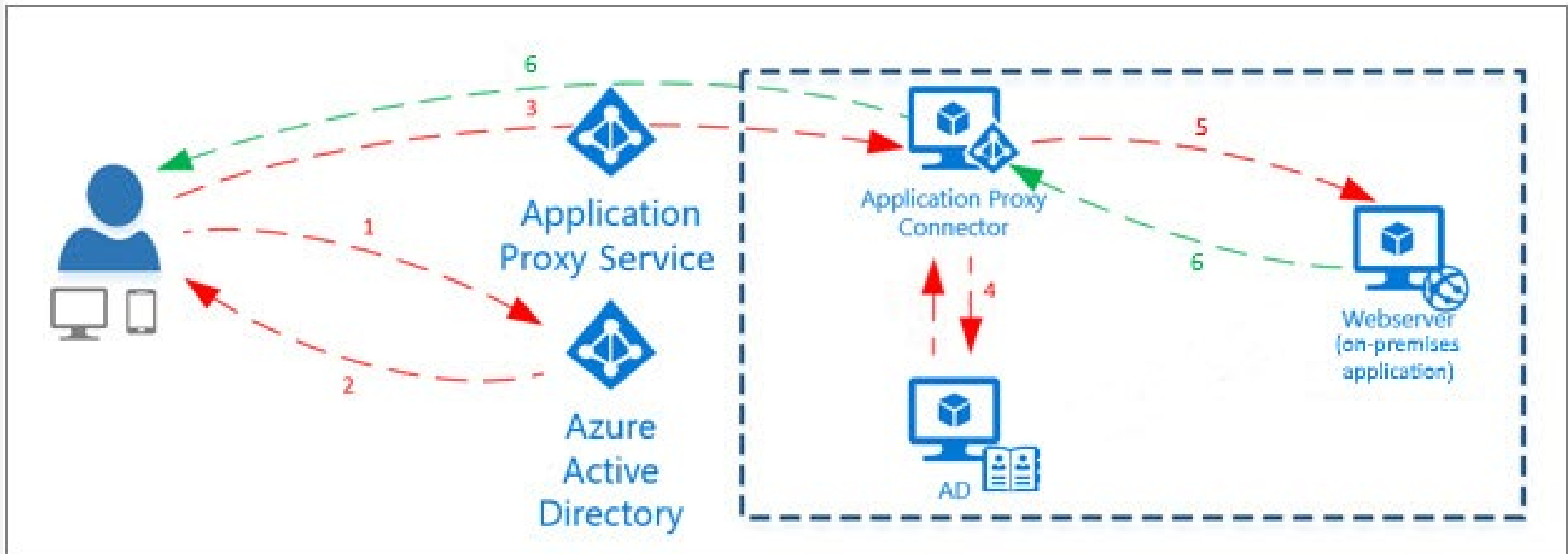
WHAT IS AZURE ACTIVE DIRECTORY APPLICATION PROXY?

- Works as a reverse proxy with AAD identity integrated
- One or more connectors are installed to create an open HTTPS connection
- Integrated authentication is available
- No need to change the network infrastructure



USER ACCESS FLOW

1. Authentication to AAD
2. Authentication passed to service
3. Service passed auth to proxy connector using open HTTPS
4. Optional authentication using internal AD by connector
5. Web Request passed to internal Web Server
6. Reply passed to connector & service to user



APPLICATION PROXY CONNECTOR SETTINGS

Enterprise applications - Application proxy

Realdolmen Education - Azure Active Directory

Overview

Manage

All applications

Application proxy

User settings

Security

Conditional Access

Activity

Sign-ins

Audit logs

Disable application proxy + Configure an app

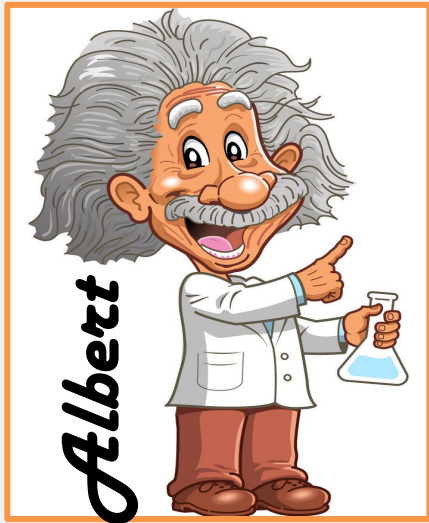
Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. [Learn more about Application Proxy](#)

Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

New Connector Group Download connector service

GROUPS	IP	STATUS
Default		
srv-rdg01.gallia.local	85.234.194.188	Active



APPLICATION PROXY CONFIGURATION

- Internal URI
- Msaproxy.net domain or allowed domain of AAD tenant with own certificate
- Pre authentication AAD or not
- Cookie settings
- URL translation settings



Basic Settings

* Internal Uri ⓘ

External Uri ⓘ 📄

Pre Authentication ⓘ

Connector Group ⓘ

ⓘ We recommend at least two active connectors in each group. Click here to download a new connector or manage your connector groups.

Additional Settings

Backend Application Timeout ⓘ

Use HTTP-Only Cookie ⓘ

Use Secure Cookie ⓘ

Use Persistent Cookie ⓘ

Translate URLs In

Headers ⓘ

Application Body ⓘ



APPLICATION SIGN-ON SETTINGS



Select a single sign-on method [Help me decide](#)



Disabled

User must manually enter their username and password.



SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.



Password-based

Password storage and replay using a web browser extension or mobile app.



Linked

Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.



Windows Integrated Authentication

Allows the Application Proxy Connectors permission in Active Directory to impersonate users to the published application.



Header-based

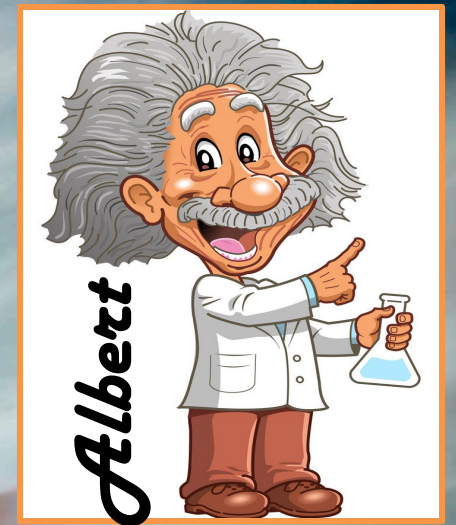
A PingAccess offering that gives users access and single sign-on to applications that use headers for authentication.



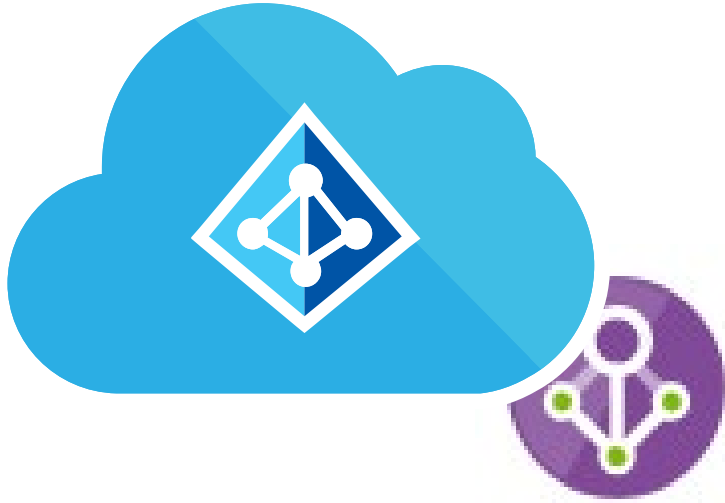
APPLICATION USAGE LOGGING

DATE	↑↓	USER	↑↓	APPLICATION	↑↓	STATUS	CONDITIONAL ACCESS	MFA REQUIRED
15/3/2019 12:49:12		admin EducRD		PanoramixWEB		Success	Not Applied	No
14/3/2019 18:47:54		admin EducRD		PanoramixWEB		Success	Not Applied	No
14/3/2019 18:46:45		Harold Baele		PanoramixWEB		Failure	Not Applied	No
14/3/2019 18:36:41		admin EducRD		PanoramixWEB		Success	Not Applied	No
14/3/2019 18:30:12		admin EducRD				Success	Not Applied	No





