

A stylized illustration on the left side of the slide shows a blue silhouette of a person climbing a tree. The tree is composed of several thick, vertical lines in shades of green and blue, representing tree trunks. Swirling around these trunks are several thick, curved lines in shades of blue and purple, representing vines or branches. The person is positioned on one of the vertical lines, with their arms and legs extended as if climbing.

A safari through the Intune device management scenario jungle

Nicola Suter

Workplace Engineer itnetX (Switzerland) AG

Blog tech.nicolonsky.ch

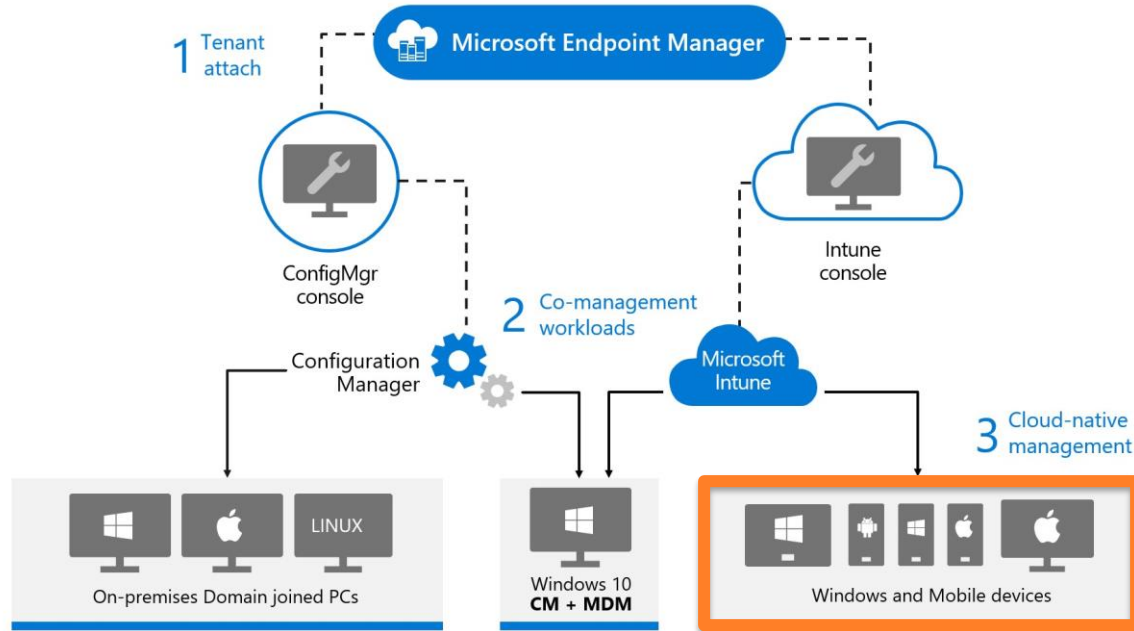
Twitter [@nicolonsky](https://twitter.com/nicolonsky)



Content

- Intune basics
- MAM
- Android Enterprise
- iOS / macOS
- Windows 10
- Recent announcements

Current MEM capabilities





How to get started with Intune

- Identify use cases
- Which devices do you want to manage?
- Ownership?
- Management mode?



Prerequisites

- Licenses (EM+S E3)
- Azure AD (identities)
- Compatible devices
 - OS version
 - Hardware capabilities
 - Encryption support



Now what?

×

Use this account everywhere on your device

Windows will remember your account and make it easier to sign in to apps and websites. You won't have to enter your password each time you access your organization's resources. You may need to allow them to manage certain settings on your device.

☒ Allow my organization to manage my device

This app only

Yes



Default enrollment restrictions

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	<input type="text" value="Manufacturer name here"/>
Android device administrator	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	<input type="text" value="Manufacturer name here"/>
iOS/iPadOS	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported
macOS	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported
Windows (MDM) ⓘ	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported

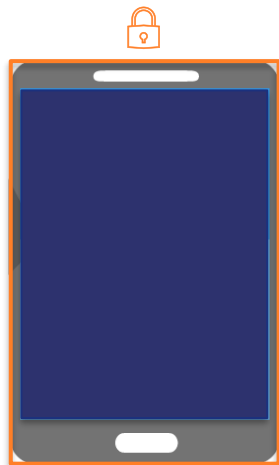


Distinguish personal / company owned?

