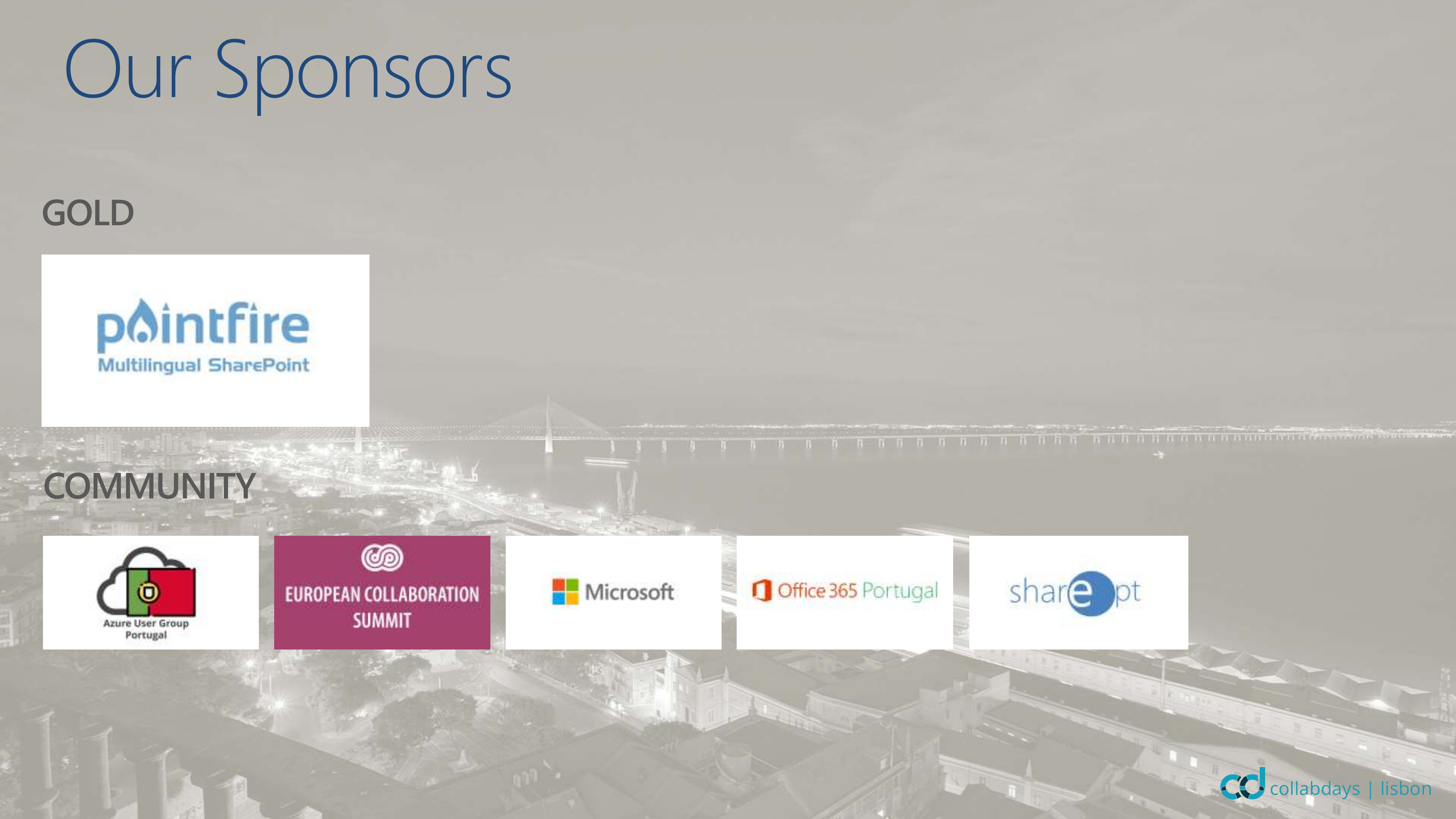
collabdays | lisbon

November 13th, 2021

Azure Active Directory Best practices from the field

by Mustafa Toroman and Sasha Kranjac



Our Sponsors

GOLD

pointfire
Multilingual SharePoint

COMMUNITY

Azure User Group
Portugal

EUROPEAN COLLABORATION
SUMMIT

Microsoft

Office 365 Portugal

sharept

MVP Microsoft® Most Valuable Professional

