

Microsoft Ignite

Learn.
Connect.
Explore.



Hybrid Identity and Access Management Best Practices

Adam Steenwyk ([@ajamess](#))

Mark Morowczynski ([@markmorow](#))

Program Managers-Identity Division

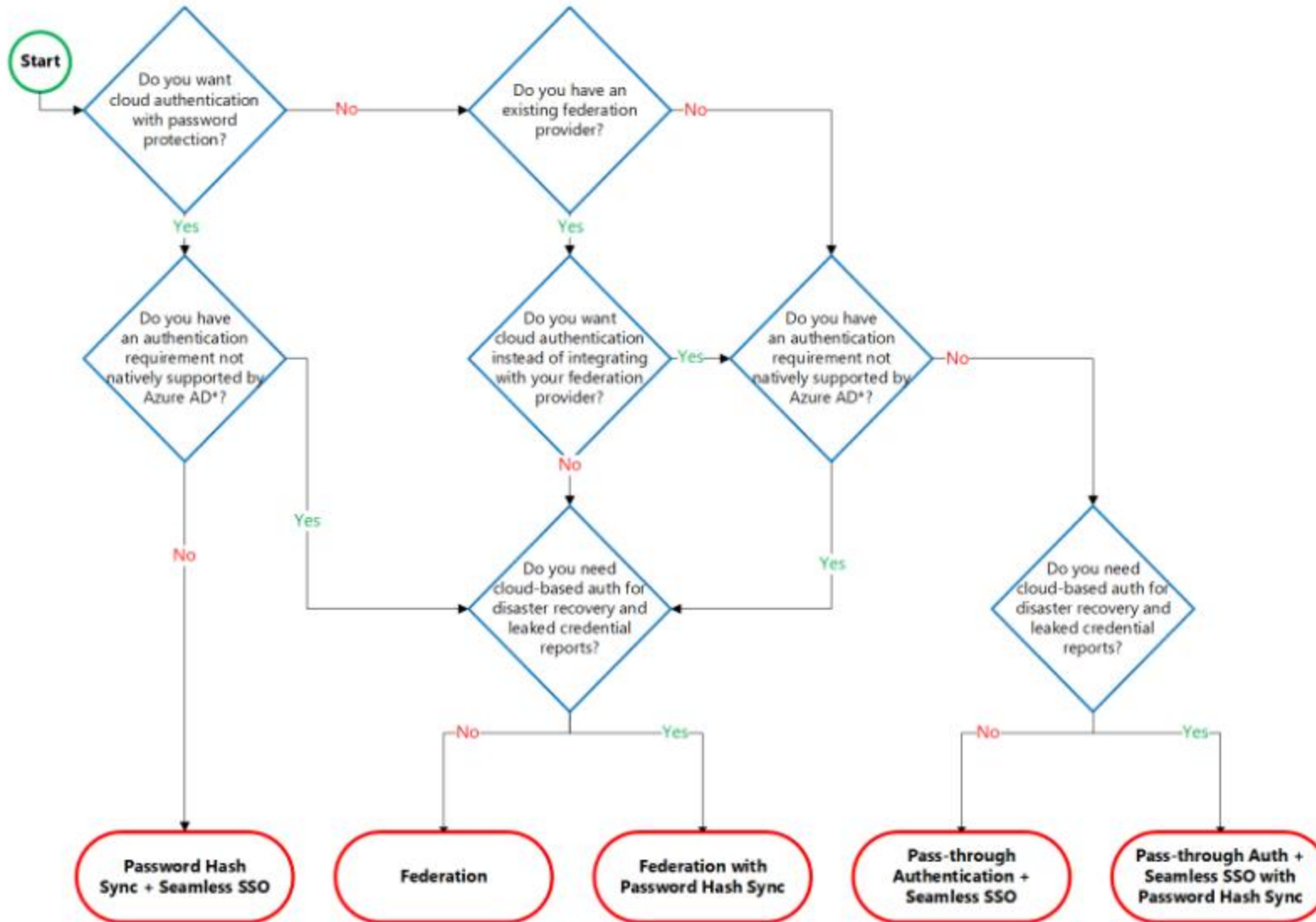
Agenda

- Get Users – Authenticate all your users seamlessly
- Get Apps – Get any app connected in no time
- Get Insights – Easily discover insights about your org
- Get Excited – Leverage this great foundation with exciting new features
- Go Dos

