#NVSummit2021

Welcome in the Android Enterprise device management jungle

- Peter van der Woude
- Modern Workplace enthousiast
- @pvanderwoude
- https://petervanderwoude.nl/
- Enterprise Mobility MVP | Windows Insider MVP

NORDIC — VIRTUAL SUMMIT —

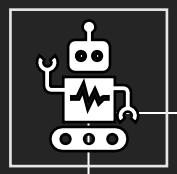
NORDIC
– VIRTUAL SUMMIT –

Welcome in the Android Enterprise device management jungle

Learn all about the management capabilities for Android Enterprise that are available within Microsoft Intune

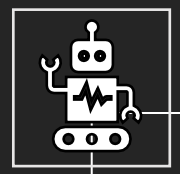
A fully packed agenda

NORDIC
– VIRTUAL SUMMIT –



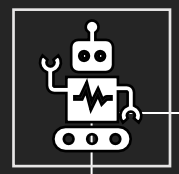
Android management basics

- Android device administrator
- Management APIs for Android
- Android Management API
- Enrollment methods
- Android zero-touch



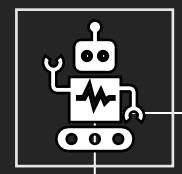
Personally-Owned devices

- Device with MAM-only
- Device with Work Profile



Corporate-Owned devices

- Fully Managed device
- Company-branded Fully Managed device
- Dedicated device
- Azure AD shared device mode
- Device with Work Profile
- Android management summary



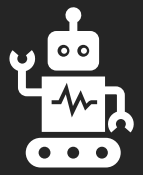
Additions and integrations

- Support for OEMConfig
- Support for Conditional Access
- Support for Microsoft Tunnel Gateway
- Support for Microsoft Defender for Endpoint

NORDIC
– VIRTUAL SUMMIT –

Android management basics

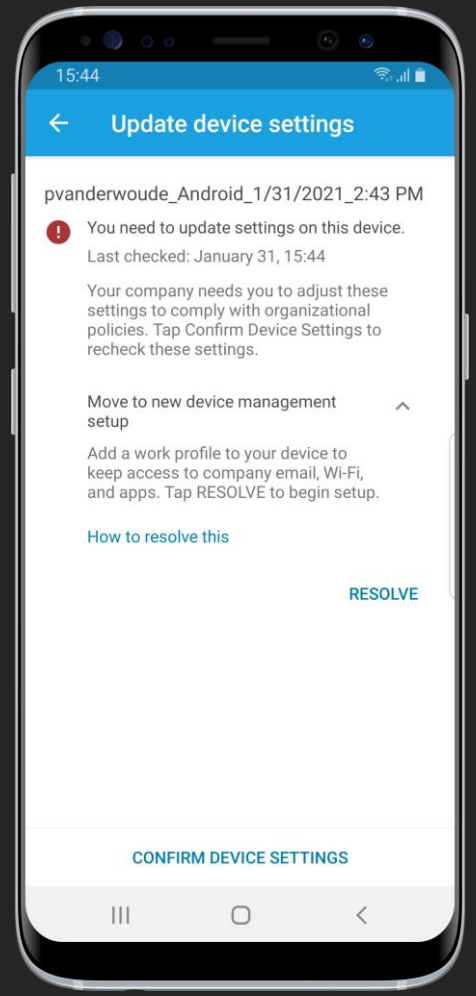
The basics of Android management: briefly explaining the management APIs, the DPCs and the enrollment options

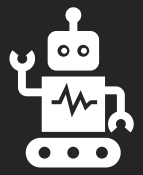


Android device administrator devices

Often refered to as legacy Android management

- Works with Android 2.2 and later
- Provided via the Device Administrator APIs
- Limited management capabilities
- Additional management capabilities via third-parties (like Samsung Knox or Zebra)
- Multiple device administrator apps
- No dependency on Google Mobile Services (GMS)
- Migration options available



