

What is Microsoft Enterprise Mobility Suite and how to configure it

Peter Daalmans
@pdaalmans
<http://ref.ms/aboutme>

Mirko Colemberg
@mirkocolemberg
<http://blog.Colemberg.ch>



Peter Daalman



@pdaalman



Sn. Technical
Consultant,
IT-Concern



Configmgrblog.com
ref.ms/aboutme



#MMSMOA

Mirko Colemborg



Solothurn, Switzerland



@mirkocolemborg



Principal
Consultant



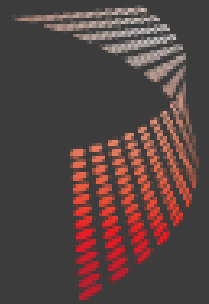
Blog.Colemborg.ch



#MMSMOA

Agenda

- EMS Components
 - Azure AD Premium
 - Microsoft Intune
 - Azure RMS
- How to get started?



Enterprise Mobility Suite

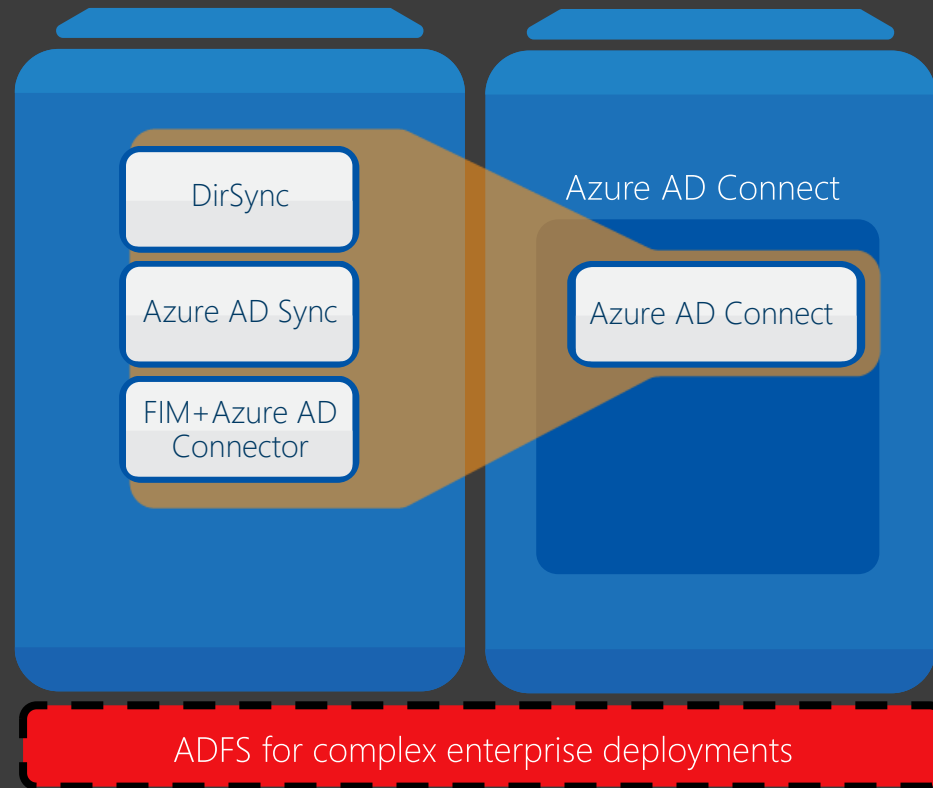
#MMSMOA

What is MS EMS?

- Enterprise Mobility Suite
 - Azure Active Directory Premium
 - Microsoft Intune
 - Azure Rights Management



Making hybrid identity simple – 6 clicks to the cloud



Azure AD Connect

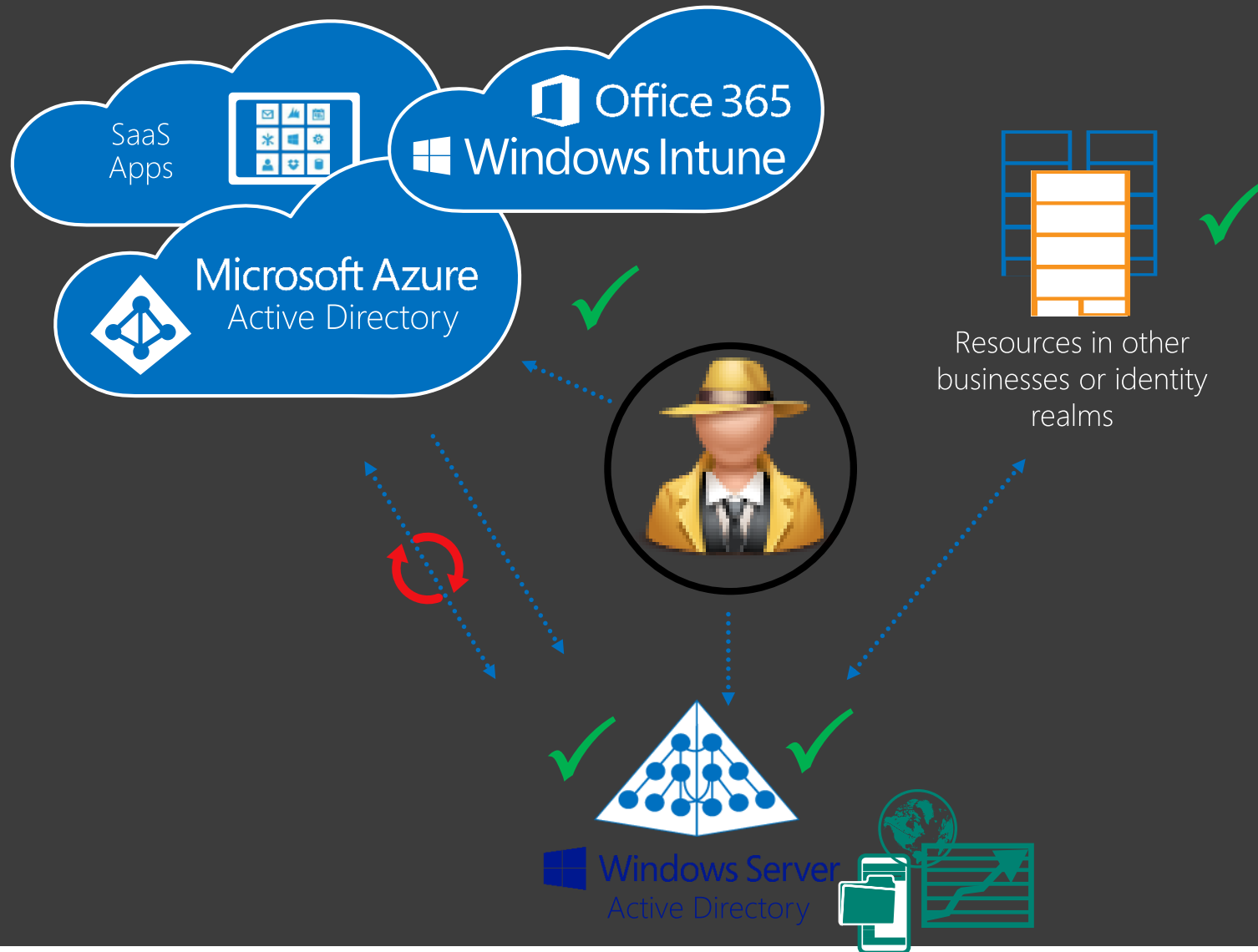
Consolidated deployment assistant for your identity bridge components

(The difference is the Password)

ADFS use cases

- Tighter AD integration
- Security Policy
- Conditional Access
- Smart Card Authentication

Identity: Cloud, Sync or Federated?



