LAKEFOREST

CONSULTING

LAKEFOREST

CONSULTING

Protecting the Keys to the Kingdom

Kaido Järvemets

About me

- Enterprise Architect and partner @LakeForest Consulting
  - Microsoft MVP: Enterprise Mobility
  - Microsoft Certified Trainer
  - Security+
  - Certified Red Team Professional
  - Azure Security Engineer

Microsoft® MVP Most Valuable Professional

@Kaidja

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

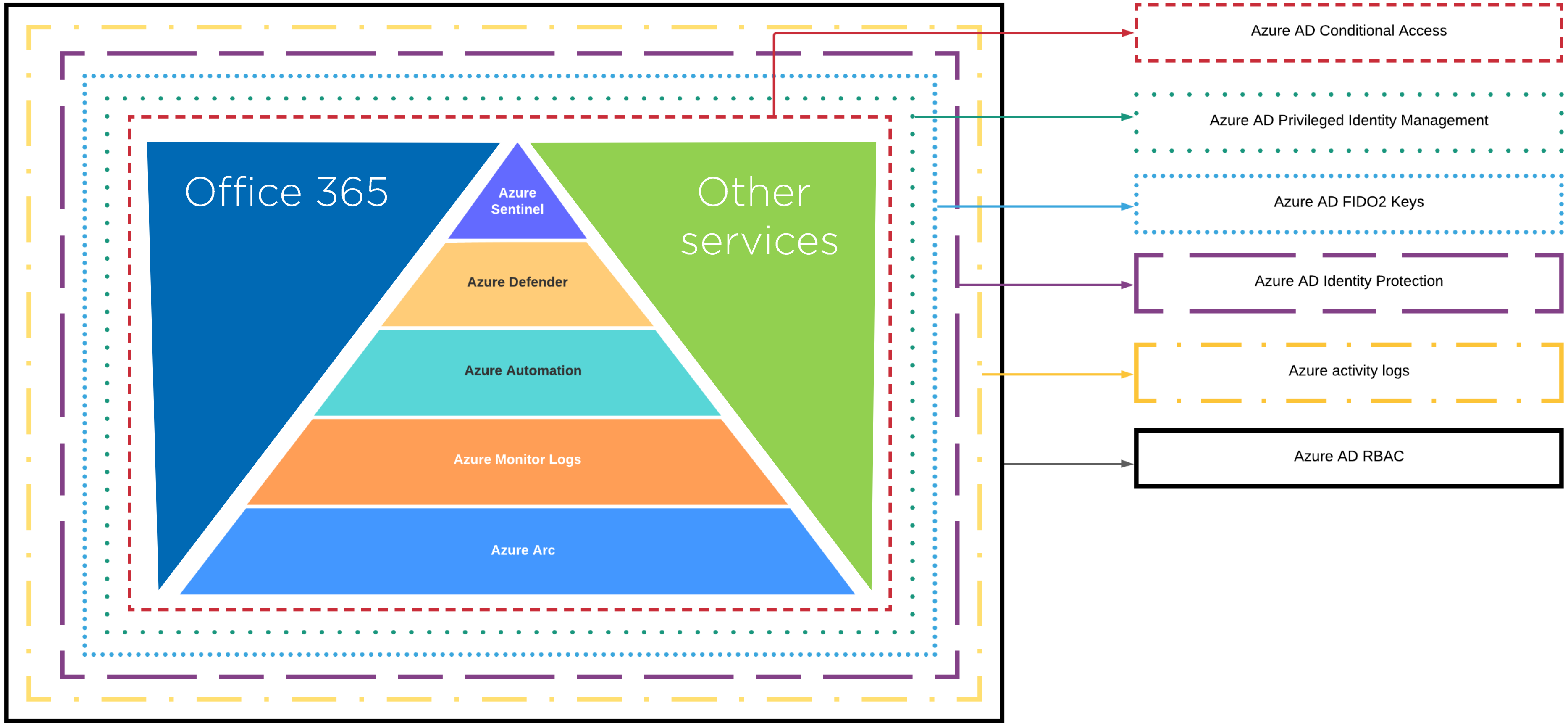
https://lakeforestconsulting.com/

https://www.linkedin.com/company/lakeforest-consulting

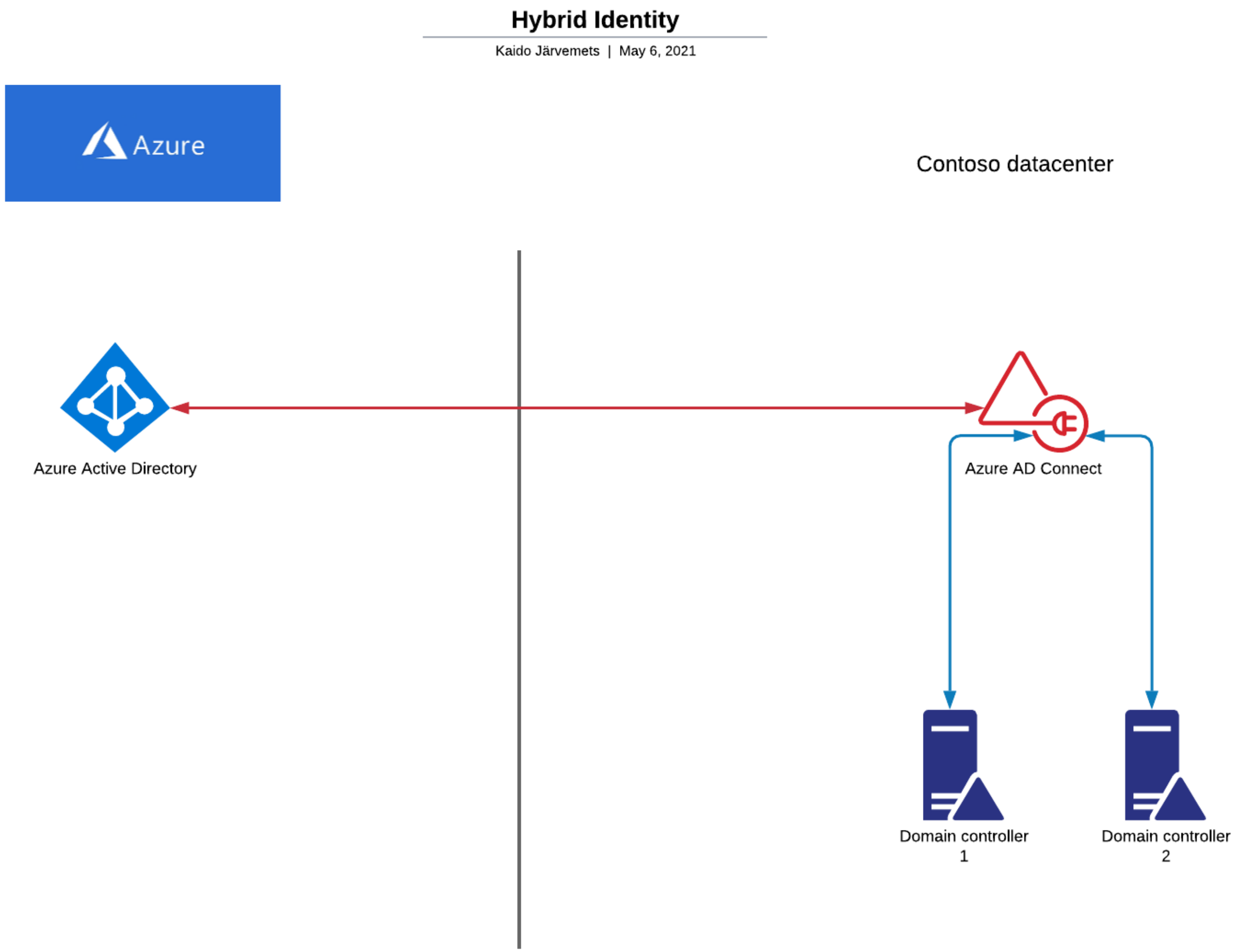
Today

Azure Administrative model

Kaido Järvemets



Hybrid Identity



Hybrid Identity

Kaido Järvemets | May 6, 2021

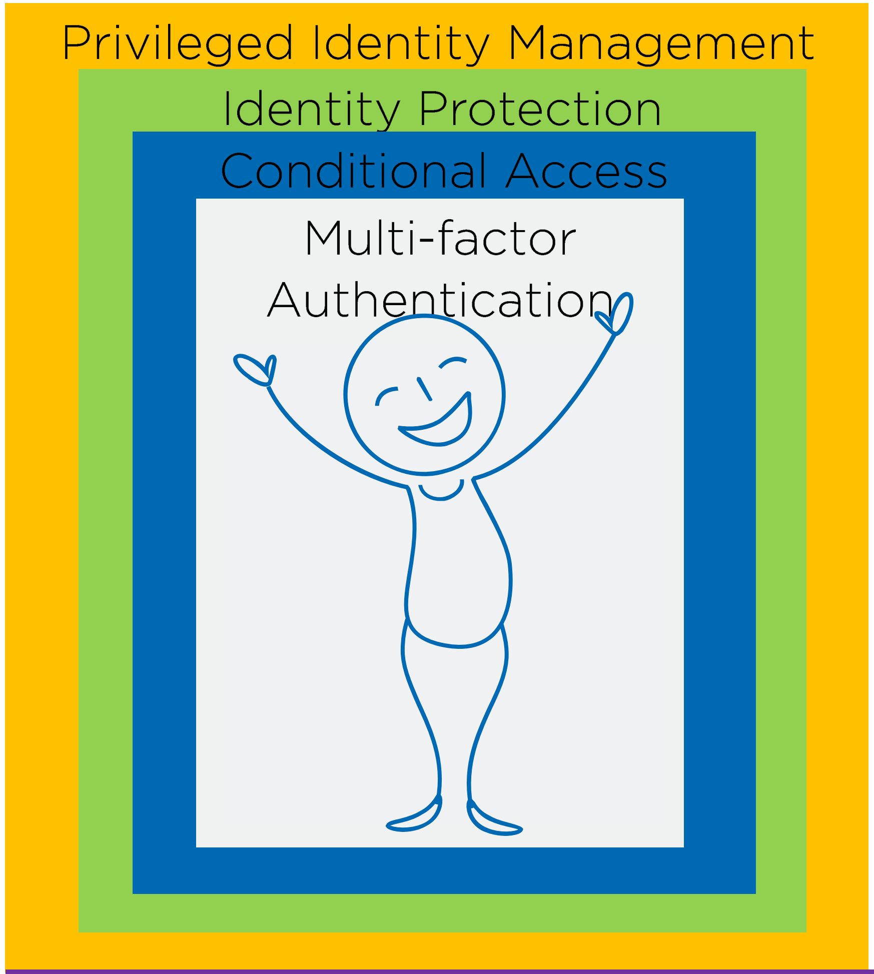
How much?

TECHNICAL DEBT
I DON'T UNDERSTAND WHY IT TAKES SO LONG TO ADD A NEW WINDOW.
@VINCENTDNL

What do we need?

Teenus	Azure AD Premium P2 / Microsoft 365 E5 / Enterprise Mobility +Security E5	Azure AD Premium P1 / Microsoft 365 E3 / Enterprise Mobility +Security E3
Conditional Access	Yes	Yes
Multi-factor Authentication	Yes	Yes
Identity Protection	Yes	No
Privileged Identity Management	Yes	No

Combined package



Privileged Identity Management

Identity Protection

Conditional Access

Multi-factor Authentication

+

Secure Access Workstation

Important!

If you are going to implement Azure Administrative Model make sure to you agree the principles first!

For some, this will be hard to understand and accept.

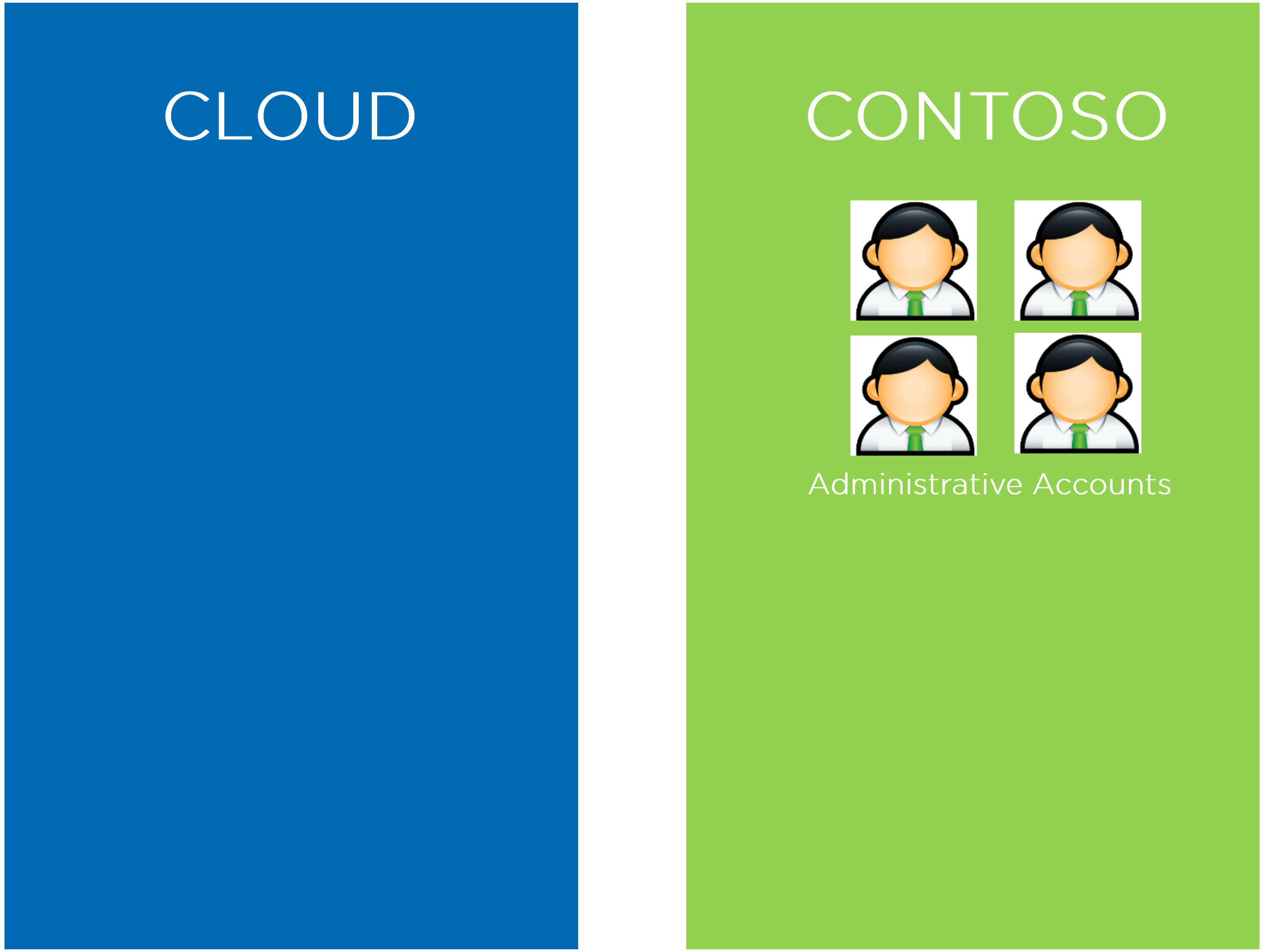
Important! #2

Today we are primarily focusing on administrators

What do we want?

