



MOVING OFF AD FS

TONY MORROW

BELLARMINE UNIVERSITY

PRINCIPAL SOLUTIONS ARCHITECT

KEVIN OPPIHLE

MIRAZON

SYSTEMS ENGINEER

TOPICS

- AD FS – What it is, and why you have it
 - Do you still have it, but don't know?
- Why you should move off AD FS
- License requirements
- How to move off AD FS
- MFA and what to expect when migrating to Azure MFA
- Live Demo

WHO AM I (TONY)?

- Tony Morrow
 - [@atgizmo](#)
 - @agizmo@mindly.social
 - <https://lookanotherblog.com>
- Principal Solutions Architect @ Bellarmine University
- 13 years working at Bellarmine
- Focus
 - Networking
 - Wireless
 - Servers/Virtualization
 - Systems Integration
 - Problem Solving
 - PowerShell, PowerShell, PowerShell

DISCLAIMER 😊

- I am not a Microsoft MVP or Partner
- All technologies showcased are using free, trial, or paid licenses
- All the opinions here are my own
- ~~Nobody is paying me for this presentation~~

WHO AM I (KEVIN)?

- Kevin Oppihle
 - Kevin.Oppihle@Mirazon.com
 - <https://koppihle3.blogspot.com>
 - <https://www.mirazon.com/blog/>
- Systems Engineer @ Mirazon
- 14.9 years working at Mirazon
- Focus
 - SMB Specialist
 - Office 365/Azure AD Migrations and Administration
 - Servers/Virtualization
 - Corporate Domain Divestitures/Acquisitions/Migrations
 - Solution Provider



DISCLAIMER 😊

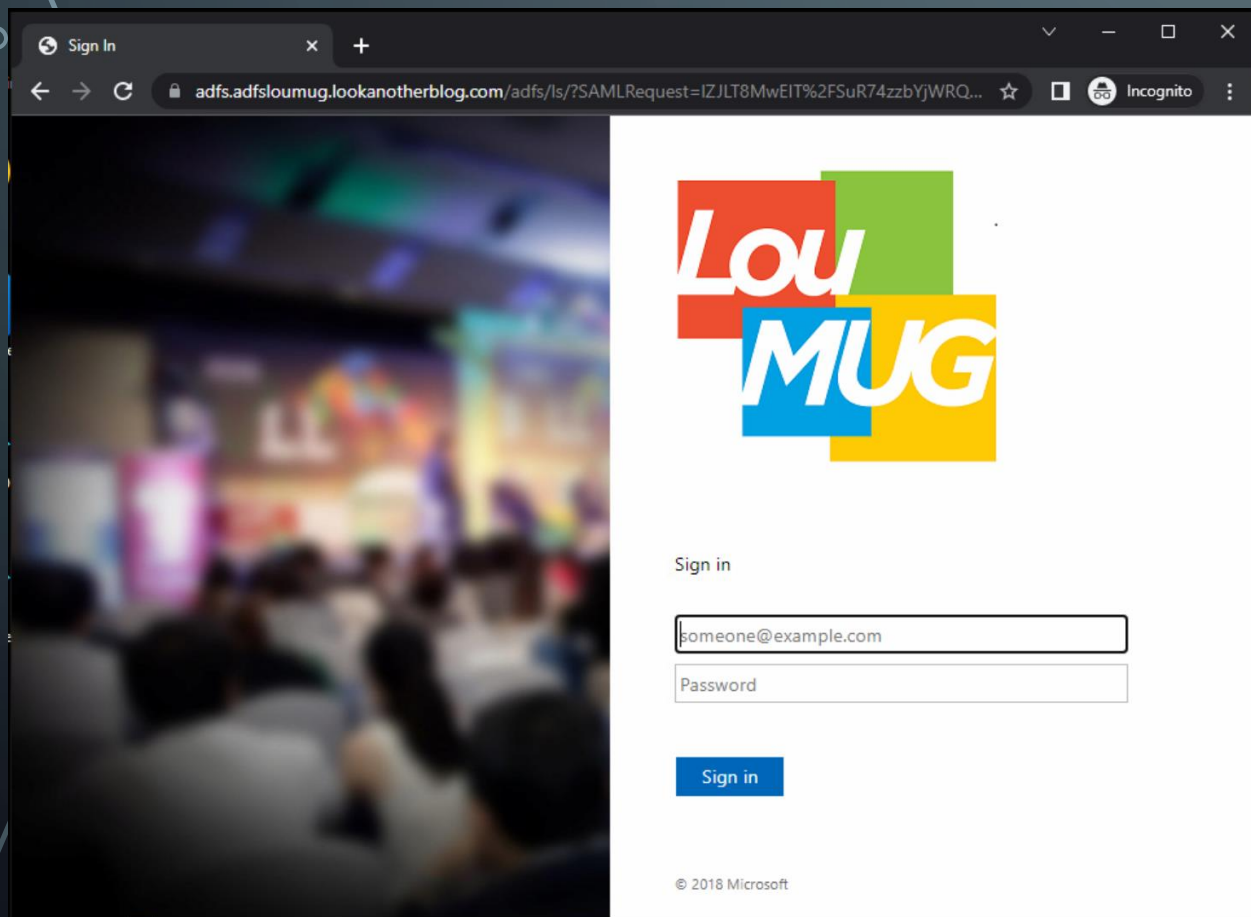
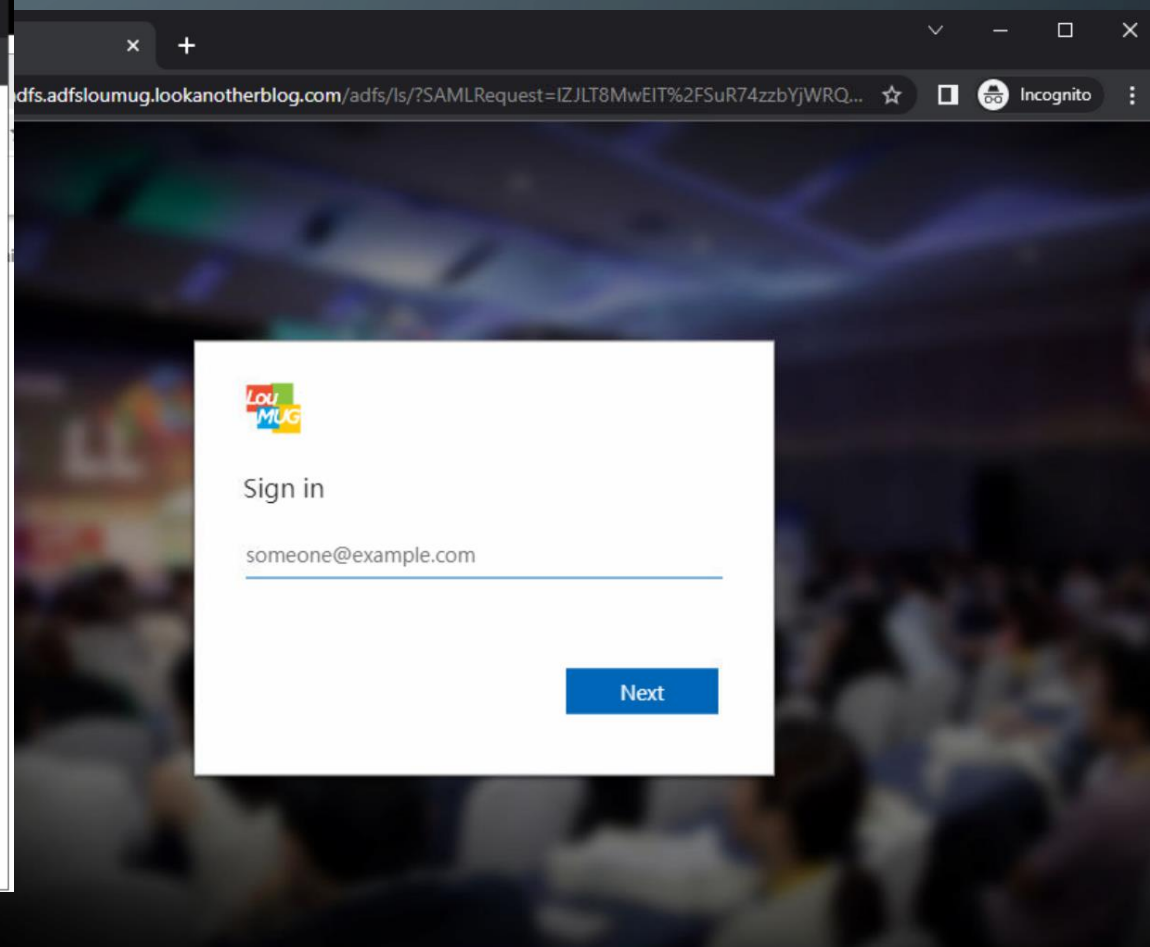
- I am Microsoft Certified and work for a Microsoft Partner
- All technologies showcased are using free, trial, or paid licenses
- All the opinions here are my own
- I am being paid for this presentation in food



