



# Microsoft Ignite The Tour



# Lessons learned – Doing Azure MFA Right

Jan Ketil Skanke  
MVP Enterprise Mobility  
Principal Cloud Architect – CloudWay

Twitter @JankeSkanke



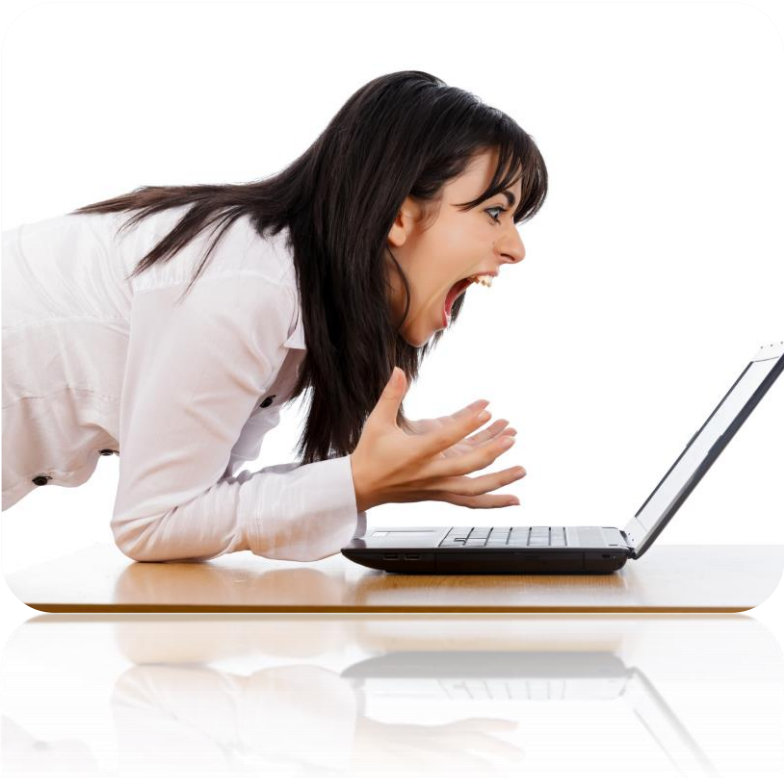
# Main Concern

# The User Experience



# User Experience enabling Multifactor Authentication

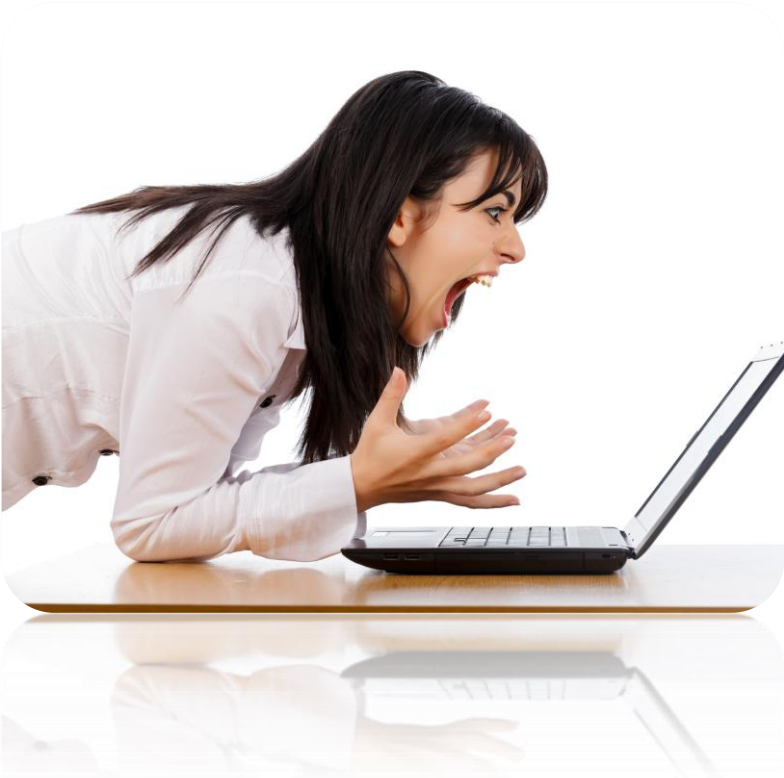
Frustrated



# User Experience enabling Multifactor Authentication

Frustrated

VS

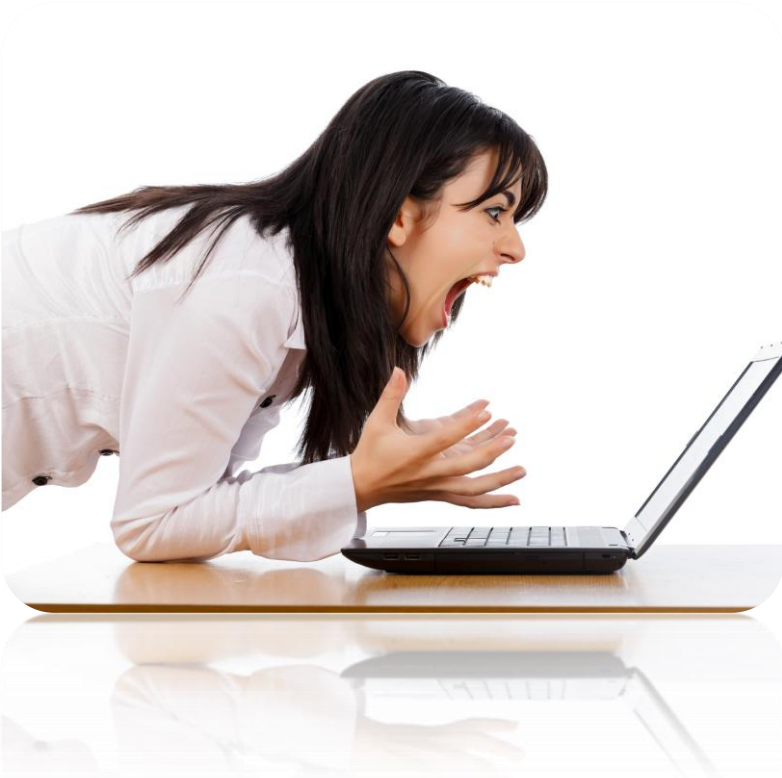


# User Experience enabling Multifactor Authentication

Frustrated

VS

Happy



# Are you enabling MFA in here?

multi-factor authentication

users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#).

bulk update

View: Sign-in allowed users



Multi-Factor Auth status: Any

☐ DISPLAY NAME ▲ USER NAME MULTI-FACTOR AUTH STATUS

Admin M2	admin@darkwebz.com
Ben The Geek	ben@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com
John	john@darkwebz.com

Disabled  
Disabled  
Disabled  
Disabled  
Disabled  
Disabled  
Disabled  
Disabled  
Disabled  
Disabled

Select a user



# Enable MFA in MFA Service

multi-factor authentication

users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#)

bulk update

View: Sign-in allowed users

Multi-Factor Auth status:

<input type="checkbox"/>	DISPLAY NAME ^	USER NAME	MULTI-FA STATUS
<input type="checkbox"/>	John Doe	john.doe@company.com	Disabled
<input type="checkbox"/>	Jane Smith	jane.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled
<input type="checkbox"/>	John Smith	john.smith@company.com	Disabled

Select a user



**So where to start?**

A long, straight asphalt road stretches from the foreground into the distance, flanked by dry, grassy fields. In the far distance, snow-capped mountains are visible under a blue sky with scattered white clouds. On the left side of the road, several utility poles with cross-arms are visible. The road has a double yellow line down the center. In the foreground, the word "START" is painted in large, white, italicized capital letters across the road, with a large white arrow pointing forward from the center of the word, following the road's path.

