

# Motion 10





*Complexity is the worst enemy of Security.*

*In this digital world, your users are the Firewall*

-Anonymous



# Windows Information Protection

Microsoft Intune, Application Protection policies



# Albert Hoitingh

Solution Architect

Microsoft MVP Enterprise Mobility  
Microsoft Certified Security Administrator Associate

Internationaal spreker

Blog: <https://Alberthoitingh.com>

Twitter: @Alberthoitingh

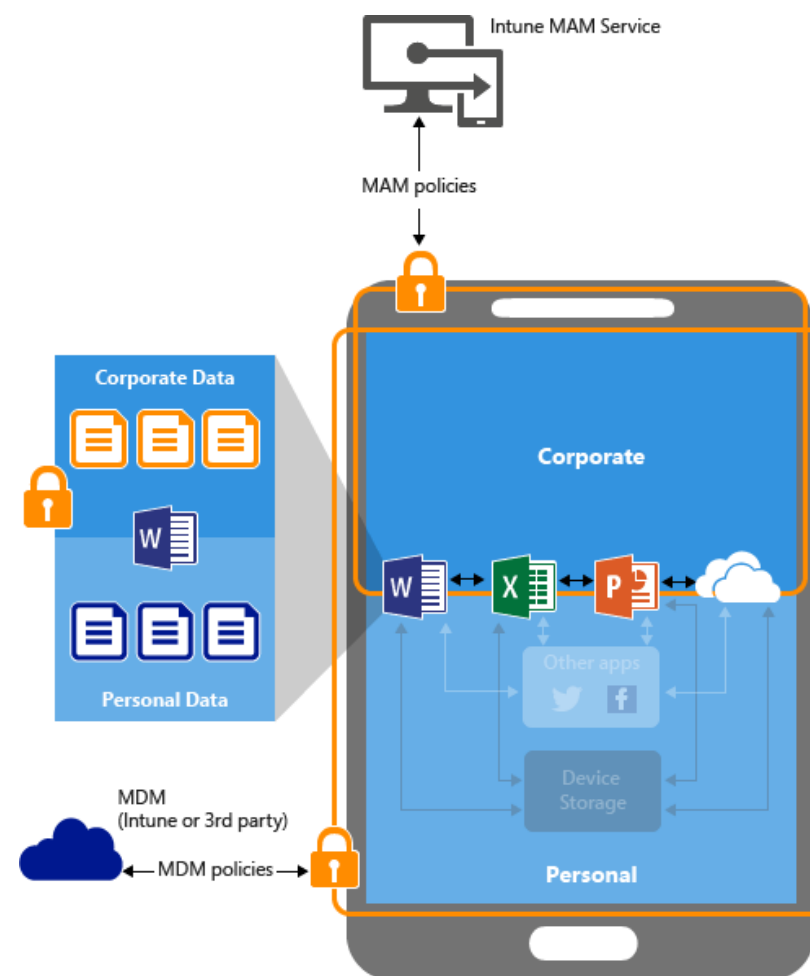
Mail: [Albert.Hoitingh@Motion10.com](mailto:Albert.Hoitingh@Motion10.com)



# Vier punten om mee te nemen

Oftewel “key take-aways”

1. Nieuws vanuit Microsoft Information Protection
2. Het concept achter Windows Information Protection
3. Hoe werkt het?
4. Hoe kunnen onze beheerders het inrichten?





# Wat meer context

## Microsoft Information Protection



What Consistent content detection and classification to protect and preserve sensitive data