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

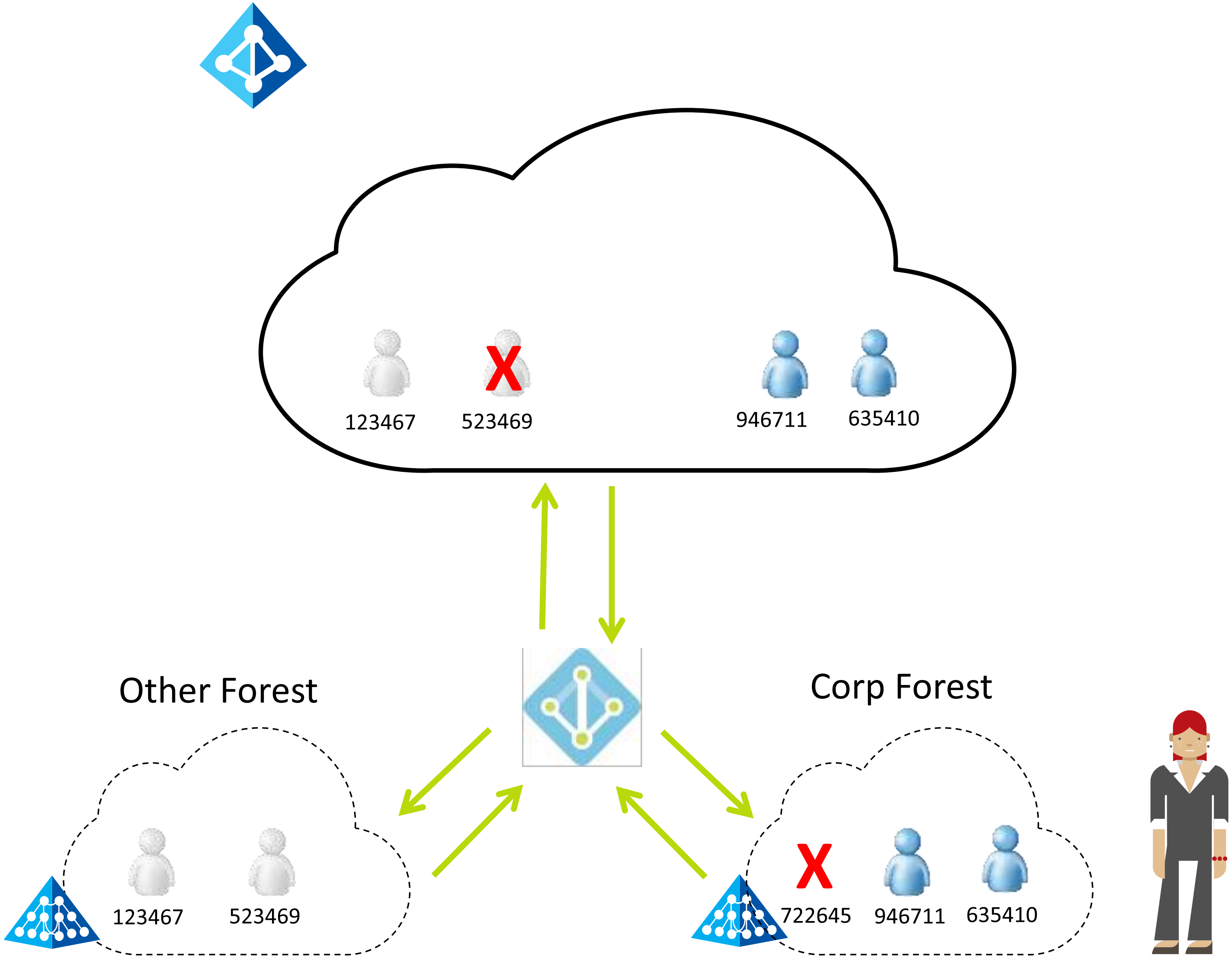
Microsoft Azure MVP

MCT, MCT Regional Lead, Certified EC-Council Instructor

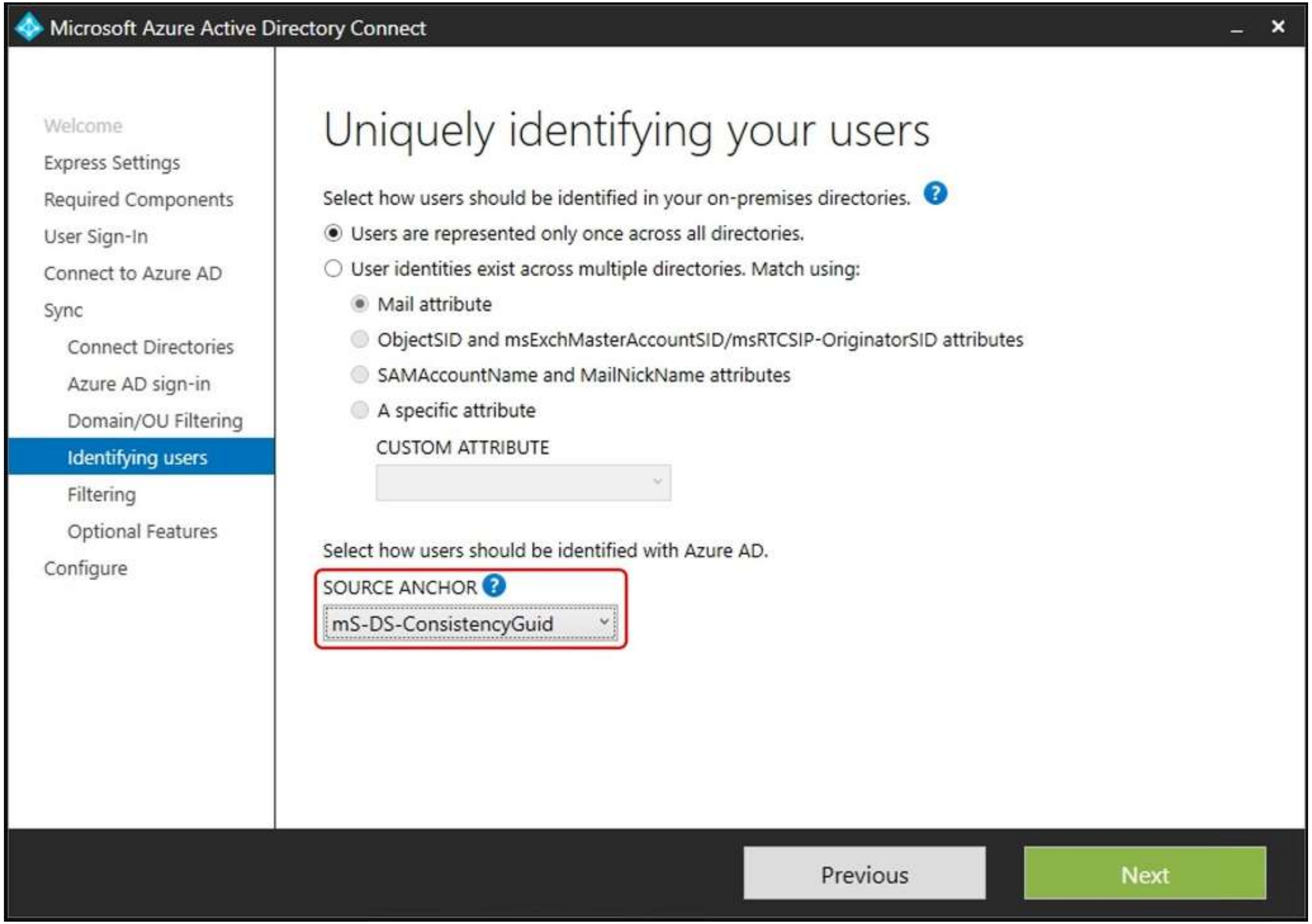
@SasaKranjac

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

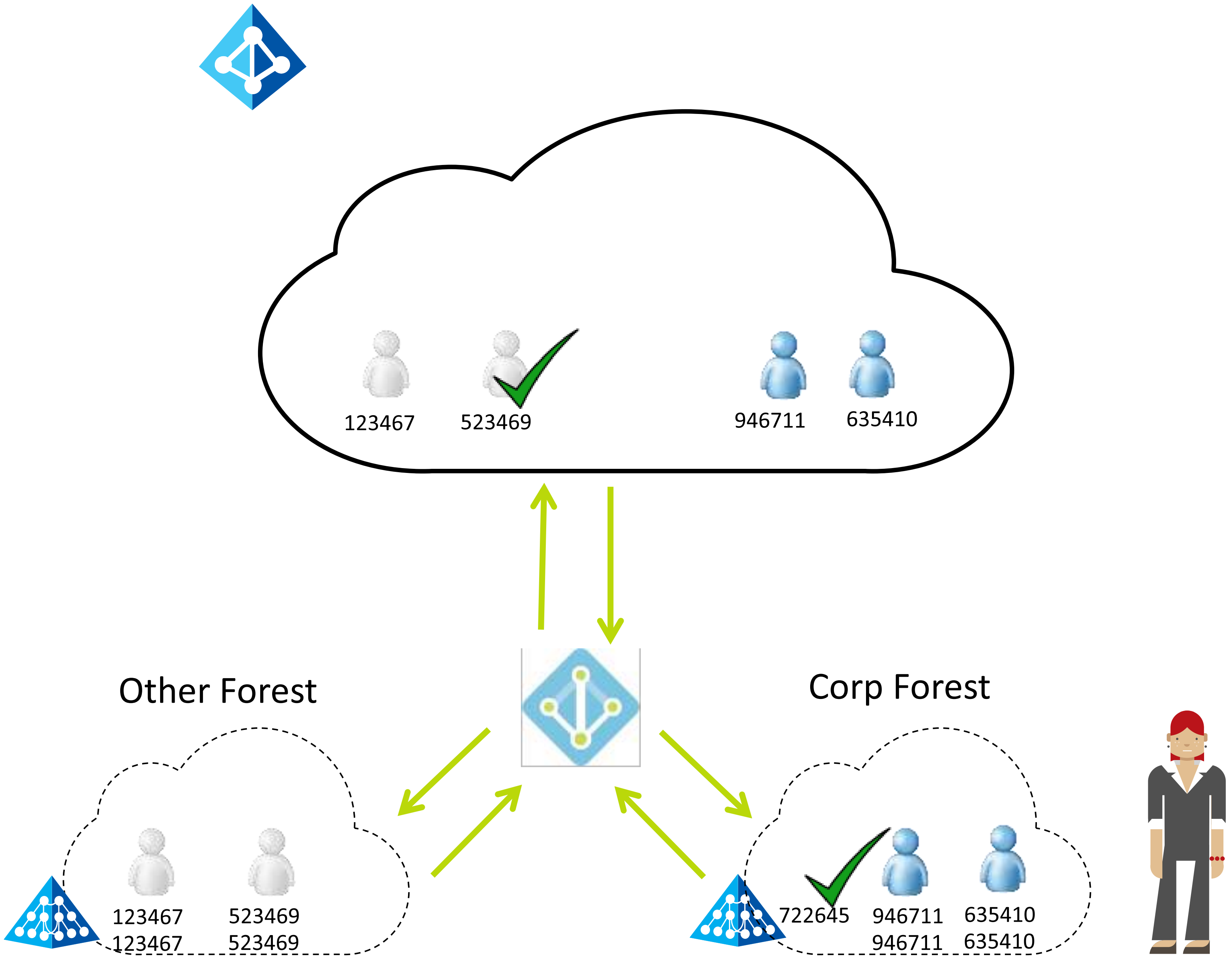
CUSTOM ATTRIBUTE

