collabdays | lisbon

October 10th, 2020

Azure Active Directory - Best practices from the field

by Mustafa Toroman and Sasha Kranjac

Our Sponsors

DIAMOND

pointfire
Multilingual SharePoint

veeAM

COMMUNITY

ESPC20
ONLINE
14-15 OCTOBER 2020

EUROPEAN COLLABORATION SUMMIT

Microsoft

Office 365 Portugal

sharept

Microsoft® Most Valuable Professional

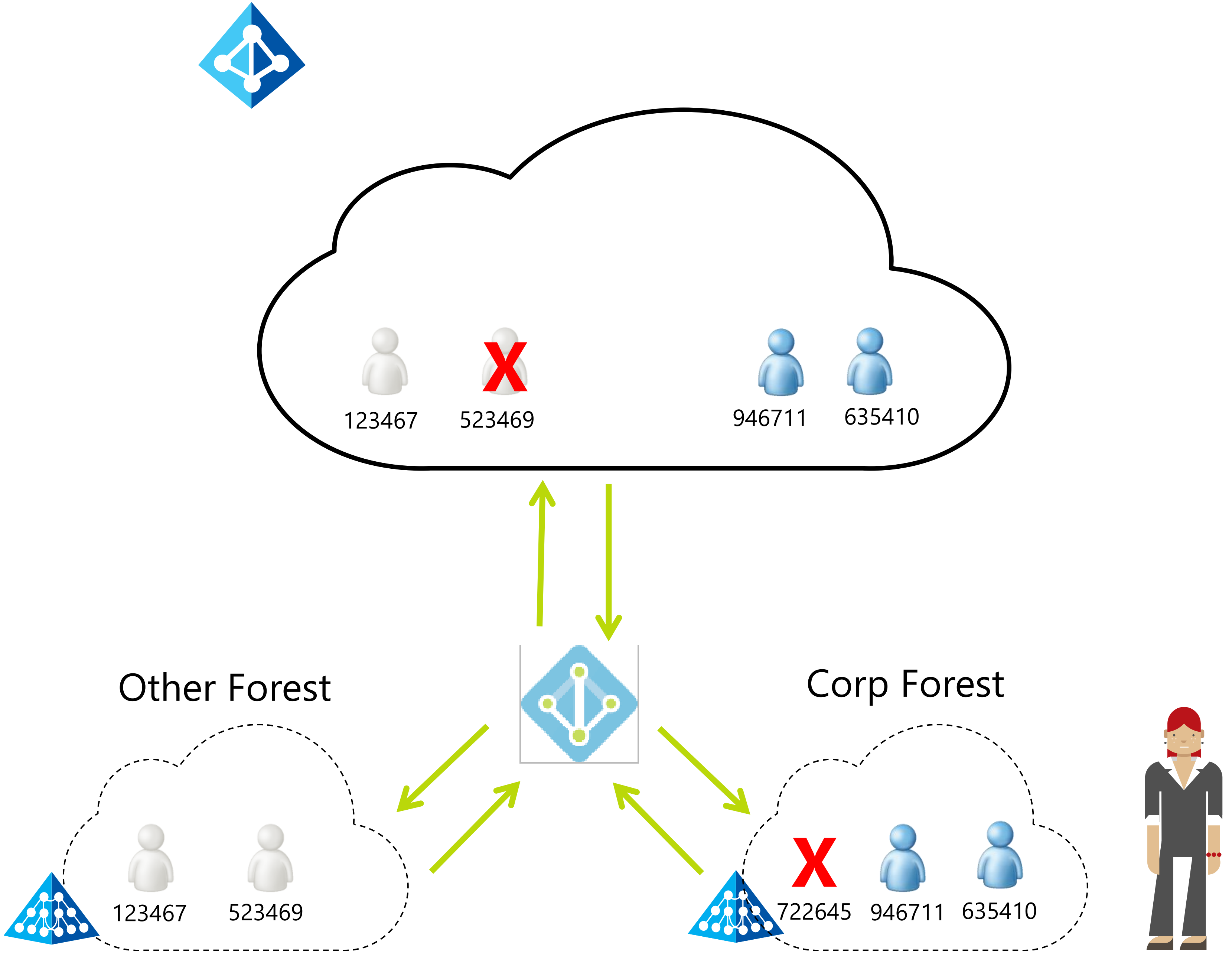
MUSTAFA TOROMAN
SolutionArchitect
@toromust
Microsoft Azure MVP
MCSE, MCP, MCSA, MCITP, MCSD, MCT, MS v-TSP