WHAT IS AD FS? WHY DO I HAVE THIS?

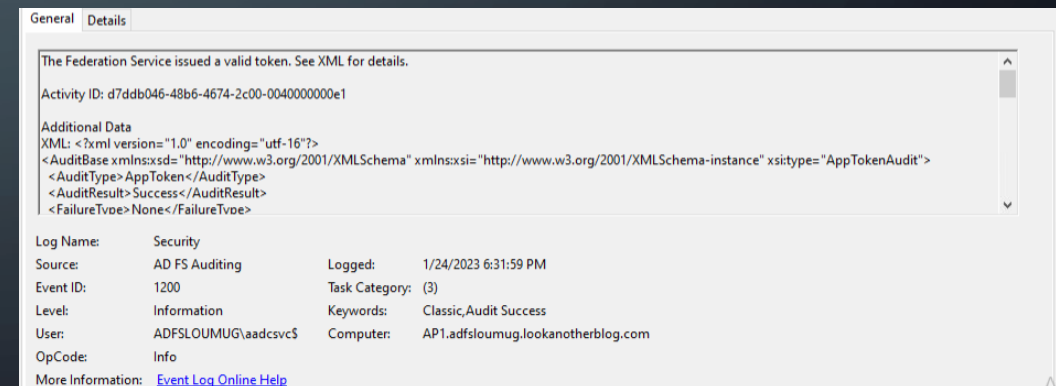
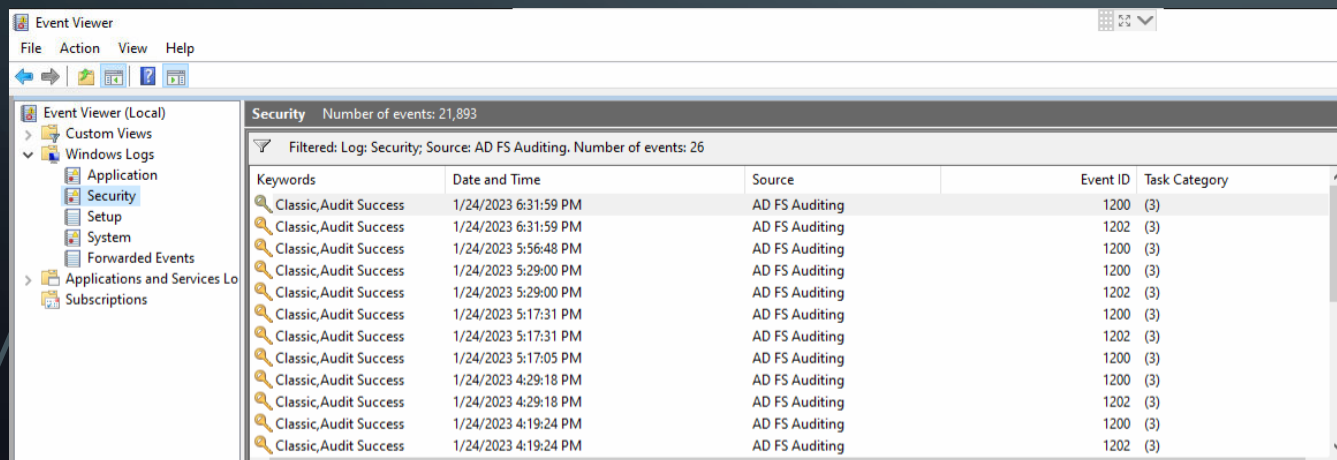
- AD FS = Active Directory Federation Services
- Offers a method of modern claims-based authentication using AD
 - No more requiring direct LDAP communication between applications and AD
 - No more opening your AD/LDAP server up to the Internet
 - You can control what information is shared to an application during authentication
 - Supports SAML 2 based authentication
- It was Microsoft's best practice authentication method for hybrid O365 tenants for a long time.