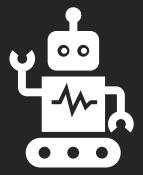


Management APIs for Android

A brief overview of the main management APIs

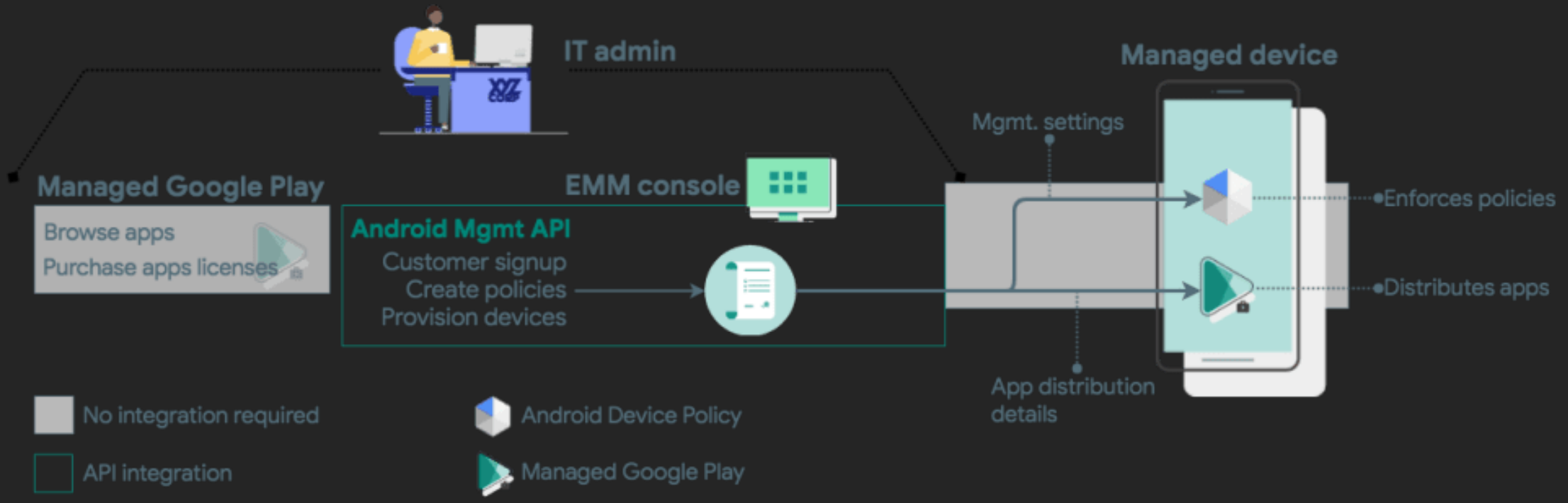
NORDIC
– VIRTUAL SUMMIT –

- **Device Administrator API**
  - Any app can take advantage – For Intune that is Company Portal app
  - Permissions can only be managed by the user – Always device admin
  - Provides limited management options
- **Google Play EMM API**
  - Build your own management app – For Intune that is Company Portal app
  - Permissions are related to the deployment – For Intune that is profile owner
  - Google is no longer accepting new registrations
- **Android Management API**
  - Completely rely on Google management app – That is Android Device Policy
  - Permissions are related to the deployment – For Intune that can be profile owner, device owner or something in between



Android Management API

More details about the most important API



Overview of the Android Device Policy flow
(picture taken from the Google docs)

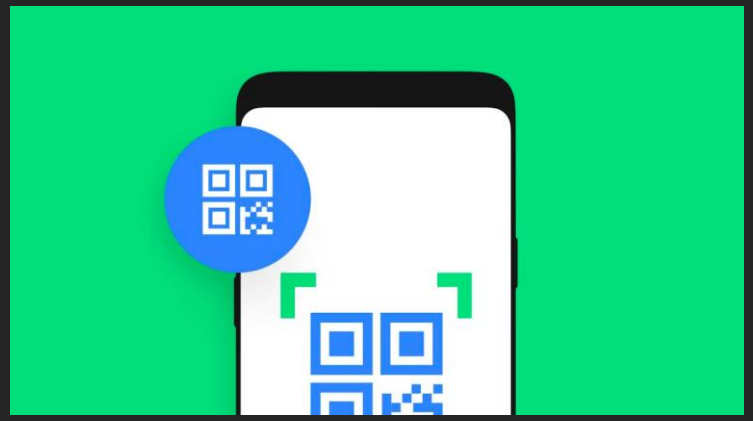
Enrollment methods

A brief overview for corporate-owned devices

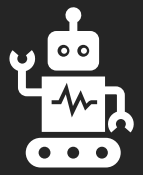
NORDIC
– VIRTUAL SUMMIT –

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.