Microsoft® MVP Most Valuable Professional

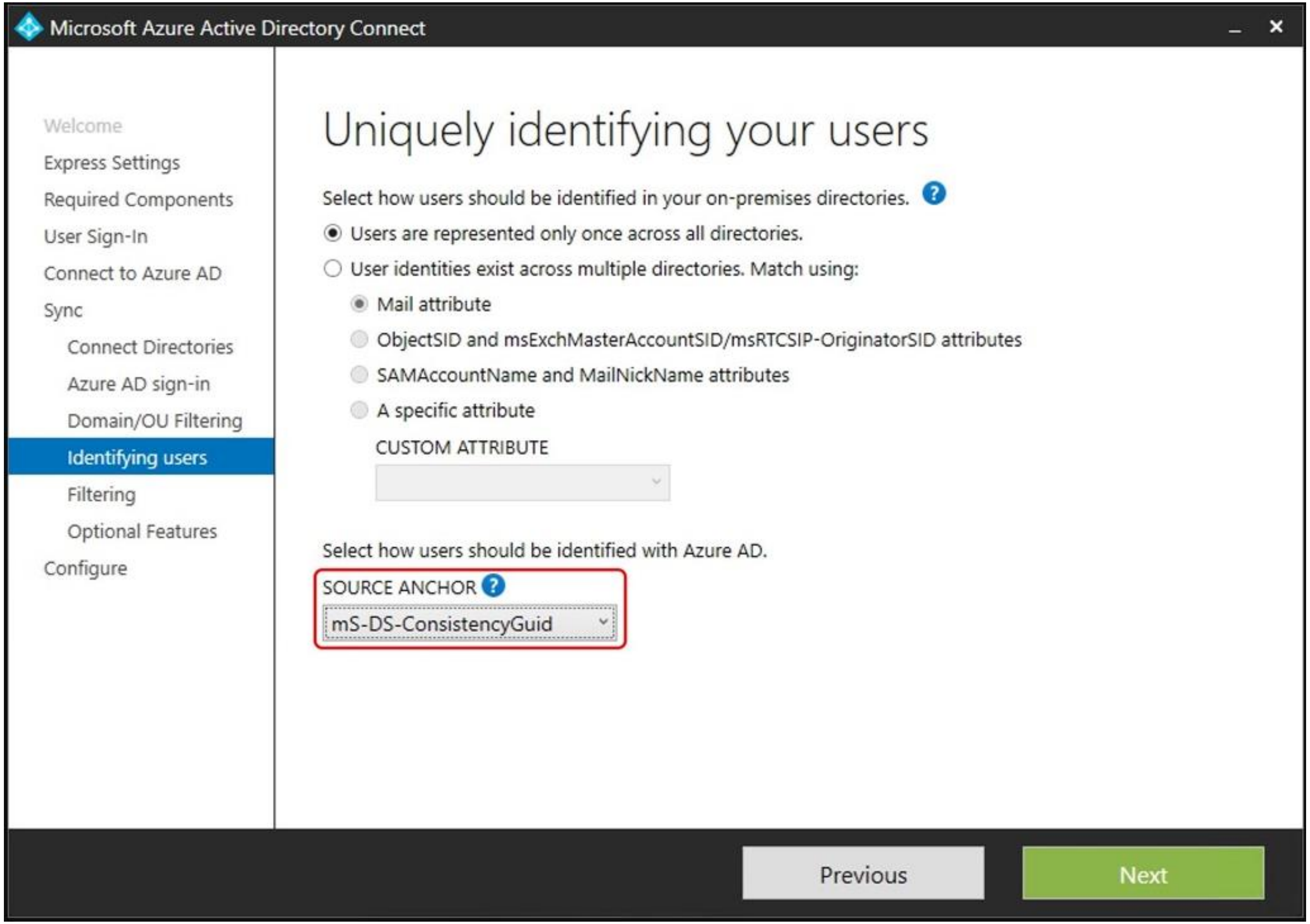
SASHA KRANJAC
Cloud Security Architect
CEO @ Kloudatech OÜ
@SasaKranjac
Microsoft Azure MVP
MCSE, MCSA, MCITP, MCT, MCT Regional Lead, Certified EC-Council Instructor

Sync & Auth

Sync Consistency GUID:



Sync Consistency GUID:



Uniquely identifying your users

Select how users should be identified in your on-premises directories.

● Users are represented only once across all directories.

○ User identities exist across multiple directories. Match using:

● Mail attribute

○ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes

○ SAMAccountName and MailNickName attributes

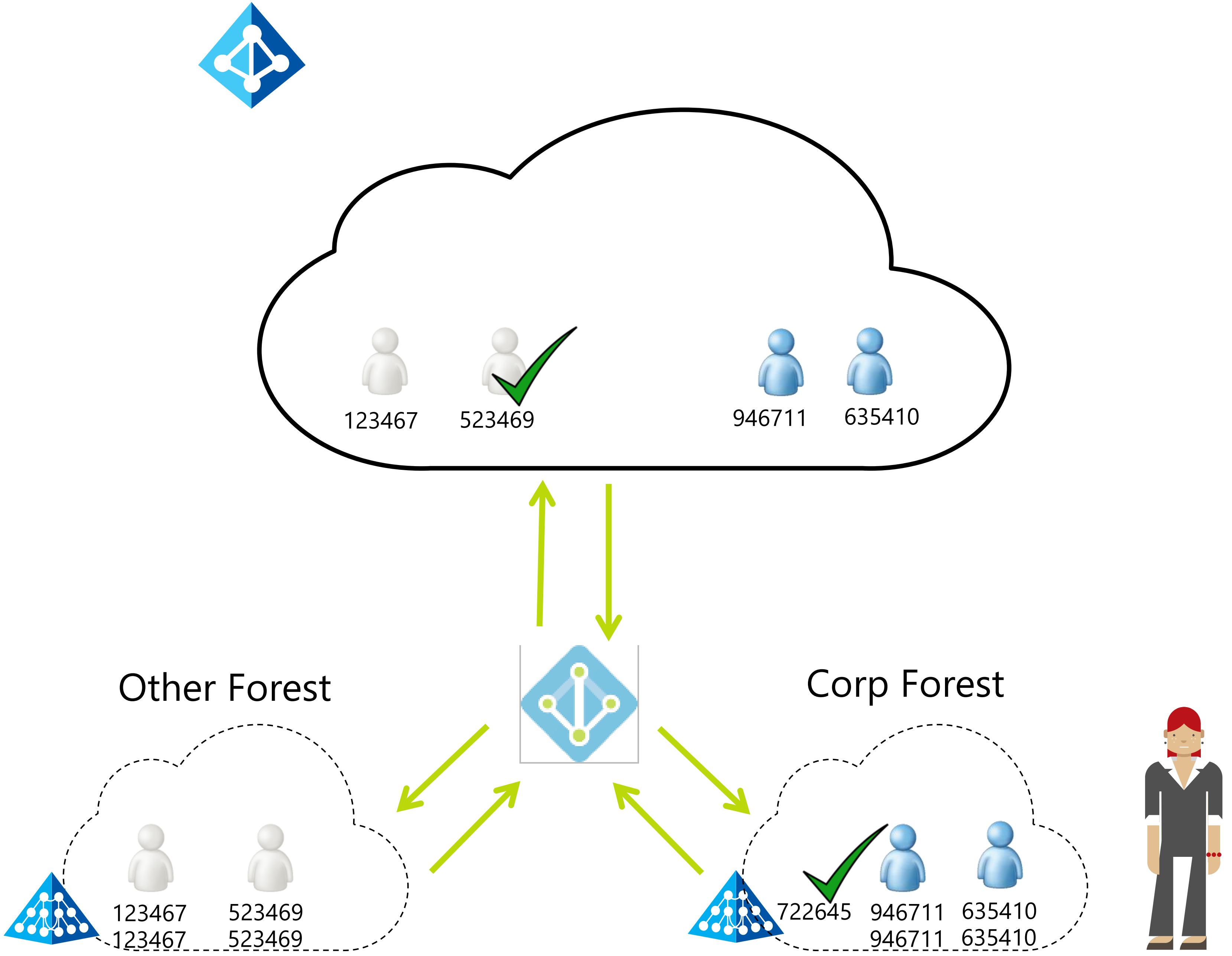
○ A specific attribute

CUSTOM ATTRIBUTE

Select how users should be identified with Azure AD.

SOURCE ANCHOR: mS-DS-ConsistencyGuid

Sync Consistency GUID:



Sync Do's and Don't's

Do: Plan your Upgrade

Do: Enable Azure AD Connect Health, ADFS Health, ADDS Health

Do: Sync what you need

Do: Use a "Consistency GUID" if you are Multi-Forest

Don't: Forget about Quota

- 50K by default
- 300K if you verify a domain
- Support ticket to raise it beyond