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

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

Security Taxonomies

User Type:

Employee or Contractor or Partner

Device Type:

Managed Device or BYOD

Network Location:

Inside or Outside Network

Application:

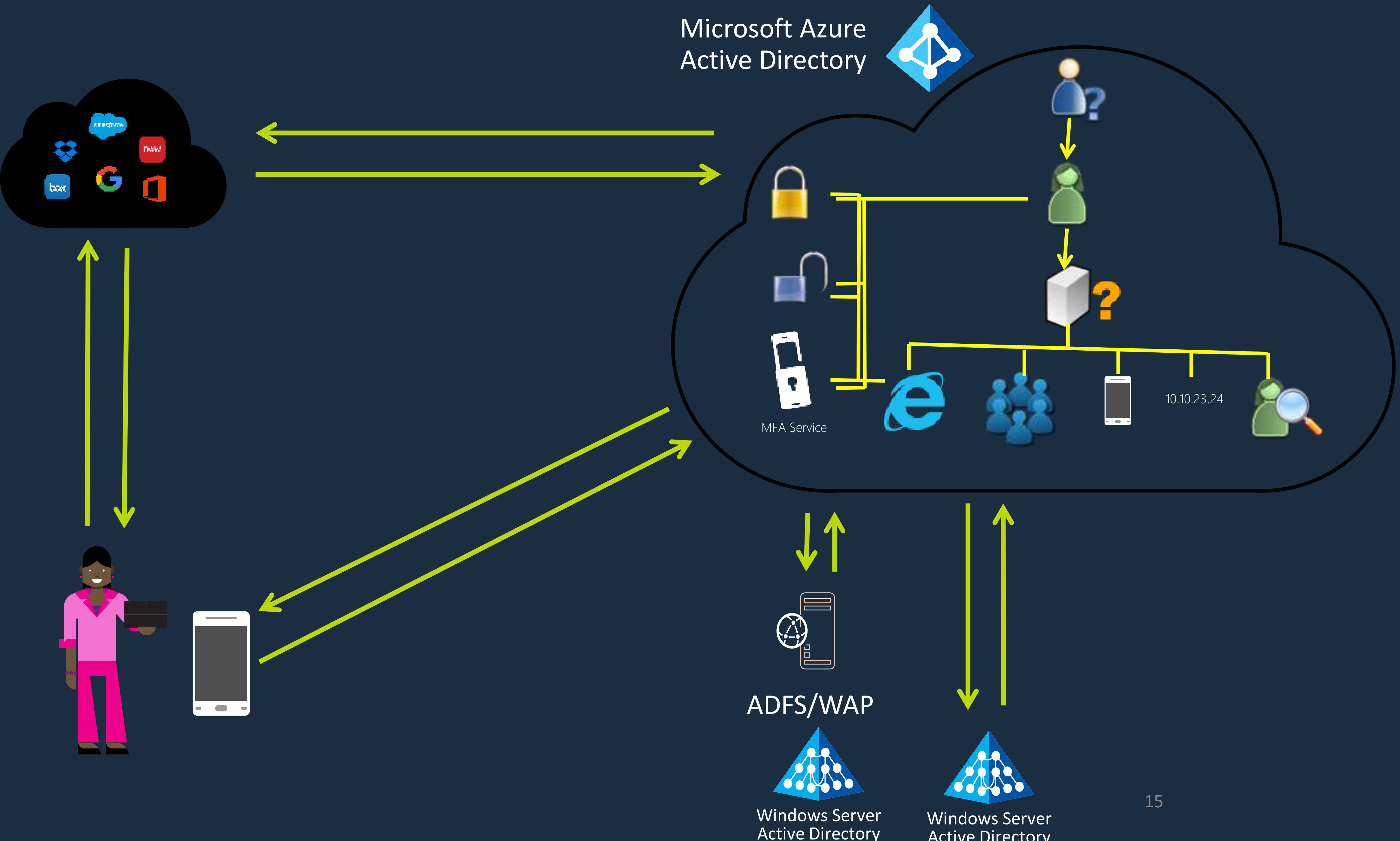
What resources is the user accessing

Client Type:

Mobile/Desktop App or Web App

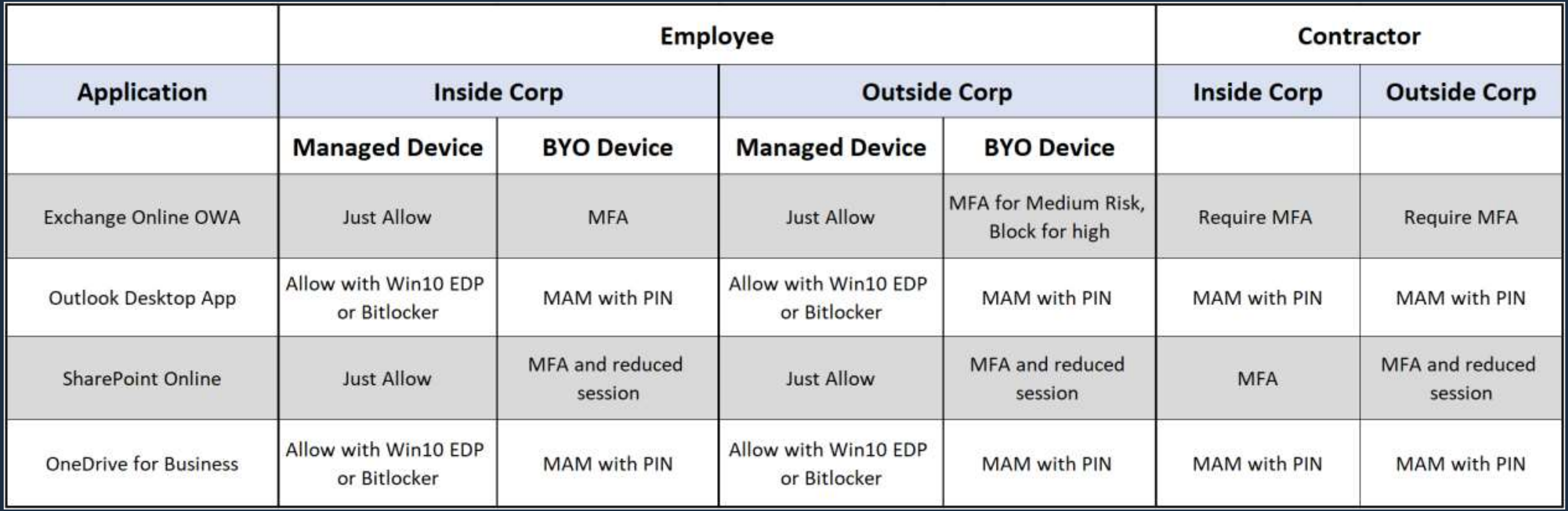
Risk Score:

High, Medium, or Low

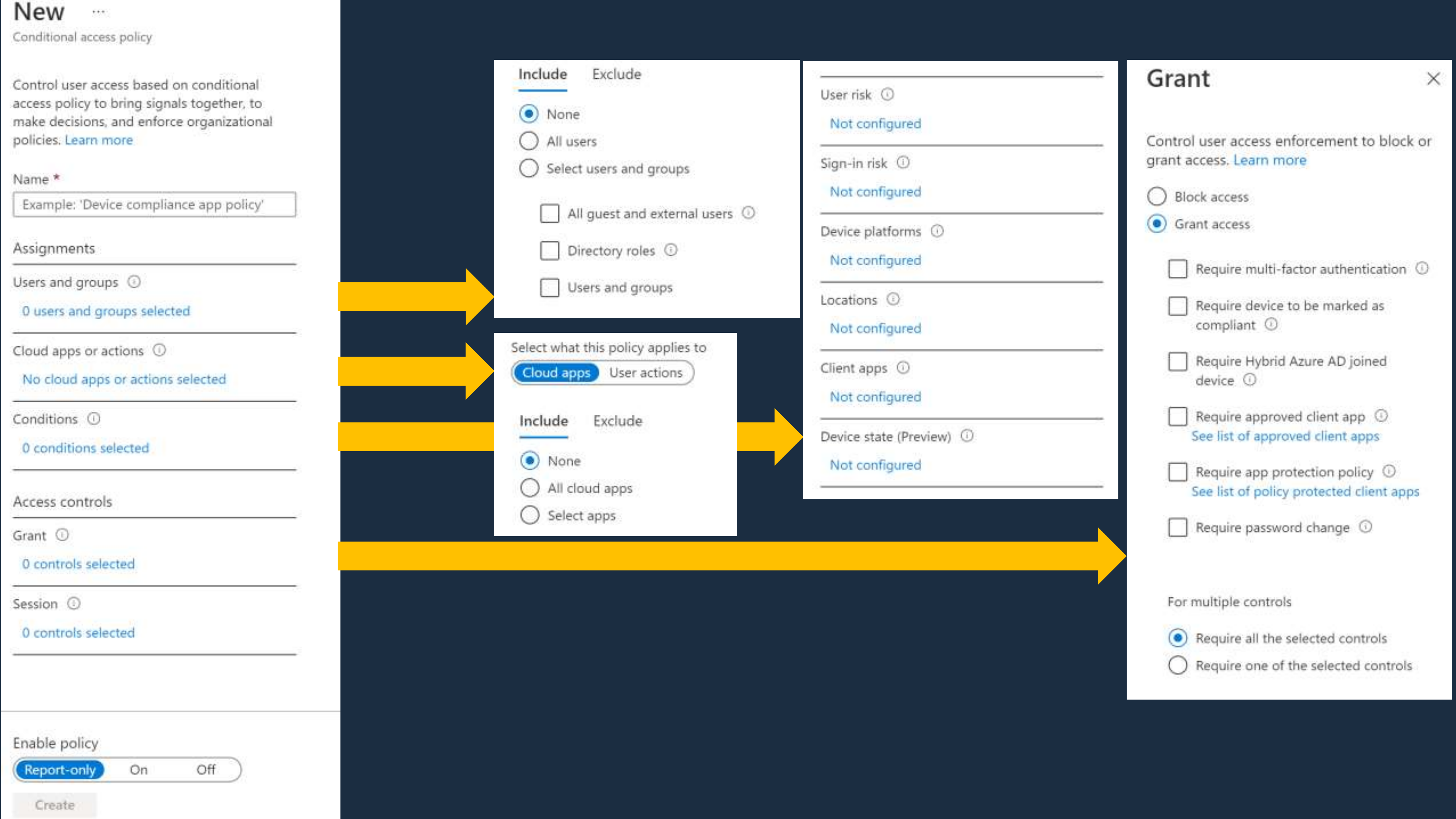


Microsoft Azure
Active Directory
MFA Service
10.10.23.24
ADFS/WAP
Windows Server
Active Directory
Windows Server
Active Directory

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

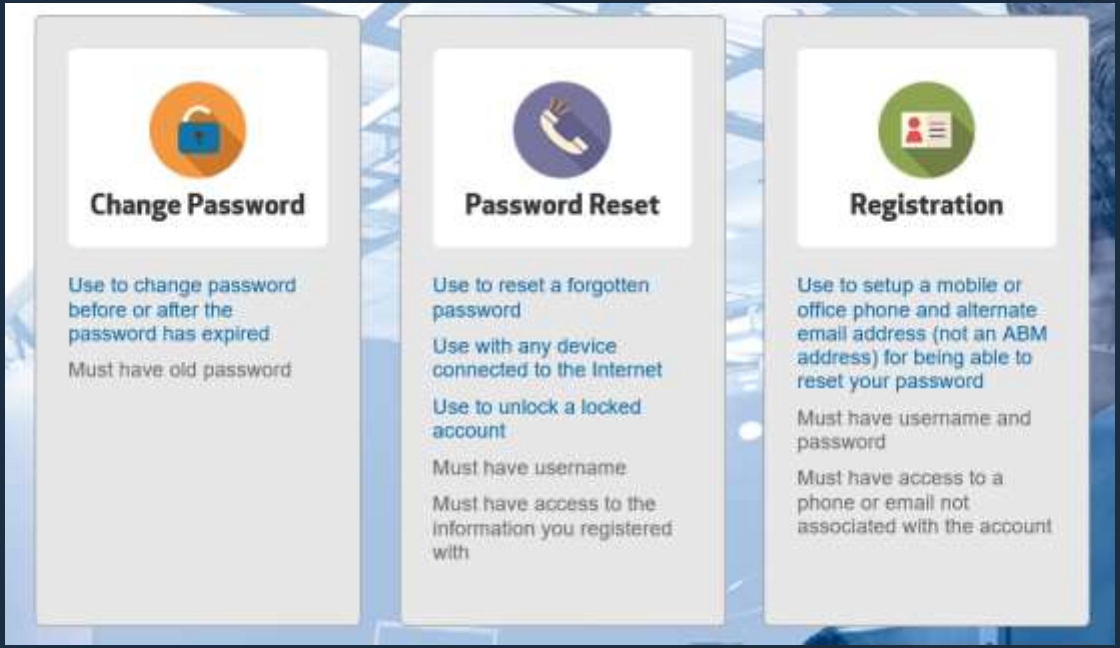
- Don’t: Assume users/business units will understand why
- Don’t: Forget to about the last 5%. But don’t block on them.
- Don’t: Underestimate the complexity of hybrid CA