- No passwords!
- We want to control the access paths
  - Compliant, managed, location etc.
- We do not want administrators to have administrative rights 24H
- All high privileged accounts should be “*Approve*” only

What many are doing today #1

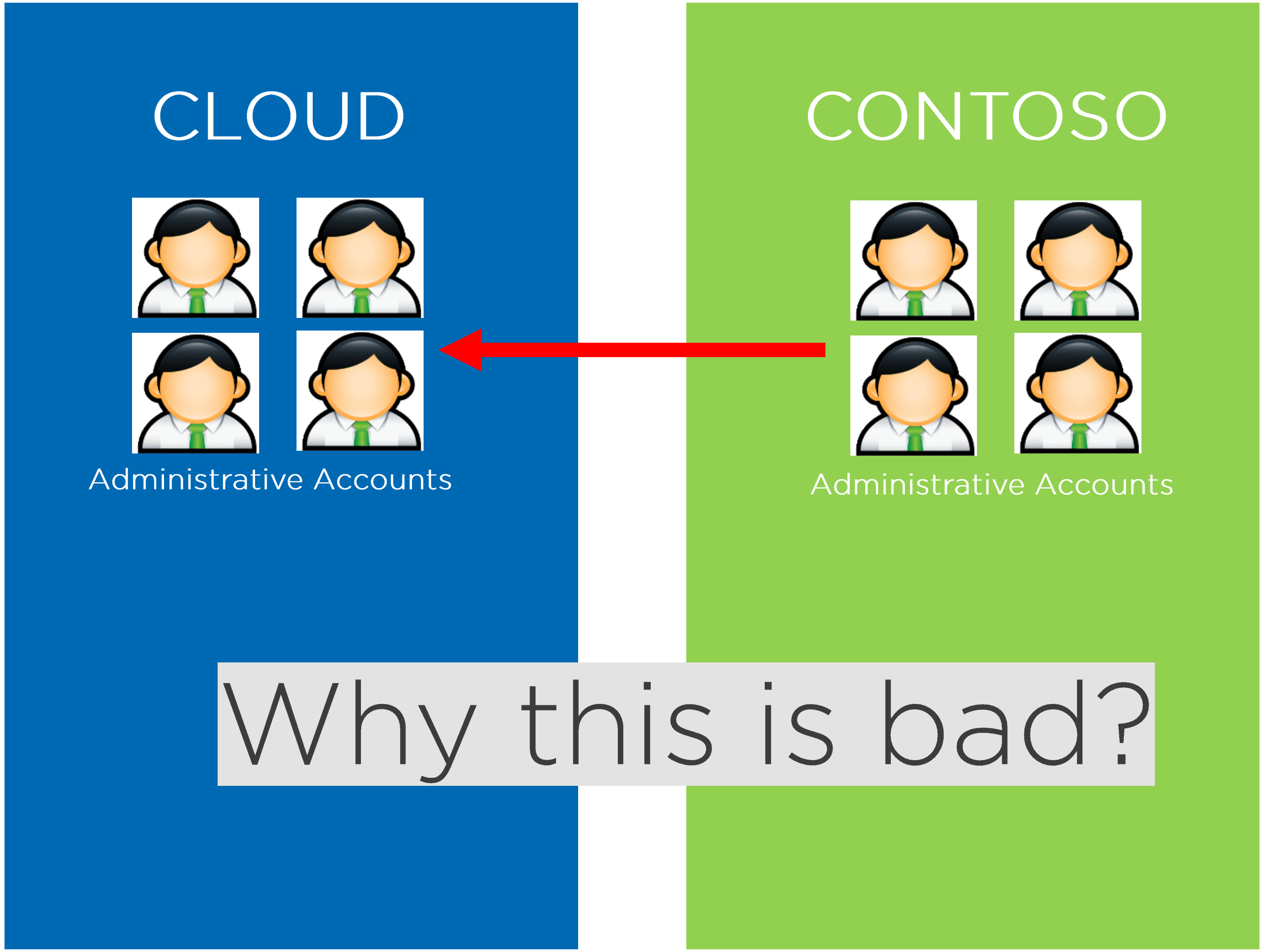


CLOUD

CONTOSO

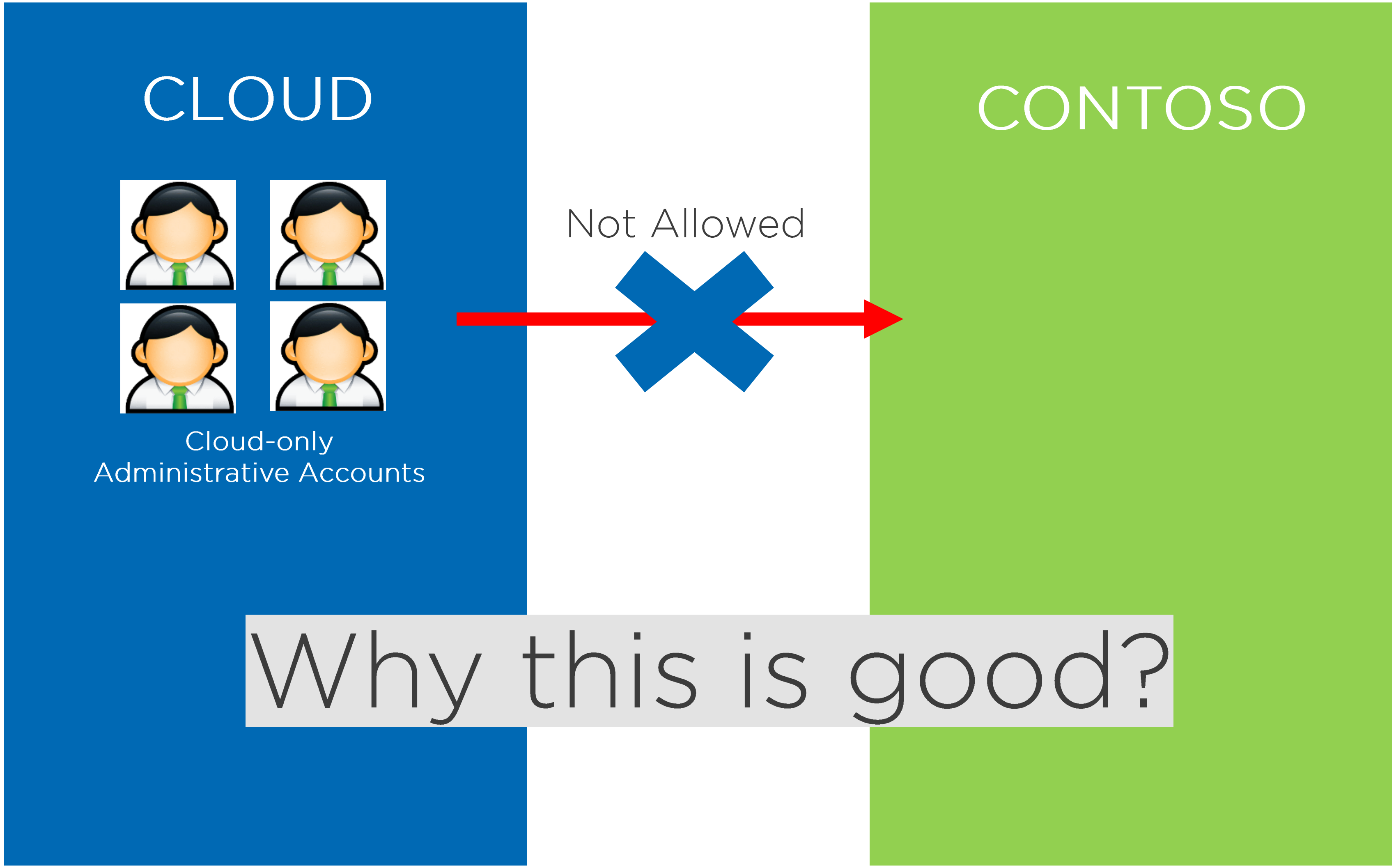
Administrative Accounts

What many are doing today #2



Why this is bad?

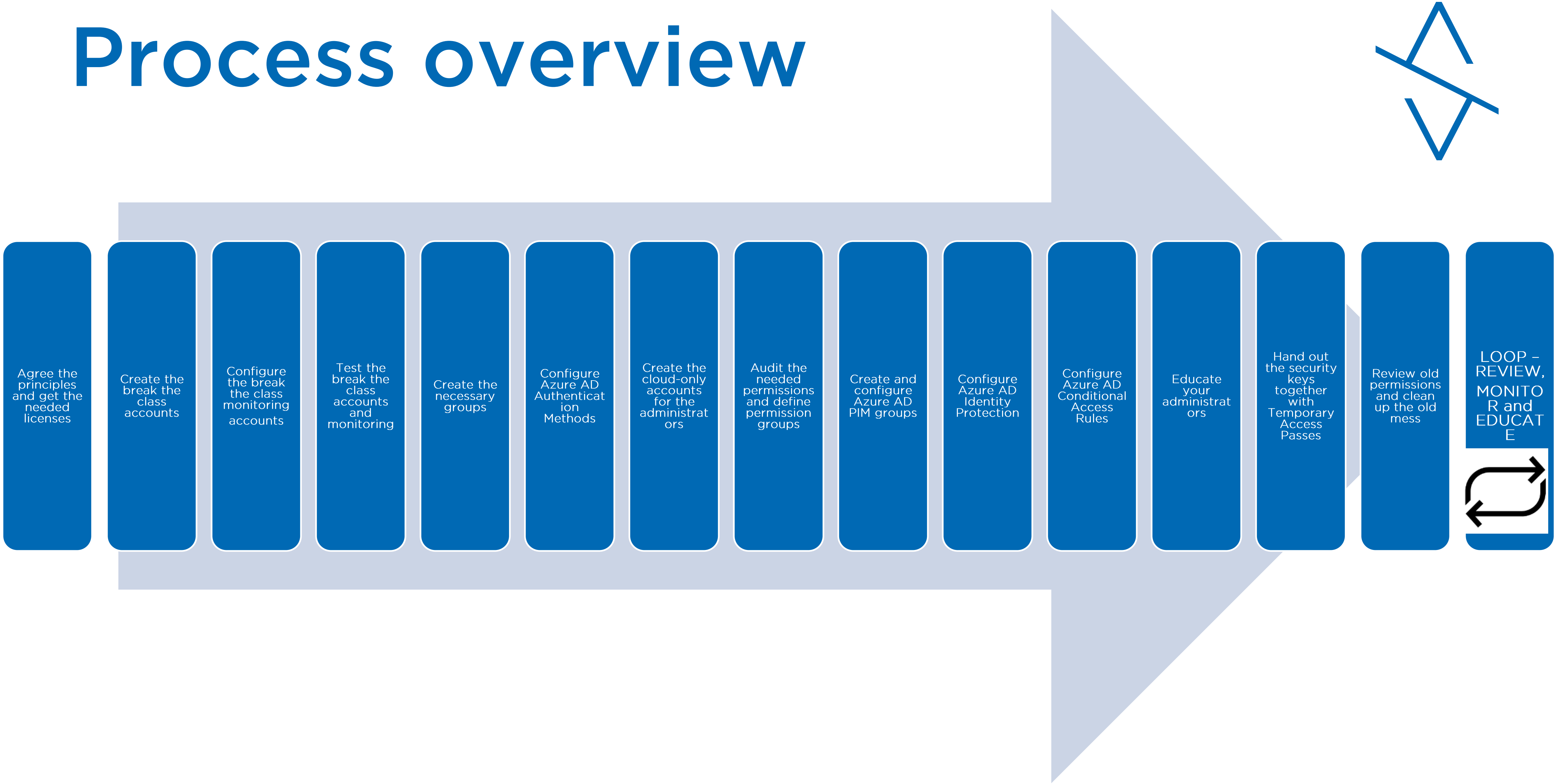
What should we do?



Why this is good?

Passwordless
authentication
ctrl
alt

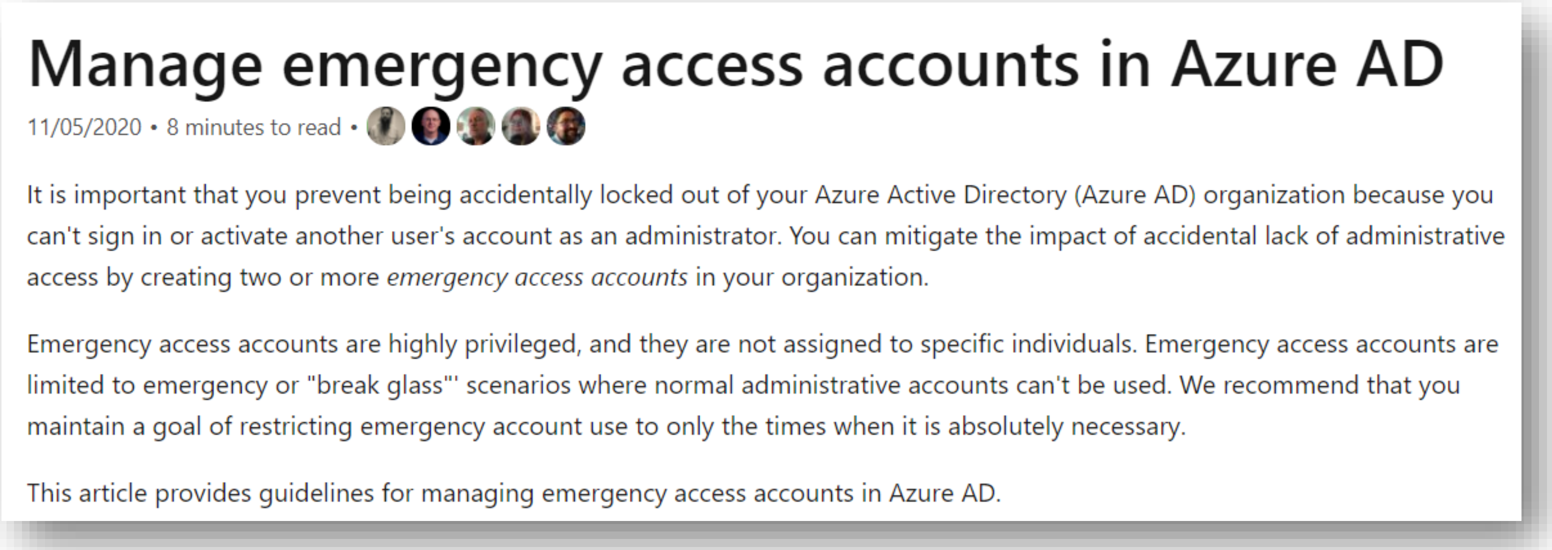
Process overview



- Agree the principles and get the needed licenses
- Create the break the class accounts
- Configure the break the class monitoring accounts
- Test the break the class accounts and monitoring
- Create the necessary groups
- Configure Azure AD Authentication Methods
- Create the cloud-only accounts for the administrators
- Audit the needed permissions and define permission groups
- Create and configure Azure AD PIM groups
- Configure Azure AD Identity Protection
- Configure Azure AD Conditional Access Rules
- Educate your administrators
- Hand out the security keys together with Temporary Access Passes
- Review old permissions and clean up the old mess
- LOOP – REVIEW, MONITOR and EDUCATE

Before you begin!

- Make sure you have at least two different “Break the class accounts” for Azure Active Directory
- These accounts must be cloud-only
- Protect the accounts with FIDO2 security keys
  - No stored passwords!
- Monitoring must be enabled!
  - Use Azure Sentinel!



Manage emergency access accounts in Azure AD

11/05/2020 • 8 minutes to read •

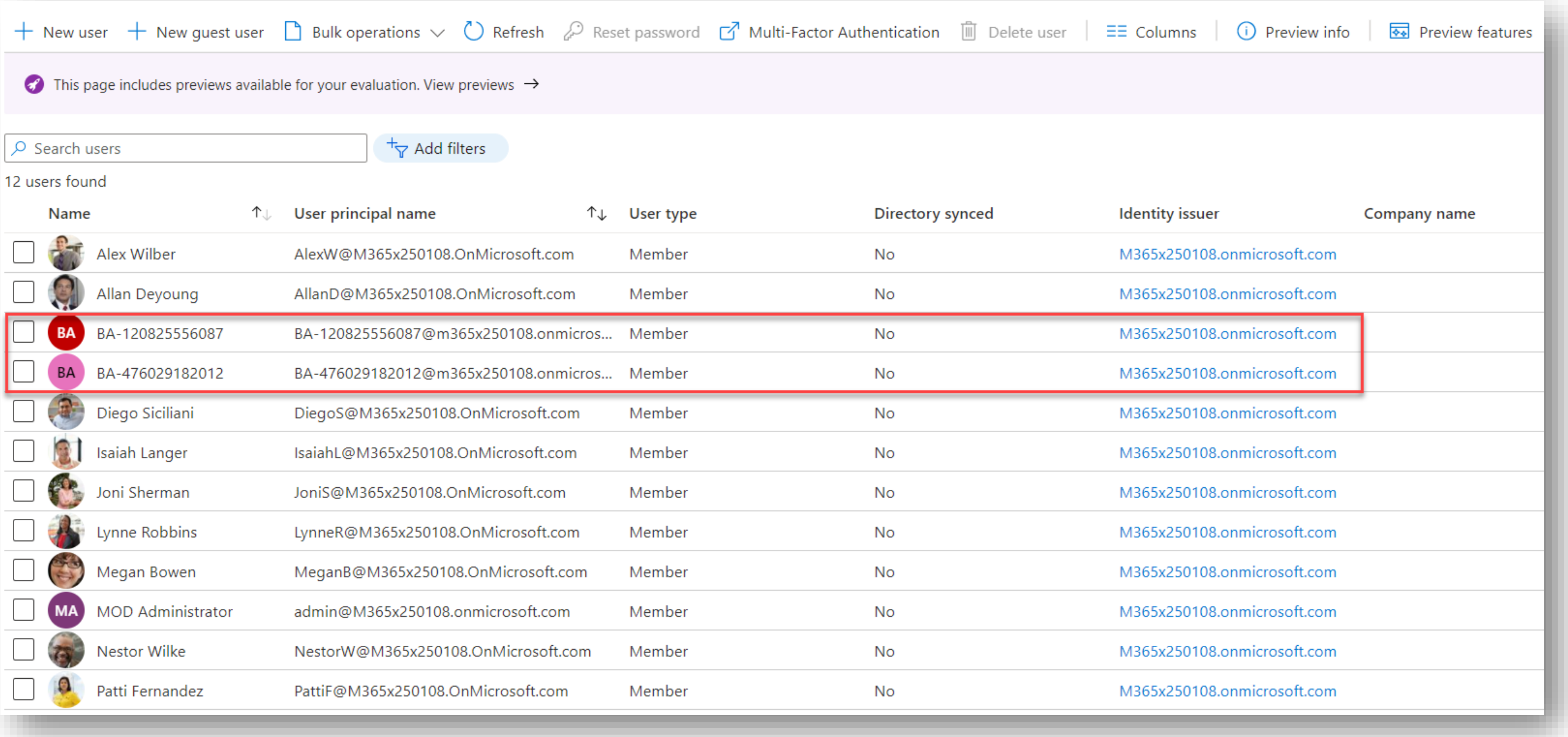
It is important that you prevent being accidentally locked out of your Azure Active Directory (Azure AD) organization because you can't sign in or activate another user's account as an administrator. You can mitigate the impact of accidental lack of administrative access by creating two or more *emergency access accounts* in your organization.