Don't: Forget about Pass Through Auth & Seamless SSO

Don't: Have to use ADFS

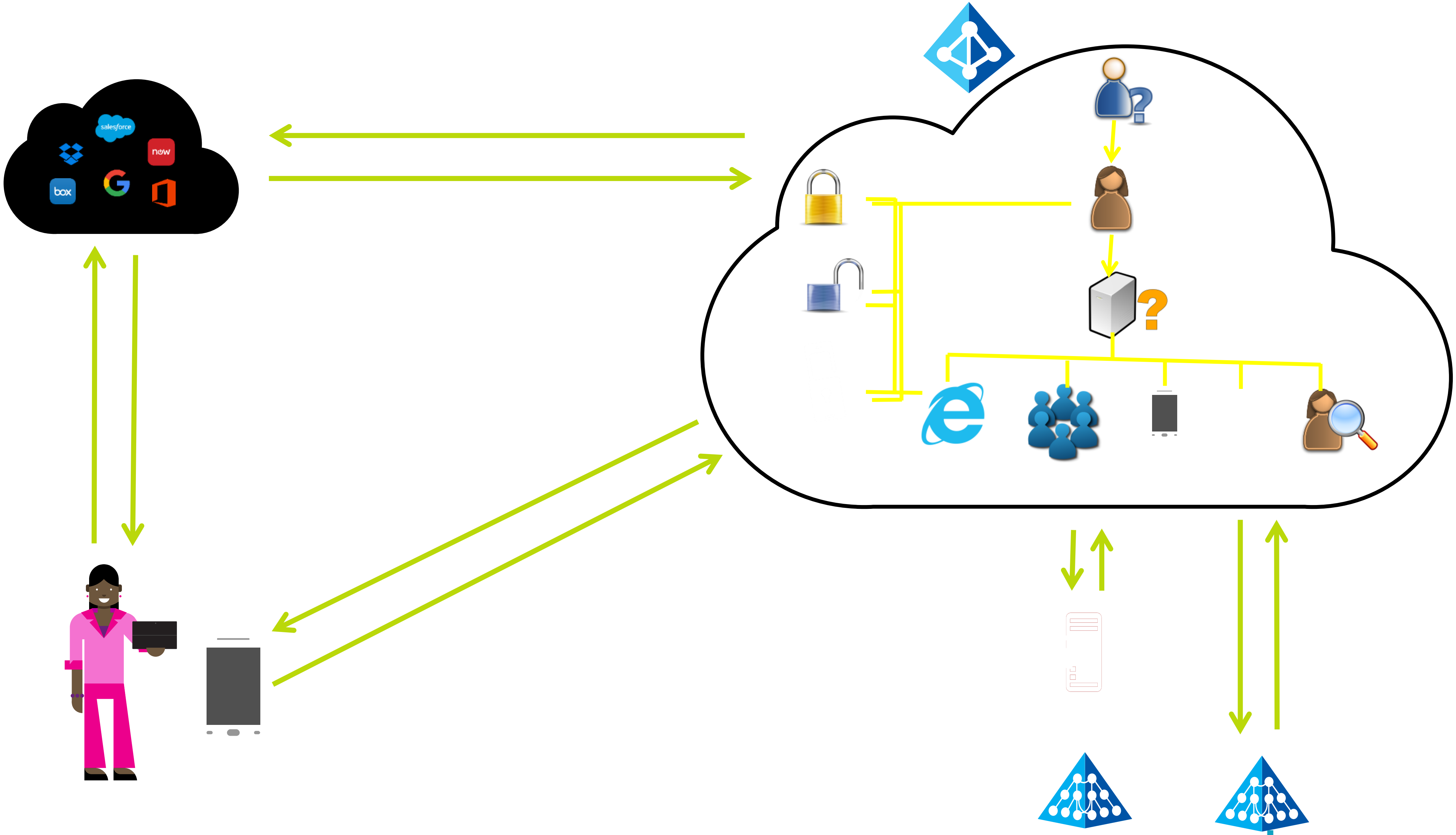
Password Hash Sync

- Password Hash != Password
- You don’t have to change your authentication flow
- You get Leaked Credentials Report as part of Azure AD P1
  - **Pull this and all Azure AD reports into your SIEM system**
- If everything goes down, this might end up saving your job
- Turn on Password Hash Sync!
- Turn on Seamless SSO

Conditional Access

What is Conditional Access?

- Goals it can help you achieve:
  - Prevent access to data from locations/clients that are undesirable
  - Prevent data download to devices that you are not comfortable with
  - Help you manage and reduce user and sign in risk
  - Reduce user friction, too many MFA prompts teach the user the wrong thing
- It's a part of your companies data loss prevention strategy
  - Intune to manage the device or the Apps
  - Azure information protection to Encrypt the data on the devices
  - Windows 10 with Windows HELLO for Business ultimately for strong auth across the board


salesforce
now
box

Security Taxonomies

User Type:

Employee or Contractor or Partner

Device Type:

Managed Device or BYOD

Network Location:

Inside or Outside Network

Application:

What resources is the user accessing

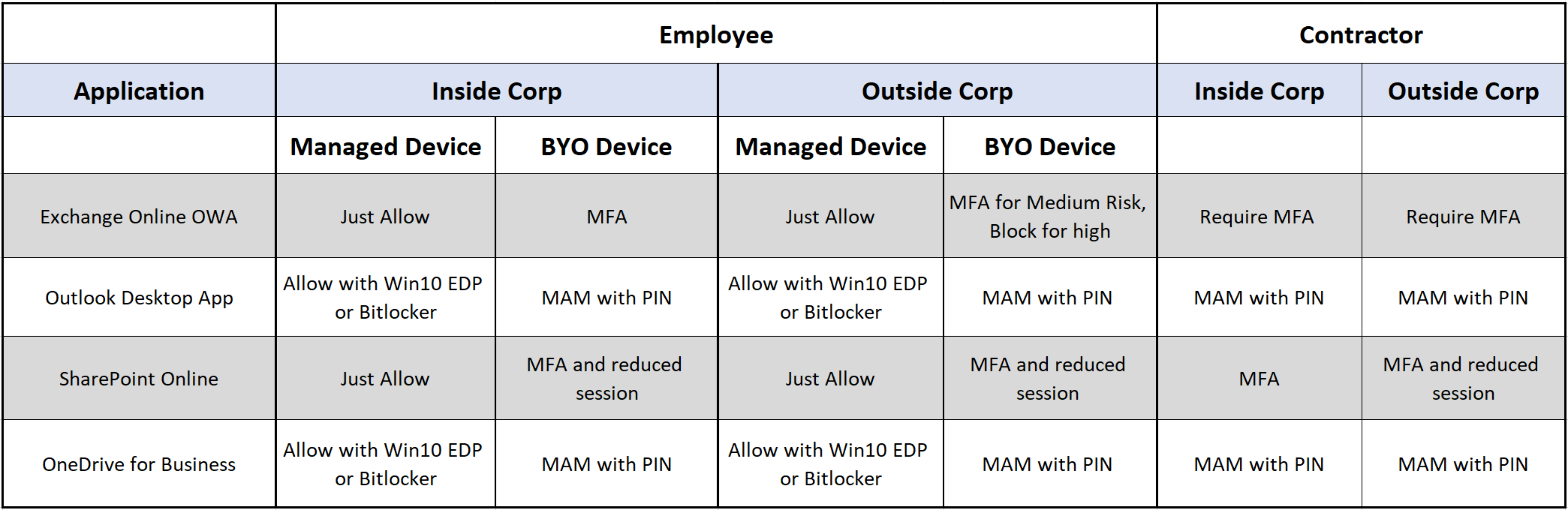
Client Type:

Mobile/Desktop App or Web App

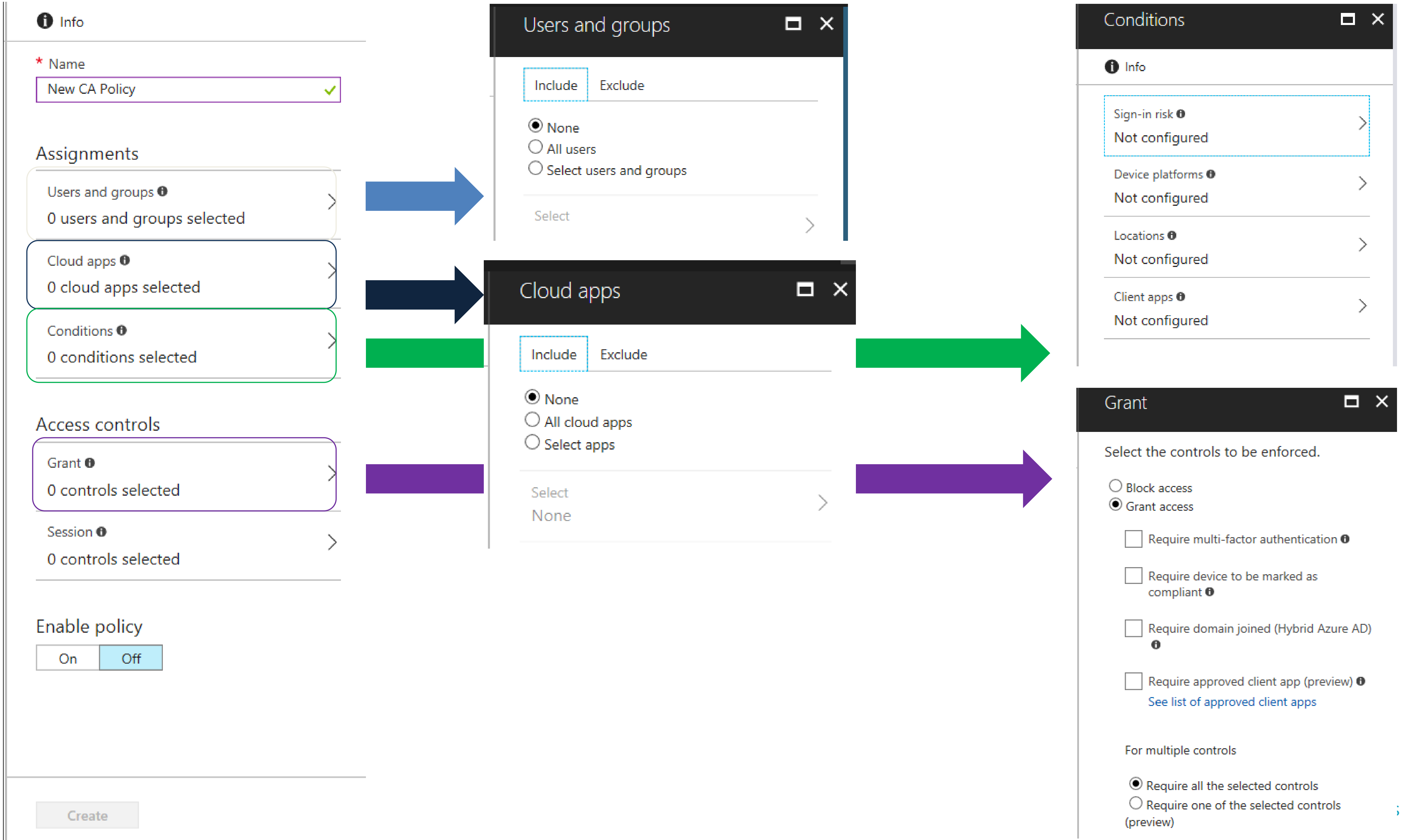
Risk Score:

High, Medium, or Low

Conditional Access Matrix



	Employee				Contractor	
Application	**Inside Corp**		**Outside Corp**		**Inside Corp**	**Outside Corp**
	Managed Device	**BYO Device**	**Managed Device**	**BYO Device**		
Exchange Online OWA	Just Allow	MFA	Just Allow	MFA for Medium Risk, Block for high	Require MFA	Require MFA
Outlook Desktop App	Allow with Win10 EDP or Bitlocker	MAM with PIN	Allow with Win10 EDP or Bitlocker	MAM with PIN	MAM with PIN	MAM with PIN
SharePoint Online	Just Allow	MFA and reduced session	Just Allow	MFA and reduced session	MFA	MFA and reduced session
OneDrive for Business	Allow with Win10 EDP or Bitlocker	MAM with PIN	Allow with Win10 EDP or Bitlocker	MAM with PIN	MAM with PIN	MAM with PIN



Info

* Name

New CA Policy ✓

Assignments

Users and groups
0 users and groups selected

Cloud apps
0 cloud apps selected

Conditions
0 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy

On | Off

Create

Users and groups

Include | Exclude

● None
○ All users
○ Select users and groups

Select

Cloud apps

Include | Exclude

● None
○ All cloud apps
○ Select apps

Select
None

Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Grant

Select the controls to be enforced.

○ Block access
● Grant access

□ Require multi-factor authentication

□ Require device to be marked as compliant

□ Require domain joined (Hybrid Azure AD)

□ Require approved client app (preview)
See list of approved client apps

For multiple controls

● Require all the selected controls
○ Require one of the selected controls (preview)

Conditional Access Do's and Don't's

Do: Use the Authenticator App

Do: Exclude 1 Admin account from the policy

Do: Enable Identity Protection Users respond much more favorably to conditional/situational MFA