DO YOU HAVE AD FS?

A screenshot of a web browser window. The address bar shows a URL starting with 'adfs.adfsloumug.lookanootherblog.com'. The page content includes the 'Lou MUG' logo at the top, followed by the text 'Sign in'. Below this are two input fields: the first contains 'someone@example.com' and the second is labeled 'Password'. A blue 'Sign in' button is positioned below the fields. At the bottom of the page, there is a copyright notice: '© 2018 Microsoft'.A screenshot of a web browser window showing a modal dialog box. The dialog has the 'Lou MUG' logo in the top left corner, followed by the text 'Sign in'. Below this is an input field containing 'someone@example.com'. A blue 'Next' button is located at the bottom right of the dialog. The background of the browser window is blurred, showing a crowd of people.

HOW TO KNOW WHO'S LOGGING IN?

- Enable AD FS Verbose logging
 - <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#enable-auditing-for-ad-fs>
- Look for AD FS Auditing in Windows Security logs

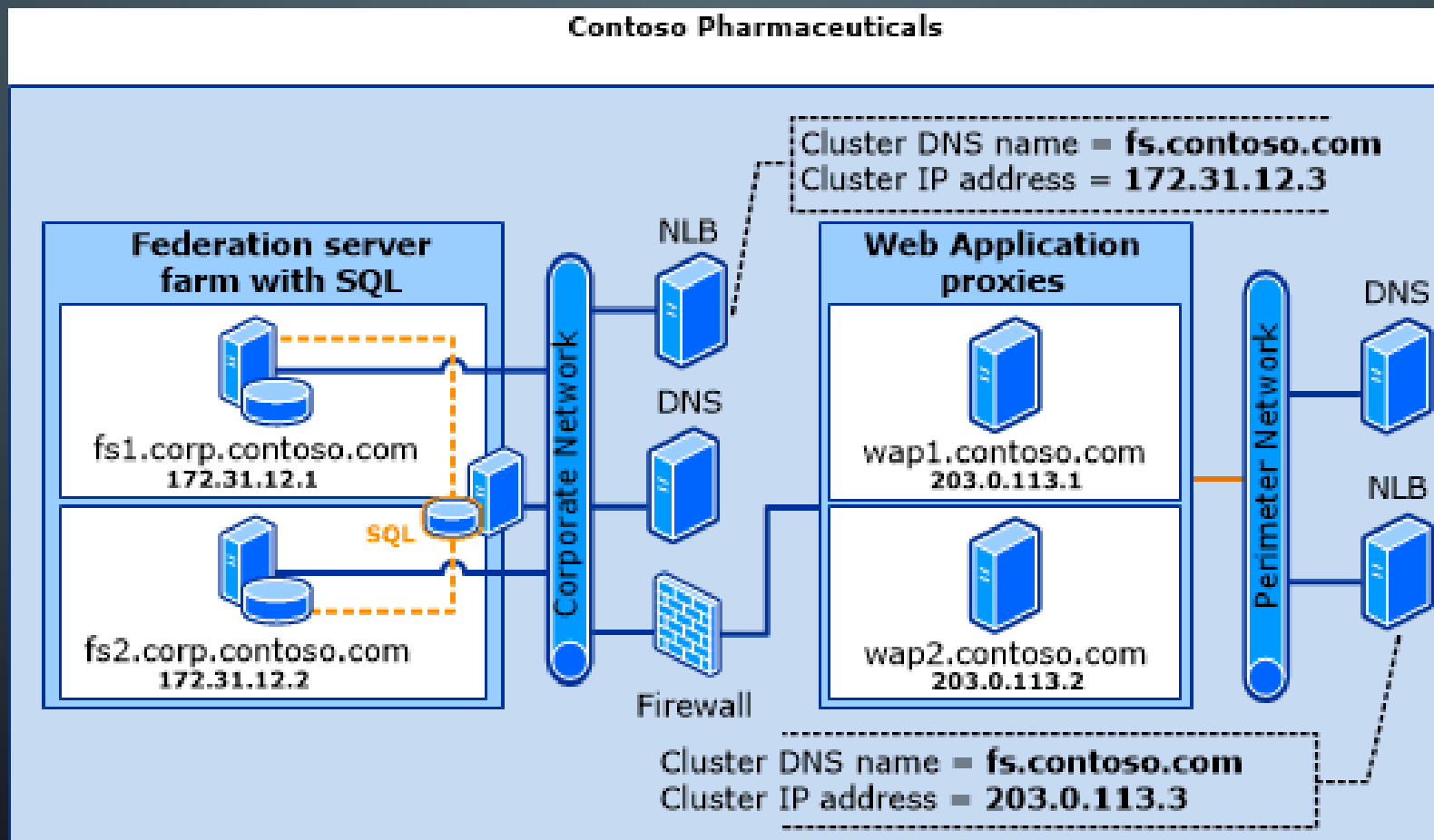




WHY MOVE FROM AD FS?