Emergency access accounts are highly privileged, and they are not assigned to specific individuals. Emergency access accounts are limited to emergency or "break glass"' scenarios where normal administrative accounts can't be used. We recommend that you maintain a goal of restricting emergency account use to only the times when it is absolutely necessary.

This article provides guidelines for managing emergency access accounts in Azure AD.

https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

Before you begin! #2



This page includes previews available for your evaluation. View previews →

12 users found

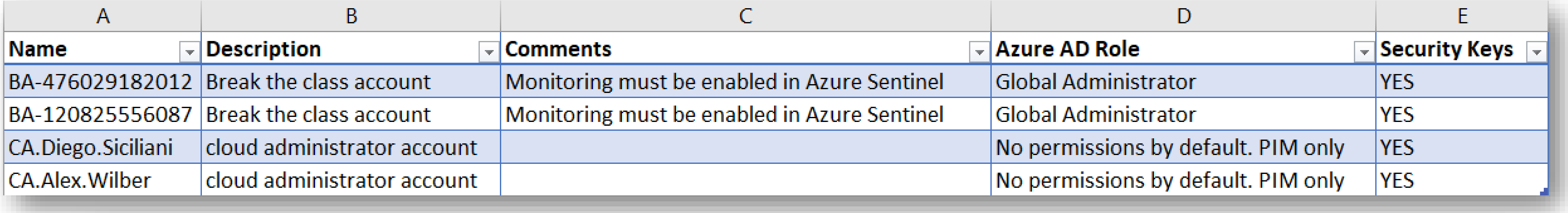
Name	User principal name	User type	Directory synced	Identity issuer	Company name
Alex Wilber	AlexW@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
Allan Deyoung	AllanD@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
BA-120825556087	BA-120825556087@m365x250108.onmicros...	Member	No	M365x250108.onmicrosoft.com	
BA-476029182012	BA-476029182012@m365x250108.onmicros...	Member	No	M365x250108.onmicrosoft.com	
Diego Siciliani	DiegoS@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
Isaiah Langer	IsaiahL@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
Joni Sherman	JoniS@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
Lynne Robbins	LynneR@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
Megan Bowen	MeganB@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
MOD Administrator	admin@M365x250108.onmicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
Nestor Wilke	NestorW@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	
Patti Fernandez	PattiF@M365x250108.OnMicrosoft.com	Member	No	M365x250108.onmicrosoft.com	

Azure Sentinel Analytics Rule

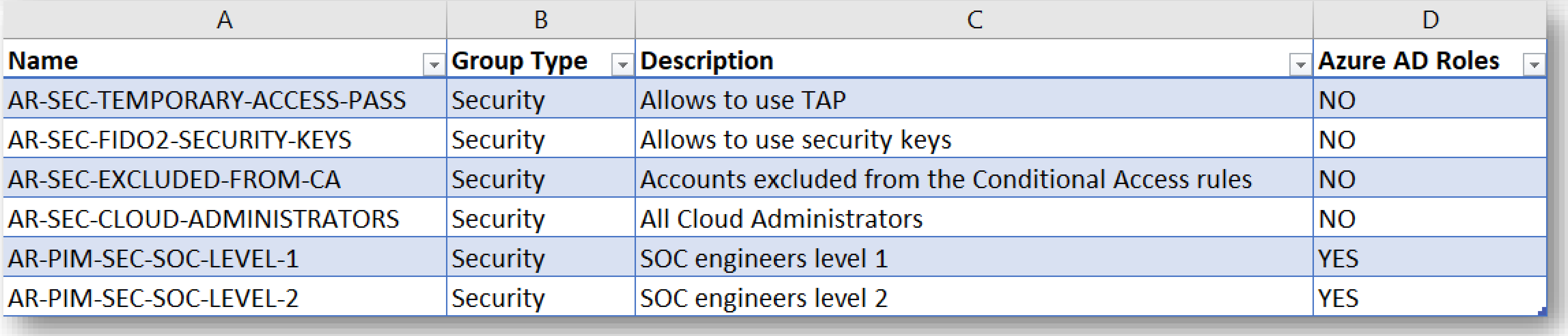
```
SigninLogs
| where UserPrincipalName == “MYBREAKTHELCASSACCOUNT1ACCOUNTID1" or
UserPrincipalName == "MYBREAKTHELCASSACCOUNT1ACCOUNTID2"
| where Status.errorCode == 0
| extend AccountCustomEntity = Identity
| extend IPCustomEntity = IPAddress
| extend HostCustomEntity = SourceSystem
```

Users and Groups

- Define and agree the naming standards for Azure AD objects
    - Groups, users etc.



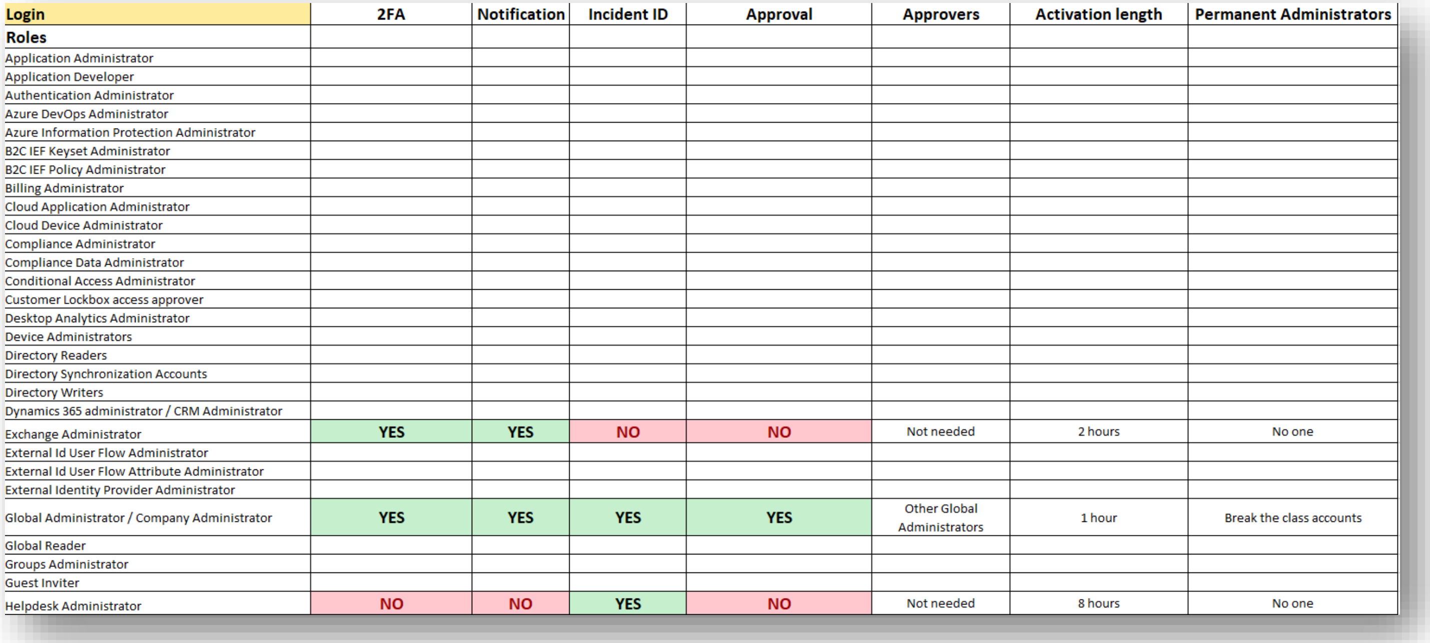
A	B	C	D	E
Name	**Description**	**Comments**	**Azure AD Role**	**Security Keys**
BA-476029182012	Break the class account	Monitoring must be enabled in Azure Sentinel	Global Administrator	YES
BA-120825556087	Break the class account	Monitoring must be enabled in Azure Sentinel	Global Administrator	YES
CA.Diego.Siciliani	cloud administrator account		No permissions by default. PIM only	YES
CA.Alex.Wilber	cloud administrator account		No permissions by default. PIM only	YES



A	B	C	D
Name	**Group Type**	**Description**	**Azure AD Roles**
AR-SEC-TEMPORARY-ACCESS-PASS	Security	Allows to use TAP	NO
AR-SEC-FIDO2-SECURITY-KEYS	Security	Allows to use security keys	NO
AR-SEC-EXCLUDED-FROM-CA	Security	Accounts excluded from the Conditional Access rules	NO
AR-SEC-CLOUD-ADMINISTRATORS	Security	All Cloud Administrators	NO
AR-PIM-SEC-SOC-LEVEL-1	Security	SOC engineers level 1	YES
AR-PIM-SEC-SOC-LEVEL-2	Security	SOC engineers level 2	YES

Auditing #1

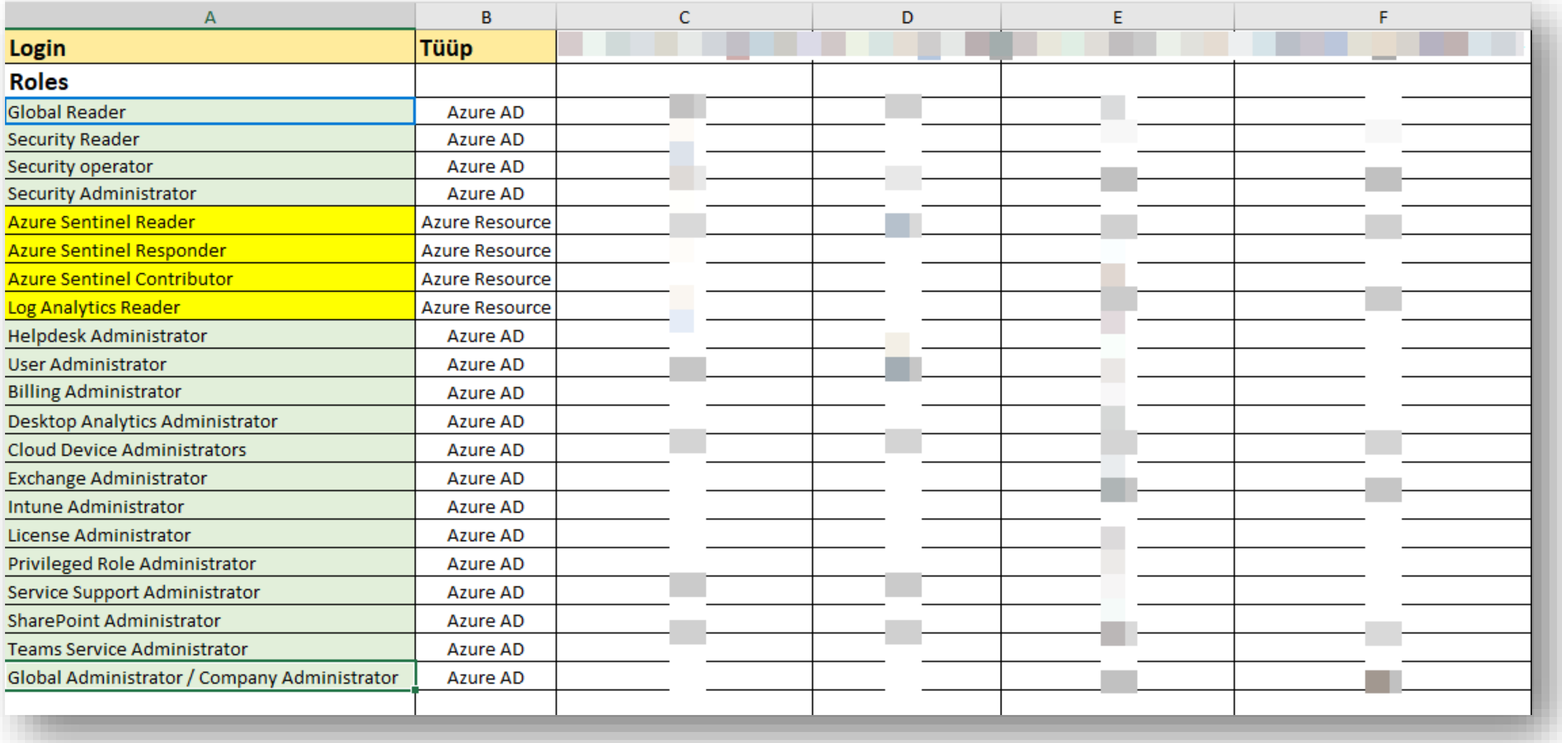
- Gather the needed permissions and define the roles
- Use Excel spreadsheet for this exercise
- Start small and move step by step



Login	2FA	Notification	Incident ID	Approval	Approvers	Activation length	Permanent Administrators
Roles							
Application Administrator							
Application Developer							
Authentication Administrator							
Azure DevOps Administrator							
Azure Information Protection Administrator							
B2C IEF Keyset Administrator							
B2C IEF Policy Administrator							
Billing Administrator							
Cloud Application Administrator							
Cloud Device Administrator							
Compliance Administrator							
Compliance Data Administrator							
Conditional Access Administrator							
Customer Lockbox access approver							
Desktop Analytics Administrator							
Device Administrators							
Directory Readers							
Directory Synchronization Accounts							
Directory Writers							
Dynamics 365 administrator / CRM Administrator							
Exchange Administrator	YES	YES	NO	NO	Not needed	2 hours	No one
External Id User Flow Administrator							
External Id User Flow Attribute Administrator							
External Identity Provider Administrator							
Global Administrator / Company Administrator	YES	YES	YES	YES	Other Global Administrators	1 hour	Break the class accounts
Global Reader							
Groups Administrator							
Guest Inviter							
Helpdesk Administrator	NO	NO	YES	NO	Not needed	8 hours	No one

Auditing #2

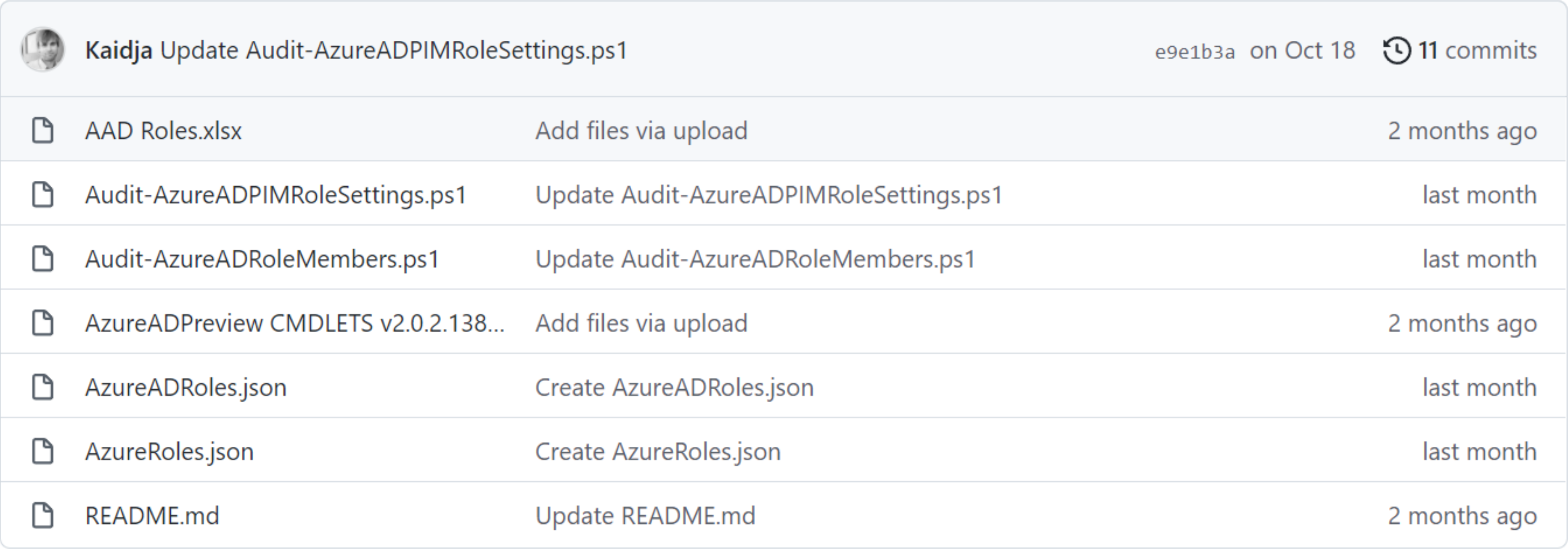
- Create Azure AD PIM enabled groups and add members and permissions
- Start with Azure AD roles and then mover over to resource-based roles.



