Azure Active Directory Best Practices From the Field

Mustafa Toroman• @toromust

Sasha Kranjac • @sasakranjac

BIWUG

DIWUG

Dutch Information Worker User Group

Our Platinum Sponsors

advantive
innovative people valuable solutions

cegeka
IN CLOSE COOPERATION

ShareValue

Community Sponsor

EUROPEAN COLLABORATION SUMMIT

Our Gold Sponsors

AMPLEXOR
AN ACOLAD COMPANY

avanade

AvePoint

BLIS.digital

CTG

delaware

inetum.
realdolmen
Positive digital flow

INSPARK

KWizCom
Knowledge Worker Components

macaw

MARTELLO

Motion10

pointfire
Multilingual SharePoint

Quest

Rapid Circle

RECOMATICS

ShareGate:

the flow
Digital Workplace Consulting

VALID
STAY AHEAD

Xylos

Code of Conduct

As event and experience organizers, we seek to provide a respectful, friendly, professional experience for everyone, regardless of gender, sexual orientation, physical appearance, disability, age, race or religion.

We do not tolerate any behavior that is degrading to any gender, race, sexual orientation, or disability, or any behavior that would be deemed harassment or discrimination.

Individuals are responsible for knowing and abiding by our standards and we encourage everyone to assist in creating a welcoming and safe environment. Please report any concerns, suspicious or disruptive activity or behavior to the organizing team, so that we can address the issue immediately.

More information can be found on the CollabDays Belgium & Netherlands website at https://www.collabdays.org/2021-benl/about

