

Conditional Access and Mobile Application Management explained

Peter van der Woude

AZURE
OFFICE 365
ENTERPRISE MOBILITY SUITE
OPERATIONS MANAGEMENT SUITE
AZURE STACK
HYPER-V
WINDOWS



Peter van der Woude

Consultant inovativ
Enterprise Mobility MVP
petervanderwoude.nl
[@pvanderwoude](https://twitter.com/pvanderwoude)



Agenda

- Quick introduction to EMS
- Conditional Access
 - **SharePoint Online**
 - **Exchange Online**
- Mobile Application Management
- Retire Mobile Device
- Questions

NEW



EMS

Enhancing mobile productivity

- **Managing Office mobile apps without MDM:** Microsoft Intune Mobile Application Management (MAM) without requiring the device to be enrolled for management.
- **Managing additional Microsoft apps:** Intune MAM support for additional Microsoft apps, including [Power BI](#) and [Remote Desktop client](#), will be available in the next few weeks. Support for Skype for Business and Dynamics CRM apps is coming soon.
- **Managing 3rd party apps:** Major companies like [Box](#) and [Adobe](#) have announced iOS and Android apps with native support for Intune mobile application management (MAM). Custom [SAP](#) Fiori mobile apps customized and built by SAP's customers using SAP Fiori mobile service will also support these management and data protection capabilities delivered by Microsoft Intune. Additionally, [Acronis](#), [Foxit](#), and [Citrix](#) have integrated support for Intune MAM into their mobile apps.



Quick introduction to EMS



EMS with Office 365



Unify identity

Microsoft Azure

Active Directory Premium



Manage apps & devices

Microsoft Intune



Apply security policies to the
O365 apps on user devices



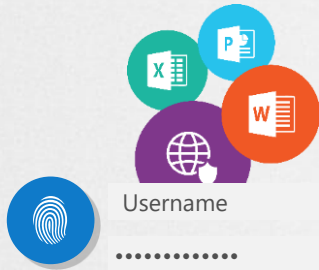
Protect data

Microsoft Azure

Rights Management



Secure and protect data and
documents in O365 apps



Easy, secure access to all
O365 productivity apps

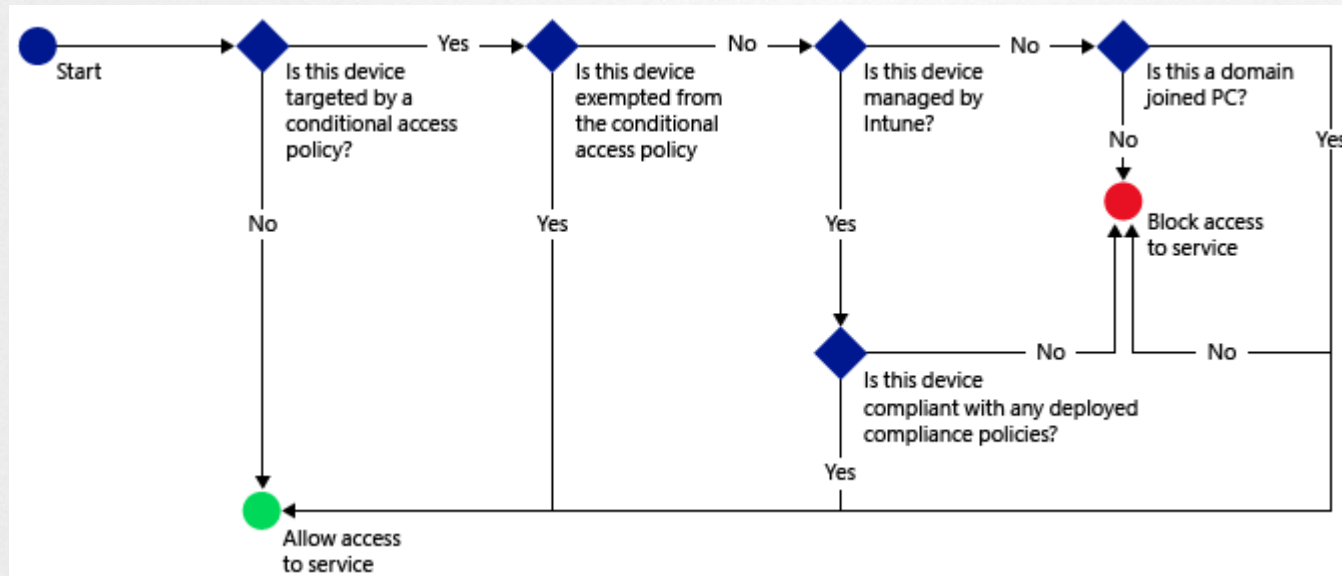


Conditional Access



What is Conditional Access

Conditional access provides access to a service if a device meets specific criteria