A	B	C	D	E	F
Login	**Tüüp**	[redacted]	[redacted]	[redacted]	[redacted]
Roles					
Global Reader	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Security Reader	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Security operator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Security Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Azure Sentinel Reader	Azure Resource	[redacted]	[redacted]	[redacted]	[redacted]
Azure Sentinel Responder	Azure Resource	[redacted]	[redacted]	[redacted]	[redacted]
Azure Sentinel Contributor	Azure Resource	[redacted]	[redacted]	[redacted]	[redacted]
Log Analytics Reader	Azure Resource	[redacted]	[redacted]	[redacted]	[redacted]
Helpdesk Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
User Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Billing Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Desktop Analytics Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Cloud Device Administrators	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Exchange Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Intune Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
License Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Privileged Role Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Service Support Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
SharePoint Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Teams Service Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]
Global Administrator / Company Administrator	Azure AD	[redacted]	[redacted]	[redacted]	[redacted]

Auditing #3

- Audit existing Azure AD roles and consumption-based resources
  - You can use it as a backup when starting to clean these up



Kaidja Update Audit-AzureADPIMRoleSettings.ps1 e9e1b3a on Oct 18 11 commits

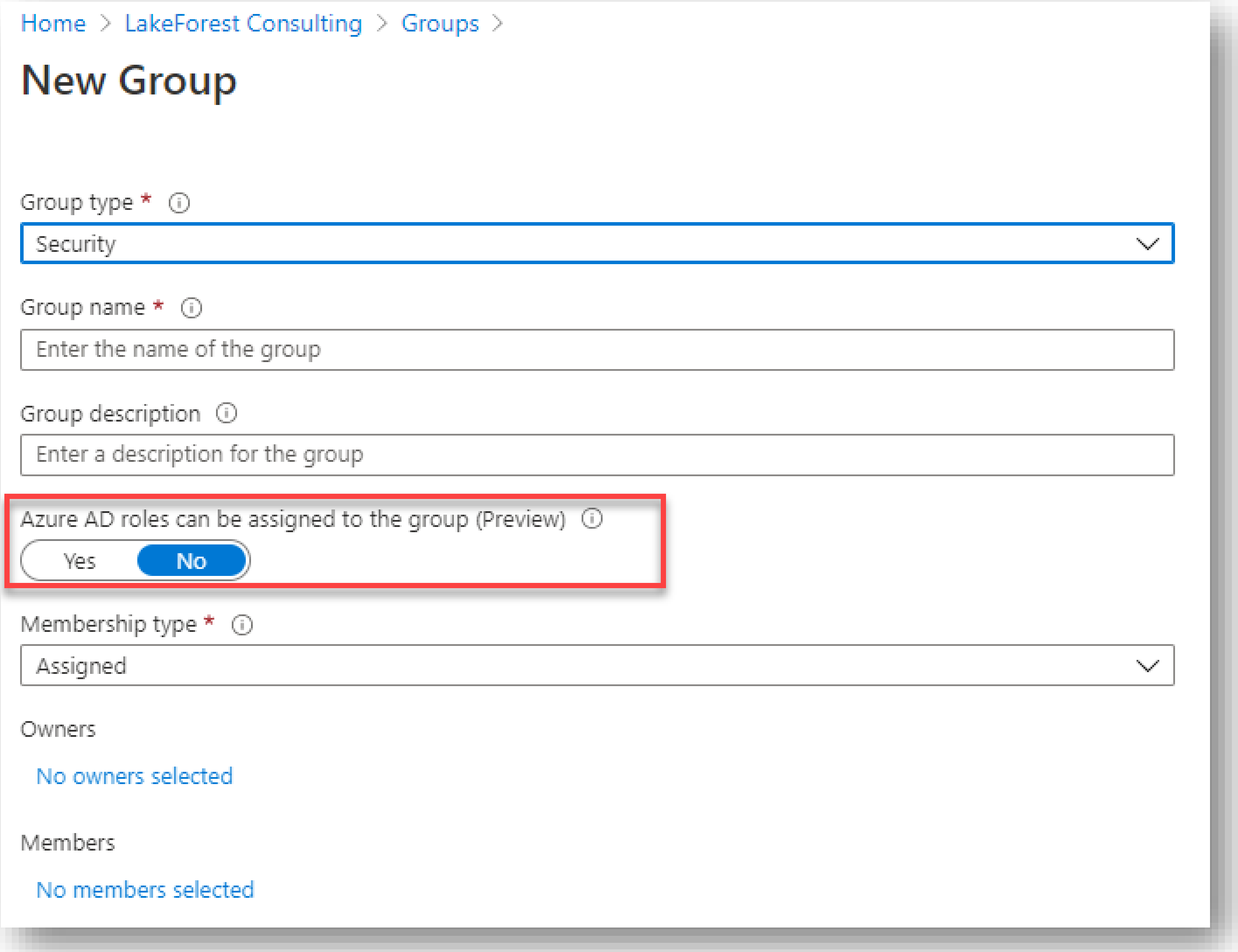
AAD Roles.xlsx	Add files via upload	2 months ago
Audit-AzureADPIMRoleSettings.ps1	Update Audit-AzureADPIMRoleSettings.ps1	last month
Audit-AzureADRoleMembers.ps1	Update Audit-AzureADRoleMembers.ps1	last month
AzureADPreview CMDLETS v2.0.2.138...	Add files via upload	2 months ago
AzureADRoles.json	Create AzureADRoles.json	last month
AzureRoles.json	Create AzureRoles.json	last month
README.md	Update README.md	2 months ago

DEMO: Auditing

Azure AD PIM

- Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.
  - Provide just-in-time privileged access to Azure AD and Azure resources
  - Assign time-bound access to resources using start and end dates
  - Require approval to activate privileged roles
  - Enforce multi-factor authentication to activate any role
  - Use justification to understand why users activate
  - Get notifications when privileged roles are activated
  - Conduct access reviews to ensure users still need roles
  - Download audit history for internal or external audit

Azure AD PIM Groups



Home > LakeForest Consulting > Groups >

New Group

Group type *

Security

Group name *

Enter the name of the group

Group description

Enter a description for the group

Azure AD roles can be assigned to the group (Preview)

Yes [✓ No]

Membership type *

Assigned

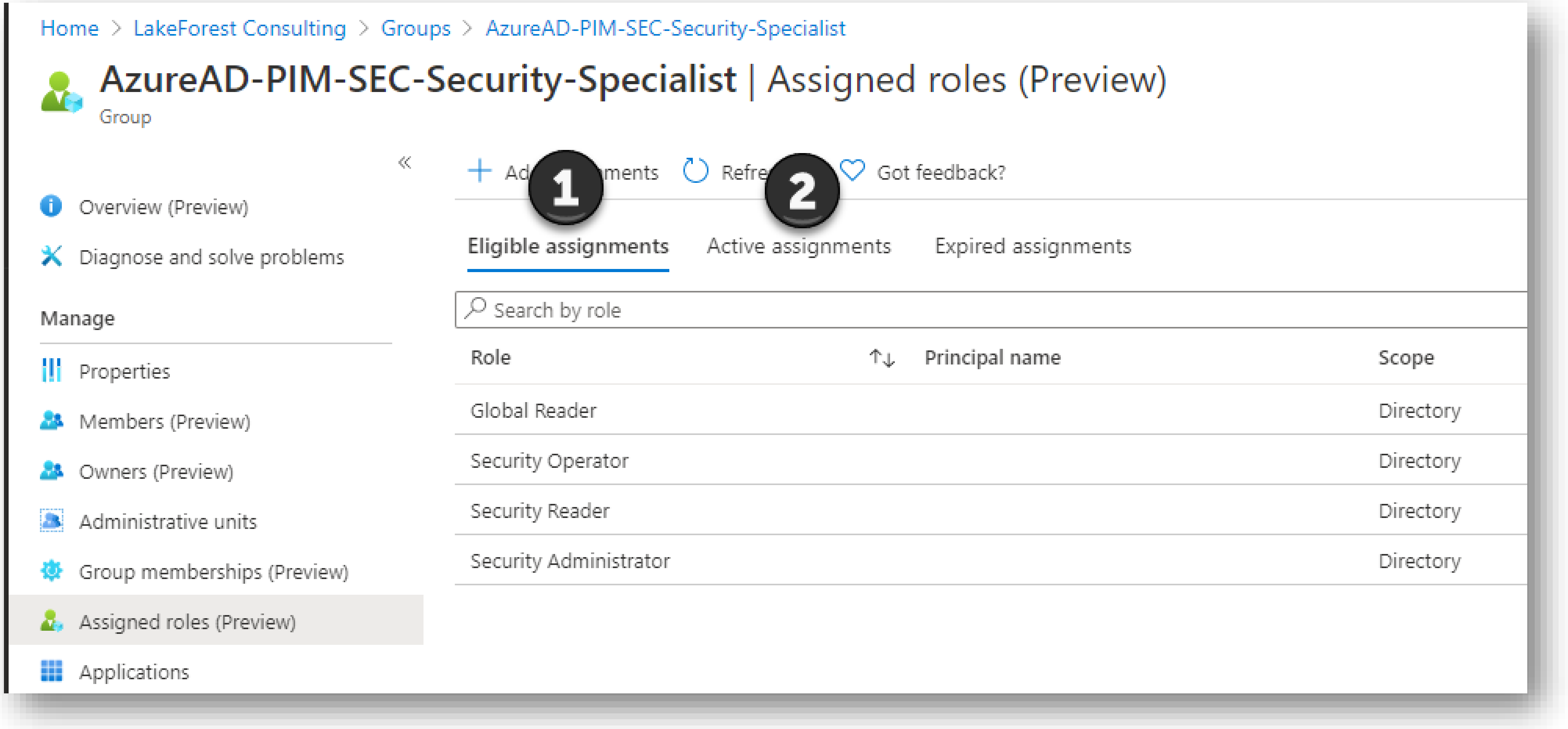
Owners

No owners selected

Members

No members selected

Azure AD PIM Groups #2



Home > LakeForest Consulting > Groups > AzureAD-PIM-SEC-Security-Specialist

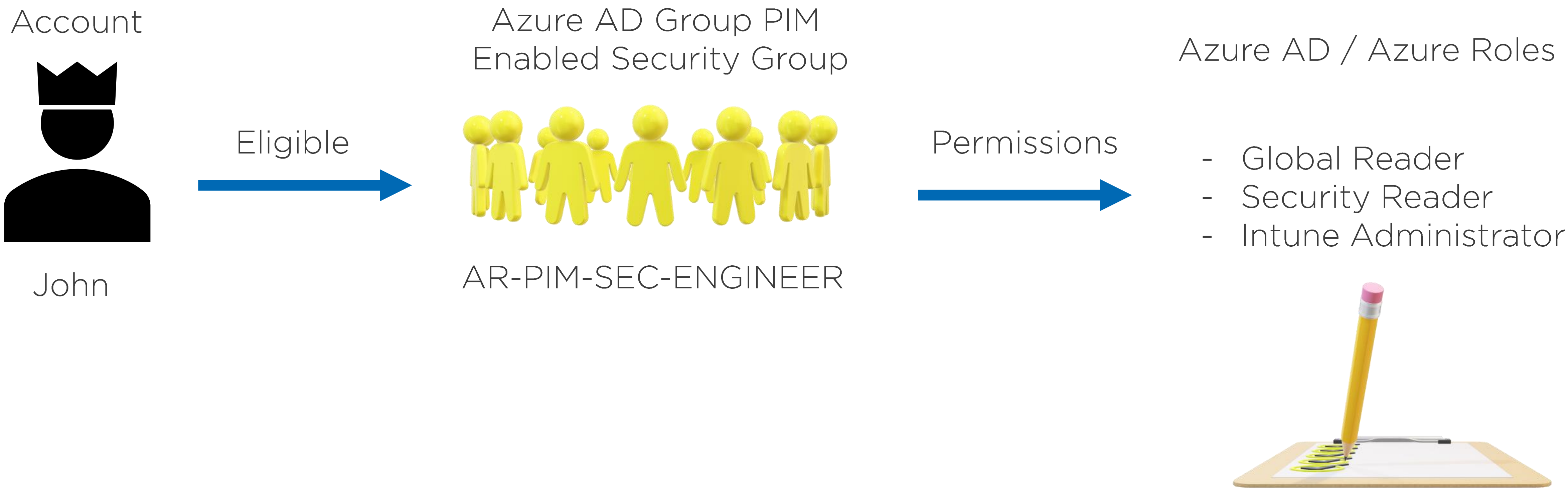
AzureAD-PIM-SEC-Security-Specialist | Assigned roles (Preview)

Group

Eligible assignments | Active assignments | Expired assignments

Role	Principal name	Scope
Global Reader		Directory
Security Operator		Directory
Security Reader		Directory
Security Administrator		Directory

Permissions



Account

John

Eligible

Azure AD Group PIM Enabled Security Group

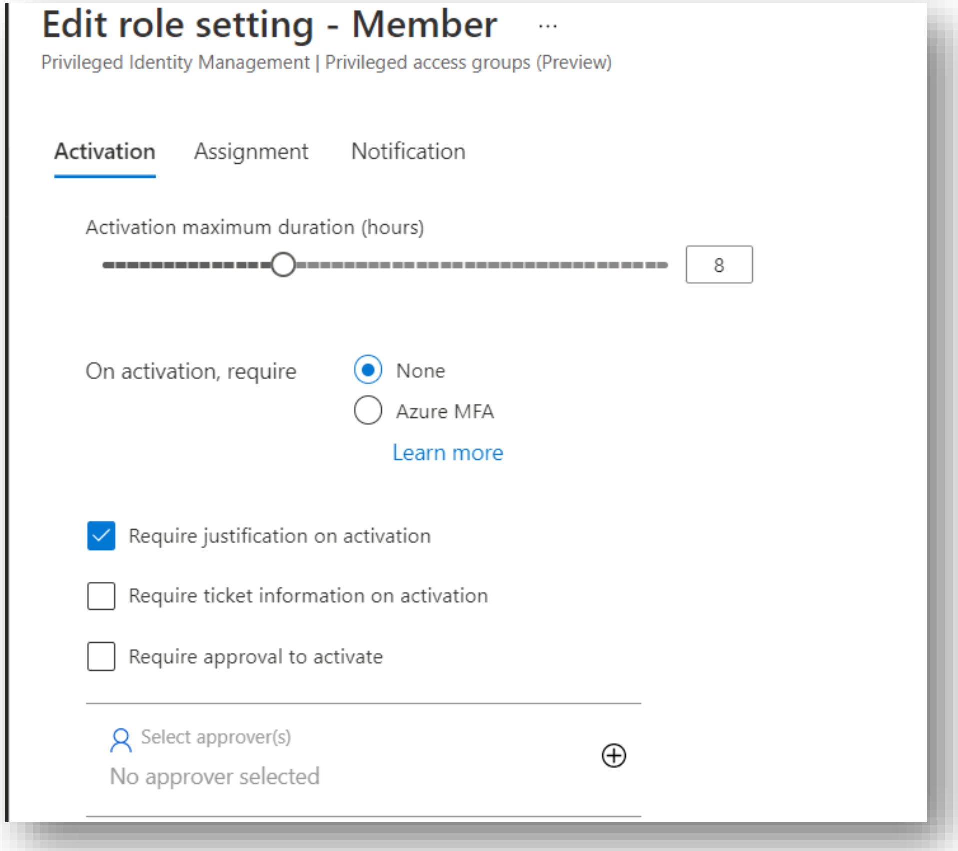
AR-PIM-SEC-ENGINEER

Permissions

Azure AD / Azure Roles

- Global Reader
- Security Reader
- Intune Administrator

Azure AD PIM Groups #3



Edit role setting - Member ···

Privileged Identity Management | Privileged access groups (Preview)

