Azure Active Directory best practices from around the world

Tarek Dawoud @azuread
Mark Morowczynski @markmorow
Program Managers
Identity Division

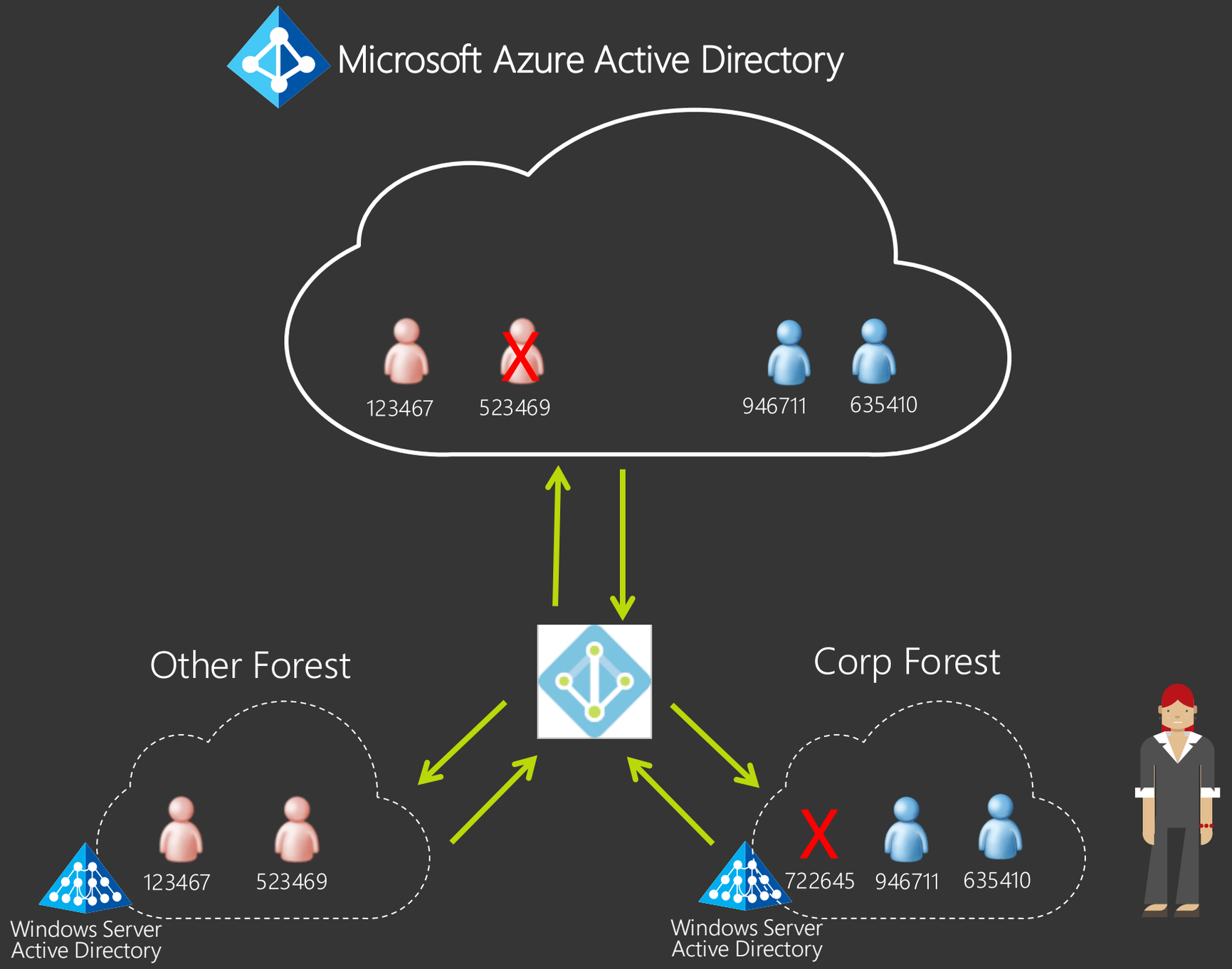
Microsoft

Agenda & Goals

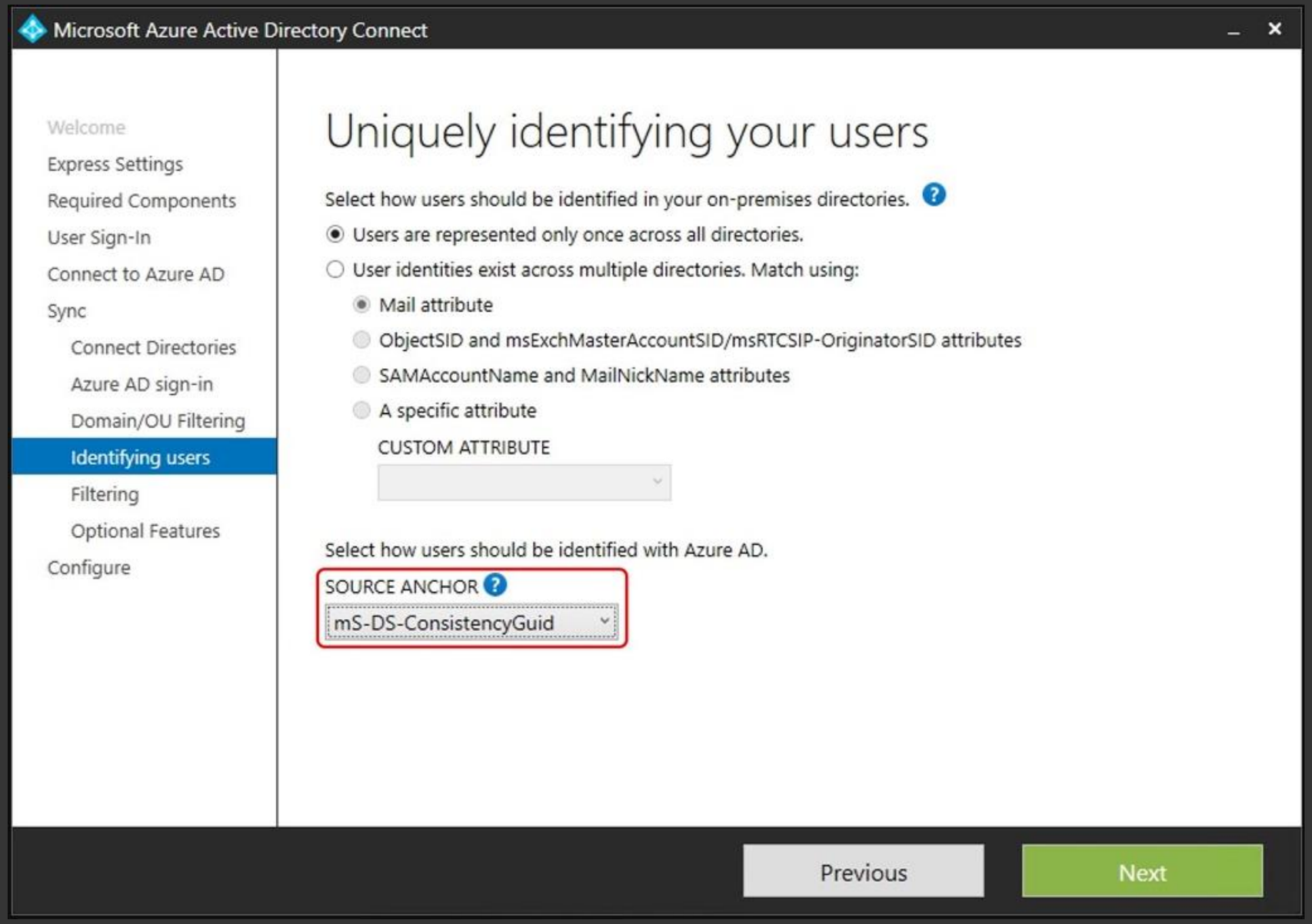
- Let you know we're out there deploying with you
- Deployment lessons from the real world
  - Things that can accelerate your deployment
  - Avoid things that can slow you down
- Deep Dive on a few technical areas and how you can approach them
- Get your feedback on how your deployments are going

