|  |
| --- |
|  |
|  |
| **D** |
|  |
|  |
|  |
|  |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  |  |  |  |  | |  | **Detailed design Mobile devices** |  |  |  | |  | <Customer> |  |  |  | |  |  |  |  | |  |  |  |  |  | |
|  |
|  |
|  |
|  |
|  |

Versie informatie

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Bijzonderheden | Auteur |
|  |  |  |  |

Verzendlijst

|  |  |
| --- | --- |
| Titel |  |
|  |  |

Inhoudsopgave

[1 Purpose of this document 1](#_Toc36219090)

[1.1 Scope 1](#_Toc36219091)

[2 Requirements and solution direction 2](#_Toc36219092)

[2.1 Requirements and use case 2](#_Toc36219093)

[2.2 Solution 2](#_Toc36219094)

[3 Design 4](#_Toc36219095)

[3.1 Technical requirements 4](#_Toc36219096)

[3.2 Device Requirements 4](#_Toc36219097)

[3.2.1 Android 4](#_Toc36219098)

[3.2.2 iOS 4](#_Toc36219099)

[3.3 Deployment and management platform 5](#_Toc36219100)

[3.3.1 Support for Android devices 5](#_Toc36219101)

[3.3.2 Support for Apple devices 7](#_Toc36219102)

[3.4 Configuration and compliance policies 9](#_Toc36219103)

[3.4.1 Compliance policies 10](#_Toc36219104)

[3.4.2 Device configuration Policies 12](#_Toc36219105)

[3.5 Applications: provisioning and protection 14](#_Toc36219106)

[3.5.1 Application provisioning 14](#_Toc36219107)

[3.5.2 Application protection policies 15](#_Toc36219108)

[3.6 OS Updates 17](#_Toc36219109)

# Purpose of this document

Welcome to the detailed technical design document for the Mobile devices. This document describes the technical design for the Mobile devices (Apple and Android) that will be used in the workspace environment for <Customer>, Sogeti Smart Workspace (SSW).

## Scope

This document is limited to devices with the operating system for mobile devices; Android, iOS and iPadOS. These mobile devices will be used for providing users with a device that can be used for secure access to the <Customer> Office 365 apps and content, and to <Customer> approved apps;

This design covers the onboarding and configuration for mobile devices into the SSW platform. The following items are partly covered in this design only. Because these items are important for the configuration, use and user experience, they will be mentioned in this design:

* Devices will be registered to Azure Active Directory;
* Device management is covered by Microsoft Intune;
* Conditional Access for Office 365 is covered from the Collaboration platform;

# Requirements and solution direction

## Requirements and use case

In the SSW, <Customer> will be using iOS and Android devices for where these concern company owned devices. As the SSW is cloud based, these devices will be registered in Azure Active Directory (AAD) and managed with Microsoft Intune.

The devices will be provided with a base set of local applications only. Line of Business Applications (LOB) will be offered through SaaS, Web or approved apps that users can install from the (device specific-) app store.

Mobile devices that are provided to users by Securitas will be enrolled into Intune as company owned devices. Users who want to use their personal device, need to enroll their device first and comply with base requirements. These devices will be enrolled as personal devices.

## Solution

The table below shows the different tiers that are defined for the various devices and use cases (scenario’s) in the Securitas IT Workplace for SSW:

|  |  |  |  |
| --- | --- | --- | --- |
| **Tier 1: High Security Devices​** | **Tier 2: Standard Corporate Devices​** | **Tier 3: Low trust Devices​** | **Tier 4: Unmanaged Devices​** |
| **Description**​  High Security devices operate in data environment containing highly sensitive data. These devices are restricted from connecting to less trusted data environments. ​ | **Description**​  The standard corporate device is a Securitas managed device that can access most business application and can connect to the corporate network. This device type is the most common device for office workers. ​ | **Description**​  Low trust devices are devices operating in a low data environment with limited control. These devices are not allowed to connect to (or are segmented from) the Securitas corporate network and only has access to a very limited set of business applications and limited access to sensitive information. ​ | **Description**​  Unmanaged devices are devices that are not managed and controlled by Securitas and therefore no policies and controls can be enforced on the device itself. The devices can be used to read some business data but not allowed to store the data on device itself\* ​ |
| **Characteristics**​  Exposure: Low​  Business Impact if stolen or compromised: High​  Access to sensitive information: Yes​  Allowed on high trust network​ | **Characteristics**​  Exposure: Medium/High ​  Business Impact if stolen or compromised: Medium/High​  Access to sensitive information: Yes​  Allowed on corporate network​ | **Characteristics**​  Exposure: High​  Business Impact if stolen or compromised: Low​  Access to sensitive information: Limited​  Only allowed on isolated network (e.g. guest network) ​ | **Characteristics**​  Exposure: High ​  Business Impact if stolen or compromised: None​  Access to sensitive information: Limited​  Only allowed on isolated guest networks​ |

