www.wpninjas.eu

Welcome to the still growing Android device management jungle

Peter van der Woude

Workplace Ninja Summit 2022

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_
SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

AppManagEvent.com
2022
October 7
NETHERLANDS

dinext.

About Peter van der Woude

Enterprise Mobility MVP
Windows Insider MVP

Focus

Modern Workplace

From

Groningen, Netherlands

My Blog

https://petervanderwoude.nl

Certifications

Microsoft 365 Certified: Enterprise Administrator Expert

Microsoft 365 Certified: Modern Desktop Administrator Associate

Hobbies

Family

Basketball

Gaming

Contact

✉ pvanderwoude@hotmail.com

@pvanderwoude

/peterwoude

Agenda

Key takeaways:

- Learn about the still growing device management options for Android devices
- Understand when to use the different Android device management options
- Grow at least a little bit of love for Android devices

Android (device) management options

What are the Android (device) management options

Android device enrollment options

What are the Android **device** enrollment options

Choose the right Android device management option

What is the best Android **device** management option for your organization

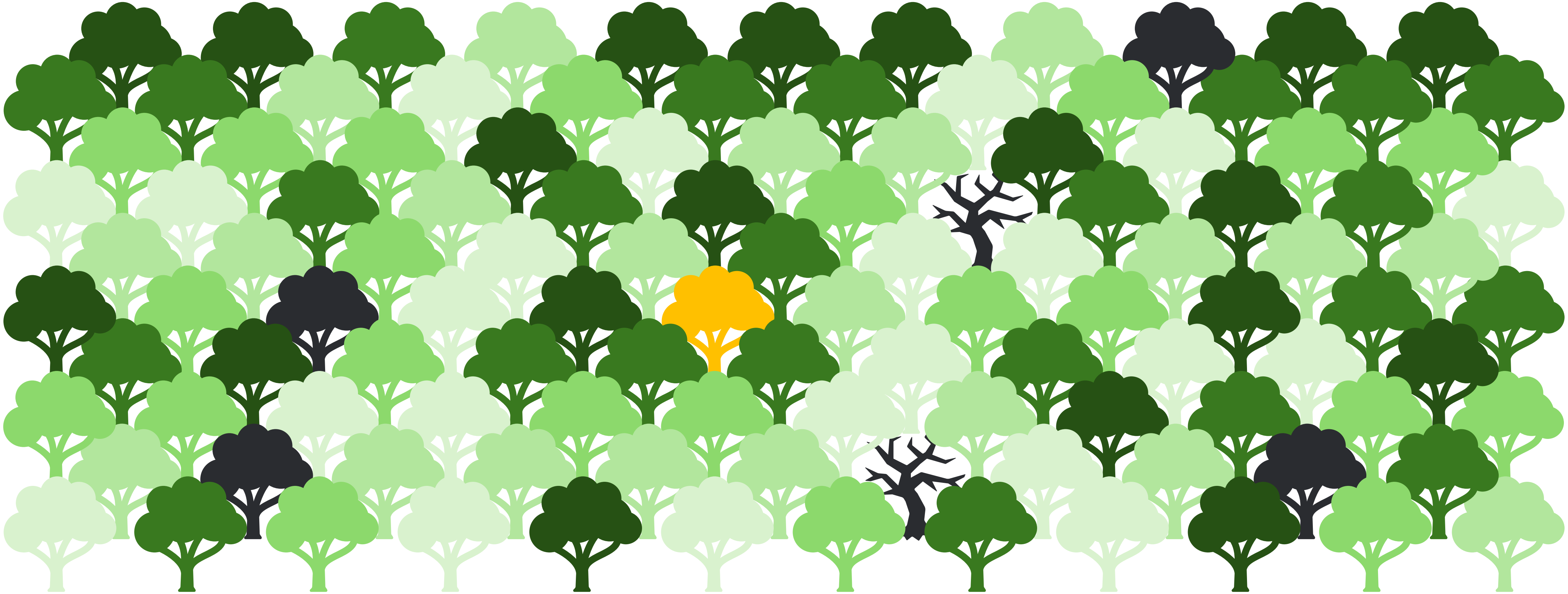
Android device management integrations

What management integrations are available for your Android devices

Android device management (third-party) additions

What (third-party) management additions are available to fill any gaps in the management options

Goal of this session



Android (device) management options

What are the Android (device) management options

To get started: Different management APIs

Device Administrator API (Mostly deprecated and removed, but still alive)	
Any app can take advantage	Microsoft Intune >> Company Portal app
Permissions can only be managed by the user	Any app >> Always device admin
Provides limited management options	

Google Play EMM API (Android Enterprise)	
Build your own management app	Microsoft Intune >> Company Portal app
Permissions are related to the deployment	Microsoft Intune >> Profile owner
Google is not longer accepting new registrations	

Android Management API (Android Enterprise)	
Completely rely on Google management app	Microsoft Intune >> Android Device Policy
Permissions are related to the deployment	Microsoft Intune >> Device owner, profile owner, enhanced profile owner
Google manages the introduction of new features	