Activation | Assignment | Notification

Activation maximum duration (hours) 8

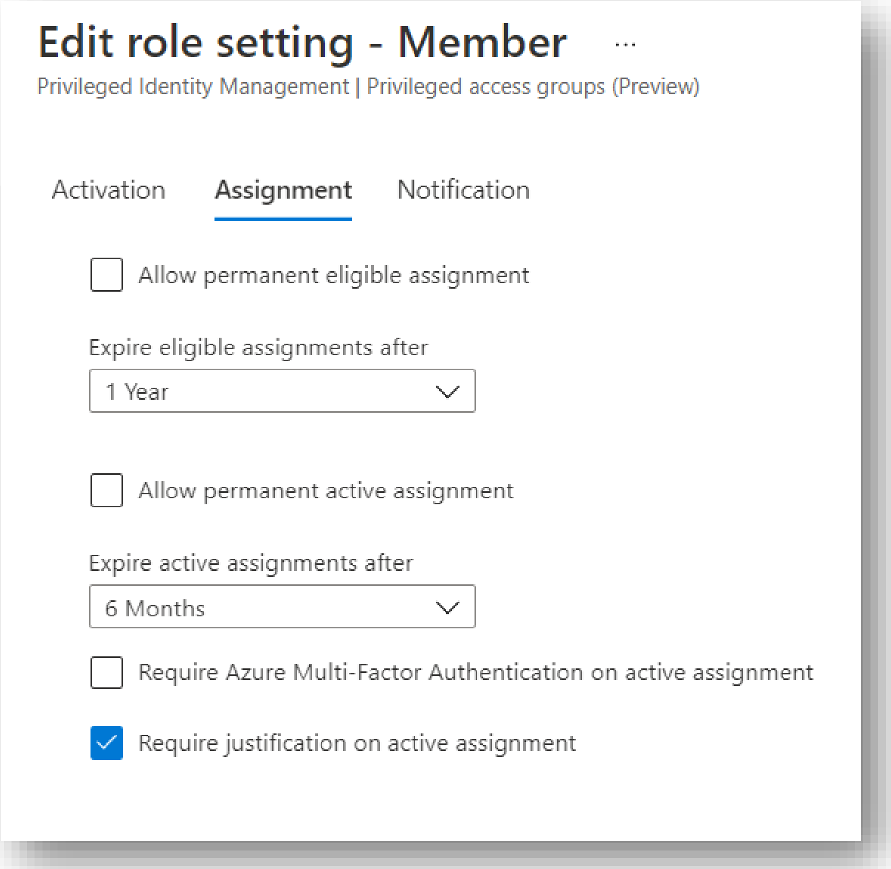
On activation, require
● None
○ Azure MFA
Learn more

☑ Require justification on activation

□ Require ticket information on activation

□ Require approval to activate

Select approver(s)
No approver selected ⊕



Edit role setting - Member ···

Privileged Identity Management | Privileged access groups (Preview)

Activation | Assignment | Notification

□ Allow permanent eligible assignment

Expire eligible assignments after: 1 Year

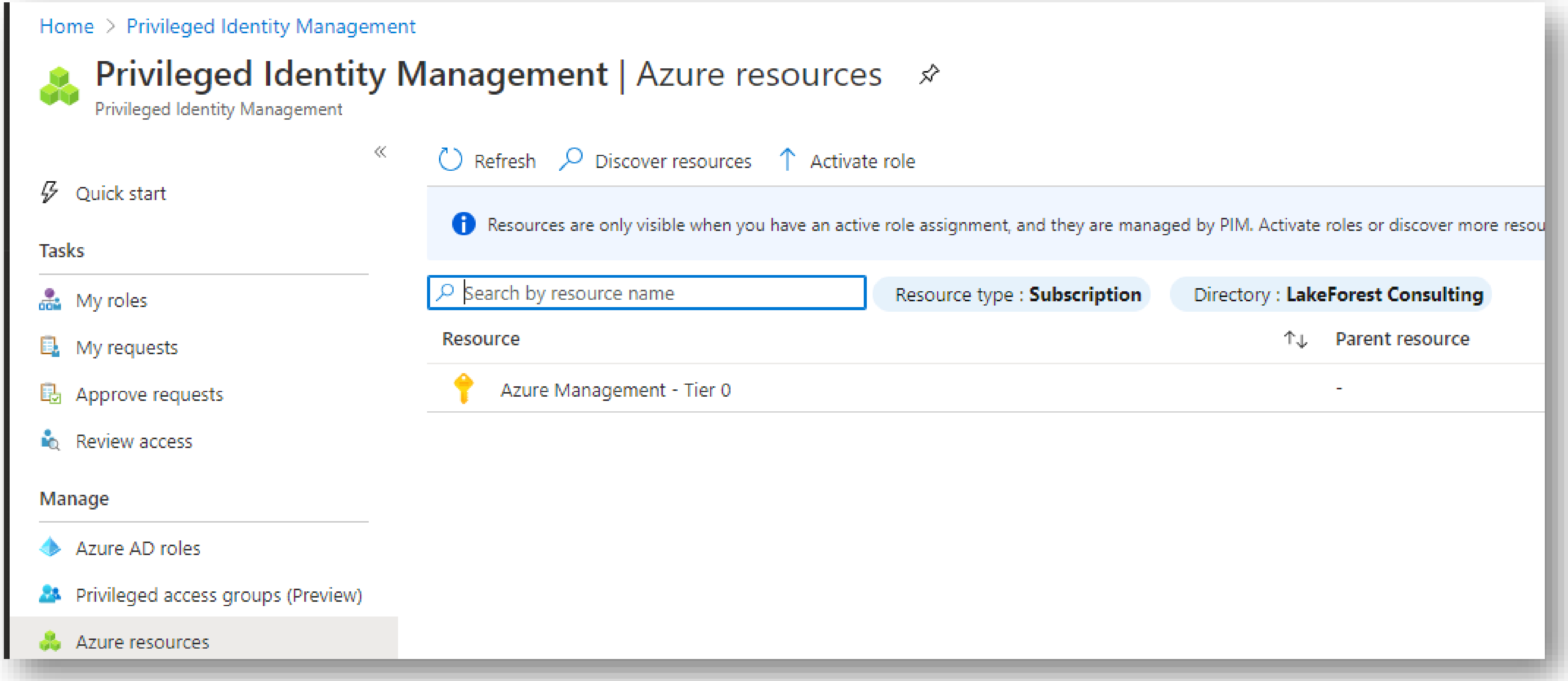
□ Allow permanent active assignment

Expire active assignments after: 6 Months

□ Require Azure Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Azure Resources



Home > Privileged Identity Management

Privileged Identity Management | Azure resources

Privileged Identity Management

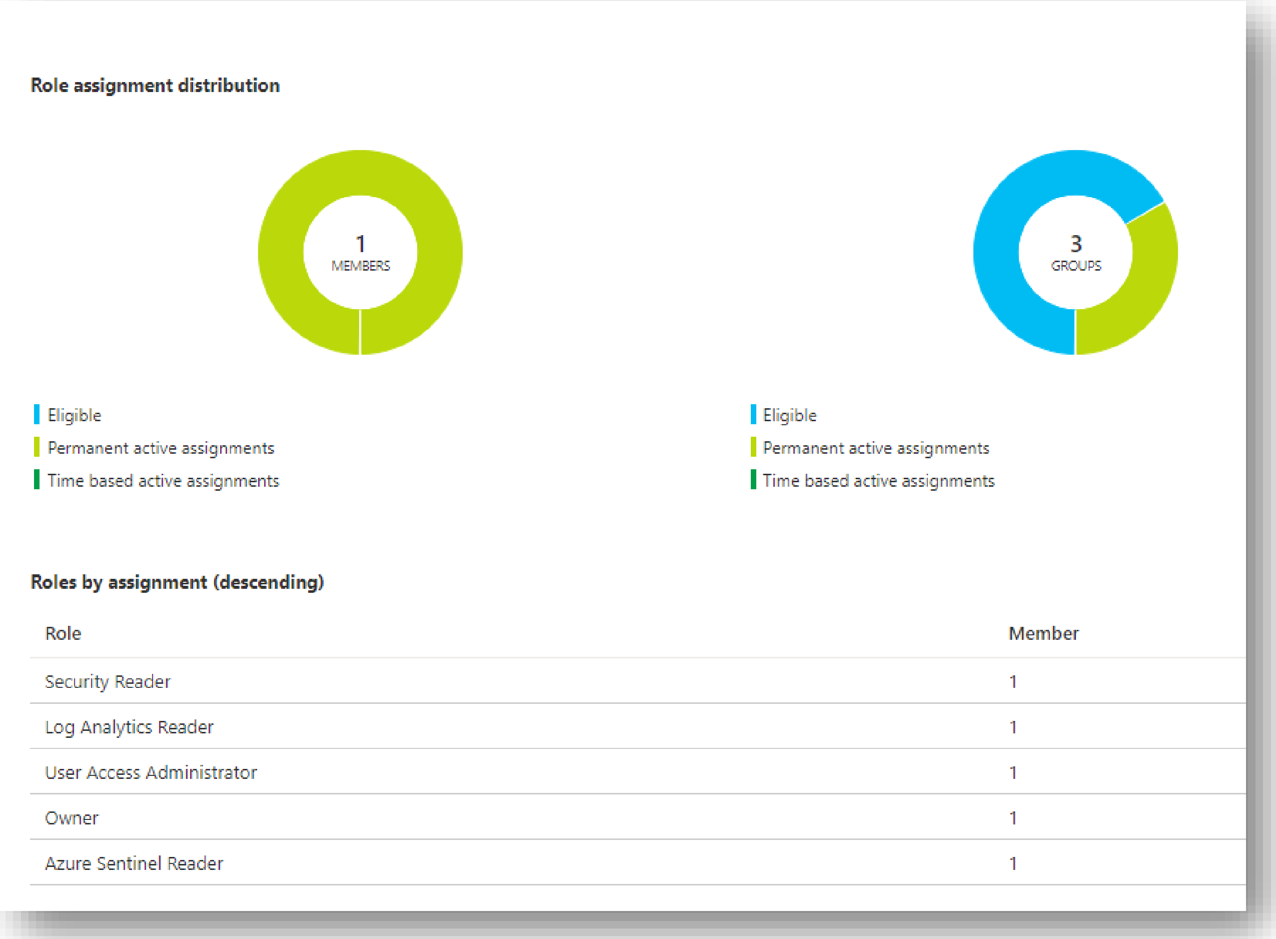
Refresh   Discover resources   Activate role

Resources are only visible when you have an active role assignment, and they are managed by PIM. Activate roles or discover more resou

Search by resource name   Resource type : **Subscription**   Directory : **LakeForest Consulting**

Resource	Parent resource
Azure Management - Tier 0	-

Azure Resources #2



Role assignment distribution

- Eligible
- Permanent active assignments
- Time based active assignments

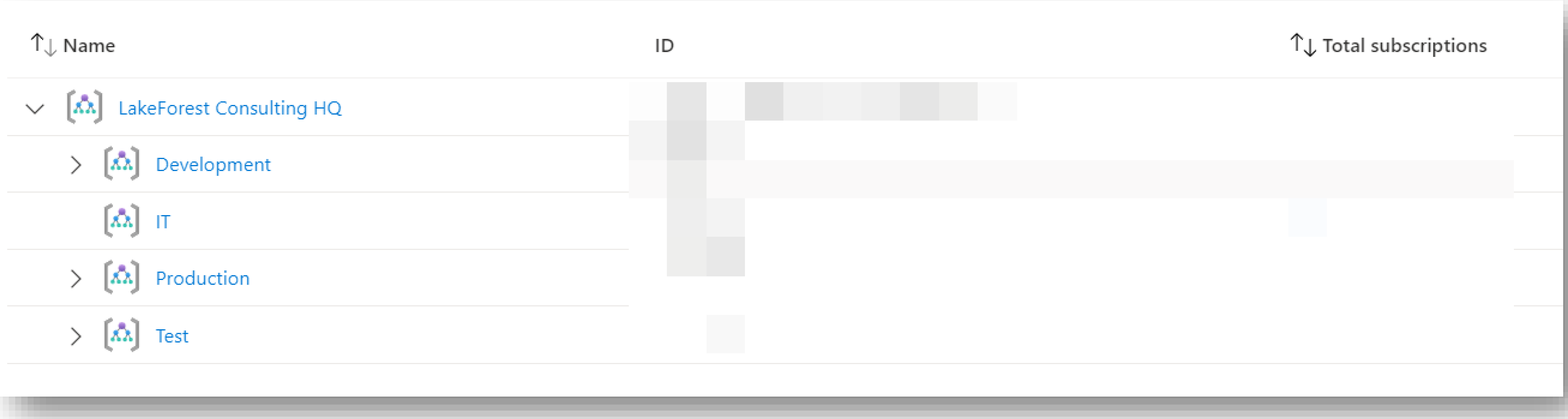
- Eligible
- Permanent active assignments
- Time based active assignments

Roles by assignment (descending)

Role	Member
Security Reader	1
Log Analytics Reader	1
User Access Administrator	1
Owner	1
Azure Sentinel Reader	1

Azure Resources #3

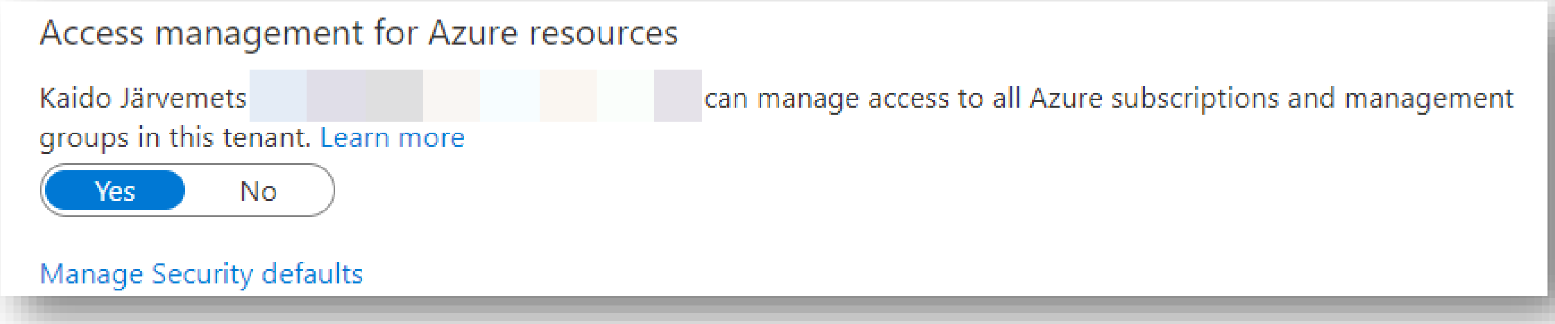
- You can manage Azure Management Groups with PIM too!
- Make sure to have a proper structure before you start!
- How are you going to manage these?
  - It may take some time to figure this out



Name	ID	Total subscriptions
LakeForest Consulting HQ	[redacted]	
Development	[redacted]	
IT	[redacted]	
Production	[redacted]	
Test	[redacted]	

Azure Resources #4

- No detection by default!
  - Access management for Resources assigns User Access Administrator role on the tenant root management group level. This gives you all the necessary permissions to take over everything!

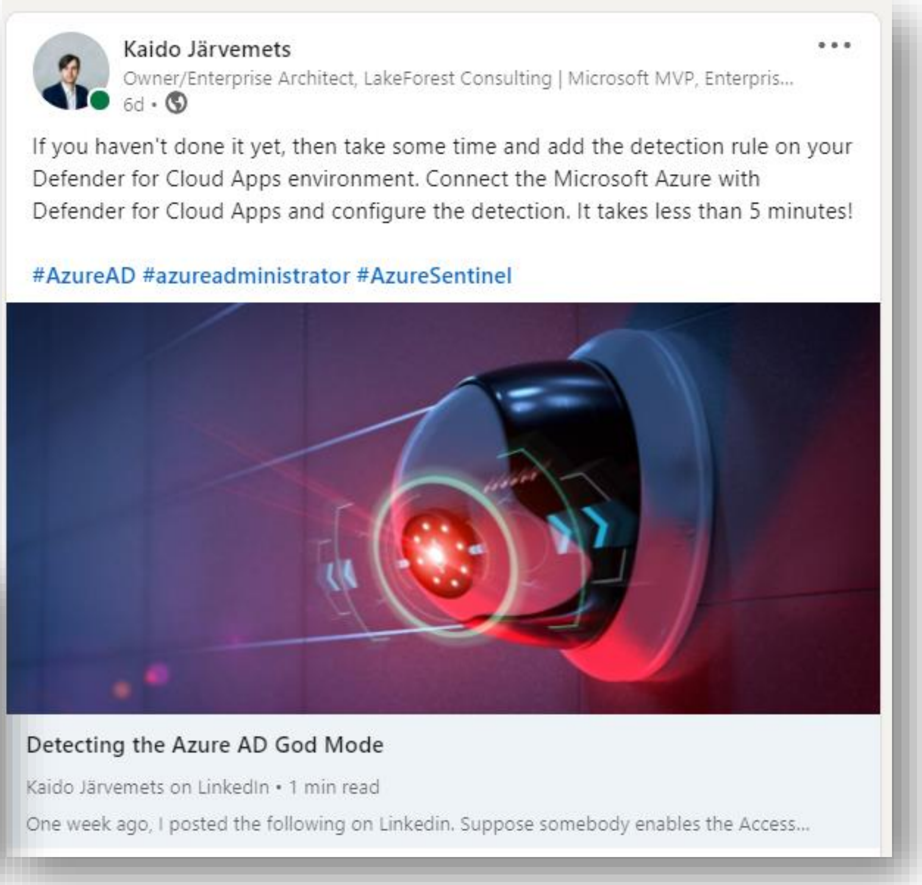


Access management for Azure resources

Kaido Järvemets [redacted] can manage access to all Azure subscriptions and management groups in this tenant. Learn more

[✓ Yes] No

Manage Security defaults



Kaido Järvemets

Owner/Enterprise Architect, LakeForest Consulting | Microsoft MVP, Enterpris...