Cloud identity provides a solution where all identity resides in the cloud

Identity sync enables customers to bridge their existing identity into the cloud

Federated identity allows customers to retain all authentication on-premises

B2B federated identity allows customers to securely share and collaborate with each other

Azure Active Directory Premium

Active Directory in the cloud

- Federation and identity provisioning

Centrally managed identities

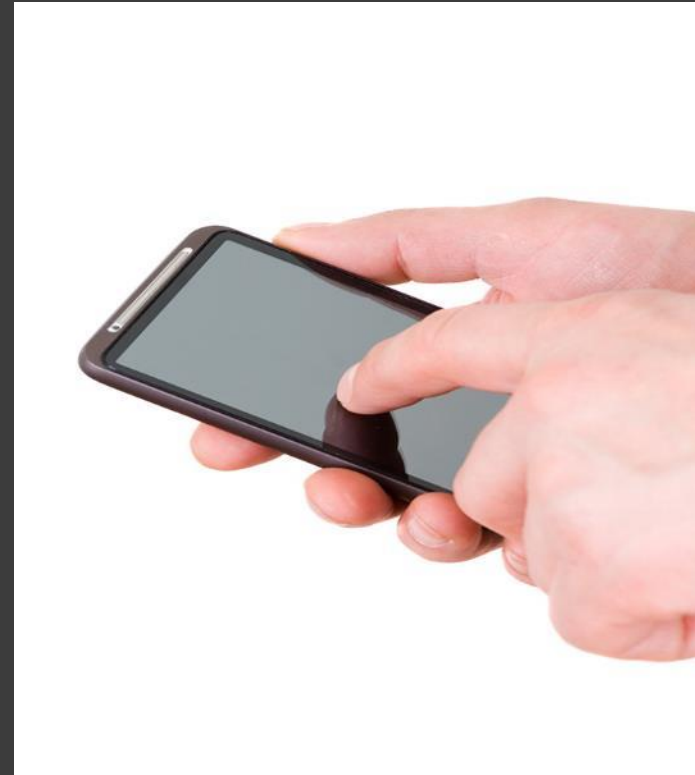
- Synchronization
- Single User Identity (SSO)

Monitoring and protect access to cloud apps

- Authentication and Security reports
- Multi-Factor Authentication (MFA)

Empower end Users

- Self-Service password reset



AAD editions comparison

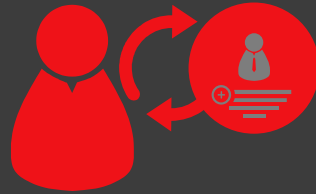
		Azure Active Directory Free	Azure Active Directory Basic	Azure Active Directory Premium	Office 365 IAM features
Common Features	Directory as a Service	500,000 Object Limit	No Object Limit	No Object Limit	No Object limit for Office 365 user accounts
	User/Group Management (add/update/delete)	Yes	Yes	Yes	Yes
	SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	10 apps per user	No Limit	10 apps per user
	User-Based access management/provisioning	Yes	Yes	Yes	Yes
	Self-Service Password Change for cloud users	Yes	Yes	Yes	Yes
	Identity Synchronization Tool (Windows Server Active Directory integration, Multi Forest)	Yes	Yes	Yes	Yes
	Security Reports	3 Basic Reports	3 Basic Reports	Advanced Security Reports	3 Basic Reports
	Cloud App Discovery*	Yes(Basic)	Yes(Basic)	Yes(Advanced)**	Yes(Basic)
Premium + Basic Features	Group-based access management/provisioning		Yes	Yes	
	Self-Service Password Reset for cloud users		Yes	Yes	
	Company Branding (Logon Pages/Access Panel customization)		Yes	Yes	
	SLA		Yes	Yes	Yes
Premium Features	Identity Synchronization Tool advanced write-back capabilities * (FY15 Roadmap)			Yes	
	Self-Service Group Management			Yes	
	Self-Service Password Reset/Change with on-premises write-back			Yes	
	Advanced Usage Reporting			Yes	
	Multi-Factor Authentication (Cloud and On-premises (MFA Server))			Yes	Limited Cloud only features for accessing Office 365
	Azure Active Directory Application proxy*			Yes	
	MIM CAL + MIM Server			Yes	
	Administrative Delegation* (FY15 Roadmap)			Yes	



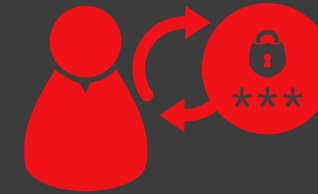
Other premium features

Self service experience for users

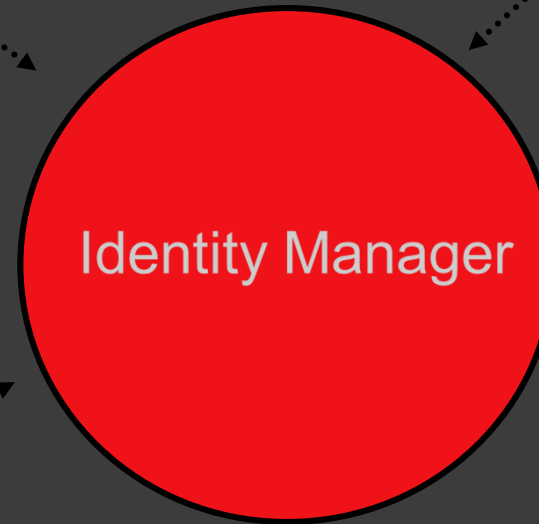
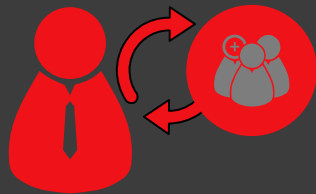
Users can edit their profile details to update and add missing information



Users can reset their passwords significantly reducing help desk burden and costs.



Self-service group management, including dynamic membership calculation in these groups and distribution lists, based on the user's attributes.



Monitor and protect access on go-anywhere devices

Built-in security features, like "you can't be in two places at once".

Security reporting that tracks inconsistent access patterns, analytics and alerts.

Ensure secure access by enabling MFA



Multi-factor authentication

Any two or more of the following factors:

- Something you know: a password or PIN.
- Something you have: a phone, credit card or hardware token.
- Something you are: a fingerprint, retinal scan or other biometric.

Stronger when using two different channels (out-of-band).



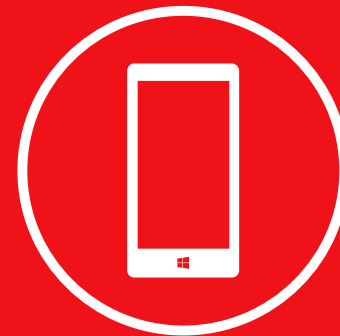
Hardware token



Certificates



Smartcard



Phone

Premium Reports

Premium reports:

- Advanced application usage reporting
- Password reset activity
- Selfservice activity
- Identify unexpected logon behavior

Premium Reports

The screenshot shows a Microsoft Dynamics CRM Premium Report for user PETER DAALMANS. The report is titled "SIGN IN DETAILS" and provides a summary of the user's login activity. The left sidebar contains various system icons, and the right sidebar shows a list of related records. The main content area displays the following information:

- PETER DAALMANS**
- SIGN IN DETAILS**
- REASON**
Signed in from geo-distant locations.
- FIRST SIGN IN FROM**
Breda, Noord-Brabant, NL
- TIME OF FIRST SIGN IN**
9/25/2015 5:09:05 PM
- SECOND SIGN IN FROM**
Redmond, Washington, US
- TIME OF 2ND SIGN IN**
9/25/2015 7:06:03 PM
- TIME BETWEEN SIGN INS**
01:56:58
- ESTIMATED TRAVEL HOURS**
13

The report is displayed in a window titled "admin@emsfans.com". The left sidebar includes a "NEW" button at the bottom. The right sidebar shows a list of records with a search icon and a checkmark icon. The bottom of the window features a status bar with a question mark icon.

