


## Success strategies for your strong authentication journey

Inbar Cizer Kobrinsky  @inbarck

Mark Morowczynski  @markmorow

Program Managers  
Azure Active Directory - Microsoft



Sponsored by:

Google

 Microsoft

yubico

[authenticatecon.com](https://authenticatecon.com)

# Agenda

The “new normal” of working from home

**Key decisions** in a strong authentication deployment

Strong authentication **deployment tips**

Day to day **tricks** in managing strong authentication

Go do's



# Digital transformation roadmap





# Digital transformation roadmap

“ We just completed more than 2 years of digital transformation in 2 months. ”

Scope requirements  
for Work-from-  
Anywhere  
transformation  
initiative

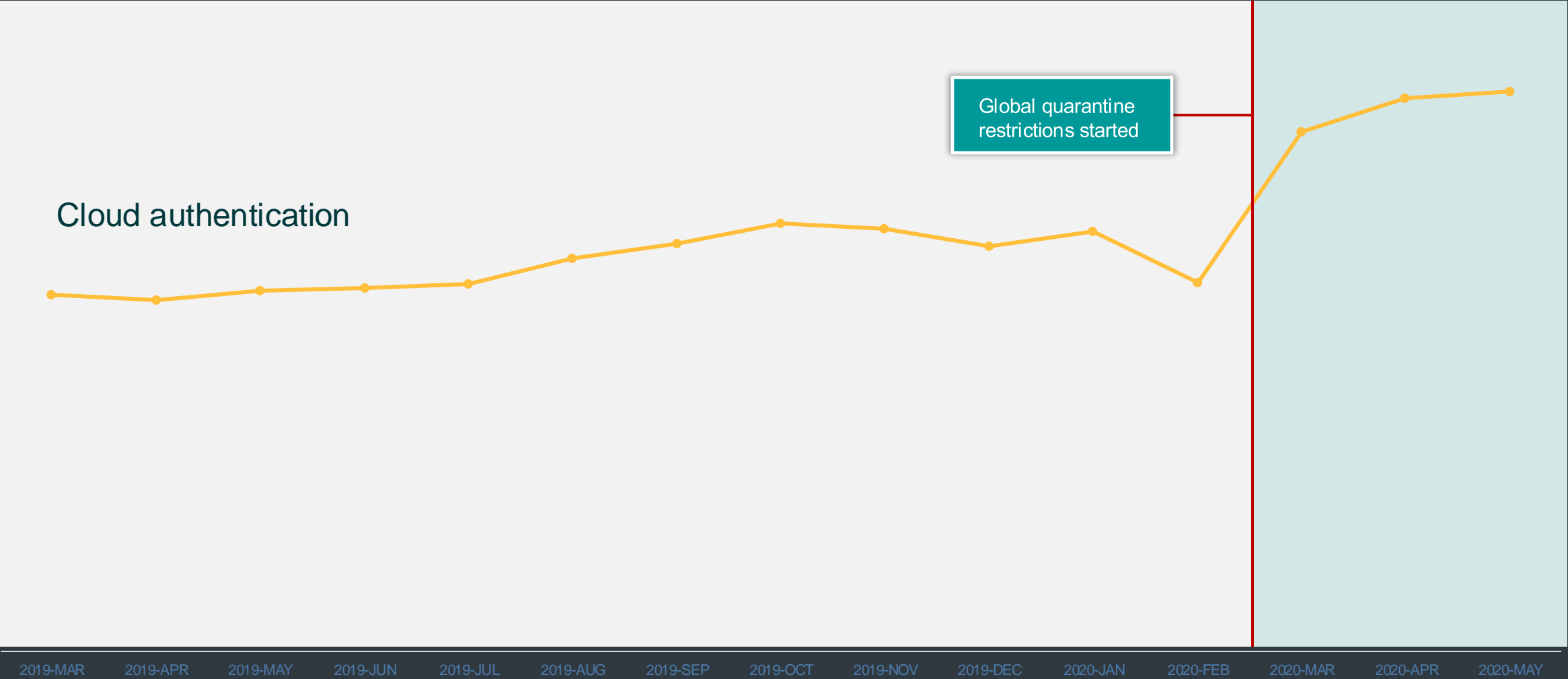
Complete  
Work-from-  
Anywhere rollout