**START**

# 5 Important steps to do it right





# 5 Important steps to do it right

Educate your users on how and why



# 5 Important steps to do it right

Educate your users on how and why

Create a Break the Glass Admin



# 5 Important steps to do it right

Educate your users on how and why

Create a Break the Glass Admin

Block Basic Auth – Force Modern



# 5 Important steps to do it right

Educate your users on how and why

Create a Break the Glass Admin

Block Basic Auth – Force Modern

Use Conditional Access





# 5 Important steps to do it right

Educate your users on how and why

Create a Break the Glass Admin

Block Basic Auth – Force Modern

Use Conditional Access

Use Device / User Trust



# 5 Important steps to do it right

Educate your users on how and why

1

Create a Break the Glass Admin

2

Block Basic Auth – Force Modern

3

Use Conditional Access

4

Use Device / User Trust

5



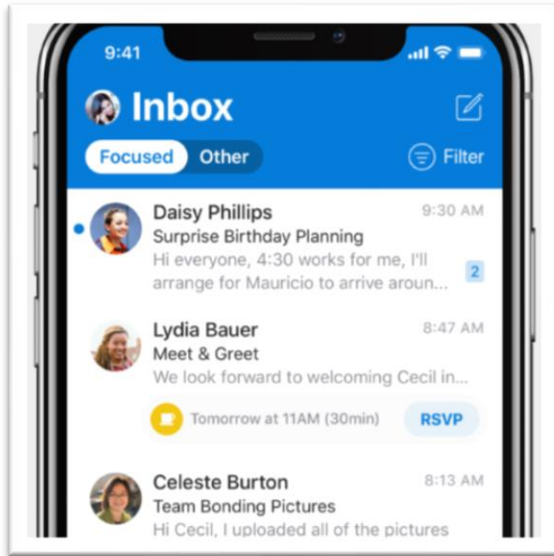


# Educate your users

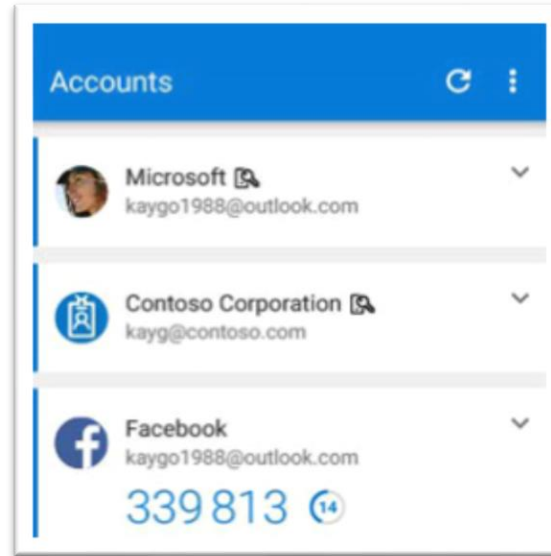
# 1

# Educate your users

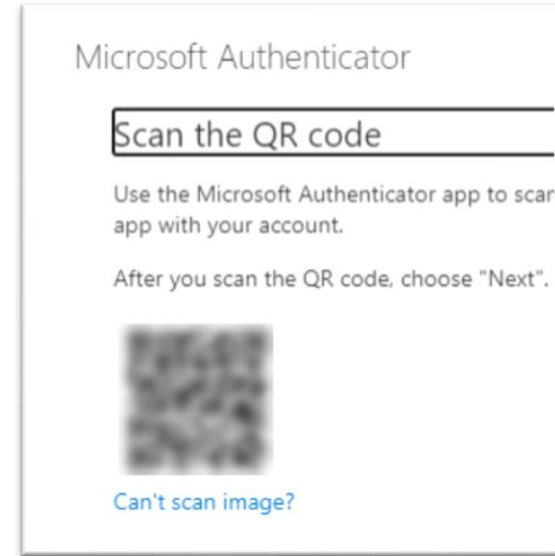
1



Why Outlook Mobile



Why and How to use  
Authenticator App