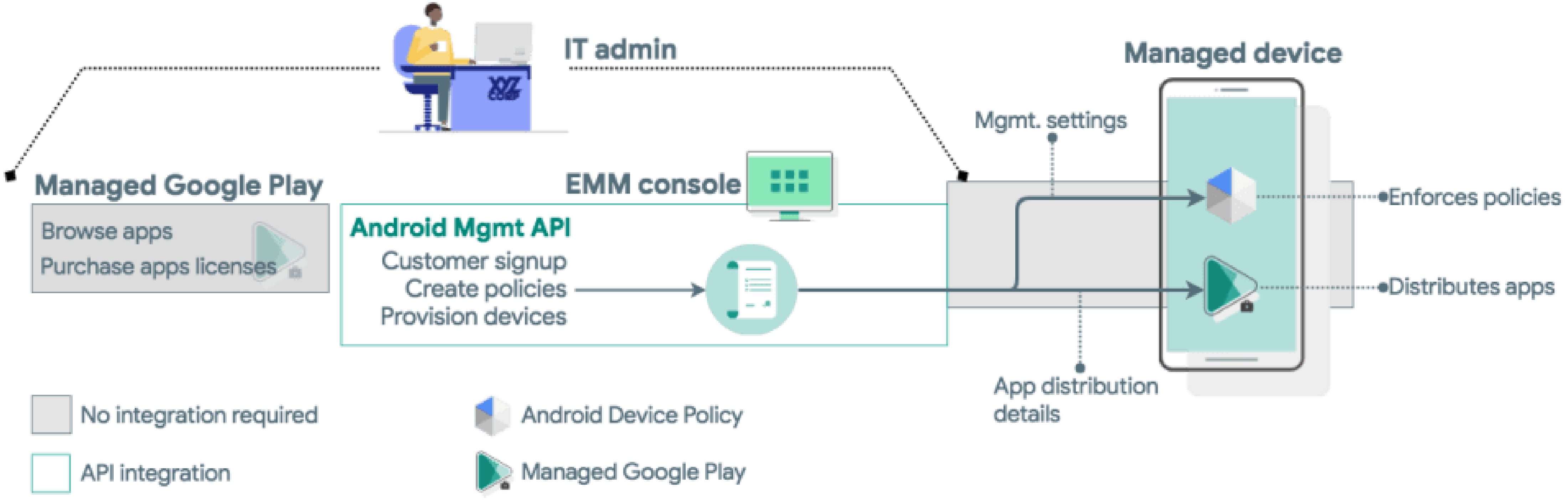
To get started: Different management APIs

Device Administrator API (Mostly deprecated and removed, but still alive)	
Any app can take advantage	Microsoft Intune >> Company Portal app
Permissions can only be managed by the user	Any app >> Always device admin
Provides limited management options	

Google Play EMM API (Android Enterprise)	
Build your own management app	Microsoft Intune >> Company Portal app
Permissions are related to the deployment	Microsoft Intune >> Profile owner
Google is not longer accepting new registrations	

Android Management API (Android Enterprise)	
Completely rely on Google management app	Microsoft Intune >> Android Device Policy
Permissions are related to the deployment	Microsoft Intune >> Device owner, profile owner, enhanced profile owner
Google manages the introduction of new features	

In more detail: Android Management API



Picture taken from the Google docs

Android management options

www.wpninjas.eu

Device ownership	Personal	Personal & Corporate	Personal	Corporate				
Management technology	Intune management	Google management	Google Android Enterprise management				Android Open Source Project management	
							Public preview and RealWear devices only	Public preview and RealWear devices only
	1	2	3	4	5	6	7	8
Solution name	**Application protection policies**	**Device administrator**	**Personally-owned with work profile**	**Corporate-owned with work profile**	**Fully managed**	**Dedicated**	**User affiliated**	**Shared device**
Also known as	**APP**	**DA**	**WP**	**COPE**	**COBO**	**COSU**	**AOSP**	**AOSP**
Management type	Application management only	Full device management	Work profile with limited device management	Work profile with some device management	Full device management with user identity	Full device management for shared scenarios ✦	Full device management with user identity	Full device management for shared scenarios ✦
		APP can be used in combination with all Android device management options*						
Management app	Company Portal	Company Portal	Company Portal	Intune app	Intune app	Intune app	Intune app	Intune app

*Except for Android Enterprise dedicated devices **without** Azure AD Shared device mode

Android management options

Device ownership	Personal	Personal & Corporate	Personal	Corporate				
Management technology	Intune management	Google management	Google Android Enterprise management				Android Open Source Project management	
							Public preview and RealWear devices only	Public preview and RealWear devices only
	1	2	3	4	5	6	7	8
Solution name	**Application protection policies**	**Device administrator**	**Personally-owned with work profile**	**Corporate-owned with work profile**	**Fully managed**	**Dedicated**	**User affiliated**	**Shared device**
Also known as	**APP**	**DA**	**WP**	**COPE**	**COBO**	**COSU**	**AOSP**	**AOSP**
Management type	Application management only	Full device management	Work profile with limited device management	Work profile with some device management	Full device management with user identity	Full device management for shared scenarios	Full device management with user identity	Full device management for shared scenarios
		APP can be used in combination with all Android device management options*						
Management app	Company Portal	Company Portal	Company Portal	Intune app	Intune app	Intune app	Intune app	Intune app

*Except for Android Enterprise dedicated devices **without** Azure AD Shared device mode

Android management options

www.wpninjas.eu

Device ownership	Personal	Personal & Corporate	Personal	Corporate				
Management technology	Intune management	Google management	Google Android Enterprise management				Android Open Source Project management	
							Public preview and RealWear devices only	Public preview and RealWear devices only
	1	2	3	4	5	6	7	8
Solution name	**Application protection policies**	**Device administrator**	**Personally-owned with work profile**	**Corporate-owned with work profile**	**Fully managed**	**Dedicated**	**User affiliated**	**Shared device**
Also known as	**APP**	**DA**	**WP**	**COPE**	**COBO**	**COSU**	**AOSP**	**AOSP**
Management type	Application management only	Full device management	Work profile with limited device management	Work profile with some device management	Full device management with user identity	Full device management for shared scenarios	Full device management with user identity	Full device management for shared scenarios
		APP can be used in combination with all Android device management options*						
Management app	Company Portal	Company Portal	Company Portal	Intune app	Intune app	Intune app	Intune app	Intune app