Discovery from non-Windows devices

- Cloud App Discovery gateway
- Devices can be configured to go through gateway
- Requires MDM for deployment across organization



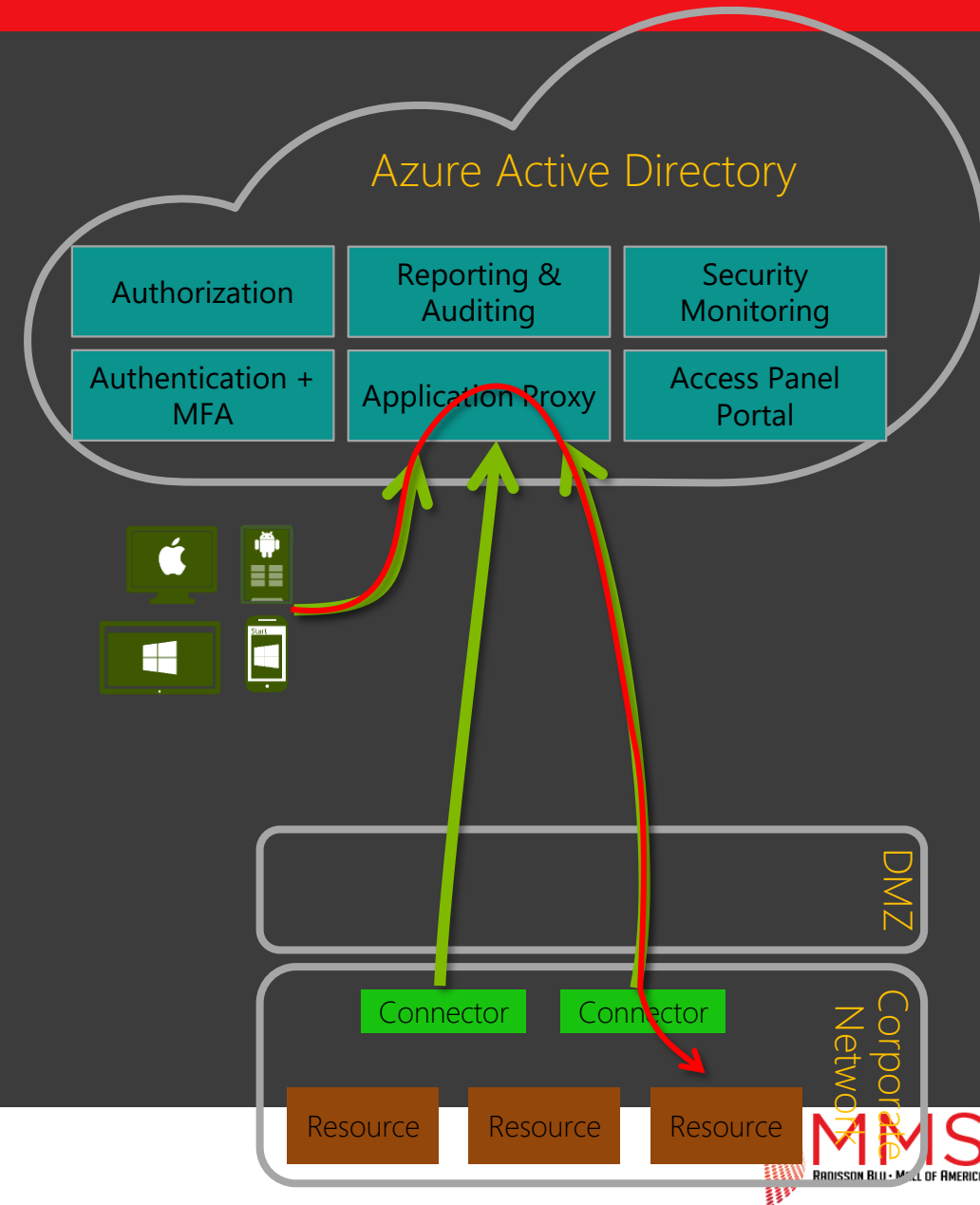
Integrate on-prem apps with Azure AD

End-user portal – Access Panel

Azure AD authentication capabilities:

- Username and password synced from on-prem AD
- Federated login to on-prem or other federation servers
- Multi-factor authentication
- Customized login screen
- Authorization based on user or groups
- SSO to Office365, thousands of SaaS apps and all applications integrated with AAD

Reports, auditing and security monitoring based on big data and machine learning.





Demo

Azure Active Directory Premium

The logo graphic for Microsoft Intune, featuring a stylized, multi-colored (red, orange, yellow) wing-like shape composed of many small, overlapping rectangular segments.

Microsoft Intune

MDM, MAM and more

#MMSMOA

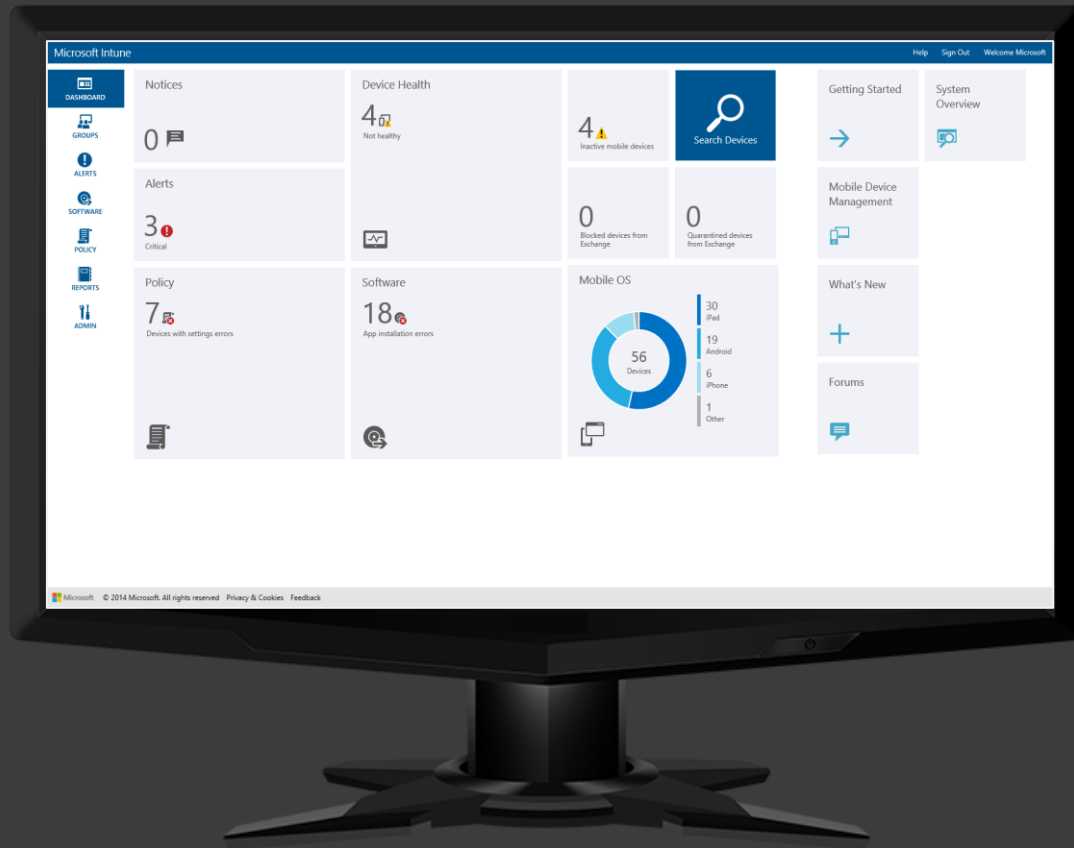
Microsoft Intune

- Mobile Device Management
 - Windows, Windows Phone, IOS and Android
- Policy and Application Management
- Compliance reporting
- Conditional Access to resources
- Selective Wipe Devices
- Hybrid / Cloud solution

