Why you might want to use corporate-owned devices with Work Profile

Peter van der Woude

Workplace Ninja Virtual Edition 2021

V-Platin Sponsor

nwc services
one step ahead

RECAST SOFTWARE

Patch My PC
PATCH MANAGEMENT MADE EASY

glueckkanja gab

Lenovo

Microsoft

V-Gold Sponsor

scopewyse
we are what's next

sepago®

baseVISION
SECURE & MODERN WORKPLACE

Patron Sponsors

SD:>_
SwissDev Jobs

About Peter van der Woude

www.wpninjas.eu

Focus

Modern Workplace

From

Groningen, Netherlands

My Blog

https://petervanderwoude.nl

Enterprise Mobility MVP
Windows Insider MVP

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:

- **Getting familiar with Android management**
- **Getting familiar with corporate-owned devices with Work Profile**
- **Understanding the management options in Microsoft Intune**

● **Android management basics**

The basics of Android management

● **Android management options**

What are the Android management options

● **Corporate-owned devices with Work Profile**

What management options are available for corporate-owned devices with Work Profile

● **Android management integrations**

What management integrations are available and working with corporate-owned devices with Work Profile

● **Android management (third-party) additions**

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

Android management basics

The basics of Android management

Different management APIs

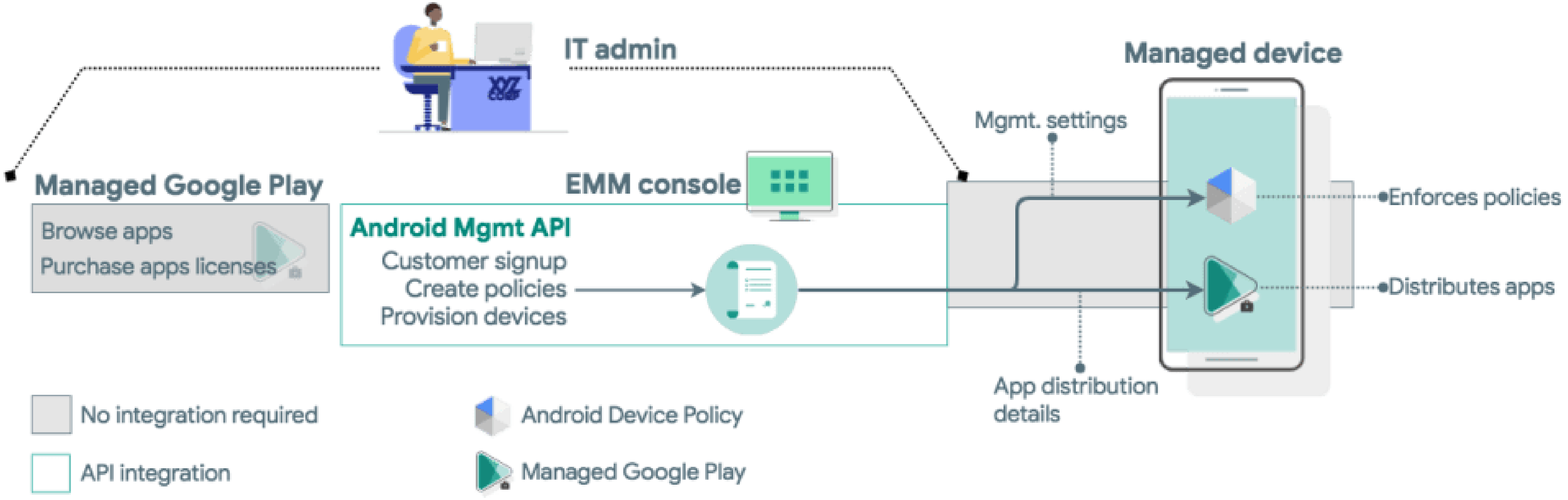
Device Administrator API	
Any app can take advantage	Microsoft Intune >> Company Portal app
Permissions can only be managed by the user	Always device admin
Provides limited management options	