*Except for Android Enterprise dedicated devices **without** Azure AD Shared device mode

Android management options

Device ownership	Personal	Personal & Corporate	Personal	Corporate				
Management technology	Intune management	Google management	Google Android Enterprise management				Android Open Source Project management	
							Public preview and RealWear devices only	Public preview and RealWear devices only
Solution name	1 Application protection policies	2 Device administrator	3 Personally-owned with work profile	4 Corporate-owned with work profile	5 Fully managed	6 Dedicated	7 User affiliated	8 Shared device
Also known as	APP	DA	WP	COPE	COBO	COSU	AOSP	AOSP
Management type	Application management only	Full device management	Work profile with limited device management	Work profile with some device management	Full device management with user identity	Full device management for shared scenarios	Full device management with user identity	Full device management for shared scenarios
		APP can be used in combination with all Android device management options*						
Management app	Company Portal	Company Portal	Company Portal	Intune app	Intune app	Intune app	Intune app	Intune app

*Except for Android Enterprise dedicated devices **without** Azure AD Shared device mode

Android management options

www.wpninjas.eu

Device ownership	Personal	Personal & Corporate	Personal	Corporate				
Management technology	Intune management	Google management	Google Android Enterprise management				Android Open Source Project management	
							Public preview and RealWear devices only	Public preview and RealWear devices only
	1	2	3	4	5	6	7	8
Solution name	**Application protection policies**	**Device administrator**	**Personally-owned with work profile**	**Corporate-owned with work profile**	**Fully managed**	**Dedicated**	**User affiliated**	**Shared device**
Also known as	**APP**	**DA**	**WP**	**COPE**	**COBO**	**COSU**	**AOSP**	**AOSP**
Management type	Application management only	Full device management	Work profile with limited device management	Work profile with some device management	Full device management with user identity	Full device management for shared scenarios	Full device management with user identity	Full device management for shared scenarios
		APP can be used in combination with all Android device management options*						
Management app	Company Portal	Company Portal	Company Portal	Intune app	Intune app	Intune app	Intune app	Intune app

*Except for Android Enterprise dedicated devices **without** Azure AD Shared device mode

Android management options

www.wpninjas.eu

Device ownership	Personal	Personal & Corporate	Personal	Corporate				
Management technology	Intune management	Google management	Google Android Enterprise management				Android Open Source Project management	
Solution name	1 Application protection policies	2 Device administrator	3 Personally-owned with work profile	4 Corporate-owned with work profile	5 Fully managed	6 Dedicated	Public preview and RealWear devices only 7 User affiliated	Public preview and RealWear devices only 8 Shared device
Also known as	APP	DA	WP	COPE	COBO	COSU	AOSP	AOSP
Management type	Application management only	Full device management	Work profile with limited device management	Work profile with some device management	Full device management with user identity	Full device management for shared scenarios	Full device management with user identity	Full device management for shared scenarios
	APP can be used in combination with all Android device management options*							
Management app	Company Portal	Company Portal	Company Portal	Intune app	Intune app	Intune app	Intune app	Intune app

*Except for Android Enterprise dedicated devices **without** Azure AD Shared device mode

Android management options

www.wpninjas.eu

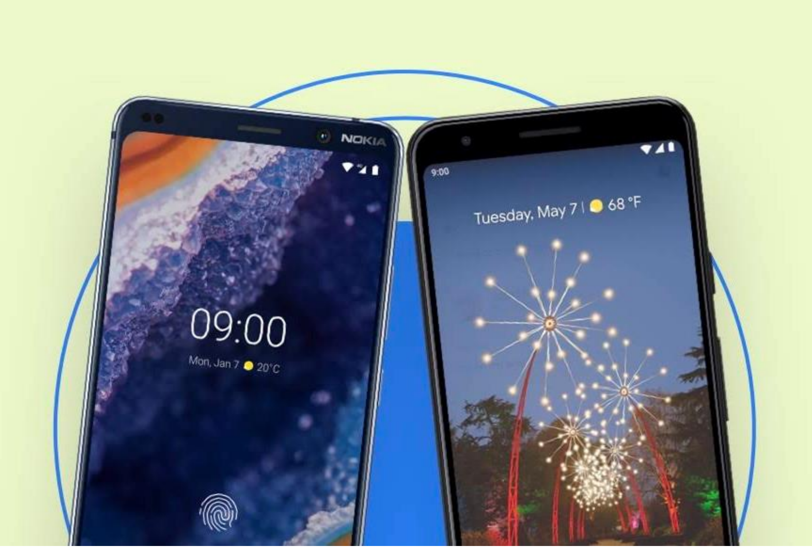
Device ownership	Personal	Personal & Corporate	Personal	Corporate				
Management technology	Intune management	Google management	Google Android Enterprise management				Android Open Source Project management	
Solution name	1 Application protection policies	2 Device administrator	3 Personally-owned with work profile	4 Corporate-owned with work profile	5 Fully managed	6 Dedicated	Public preview and RealWear devices only 7 User affiliated	Public preview and RealWear devices only 8 Shared device
Also known as	APP	DA	WP	COPE	COBO	COSU	AOSP	AOSP
Management type	Application management only	Full device management	Work profile with limited device management	Work profile with some device management	Full device management with user identity	Full device management for shared scenarios	Full device management with user identity	Full device management for shared scenarios
	APP can be used in combination with all Android device management options*							
Management app	Company Portal	Company Portal	Company Portal	Intune app	Intune app	Intune app	Intune app	Intune app