- Register Serial / IMEI
- Use enrollment service
 - Autopilot
 - Apple automated device enrollment (DEP)
 - Google Zero Touch / Samsung Knox

[more infos](#)

Management scenarios



MDM





MAM



MDM + MAM



MAM 101

- Fully fledged DLP solution
 - Data protection
 - Access requirements
- App configurations
- Broker apps  
- Apps need to implement Intune SDK
 - [List of supported apps](#)
 - App wrapping possible -> ☹️



Experiences from the field

- Usability vs. security
- Contact sync to native address book
- [about:intunehelp](#)

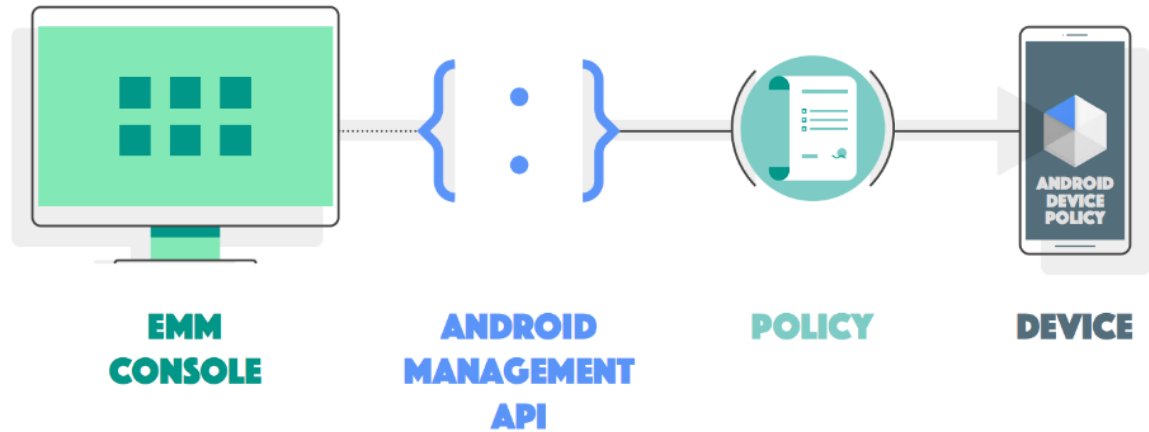
```
App Bundle ID: com.microsoft.Office.Outlook
App Version: 4.56.0 (5781411)
Intune SDK Version: 13.0.0
Last Attempted Policy Check-in: 28.09.20,
19:42:01 CEST
Last Completed Policy Check-in: 28.09.20,
19:42:01 CEST
IntuneMAMPolicySource: 2
Intune MAM Policy Settings:
{
  AccessRecheckOfflineTimeout = 720;
  AccessRecheckOnlineTimeout = 5;
  AllowedIOSModelsElseBlock = "";
  AllowedIOSModelsElseWipe = "";
  AppPinDisabled = 1;
  AppSharingFromLevel = 2;
  AppSharingToLevel = 1;
  AuthenticationEnabled = 0;
  ClipboardCharacterLengthException = 15;
  ClipboardEncryptionEnabled = 1;
  ClipboardSharingLevel = 2;
```



How to enforce usage of MAM?

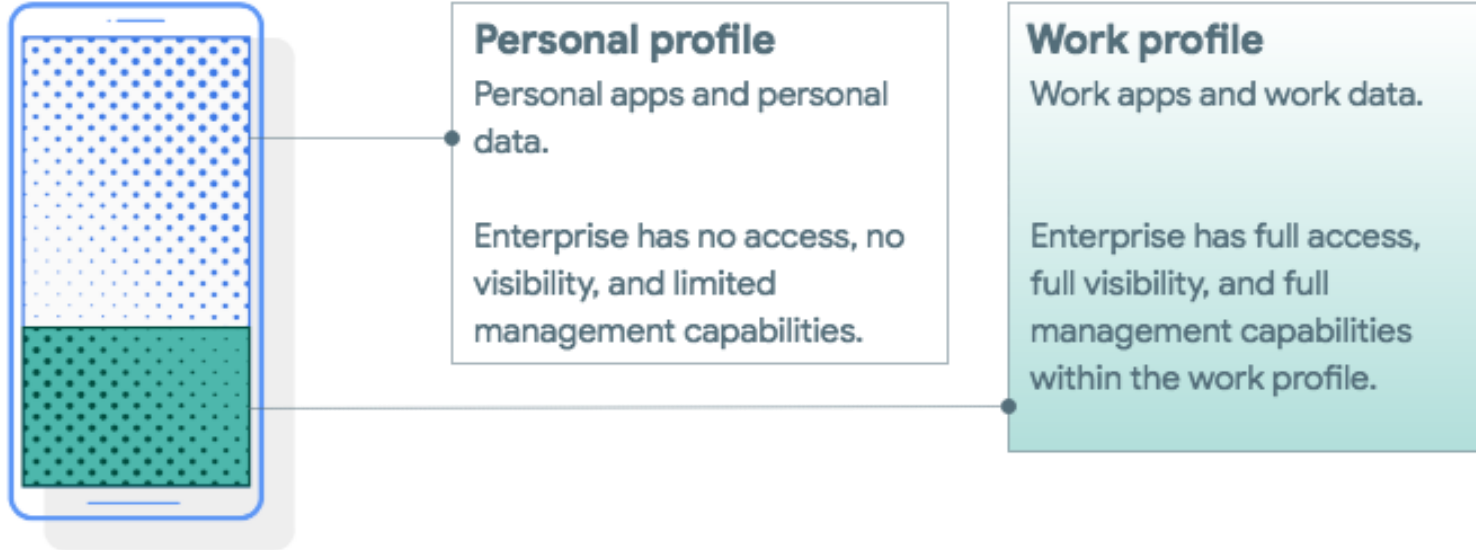
- Conditional Access «require approved client app» [supported apps](#)
- Conditional Access «require app protection policy» [supported apps](#)
- 3rd party / LOB apps -> ☹️