Management for mobile devices covers the following tiers:

* Tier 2: This profile involves the company (Securitas) owned mobile devices
* Tier 3: This profile involves personal devices, owned by Securitas employees

Both iOS and Android support different scenarios for enrollment, where each scenario may have different options and features for support and management. The following principles are used in the solution:

* All devices, company owned and personal, need to be enrolled into management before they can be used to consume Securitas content and services;
* After enrollment, devices need to comply with base security requirements;
* Company owned devices will use Zero Touch deployment when this is supported, depending on the device manufacturer and reseller;
* Android devices will be managed using Android Enterprise, device administrator management for Android will be deprecated;
* iOS devices will be enrolled using the Apple Device Enrollment Program (DEP, renamed to Apple Business Manager), depending support from the reseller;

During onboarding, the devices are enrolled into Microsoft Intune after which configuration settings (policies) and mandatory software is pushed to the device. This includes the following settings and applications:

* Minimum security configurations that must be met before connection to Securitas Business services is enabled. For example, the requirement for a pin code to unlock the device and encryption of storage on the device;
* Device management software like Microsoft Intune and the Microsoft Authenticator App;
* Productivity software like MicrosoftOffice 365 ProPlus;

Company owned devices are configured with additional required settings (outlined in the following chapters).

After onboarding, users will be able to connect to Securitas business services with their mobile device and install apps from the app store. Users will be able to only install approved apps in the managed area on the device.

Using Microsoft Intune, the Securitas IT organization (service management, security management and IT Support) can manage and monitor the onboarded devices:

* Onboard and retire devices into and from management
* Inventory of all onboarded company owned and personal devices;
* Apply configuration and security settings;
* Offer optional or push required applications to the managed devices;
* Control access policies to business applications using conditional access and device compliance;
* Remotely wipe devices or business data in case of lost or stolen devices;

# Design

## Technical requirements

To enable management for mobile devices, the following technical requirements must be met:

* An Intune standalone tenant must be used. This means the mobile device management (MDM) authority must be set to Microsoft Intune.
* To enable management for iOS devices, an Apple MDM push certificate must be created and enabled. This certificate has a limited lifetime and needs to be renewed periodically (typically once every year). The certificate is to be created using a Company Apple ID that is registered with a business (Securitas) email account, preferably shared.
* Users must have an Intune license. For conditional access and MFA, users also need an Azure Active Directory P1 license. Both are part of the EM+S subscription.

Additional configurations and settings may be required to support bulk enrollment scenarios, these are covered on the device specific paragraphs for enrollment and provisioning.

Note: in production above settings are already configured.

## Device Requirements

This section defines the recommended device requirements to support the required configurations and enrollment scenarios.

### Android

The Microsoft minimum requirement for Android devices that can be managed by Intune is that the device is running Android 5.0 or higher. The preferred management profile is based on Android Enterprise which is supported as well on devices running Android 5.0 or newer. Over time, Android Enterprise has evolved, and older devices do not support all available features. The following table shows the recommended requirement as specified by Google (<https://androidenterprisepartners.withgoogle.com/glossary/device/>). The minimum version for the OS is mainly given by the requirement for Zero Touch deployment.

|  |  |
| --- | --- |
| Hardware | Requirement |
| OS | Android 8.0+ |
| CPU | 1.4 GHz |
| RAM | 2 GB |
| Storage | 32 GB |
| Battery life | 8+ hours |
| Camera | 2MP / 10MP |
| Architecture | 64 bits |

### iOS

Microsoft Intune supports management for Apple devices that meet the following criteria:

* Apple iOS 11.0 and later
* Apple iPadOS 13.0 and later

## Deployment and management platform

This paragraph describes the options and characteristics available to deploy and manage mobile devices within the SSW Platform. This paragraph breaks down further to support for Android devices and Apple devices.

Within the scope of management for mobile devices, you can manage de device (enroll in Mobile Device Management, MDM) or manage the applications on the device (enroll in Mobile Application Management, MAM).

#### MDM Managed devices

In this model, Intune manages the complete device. This means that the device is enrolled into Intune MDM and Intune can configure and restrict the device by enforcing policies. This also includes a compliance policy in which conditions are specified on which devices will get state *Compliant* (all conditions are met) or *Non-Compliant* (one or more conditions do not meet requirements). The compliance state can be used to monitor (basic) health and can be used in Conditional Access policies. Also, applications can be managed from Intune, either required or available for users to optionally install applications. When devices are lost or stolen, IT administrators can remotely wipe the device, so all company resources are removed from the device in order to prevent security breaches.