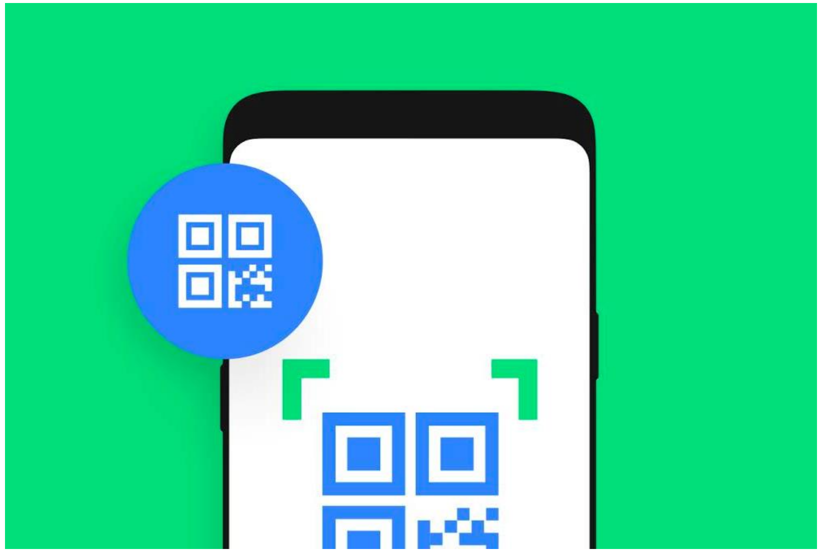
*Except for Android Enterprise dedicated devices **without** Azure AD Shared device mode

Android device enrollment options

What are the Android device enrollment options

Android device enrollment methods





NFC bump

Configure a new device by bumping an NFC tag

Token entry

Configure a new device by entering **afw#setup** as token

Manual enrollment

Use the Company Portal app to enroll a personal device

QR code

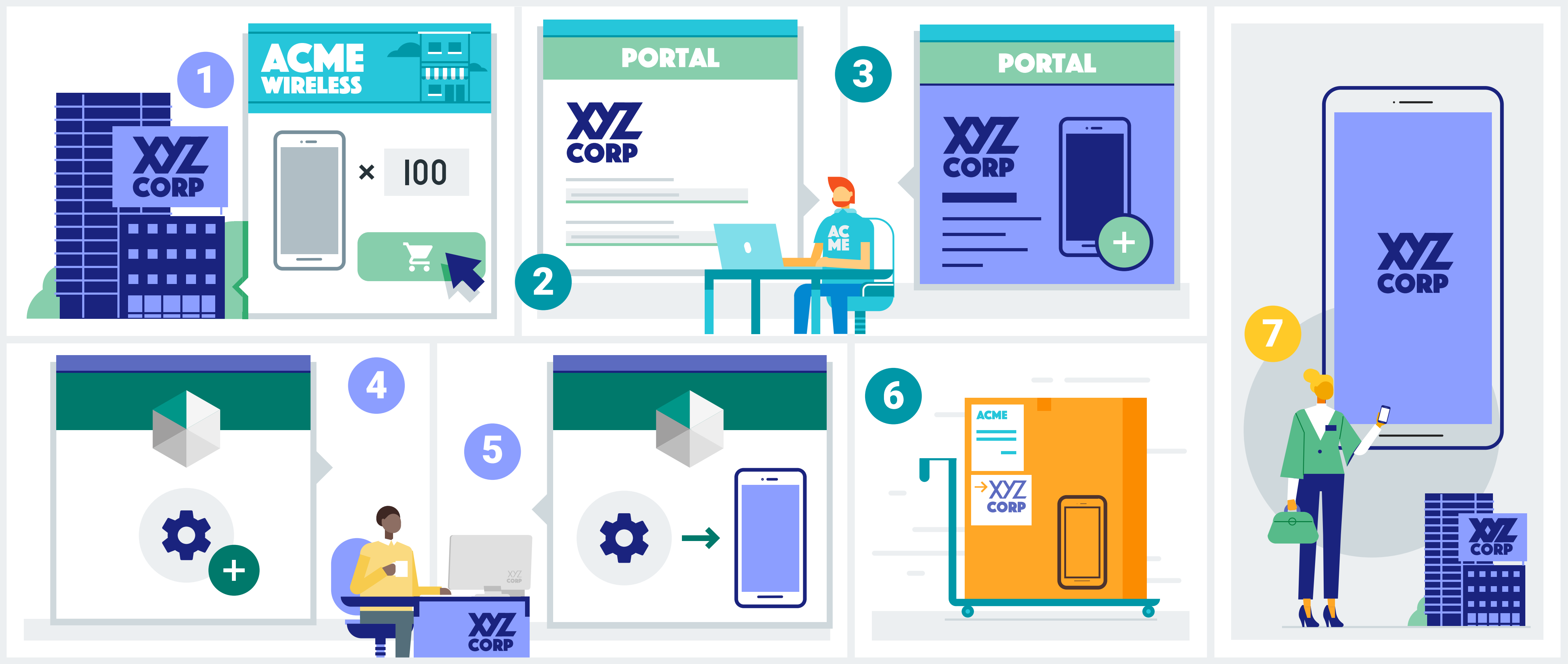
Configure a new device from the setup wizard by scanning a QR code

AOSP enrollment

Configure a new device from the setup wizard by scanning a QR code

Pictures taken from the Google docs

Android zero-touch enrollment



Alternatively look at Samsung Knox Mobile Enrollment

Picture taken from the Google docs

Filters based on enrollment profile

Create filters based on the enrollment profile of the Android devices

- (device.enrollmentProfileName -eq null) and (device.deviceOwnership -eq "Corporate")
- (device.enrollmentProfileName -eq "Default corporate-owned dedicated devices")
- (device.enrollmentProfileName -eq "Default corporate-owned devices with work profile")