Demo

Conditional Access on Exchange Online and Sharepoint Online



Protecting Resources

- Microsoft Exchange On-Premises
 - **Connector required**
- Microsoft Exchange Online
 - **Connector optional**
- Exchange Online Dedicated
 - **Legacy: Connector required**
 - **New: Connector optional**
- Microsoft SharePoint Online
 - **Connector optional**



Policy Types

- Compliance policies
 - Optional policies
 - Deploy to user collections in ConfigMgr or to user groups in Microsoft Intune
- Conditional access policies
 - Required policies
 - Target or exempt Azure Active Directory security user groups



Platform and App Applicability

EXCHANGE ONLINE

- Built-in email client on Android 4.0 and later, Samsung Knox Standard 4.0 and later
- Built-in email client on iOS 7.1 and later
- Built-in email client on Windows Phone 8.1 and later
- Mail application on Windows 8.1 and later
- Microsoft Outlook app for iOS and Android

SHAREPOINT ONLINE

- Microsoft Office Mobile for Android
- Microsoft OneDrive for Android and iOS
- Microsoft Word for iOS
- Microsoft Excel for iOS
- Microsoft PowerPoint for iOS
- Microsoft OneNote for iOS

OFFICE DESKTOP

- Office desktop 2013 and later with modern authentication enabled
- Windows 8.1 and later (when Microsoft Intune enrolled)
- Windows 7.0 and later (when domain joined)