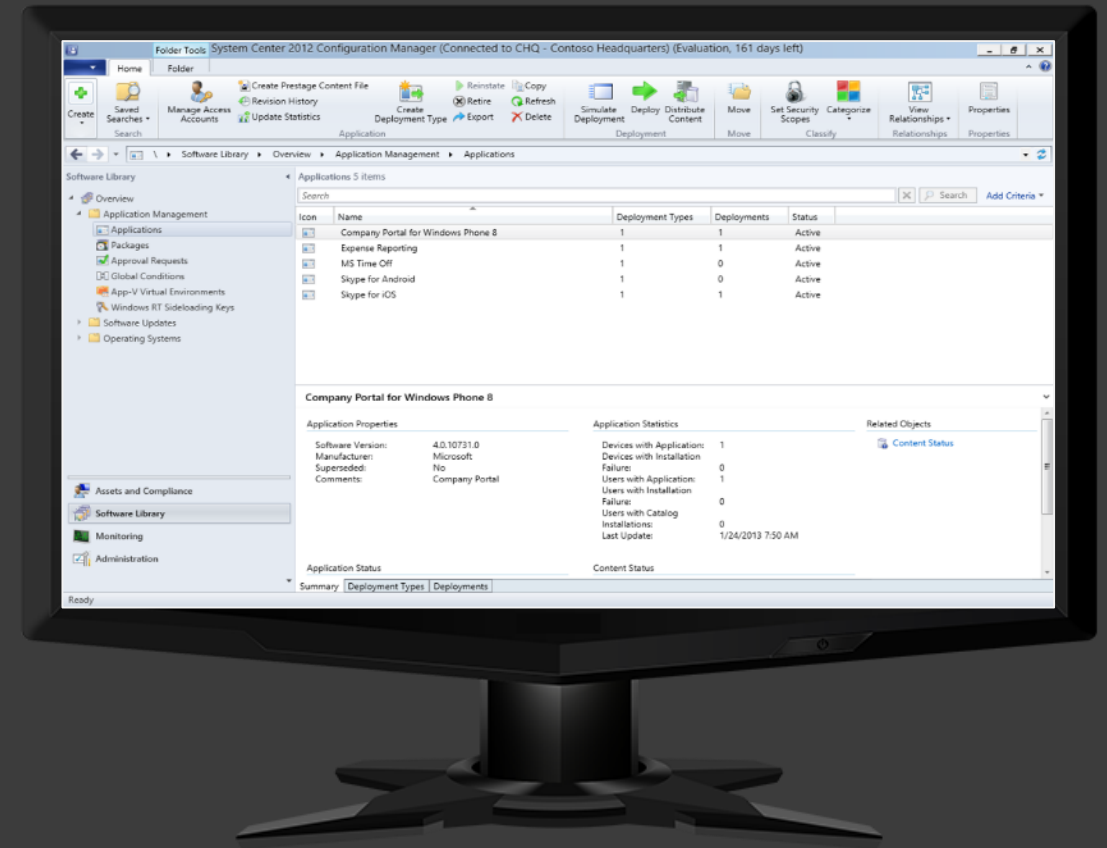


Single management console for IT admins

Intune web console (cloud only)



Configuration Manager console (hybrid)



Comprehensive lifecycle management

▶ Enroll

- Provide a self-service Company Portal for users to enroll devices
- Deliver custom terms and conditions at enrollment
- Bulk enroll devices using Apple Configurator or service account
- Restrict access to Exchange email if a device is not enrolled

▶ Retire

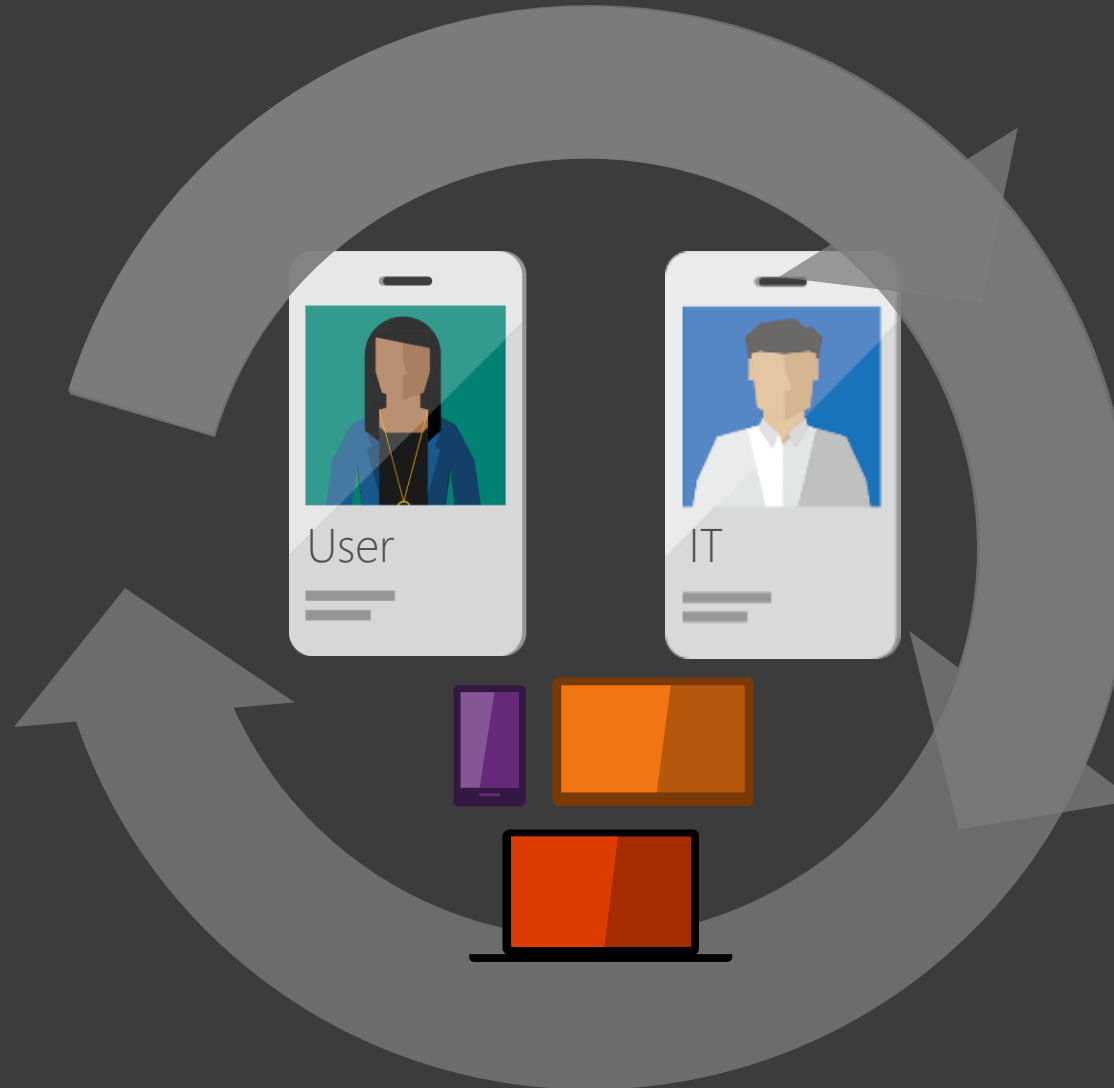
- Revoke access to corporate resources
- Perform selective wipe
- Audit lost and stolen devices

▶ Provision

- Deploy certificates, email, VPN, and WiFi profiles
- Deploy device security policy settings
- Install mandatory apps
- Deploy app restriction policies
- Deploy data protection policies

▶ Manage and Protect

- Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem
- Report on device and app compliance