Choose the right Android device management option

What is the best Android **device** management option for your organization

The right device management options

Quick first filter for the device management options

App management

My personal favorite for personal devices. **Use whenever possible for personal devices.**

Device administrator

Legacy method for managing devices. **Only use as a last resort for device management.**

AOSP management

New method for managing specific devices. **Use whenever possible for supported devices.**

Choose the right management option

	Personally-owned with work profile	Corporate-owned with work profile	Fully managed	Dedicated	User affiliated (AOSP)	Shared (AOSP)
Use Google Mobile Services (GMS)	✓	✓	✓	✓	✗	✗
Devices are personal or BYOD	✓	✗	✗	✗	✗	✗
You have new or existing devices	✓	✓	✓	✓	✓	✓
Need to enroll a few, or many devices	✓	✓	✓	✓	✗	✗
Devices are associated with a single user	✓	✓	✓	✗	✓	✗
You use the device enrollment manager	✓	✗	✗	✗	✗	✗
Devices are managed by another MDM	✗	✗	✗	✗	✗	✗
Devices are owned by the organization	✗	✓	✓	✓	✓	✓
Devices are user-less	✗	✗	✗	✓	✗	✓

More information: Android device enrollment guide for Microsoft Intune | Microsoft Docs

Choose the right management option

	Personally-owned with work profile	Corporate-owned with work profile	Fully managed	Dedicated	User affiliated (AOSP)	Shared (AOSP)
Use Google Mobile Services (GMS)	✓	✓	✓	✓	At this moment only for RealWear devices, updated to Firmware 11.2 or later	
Devices are personal or BYOD	✓	✗	✗	✗		
You have new or existing devices	✓	✓	✓	✓		
Need to enroll a few, or many devices	✓	✓	✓	✓		
Devices are associated with a single user	✓	✓	✓	✗		
You use the device enrollment manager	✓	✗	✗	✗		
Devices are managed by another MDM	✗	✗	✗	✗		
Devices are owned by the organization	✗	✓	✓	✓		
Devices are user-less	✗	✗	✗	✓		

More information: Android device enrollment guide for Microsoft Intune | Microsoft Docs

Choose the right management option

	Personally-owned with work profile	Corporate-owned with work profile	Fully managed	Dedicated	User affiliated (AOSP)	Shared (AOSP)
Use Google Mobile Services (GMS)	✓	At this moment still the main focus for most Android device management scenarios for corporate devices			At this moment only for RealWear devices, updated to Firmware 11.2 or later	
Devices are personal or BYOD	✓					
You have new or existing devices	✓					
Need to enroll a few, or many devices	✓					
Devices are associated with a single user	✓					
You use the device enrollment manager	✓					
Devices are managed by another MDM	✗					
Devices are owned by the organization	✗					
Devices are user-less	✗					

More information: Android device enrollment guide for Microsoft Intune | Microsoft Docs

Choose the right management option

	Personally-owned with work profile	Corporate-owned with work profile	Fully managed	Dedicated	User affiliated (AOSP)	Shared (AOSP)
Use Google Mobile Services (GMS)	At this moment still the most obvious for Android **device** management scenarios for personal devices	At this moment still the main focus for most Android device management scenarios for corporate devices			At this moment only for RealWear devices, updated to Firmware 11.2 or later	
Devices are personal or BYOD						
You have new or existing devices						
Need to enroll a few, or many devices						
Devices are associated with a single user						
You use the device enrollment manager						
Devices are managed by another MDM						
Devices are owned by the organization						
Devices are user-less						

More information: Android device enrollment guide for Microsoft Intune | Microsoft Docs

What about non-technical requirements like privacy?

Choose the right management option

	Personally-owned with work profile	Corporate-owned with work profile	Fully managed	Dedicated
Use case	Bring Your Own Devices (BYOD)	Corporate-Owned, Personally Enabled (COPE)	Corporate-Owned, Business Only (COBO)	Corporate-Owned, Single Use (COSU)
Device ownership	Personal	Corporate	Corporate	Corporate
Personal use	Personal use and work use	Work use and personal use	Work use with personal use options	Work use only
Privacy guaranteed	Yes	Yes	No	No
Enrollment method	Enrollment via Company Portal app	Enrollment via NFC, Token, QR-code, Zero Touch, Samsung KME	Enrollment via NFC, Token, QR-code, Zero Touch, Samsung KME	Enrollment via NFC, Token, QR-code, Zero Touch, Samsung KME
Management reach	Profile owner	Profile owner with device level settings	Device owner	Device owner
Remote actions	Retire, Delete, Remote lock, Sync, Reset passcode, New remote assistance session, Send custom notification	Retire, Wipe, Delete, Remote lock, Reset work profile passcode, Play lost device sound	Wipe, Delete, Remote lock, Reset passcode, Restart, Play lost device sound	Wipe, Delete, Remote lock, Reset passcode, Restart, Play lost device sound, Locate device
Reset required	No	Yes	Yes	Yes
User affinity	Yes	Yes	Yes	No