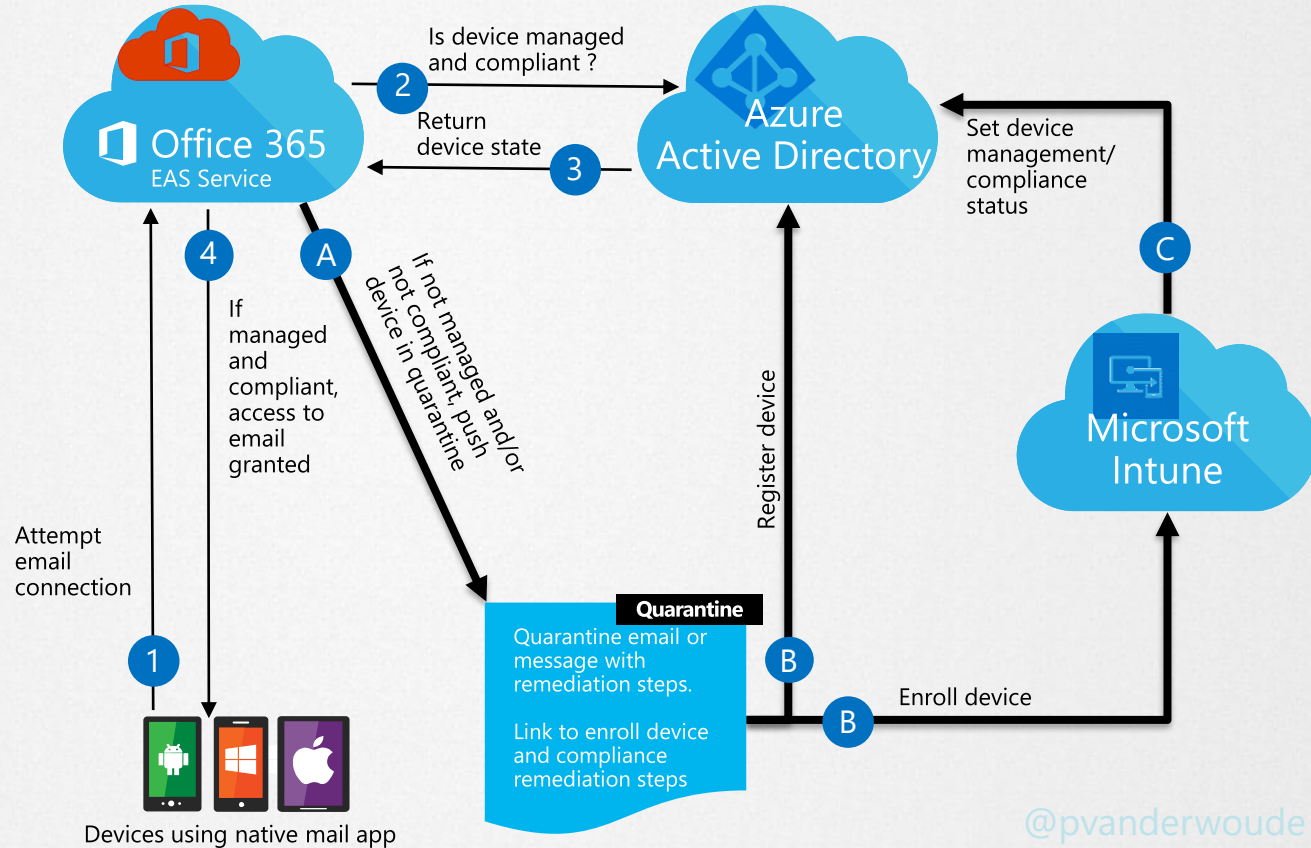
Mail app and Conditional Access

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



Outlook app and Conditional Access

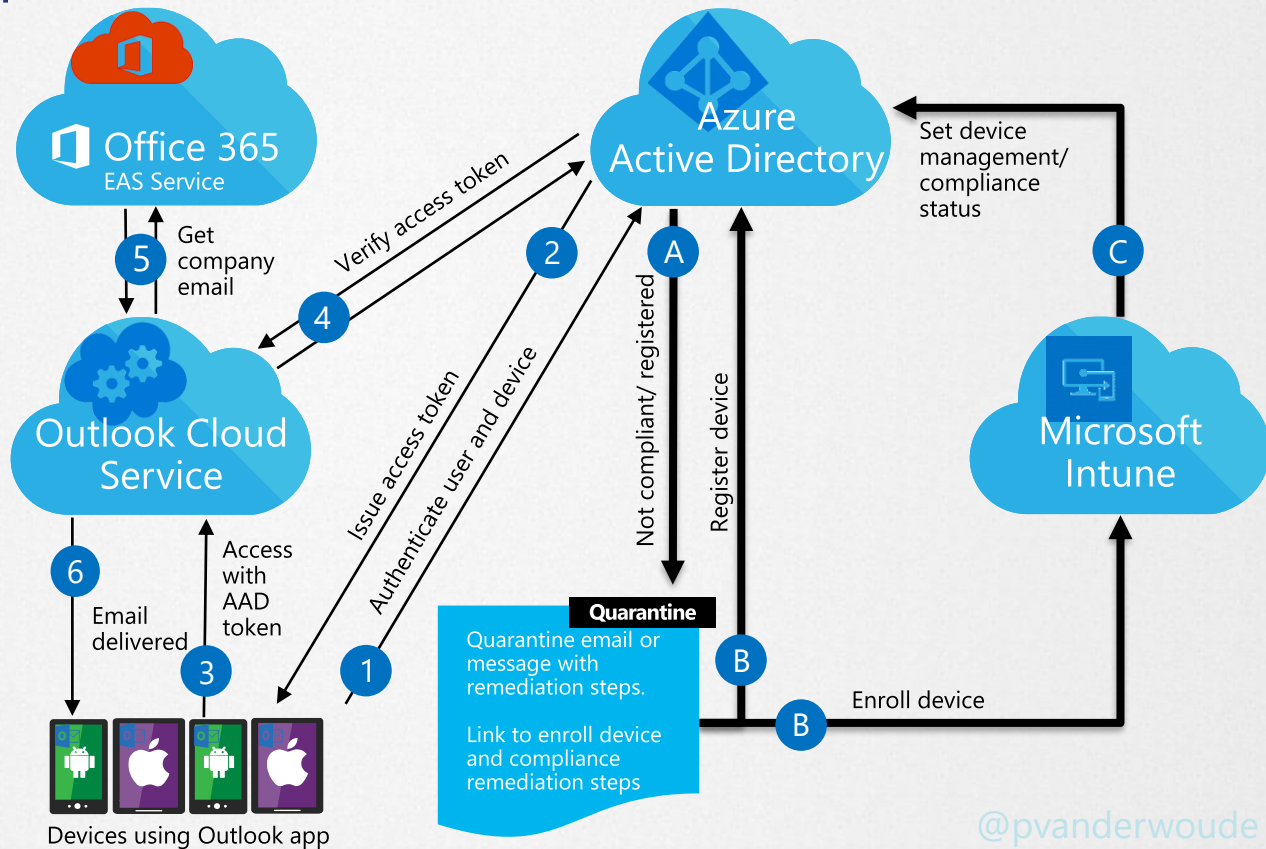
Who does what?