MUSTAFA TOROMAN
Solution Architect @ Cloudeon

Microsoft Azure MVP
MCSE, MCP, MCSA, MCITP, MCSD, MCT, MS v-TSP

@toromust

SASHA KRANJAC

Cloud Security Architect |CEO @ Kloudatech

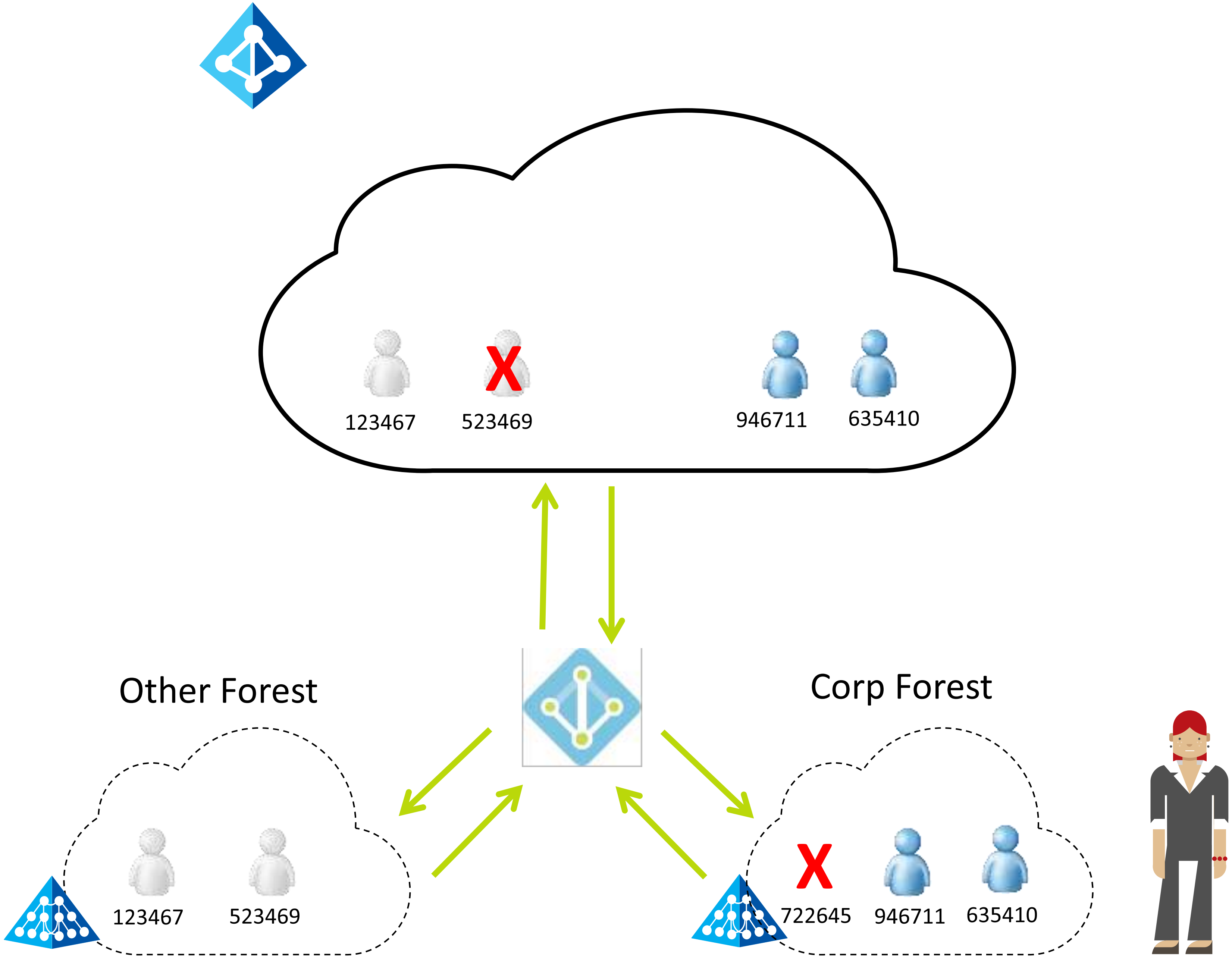
Microsoft Azure MVP

MCT, MCT Regional Lead, Certified EC-Council Instructor

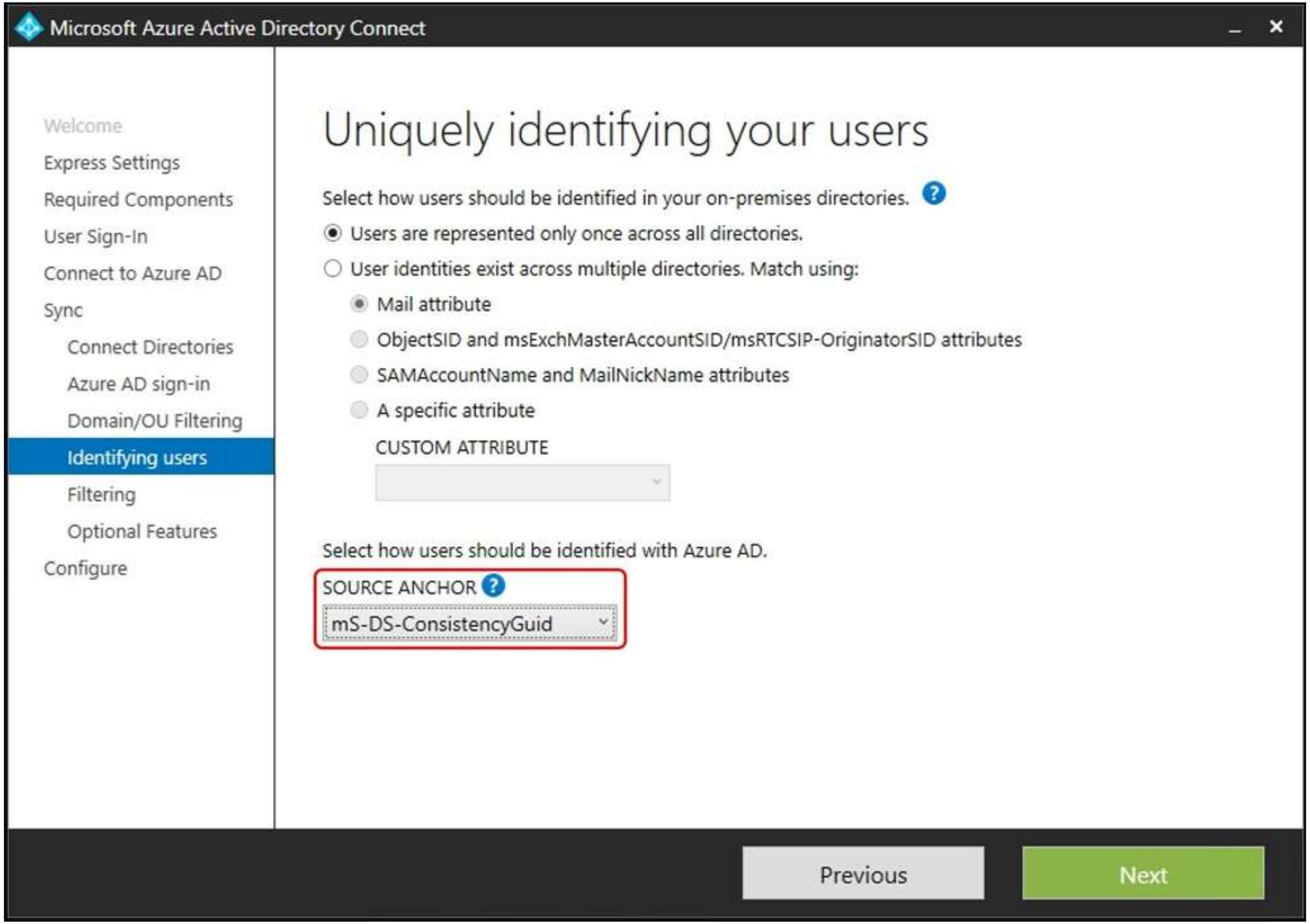
@SasaKranjac

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:

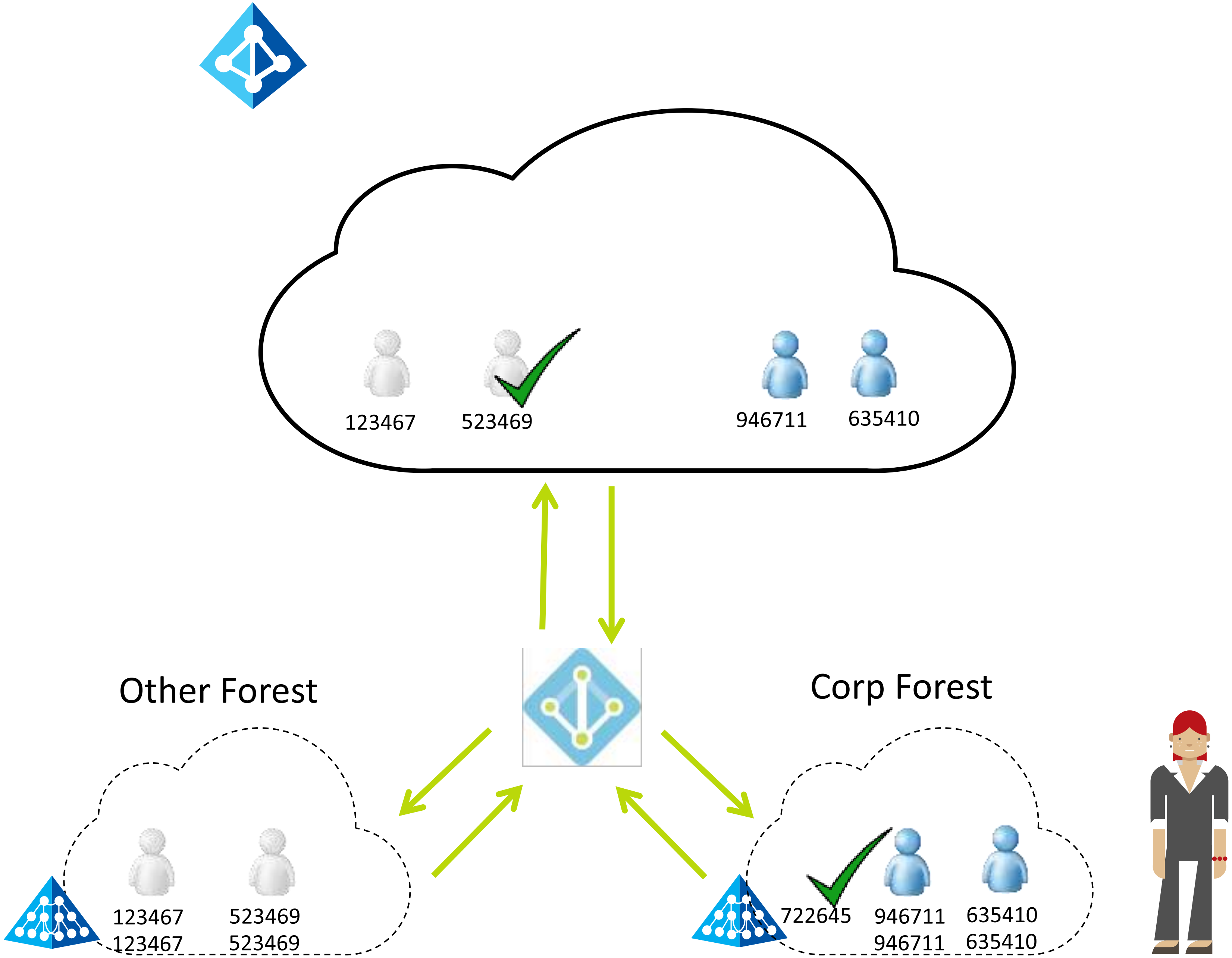
- ● Mail attribute
- ○ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
- ○ SAMAccountName and MailNickName attributes
- ○ A specific attribute