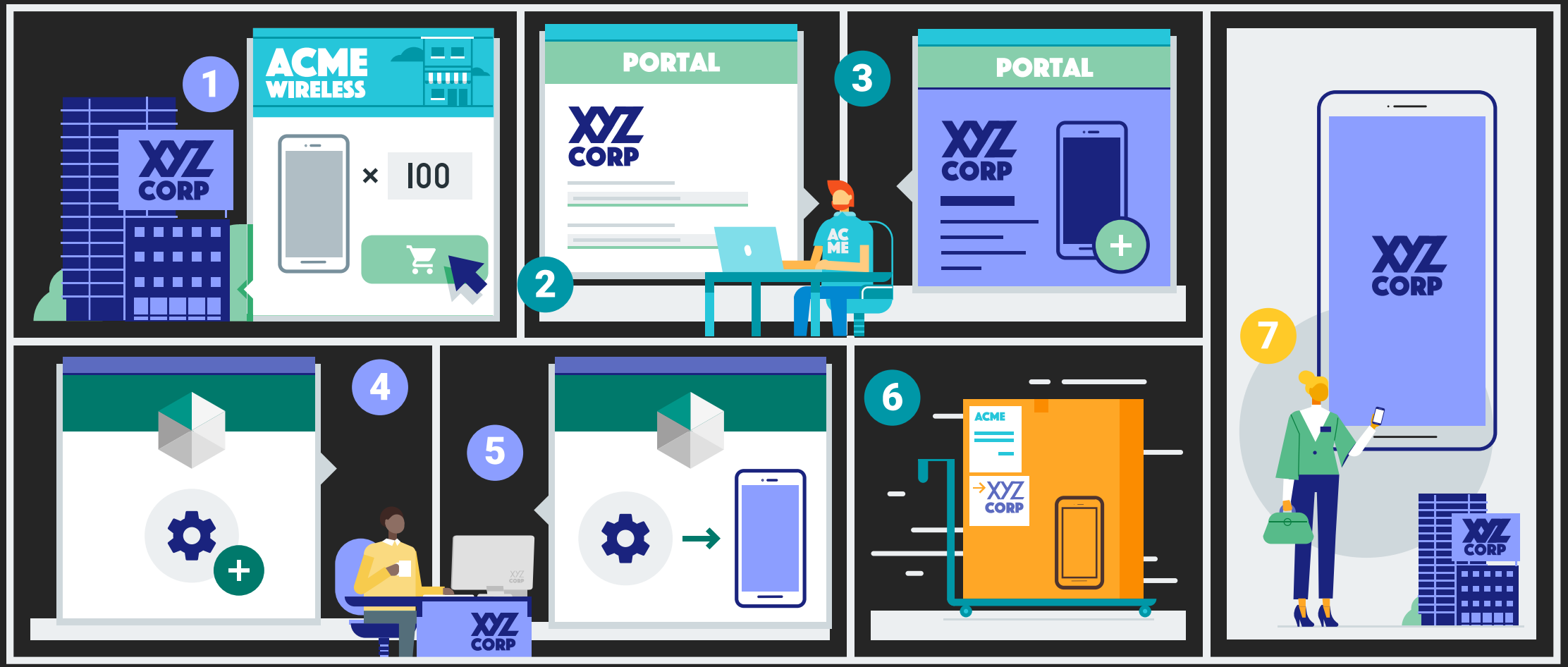


Pictures taken from the Google docs

Android zero-touch

More details about the most promising option

NORDIC
– VIRTUAL SUMMIT –

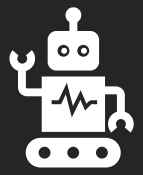


Picture taken from the Google docs

NORDIC
– VIRTUAL SUMMIT –

Personally-owned devices

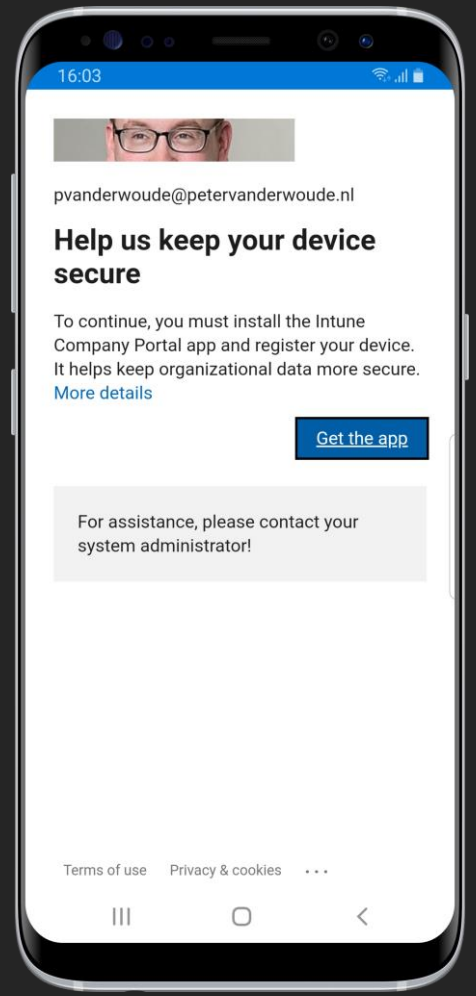
What are the device and app management options for personal devices