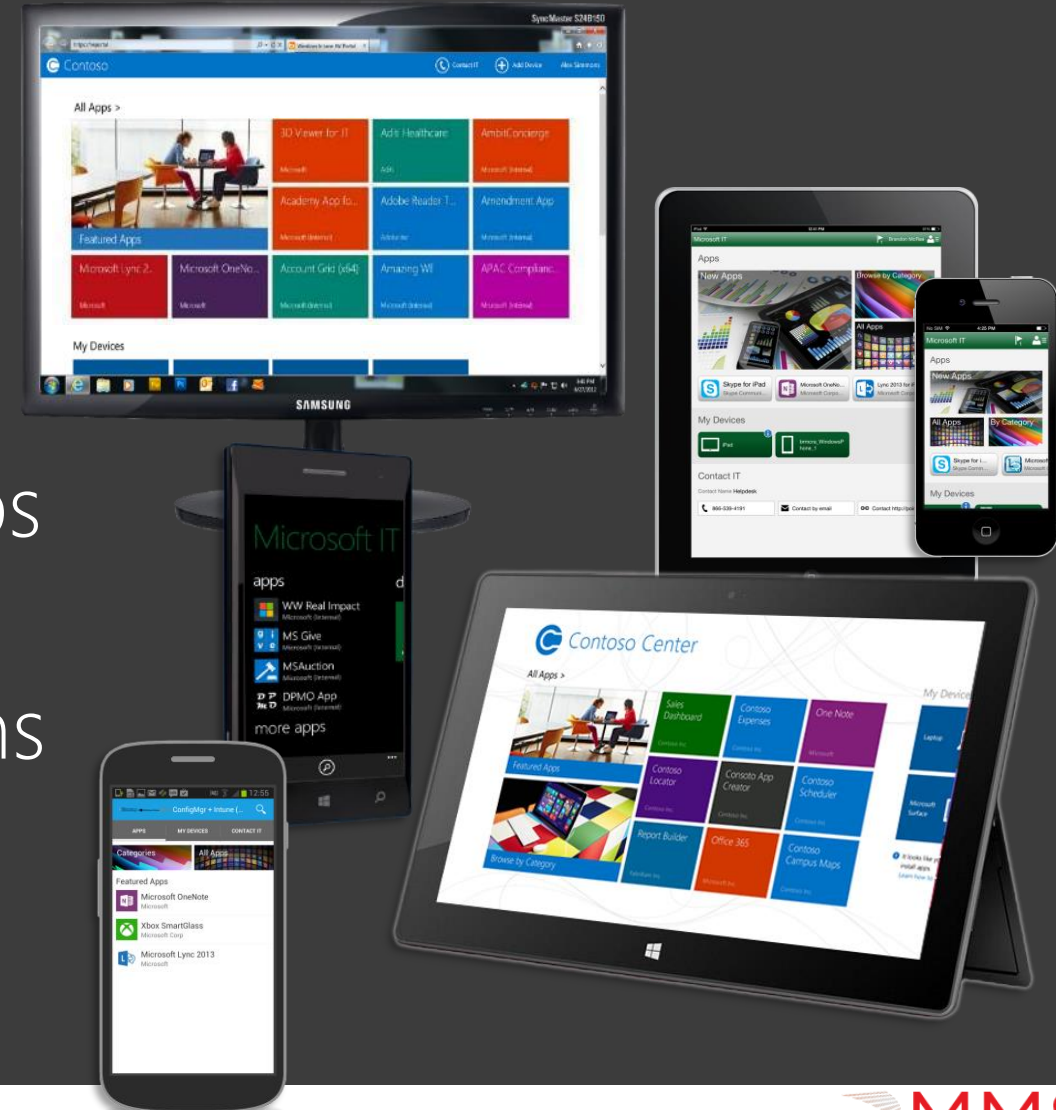
Microsoft Intune

Company Portal(s)

#MMSMOA

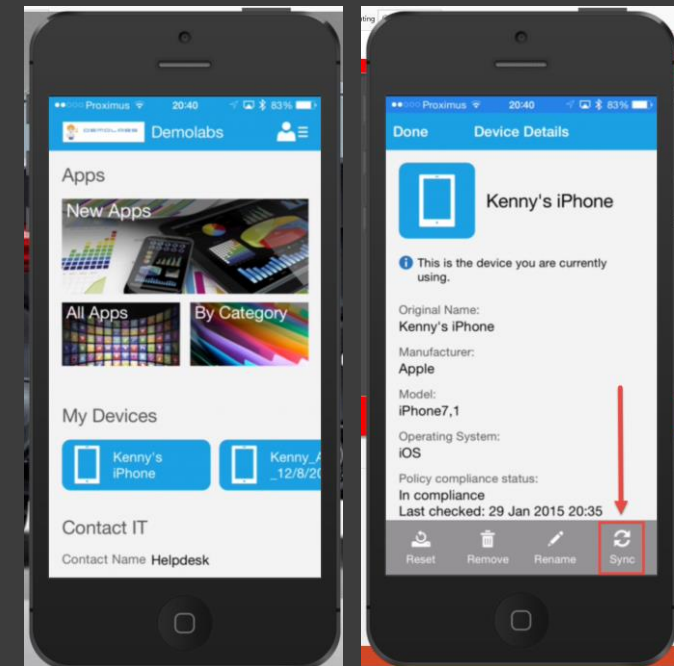
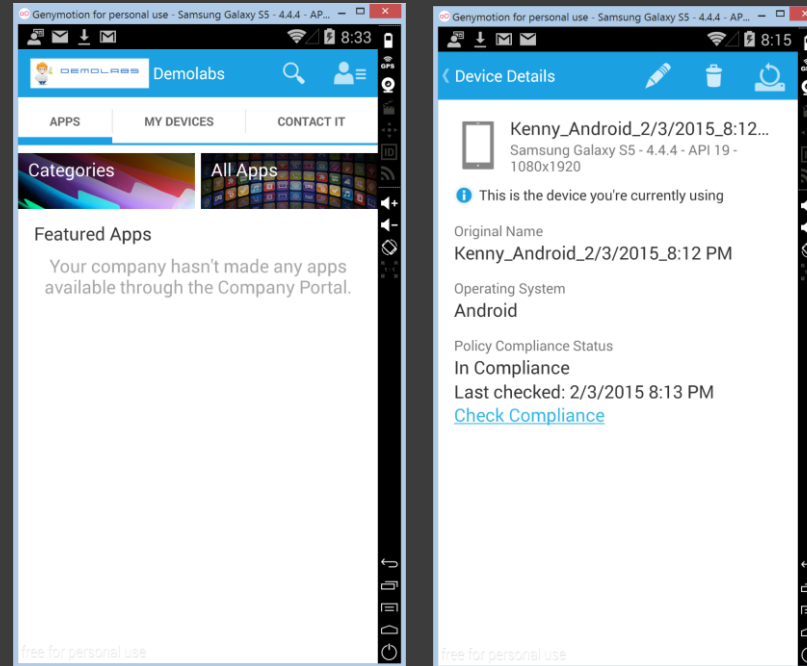
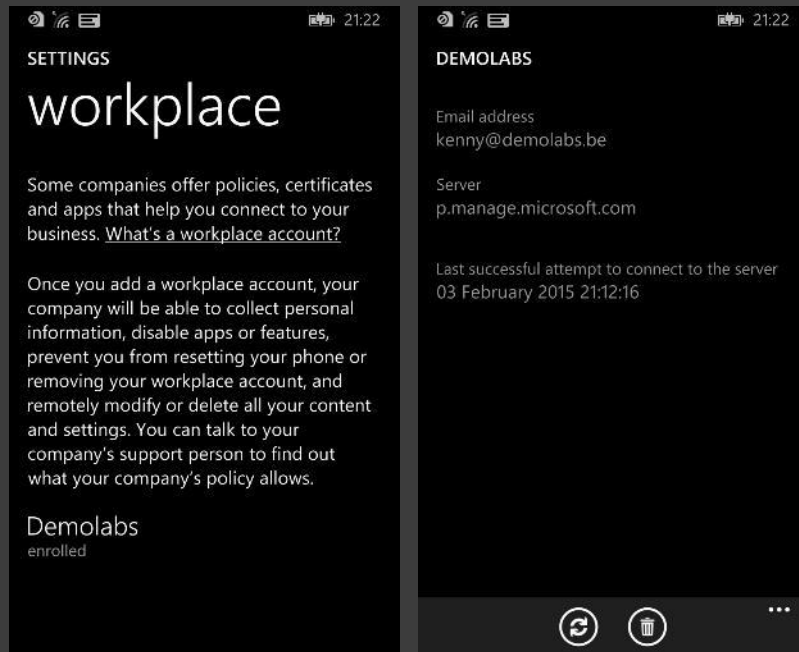
Company portal self-service experience

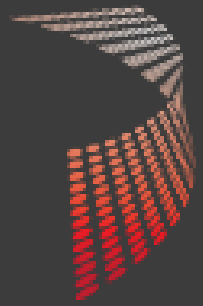
- Consistent experience across:
 - Windows
 - Windows Phone
 - Android
 - iOS
- Discover and install corporate apps
- Manage devices and data
- Customizable terms and conditions
- Ability to contact IT
- Force the Policy refresh



Mobile Device – Portals

All portals offer the same experience
(except for Windows Phone)