Sync & Auth

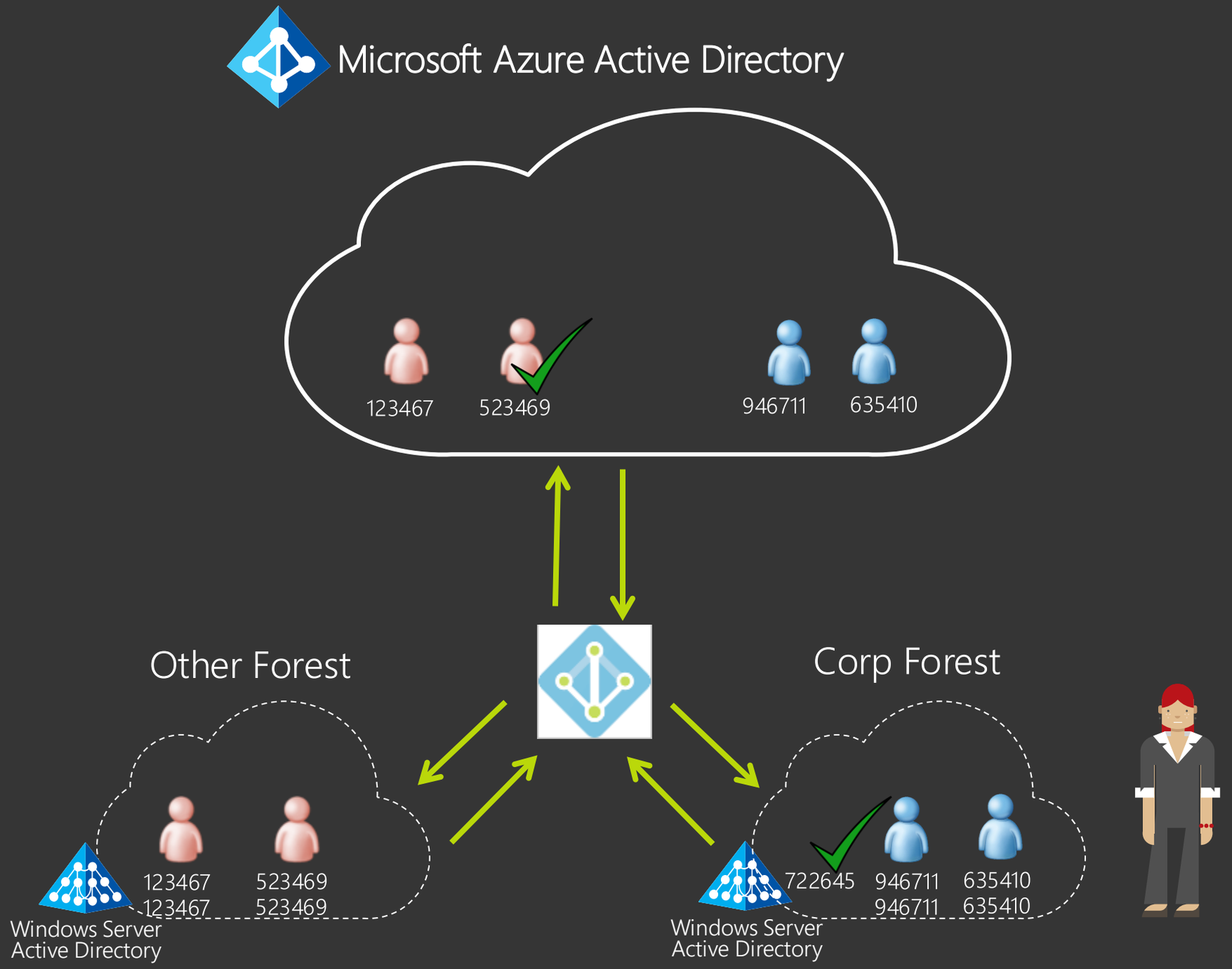
Sync Consistency GUID:



Sync Consistency GUID:



Sync Consistency GUID:



Sync Do's and Don't's

Do: Plan your Upgrade:
- In-place
- Parallel (staging) box
- Documentation

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

Don't': Sync with DA/EA Account

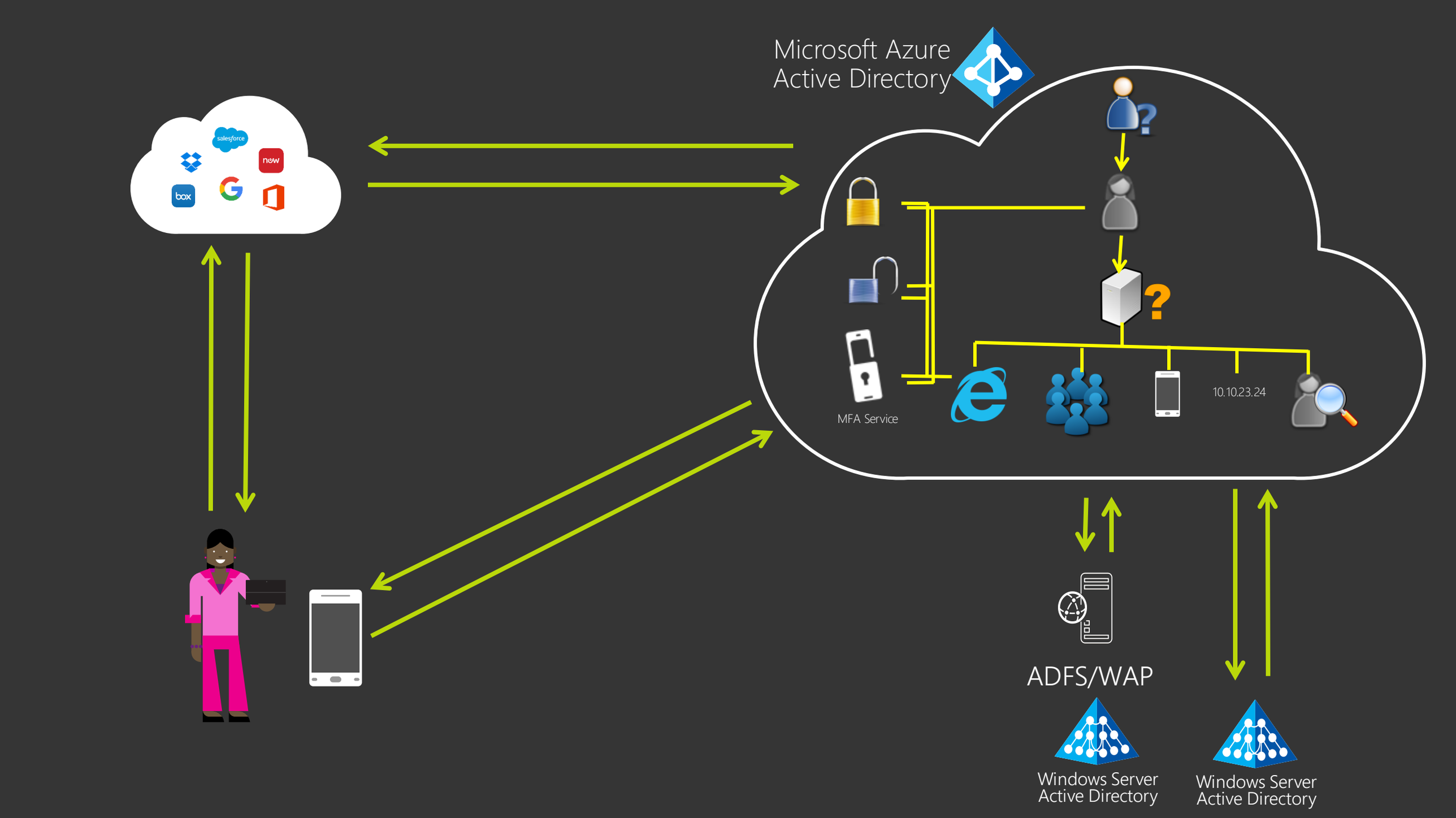
Password Hash Sync

- 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
- To understand how it works: aka.ms/aadpwhs
- 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 (BRK2076)