Get Users Authenticated



Choosing the Right Authentication

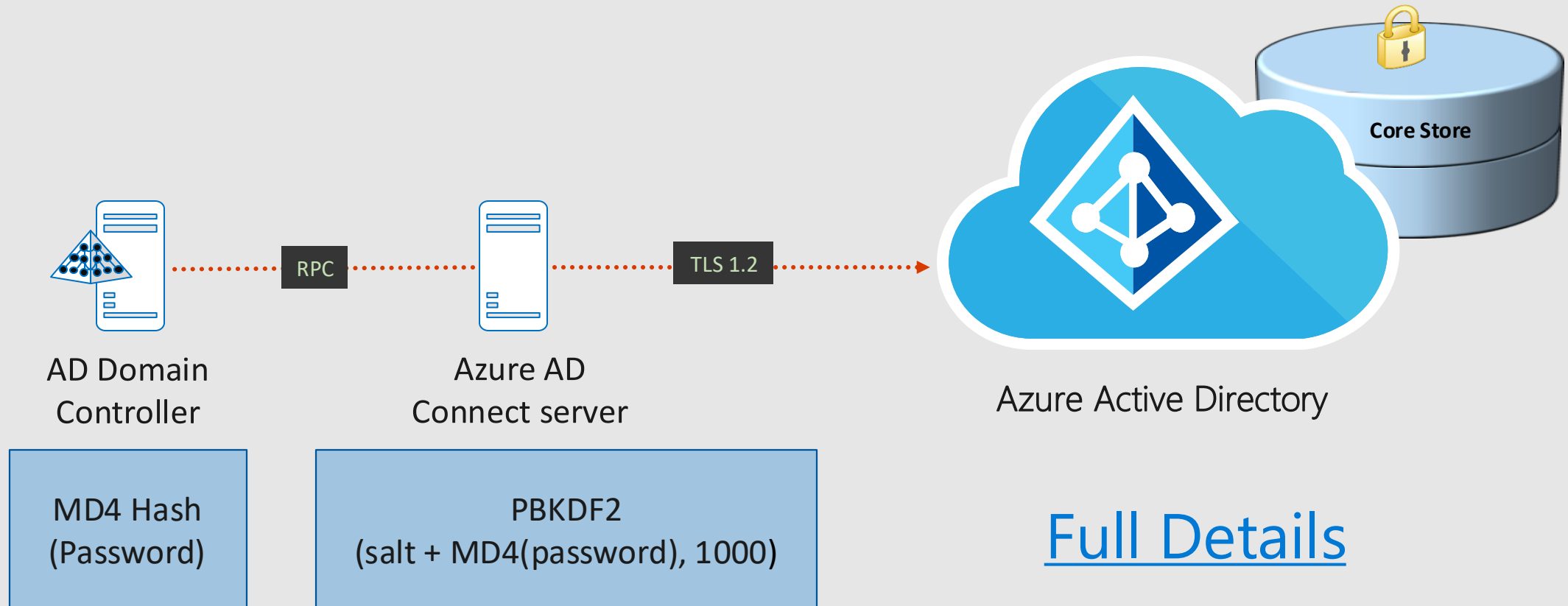


- First, use PHS with Seamless SSO
- Second, use PTA with Seamless SSO
- Third, use Federation
- For More see THR3046
- [Documentation](#)

Why Should You Care About Password Hash Sync

- Leaked Credentials
 - Dark Web, Law Enforcement, Security Researches
- When something catastrophic happens
 - WannaCry, NotPetya
- Could this have been you? Could your company survive this?

How Password Hash Sync Works



Why You Should Care About Seamless SSO

- Gives you the ability to get SSO without Federation for domain joined machines
- Works with PHS or PTA
- No additional components needed on-prem to make this work
 - Uses Kerberos and TrustedSites
 - [Full Details](#)

Migrating Users From Federation to PHS with Seamless SSO

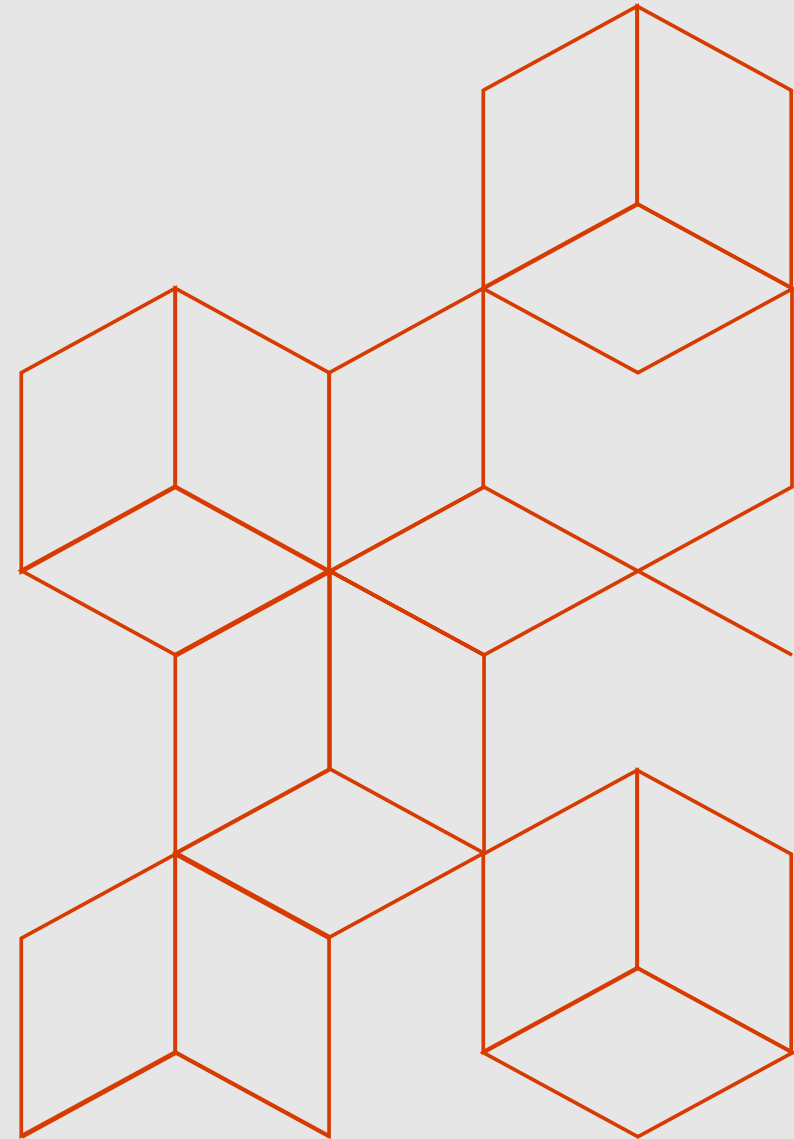
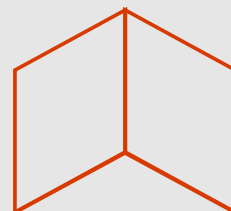
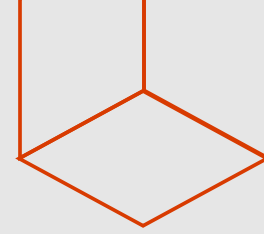
Demo



