Conditional Access and Mobile Application Management explained

Peter van der Woude
Peter van der Woude

Consultant inovativ
Enterprise Mobility MVP
petervanderwoude.nl
@pvanderwoude
Agenda

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

Protect data
Microsoft Azure
Rights Management

Easy, secure access to all O365 productivity apps

Apply security policies to the O365 apps on user devices

Secure and protect data and documents in O365 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

<table>
<thead>
<tr>
<th>EXCHANGE ONLINE</th>
<th>SHAREPOINT ONLINE</th>
<th>OFFICE DESKTOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Built-in email client on Android 4.0 and later, Samsung Knox Standard 4.0 and later</td>
<td>• Microsoft Office Mobile for Android</td>
<td>• Office desktop 2013 and later with modern authentication enabled</td>
</tr>
<tr>
<td>• Built-in email client on iOS 7.1 and later</td>
<td>• Microsoft OneDrive for Android and iOS</td>
<td>• Windows 8.1 and later (when Microsoft Intune enrolled)</td>
</tr>
<tr>
<td>• Built-in email client on Windows Phone 8.1 and later</td>
<td>• Microsoft Word for iOS</td>
<td>• Windows 7.0 and later (when domain joined)</td>
</tr>
<tr>
<td>• Mail application on Windows 8.1 and later</td>
<td>• Microsoft Excel for iOS</td>
<td></td>
</tr>
<tr>
<td>• Microsoft Outlook app for iOS and Android</td>
<td>• Microsoft PowerPoint for iOS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Microsoft OneNote for iOS</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Apple</th>
<th>Android</th>
<th>Windows</th>
<th>ENVIRONMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require a password to unlock mobile devices</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Allow simple passwords</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Required password type</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Minimum number of character sets</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Password quality</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Minutes of inactivity before password is required</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Password expiration (days)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Remember password history</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Prevent reuse of previous passwords</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Require encryption on mobile device</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Device must not be jailbroken or rooted</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Email account must be managed by Intune</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Select the email profile that must be managed by Intune</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Minimum</td>
<td>Maximum operating system required</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### Policy check-in frequency

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>CHECK-IN FREQ</th>
<th>PLATFORM</th>
<th>FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>Every 6 hours</td>
<td>iOS</td>
<td>Every 15 minutes for 6 hours and then every 6 hours</td>
</tr>
<tr>
<td>Android</td>
<td>Every 8 hours</td>
<td>Android</td>
<td>Every 3 minutes for 15 minutes then every 15 minutes for 2 hours, and then every 8 hours</td>
</tr>
<tr>
<td>Windows Phone</td>
<td>Every 8 hours</td>
<td>Windows Phone</td>
<td>Every 5 minutes for 15 minutes then every 15 minutes for 2 hours, and then every 8 hours</td>
</tr>
<tr>
<td>Windows PCs enrolled as devices</td>
<td>Every 24 hours</td>
<td>Windows PCs enrolled as devices</td>
<td>Every 3 minutes for 30 minutes, and then every 24 hours</td>
</tr>
</tbody>
</table>
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

Managed apps

- Maximize mobile productivity and protect corporate resources with Office mobile apps
- Extend these capabilities to existing line-of-business apps using the Intune app wrapper
- Enable secure viewing of content using the Managed Browser, PDF Viewer, AV Player, and Image Viewer apps

Personal apps
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

<table>
<thead>
<tr>
<th>MICROSOFT APPS</th>
<th>INTUNE COMPANION APPS</th>
<th>APP WRAPPING TOOL</th>
<th>APP SDK</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Microsoft Office and productivity apps</td>
<td>• Support for protected web browsing and content viewing</td>
<td>• Enables protection for line of business (LOB) apps</td>
<td>• Includes full DLP for any app</td>
</tr>
<tr>
<td>• Natively manageable apps with Intune mobile application management</td>
<td></td>
<td>• No code changes required</td>
<td>• Requires app participation</td>
</tr>
<tr>
<td>• Same App Store apps for personal and corporate</td>
<td></td>
<td></td>
<td>• Available for iOS and Android</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>POLICY SETTING</th>
<th>ENVIRONMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict web content to display in the Managed Browser</td>
<td>X</td>
</tr>
<tr>
<td>Prevent iTunes and iCloud backups</td>
<td>-</td>
</tr>
<tr>
<td>Prevent Android backups</td>
<td>X</td>
</tr>
<tr>
<td>Allow app to transfer data to other apps</td>
<td>-</td>
</tr>
<tr>
<td>Allow app to receive data from other apps</td>
<td>X</td>
</tr>
<tr>
<td>Prevent “Save Ass”</td>
<td>-</td>
</tr>
<tr>
<td>Require simple PIN for access</td>
<td>X</td>
</tr>
<tr>
<td>Number of attempts before PIN reset</td>
<td>X</td>
</tr>
<tr>
<td>Require corporate credentials for access</td>
<td>X</td>
</tr>
<tr>
<td>Require device compliance with corporate policy</td>
<td>X</td>
</tr>
<tr>
<td>Recheck access requirement after (minutes)</td>
<td>X</td>
</tr>
<tr>
<td>Encrypt app data</td>
<td>X</td>
</tr>
<tr>
<td>Block screen capture</td>
<td>X</td>
</tr>
</tbody>
</table>

Standalone | Hybrid
Retire Mobile Device
Selective wipe

Are you sure you want to wipe corporate data and applications from the user’s device?

- OK
- Cancel

- 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
Experts Live 2015 wordt mede mogelijk gemaakt door:

Diamond

Microsoft

hp

Platinum

derdack

Nutanix

Trend Micro

Veeam

Double-Take

Inovativ

LiveCare

Gold

Barracuda

OpsLogix

Squared-Up

Silver

cireson

KEMP

Partners

ICT

@pvanderwoude
Volgende sessie 09:00 – 10:00 uur

Openings keynote

Jeff Woolsey