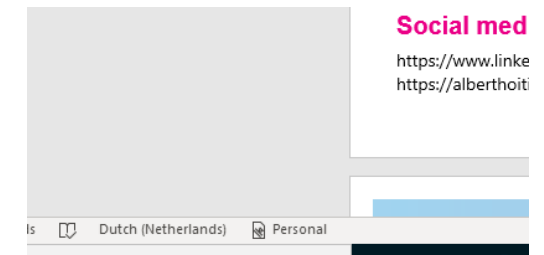
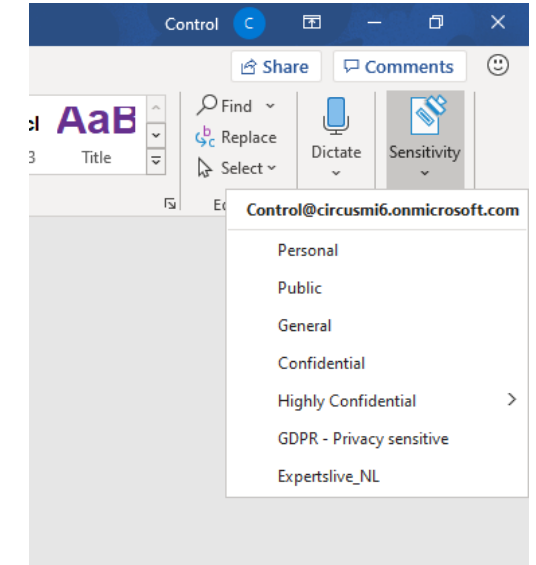
Where Office 365 apps & services, Windows clients & desktops, mobile, on premises + 3<sup>rd</sup> party apps and services

How Microsoft 365 Security and Compliance Center

# Nieuws van Azure Information Protection

Mooie nieuwe dingen 😊

- UL scanner nu in preview
- Client integratie in alle Office versies
- Laatste (preview) versie voor UL client (V2.4.38.0 - 17/09/2019)
- Nieuwe parameters voor Set-AIPAuthentication
- Informatie wordt verstuurd naar Azure Information Protection analytics.
- De kleur van het label wordt getoond
- Nieuw cmdlet (Export-AIPLogs) – maakt een zip-bestand van de lokale logs (tbv. Microsoft Support)

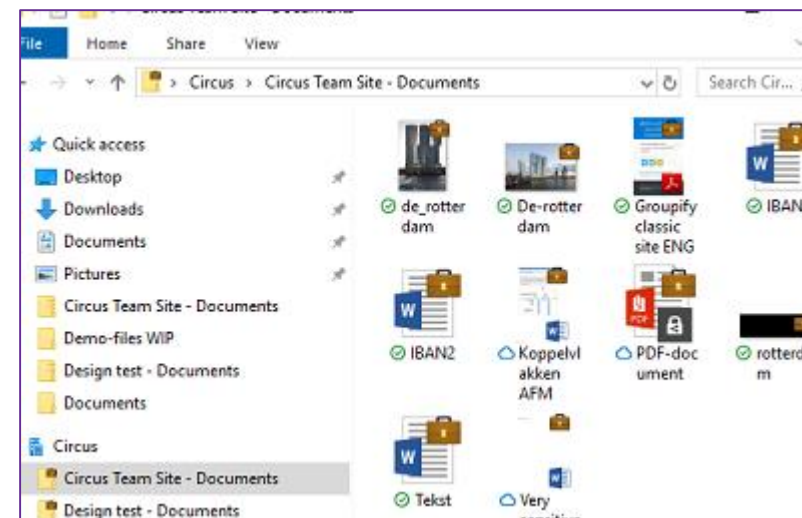






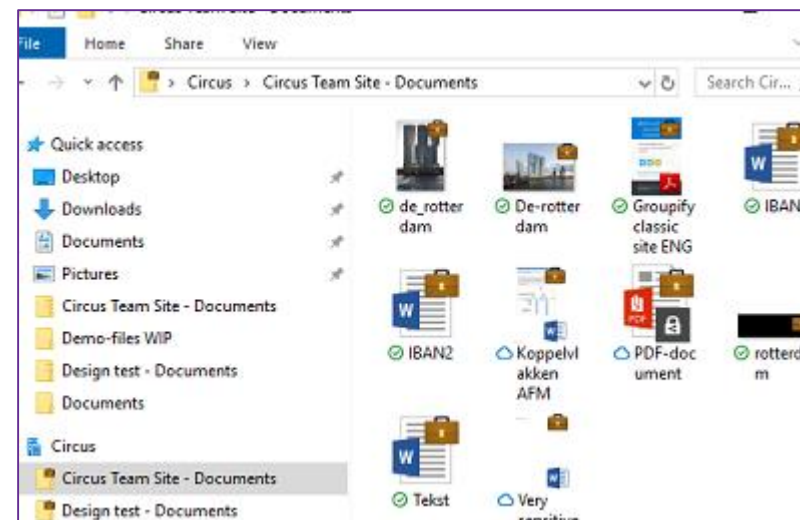
# Het concept in een notedop

- Beschermdde locaties
- “Slimme” toepassingen
- Beschermdde (versleutelde) documenten (het koffertje) op het device
- Informatie uit een beschermd document mag niet naar een onbeschermd locatie (bijvoorbeeld)
- Een document kan worden omgezet naar “bedrijfsdocument”