How to enroll into  
Azure MFA



Why Azure MFA

# Break The Glass Admin

2

# Break The Glass Admin

2

**IN CASE OF  
EMERGENCY  
BREAK GLASS**

# Break the Glass Account

2

## Why

MFA Solution Down

Network/Mobile outage

The "Admin" leaves company

Other

## How

Cloud Only Account

Not Personal

No Conditional Access

No Password Expiry

Global Admin

Monitor Usage

# Monitor the Break the Glass Account

2

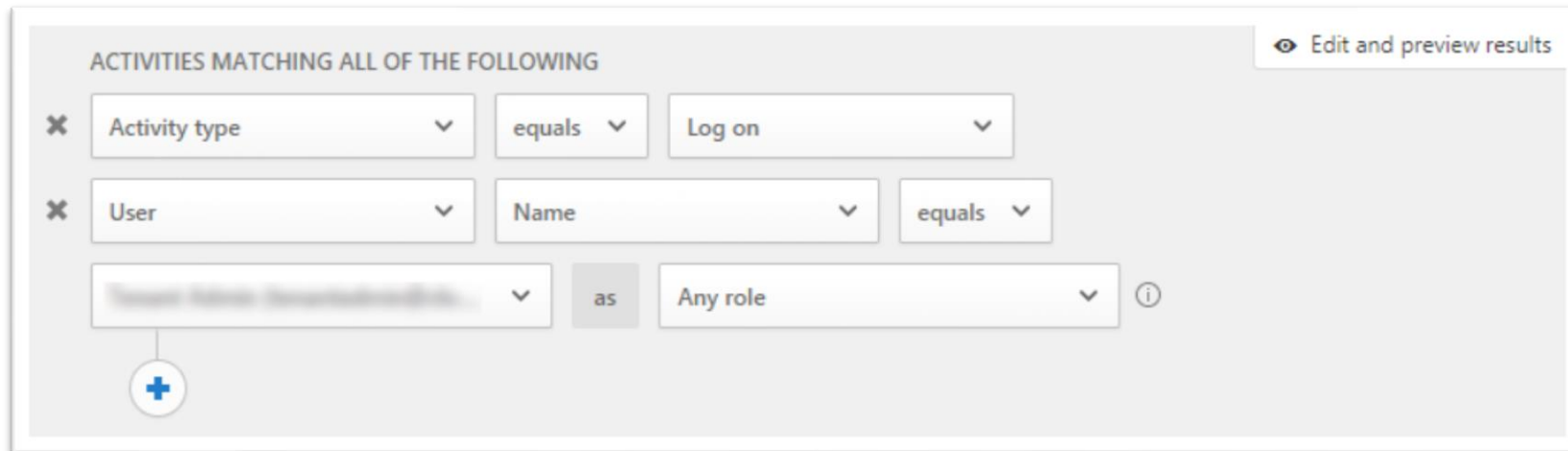
- GOOD: Azure Monitor Log Search Alert

SigninLogs

| where UserPrincipalName == "mybreakglassadmin@domain.com"

| project AppDisplayName , IPAddress , Location , UserPrincipalName , TimeGenerated

- BETTER: Microsoft Cloud App Security



ACTIVITIES MATCHING ALL OF THE FOLLOWING

✕ Activity type equals Log on


✕ User Name equals

▼ as Any role ⓘ



+

Edit and preview results

# Forward alert to Teams



**Flow** 1/16 8:11 PM

**MCASAlert: Emergency Account Used**  
UserName: [redacted]@cloudways.onmicrosoft.com  
Time: 2020-01-16T19:11:14.775Z  
Application: Microsoft Exchange Online  
IP: [redacted]  
Location: NO

Jan Ketil Skanke ([redacted]) used Microsoft Flow to automate this notification. [Learn more](#)