Jan 1, 2020

Apr 1, 2020

Jun 1, 2022

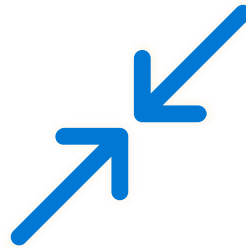
# Accelerated shift to Azure AD cloud authentication



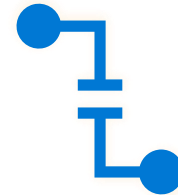
# Principles for Zero Trust



Verify explicitly



Use least privilege  
access



Assume breach

The “new normal” of working from home

## **Key decisions in a strong authentication deployment**

Strong authentication deployment tips

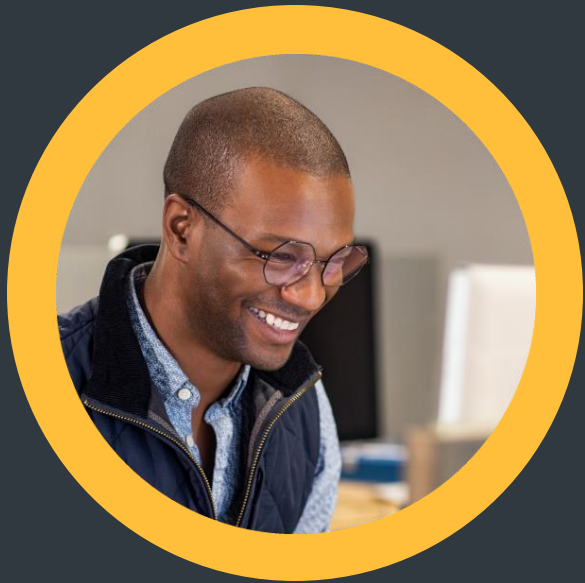
Day to day tricks in managing strong authentication

Go do's

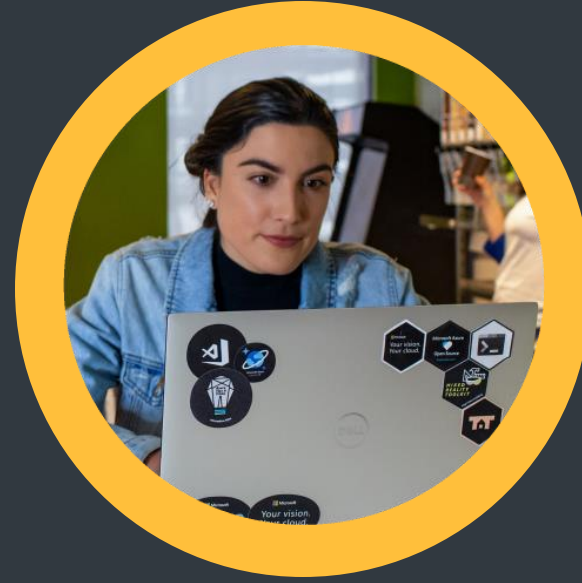


# Key decisions in a strong authentication deployment

Balance between security and usability



THE SECURITY FOLKS:  
FREQUENT MFA PROMPTS WILL  
INCREASE THE SECURITY OF MY  
ORGANIZATION



THE BUSINESS FOLKS:  
ENABLING MFA ON MY USERS WILL  
CAUSE BAD END USER  
EXPERIENCE



# Key decision #1: Authentication frequency

More Prompts != More Security

Need to strike the correct balance between usability and security

Trains end users to give up their credentials for phishing attacks

Frequent MFA prompting can lead to “MFA fatigue”

Attacker has username/password, end user accepts the MFA prompt

Users are always prompted on a new device

# Key decision #2: Choosing authentication methods

Bad: Password

Good: Password  
and ...

Better: Password  
and...