CUSTOM ATTRIBUTE

Select how users should be identified with Azure AD.

SOURCE ANCHOR: mS-DS-ConsistencyGuid

Sync Consistency GUID:



Sync Dos and Don'ts

- 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

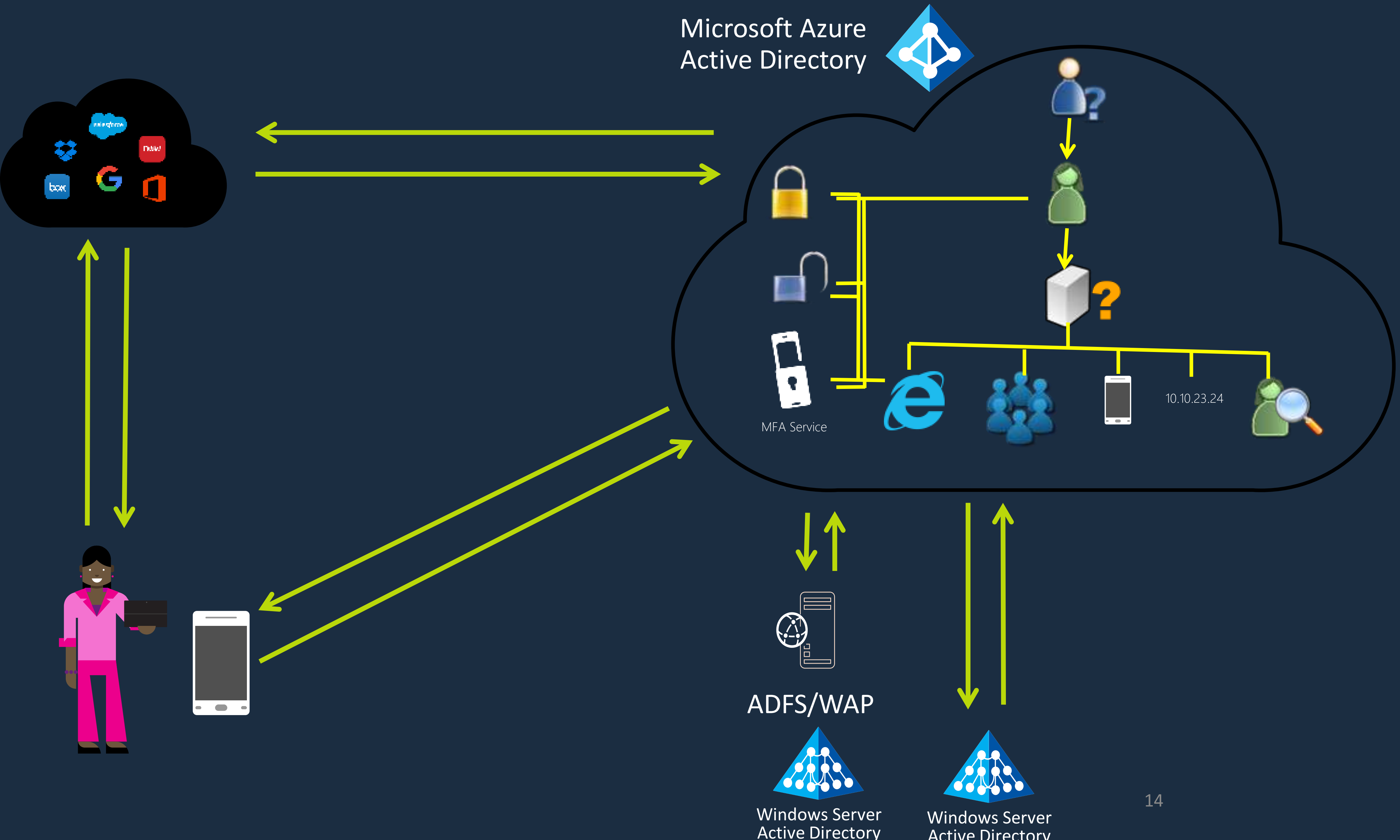
Password Hash Sync

- 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 company's 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