- Security best practices has changed
- AD FS requires a lot of infrastructure
 - 5 Windows servers for minimum production environment
 - (6 if you like doing SQL redundancy)
- AD FS needs Active Directory connectivity
 - On Premise ISP or authentication service failures can impact access to external cloud services
- AD FS has less flexibility for MFA compared to alternative solutions
- AD FS uses a single signing certificate for entire environment
 - Every app needs to be updated at the same time when the certificate expires
- Some migration options
 - Azure AD
 - Okta

AD FS SQL DEPLOYMENT





AZURE AD BASED AUTHENTICATION

- SAML 2 based authentication built-in
- Hundreds of pre-made templates for configuring SSO
 - <https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/tutorial-list>
 - Or add any application you can configure yourself
- Licensing
 - Included with Azure AD (aka your O365/M365 user licenses)

AZURE USER LICENSING

Azure AD Premium required for Conditional Access

	AAD Free/AAD Office 365	AAD Premium P1	AAD Premium P2
Basic user and group management (inc MFA)	X	X	X
Conditional Access		X	X
Advanced group management		X	X
Password protection		X	X
Self-service password reset (Cloud User)	X	X	X
Self-service password reset (On-Premise User)		X	X
Microsoft Defender for Cloud Apps		X	X
AAD Application Proxy		X	X
Microsoft Identity Manager		X	X
Azure AD Connect	X	X	X
Azure AD Connect Health Monitoring		X	X
Terms of use attestation		X	X
SLA		X	X
Access reviews			X
Privileged Identity Management (PIM)			X
Identity Protection			X

- O365 E1: \$10.00/user/month
- O365 E3: \$23.00/user/month
- O365 E5: \$38.00/user/month

AND

- Azure AD P1: \$6.00/user/month
- Azure AD P2: \$9.00/user/month

OR

- EMS E3: \$10.60/user/month
- EMS E5: \$16.40/user/month

OR JUST GET

- M365 E3: \$36.00/user/month
- M365 E5: \$57.00/user/month
- M365 Business Premium: \$22.00/user/month

O365/M365 LICENSING



Information Worker Plans									Frontline Worker Plans					
Microsoft 365				Office 365			Enterprise Mobility + Security		Microsoft 365				Office 365	
E3	E5	E5 Security ¹	E5 Compliance ¹	E1	E3	E5	E3	E5	F1	F3	F5 Security ²	F5 Compliance ²	F5 Sec+Comp ²	F3

¹ Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

² Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).

Identity and access management

Azure Active Directory Premium Plan 1	•							•		•	•			
Azure Active Directory Premium Plan 2		•	•						•			•		•
User Provisioning	•	•	•	•	•	•	•	•	•	•	•			•
Cloud user self-service password change	•	•	•	•	•	•	•	•	•	•	•			•
Cloud user self-service password reset	•	•	•				•	•	•	•	•			•
Hybrid user self-service password change/reset with on-premises write-back	•	•	•				•	•	•	•	•			•
Advanced Security Reports	•	•	•				•	•	•	•	•			•
Multi Factor Authentication	•	•	•	•	•	•	•	•	•	•	•			•
Conditional Access	•	•	•				•	•	•	•	•			•



MOVE TO AZURE AD

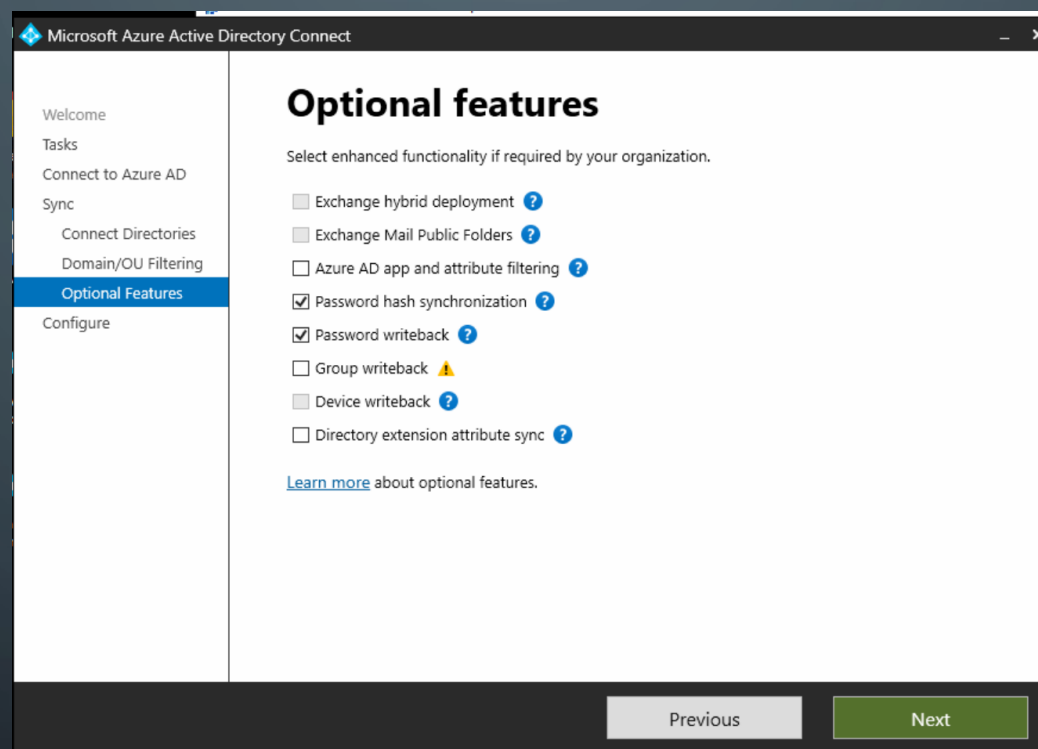
1. Enable Password hash synchronization in Azure AD Connect
 1. (Optional) Enable Password writeback to support SSPR
2. Change user sign-in method to Password Hash Synchronization in Azure AD Connect

Important Docs:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/migrate-from-federation-to-cloud-authentication>