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

Security Taxonomies

User Type:

Employee or Contractor or Partner

Device Type:

Managed Device or BYOD

Network Location:

Inside or Outside Network

Application:

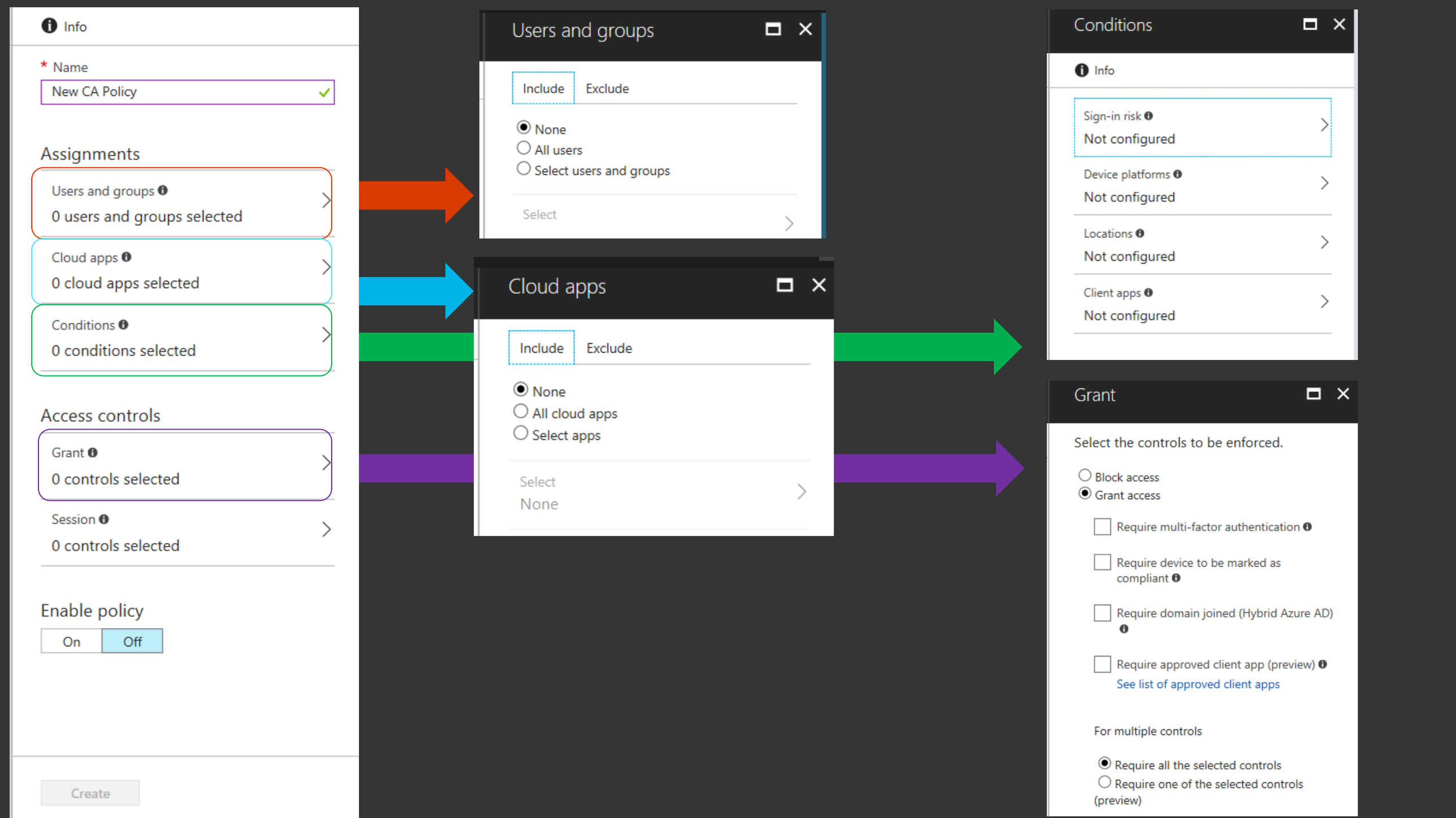
What resources is the user accessing

Client Type:

Mobile/Desktop App or Web App

Risk Score:

High, Medium, or Low


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 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

Conditional Access Do's and Don't's

Do: Use the Authenticator App

Do: Exclude 1 Admin account fron

Do:
Use
favo
conditional/situational MFA

Don't: Underestimate the complexity of hybrid CA

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

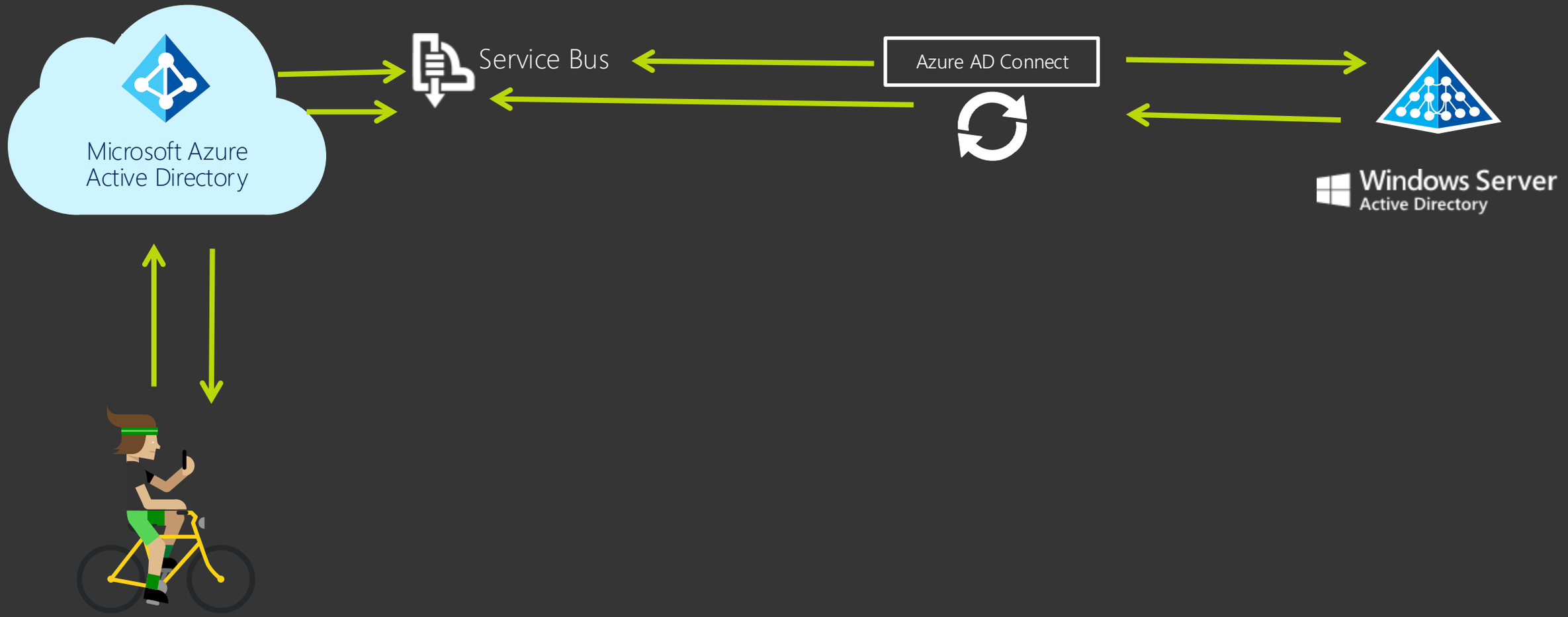
e last
them.