Microsoft Intune:
Evaluate policy compliance for device

Azure Active Directory:
Authenticate user and provide device compliance status

Outlook Cloud Service:
Aggregation service that grabs the company email for the user

Office 365: Provides company email





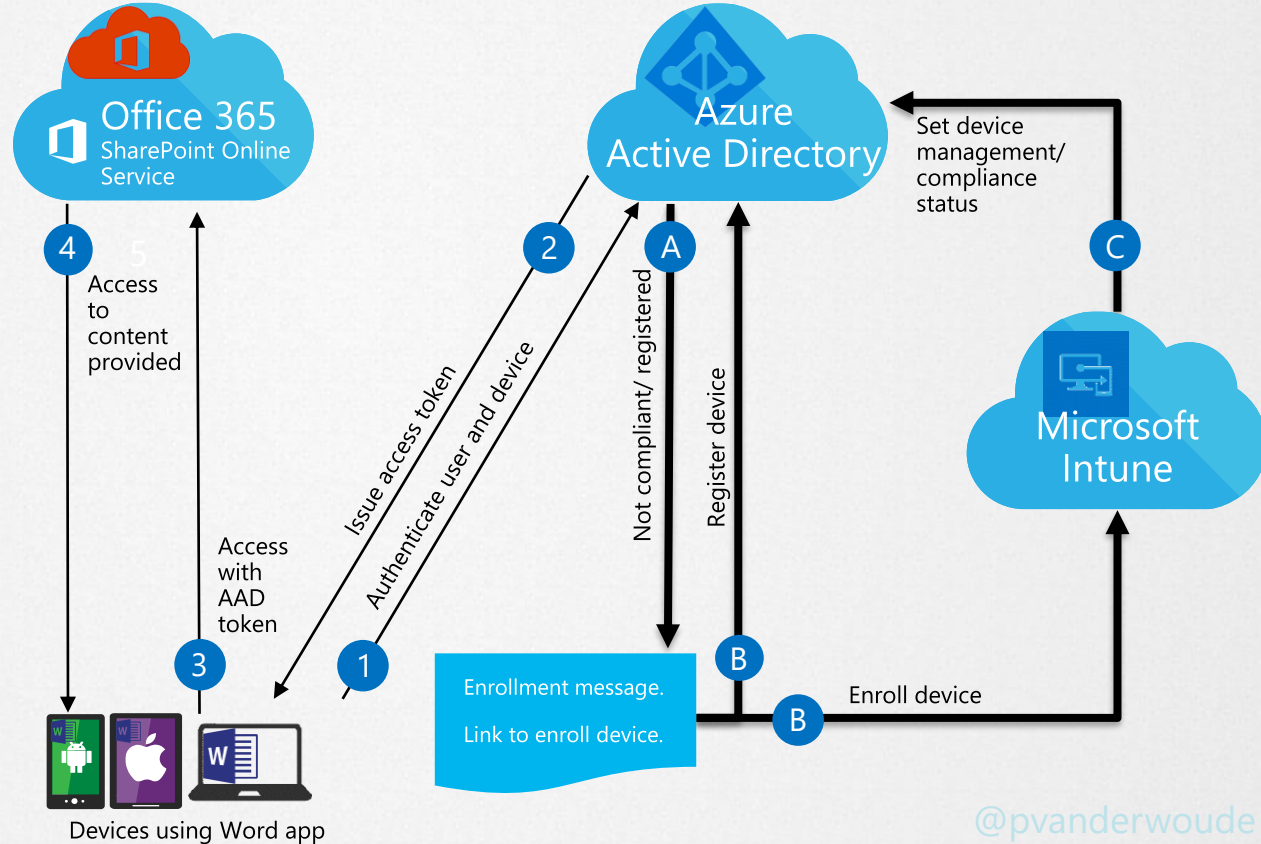
Word app and Conditional Access

Who does what?