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

External Collaboration Controls

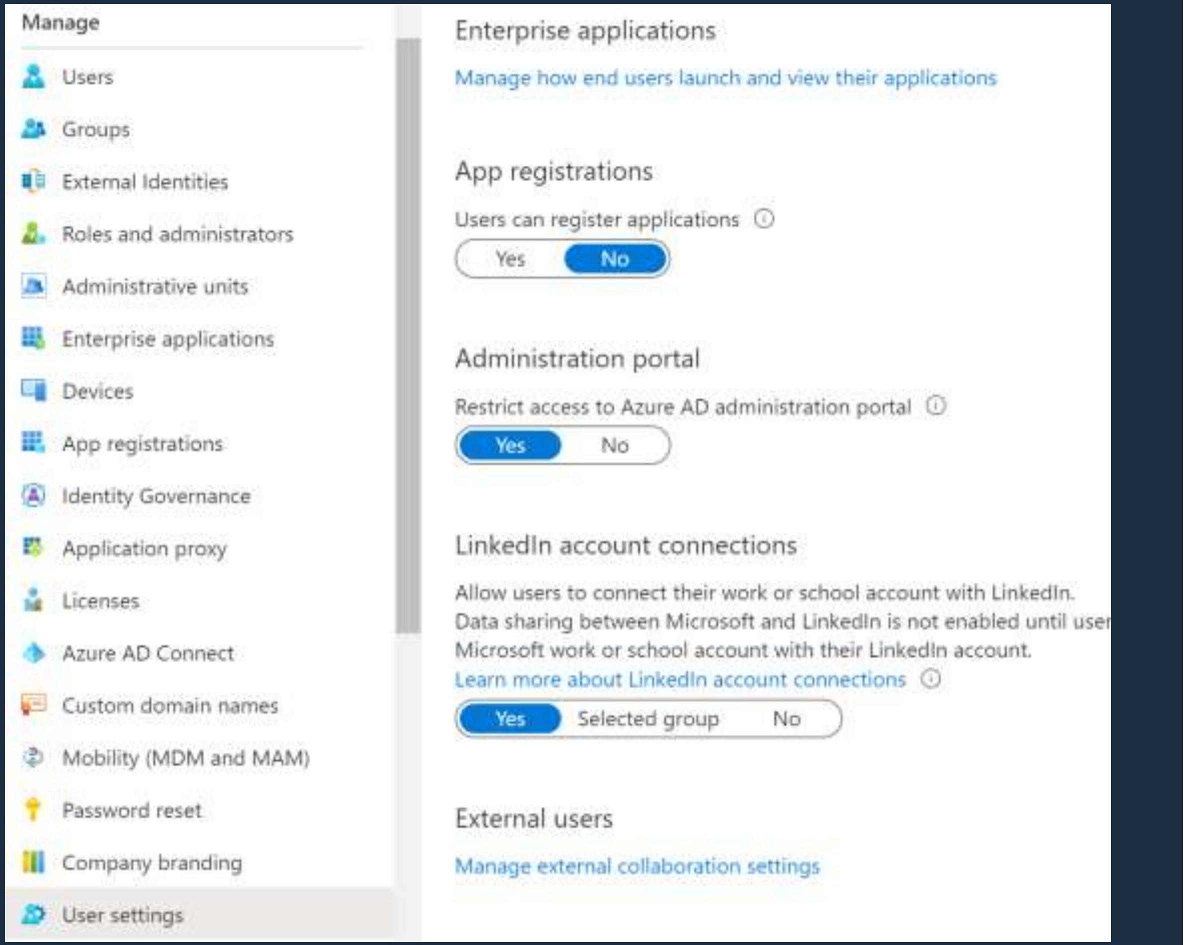
External Collaboration Controls

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

Azure AD B2B Controls



Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications ⓘ

Yes [✓ No]

Administration portal

Restrict access to Azure AD administration portal ⓘ

[✓ Yes] No

LinkedIn account connections

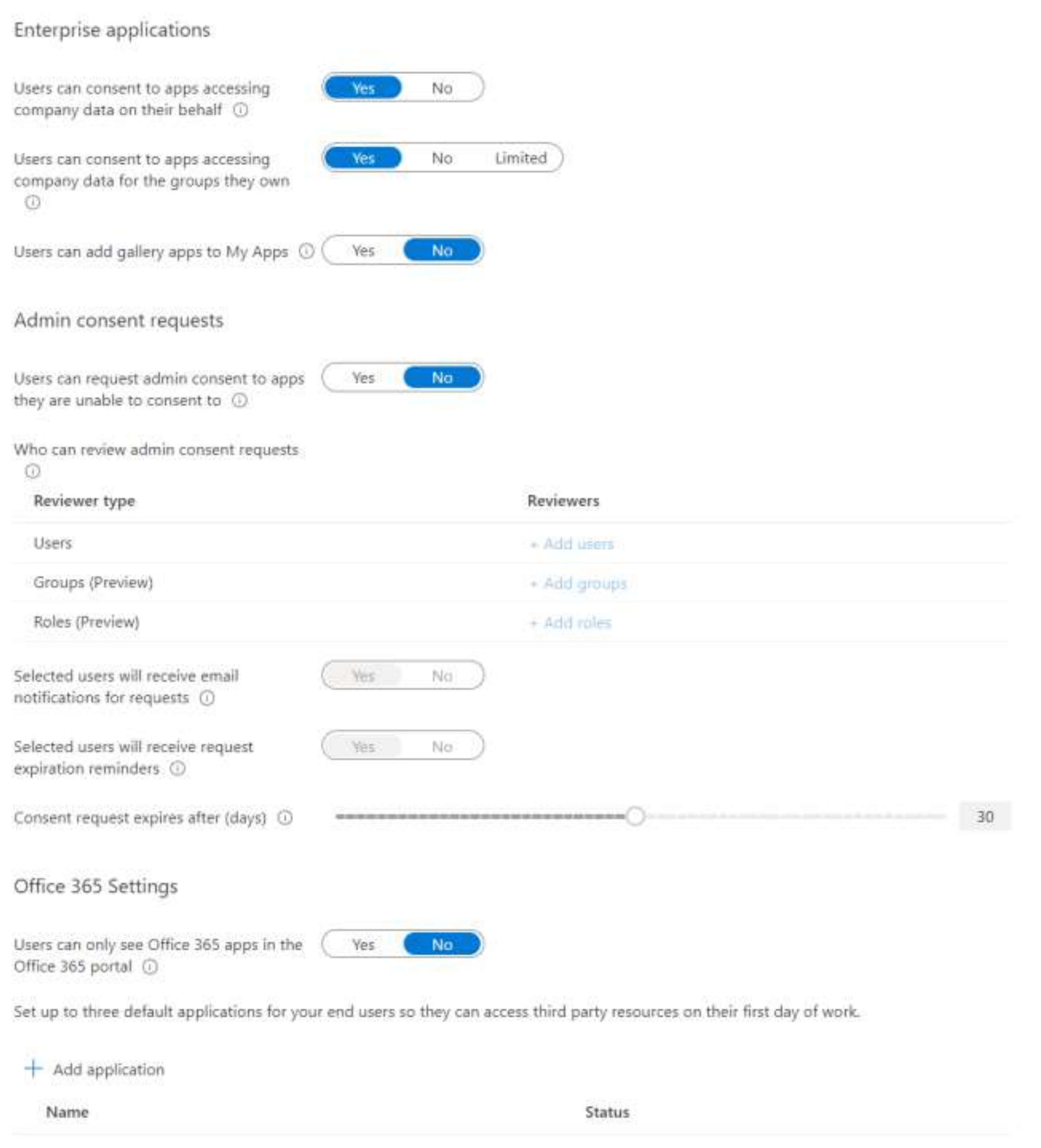
Allow users to connect their work or school account with LinkedIn. Data sharing between Microsoft and LinkedIn is not enabled until user Microsoft work or school account with their LinkedIn account.

Learn more about LinkedIn account connections ⓘ

[✓ Yes] Selected group No

External users

Manage external collaboration settings



Enterprise applications

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

Users can consent to apps accessing company data for the groups they own ⓘ — [✓ Yes] No Limited

Users can add gallery apps to My Apps ⓘ — Yes [✓ No]

Admin consent requests

Users can request admin consent to apps they are unable to consent to ⓘ — Yes [✓ No]

Who can review admin consent requests ⓘ

Reviewer type	Reviewers
Users	+ Add users
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests ⓘ — Yes No