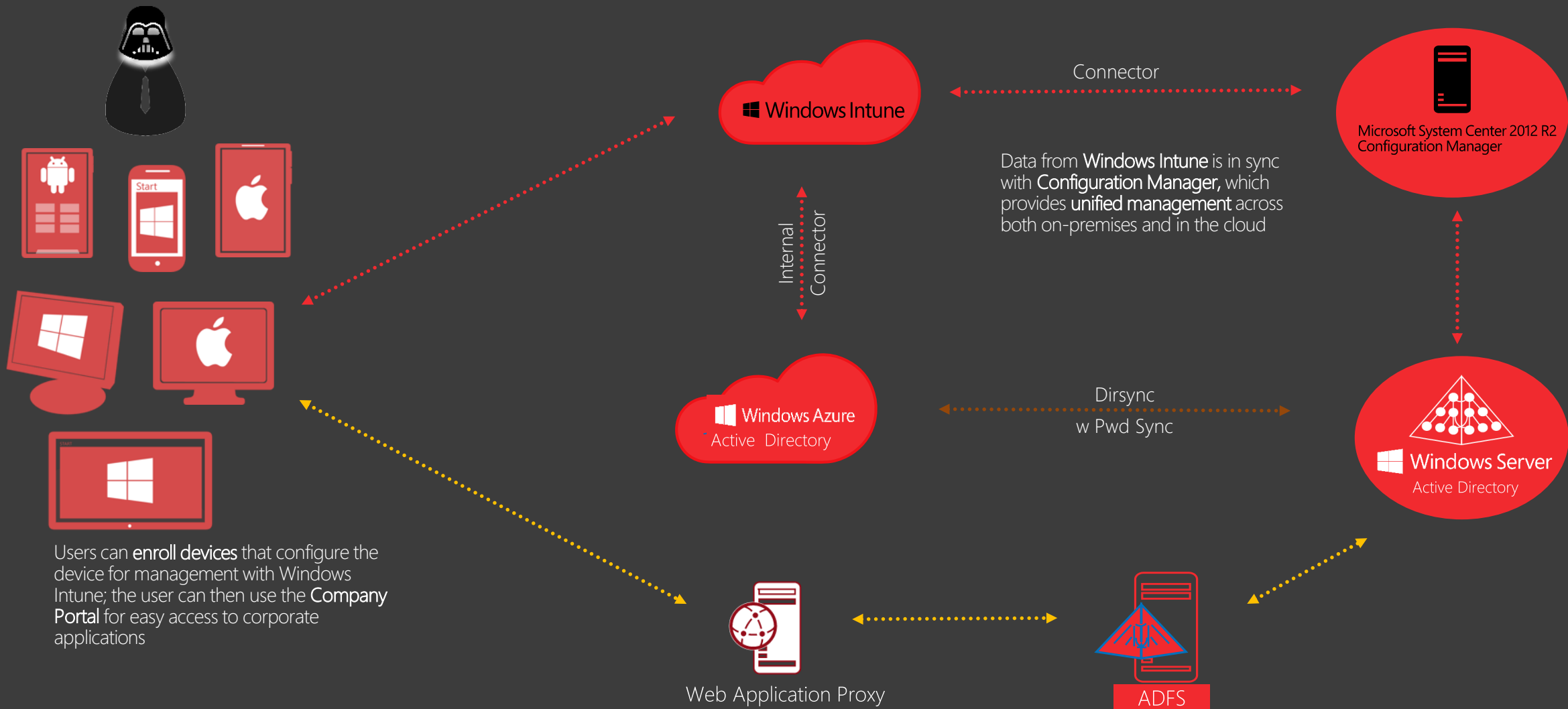




Microsoft Intune

Device Enrolment – The new way
Conditional access

Enrolling Devices



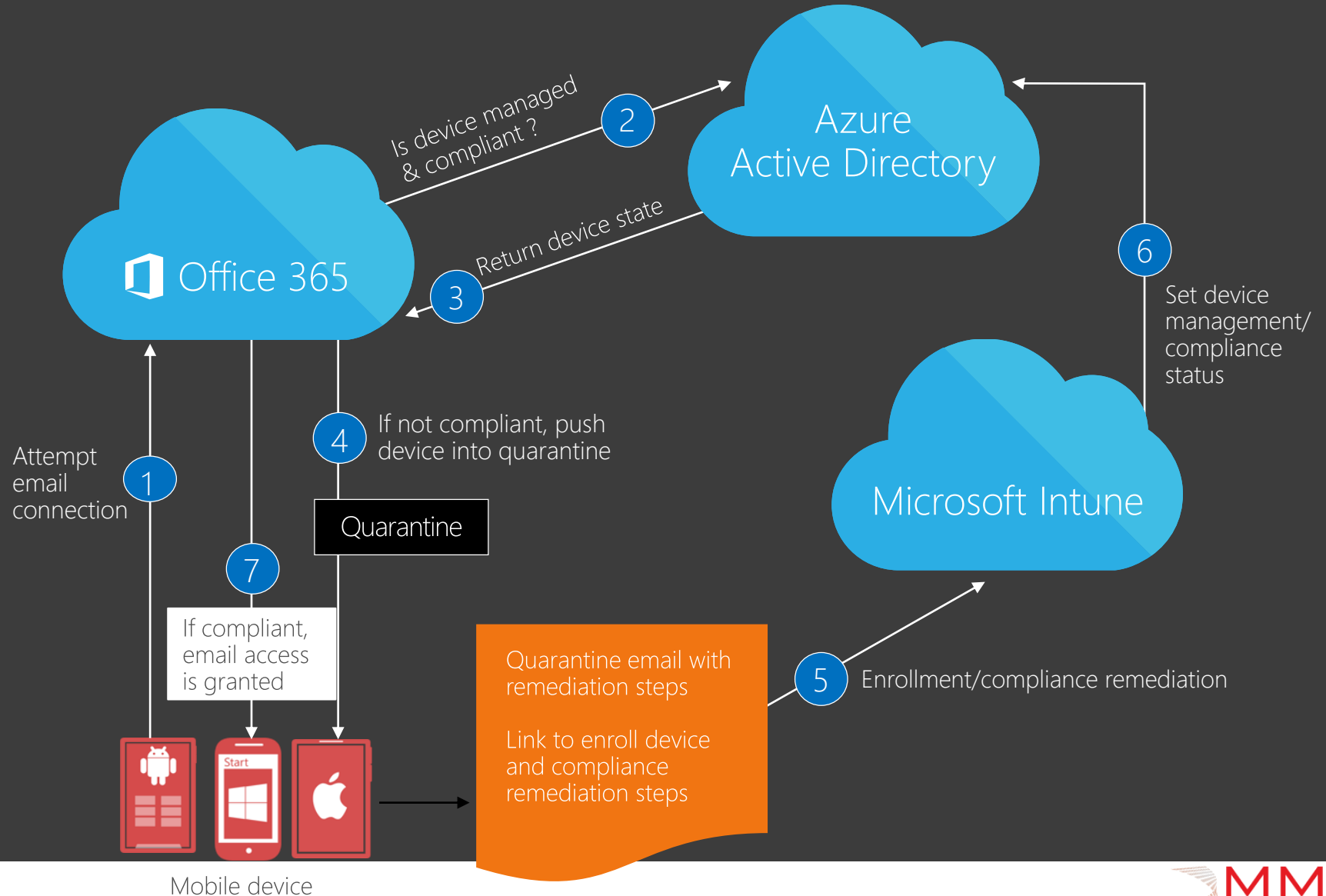
Conditional access for Office 365

Who does what?

Intune: Evaluate policy compliance for device

Azure AD: Authenticate user and provide device compliance status

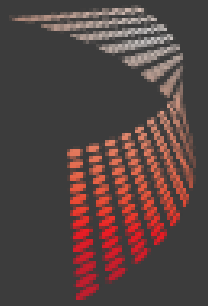
Exchange Online: Enforces access to email based on device state