Microsoft Intune:
Evaluate policy
compliance for device

Azure Active Directory:
Authenticate user and
provide device
compliance status

Office 365: Provides
access to company
content










Demo

Configuring Conditional Access on Exchange Online and Sharepoint Online



Compliance Policies by Platform

POLICY SETTING					ENVIRONMENT
Require a password to unlock mobile devices	X	X	X	-	Standalone Hybrid
Allow simple passwords	X	-	X	-	Standalone Hybrid
Minimum password length	X	X	X	X	Standalone Hybrid
Required password type	X	-	X	X	Standalone Hybrid
Minimum number of character sets	X	-	X	X	Standalone
Password quality	-	X	-	-	Standalone
Minutes of inactivity before password is required	X	-	-	-	Standalone
Password expiration (days)	X	X	X	X	Standalone
Remember password history	X	X	X	X	Standalone
Prevent reuse of previous passwords	X	X	X	X	Standalone
Require encryption on mobile device	X	X	X	X	Standalone Hybrid
Device must not be jailbroken or rooted	X	X	-	-	Standalone Hybrid
Email account must be managed by Intune	X	-	-	-	Standalone Hybrid
Select the email profile that must be managed by Intune	X	-	-	-	Standalone Hybrid
 Minimum Maximum operating system required	X	X	X	X	Hybrid



Policy check-in frequency

PLATFORM	CHECK-IN FREQ
iOS	Every 6 hours
Android	Every 8 hours
Windows Phone	Every 8 hours
Windows PCs enrolled as devices	Every 24 hours

PLATFORM	FREQUENCY
iOS	Every 15 minutes for 6 hours and then every 6 hours
Android	Every 3 minutes for 15 minutes then every 15 minutes for 2 hours, and then every 8 hours
Windows Phone	Every 5 minutes for 15 minutes then every 15 minutes for 2 hours, and then every 8 hours
Windows PCs enrolled as devices	Every 3 minutes for 30 minutes, and then every 24 hours



Mobile Application Management



What is Mobile Application Management

Mobile app management policies modifies the functionality of apps that are deployed to help bring them into line with the company compliance and security policies

Example: It's possible to restrict cut, copy and paste operations within a managed app, or to configure a managed app to open all web links inside the managed browser.



Mobile application management





Multi-identity Protection

- Identity-level protection
 - Multi-identity extend the Intune data protection capabilities to target corporate identities instead of the complete app



Demo

Mobile Application Management



Platform Applicability

- Devices that run Android 4 and later.
- Devices that run iOS 7 and later





Enabling Protection for Apps

MICROSOFT APPS

- Microsoft Office and productivity apps
- Natively manageable apps with Intune mobile application management
- Same App Store apps for personal and corporate

INTUNE COMPANION APPS

- Support for protected web browsing and content viewing

APP WRAPPING TOOL

- Enables protection for line of business (LOB) apps
- No code changes required

APP SDK

- Includes full DLP for any app
- Requires app participation
- Available for iOS and Android



Managing App-Layer Protection

- Enforce corporate data access requirements
- Prevent data leakage on the device
- Enforce encryption of data at rest
- App-level selective wipe