Android management 101



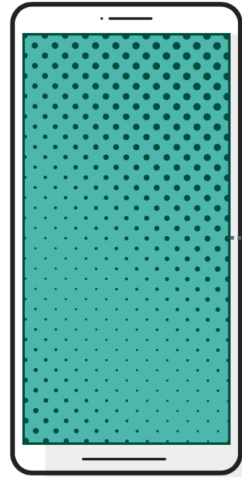
AE Work Profile

personal owned

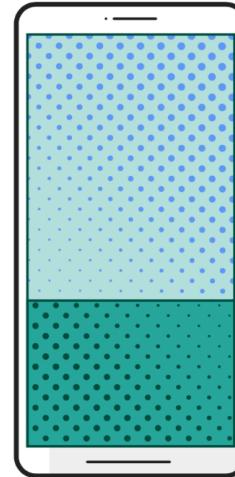


AE Fully Managed

company owned



Contains **only** work apps and work data.



Personal profile

Contains personal apps and personal data

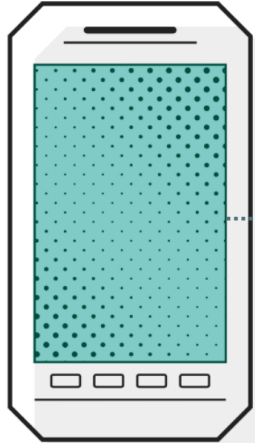
Work profile

Contains work apps and work data.

Former «COPE»

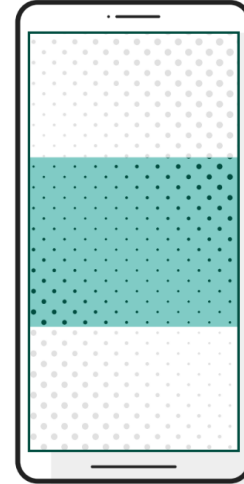
AE Dedicated

company owned



Employee facing

Inventory management
Field service management
Transport & logistics



Customer facing

Digital signage
Hospitality check-in
Kiosks

[more info about scenarios](#)



Enrollment methods

Management type	Token needed	Options
Work profile	-	Company Portal
Dedicated	x (expires)	NFC, QR, Token entry, Knox, Zero Touch
Fully managed	x	
Fully managed with work profile	x (expires)	

[more info](#)



Microsoft Launcher

- Customize Android appearance
- M365 Newsfeed
- Icons, groups, background
- For fully managed / dedicated devices
- No default browser setting ☹
- JSON configuration



[Configure Microsoft Launcher](#)



Android OEMConfig

- Configure manufacturer specific device settings
- Requires manufacturer specific app



Apple management 101

- MDM: APNS certificate
- VPP: App deployment
- Monitor token expiration
- (Onboard apple business/school manager)



«Work profile»

- Apple [User Enrollment](#) in preview
 - BYOD scenarios
 - More privacy for end users
 - Limited management capabilities
 - Dedicated container
 - User based app deployment



Managing macOS?