32	200	HTTPS	login.microsoftonlin...	/common/SAS/BeginAuth	1,900	no-cac...	application/...
33	200	HTTP	Tunnel to	login.microsoftonline.com:443	1,072		
34	200	HTTPS	login.microsoftonlin...	/common/instrumentation/reportpageload	264	private	application/...
35	200	HTTPS	login.microsoftonlin...	/common/SAS/EndAuth	1,976	no-cac...	application/...
36	200	HTTPS	login.microsoftonlin...	/common/SAS/EndAuth	1,976	no-cac...	application/...
37	200	HTTPS	login.microsoftonlin...	/common/SAS/EndAuth	1,900	no-cac...	application/...
38	**200**	**HTTPS**	**login.microsofton...**	**/common/SAS/ProcessAuth**	**4,158**	**no-cac...**	**text/html;...**

https://diagnostics.outlook.com/#/?env=ExRCA

Do: Know how to debug MFA authentications

Self-Service Password Reset


Microsoft Azure
Active Directory
Service Bus
Azure AD Connect
Windows Server
Active Directory

SSPR Do's and Don't's

Do: Your pre and post data homework

Do: Get executive sponsorship

Do: Stage using "Restrict Access to Password Reset"

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

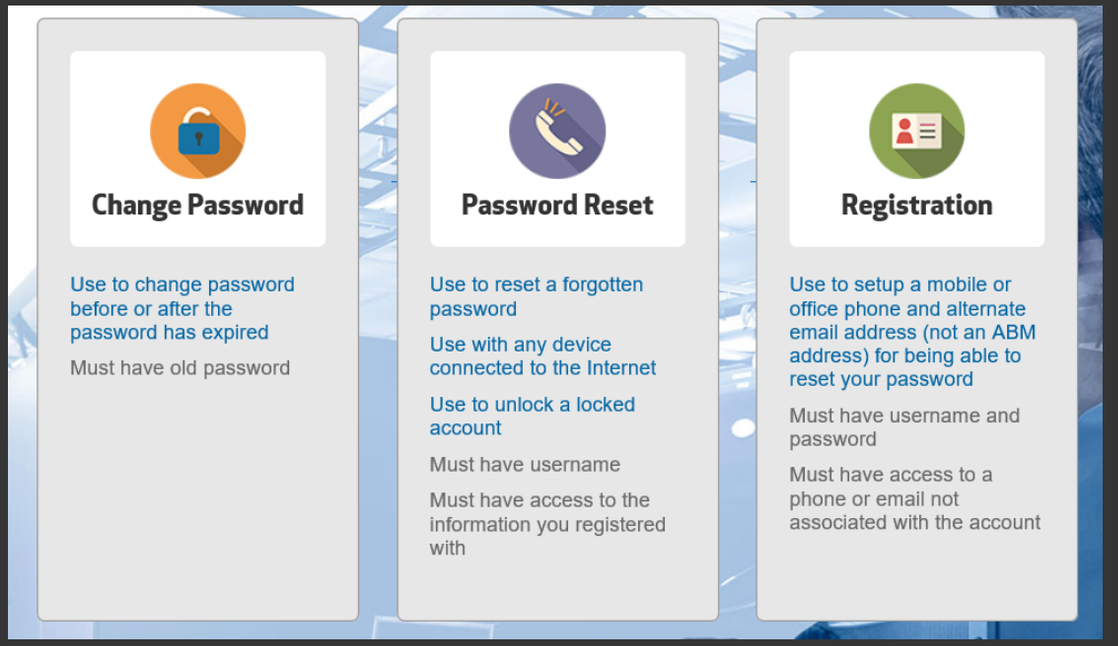
Do: Deploy alongside an app that users want to use

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



Integrating SaaS apps with Azure AD

SaaS integration Do's and Don't's

Do: Use Dy
automate

Do: Use Pr
possible

Do: Under
of SSO:

- IdP vs SP ir
- SAML Iden
- Idle Timeou
- Single Sign

haveibeenpwned.com

email address or username

pwned?

233	4,729,225,727	54,932	52,213,555
pwned websites	pwned accounts	pastes	paste accounts

Top 10 breaches

711,477,622	Onliner Spambot accounts	
593,427,119	Exploit.In accounts	
457,962,538	Anti Public Combo List accounts	
393,430,309	River City Media Spam List accounts	
359,420,698	MySpace accounts	
234,842,089	NetEase accounts	
164,611,595	LinkedIn accounts	
152,445,165	Adobe accounts	
112,005,531	Badoo accounts	
105,059,554	B2B USA Businesses accounts	