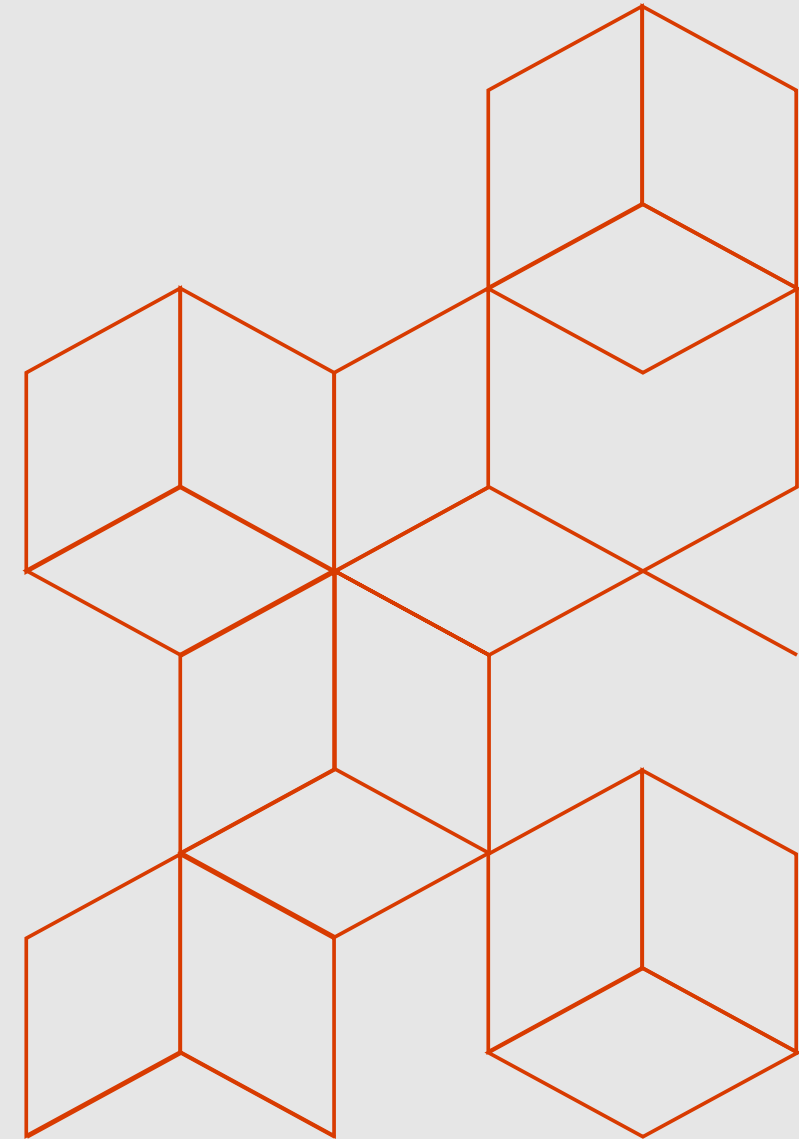
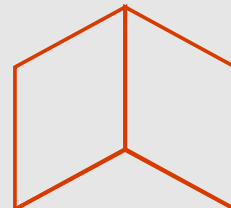
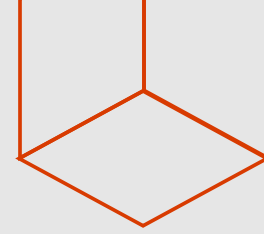
Authentication Best Practices

- Enable Password Hash Sync!
- Enable Seamless SSO, start with small pilot to get started
- Start migration to PHS + Seamless SSO