Demo

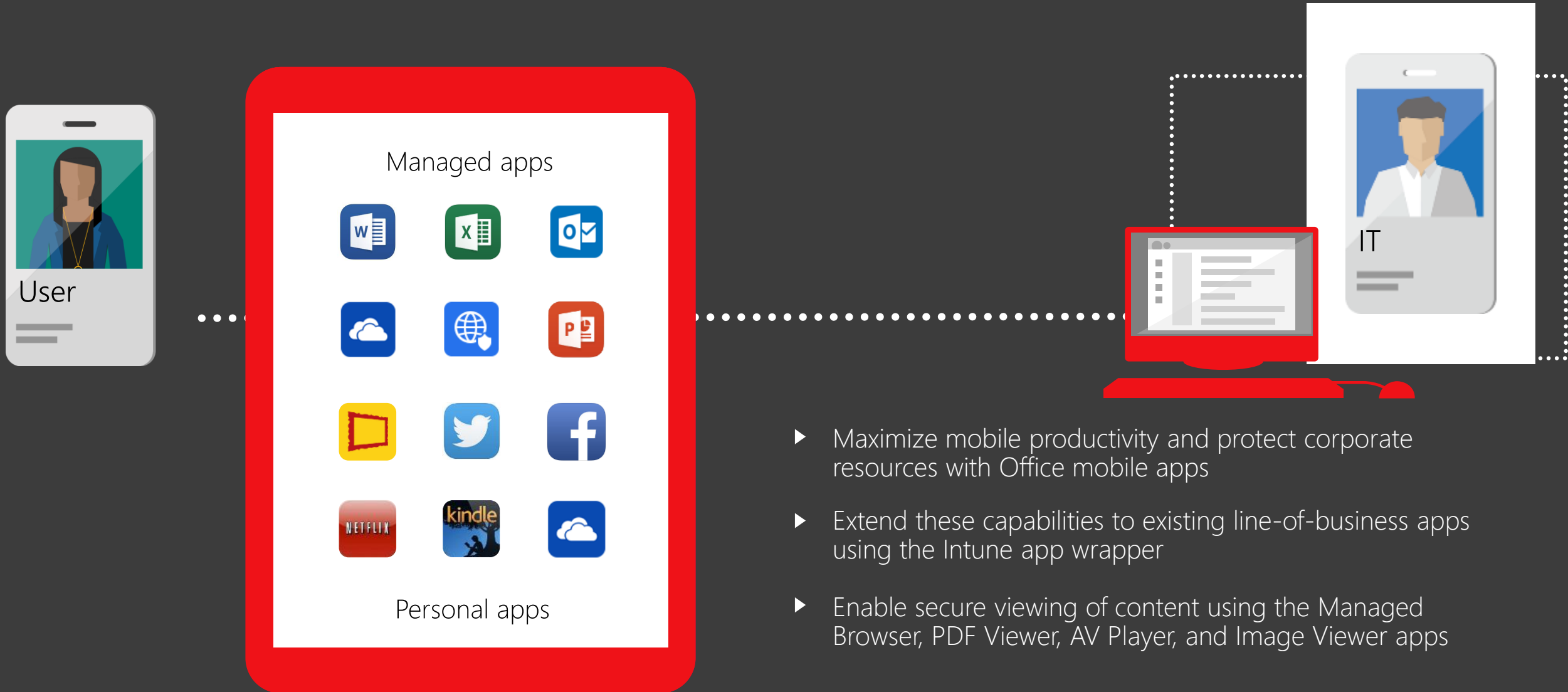
Device Enrolment – The new way
Conditional access



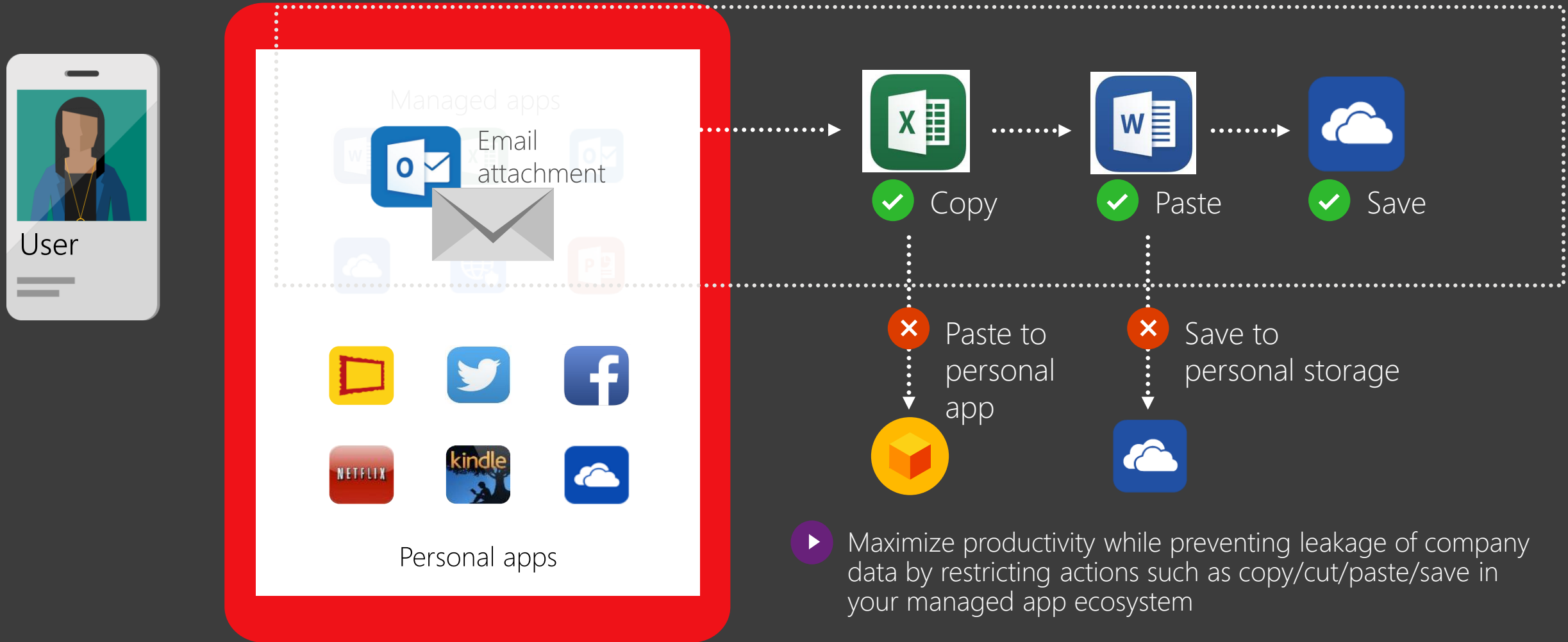
Microsoft Intune

Application Management

Mobile Application Management



Mobile Application Management



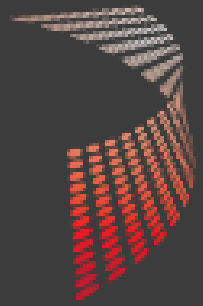
Mobile App Config Policy

- Preconfigure iOS Apps with settings
 - App need to support iOS App Config Policy
 - See for more info: <http://ref.ms/mamlist>



Demo

Mobile Application Management



Microsoft Intune

Soon available: Mac OS X management

Mac OS X support for

- Enrollment
- Deploying policies
- Deploying profiles
- Remote actions
- Reporting



Demo

Mac OS X



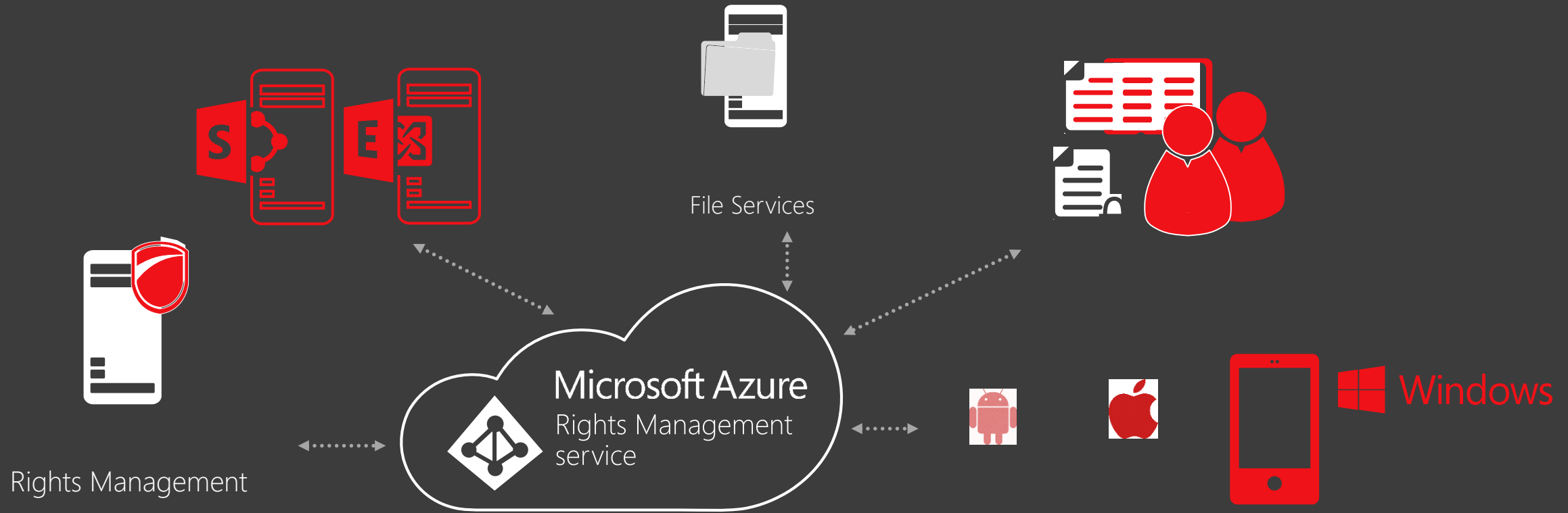
Rights Management

Protecting the data

Microsoft Rights Management

- Encrypt and control
 - Documents
 - Mails
- Prevent unwanted viewing/printing or access to Corporate data