all vendors
v SSO works

bout Conditional
nS

o get in the

eadlistyourapp

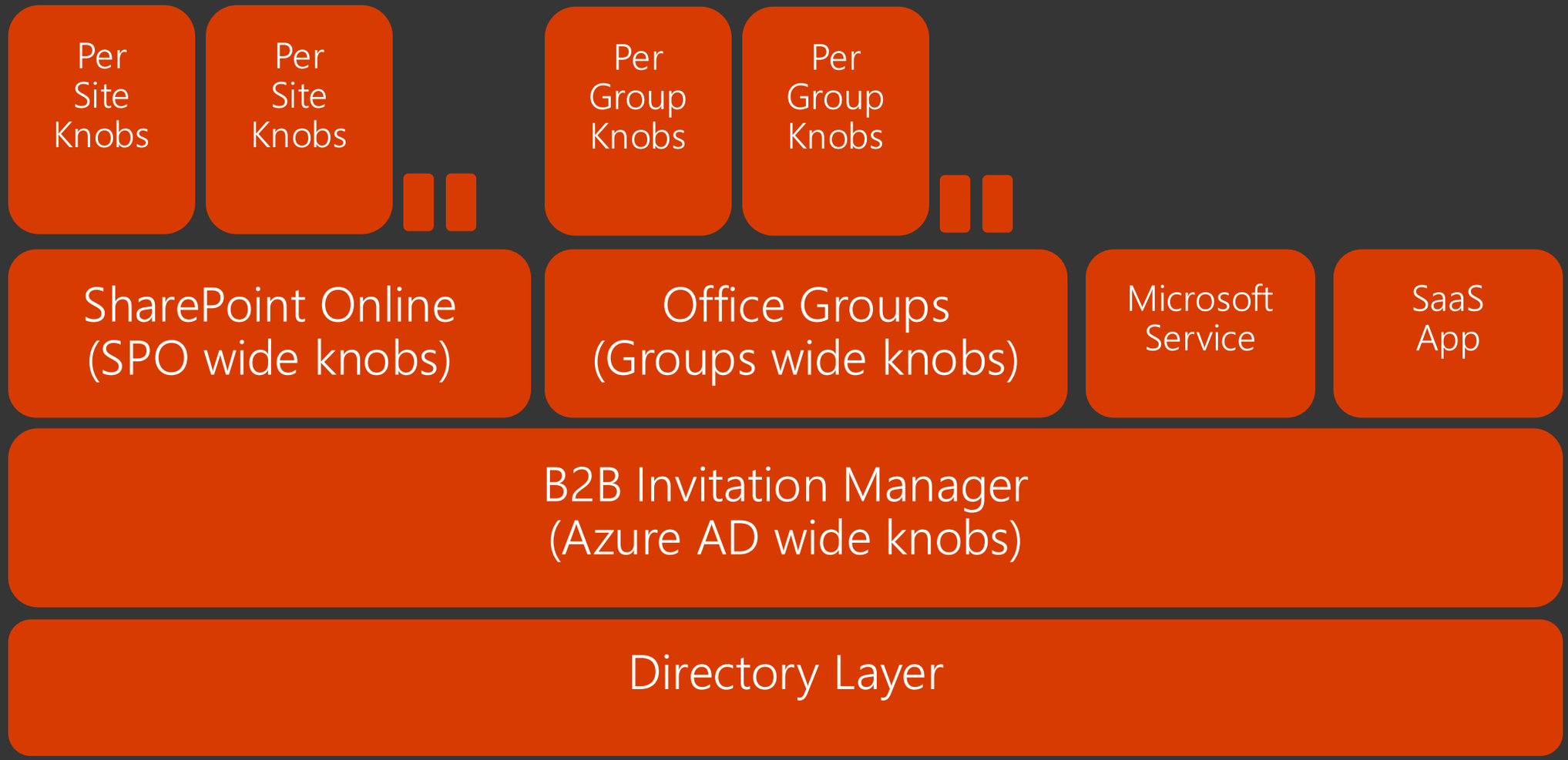
leadership:
y posture, not
convenience

External Collaboration Controls

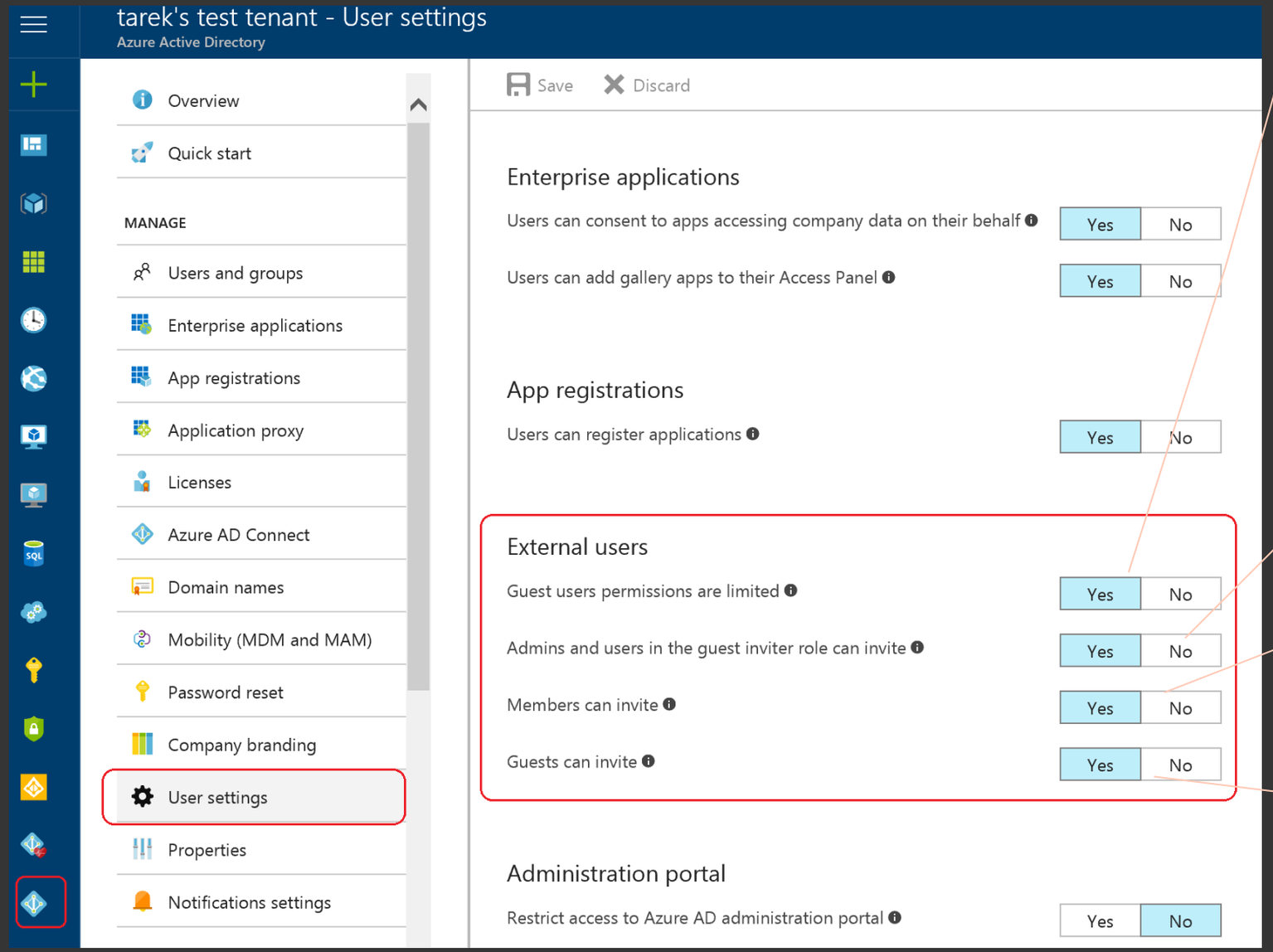
B2B Basics

- 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

B2B Control Layers



Azure AD B2B Controls



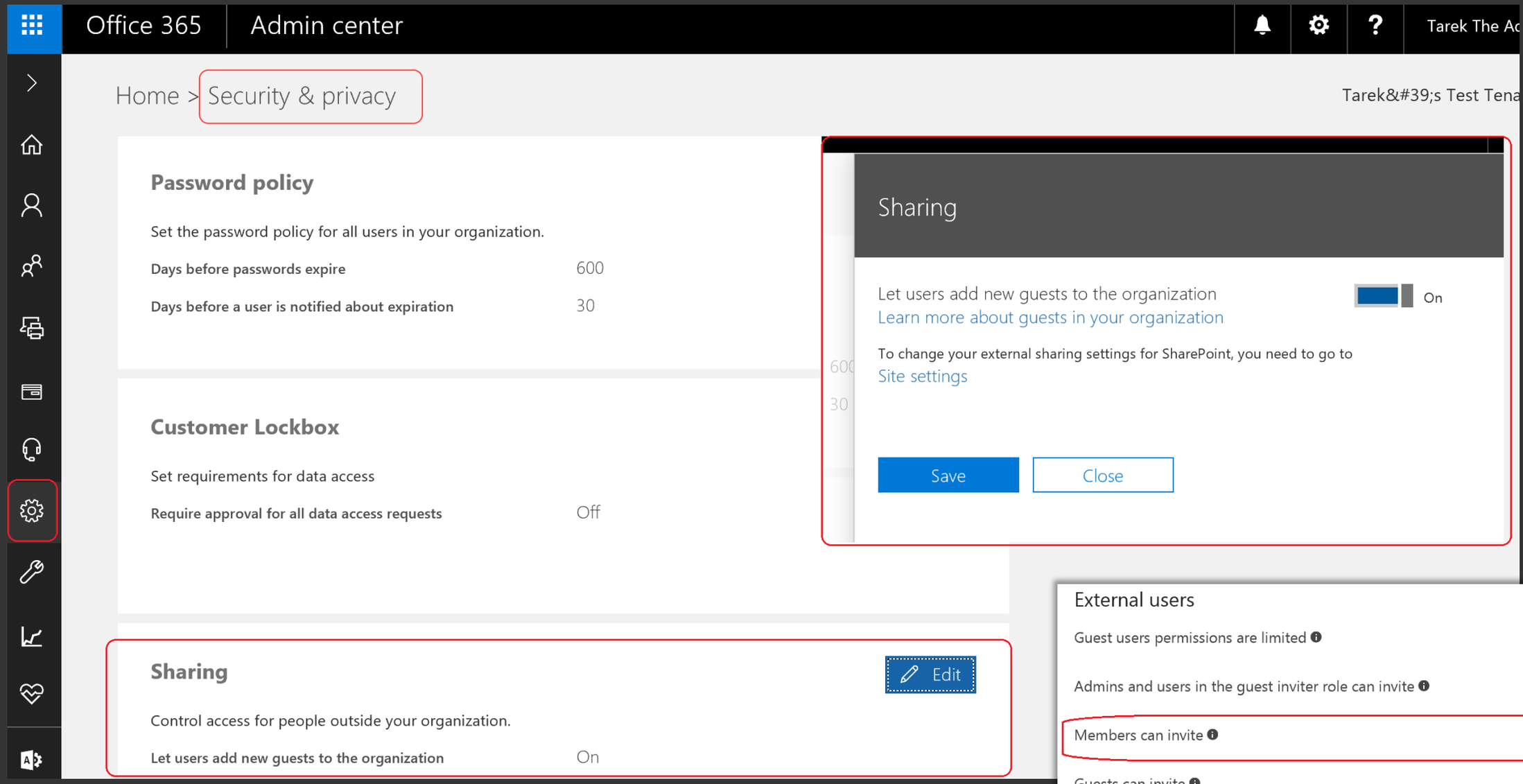
Good. Otherwise Guests have the same directory access as members.