6d •

If you haven't done it yet, then take some time and add the detection rule on your Defender for Cloud Apps environment. Connect the Microsoft Azure with Defender for Cloud Apps and configure the detection. It takes less than 5 minutes!

#AzureAD #azureadministrator #AzureSentinel

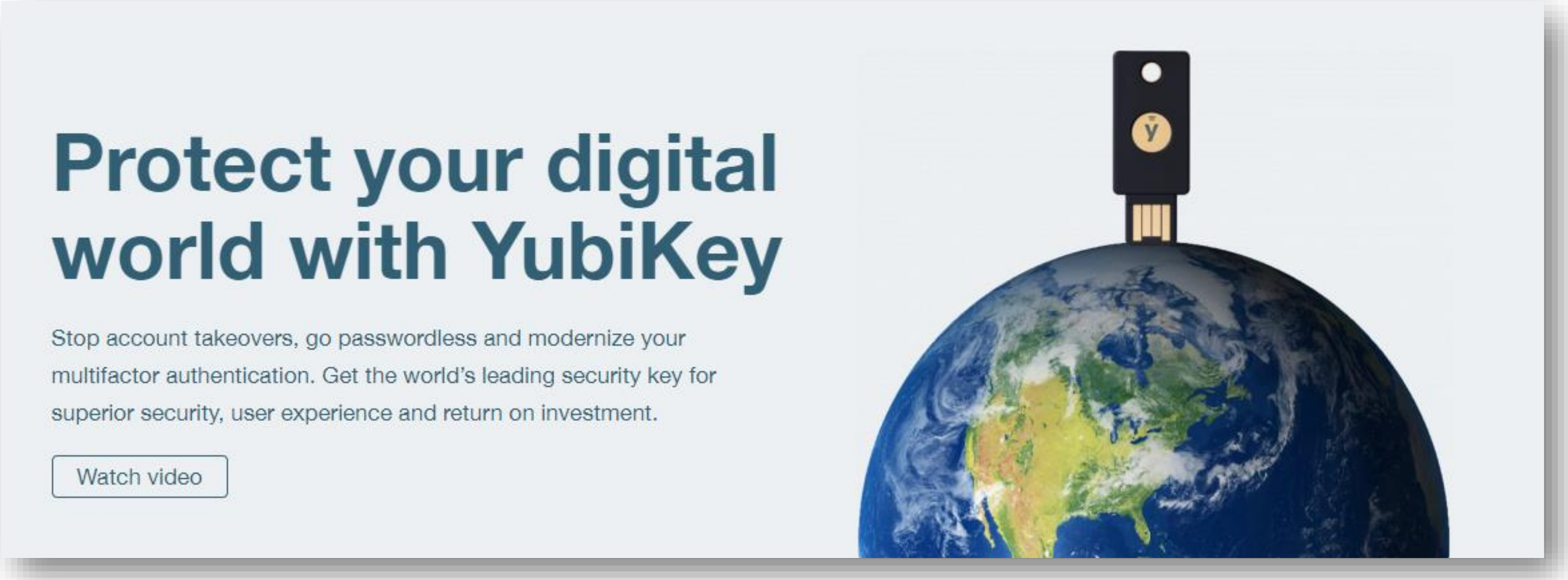
Detecting the Azure AD God Mode

Kaido Järvemets on LinkedIn • 1 min read

One week ago, I posted the following on Linkedin. Suppose somebody enables the Access...

DEMO: Create Azure AD PIM groups

Keys

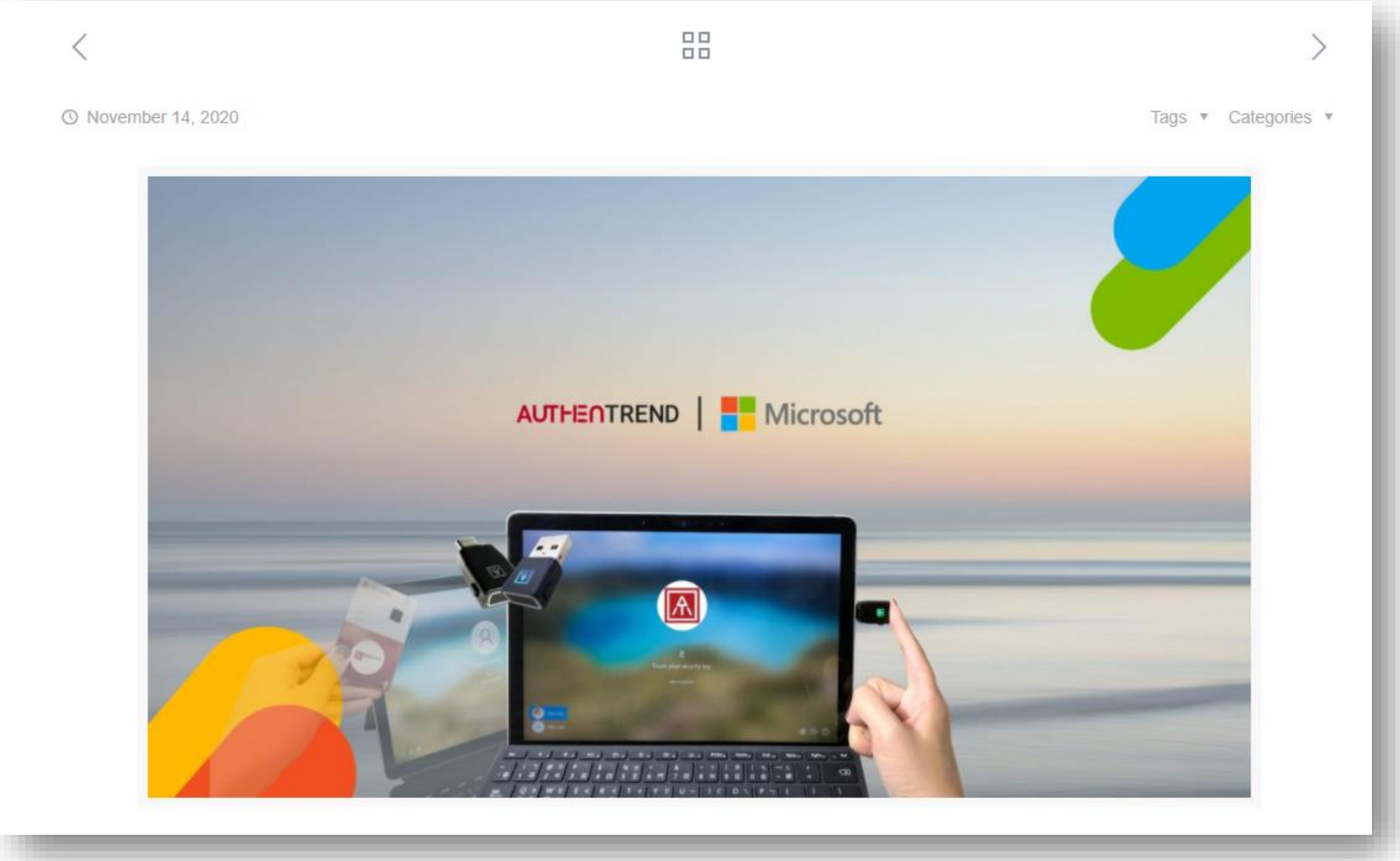


Protect your digital world with YubiKey

Stop account takeovers, go passwordless and modernize your multifactor authentication. Get the world's leading security key for superior security, user experience and return on investment.

Passwordless authentication

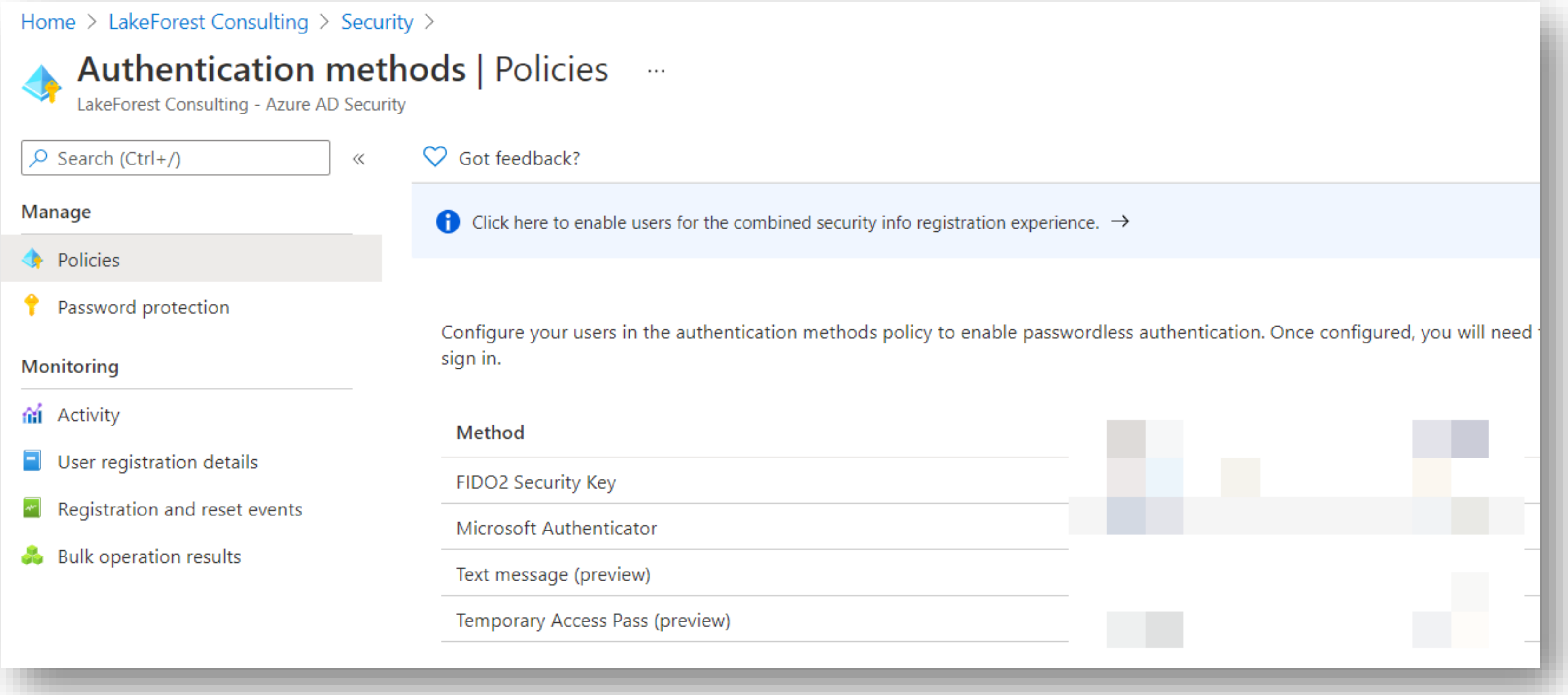
Keys #2



November 14, 2020

Tags ▾ Categories ▾

Authentication Methods



Home > LakeForest Consulting > Security >

Authentication methods | Policies ...

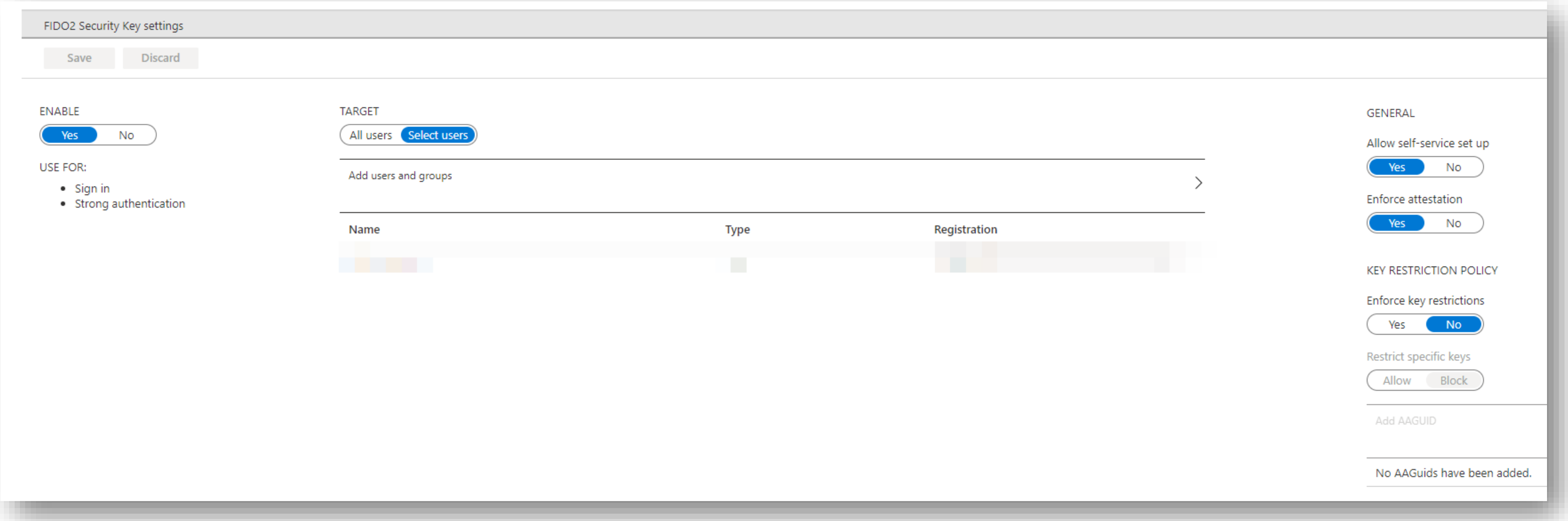
LakeForest Consulting - Azure AD Security

Click here to enable users for the combined security info registration experience. →

Configure your users in the authentication methods policy to enable passwordless authentication. Once configured, you will need
sign in.

Method
FIDO2 Security Key
Microsoft Authenticator
Text message (preview)
Temporary Access Pass (preview)

Authentication Methods #2



FIDO2 Security Key settings

ENABLE

[✓ Yes] No

USE FOR:

- Sign in
- Strong authentication

TARGET

All users [✓ Select users]

Add users and groups

Name	Type	Registration
[redacted]	[redacted]	[redacted]

GENERAL

Allow self-service set up

[✓ Yes] No

Enforce attestation

[✓ Yes] No

KEY RESTRICTION POLICY

Enforce key restrictions

Yes [✓ No]

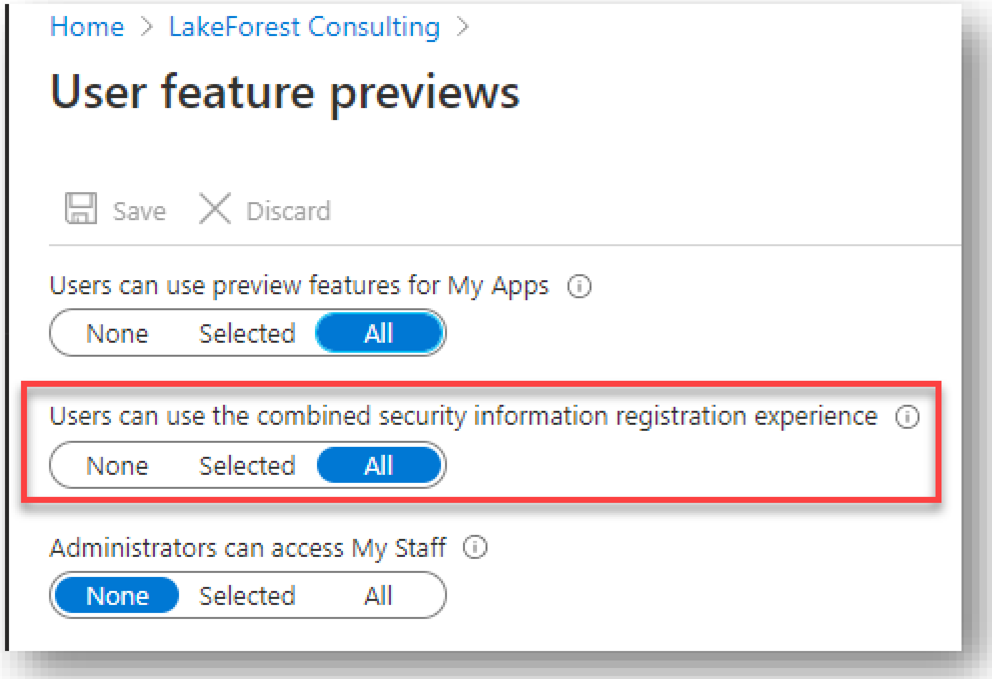
Restrict specific keys

Allow Block

Add AAGUID

No AAGuids have been added.