- Basic management capabilities 😊
 - Encryption, Firewall, Gatekeeper
 - Certificates, VPN, Wi-Fi
 - App deployment, scripts
- Advanced use cases -> Jamf
 - Conditional Access integration



Automated device enrollment (ADE)

- Requires «special» ordered devices
- Federate Apple Business manager with Intune for managed apple id's
- Additional settings available
- Single app mode to force MDM enrollment



Windows 10 device states

- Azure AD Joined
- Hybrid Azure AD Joined
- On premises resource access
- Windows Hello for Business



Windows 10 management 101

- Try out Azure AD Joined devices & Autopilot
- Keep it simple & secure
- Use best of both worlds with cloud attach
- Lots of new ADMX policies



General recommendations

- Use shared mailbox for EMM accounts
- Don't mix Intune with Office 365 policies
- Asset management
- Housekeeping



Conditional Access

- Configure device compliance policies for all your supported platforms
- Block enrollment of platforms you're not supporting

☒ Grant access

☐ Require multi-factor authentication ⓘ

☒ Require device to be marked as compliant ⓘ



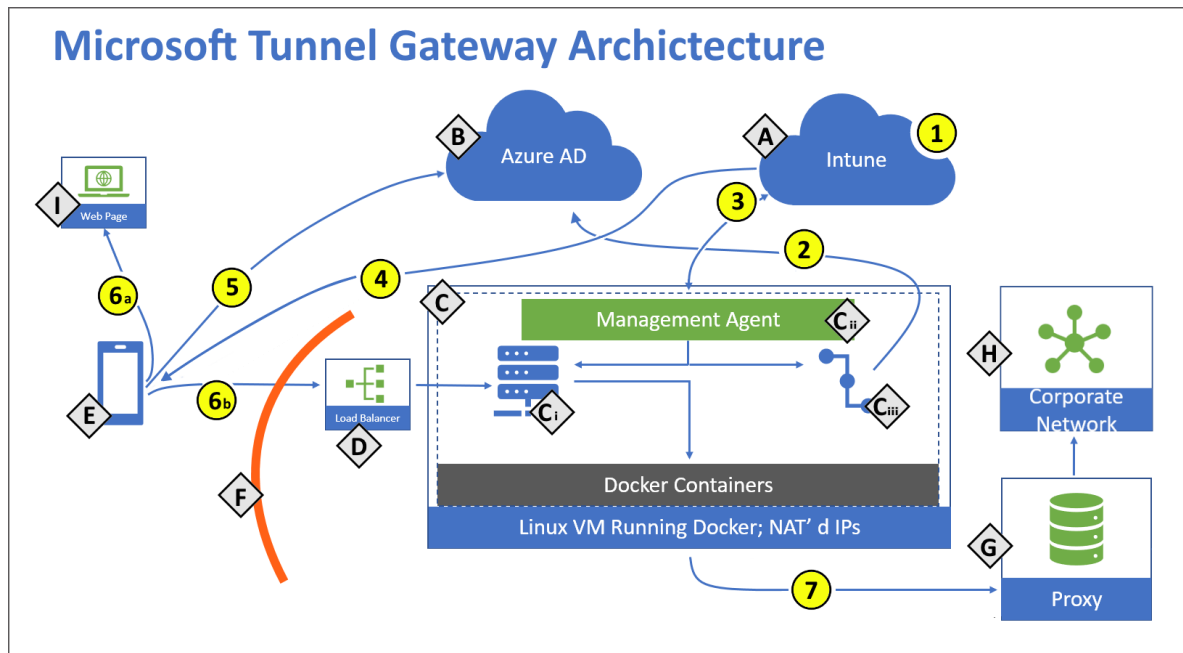
Recent announcements (Ignite)

- Microsoft Tunnel (preview)
- Endpoint Analytics GA
- Group policy migration (preview)
- Defender Antivirus reports (preview)
- Advanced Autopilot troubleshooting (Q4)
- WVD management (Q4)