← Reply

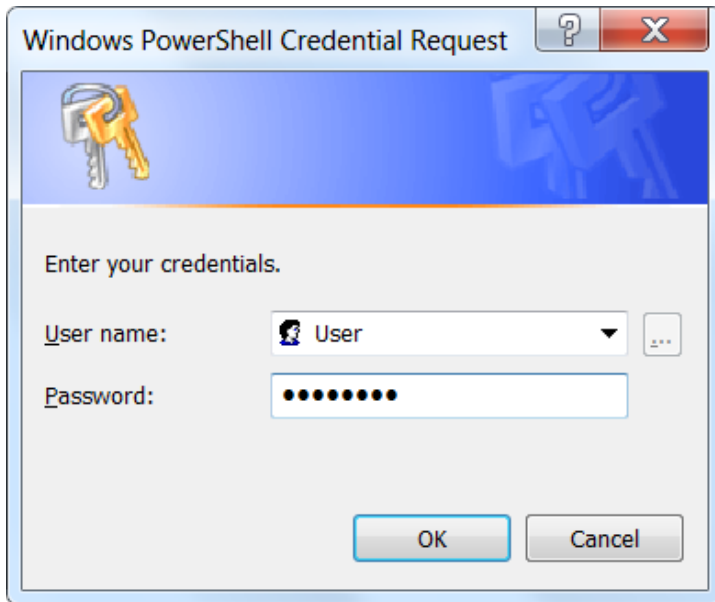
# Block Basic Auth – Enforce Modern

3



# Basic Auth – Examples

3

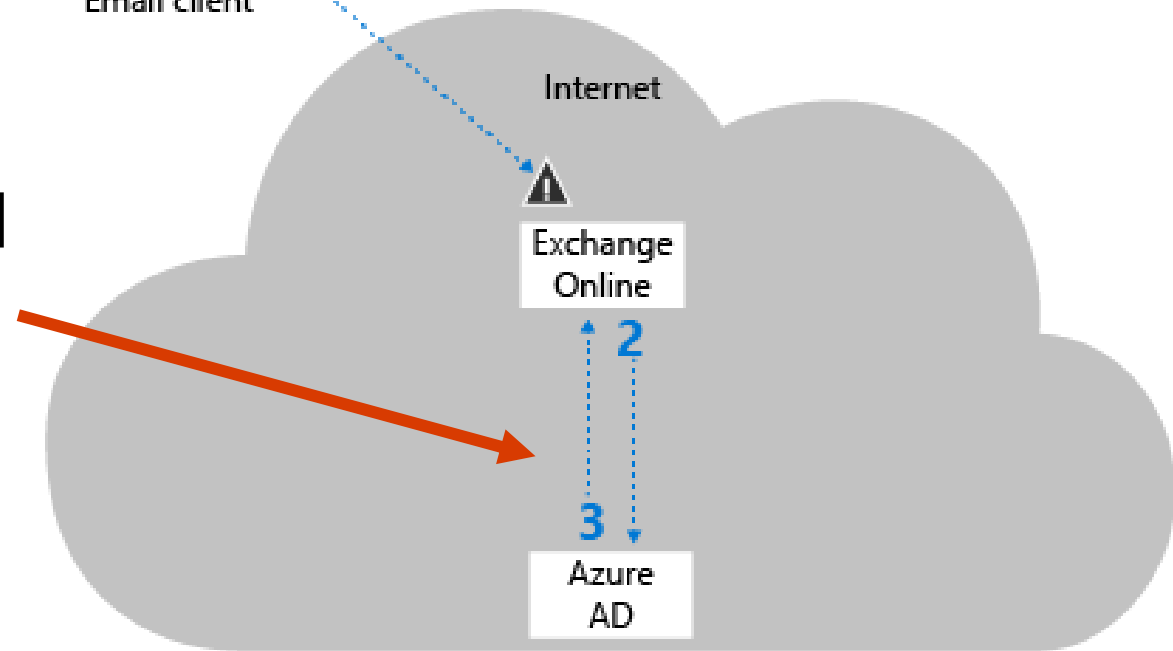


# Blocking Basic Authentication

- Exchange Online Authentication Policy will block pre-authentication

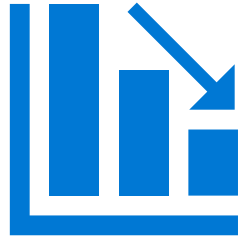


- Conditional Access Policy will block post-authentication



# Why is Blocking Legacy auth so important?

3



## **Reduce Risk of Compromise**

Cause of nearly 100% of password spray attacks  
Reduces compromise rate by 66%



## **Prepare for upcoming breaking change from Microsoft**

It's being disabled Oct 13th, 2020 in EXO!