Don't: Underestimate the complexity of hybrid CA

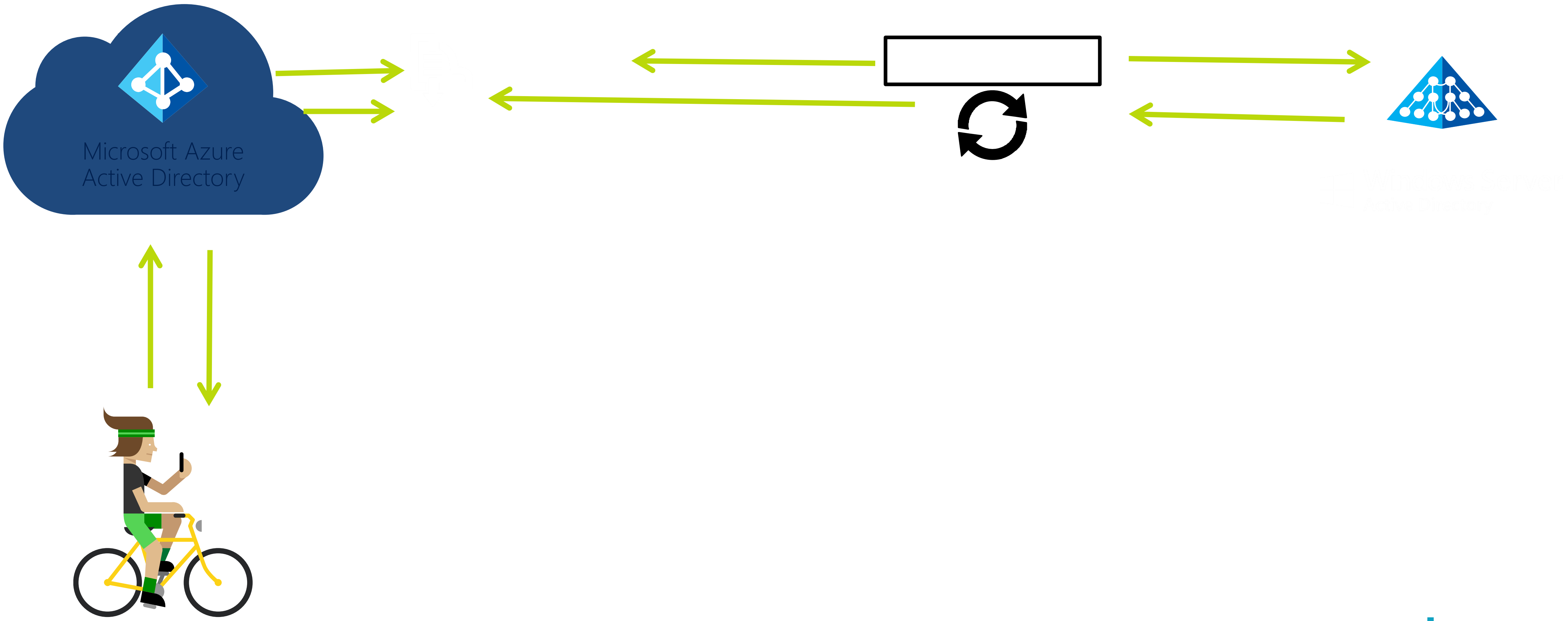
Don't: Assume users/business units will understand why

Don't: Forget to about the last 5%. But don't block on them.

Do: Know how to debug Modern Auth issues

Do: Know how to debug MFA authentications

Self-Service Password Reset


Microsoft Azure
Active Directory
Windows Server
Active Directory

SSPR Do's and Don't's

Do: Get executive sponsorship

Do: Stage using "Restrict Access to Password Reset"

Do: Use "Require Users To Register When Signing In"

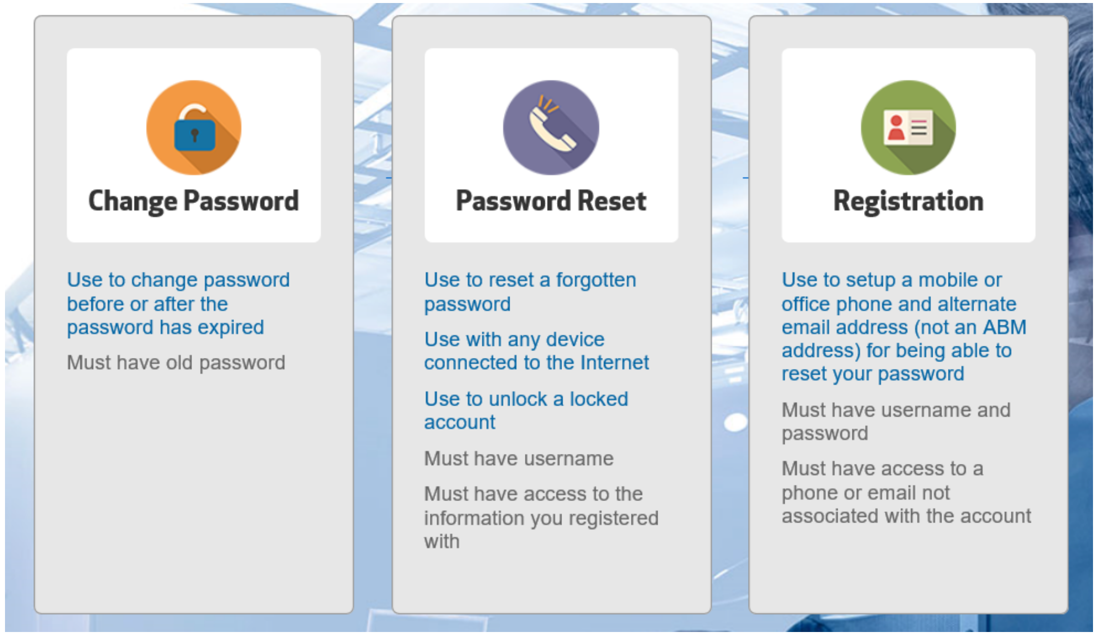
Do: Deploy alongside an app that users want to use

Do: Communicate to end users

Do: consider building an SSPR Portal (password.company.com).