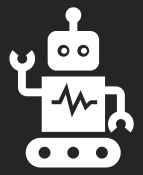


Android device with MAM-only
A brief overview of the main characteristics

NORDIC
– VIRTUAL SUMMIT –

- **Main use case**: Bring Your Own Devices
- Intune SDK or Intune App Wrapping required
- Company Portal app for providing the app protection functionality
- Separate personal account(s) and work account
- Only data in work account is protected
- Administrator can wipe work account from managed app



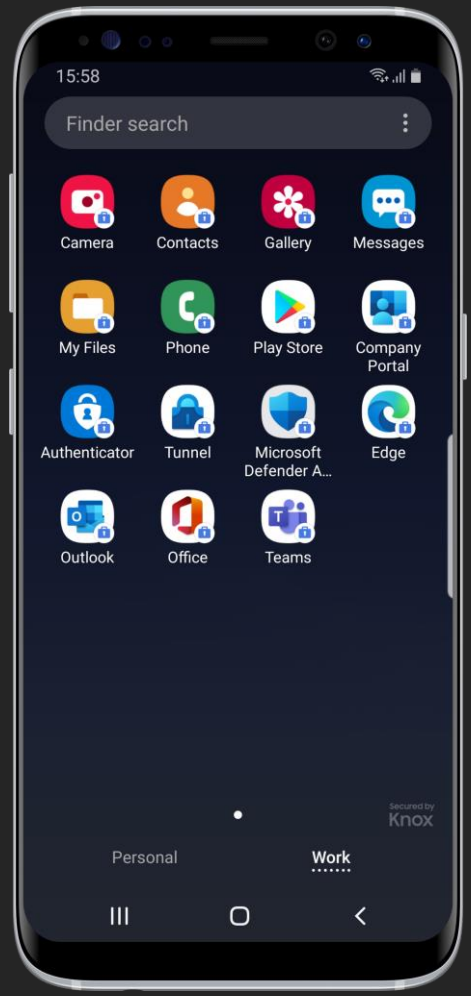


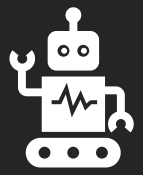
Android device with Work Profile

A brief overview of the main characteristics

NORDIC
– VIRTUAL SUMMIT –

- **Main use case**: Bring Your Own Devices
- Available with Android 5.0 and later
- Provided via the Google Play EMM API
- Company Portal app as the Device Policy Controller (DPC)
- Managed Google Play store for work apps
- Separate personal profile and work profile
- DPC has profile owner permissions within work profile
- Depends on the Google Mobile Services (GMS)
- Administrator can retire Work Profile from device
- Migration path available from Android device administrator

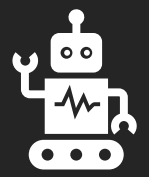




NORDIC
– VIRTUAL SUMMIT –

Corporate-owned devices

What are the device management options for personal devices (with or without app management)

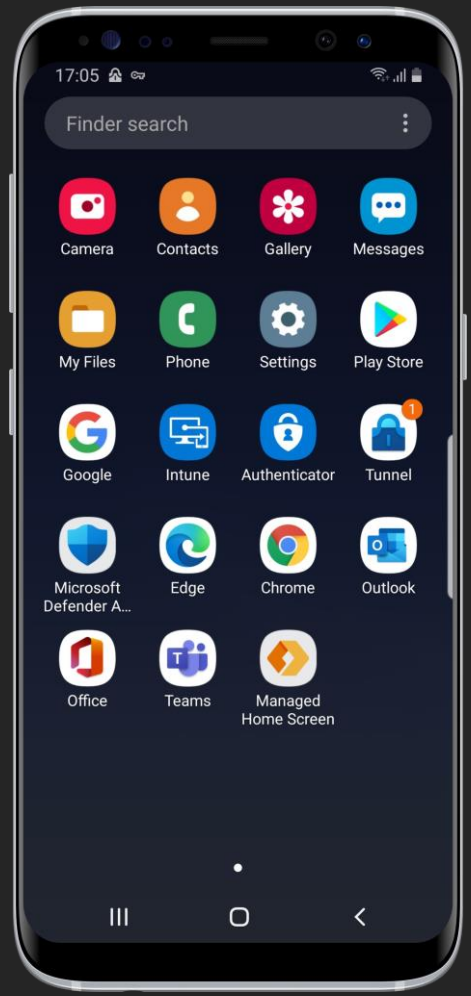


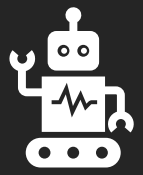
Fully Managed device

A brief overview of the main characteristics

NORDIC
– VIRTUAL SUMMIT –

- **Main use case**: Coorporate-Owned, Business Only devices
- Available for Android 6.0 and later
- Provided via the Android Management API
- Android Device Policy app as the Device Policy Controller (DPC)
- Microsoft Intune app for device compliance
- Managed Google Play store for work apps
- Single profile for work
- DPC has device owner permissions
- Depends on the Google Mobile Services (GMS)
- Administrator can wipe device
- Microsoft Launcher for device customization