SaaS Apps



**I already have my SaaS Apps in
ADFS, why do I need them in
Azure AD**



ADFS is an STS

**Azure AD is an IAM
Solution**

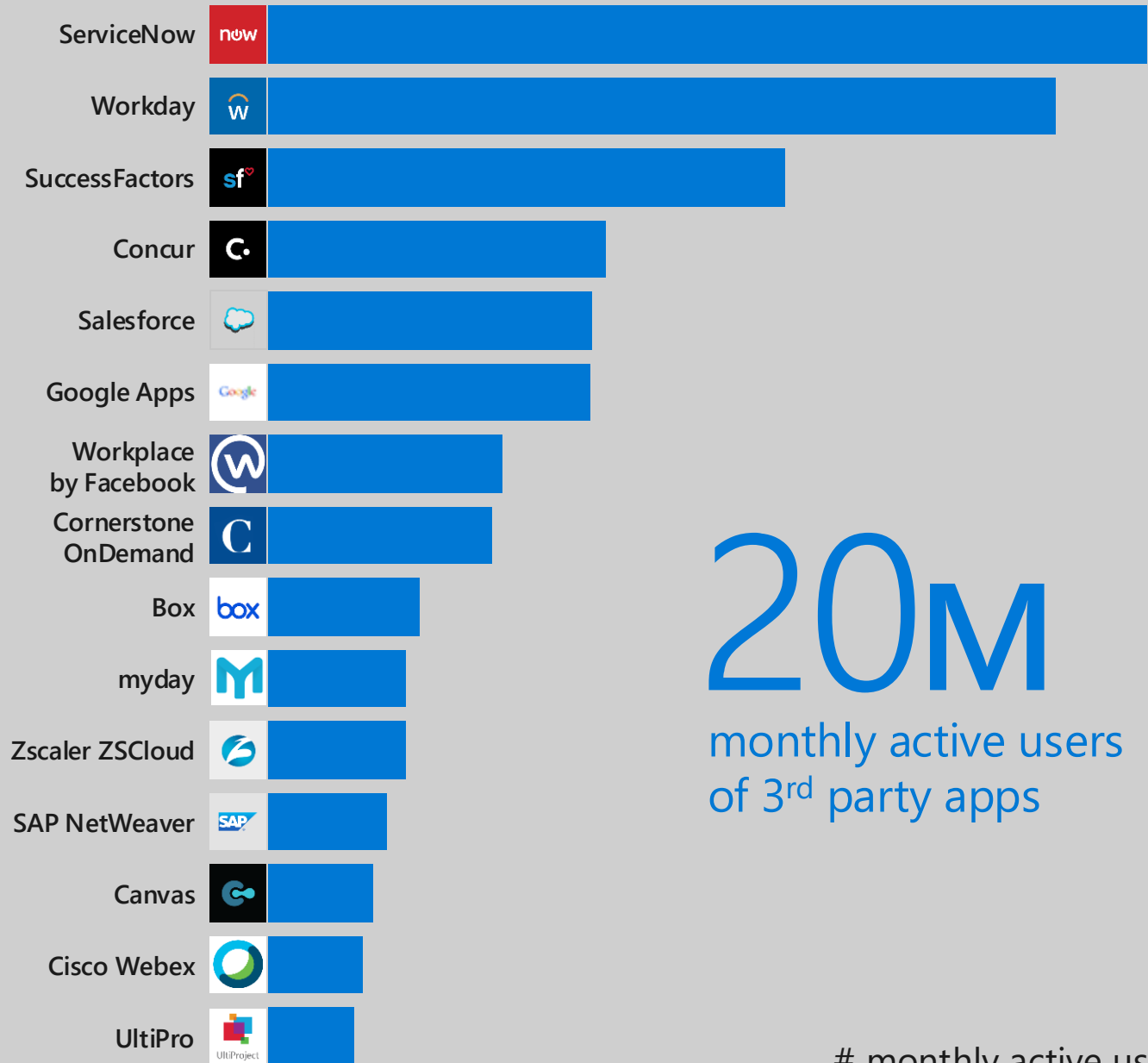


Azure AD

3rd party applications

634,000

Active Azure AD integrated applications and services



20M

monthly active users
of 3rd party apps

monthly active users

SaaS Apps in Azure AD Benefits

- Security
 - If you aren't using SSO, securing your credentials is going to be difficult...
 - Conditional Access policies, Identity Protection and Azure AD Security apply to SaaS Apps
- Provisioning and De-provisioning
 - Timothy API
 - No more mystery scripts
- Integrated end user experience across Microsoft
- Works with any app
- Quick to get started and easy to manage

Adding SaaS App to Azure AD

Demo



Migrating SaaS Apps

- All your migration needs in one place: <http://aka.ms/migrateapps>
- High level migration whitepaper
- ADFS-specific solution guide and tooling
- Deployment plans for specific workloads
- Give us feedback at aadappfeedback@microsoft.com

Apps Migration Resources

<http://aka.ms/migrateapps>

Demo



SaaS App Best Practices

- Use <http://aka.ms/migrateapps> for lots of migration goodies to get started
 - Give feedback on the tools at aadappfeedback@microsoft.com
- Incorporate provisioning in your plans
- Check out deployment plans at <http://aka.ms/deploymentplans> for step-by-step guidance
- Use the MyApps Secure Sign-In Extension to configure and test SSO
 - Use in portal feedback if you run into a problem
- Need an app? Let us know at <http://aka.ms/azureadapprequest>
- Check out BRK3244-Modernize Your Identity Lifecycle Management