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-staged-rollout>

ENABLE PASSWORD HASH SYNC



Microsoft Azure Active Directory Connect

Optional features

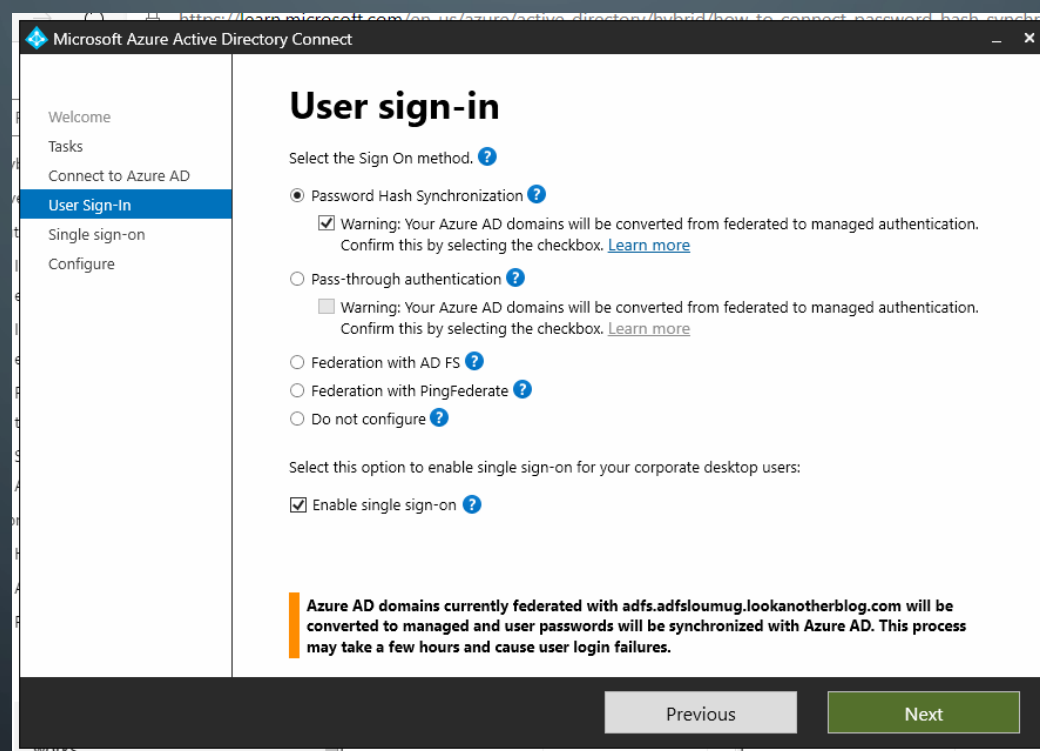
Select enhanced functionality if required by your organization.

- Exchange hybrid deployment ?
- Exchange Mail Public Folders ?
- Azure AD app and attribute filtering ?
- Password hash synchronization ?
- Password writeback ?
- Group writeback ⚠
- Device writeback ?
- Directory extension attribute sync ?

[Learn more](#) about optional features.

Previous Next

CHANGING AZURE AD AUTHENTICATION



Microsoft Azure Active Directory Connect

Welcome
Tasks
Connect to Azure AD
User Sign-In
Single sign-on
Configure

User sign-in

Select the Sign On method. ?

- Password Hash Synchronization ?
 - Warning: Your Azure AD domains will be converted from federated to managed authentication. Confirm this by selecting the checkbox. [Learn more](#)
- Pass-through authentication ?
 - Warning: Your Azure AD domains will be converted from federated to managed authentication. Confirm this by selecting the checkbox. [Learn more](#)
- Federation with AD FS ?
- Federation with PingFederate ?
- Do not configure ?

Select this option to enable single sign-on for your corporate desktop users:

- Enable single sign-on ?

Azure AD domains currently federated with adfs.adfsloumug.lookanotherblog.com will be converted to managed and user passwords will be synchronized with Azure AD. This process may take a few hours and cause user login failures.

Previous Next

MIGRATION COMPLETE

- Comments?
- Questions?

The text 'The End' is written in a white, elegant cursive script. It is centered within a series of three overlapping, dark gray circles that create a tunnel-like effect, receding into the distance. The background of the entire slide is a dark blue-gray color with faint white circuit-like patterns in the corners.

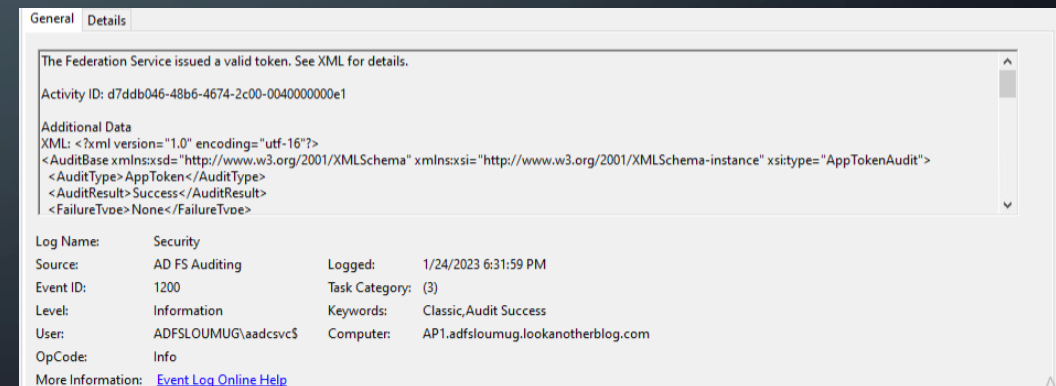
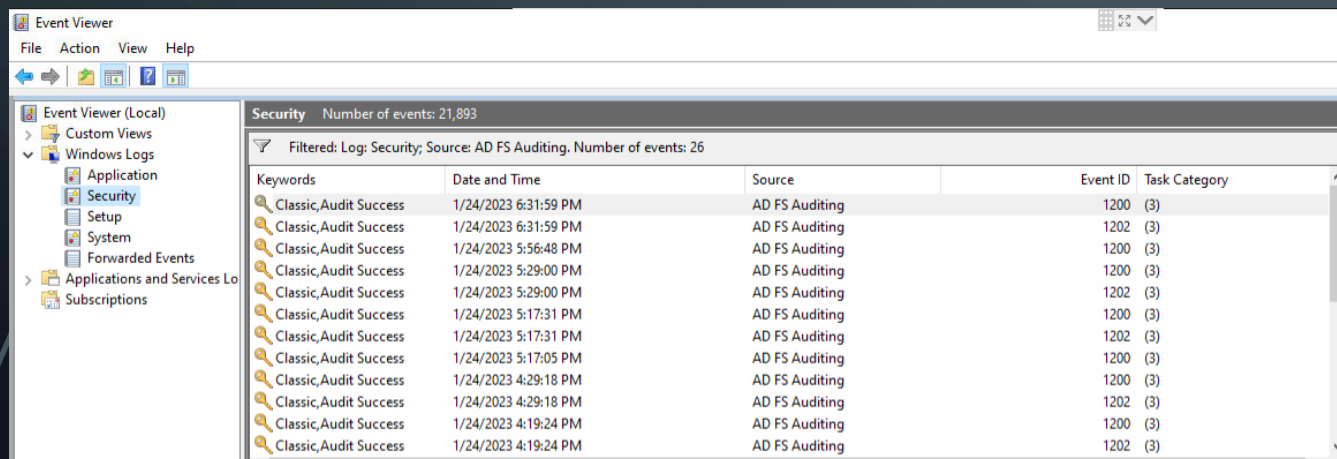
The End