Company-branded Fully Managed device

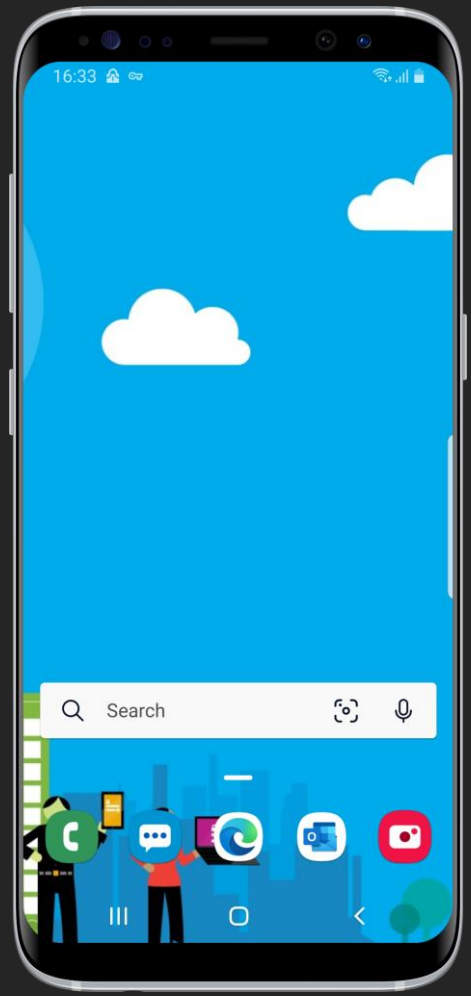
Using the Microsoft Launcher for customizations

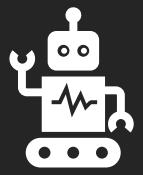
NORDIC
– VIRTUAL SUMMIT –

- Consistent home screen experience
- Device configuration profile to set default launcher
- ~~App configuration policy to customize~~
  Device configuration profile to customize device

New in latest release

- Set wallpaper
- Enable feed
- Set grid
- Set visible apps home screen
- Set application order
- Set dock mode
- Set search bar placement



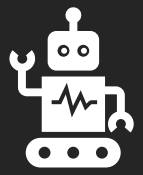


Dedicated device

A brief overview of the main characteristics

NORDIC
– VIRTUAL SUMMIT –

- **Main use case**: Corporate-Owned, Single Use devices
- Available for Android 6.0 and later
- Provided via the Android Management API
- Android Device Policy app as the Device Policy Controller (DPC)
- Microsoft Intune app for device compliance
- Managed Google Play store for work apps
- Single profile for work and dedicated use cases
- Available in single and multi-app variation
- DPC has device owner permissions
- Depends on the Google Mobile Services (GMS)
- Administrator can wipe device



Azure AD shared device mode

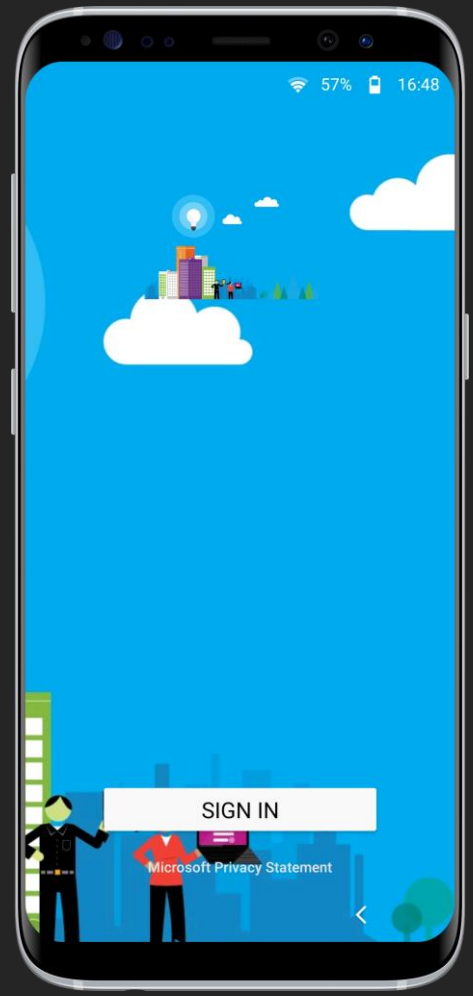
Using the Managed Home Screen for customization