Operational Insights



Operational Insights Benefits

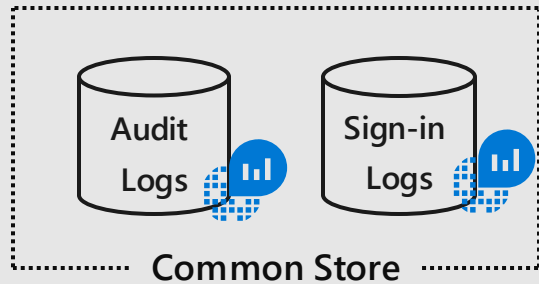
- This is where the value add is
- Usage metrics
 - Are we using what we are paying for?
 - What is happening in our environment (looking for trouble)
- Investigating a security incident
 - The more dispersed the data is, the harder it is to correlate
 - Can you tell who was impacted?
- This is a quick win and will be a jumping off point

Azure Monitor



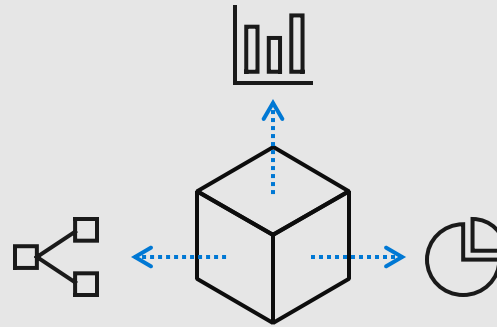
Azure AD in Azure Monitor

Full observability for your Azure AD Infrastructure



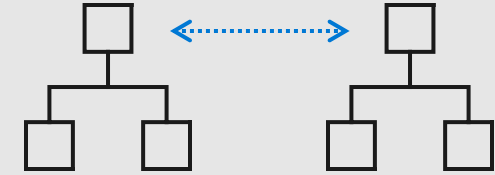
Unified Monitoring

A common platform for all Azure AD logs



Analyze


Rich Insights, advanced analytics and smart machine learning powered by Log Analytics




Workflow Integrations

Rich ecosystem of popular issue management, SIEM, and ITSM tools


Azure Monitor Setup




Sign-in Logs




Self-Service capabilities




Provisioning-Deprovisioning




Conditional Access




Access Panel/MyApps



Privileged Identity Management



HR App Integration



Access Reviews

Home > f/128 Photography - Diagnostic settings > Diagnostics settings

Diagnostics settings

Save Discard Delete

azureadlogstoEH

☒ Archive to a storage account

Storage account

azureadactivitylogs1

>

☒ Stream to an event hub

Event hub

azureadlogs2EH (RootManageSharedAccessKey)

>

☒ Send to Log Analytics

Log Analytics

AzureADLogsWS

>

LOG

☒ AuditLogs

Retention (days)

0

☒ SignInLogs

Retention (days)