Demo- PanoramixWeb in
myapps.microsoft.com



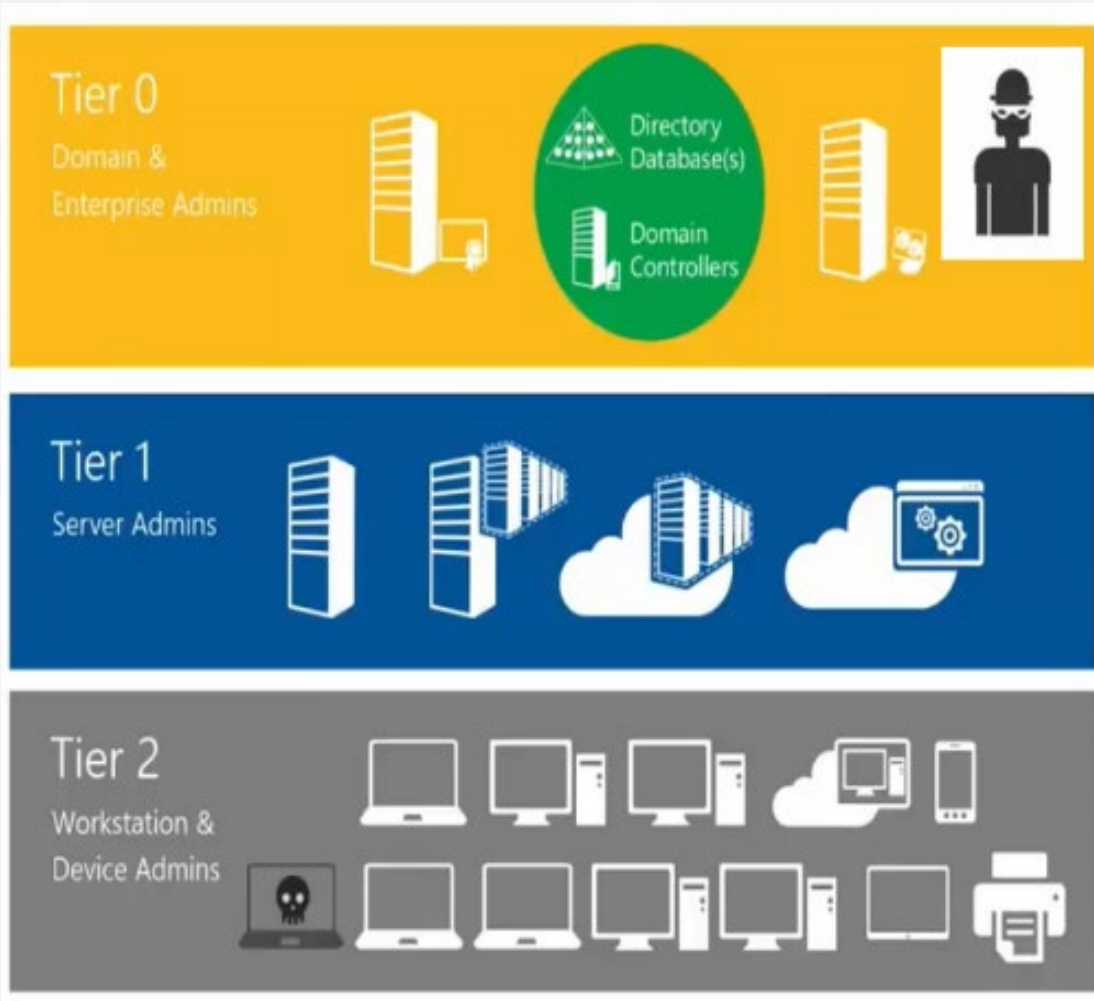
AAD PRIVILEGED IDENTITY MANAGEMENT



Why PIM? Think like a bad guy...