Best: Passwordless

123456

qwerty

password

iloveyou

Password1



SMS



Voice



Microsoft Authenticator



Software  
Tokens OTP



Hardware Tokens OTP  
(Preview)



Windows  
Hello



Microsoft Authenticator  
(Preview)

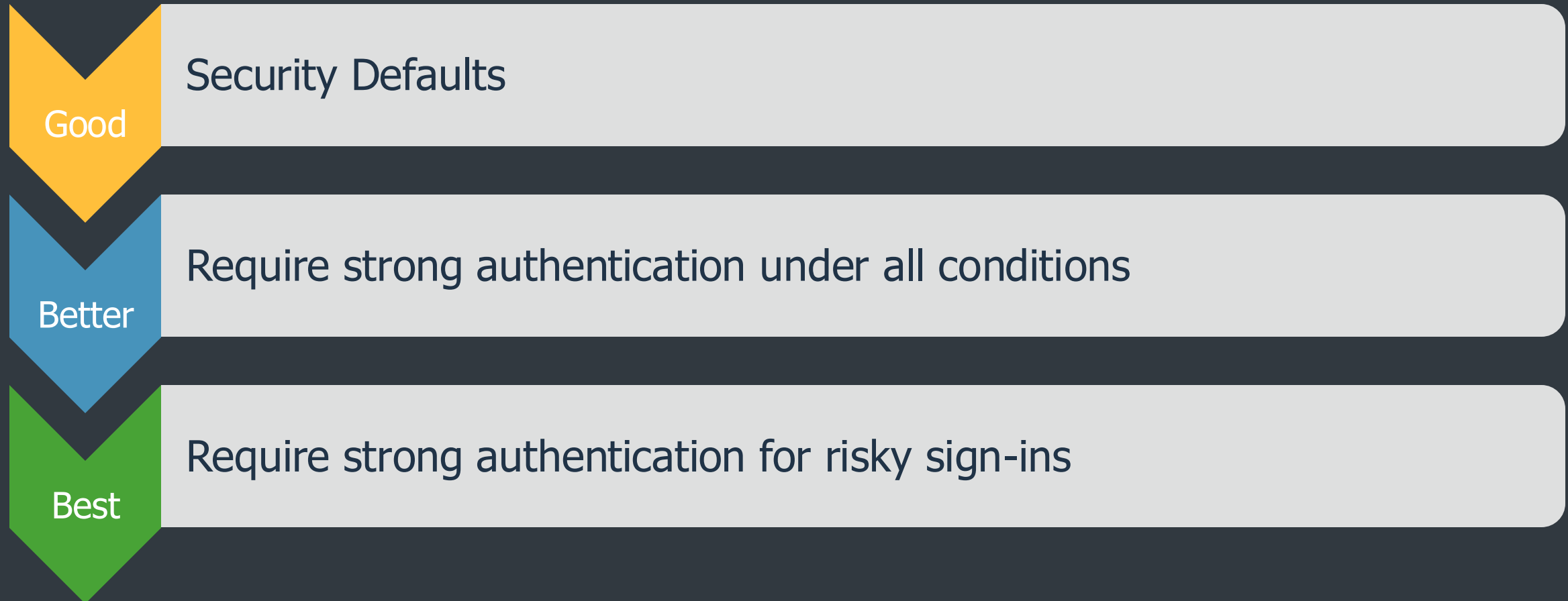


FIDO2 security key  
(Preview)

[aka.ms/gopasswordless](https://aka.ms/gopasswordless)