# How to block Basic Auth with Conditional Access

3

- Conditional Access policies will block post-authentication
- Report-only mode can help measure the impact

The screenshot displays the Microsoft Azure portal interface. At the top, there are two tabs: 'Conditions' and 'Client apps (preview)'. Below these, the main content area shows the 'Sign-ins' section for 'Contoso - Sign-ins'. The left sidebar contains a navigation menu with options like 'Company branding', 'User settings', 'Properties', 'Notifications settings', 'Security', 'Monitoring', 'Sign-ins', 'Audit logs', 'Provisioning logs (Preview)', 'Logs', 'Diagnostic settings', 'Workbooks', 'Usage & insights', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The 'Sign-ins' option is highlighted with a red box. The main content area shows a table of sign-in events with columns for Date, User, App, Status, IP Address, Location, and Result. Below the table, the 'Details' section is visible, with the 'Report-only (Preview)' tab selected and highlighted with a red box. This tab shows a table of Conditional Access policies with columns for Policy Name, Grant Controls, Session Controls, and Result. The policies listed are 'Common Policy - Require compliant devices', 'Common Policy - Block legacy authentication', and 'Common Policy - Block access by location'. The results for these policies are 'Report-only: Failure', 'Report-only: Not applied', and 'Report-only: Not applied' respectively. A note at the bottom states: 'A sign-in can also be interrupted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.'

Date	User	App	Status	IP Address	Location	Result	
10/24/2019, 1:1...	7d34f2d8-9d4b...	Bala Sandhu	My Access	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	85c76bdf-9fd2...	Bala Sandhu	My Access	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	8c8f0cac-d81b...	Bala Sandhu	Microsoft AppS...	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	d0da029f-c682...	Bala Sandhu	Microsoft App ...	Success	73.83.66.107	Redmond, Was...	Not Applied
10/24/2019, 1:1...	7f4c28b5-aca7...	Bala Sandhu	Microsoft App ...	Interrupted	73.83.66.107	Redmond, Was...	Not Applied

Policy Name	Grant Controls	Session Controls	Result
Common Policy - Require compliant devices	require compliant device		Report-only: Failure
Common Policy - Block legacy authentication	block		Report-only: Not applied
Common Policy - Block access by location	block		Report-only: Not applied

# Use Conditional Access

# 4

## Conditional Access for your End Users

Require Compliant Device /  
Hybrid AD Join on Windows

Require Compliant Device / App  
for iOS and Android for Mobile

**Or MFA**

Include All Cloud Apps

Block unsupported platforms

Block Basic Auth

# Conditional Access for your End Users

Home > Skanke Domain > Security > Conditional Access

All Users: PC Require Compliant Device... ☐ ☐

Name \*

All Users: PC Require Compliant Device... ☐

Assignments

Users and groups

All users included and specific us...

Cloud apps or actions

All cloud apps

Conditions

2 conditions selected

Access controls

Grant

2 controls selected

Session

0 controls selected

## Grant

Select the controls to be enforced.

- ☐ 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 (Preview)   
[See list of policy protected client apps](#)

For multiple controls

- ☐ Require all the selected controls
- ☒ Require one of the selected controls

Don't lock yourself out! Make sure that your device is compliant.

4

Or MFA

**Use Device Trust / User Trust**

**5**



# Establish Basic Device Trust for Windows

5



Intune  
(for cloud-first environments)

Create compliance policies  
Create configuration policies



SCCM and Intune co-managed  
(for hybrid environments)

Move Compliance Workload to Intune  
Create Compliance Policies in Intune



No management solution, or  
3<sup>rd</sup> party management

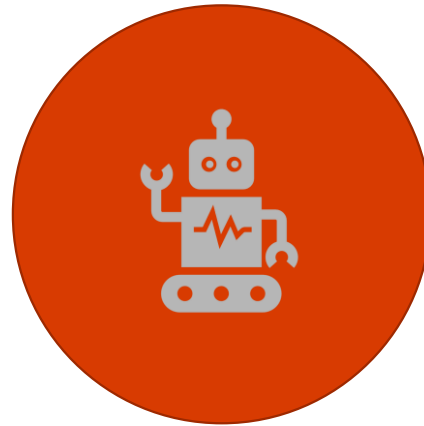
Trust on Hybrid AD Join only (Basic)  
Enroll to Intune via GPO (Recommended)

# Device trust also on other platforms

5



IOS



ANDROID



MAC

# Recap

Educate your users on how and why

Create a Break the Glass Admin

Block Basic Auth – Force Modern

Use Conditional Access

Use Device / User Trust



Enable MFA

Today!

# Lessons learned – Doing Azure MFA Right

Jan Ketil Skanke  
MVP Enterprise Mobility  
Principal Cloud Architect – CloudWay

Twitter @JankeSkanke