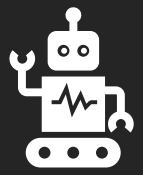
NORDIC
– VIRTUAL SUMMIT –

- Customized sign-in experience
- Enrollment profile to set Azure AD shared device mode
- ~~App configuration policy to customize device~~
  Device configuration profile to customize device

New in latest release

- 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

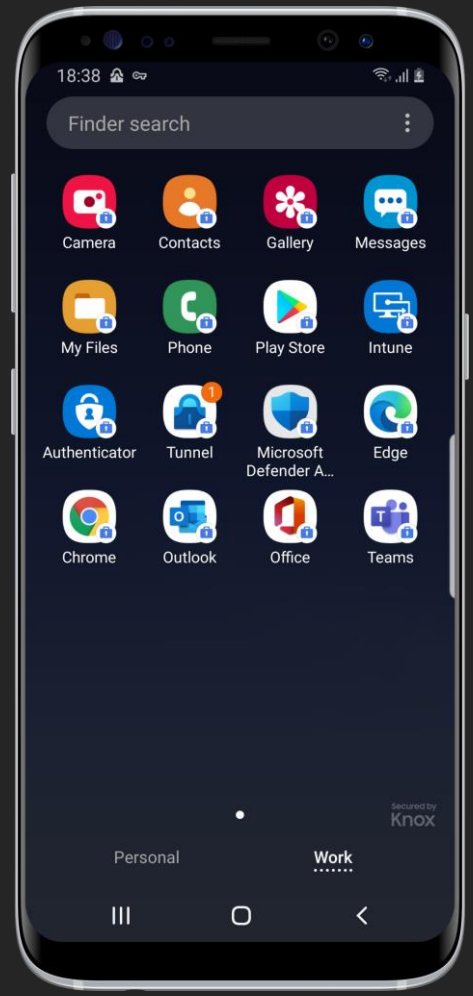




Device with Work Profile

A brief overview of the main characteristics

- **Main use case**: Corporate-Owned devices with Work Profile
- Available for Android 8.0 and later
- Provided via the Android Management API
- Android Device Policy app as the Device Policy Controller (DPC)
- Microsoft Intune app for device compliance
- Managed Google Play store for work apps
- 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



Android management summary

A brief summary of the main characteristics

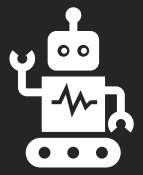
NORDIC
– VIRTUAL SUMMIT –

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 device with Work Profile	Corporate-Owned, Personally Enabled (COPE)	Yes	Yes	NFC, Token, QR code, or Zero touch	Profile owner with device-level settings	Yes	Yes
Fully Managed device	Corporate-Owned, Business Only (COBO)	Yes	No	NFC, Token, QR code, or Zero touch	Device owner	Yes	Yes
Dedicated device	Corporate-Owned, Single Use (COSU)	No	No	NFC, Token, QR code, or Zero touch	Device owner	Yes	No