Android management based on work profile

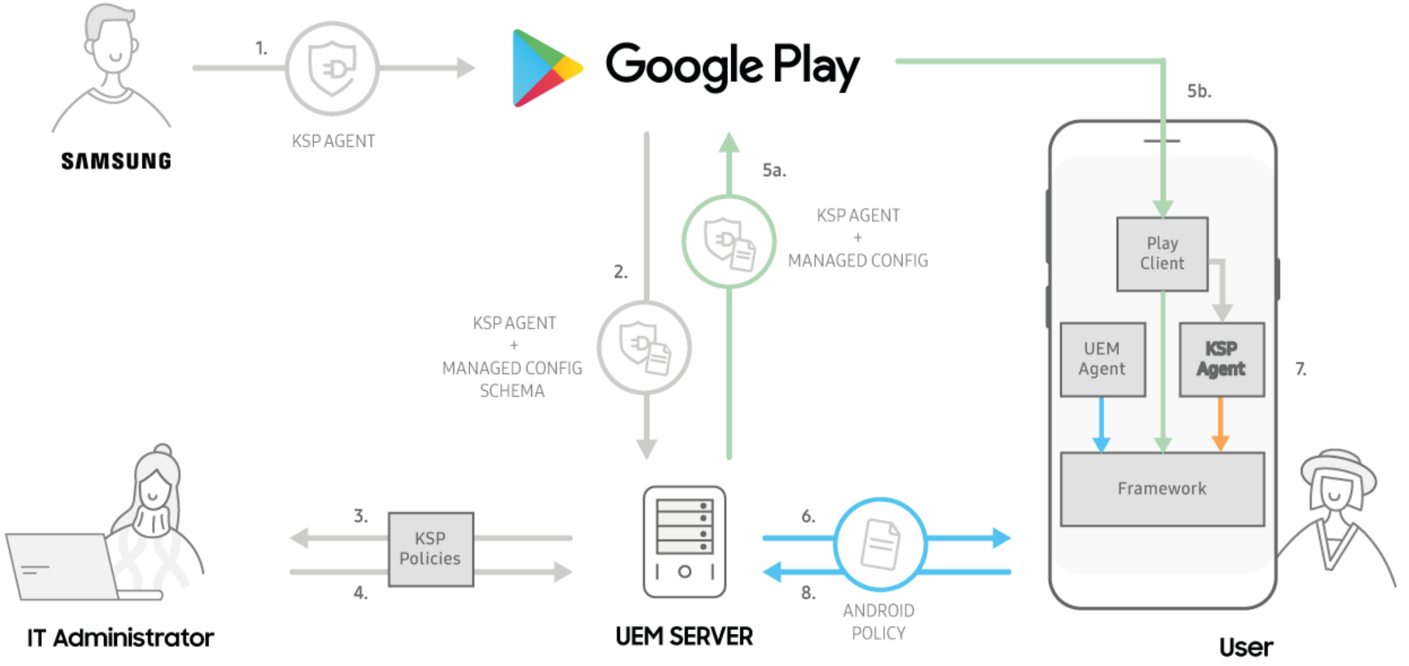
Highlight some of the love it or hate it points of using a work profile (privacy versus usability)

- Cross-profile experience
- Management options
- What’s next

Android device management integrations

What device management integrations are available for Android devices

What’s next with OEMConfig

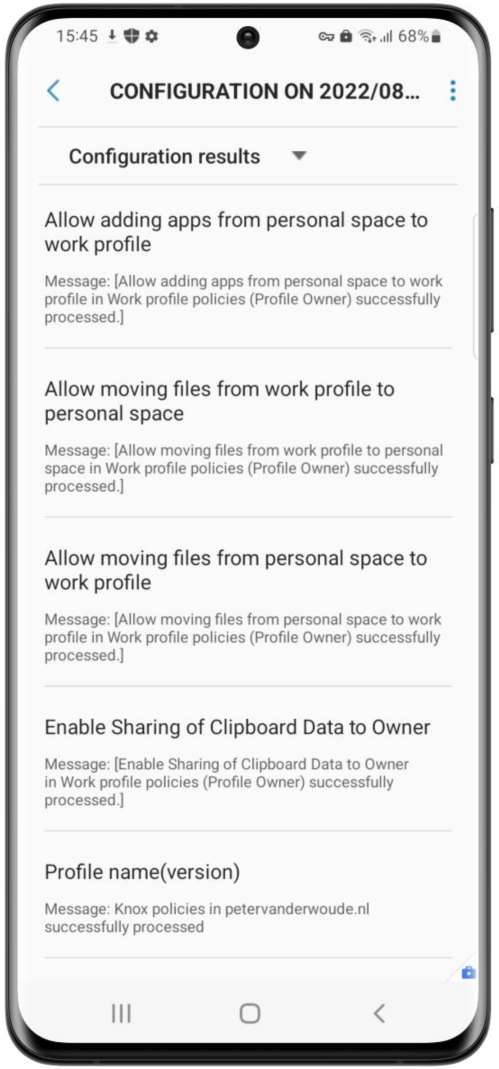


- Steps 2, 3 and 4 happen when IT Admin is setting up IT policies on UEM Console
- Steps 5-8 happen with each device/user enrollment

🟩 → Google play channel

🟦 → UEM Channel

Picture taken from the Samsung docs



CONFIGURATION ON 2022/08...

Configuration results

Allow adding apps from personal space to work profile

Message: [Allow adding apps from personal space to work profile in Work profile policies (Profile Owner) successfully processed.]

Allow moving files from work profile to personal space

Message: [Allow moving files from work profile to personal space in Work profile policies (Profile Owner) successfully processed.]

Allow moving files from personal space to work profile

Message: [Allow moving files from personal space to work profile in Work profile policies (Profile Owner) successfully processed.]

Enable Sharing of Clipboard Data to Owner

Message: [Enable Sharing of Clipboard Data to Owner in Work profile policies (Profile Owner) successfully processed.]