Protect data with Rights Management



Take advantage of **HYBRID** options across Windows Server and Azure Rights Management service

INTEGRATE Microsoft SharePoint and Microsoft Exchange Server

Automatically **IDENTIFY AND CLASSIFY** data based on content with **AUTOMATIC ENCRYPTION**

MORE SECURELY SHARE documents with colleagues and business partners

Improve ease of use through **INTEGRATION WITH OFFICE 2010/13, WINDOWS SHELL** extensions, and **CROSS-PLATFORM CLIENTS**

Integrating RMS into workflows

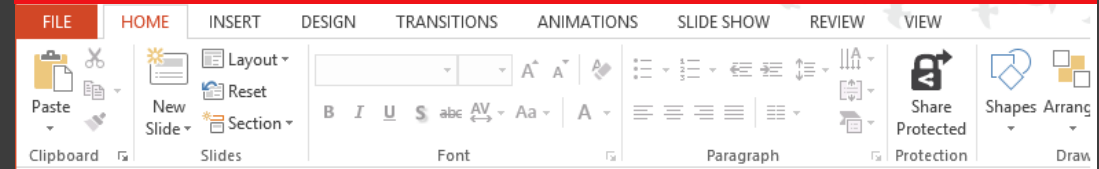


HYBRID OPTIONS ACROSS WINDOWS SERVER
AND MICROSOFT AZURE

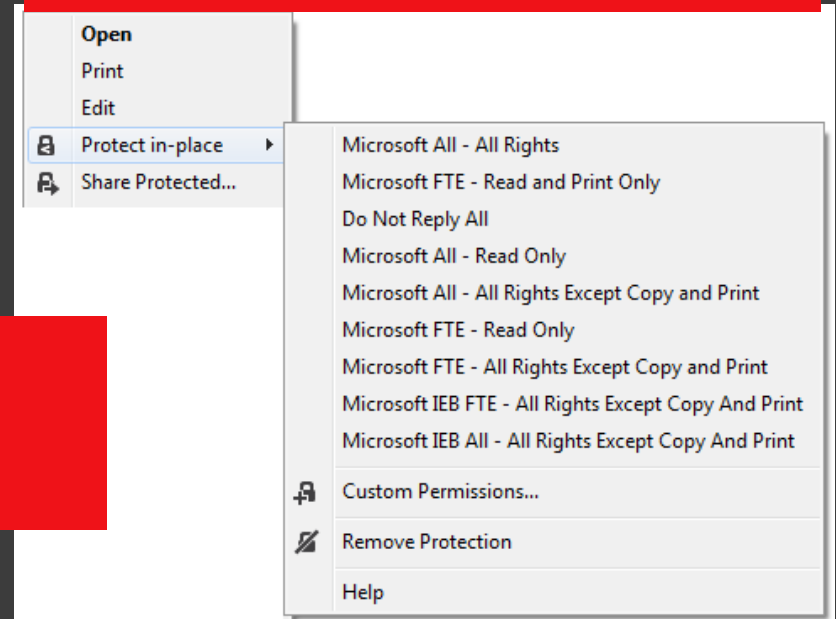
Automatically identify
and classify data
based on content with
automatic encryption

Integration with
Windows Shell, DAC/FCI,
SharePoint and Exchange

Integration with Office 2010/13



Windows Shell Extensions

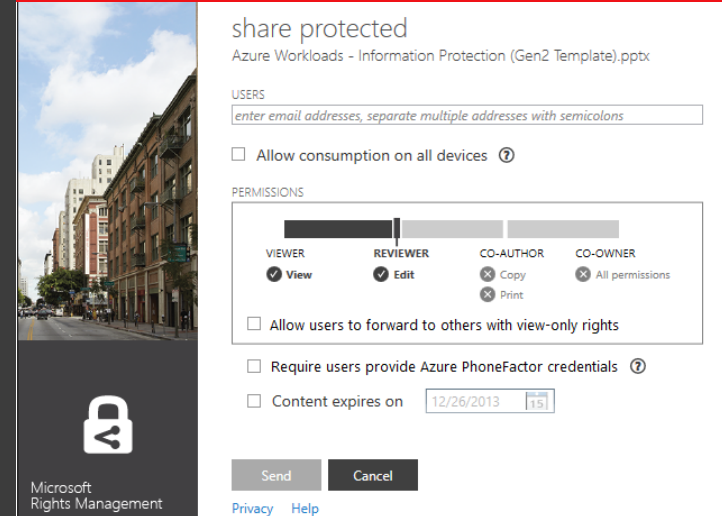


Sharing documents securely

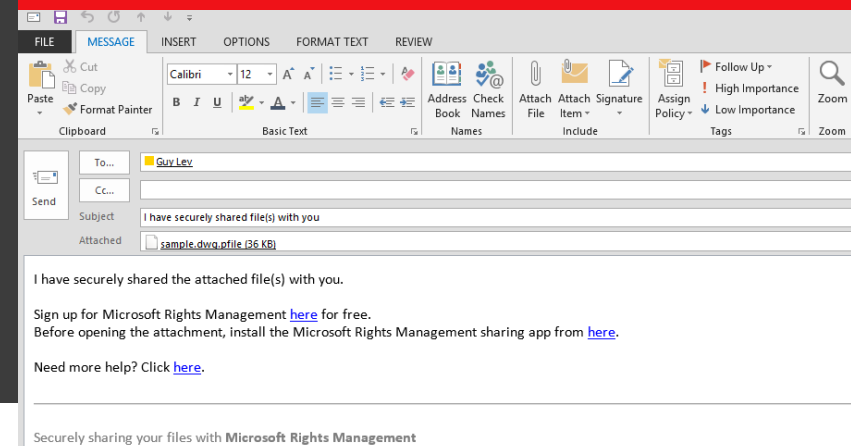


HYBRID OPTIONS ACROSS WINDOWS SERVER AND WINDOWS AZURE TO SECURELY SHARE DOCUMENTS WITH COLLEAGUES AND BUSINESS PARTNERS

Sharing files using Windows Azure RMS



Consuming WA RMS protected files



Consuming AD RMS protected documents in Office 2013



#MMSMOA



Demo

Rights Management



How to get started?

With Microsoft EMS

#MMSMOA

How to get started?

Go to ref.ms/ems > Try now

- Sign up
- Setup AAD Connect (synchronize accounts)
- Set MDM authority
- Configure platforms
- Enroll!

Share your ideas

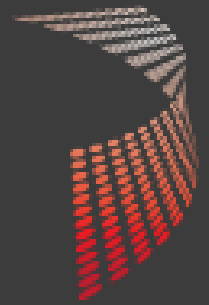
- Share your voice / ideas!
 - <http://microsoftintune.uservoice.com/>
 - <http://configurationmanager.uservoice.com/>





Questions

#MMSMOA



Thank you!

#MMSMOA

Discuss...



Ask your questions-real world answers!
Plenty of time to engage, share knowledge.

Evaluations: Please provide session feedback by clicking the **EVAL** button in the scheduler app (also download slides). One lucky winner will receive a free ticket to the next MMS!

Session Title: What is Microsoft Enterprise Mobility Suite and how to configure it

SPONSORS