0

In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

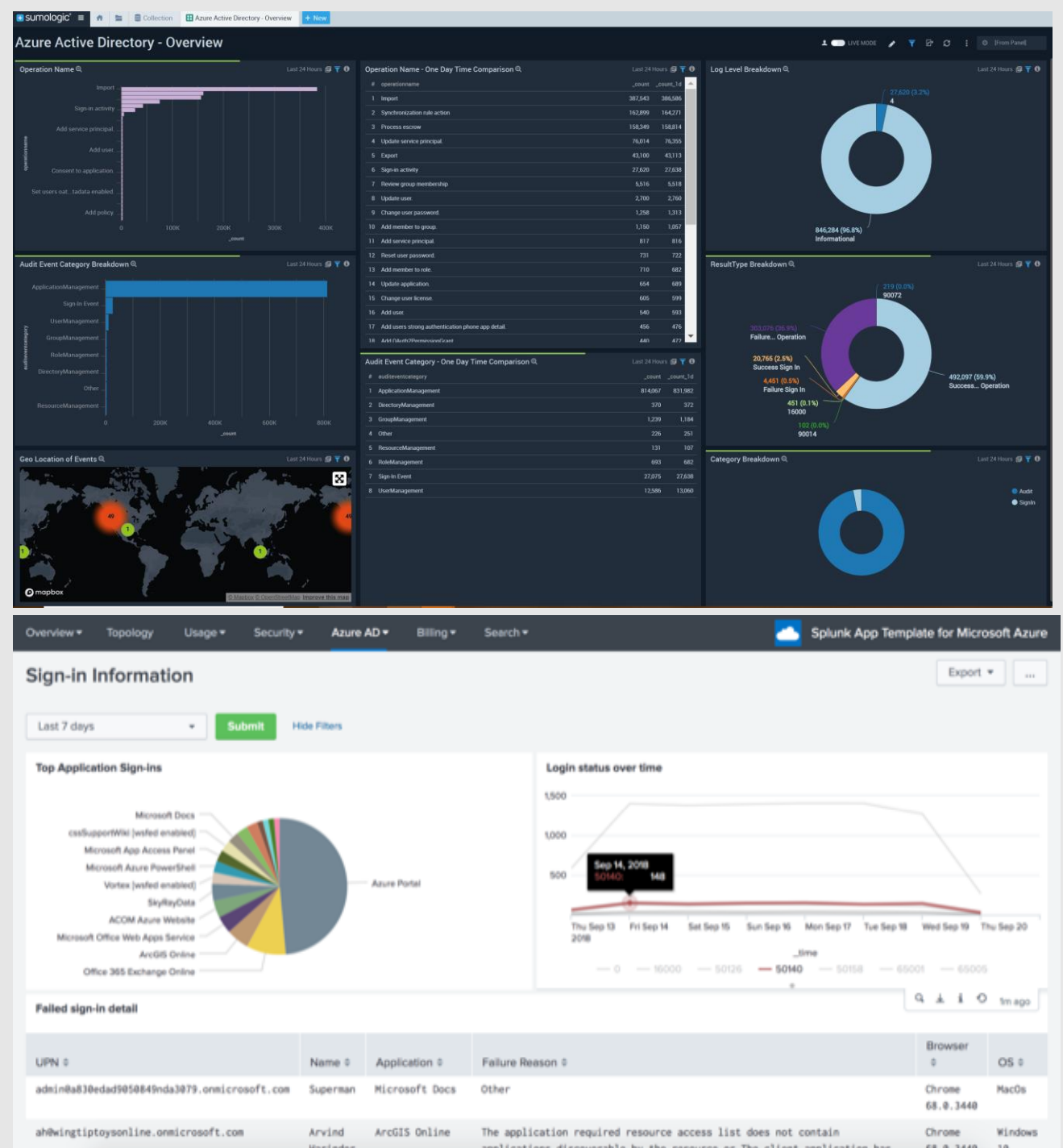
SIEM Integration

Azure Monitor
Integration

Sumologic

Splunk

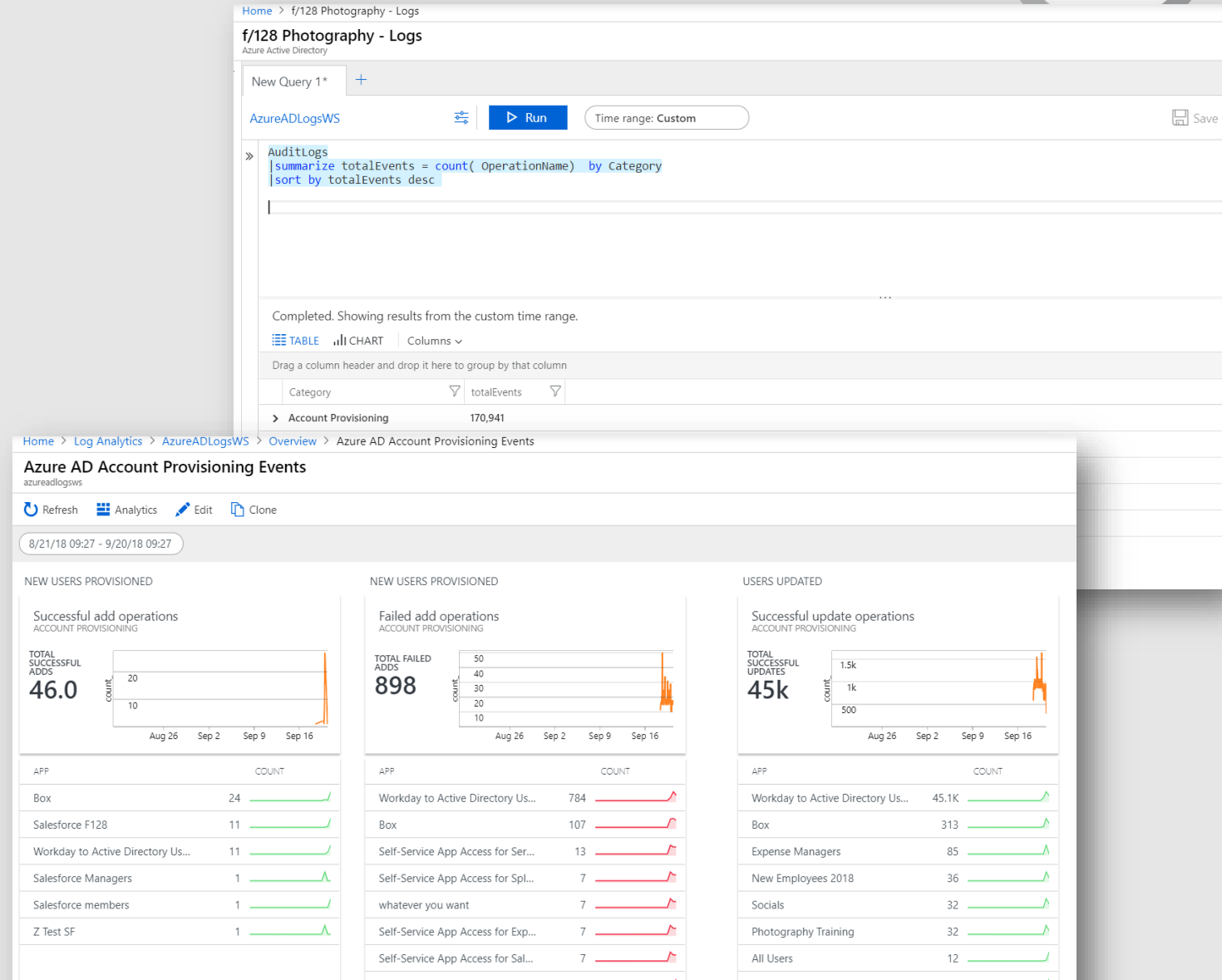
ArcSight



Advanced Queries with Log Analytics



- Log Analytics advanced query experience now in Azure Portal
- Central Analytics Platform across Monitoring, Management, Security
- Run ADEQL queries for investigations, statistics, and root cause + trend analyses
- Utilize ML algorithms for clustering and anomaly detection
- Setup custom alerts and actions
- Dashboard views