Microsoft Azure Active Directory

MFA Service

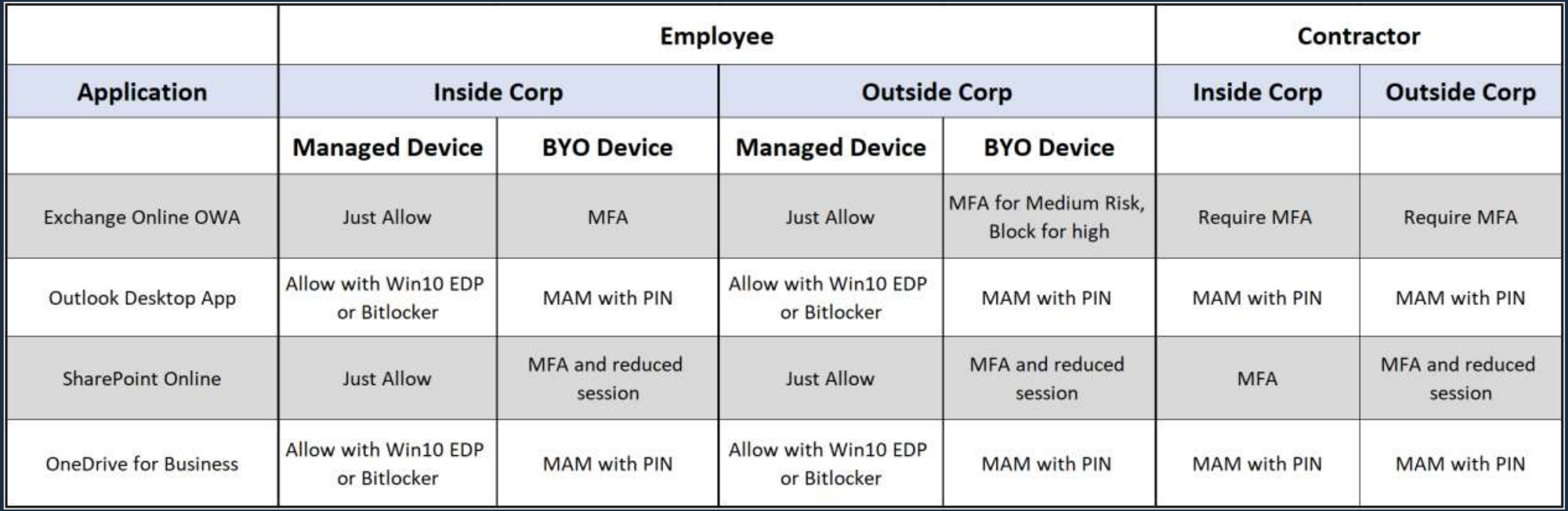
10.10.23.24

ADFS/WAP

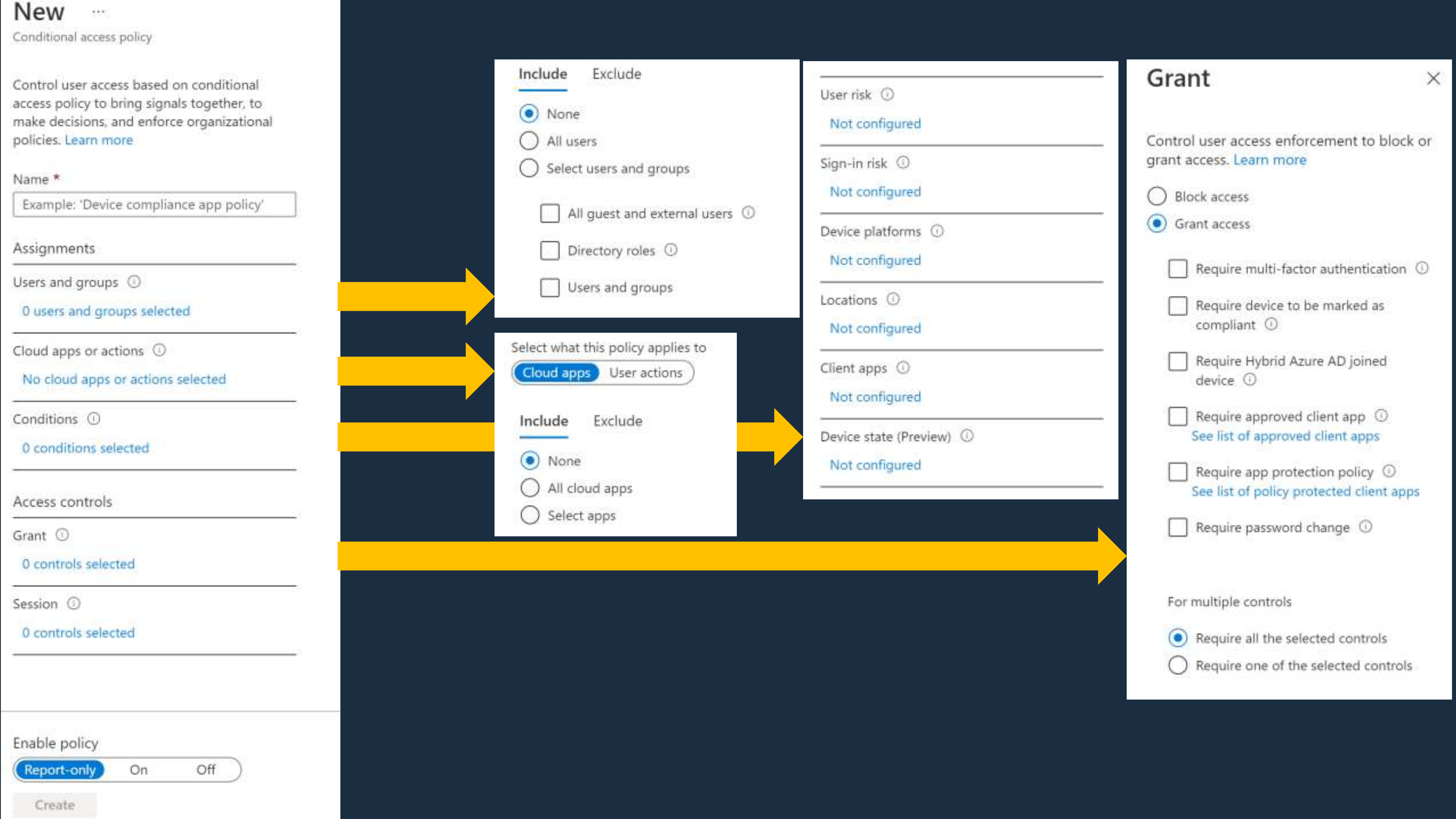
Windows Server Active Directory

Windows Server Active Directory

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



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

Enable policy

[✓ Report-only] On Off

Create

Include Exclude

● None
○ All users
○ Select users and groups

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

Select what this policy applies to

[✓ Cloud apps] User actions

Include Exclude

● None
○ All cloud apps
○ Select apps

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 ⓘ

For multiple controls

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

Conditional Access Dos and Don’ts

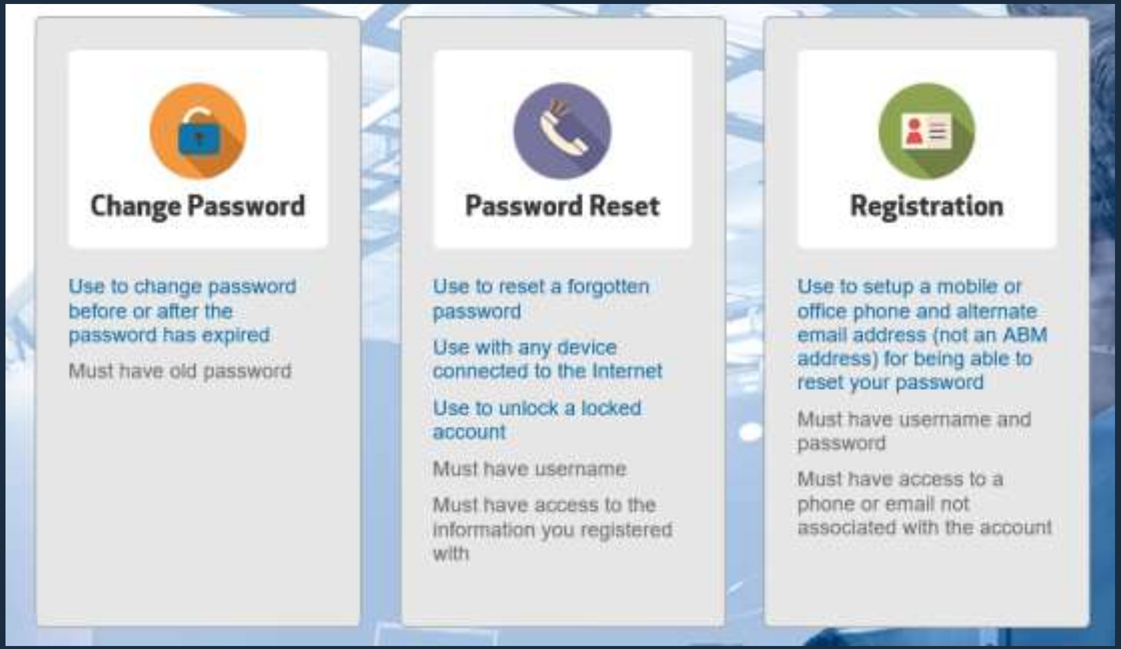
- Do: Use the Authenticator App
- Do: Exclude 1 Admin account from the policy
- Do: Enable Identity Protection Users respond much more favorably to conditional/situational MFA
- Do: Know how to debug Modern Auth issues
- Do: Know how to debug MFA authentications

- Don’t: Assume users/business units will understand why
- Don’t: Forget to about the last 5%. But don’t block on them.
- Don’t: Underestimate the complexity of hybrid CA

Self-Service Password Reset

SSPR Dos and Don'ts

- 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 Dos and Don’ts

- 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
- 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.
- Don’t: Assume all vendors understand how SSO works
- Don’t: Forget about Conditional Access with SaaS

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

Our Platinum Sponsors

advantive
innovative people valuable solutions

cegeka
IN CLOSE COOPERATION

ShareValue

Community Sponsor

EUROPEAN COLLABORATION SUMMIT

Our Gold Sponsors

AMPLEXOR
AN ACOLAD COMPANY

avanade

AvePoint

BLIS.digital

CTG

delaware

inetum.
realdolmen
Positive digital flow

INSPARK

KWizCom
Knowledge Worker Components

macaw

MARTELLO

Motion10

pointfire
Multilingual SharePoint

Quest

Rapid Circle

RECOMATICS

ShareGate:

the flow
Digital Workplace Consulting

VALID
STAY AHEAD

Xylos