Combined registration



User feature previews

Users can use preview features for My Apps ⓘ
None Selected [✓ All]

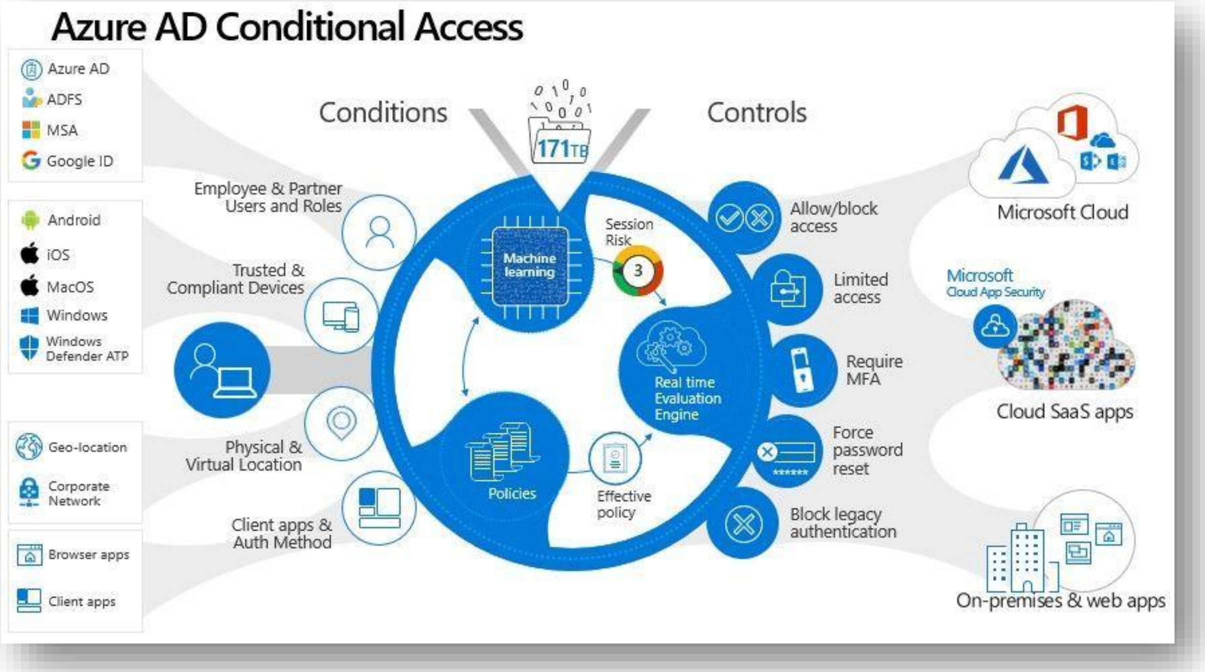
Users can use the combined security information registration experience ⓘ
None Selected [✓ All]

Administrators can access My Staff ⓘ
[✓ None] Selected All

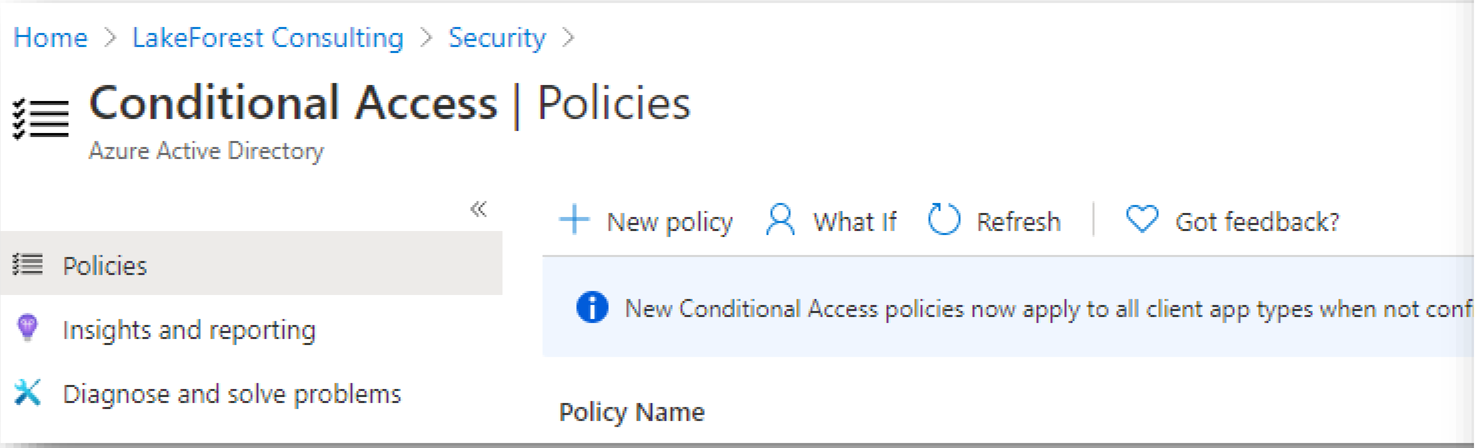
Azure AD Conditional Access

Azure AD Conditional Access

- Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and to enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.



Conditional Access



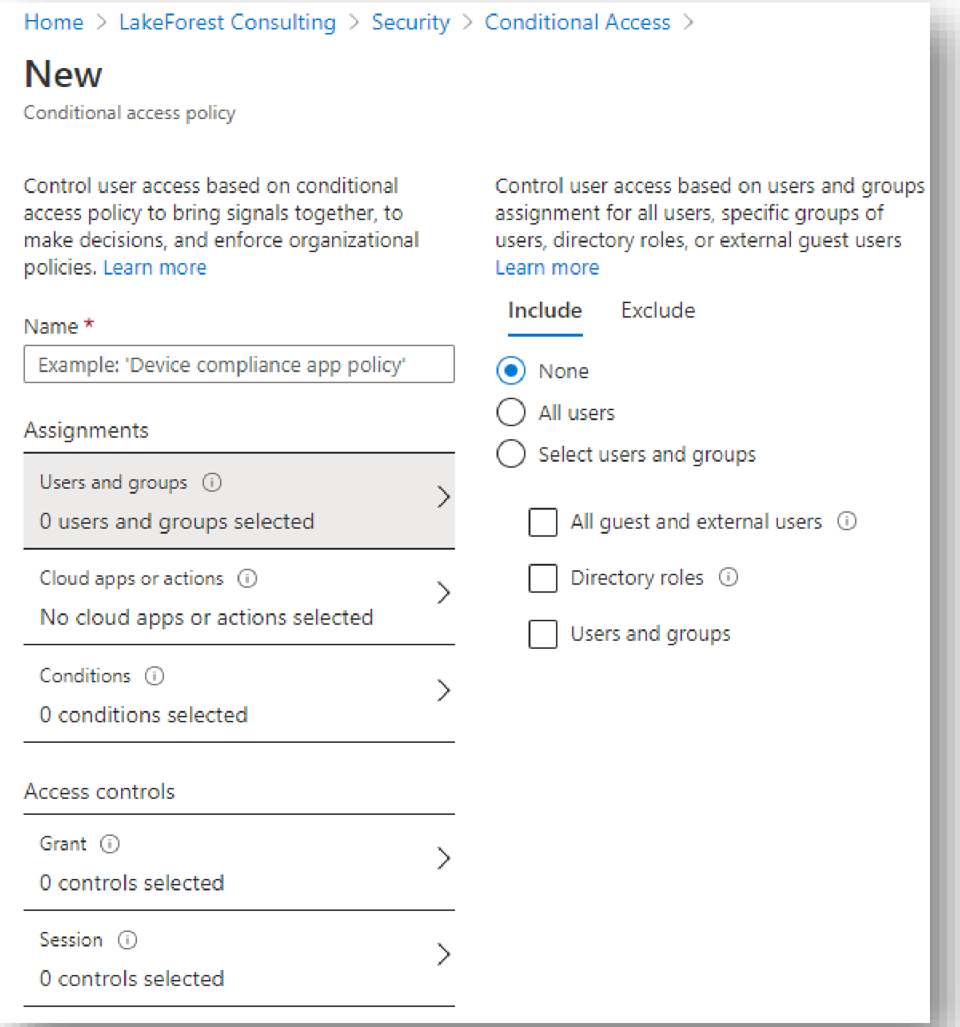
Home > LakeForest Consulting > Security >

Conditional Access | Policies

Azure Active Directory

New Conditional Access policies now apply to all client app types when not conf

Policy Name



Home > LakeForest Consulting > Security > Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ
0 users and groups selected

Cloud apps or actions ⓘ
No cloud apps or actions selected

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

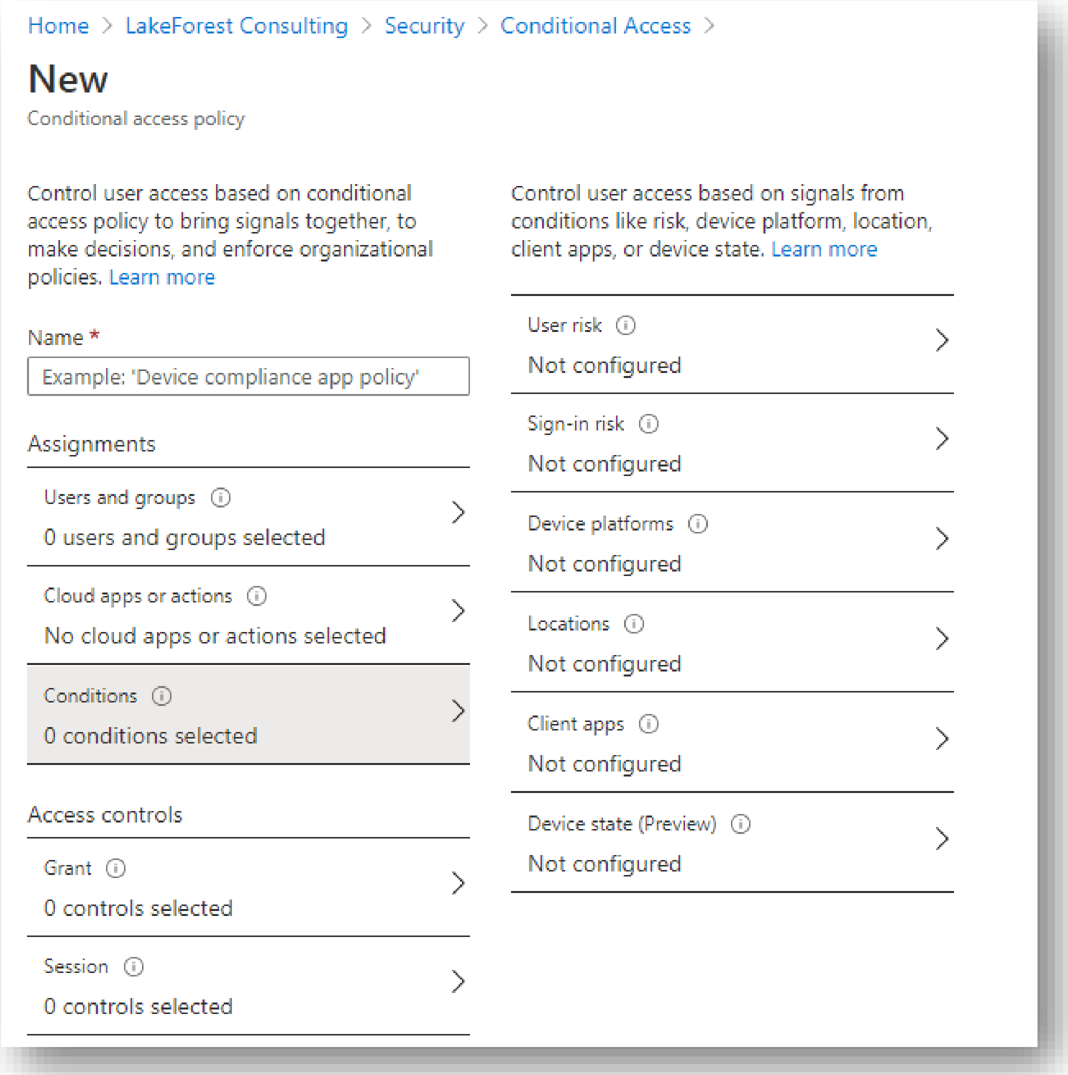
Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users Learn more

Include | Exclude

● None
○ All users
○ Select users and groups

□ All guest and external users ⓘ
□ Directory roles ⓘ
□ Users and groups

Conditional Access #2



Home > LakeForest Consulting > Security > Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users and groups
0 users and groups selected

Cloud apps or actions
No cloud apps or actions selected

Conditions
0 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk
Not configured

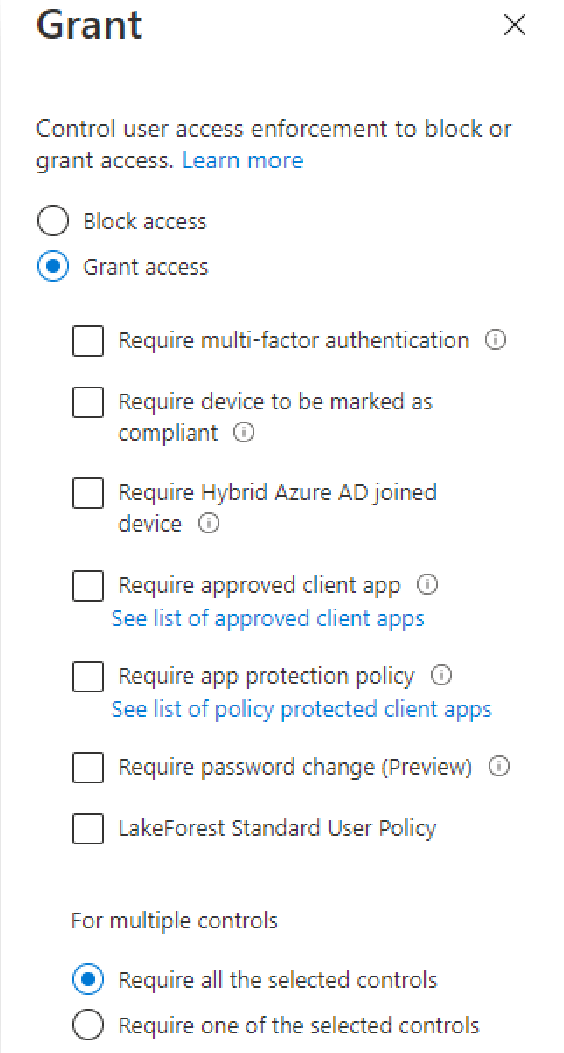
Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Device state (Preview)
Not configured



Grant

Control user access enforcement to block or grant access. Learn more

○ 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
See list of policy protected client apps

□ Require password change (Preview)

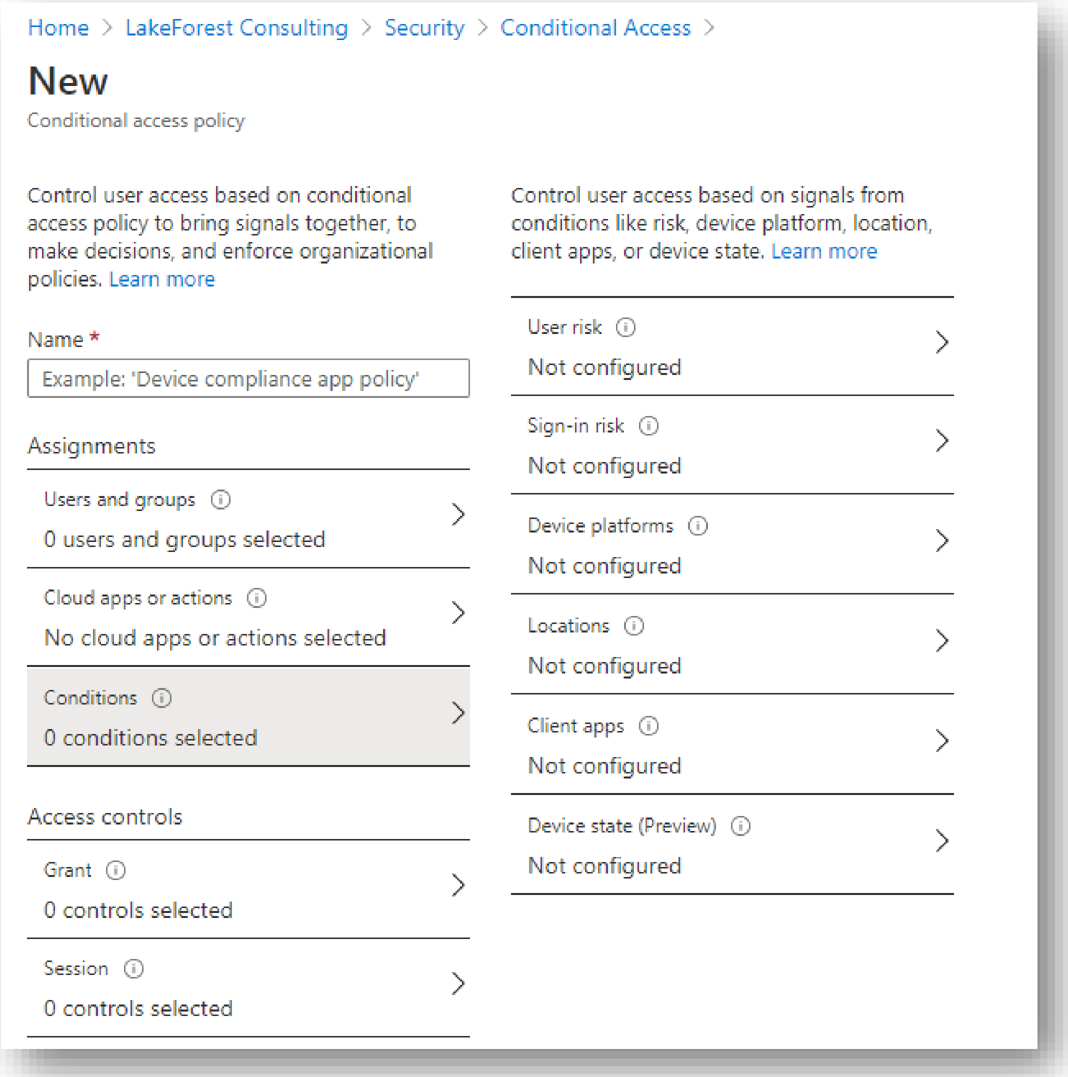
□ LakeForest Standard User Policy

For multiple controls

● Require all the selected controls

○ Require one of the selected controls

Conditional Access #3



Home > LakeForest Consulting > Security > Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users and groups
0 users and groups selected