CREDENTIAL THEFT

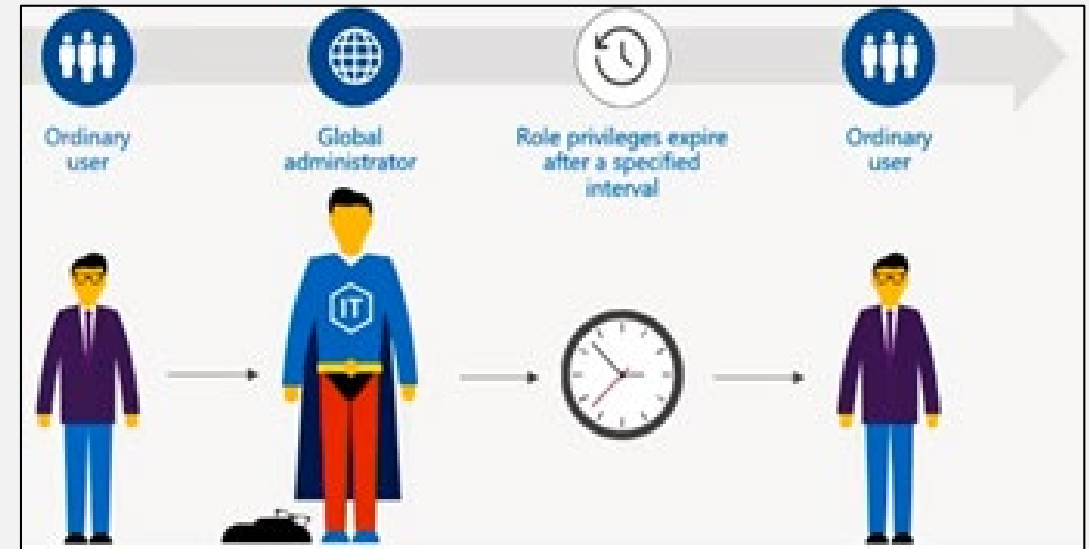


- Begins by establishing a beachhead in a Tier 2 workstation or device
- The local administrator accounts are used to compromise more hosts and credentials in Tier 2.
- When they gain Domain Admin credentials, they begin a more focused attack on your system
- At the highest level, Tier 0, the attacker has unlimited permissions



AZURE AD PIM

- PIM, just-in-time administration:
Same user becomes Admin and loses it again
- Granular admin-like roles are available
- View/Audit administrator activation
- Can require approval to activate
- Review membership of administrative roles



EXAMPLE SCENARIOS OF AAD PIM



Do more with Azure AD Privileged Identity Management

- ✓ Require Multi-Factor Authentication
- ✓ Log service/ticket numbers when activating
- ✓ Schedule activations for a specific date
- ✓ Require approval workflow to activate
- ✓ Receive notifications when users are assigned
- ✓ Configure and resolve alerts for privileged roles



MODIFY ROLES

- Just in time provides the user or group members with eligible but not persistent access to the role for a specified period or indefinitely (if configured in role settings)
- Permanent does not require the user or group members to activate the role assignment

Conditional Access Administrator

Save Discard

Activations

Maximum activation duration (hours) 8

Notifications

Send email notifying admins of activation

Enable Disable

Incident/Request ticket

Require incident/request ticket number during activation

Enable Disable

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation

Enable Disable

Require approval

Require approval to activate this role

Enable Disable

Harold Baele (Radmin)