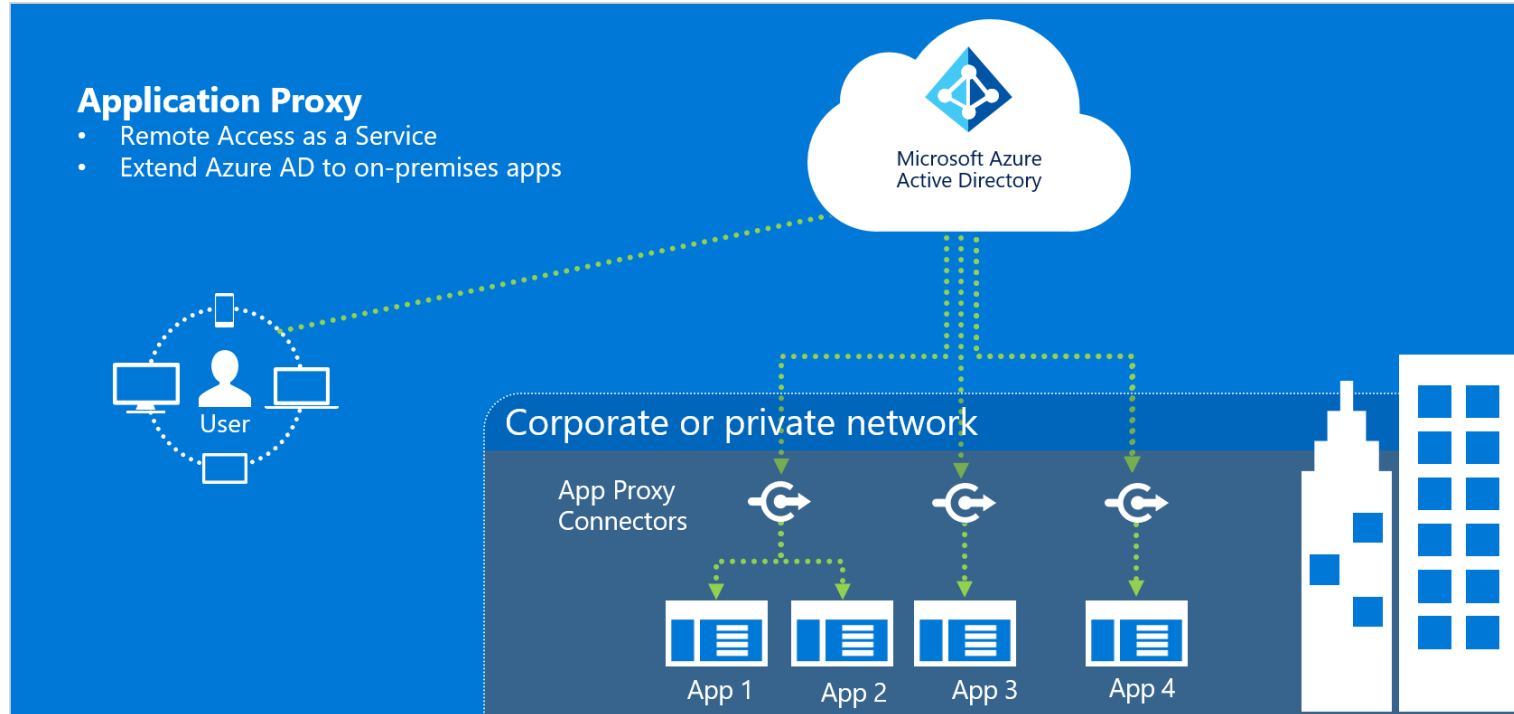


Microsoft Tunnel

«Microsoft Tunnel is a VPN gateway solution for Microsoft Intune.»

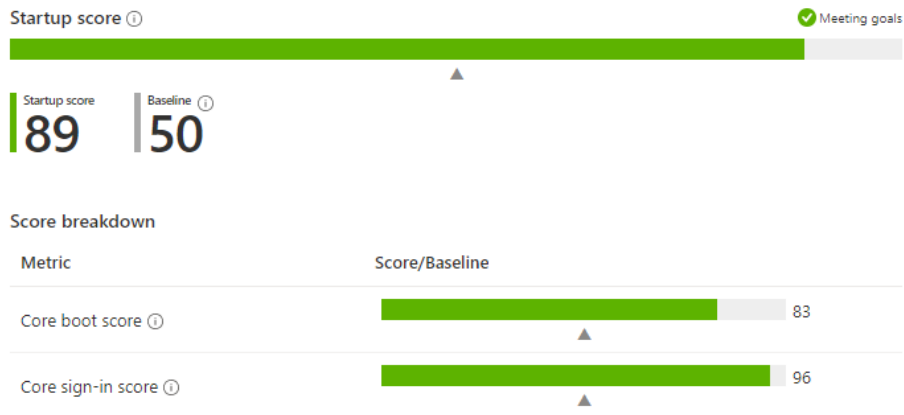


Microsoft Tunnel – WHAT?





Endpoint analytics



Model ↑↓	Manufacturer ↑↓	Disk type ↑↓	Device count ↑↓	Core boot time (seconds) ↑↓	Core sign-in time (seconds) ↑↓
Latitude 7400 2-in-1	Dell Inc.	SSD	60	21	11
HP EliteDesk 705 G4 DM 65W	HP	SSD	45	17	13



Group Policy analytics

Group policy migration readiness



Upload summary

10 Group Policy objects (with detected settings)

425 settings



Thank you!



<https://tech.nicolonsky.ch/events>

software**ONE**



Hewlett Packard
Enterprise

 **SmartIT**



swisscom



Microsoft

digicomp

base**VISION**

INGRAM MICRO



ScriptRunner



audiocodes



au2mator