Selected users will receive request expiration reminders ⓘ — Yes No

Consent request expires after (days) ⓘ — 30

Office 365 Settings

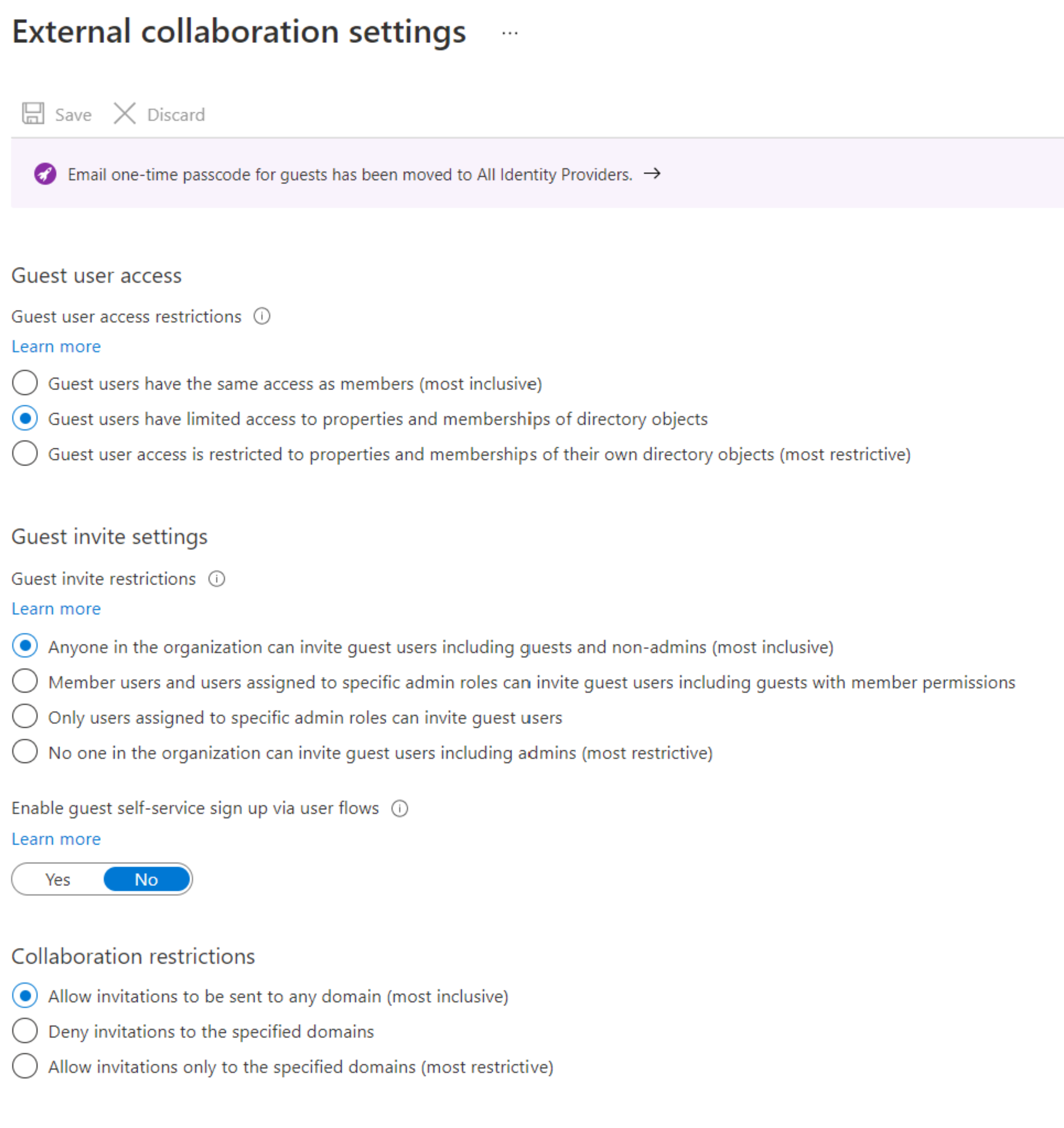
Users can only see Office 365 apps in the Office 365 portal ⓘ — Yes [✓ No]

Set up to three default applications for your end users so they can access third party resources on their first day of work.

+ Add application

Name	Status

Azure AD B2B Controls



External collaboration settings

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

Learn more

- ○ Guest users have the same access as members (most inclusive)
- ● Guest users have limited access to properties and memberships of directory objects
- ○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

- ● Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ○ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ○ Only users assigned to specific admin roles can invite guest users
- ○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