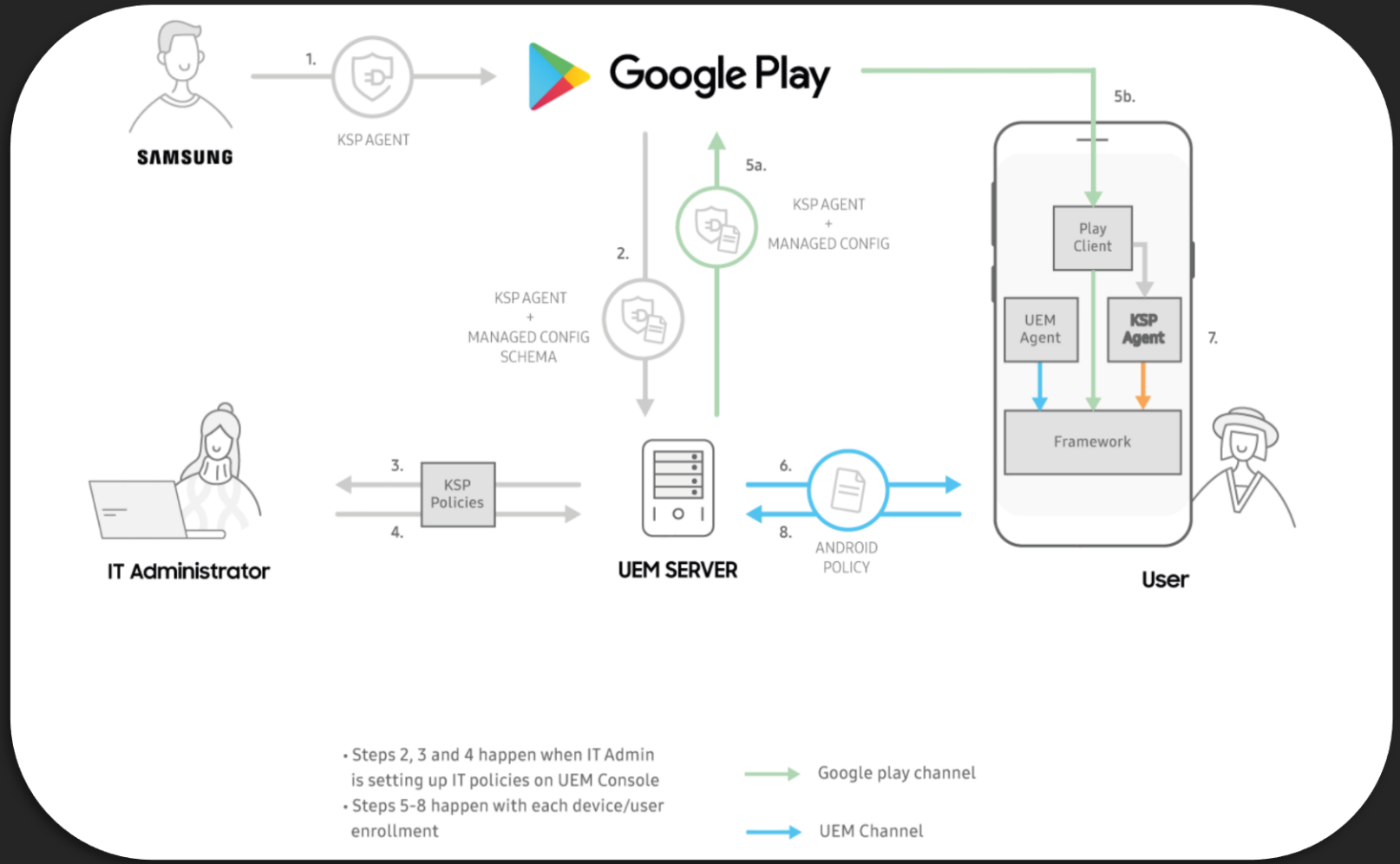
NORDIC
– VIRTUAL SUMMIT –

Additions and integrations

More advanced configurations options and different integrations with a complete Microsoft 365 solution



Support for OEMConfig
The additional configuration layer

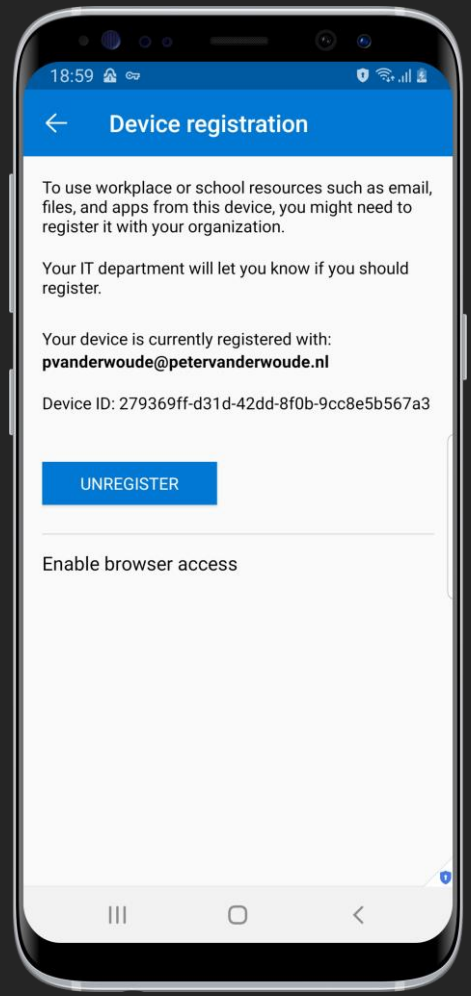


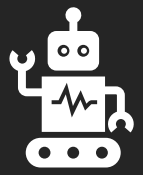
Picture taken from [the Samsung docs]