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	

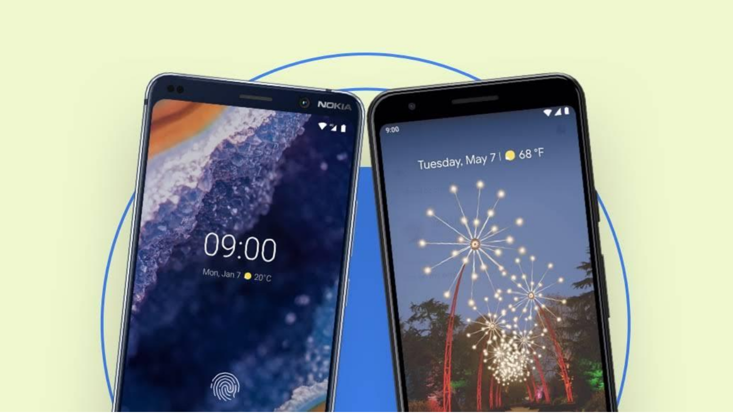
Android Management API

www.wpninjas.eu



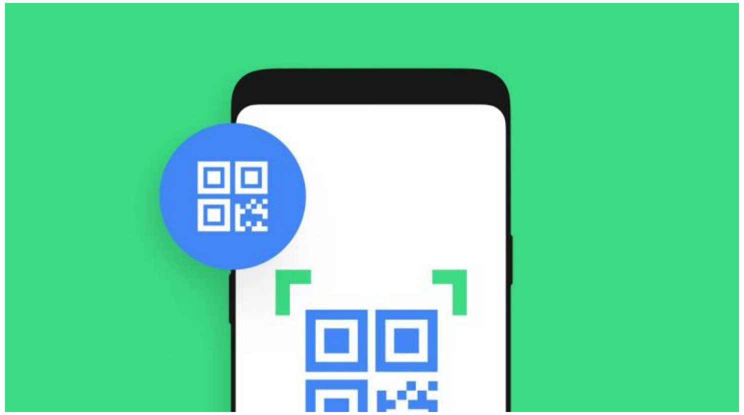
Picture taken from the Google docs

Android Enterprise enrollment methods



NFC bump
Configure a new device by bumping an NFC tag

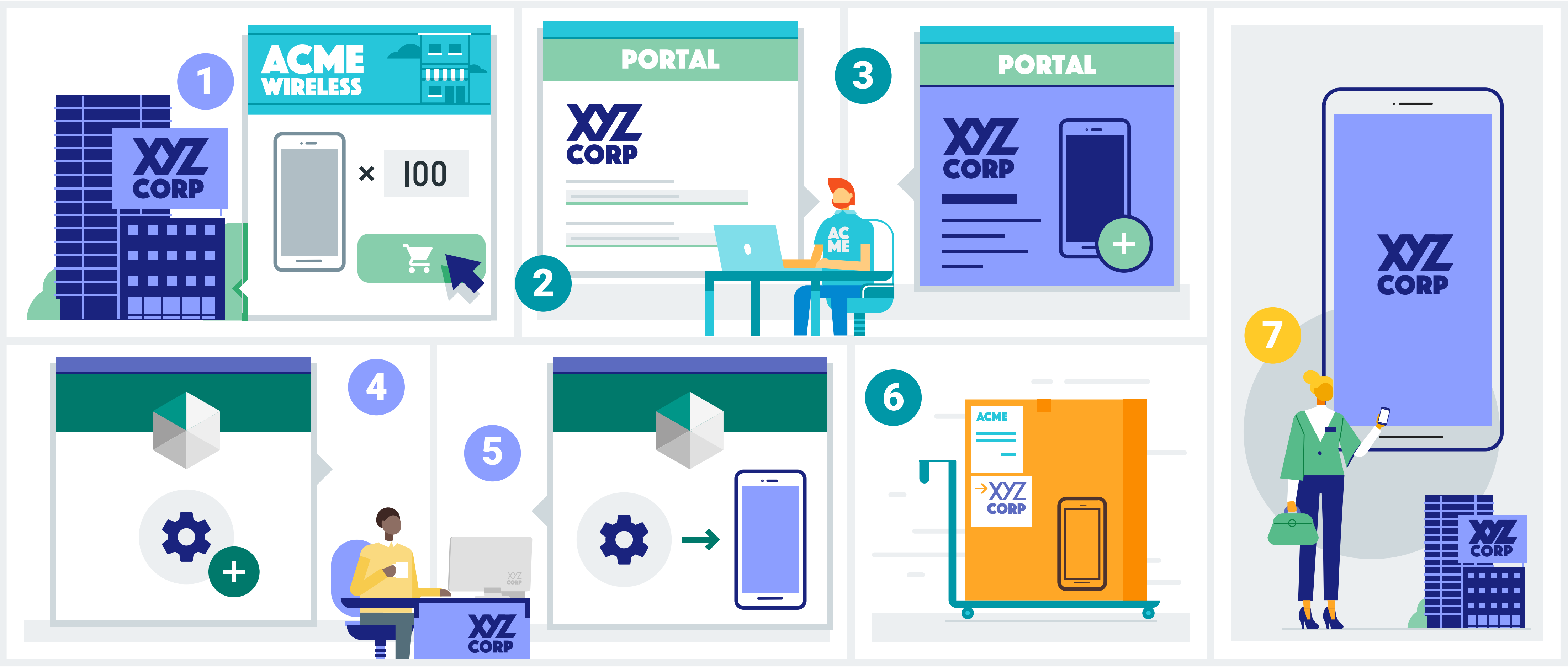
Token entry
Configure a new device by entering **afw#setup** as token