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

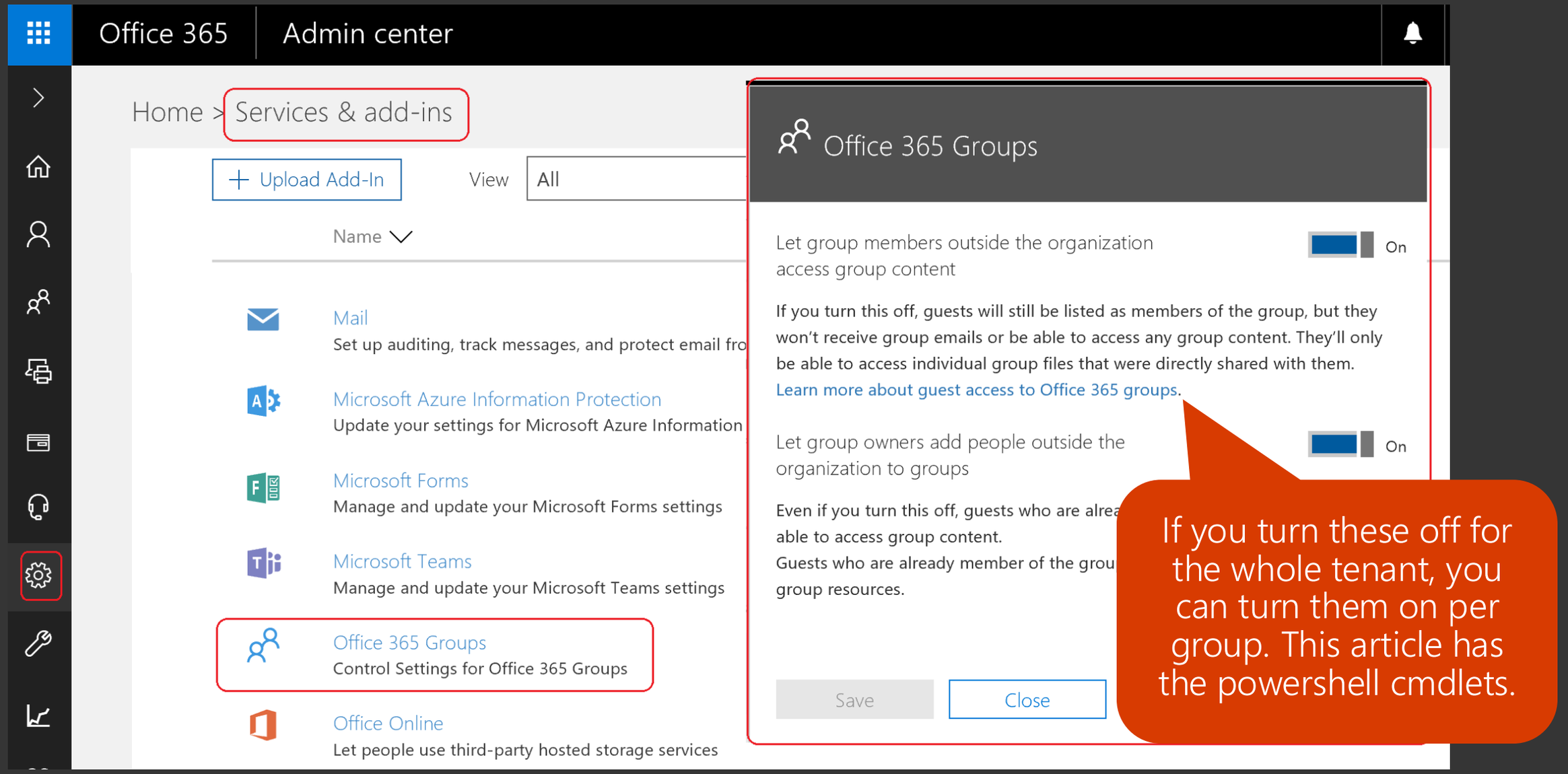
Good for customers focused on collaboration. Can be secure with Access Reviews and Audit logs

Questionable security wise unless combined with other controls.