Support for Conditional Access
Provide secure access to company data

NORDIC
– VIRTUAL SUMMIT –

- Device-based Conditional Access
  - Require device to be marked as compliant
    - Microsoft Defender for Endpoint, Device Health, Device Properties, System Security
    - Location only for legacy Android management
  - Personally-owned devices require Company Portal app
  - Corporate-owned devices require Authenticator app
- App-based Conditional Access
  - Require approved client app
  - Require app protection policy



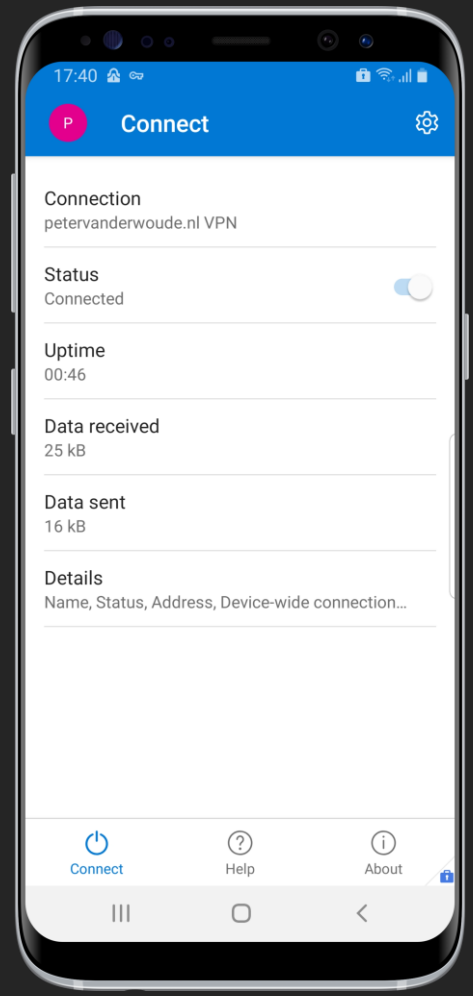


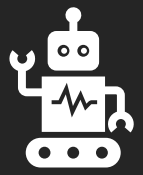
Support for Microsoft Tunnel Gateway

Provide secure access to on-premises resources

NORDIC
– VIRTUAL SUMMIT –

- Docker container that runs on a Linux server
- Server and site configuration options available
- Uses the Microsoft Tunnel app
- Provides single sign-on experience
- Configuration via a VPN profile
- Provides per-app and device-based VPN
- Included in the Microsoft Intune license!



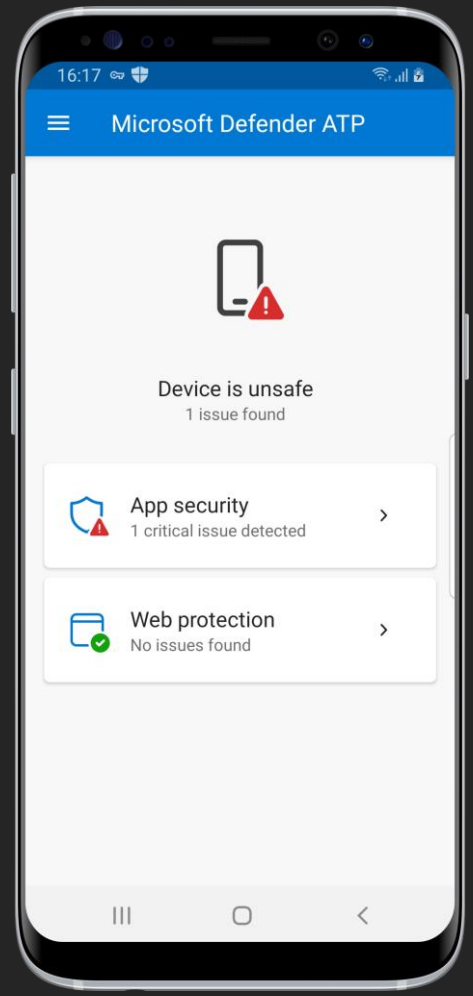


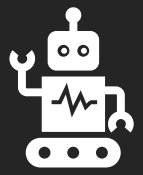
Support for Microsoft Defender for Endpoint

Provide app and web security on the device

NORDIC
– VIRTUAL SUMMIT –

- 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
- Requires additional licensing





Thank you!

MSEndPointMgr.com
#MSEndPointMgr

System Center User Group Finland
#SCUGFI

System Center User Group Denmark

#SCUGDK

System Center User Group Sweden
#SCUGSE

Modern Management User Group Norway
#MMUGNO