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

Pictures taken from the Google docs

Android zero-touch enrollment



Picture taken from the Google docs

Android management options

What are the Android management options

Android Enterprise deployment scenarios

www.wpninjas.eu

Personally-owned
device with Work Profile

Properties
Bring Your Own Devices (BYOD)
Personal use and work use
Privacy guaranteed
Enrollment via Company Portal app
Profile owner
Reset not required
User affinity

Corporate-owned
fully managed device

Properties
Corporate-Owned, Business Only (COBO)
Work use with personal use options
Privacy not guaranteed
Enrollment via NFC, Token, QR-code, Zero Touch, Samsung KME
Device owner
Reset required
User affinity

Corporate-owned
dedicated device

Properties
Corporate-Owned, Single Use (COSU)
Work use only
Privacy not guaranteed
Enrollment via NFC, Token, QR-code, Zero Touch, Samsung KME
Device owner
Reset required
No user affinity

Corporate-owned
device with Work Profile

Properties
Corporate-Owned, Personally Enabled (COPE)
Work use and personal use
Privacy guaranteed
Enrollment via NFC, Token, QR-code, Zero Touch, Samsung KME
Profile owner ++
Reset required
User affinity

Deployment scenarios summary

Deployment scenario	Use case	Personal use	Privacy guaranteed	Enrollment method	Management reach	Reset required	User affinity
Personally-owned device with Work Profile	Bring Your Own Device (BYOD)	Yes	Yes	Company Portal app	Profile owner	No	Yes
Corporate-owned fully managed device	Corporate-Owned, Business Only (COBO)	Yes	No	NFC, Token, QR code, Zero Touch, Samsung KME	Device owner	Yes	Yes
Corporate-owned dedicated device	Corporate-Owned, Single Use (COSU)	No	No	NFC, Token, QR code, Zero Touch, Samsung KME	Device owner	Yes	No
Corporate-owned device with Work Profile	Corporate-Owned, Personally Enabled (COPE)	Yes	Yes	NFC, Token, QR code, Zero Touch, Samsung KME	Profile owner with device-level settings	Yes	Yes

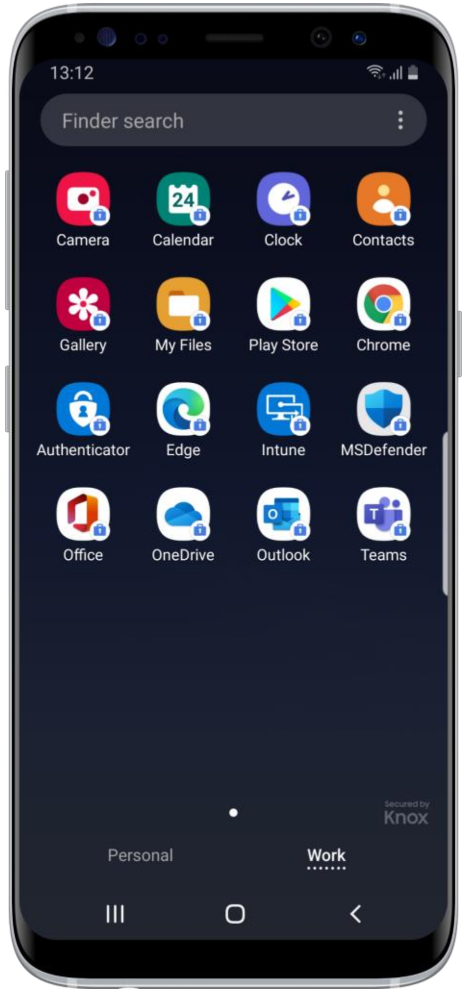
General available since service release 2106