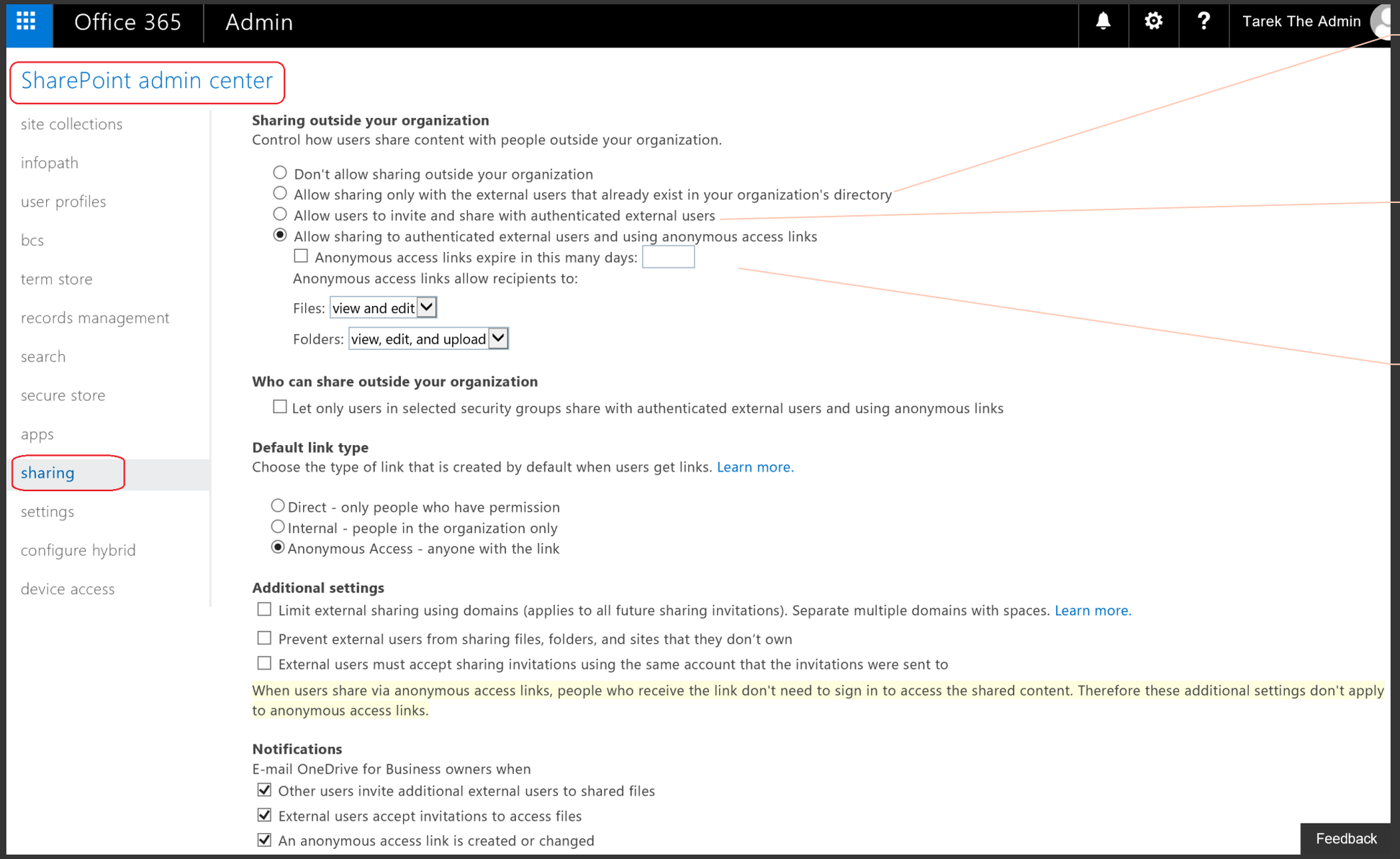
Office 365 Admin Portal B2B Controls



Office 365 Groups Controls



SharePoint Online B2B Controls



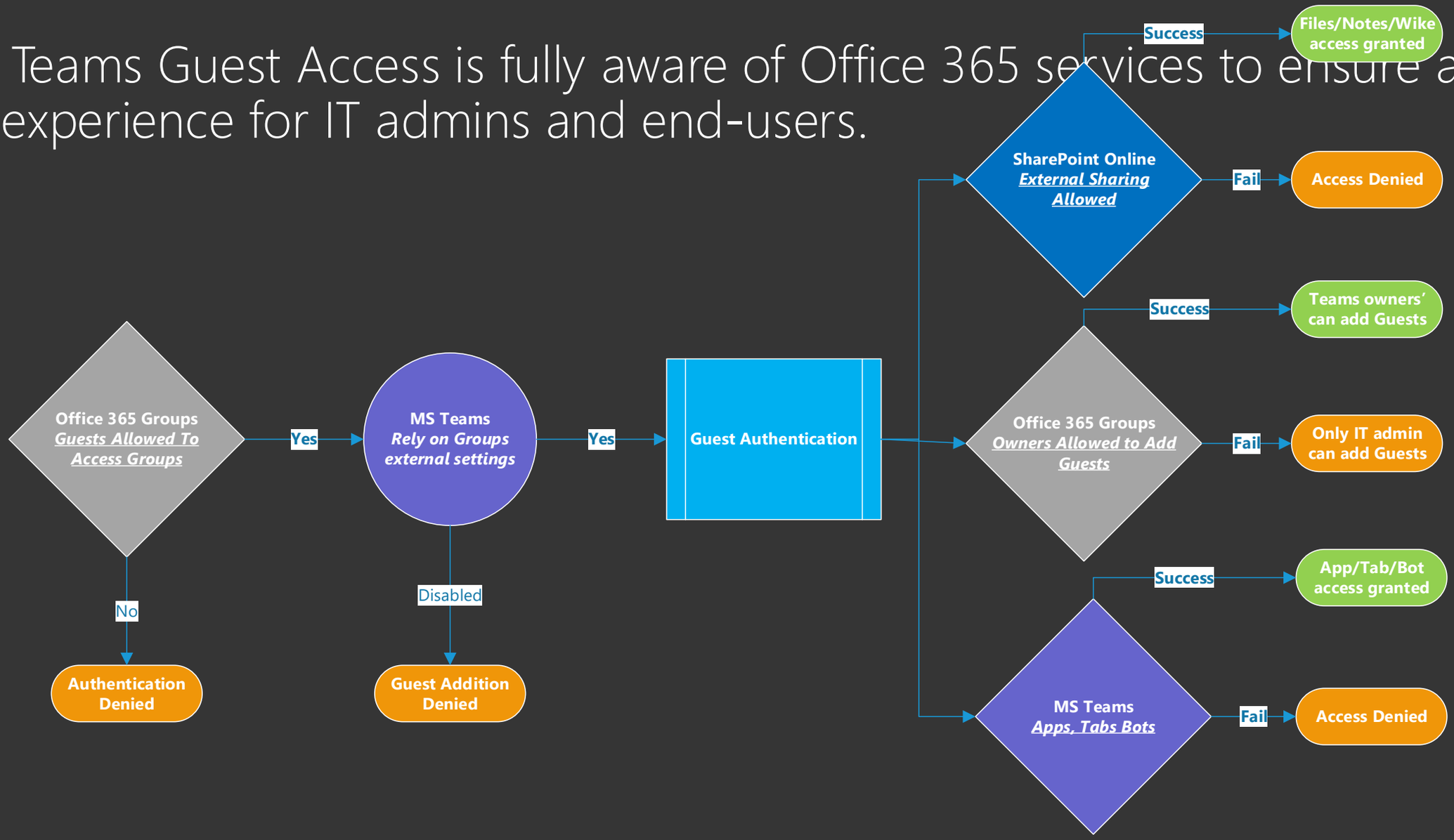
Good synergy with B2B invite solution

Good for highly collaborative customers

Golden Ticket Problem ;(

Teams B2B Controls with earlier Controls

Microsoft Teams Guest Access is fully aware of Office 365 services to ensure a coherent experience for IT admins and end-users.