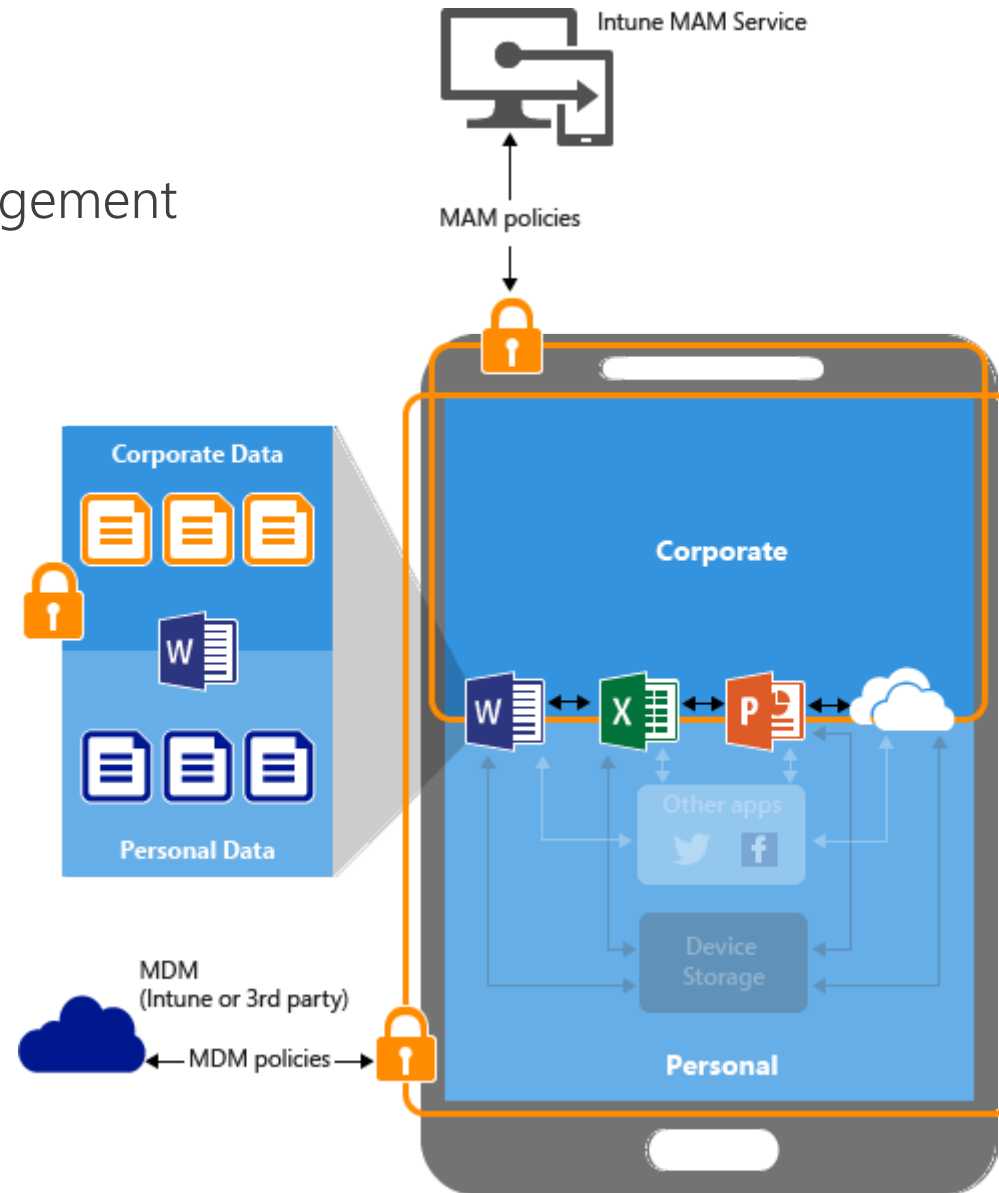
# Het concept in een notedop

- Mobile Application Management (MAM)
- Microsoft Intune, SCCM of 3rd party MDM
- Windows 10 (1607 of hoger)