Corporate-owned devices with Work Profile

What management options are available for corporate-owned devices with Work Profile

Main characteristics

Main use case formally known as Corporate-Owned, Personally enabled (COPE)
Available for Android 8.0 and later
Provided via the Android Management API
Relies on the Android Device Policy app as the Device Policy Controller (DPC)
Relies on the Microsoft Intune app for device compliance
Relies on the Managed Google Play store for work apps
Contains a separate personal profile and work profile
DPC has profile owner permissions and a few device level management options
Depends on the Google Mobile Services (GMS)
Administrator can wipe device



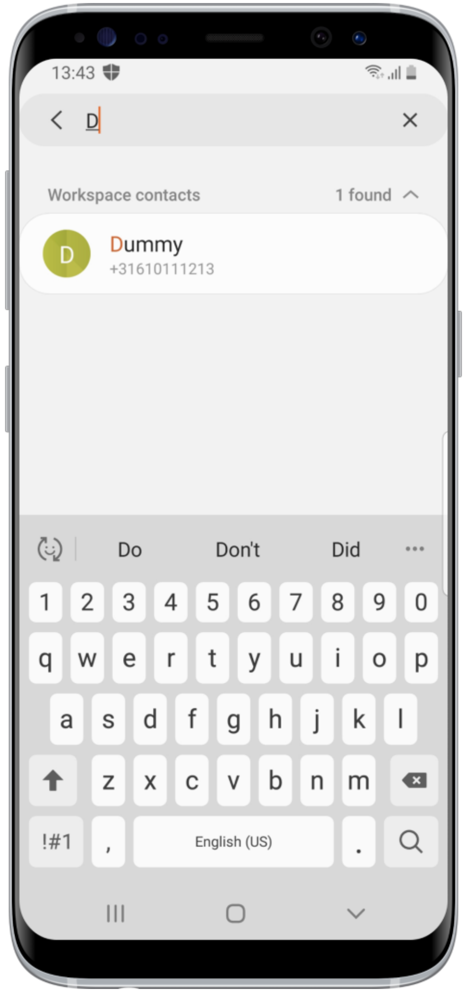
Configuration options

Category	Description
Supported version	Android 8.0 and later
Requirement	Google Mobile Service available and connectivity
Enrollment profile	Corporate-owned devices with work profile (token)
Enrollment options	Token (Android 8-10), QR code, NFC (Android 8-10), Android Zero Touch, Samsung Knox Mobile Enrollment
Device filtering	Dynamic groups and filters based on enrollment profile
Device restrictions	Fully Managed, Dedicated, and Corporate-Owned Work Profile profile type with group settings and specific Work profile password and Personal profile groups
Device compliance	Fully Managed, Dedicated, and Corporate-Owned Work Profile profile type
Android apps	Everything available for Android Enterprise
App management	Fully Managed, Dedicated, and Corporate-Owned Work Profile profile type

Important cross-profile experiences

Cross-profile experience	Configuration sugestion or behavior
Clear separation between personal profile and work profile	Enable at least the Camera and Gallery systems apps
Cross-profile clipboard is available between personal profile and work profile	If needed, use OEMConfig to disable the cross-profile clipboard and more*
Cross-profile contacts are available when searching work contacts in personal profile	Contacts Outlook app > Contacts in work profile > Contacts searchable in personal profile
Cross-profile calendar is not available yet	Calendar Outlook app > Calendar in work profile > Not available
Cross-profile app switching is available for specific apps	Outlook app > Work profile > Personal profile

*Exact behavior depends on Android version (and API-version)