Conditional Access Administrator

Make eligible More

Name: ↑ Make permanent

Harold Baele ↓ Remove

Email: admharold@rdemos.onmicrosoft.com

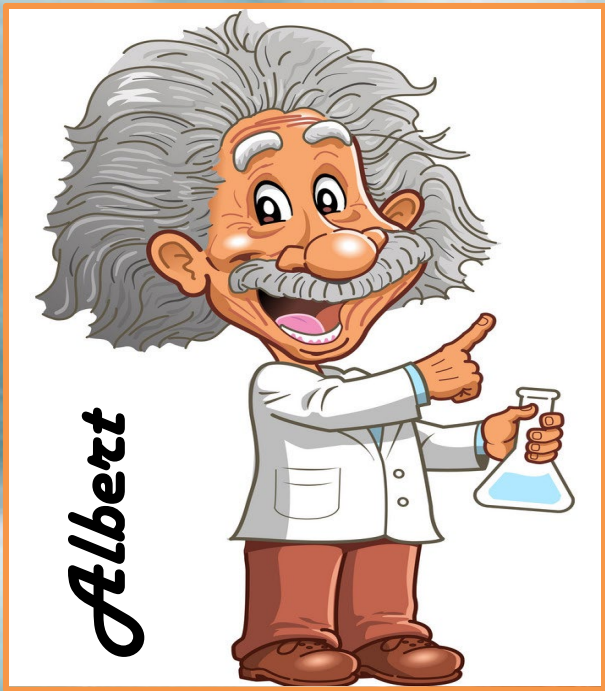
Activation

Eligible

Expiration

-





WALK THROUGH – PIM user becoming
Global Administrator

ACTIVATING GLOBAL ADMINISTRATOR ROLE USING PIM

Login using <https://aad.portal.azure.com>

Activate a eligible role

My roles - Azure AD roles

Activate

- Azure AD roles
- Azure resource roles

Troubleshooting + Support

- Troubleshoot
- New support request

Eligible roles [Active roles](#)

[Refresh](#)

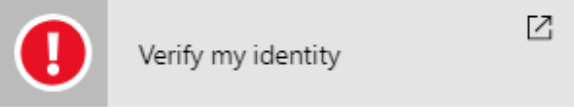
ROLE NAME	STATUS	PENDING REQUESTS	ACTION
Global Administrator	Not active	0 pending request(s)	Activate
Conditional Access Administrator	Not active	0 pending request(s)	Activate
Privileged Role Administrator	Not active	0 pending request(s)	Activate



ACTIVATING GLOBAL ADMINISTRATOR ROLE USING PIM

Verify your identity with MFA

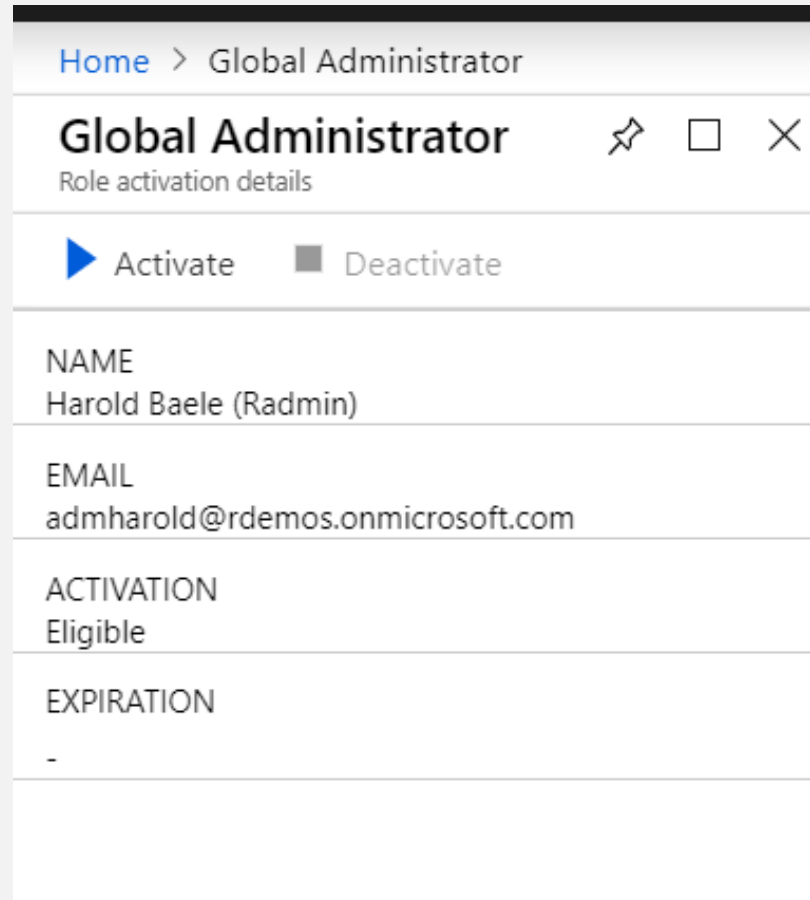
Dashboard > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Verify my identity