Azure Monitor and Log Analytics

Demo

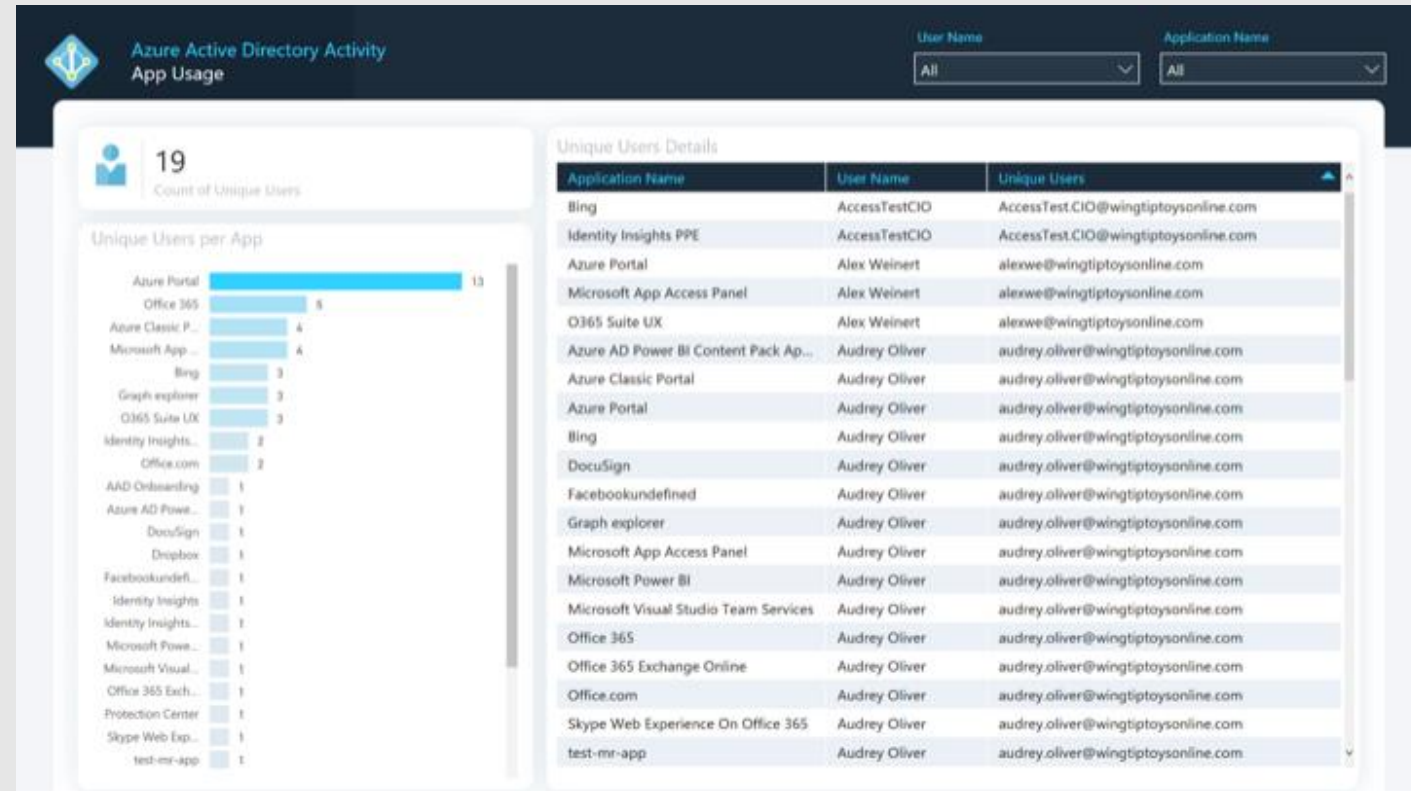


Operational Insights Best Practices

- Setup your Azure AD logs with Azure Monitor
- Integrate with your SIEM tool through Event hub
- Use Azure AD Log Analytics to
 - Gather ad-hoc insights, visualize, troubleshoot issues
- Query tips:
 - Use dot syntax, include all columns, explore with schema view
 - Columns to Get Started with AuditLogs:
 - Category, ResultType, OperationName, TargetResources, InitiatedBy, TimeGenerated
 - Smaller table on left for joins (faster)

Operational Insights Quick Wins

- No SIEM? No Problem!
- [Download the PowerBI Content Pack](#)
- Do it on the plane!