13:43

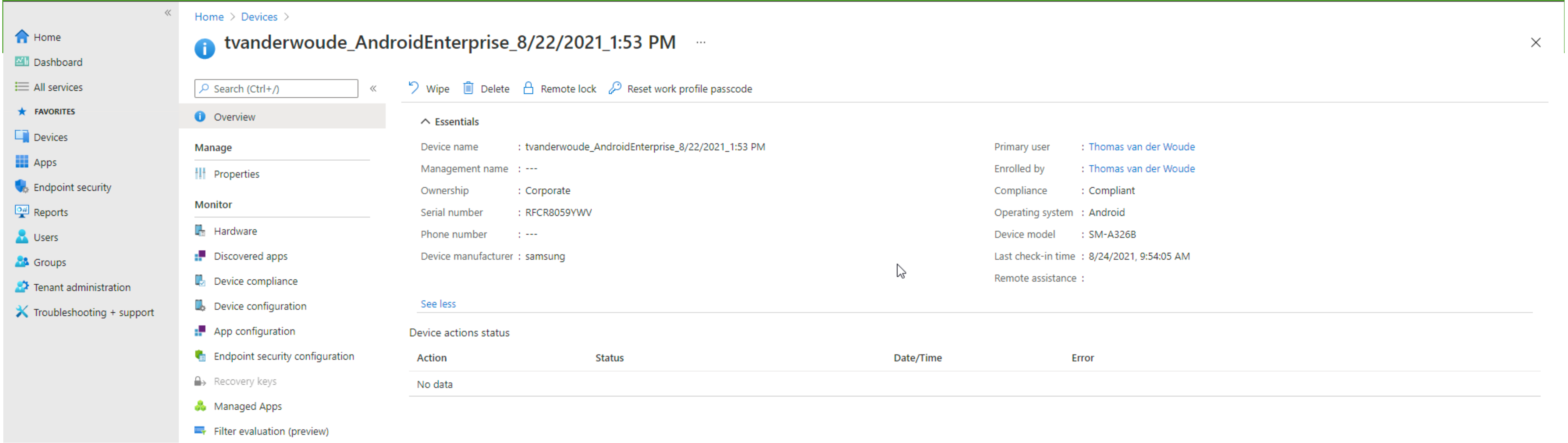
D

Workspace contacts 1 found

Dummy
+31610111213

Management differences between Work Profiles

Company-owned device	Personally-owned device
IT administrator can manage some device level settings	IT administrator can only manage work profile settings
IT administrator might miss cross profile configurations	IT administrator has control cross profile
Relies on Android Management API	Relies on Google Play EMM API
Relies on Android Device Policy and Microsoft Intune app	Relies on Company Portal app



tvanderwoude_AndroidEnterprise_8/22/2021_1:53 PM

Device name	: tvanderwoude_AndroidEnterprise_8/22/2021_1:53 PM	Primary user	: Thomas van der Woude
Management name	: ---	Enrolled by	: Thomas van der Woude
Ownership	: Corporate	Compliance	: Compliant
Serial number	: RFCR8059YWV	Operating system	: Android
Phone number	: ---	Device model	: SM-A326B
Device manufacturer	: samsung	Last check-in time	: 8/24/2021, 9:54:05 AM
		Remote assistance	:

Device actions status

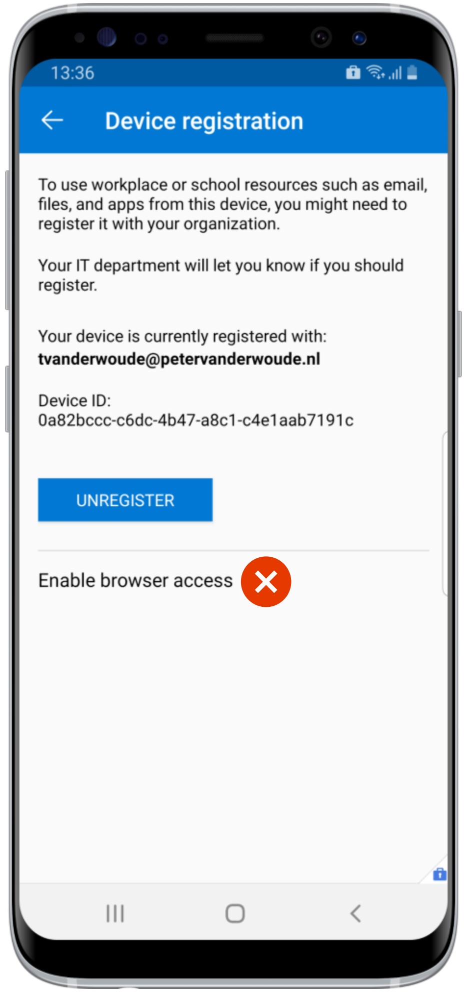
Action	Status	Date/Time	Error
No data			

Android management integrations

What management integrations are available and working corporate-owned devices with Work Profile