Quick Wins

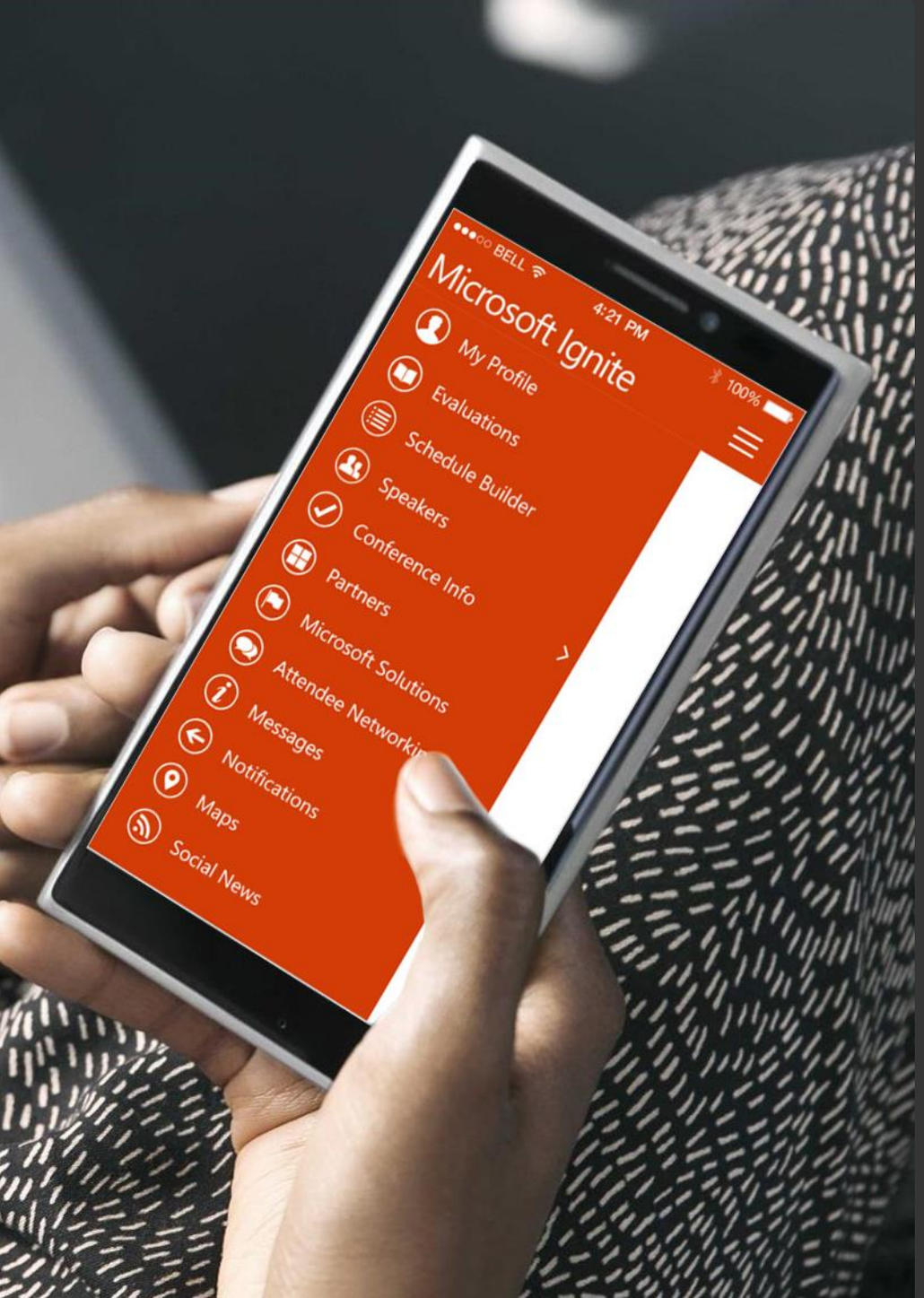
Homework! Go home and do this

- Tomorrow:
  - Turn on Password Hash Sync
    PHS White Paper:
    aka.ms/aadpwhs
  - Turn on MFA for your Admins 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

- Next Month:
  - Configure Conditional Access for SharePoint Online
  - Configure B2B policies for SharePoint Online
  - Read Secure Email Deployment Document and deploy it
    - aka.ms/m365securepolicy

Questions



Please evaluate this session

Your feedback is important to us!

From your PC or Tablet visit MyIgnite at
http://myignite.microsoft.com

From your phone download and use the Ignite Mobile App by scanning the QR code above or visiting
https://aka.ms/ignite.mobileapp

Identity @ Ignite | Monday

BRK3020	What's new and upcoming in AD FS to securely sign-in your users to Office 365 and other applications	OCCC W307	Monday 4:00–5:15	Sam Devasahayam

Identity @ Ignite | Tuesday

BRK2019	Productivity and protection for your employees, partners, and customers with Azure Active Directory	OCCC Valencia W415 AB	Tue 9:00–10:15	Alex Simons Nasos Kladakis
BRK2017	Saying goodbye to passwords	OCCC W240	Tue 12:45-1:30	Alex Simons
BRK1051	Locking down access to the Azure Cloud using SSO, Roles Based Access Control, and Conditional Access	OCCC Valencia W415 AB	Tue 2:15–3:30	Stuart Kwan

Identity @ Ignite | Wednesday

BRK3225	Office development: Authentication demystified	OCCC W315	Wed 10:45–12:00	Vittorio Bertocci
BRK3146	The power of common identity across any cloud	OCCC West Hall F3-4	Wed 12:45-1:30	Sam Devasahayam
THR2126	Azure Active Directory: Your options explained from AD sync to pass through authentication & more	MS Studio CE OCCC West MS Ignite Studios Theater	Wed 1:35-1:55	Alex Simons Simon May
BRK3352	Windows devices in Azure Active Directory: Why should I care?	OCCC S331	Wed 2:15–3:30	Jairo Cadena
BRK3040	Deliver management and security at scale to Office 365 with Azure Active Directory	Hyatt Plaza International H	Wed 3:15-4:00	Brjann Brekkan
BRK3295	What's new in Azure Active Directory Domain Services	Hyatt Plaza International I-K	Wed 4:00–5:15	Mahesh Unnikrishnan
BRK3016	Shut the door to cybercrime with Azure Active Directory risk-based identity protection	OCCC Chapin Theater W320	Wed 4:00–5:15	Alex Weinert Nitika Gupta
BRK3216	How Graph powers intelligent experiences in SharePoint and Office 365	OCCC W206	Wed 4:00–5:15	CJ Tan Torbjørn Helvik

Identity @ Ignite | Thursday

BRK2018	Share corporate resources with your partners using Azure Active Directory B2B collaboration	OCCC W208 AB	Thu 9:00–10:15	Mary Lynch Sarat Subramaniam Laith Al Shamri
BRK3207	The keys to the cloud: Use Microsoft identities to sign in and access API from your mobile+web apps	OCCC S310	Thu 10:45-12:00	Vittorio Bertocci
BRK3012	Secure access to Office 365, SaaS and on-premises apps with Microsoft Enterprise Mobility + Security	OCCC Valencia W415 AB	Thu 10:45-12:00	Caleb Baker Chris Green
BRK3013	Ensure users have the right access with Azure Active Directory	OCCC Valencia W415 AB	Thu 12:30–1:45	Joseph Dadzie Mark Wahl
BRK2079	Secure Windows 10 with Intune, Azure AD and System Center Configuration Manager	OCCC West Hall B4	Thu 12:30–1:45	Dune Desormeaux Dilip Radhakrishnan
BRK3340	Use Microsoft Graph to reach on-premises users of Exchange 2016 deployments	OCCC W208 AB	Thu 12:30–1:45	Deepak Singh
BRK3015	Deep-dive: Azure Active Directory Authentication and Single-Sign-On	OCCC W414	Thu 2:15-3:30	John Craddock
BRK2078	Microsoft's guide for going password-less	OCCC W207 AB	Thu 2:15-3:30	Karanbir Singh
BRK3014	Azure Active Directory best practices from around the world	OCCC Valencia W415 AB	Thu 4:00–5:15	Tarek Dawoud Mark Morowczynski
BRK4011	Understanding hybrid identity, authentication, and authorization with Microsoft Azure Stack	OCCC West Hall F1	Thu 4:00–5:15	Shriram Natarajan
BRK3053	Troubleshooting Office 365 identity: How modern authentication works and what to do when it doesn't	OCCC W300	Thu 4:00–5:15	Jonas Gunnemo

Identity @ Ignite | Friday

BRK2276	Modernize your customer identity management with Azure Active Directory B2C	OCCC West Hall F3-4	Friday 9:00-9:45	Saeed Akhter

References

Azure AD Conditional Access Overview

Go here

Supported Apps for Conditional Access

Go here

Azure AD Identity Protection & Privileged Identity Protection:

Go here

SSPR

Go here

SaaS

Go here

B2B References:

Go here

Video: https://aka.ms/b2bmechanics

Appendix Slides

Setting Up Your Tenant

Set Up Do's and Don't's

Do: Setup Branding

Do: Verify your Domain before Sync (Viral takeover)

Do: Setup Technical Notification Email to a DL

Do: Simplify Licensing

- All users group
- Dynamic groups
- On premises groups

Do & Re-Do: Network Pre-Reqs

Don't: Name your tenant: jimscoolthing.onmicrosoft.com

Don't: Forget about Company level permissions for users

Get-MSOLCompanyInformation

```
AllowAdHocSubscriptions                 : True
AllowEmailVerifiedUsers                 : True
UsersPermissionToCreateLOBAppsEnabled   : True
UsersPermissionToReadOtherUsersEnabled  : True
UsersPermissionToUserConsentToAppEnabled : True
```

Set-MSOLCompanySettings