**Leveraging your foundation: I
got all this stuff setup, now
what?**



Getting Secure

- Leaked Credentials
- Legacy Auth Sign-Ins
 - **BRK3408**-Azure AD Best Practices From Around The World- Fri 10:15 AM
- Permissions Remediation
- Protecting Admin accounts
 - **BRK3248** - Protect The Keys To Your Kingdom with PIM – Wed 4:30 PM
 - [Aka.ms/breakglass](https://aka.ms/breakglass)
- Shut the door on Cybercrime
 - **BRK3251** – Thurs 10:45 AM

Indicators of Compromise

Demo



Excite Your Users

- Launch any app from anywhere, even if the app is on-premises
- Enable users to add their own apps
- Delegate access control to your business
- Clean up groups with access reviews

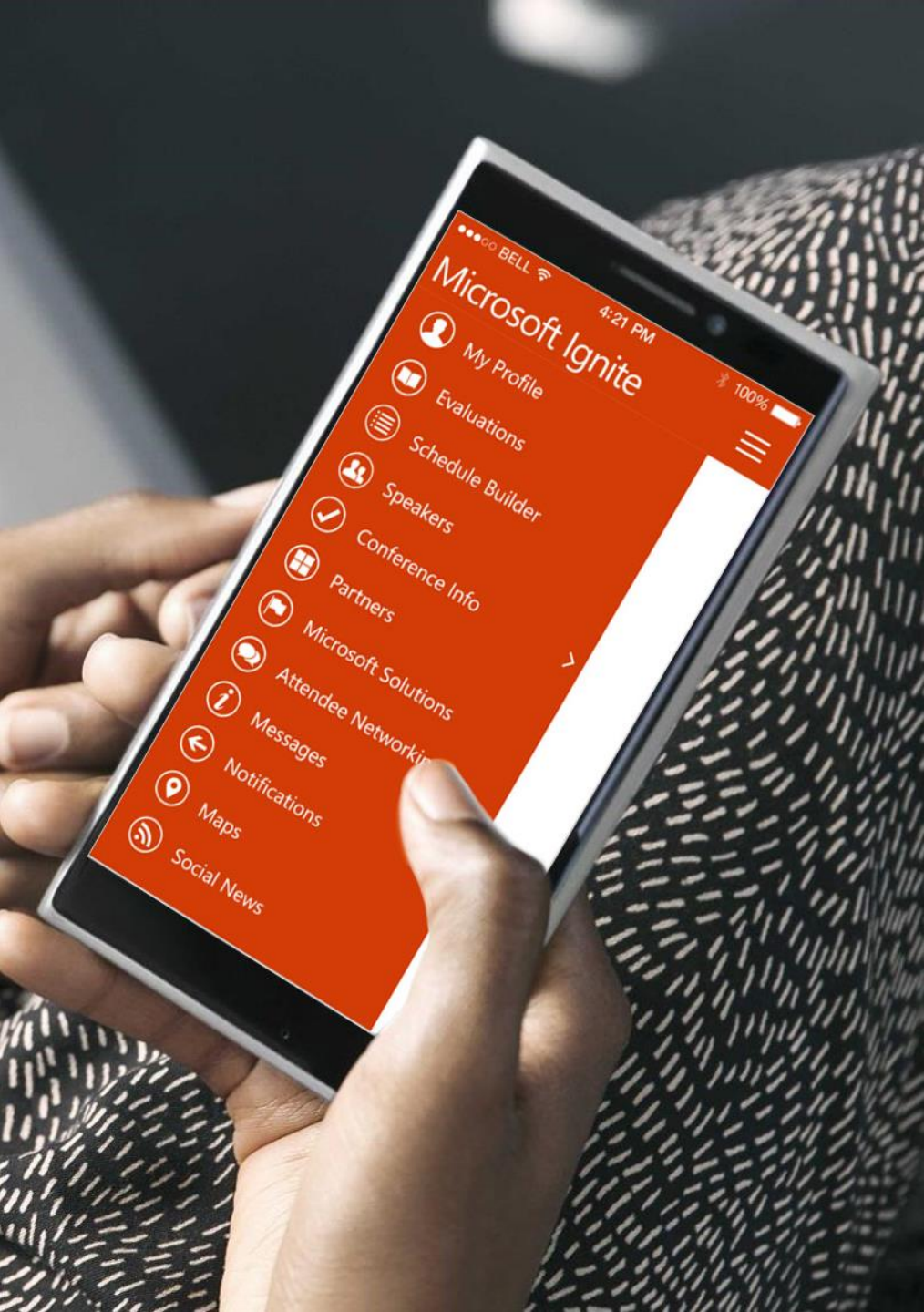
Launch apps from anywhere

Demo



Recap: All the best practices!

- Authentication
 - Enable Password Hash Sync
 - Enable Seamless SSO, start a pilot
 - Start your migration off Federation
- SaaS Apps
 - Use <http://aka.ms/migrateapps> for scripts and other goodies
 - Get going with aka.ms/deploymentplans
 - Take our survey: aka.ms/apps-survey
 - Feedback? aadappfeedback@microsoft.com
 - Include Provisioning!
 - Use the MyApps Secure Sign-In Extension
- Operational Insights
 - Setup Azure Monitor
 - Pull the logs into your SIEM
 - Use Log Analytics
- Leverage Your New Foundation
 - Use PowerBi Dashboard
 - Get Secure – Leaked Creds, Legacy Auth, & permission remediation
 - Excite your users – Show your users all the ways they can use apps



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>





Need guidance for a successful deployment?

Download our official Azure AD Deployment plans here:

aka.ms/deploymentplans