Works with Conditional Access

- Device-based Conditional Access*
  - **Require device to be marked as compliant** works only within the Work Profile and requires an enrolled device that is compliant
    - Microsoft Defender for Endpoint, Device Health, Device Properties, System Security
    - Non-compliance quarantines devices, as there are no settings that forces remediation
- App-based Conditional Access*
  - Broker apps: Company Portal app, Microsoft Authenticator app
  - **Require approved client app** to require a specific listed app
  - **Require app protection policy** to require an app with Intune SDK and policy assurance enabled and an app protection policy applied
  - A bit useless: Also possible within the Personal Profile
- Browser-based Conditional Access*
  - Supported browsers: Microsoft Edge, Google Chrome
  - Automatically enabled during enrollment corporate-owned device (2106)
  - On first sign-in through the browser, the user must select the client certificate



13:36

Device registration

To use workplace or school resources such as email, files, and apps from this device, you might need to register it with your organization.

Your IT department will let you know if you should register.

Your device is currently registered with:
tvanderwoude@petervanderwoude.nl

Device ID:
0a82bccc-c6dc-4b47-a8c1-c4e1aab7191c

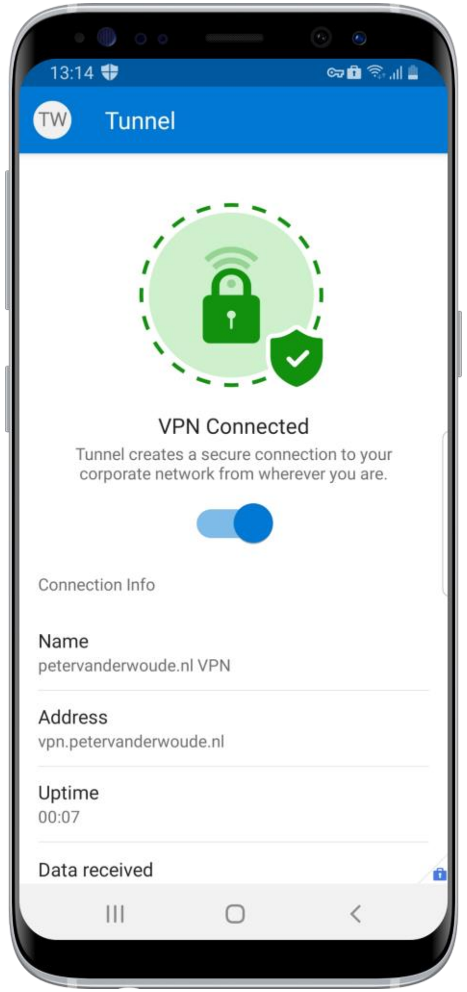
Enable browser access ✕

*Filters are available for Conditional Access, but without the Intune properties

Works with Microsoft Tunnel Gateway (and Azure AD Application Proxy)

www.wpninjas.eu

- Microsoft Tunnel Gateway
  - Docker container that runs on a Linux server
  - Server and site configuration options available
  - Uses the Microsoft Defender for Endpoint app
  - Provides single sign-on experience on the VPN (Azure AD)
  - Configuration via a VPN profile
  - Provides per-app and (always-on) device-based VPN
  - Included in the Microsoft Intune license!
- Azure AD Application proxy
  - Connector that runs on-premises with only outbound connections
  - Uses Azure AD for authentication (including Condtional Access)
  - Connector provides single sign-on on the on-premises app
  - Works with web apps that use Integration Windows Authentication