Profile name(version)

Message: Knox policies in petervanderwoude.nl successfully processed

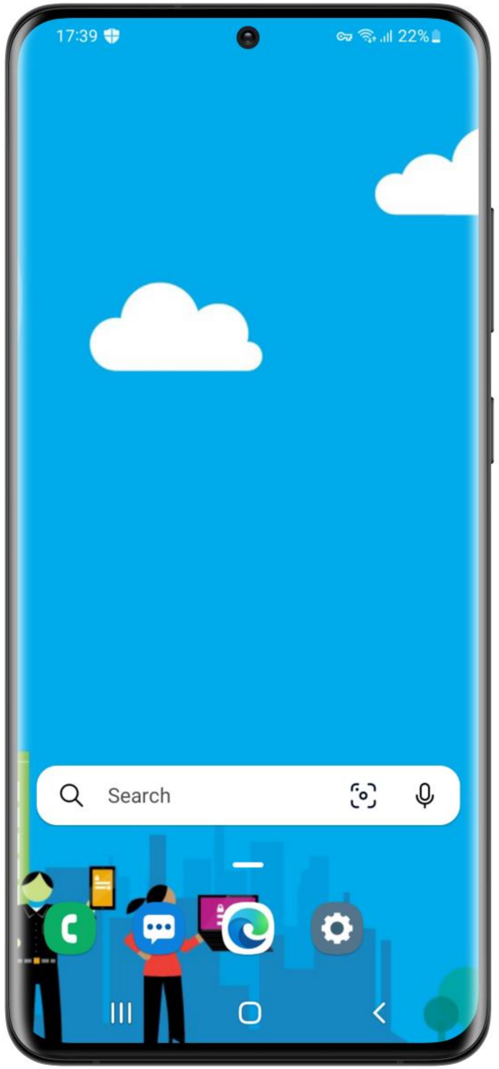
Android management with OEMConfig

Highlight some of reason why OEMConfig might add something useful to the table

- Better (consistent) cross-profile experience
- Management options

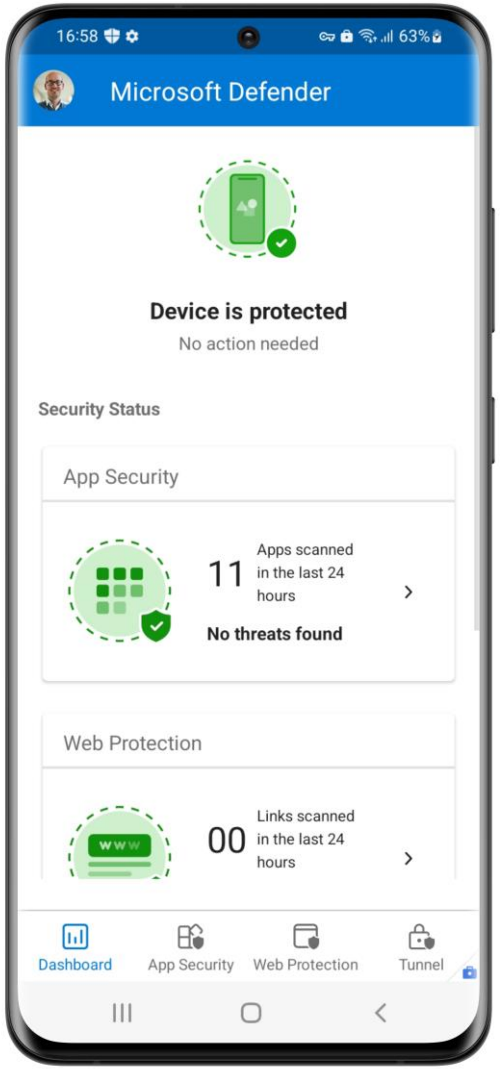
Additional Microsoft apps and features

- **Microsoft Launcher** – Customizing the device conform company standard
  - Consistent home screen experience
  - Device configuration profile to set default launcher
  - Device configuration profile to customize device
    - Set wallpaper, Enable feed, Set grid, Set visible apps home screen, Set application order, Set dock mode, Set search bar placement
- **Managed Home Screen** – Customizing the sign-in experience for dedicated devices
  - Customized sign-in experience
  - Enrollment profile to set Azure AD shared device mode
  - Device configuration profile to customize device
    - Enable sign-in, Set sign-in type, Enable auto sign-out, Set auto sign-out dialog box, Set wallpaper and logo on sign-in page, [..] all regular Microsoft Home Screen app configuration options are available



Integration with Defender for Endpoint

- Automatic app installation that requires a manual setup by the user
- Web protection via a local self looping VPN, or via Microsoft Tunnel Gateway integration
- Web protection relies on Defender SmartScreen
- App security relies on cloud protection
- Direct integration with Microsoft Intune for risk score of device
- Risk score usage with device compliance and app protection policies
- App configuration options available for different features (like VPN)
- Part of the Microsoft Defender for Endpoint Plan 1 and 2 licenses that are also included in the Microsoft 365 E3 and E5 licenses
- **Note**: according to the docs, still not available for Android Enterprise corporate-owned devices with Work Profile