MOVE TO AZURE AD (CONTINUED)

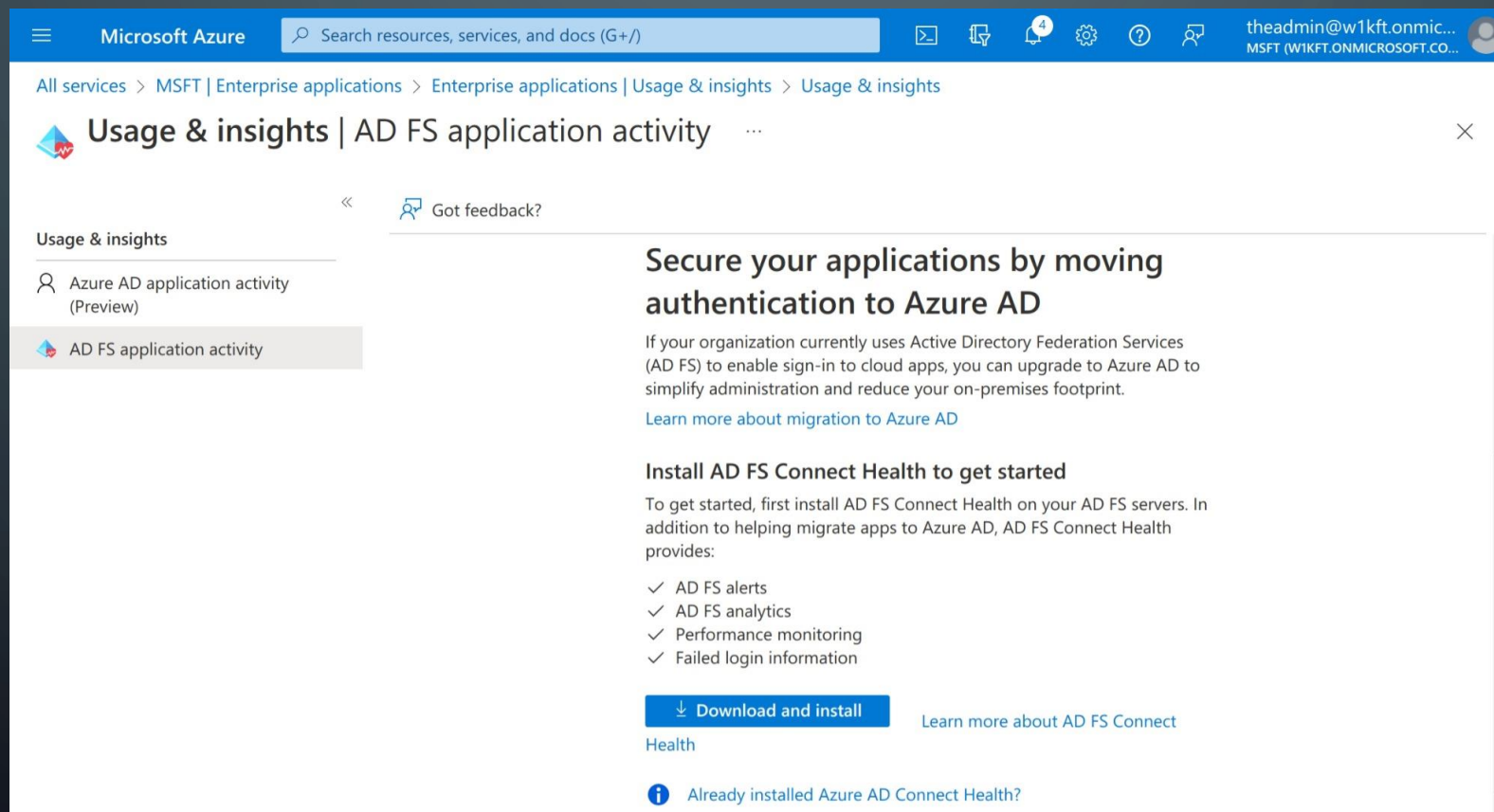
1. Audit your AD FS logins and see what RelyingParty's are used
 1. (Optional) Install Azure AD Connect Health AD FS Agent
 2. Use the reports to find/fix issues with moving applications
2. Create new Enterprise Application for each application using AD FS
 1. Import metadata or enter SAML configuration
 2. Configure attributes & claims to release to application
 3. Add monitoring email address for SAML signing certificate alerts
3. Update application to use Azure AD
 1. Import Azure AD info using metadata URL, metadata XML, or manually

HOW TO KNOW WHO'S LOGGING IN?

- Enable AD FS Verbose logging
 - <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install#enable-auditing-for-ad-fs>
- Look for AD FS Auditing in Windows Security logs



AD FS LOGGING TO AZURE AD



Microsoft Azure Search resources, services, and docs (G+/)

theadmin@w1kft.onmic... MSFT (WIKFT.ONMICROSOFT.CO...)

All services > MSFT | Enterprise applications > Enterprise applications | Usage & insights > Usage & insights

Usage & insights | AD FS application activity

Usage & insights

- Azure AD application activity (Preview)
- AD FS application activity

Got feedback?

Secure your applications by moving authentication to Azure AD

If your organization currently uses Active Directory Federation Services (AD FS) to enable sign-in to cloud apps, you can upgrade to Azure AD to simplify administration and reduce your on-premises footprint.