# Intune

## Mobile Application Management





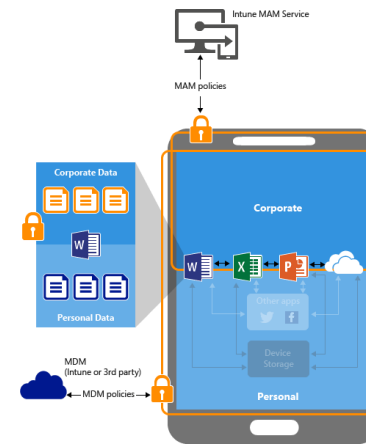
# MDM vs. MAM

## Mobile Application Management (without enrollment)

- Additionele instellingen voor Windows Hello for Business;
- Geselecteerd wissen van (organisatie) informatie;
- Eén gebruiker per device;
- Alleen zogenaamde enlightened apps.

## Mobile Device Management (with enrollment)

- Ondersteunt BitLocker CSP policies.



## Beide

- Azure Active Directory (Azure AD) Premium license.
- Beide in gebruik? MDM gaat voor bij Azure AD joined devices. MAM gaat voor bij workplace-joined devices.

# Demo Windows 10

# Inrichten



- Intune portal
- Assignments
- Protected apps
- Advanced settings

Dashboard > Microsoft Intune > Client apps - App protection policies

### Client apps - App protection policies

Microsoft Intune

Search (Ctrl+/)

Overview

Manage

- Apps
- App protection policies
- App configuration policies
- App selective wipe
- iOS app provisioning profiles

+ Create policy Refresh Columns Export

Filter by Policy Name...

POLICY	DEPLOYED	UPDATED	PLATFORM	MANAGEMENT TYPE
OneDrive mobile policy	Global	11/08/18, 3:14 PM	iOS, Android	Not Available
Sensitive labels	No	3/01/19, 5:20 PM	Windows 10	With enrollment
Windows Information Protection	Yes	3/11/19, 8:59 AM	Windows 10	With enrollment



Demo Intune

# Integratie met Office 365

- Office 365 sensitivity labels
- Windows Defender ATP detecteert label
- Op basis van label instelling wordt document gemarkeerd als "gevoelig"
- En krijgt het document het "koffer"icoon ☺



# Wat kan er mis gaan?

- Data op een USB stick;
- Direct Access is niet compatible
- Een **NetworkIsolation** Group Policy gaat voor
- **Cortana** is potentieel gevaarlijk
- Eén gebruiker per device
- Installatiemedia gekopieerd vanaf een network share
- Het wijzigen van de primaire Identiteit wordt niet ondersteund;
- Client Side Caching is niet compatible
- **Microsoft Edge** of **Internet Explorer** werken minder goed (zucht....)
- Let op met ActiveX controls;
- Resilient File System (**ReFS**) wordt niet ondersteund;
- De setting **MakeFolderAvailableOfflineDisabled** op **False** zet WIP uit indien bepaalde locaties zijn opgenomen;
- Alleen enlightened apps worden beheerd zonder het device aan te melden;
- Bestanden in %windir% of C:/Windows worden niet versleuteld.

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/limitations-with-wip>



# Troubleshoot



- MDM log bekijken (Access work or school)
- Let op /\*AppCompat\*/

## Connection info

Management Server Address:

[Redacted]

Exchange ID:

[Redacted]

## Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

Create report

# Demo

# Dank jullie wel!

## Contact?

Blog: <https://Alberthoitingh.com>

Twitter: @Alberthoitingh

E-mail: [albert.Hoitingh@motion10.com](mailto:albert.Hoitingh@motion10.com)