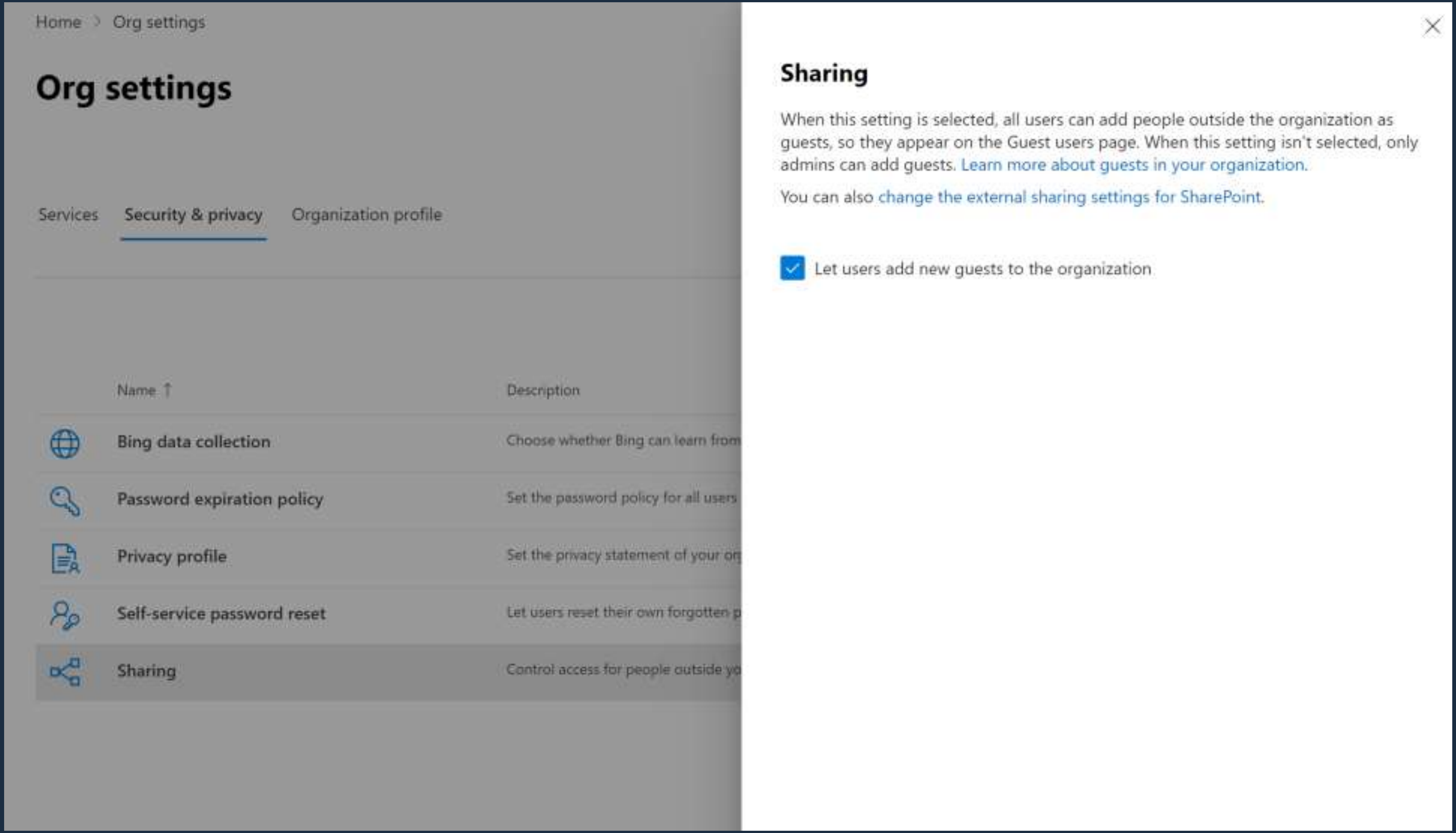
Learn more

Yes [✓ No]

Collaboration restrictions

- ● Allow invitations to be sent to any domain (most inclusive)
- ○ Deny invitations to the specified domains
- ○ Allow invitations only to the specified domains (most restrictive)

Office 365 Admin Portal B2B Controls



Home > Org settings

Org settings

Services | Security & privacy | Organization profile

	Name ↑	Description
	Bing data collection	Choose whether Bing can learn from
	Password expiration policy	Set the password policy for all users
	Privacy profile	Set the privacy statement of your or
	Self-service password reset	Let users reset their own forgotten p
	Sharing	Control access for people outside yo

Sharing

When this setting is selected, all users can add people outside the organization as guests, so they appear on the Guest users page. When this setting isn't selected, only admins can add guests. Learn more about guests in your organization.

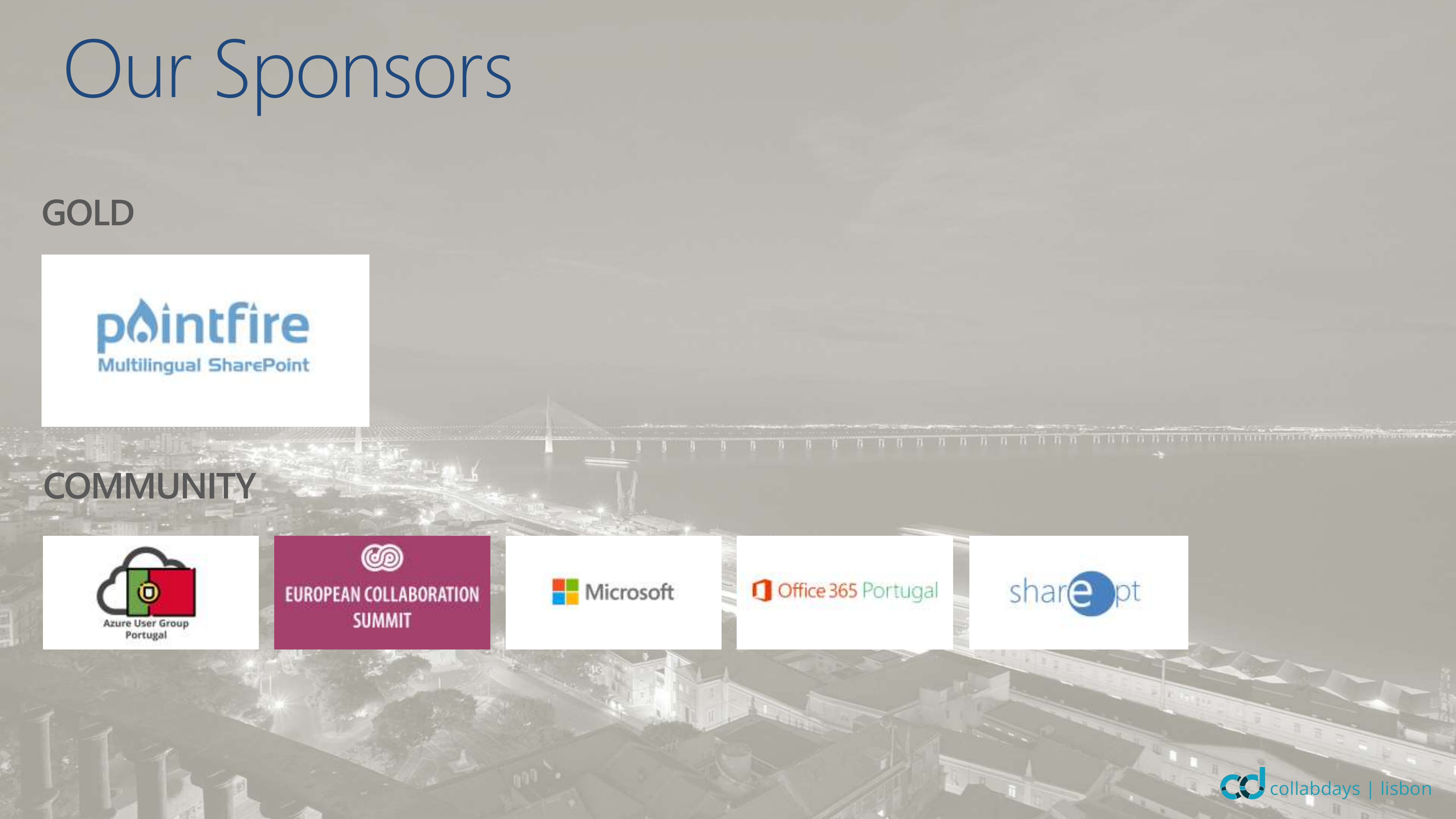
You can also change the external sharing settings for SharePoint.

☑ Let users add new guests to the organization

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 Sponsors

GOLD

pointfire
Multilingual SharePoint

COMMUNITY

Azure User Group
Portugal

EUROPEAN COLLABORATION
SUMMIT

Microsoft

Office 365 Portugal

sharept

collabdays | lisbon