Demo

Configuring Mobile Application Management Policies



Application Management Policies

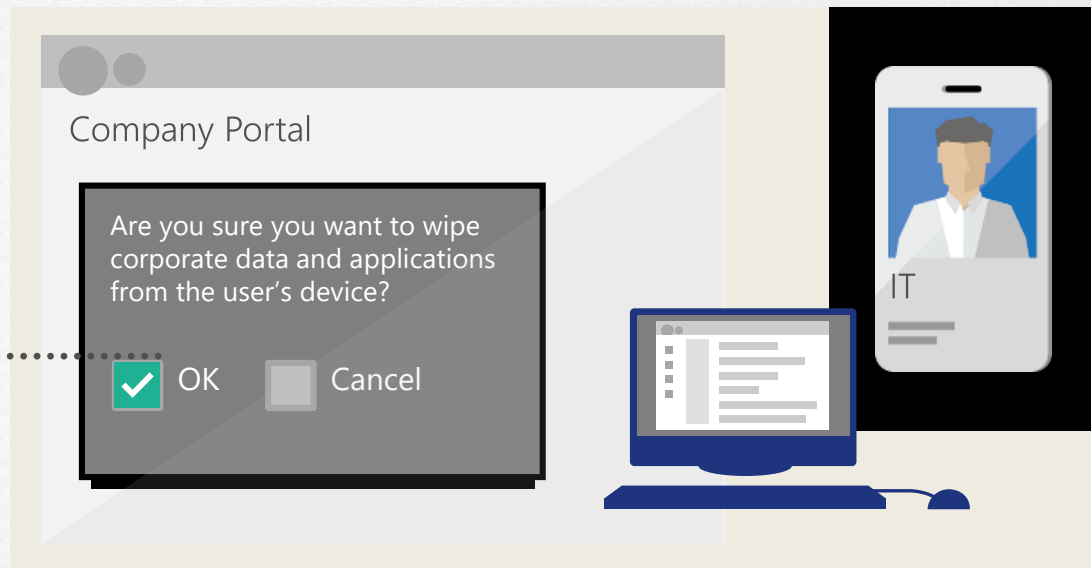
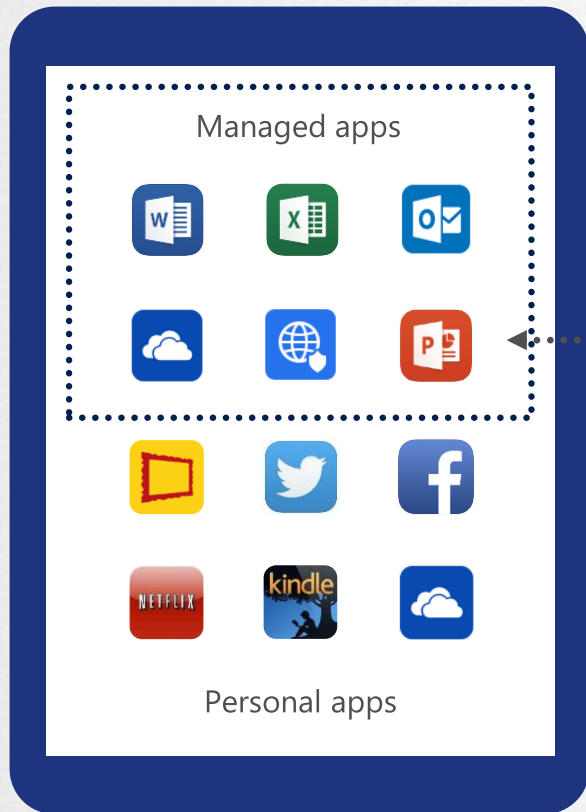
POLICY SETTING					ENVIRONMENT
Restrict web content to display in the Managed Browser	X	X	-	-	Standalone Hybrid
Prevent iTunes and iCloud backups	X	-	-	-	Standalone Hybrid
Prevent Android backups	-	X	-	-	Standalone Hybrid
Allow app to transfer data to other apps	X	X	-	-	Standalone Hybrid
Allow app to receive data from other apps	X	X	-	-	Standalone Hybrid
Prevent "Save Ass"	X	X	-	-	Standalone Hybrid
Restrict cut, copy and paste with other apps	X	X	-	-	Standalone Hybrid
Require simple PIN for access	X	X	-	-	Standalone Hybrid
Number of attempts before PIN reset	X	X	-	-	Standalone Hybrid
Require corporate credentials for access	X	X	-	-	Standalone Hybrid
Require device compliance with corporate policy	X	X	-	-	Standalone Hybrid
Recheck access requirement after (minutes)	X	X	-	-	Standalone Hybrid
Encrypt app data	X	X	-	-	Standalone Hybrid
Block screen capture	X	X	-	-	Standalone Hybrid



Retire Mobile Device



Selective wipe



- ▶ Perform selective wipe via self-service company portal or admin console
- ▶ Remove managed apps and data
- ▶ Keep personal apps and data intact



Demo

Retire Mobile Device



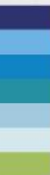
Summarization

- Configuration and impact of conditional access policy for Exchange Online
- Configuration and impact of conditional access policy for SharePoint Online
- Configuration and impact of compliance policies
- Configuration and impact of mobile application management policy
- Configuration and impact of retiring a mobile device

Questions



EMS



Experts Live 2015 wordt mede mogelijk gemaakt door:

Diamond



Platinum

derdack

NUTANIX



VEEAM

Double-Take[®]
by Vision Solutions[®]

inovativ



LIVECARE



Gold



squared•up

Silver



KEMP

Partners

ICT+



Volgende sessie 09:00 – 10:00 uur

Openings keynote

Jeff Woolsey

AZURE
OFFICE 365
ENTERPRISE MOBILITY SUITE
OPERATIONS MANAGEMENT SUITE
AZURE STACK
HYPER-V
WINDOWS