Do: Use the PowerBI Content Pack

Don't: test with an Administrative Account



Change Password

Use to change password before or after the password has expired

Must have old password

Password Reset

Use to reset a forgotten password

Use with any device connected to the Internet

Use to unlock a locked account

Must have username

Must have access to the information you registered with

Registration

Use to setup a mobile or office phone and alternate email address (not an ABM address) for being able to reset your password

Must have username and password

Must have access to a phone or email not associated with the account

Integrating SaaS apps with Azure AD

SaaS integration Do's and Don't's

Do: Use Dynamic Groups to automate entitlements

Do: Use Provisioning when possible

Do: Understand the subtleties of SSO:

- SAML Identifier
- Idle Timeout
- Single Sign Out

Don't: Assume all vendors understand how SSO works

Don't: Forget about Conditional Access with SaaS

Do: Push ISVs to get in the gallery

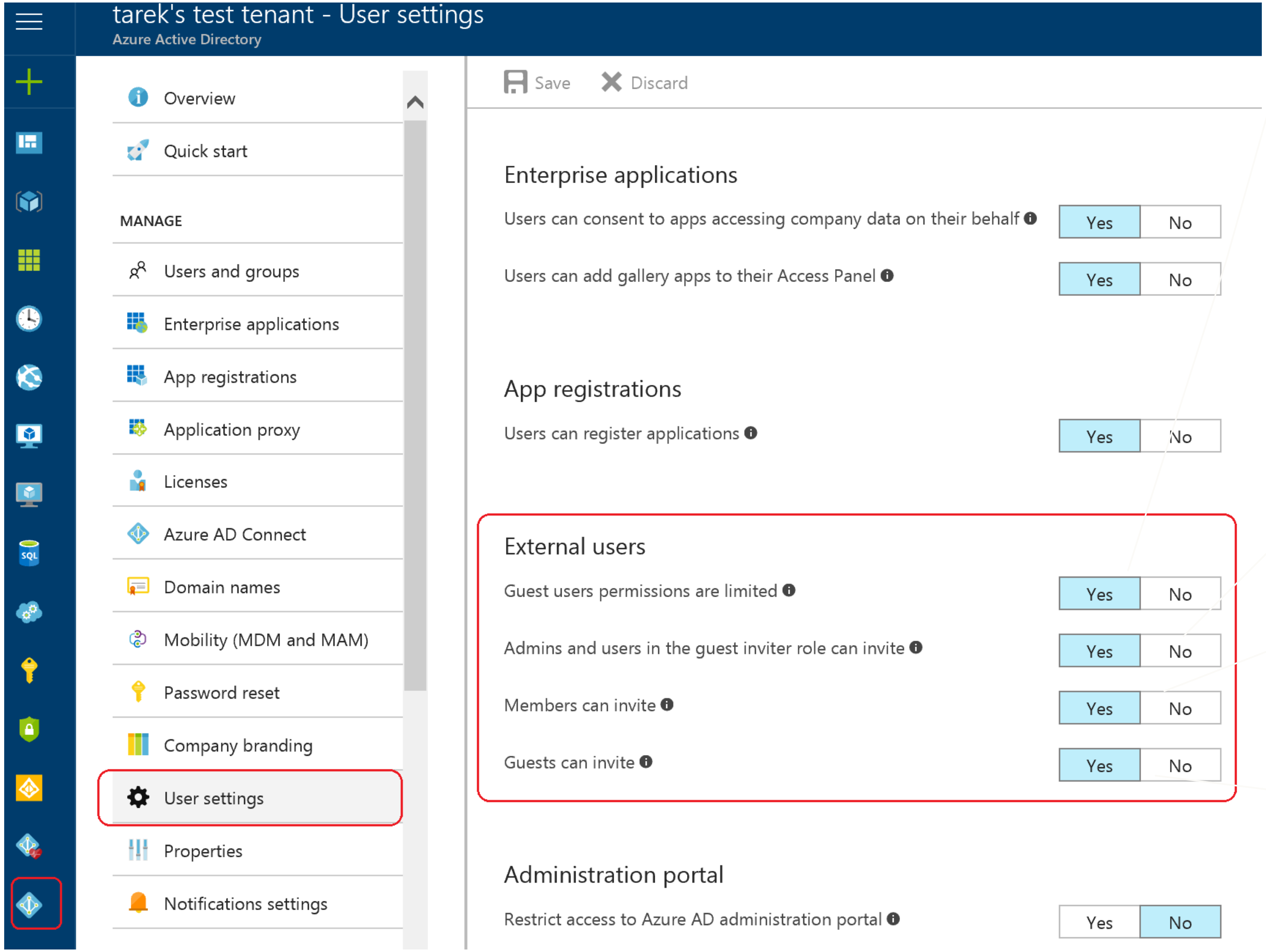
Do: Talk to your leadership: SSO is a security posture, not just an end user convenience issue.