[Learn more about migration to Azure AD](#)

Install AD FS Connect Health to get started

To get started, first install AD FS Connect Health on your AD FS servers. In addition to helping migrate apps to Azure AD, AD FS Connect Health provides:

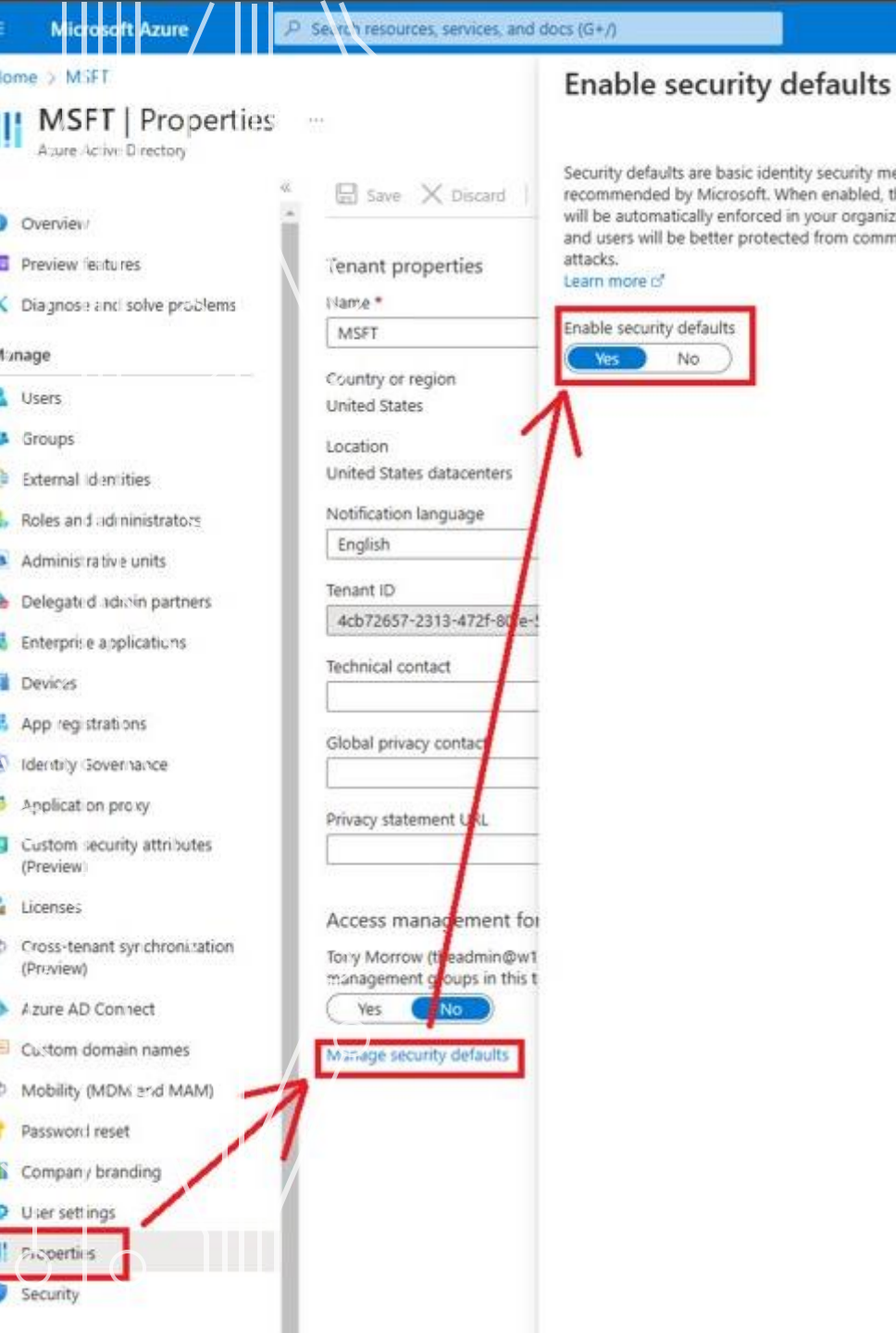
- ✓ AD FS alerts
- ✓ AD FS analytics
- ✓ Performance monitoring
- ✓ Failed login information

[Download and install](#) [Learn more about AD FS Connect Health](#)

Already installed Azure AD Connect Health?

MFA & CONDITIONAL ACCESS

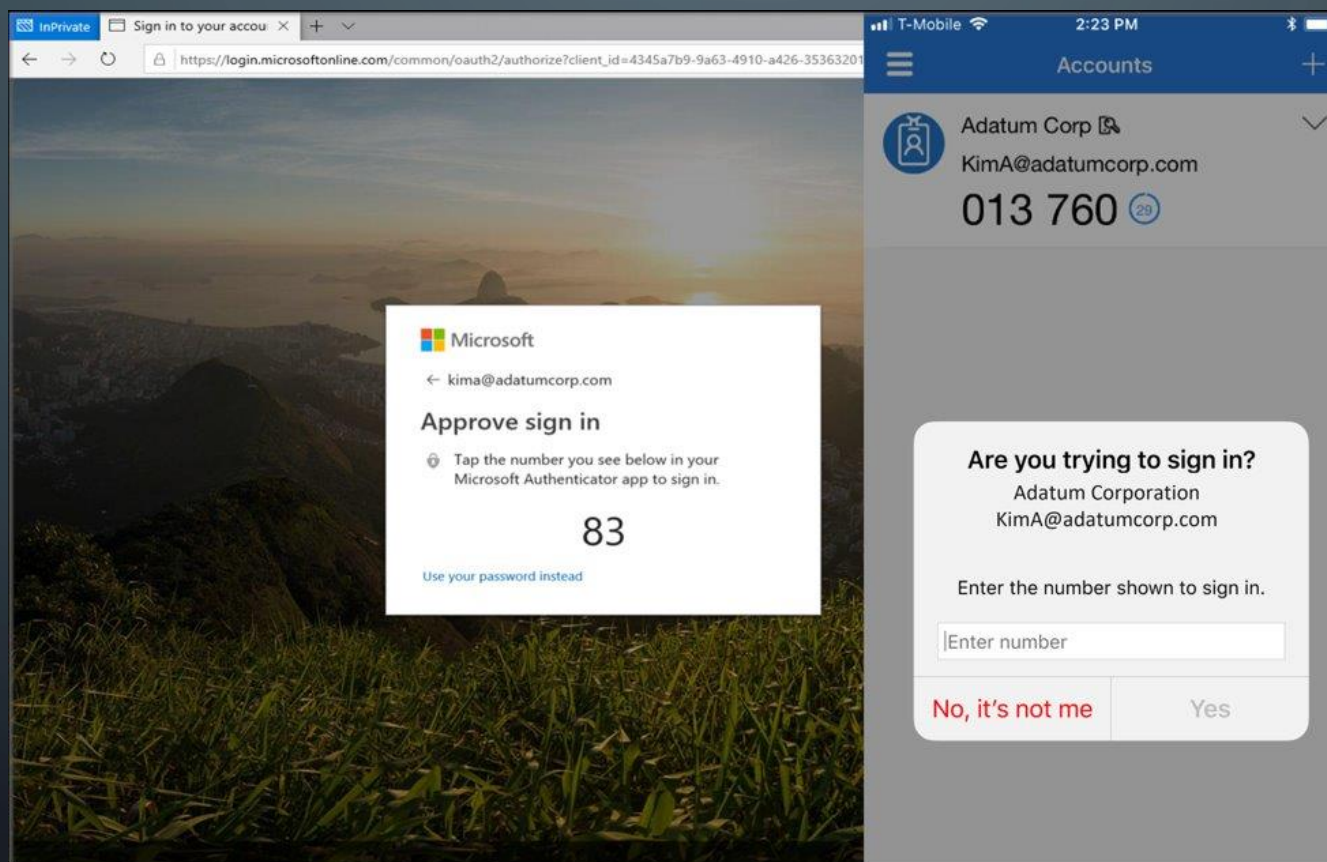
- Multifactor Authentication
 - Included with your O365/M365 licenses
 - Supports OTP, Push, FIDO2, SMS, etc
 - All or nothing approach (<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#enabling-security-defaults>)
- Conditional Access
 - Allows granular MFA control on a per application basis
 - Requires Azure AD Premium licensing for users
 - Available as an add-on license or part of M365 subscriptions
- Where is MFA!?
 - <https://www.mirazon.com/who-moved-my-microsoft-mfa/>