Cloud apps or actions
No cloud apps or actions selected

Conditions
0 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk
Not configured

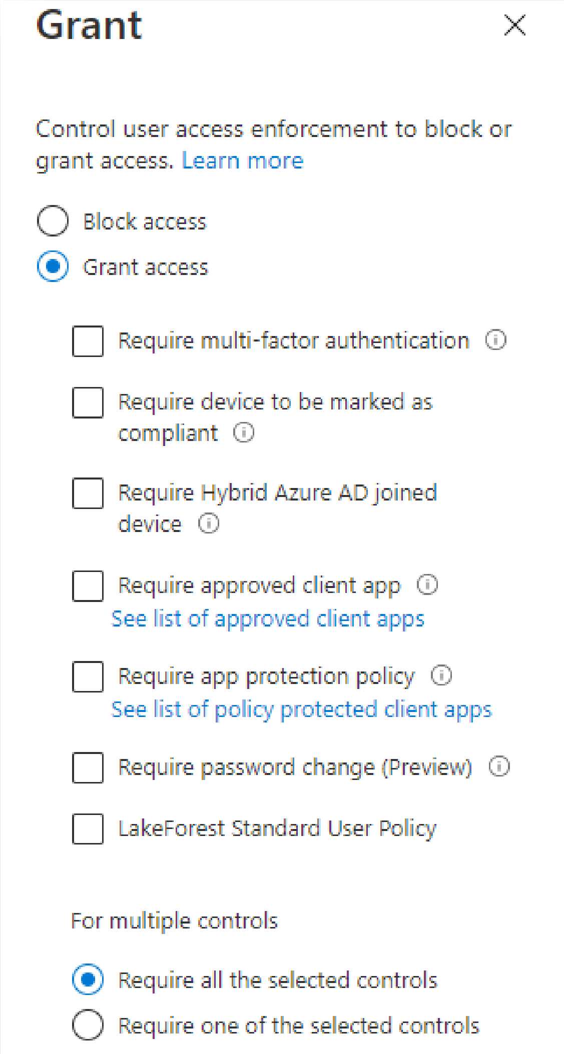
Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Device state (Preview)
Not configured



Grant

Control user access enforcement to block or grant access. Learn more

○ 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
See list of policy protected client apps

□ Require password change (Preview)

□ LakeForest Standard User Policy

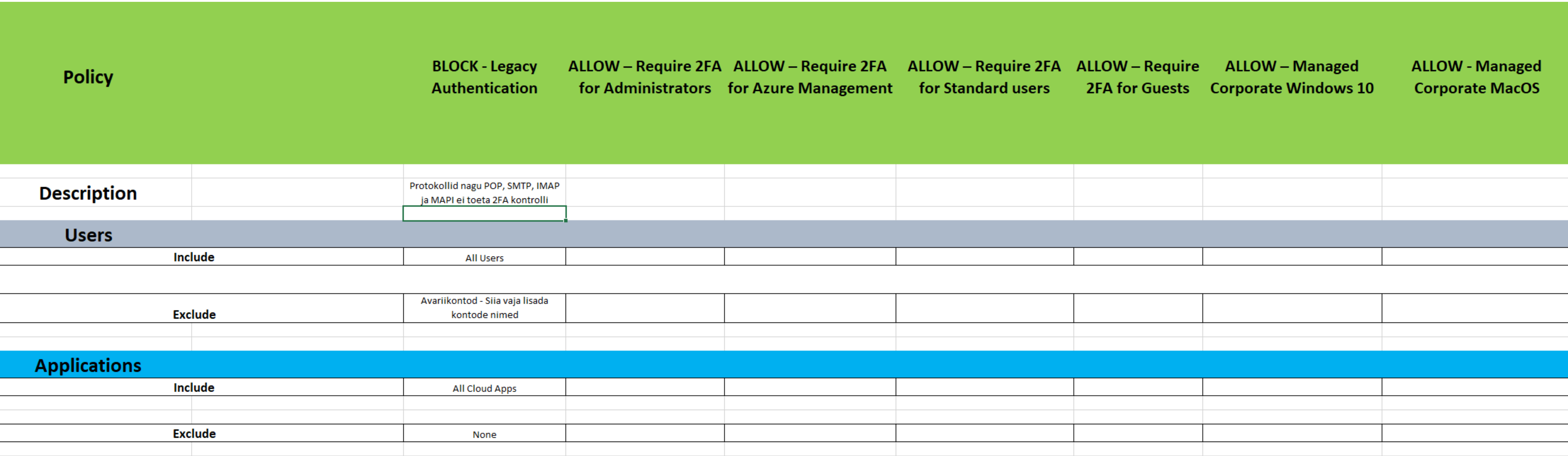
For multiple controls

● Require all the selected controls

○ Require one of the selected controls

Which rules should we apply?

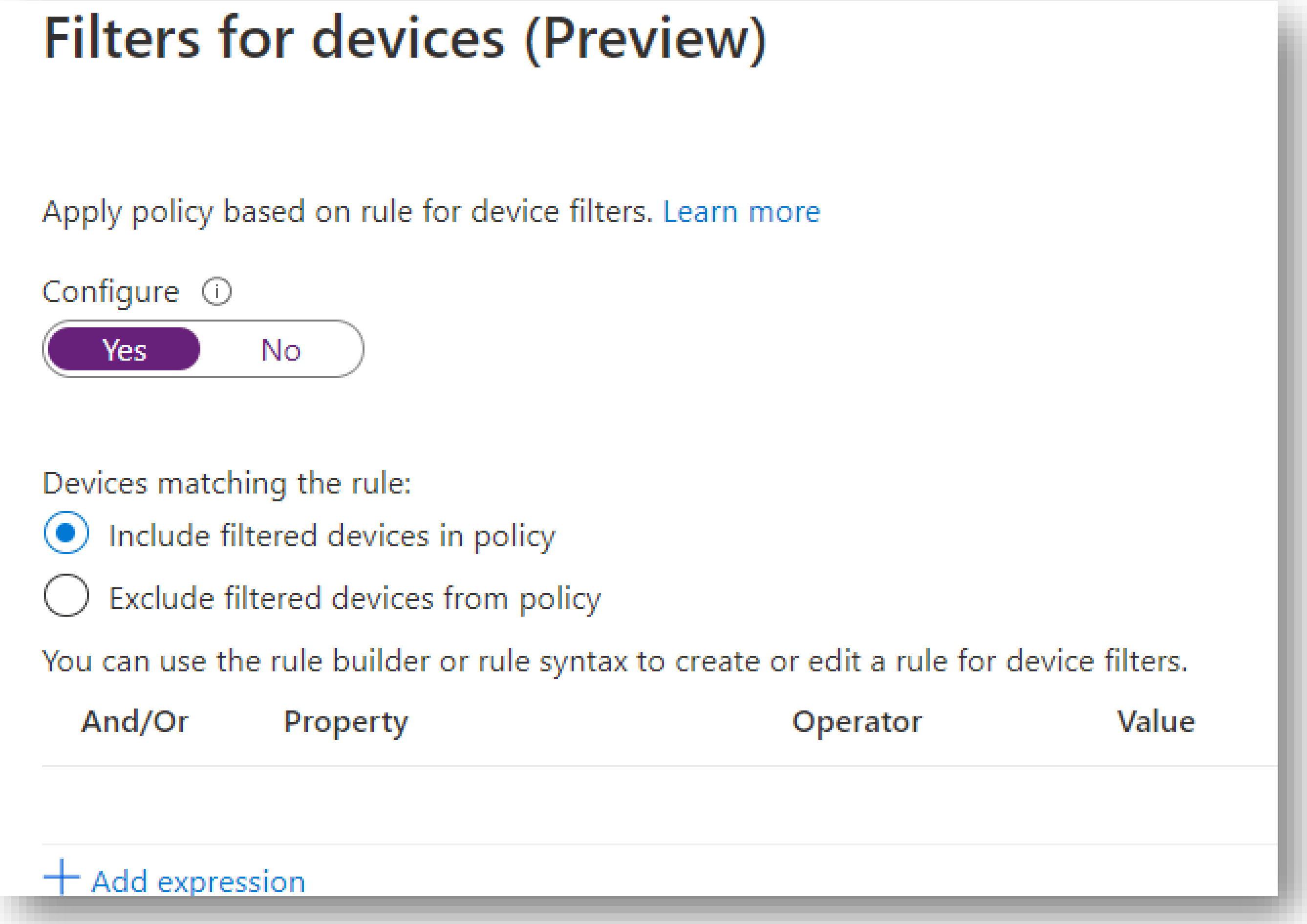
Starting point



Policy	BLOCK - Legacy Authentication	ALLOW – Require 2FA for Administrators	ALLOW – Require 2FA for Azure Management	ALLOW – Require 2FA for Standard users	ALLOW – Require 2FA for Guests	ALLOW – Managed Corporate Windows 10	ALLOW - Managed Corporate MacOS
Description	Protokollid nagu POP, SMTP, IMAP ja MAPI ei toeta 2FA kontrolli						
Users							
Include	All Users						
Exclude	Avariikontod - Siia vaja lisada kontode nimed						
Applications							
Include	All Cloud Apps						
Exclude	None						

DEMO: Azure AD Conditional Access Rules

Device filters (new)



Filters for devices (Preview)

Apply policy based on rule for device filters. Learn more

Configure ⓘ

[✓ Yes] No

Devices matching the rule:

● Include filtered devices in policy

○ Exclude filtered devices from policy

You can use the rule builder or rule syntax to create or edit a rule for device filters.

And/Or	Property	Operator	Value

+ Add expression

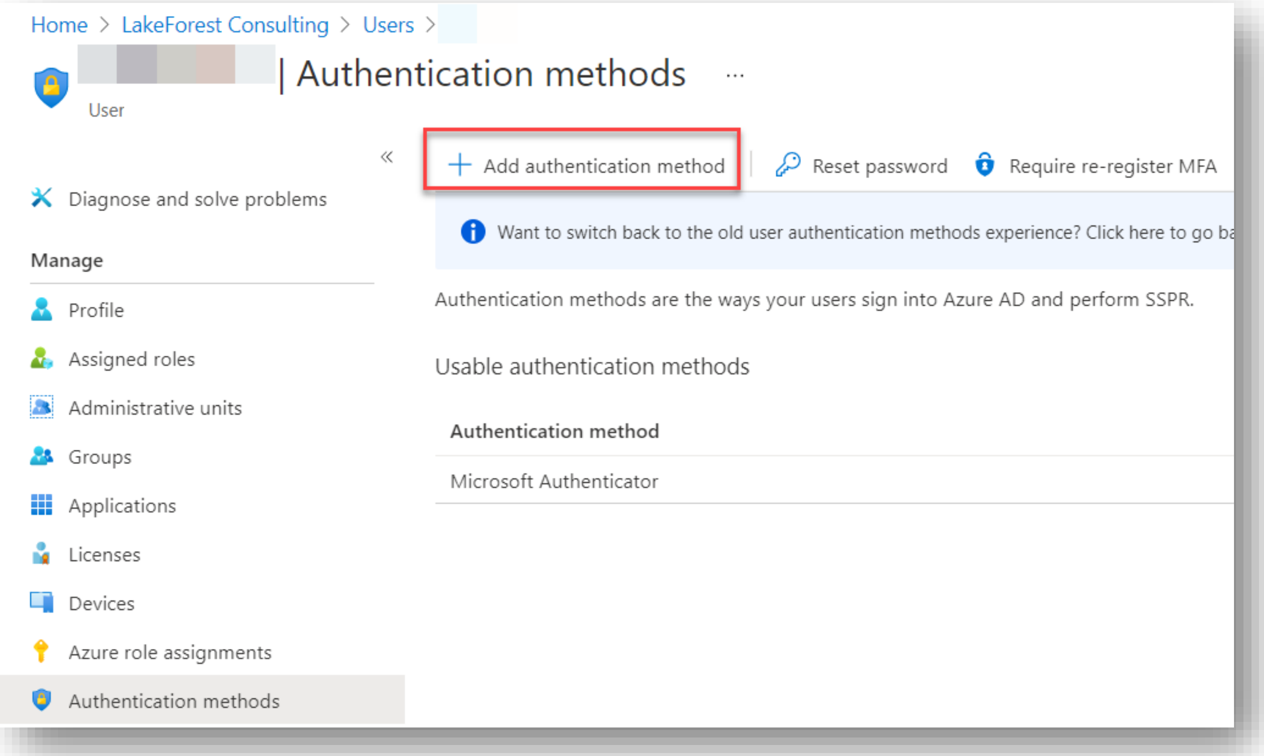
Temporary Access Pass

Temporary Access Pass (new)

- A Temporary Access Pass is a time-limited passcode issued by an admin that satisfies strong authentication requirements and can be used to onboard other authentication methods, including Passwordless ones.

- A Temporary Access Pass also makes recovery easier when a user has lost or forgotten their strong authentication factor like a FIDO2 security key or Microsoft Authenticator app, but needs to sign in to register new strong authentication methods.

Temporary Access Pass #2

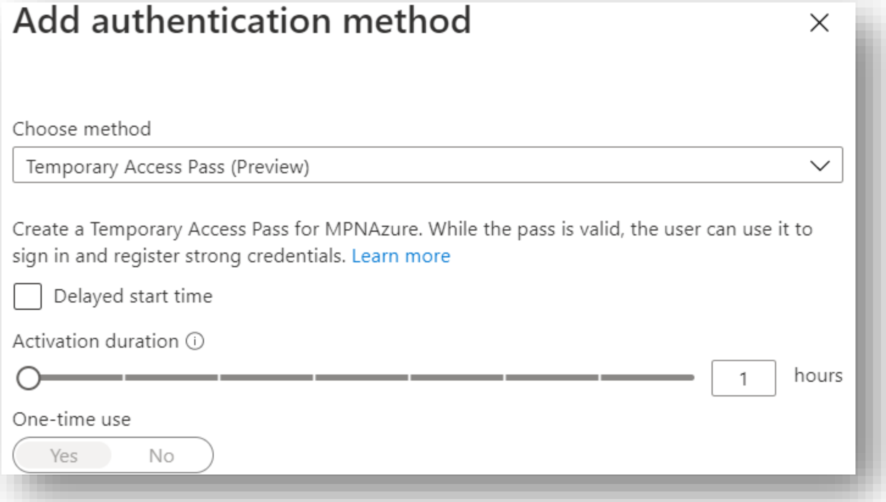


Want to switch back to the old user authentication methods experience? Click here to go ba

Authentication methods are the ways your users sign into Azure AD and perform SSPR.

Usable authentication methods

Authentication method
Microsoft Authenticator



Choose method: Temporary Access Pass (Preview)

Create a Temporary Access Pass for MPNAzure. While the pass is valid, the user can use it to sign in and register strong credentials. Learn more

□ Delayed start time

Activation duration ⓘ: 1 hours

One-time use: Yes No

Summary

- Audit your current environment
- Define the roles
- Educate your administrators, security engineers, helpdesk etc.
- Gradually roll-out new accounts with new security baseline.
- Collect feedback

- PS! Make sure to have proper processes around resource provisioning, on-boarding, off-boarding etc.

- PS #2! Some people will hate you for the rest of your life! ☺

Q&A

LakeForest Consulting

Thank you!

LakeForest Consulting