16:58 63%

Microsoft Defender

Device is protected

No action needed

Security Status

App Security

11 Apps scanned in the last 24 hours

No threats found

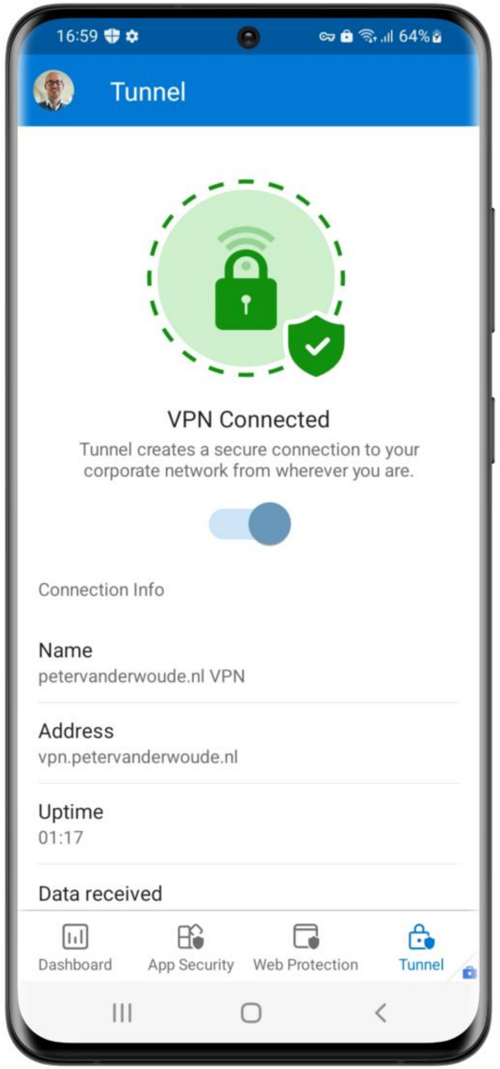
Web Protection

00 Links scanned in the last 24 hours

Dashboard | App Security | Web Protection | Tunnel

Integration with Microsoft Tunnel

- Microsoft Tunnel Gateway runs on a Docker container on a Linux server
- Server and site configuration options available to define the setup
- Integrated in the Microsoft Defender for Endpoint app for the user
- Provides single sign-on experience for the VPN connection
- Configuration can be achieved via a standard VPN profile
- Provides configuration options for per-app and device-based VPN
- Part of the existing Microsoft Intune licenses!



16:59 64%

Tunnel

VPN Connected

Tunnel creates a secure connection to your corporate network from wherever you are.

Connection Info

Name
petervanderwoude.nl VPN

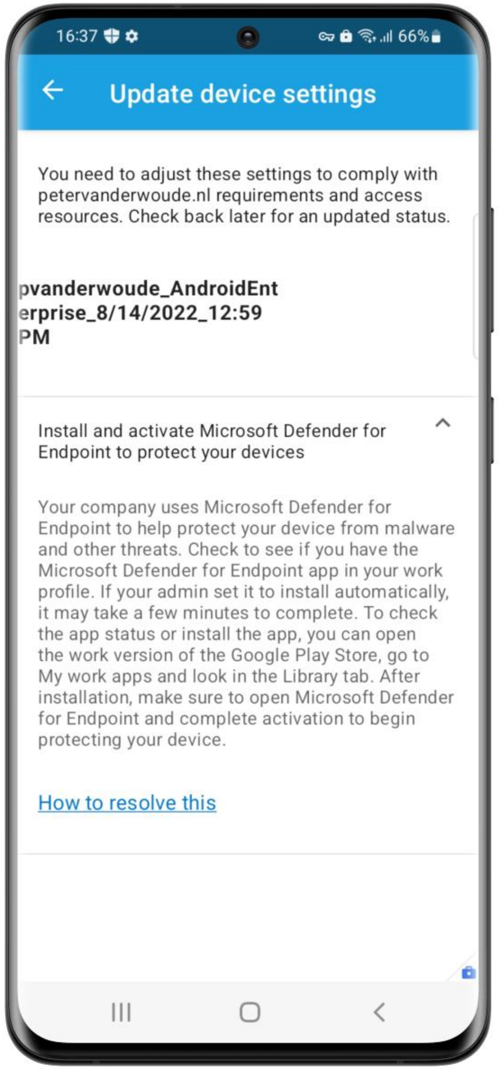
Address
vpn.petervanderwoude.nl

Uptime
01:17

Data received

Combination with Conditional Access

- Device-based Conditional Access for Android devices
  - **Require device to be marked as compliant** to look at
    - Microsoft Defender for Endpoint, Device Health, Device Properties, System Security
    - Location only for legacy Android management (device administrator)
  - Personally-owned devices require the Company Portal app
  - Corporate-owned devices require the Authenticator app
- Browser-based Conditional Access for Android devices
  - Supported with the Microsoft Edge and Google Chrome browser
  - Automatically enabled during enrollment of corporate-owned devices (2106)
  - On first sign-in through the browser the user must select the client certificate
- App-based Conditional Access for Android devices
  - **Require approved client app** to require a specific listed app
    - Requires the Microsoft Authenticator app or Company Portal app required as broker
  - **Require app protection pol**icy to require an app with Intune SDK and policy
    - Requires the Company Portal app as broker



You need to adjust these settings to comply with petervanderwoude.nl requirements and access resources. Check back later for an updated status.

pvanderwoude_AndroidEnterprise_8/14/2022_12:59 PM

Install and activate Microsoft Defender for Endpoint to protect your devices

Your company uses Microsoft Defender for Endpoint to help protect your device from malware and other threats. Check to see if you have the Microsoft Defender for Endpoint app in your work profile. If your admin set it to install automatically, it may take a few minutes to complete. To check the app status or install the app, you can open the work version of the Google Play Store, go to My work apps and look in the Library tab. After installation, make sure to open Microsoft Defender for Endpoint and complete activation to begin protecting your device.

How to resolve this

And more

Integration	Remark
Android Managed Google Play	Only for Android Enterprise managed devices
Mobile Threat Defense	Depending on the third-party capabilities
Partner compliance management	Depending on the third-party capabilities
TeamViewer connector	Only for Android device administrator (DA) and Android Enterprise personally owned devices with a work profile (BYOD)
Certificate connectors	For all Android devices
Telecom expenses	Only for Android device administrator 4.4 and newer devices that are Knox capable (Samsung)
Derived Credentials	Only for Android Enterprise fully managed devices that run version 7.0 and above

Q&A

Any questions?

Thank You