# Key decision #3: strong authentication configuration

How to enforce strong authentication in Azure AD





The “new normal” of working from home

Key decisions in a strong authentication deployment

**Strong authentication deployment tips**

Day to day tricks in managing strong authentication

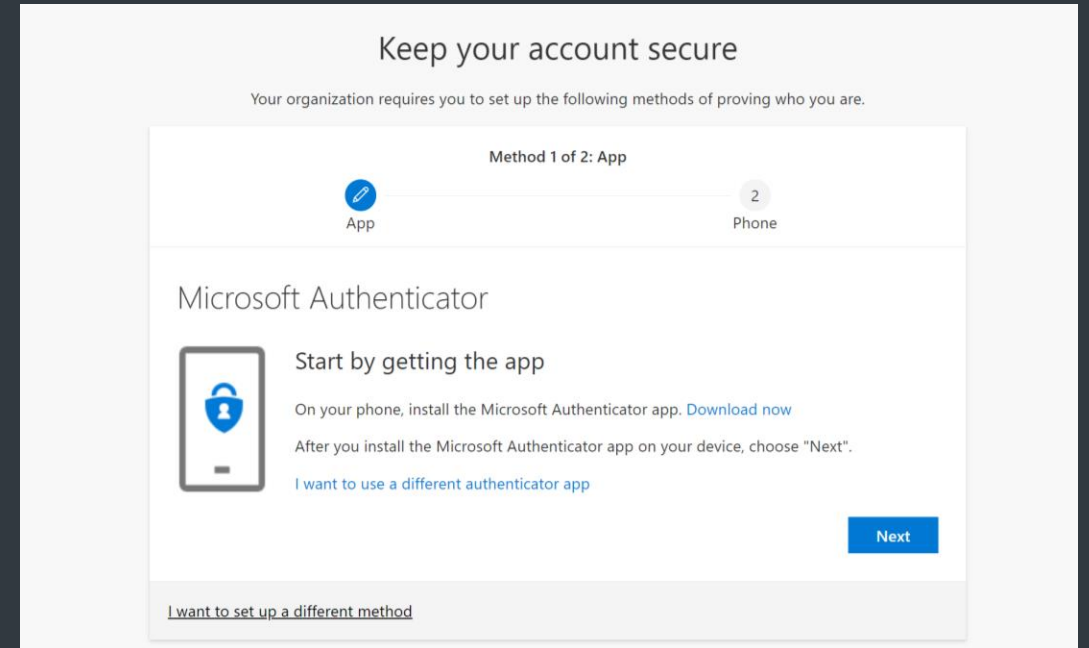
Go do's

# Tip #1: Deployment Administrative Actions

Use combined security info registration for MFA and SSPR with Conditional Access policy  
[aka.ms/securityinfodocs](https://aka.ms/securityinfodocs)

Use Microsoft Graph AuthMethods API to pre-register users phone number  
[aka.ms/AuthMethodsAPI](https://aka.ms/AuthMethodsAPI)

Use MFA deployment plans: [aka.ms/deploymentplans/mfa](https://aka.ms/deploymentplans/mfa)



# Tip #2: Reducing Prompts

Provide seamless experience to your users

Device	Windows	Mobile / MacOS
Managed	Enable single sign-on using managed devices (Azure AD Join, Hybrid Azure AD Join)*	Using the Authenticator app improves sign-in experience  Use Microsoft Enterprise SSO plug-in for Apple devices ( <a href="https://aka.ms/AADAppleSSO">aka.ms/AADAppleSSO</a> )
Unmanaged	Enable persistent browser sessions with sign-in frequency policies.	Using the Authenticator app improves sign-in experience

\* Limit reauthentication requirements for specific business scenarios using sign-in frequency policy

Learn more: <https://aka.ms/MFAPrompts>



# Tip #3: Deployment To End Users

## End User Communication Campaign

- Email, posters, contests, gamification

## Require MFA via Conditional Access on key applications

- Email, Paystub, Benefits, etc

## Registration rollout by groups

- Don't block deployment on the last 5%!

## Tip #4: Hello For Business Deployment

Deploy Key Trust where possible

Get Recommendations from [aka.ms/passwordlesswizard](https://aka.ms/passwordlesswizard)

Start with information workers first

Disable Convenience PIN via GPO

(Re-enrollment requirement to move from Convenience PIN to Windows Hello For Business)

## **Tip #5:** Authenticator Deployment Tips

BYOD & Non Windows Users (macOS/iOS/Android/Linux)

Enable verification codes, push notification and Phone Sign-in

Enable end user fraud reporting and establish a process for investigating

Educate about securing NON work accounts (personal email, bank, etc)



## Tip #6: FIDO2 Deployment

Good for frontline workers / one user to many machines

Plan for key life cycle management

Plan for key logistics (customs)

The “new normal” of working from home

Key decisions in a strong authentication deployment

Strong authentication deployment tips

**Day to day tricks in managing strong authentication**

Go do's

## Trick #1: Azure AD Logs

Use Azure AD Auditing logs to track registration

Use the Azure AD sign in logs for troubleshooting failed authentication

Many SIEMs have pre-built integration into Azure Monitor

Splunk ([aka.ms/aad2splunk](https://aka.ms/aad2splunk))