13:14

TW Tunnel

VPN Connected

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

Connection Info

Name
petervanderwoude.nl VPN

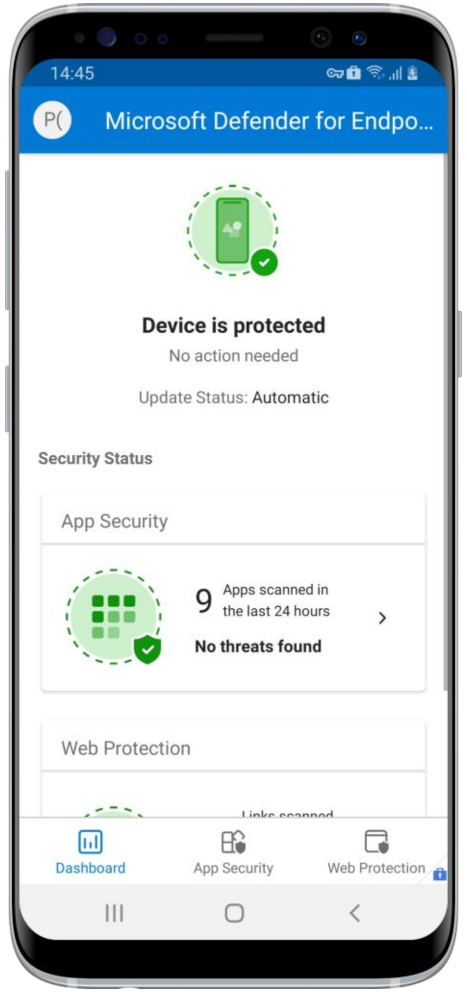
Address
vpn.petervanderwoude.nl

Uptime
00:07

Data received

Works with Microsoft Defender for Endpoint*

- Requires a manual setup by the user
- Web protection via a local self looping VPN
- Web protection relies on Defender SmartScreen
- App security relies on cloud protection
- Integration with Microsoft Intune
- Usage with device compliance
- App configuration options available
- Works only within the Work Profile
- Requires additional licensing



14:45

P(Microsoft Defender for Endpo...