Global Administrator	Verify my identity
Role activation details	Global Administrator
▶ Activate ■ Deactivate	Before you activate this role, verify your identity with Azure Multi-Factor Authentication. If you haven't registered with Azure MFA yet, we'll help you do that.
⚠ Verify your identity before proceeding →	
NAME Harold Baele (Radmin)	
EMAIL admharold@rdemos.onmicrosoft.com	
ACTIVATION Eligible	
EXPIRATION -	



ACTIVATING GLOBAL ADMINISTRATOR ROLE USING PIM

Start the activation of the role



The screenshot shows a user interface for managing roles. At the top, there is a breadcrumb navigation: "Home > Global Administrator". Below this, the title "Global Administrator" is displayed with a star icon, a square icon, and a close icon. Underneath the title, it says "Role activation details". There are two buttons: "Activate" with a blue play icon and "Deactivate" with a grey square icon. Below the buttons, there are four rows of information:

NAME	Harold Baele (Radmin)
EMAIL	admharold@rdemos.onmicrosoft.com
ACTIVATION	Eligible
EXPIRATION	-



ACTIVATING GLOBAL ADMINISTRATOR ROLE USING PIM

Home > Global Administrator > Activation

Activation

Role activation details

Custom activation start time

Activation duration (hours)

2

* Activation reason (max 500 characters)

Demonstrating PIM for Global Administrator role ✓

Activate

Activation status

- ✓ **Stage 1**
Processing your request and activating your role.
- ✓ **Stage 2**
Validating that your activation is successful.
- ✓ **Stage 3**
Activation complete, use the link below to sign out and log back in to start using your newly activated role.


[Sign out](#)

Define duration and reason

Wait for activation stages

Get the confirmation mail

Sign out

 Microsoft Azure

Your Global Administrator role was activated in the RDemos.onmicrosoft.com directory

Activation details

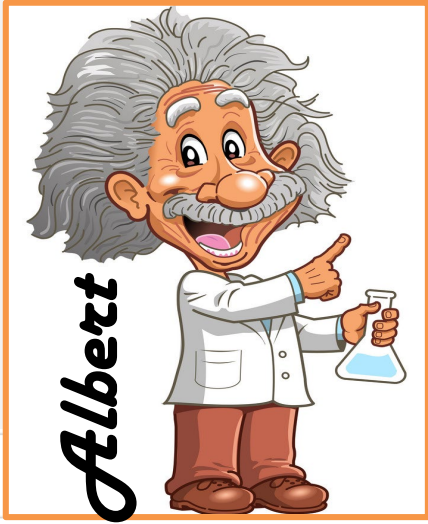
Settings	Value
Expiration:	until 3/14/2019 3:00:31 PM UTC
Justification:	Demonstrating PIM for Global Administrator role

You can re-activate or cancel your role activation in the [Azure Active Directory Privileged Identity Management extension](#) on the Azure portal.

[Learn more about Azure AD Privileged Identity Management >](#)



ACTIVATING GLOBAL ADMINISTRATOR ROLE USING PIM



Login & do your thing!

You can verify your roles & validity

Activate

- Azure AD roles
- Azure resource roles
- Troubleshooting + Support
 - Troubleshoot
 - New support request

Eligible roles [Active roles](#)

[Refresh](#)

ROLE NAME	STATUS	PENDING REQUESTS	ACTION
Global Administrator	Access valid until March 14 at 4:00 PM	0 pending request(s)	Activate
Conditional Access Administrator	Not active	0 pending request(s)	Activate
Privileged Role Administrator	Not active	0 pending request(s)	Activate



New challenges **NEW IDEAS**