Sumo Logic ([aka.ms/aad2sumo](https://aka.ms/aad2sumo))

IBM QRadar ([aka.ms/aad2QRadar](https://aka.ms/aad2QRadar))

ArcSight ([aka.ms/aad2Archsight](https://aka.ms/aad2Archsight))

SysLog ([aka.ms/aad2Syslog](https://aka.ms/aad2Syslog))

Or use Azure Sentinel, Microsoft cloud-native SIEM

# Tip #2: Logs and Insights

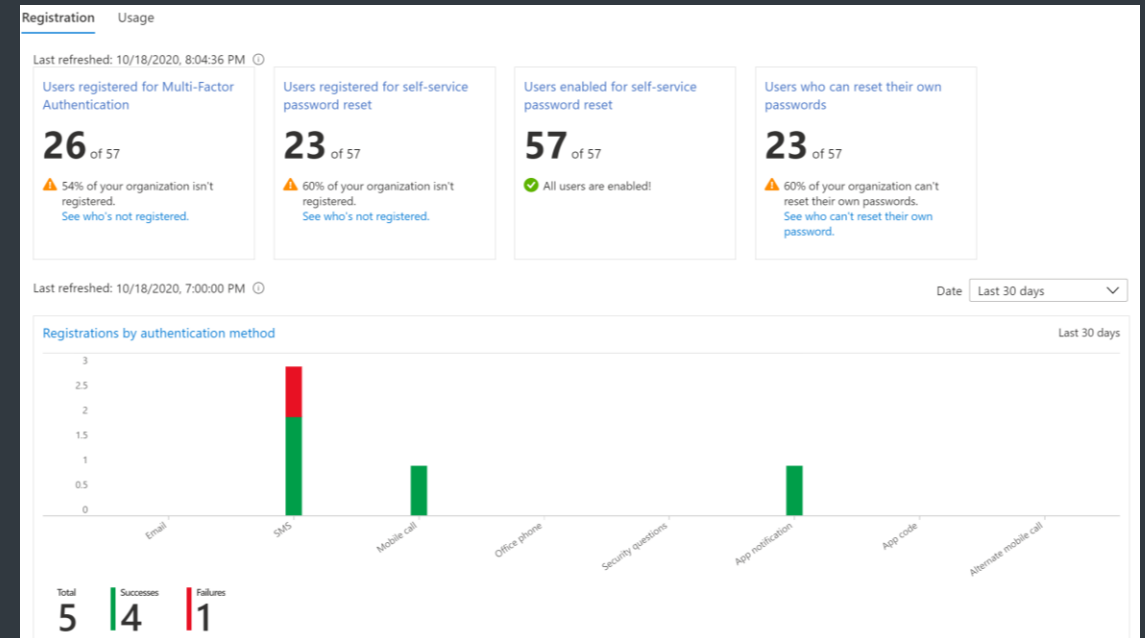
Use the Authentication methods insights dashboard

Use Azure Log Analytics for advance query and analytics

[aka.ms/AADLogAnalyticsWizard](https://aka.ms/AADLogAnalyticsWizard)

Have users register at least two different methods (or more!)

[aka.ms/MFAAuthMethodsAnalysis](https://aka.ms/MFAAuthMethodsAnalysis)





# Agenda

The “new normal” of working from home

Key decisions in a strong authentication deployment

Strong authentication deployment tips

Day to day tricks in managing strong authentication

**Go do's**

# Go Do's

[aka.ms/GoPasswordless](https://aka.ms/GoPasswordless)

## Next 7 days

- Enable combined registration
- Test strong authentication
- Determine authentication methods and other requirements (Windows version, hardware, FIDO2 keys).
- Enforce MFA for all admin accounts

## Next 90 days

- Gradually rollout strong authentication requirements for all your users
- Use Authentication methods activity to monitor the deployment

## Next 30 days

- Plan rollout including user communications, policies and managed devices
- Enforce strong authentication by using Conditional Access

# Live Q&A

Inbar Cizer Kobrinsky  @inbarck

Mark Morowczynski  @markmorow

Program Managers – Microsoft