AZURE AD SECURITY DEFAULTS

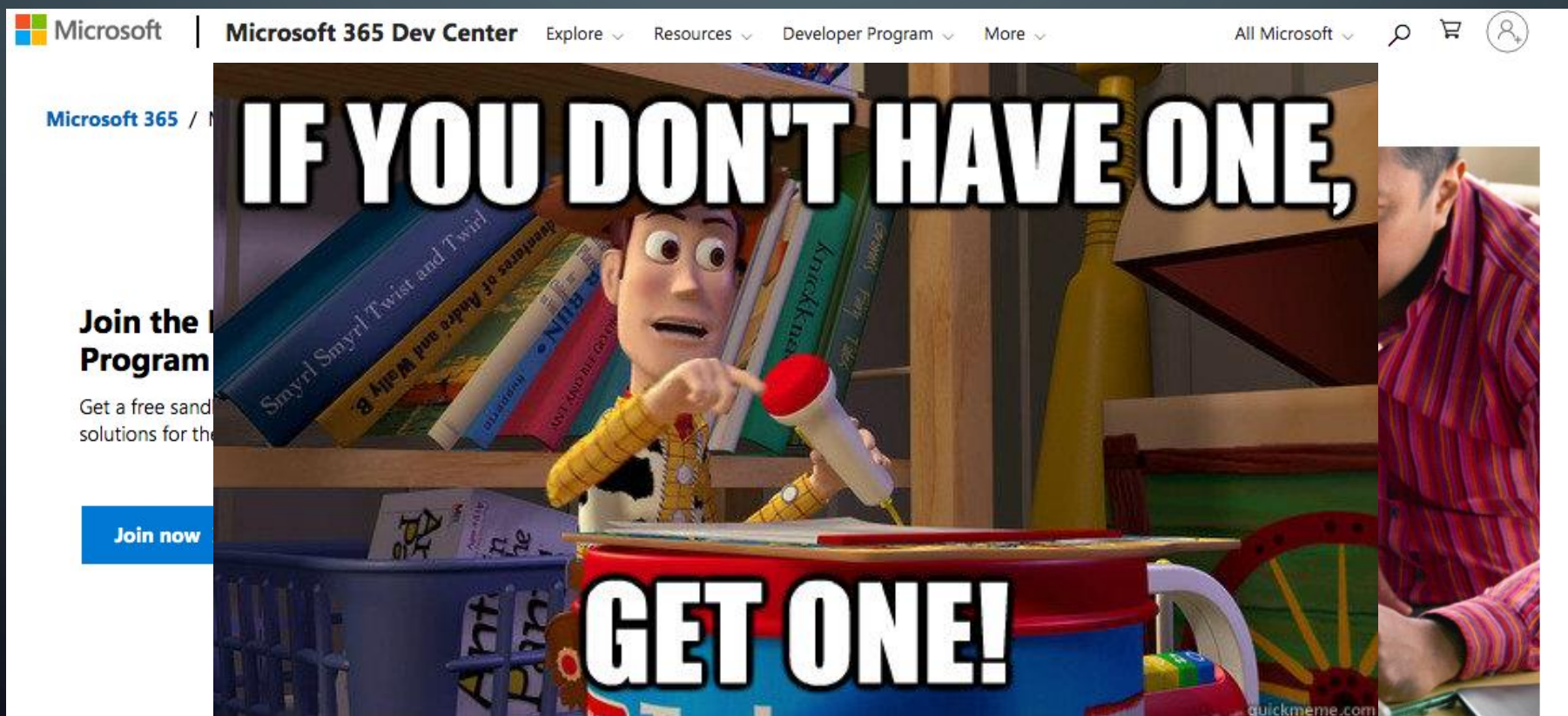
- This will enable MFA for **ALL** users in your tenant

MFA CODE MATCHING



(TANGENT) GET A DEVELOPMENT ENVIRONMENT

- <https://developer.microsoft.com/en-us/microsoft-365/dev-program>



DEMO





THANKS! Q&A

TONY MORROW

[@atgizmo](#)

[@agizmo@mindly.social](#)

<https://lookanotherblog.com>

KEVIN OPPIHLE

Kevin.Oppihle@Mirazon.com

<https://koppihle3.blogspot.com>

<https://www.mirazon.com/blog/>