Device is protected

No action needed

Update Status: Automatic

Security Status

App Security

9 Apps scanned in the last 24 hours

No threats found

Web Protection

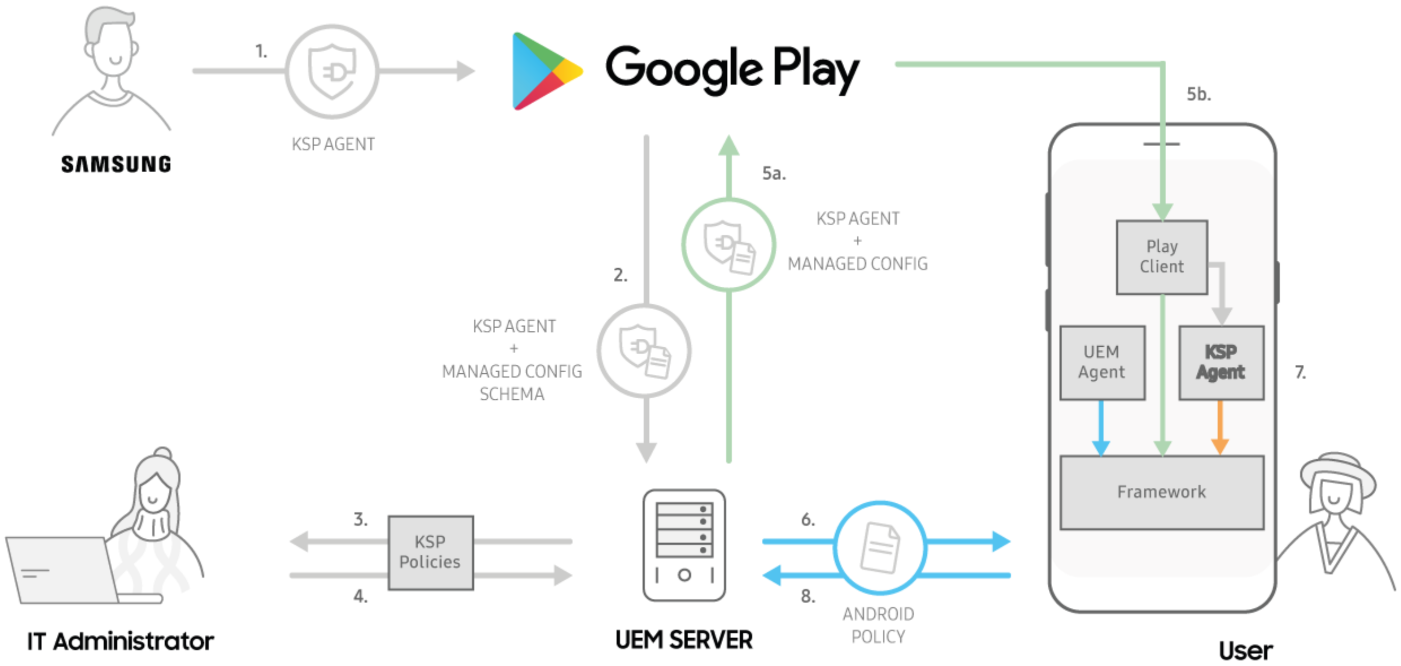
Links scanned

*Keep in mind that this is not documented as supported yet

Android management (third-party) additions

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

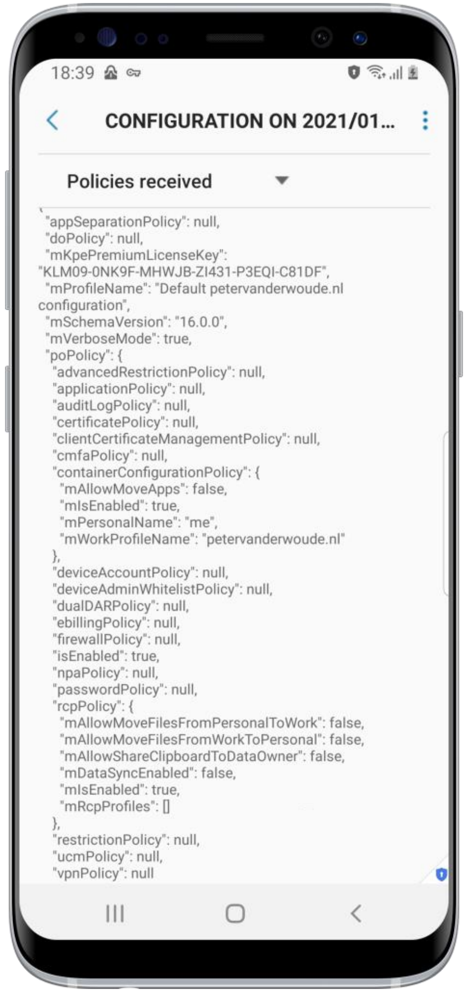
Works with OEMConfig



- 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



```
 "appSeparationPolicy": null,
 "doPolicy": null,
 "mKpePremiumLicenseKey":
"KLM09-0NK9F-MHWJB-ZI431-P3EQI-C81DF",
 "mProfileName": "Default petervanderwoude.nl
configuration",
 "mSchemaVersion": "16.0.0",
 "mVerboseMode": true,
 "poPolicy": {
  "advancedRestrictionPolicy": null,
  "applicationPolicy": null,
  "auditLogPolicy": null,
  "certificatePolicy": null,
  "clientCertificateManagementPolicy": null,
  "cmfaPolicy": null,
  "containerConfigurationPolicy": {
   "mAllowMoveApps": false,
   "mIsEnabled": true,
   "mPersonalName": "me",
   "mWorkProfileName": "petervanderwoude.nl"
  },
  "deviceAccountPolicy": null,
  "deviceAdminWhitelistPolicy": null,
  "dualDARPolicy": null,
  "ebillingPolicy": null,
  "firewallPolicy": null,
  "isEnabled": true,
  "npaPolicy": null,
  "passwordPolicy": null,
  "rcpPolicy": {
   "mAllowMoveFilesFromPersonalToWork": false,
   "mAllowMoveFilesFromWorkToPersonal": false,
   "mAllowShareClipboardToDataOwner": false,
   "mDataSyncEnabled": false,
   "mIsEnabled": true,
   "mRcpProfiles": []
  },
  "restrictionPolicy": null,
  "ucmPolicy": null,
  "vpnPolicy": null
```

Picture taken from the Samsung docs

Questions

Thank You