External Collaboration Controls

B2B Basics

- A principal is always created in the inviter directory referring to the principals of the external identities. There are 2 parts to it:
- Invitation
- Redemption
  - For a reminder on how B2B works, check out: https://aka.ms/b2bmechanics

Azure AD B2B Controls



Enterprise applications

Users can consent to apps accessing company data on their behalf: [✓ Yes] No

Users can add gallery apps to their Access Panel: [✓ Yes] No

App registrations

Users can register applications: [✓ Yes] No

External users

Guest users permissions are limited: [✓ Yes] No

Admins and users in the guest inviter role can invite: [✓ Yes] No

Members can invite: [✓ Yes] No

Guests can invite: [✓ Yes] No

Administration portal

Restrict access to Azure AD administration portal: Yes [✓ No]

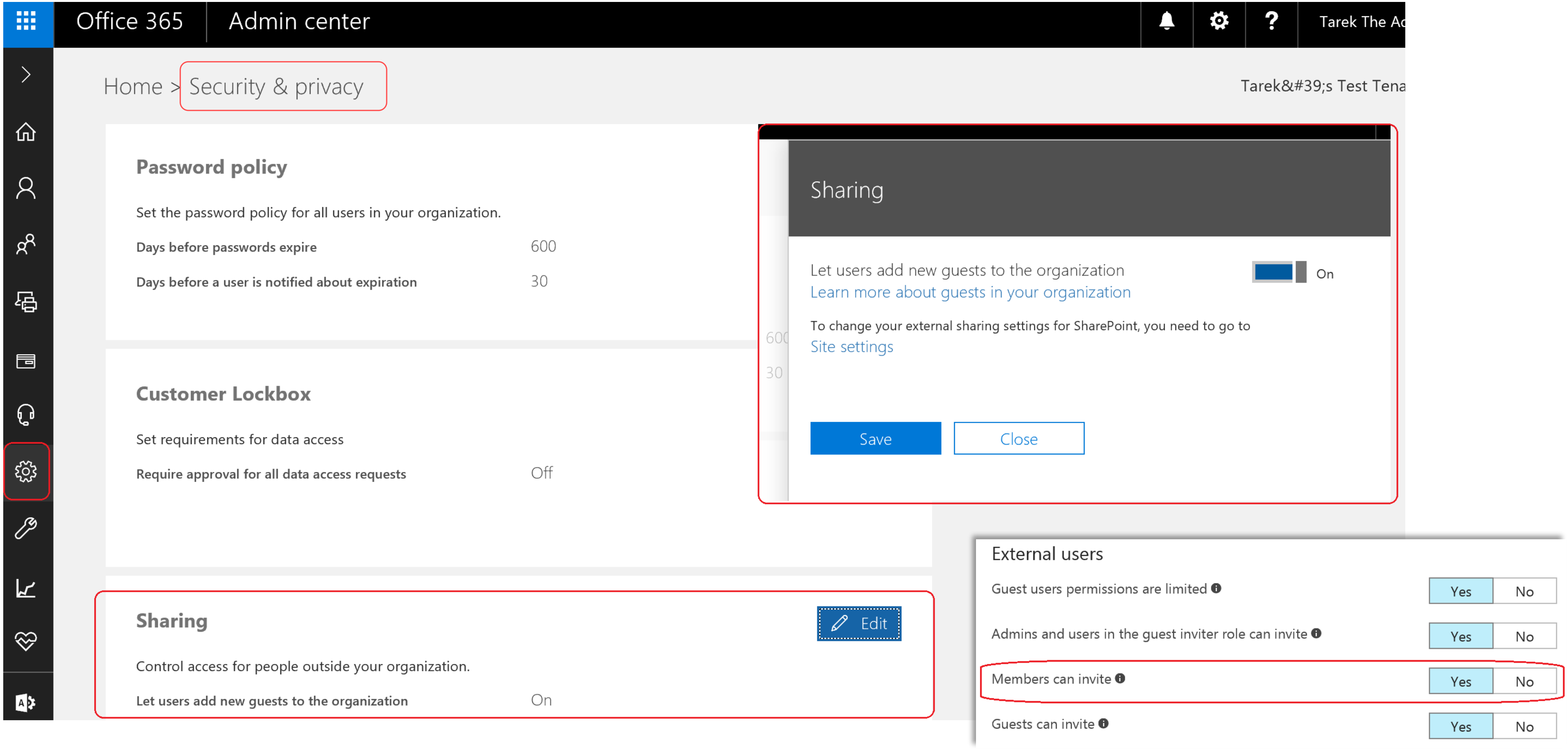
Good. Otherwise Guests have the same directory access as members.

No means Guest Inviters cannot invite, but Global Admins can always invite.

Good for customers focused on collaboration. Can be secure with Access Reviews and Audit

Questionable security wise unless combined with other controls.

Office 365 Admin Portal B2B Controls



Password policy

Set the password policy for all users in your organization.

Days before passwords expire	600
Days before a user is notified about expiration	30

Customer Lockbox

Set requirements for data access

Require approval for all data access requests	Off

Sharing

Control access for people outside your organization.

Let users add new guests to the organization	On

Sharing

Let users add new guests to the organization — On

Learn more about guests in your organization

To change your external sharing settings for SharePoint, you need to go to Site settings

External users

Guest users permissions are limited	[✓ Yes]	No
Admins and users in the guest inviter role can invite	[✓ Yes]	No
Members can invite	[✓ Yes]	No
Guests can invite	[✓ Yes]	No

Quick Wins

Homework! Go home and do this

- Turn on Password Hash Sync
- Turn on MFA or use PIM (Privileged Identity Mgmt)
- Use the PowerBI Sign-On Content Pack (here)

- Next Week:
  - Turn on Azure AD Connect Health, all of them.
  - Enable Group Based Licensing
  - Enable SSPR for a Pilot set of users
  - Setup a SaaS app
  - Configure a Conditional Access Policy on it

Homework! Go home and do this

- Configure Conditional Access
- Configure B2B policies

Thank you!

Our Sponsors

DIAMOND

pointfire
Multilingual SharePoint

veeam

COMMUNITY

ESPC20
ONLINE
14-15 OCTOBER 2020

EUROPEAN COLLABORATION SUMMIT

Microsoft

Office 365 Portugal

sharept

collabdays | lisbon

collabdays | lisbon