Using this model, the device is registered in Azure Active Directory and enrolled in Intune.

MDM management can be used for corporate (Securitas owned) devices or personal (employee owned, BYOD) devices. MDM management is only possible when the device is not already managed by another company or other third-party MDM solution.

#### MAM Managed devices

In this model, not the device is managed but the applications on the device. This will allow Securitas to protect company data that is used in the managed applications. This requires the app is protected using an application protection policy. This policy specifies requirements and app behavior to enable the use of the targeted app, in combination with company data and services. Using MAM, IYT administrators can offer applications that can be installed by users, depending on the OS (Android vs iOS). When the device is lost or stolen or when the user leaves the company, company data can be removed using an app selective wipe. Any personal data on the device is kept, company data is removed.

MAM management can be used for personal (employee owned, BYOD) devices or when the device is managed by another third-party MDM solution. When the device already is managed by the Securitas Intune tenant, MAM can be combined with the MDM model.

**Design decision**: MDM+MAM is used for all mobile devices used to consume Securitas business content and applications, both company-owned and personal devices. For company owned devices already managed by a third-party MDM solution, MAM only will be used.

### Support for Android devices

Intune supports the following deployment and management options for devices that run the Android operating system:

| Model | Use case | Supported in SSW |
| --- | --- | --- |
| Device Administrator | Used to enroll personal and company owned devices into Intune Management | No (this model will be deprecated) |
| Android Enterprise work profile | Used for personal devices, only a container for work content is managed | Yes (BYOD, tier 3 scenario) |
| Android Enterprise dedicated devices | Used for company owned kiosk or single purpose devices | No |
| Android Enterprise fully managed | Used for company owned devices, complete device is managed | Yes (CYOD, tier 2 scenario) |
| MAM Without enrollment | BYOD or Company owned when already managed by third party MDM | Yes (specific devices within Securitas) |

#### Enable Android Enterprise

Before any of the Android Enterprise models can be used, the feature needs to be enabled in the Intune portal by connecting Intune to the Securitas Managed Google Play Account, using a (corporate) Google account.

**Design decision**: Since the use if Android Enterprise is preferred, the Intune Account will be connected to the Managed Google Play account.

Note: in production this connection is already configured.

#### Android Enterprise Work profile

This model is used to support (grant permissions to) personal devices to work with company apps and data. Accounts, data and apps can be managed by the organization (Securitas) by using a separate work profile. This profile is separate from personal apps and data where Securitas IT Administrators cannot access personal apps and data.

The ability to enroll devices with Android Enterprise work profile needs to be enabled for users. By default, the option is enabled for new tenants.

When users already have their device enrolled using the device administrator, the need to re-enroll their device in Intune. This can be forced by IT Admins to initiate a remote Retire action from the Intune management console.

Users can enroll their device by installing the Intune Company portal and launch the enrollment procedure (<https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-work-profile>).

#### Android Enterprise fully managed

With an Android Enterprise fully managed device, IT administrators can manage the entire device, enforce policies and deploy applications. This model typically is used for company owned devices. To enable this feature, enrollment for Fully Managed devices needs to be enabled in Intune. When enabled, an enrollment token and QR code are generated which can be used for users enrolling their device.

**Design decision**: The use of Android Enterprise Fully Managed will be enabled in Intune.

Depending on the Android OS version, the following options exist to enroll a device into full management:

* Near Field Communication (NFC), for Android 5.1 and above
* Token, for Android 6 and above
* QR Code, for Android 7 and above
* Google Zero Touch, for Android 8 and above

The use of Google Zero Touch can only be used for specific manufacturers and the reseller must be in the program.

**Design decision**: The use of Google Zero Touch deployment is used, with a fallback using QR code when devices or the reseller do not support Google Zero Touch.

#### Android Enterprise Dedicated

This model will not be used for Securitas and will also not be enabled.

**Design decision**: The use of Android Enterprise Dedicated will not be enabled in Intune.

#### Device Administrator

This model, also referred to as legacy enrollment, is the standard way for enrolling devices prior to the ability and support for Android Enterprise in Intune. This model will be deprecated and already is no longer supported for new devices running Android 10.

**Design decision**: The use of Device Administrator will be disabled in Intune.

Today, many Securitas company owned devices already are enrolled using the device administrator model in the production environment. In order to enroll them using the Android Enterprise Fully Managed model, they need to be reset to factory defaults and then re-enrolled into management. This can be achieved by remotely wiping the device from the Intune management portal. The drawback of this approach is that users also loose their apps, settings and data stored on the device. Depending on the requirements, an alternative is to disable enrollment for new devices using the device administrator model but allow devices that are enrolled today using this model. When the user replaces the device with a new one, it will be enrolled using Android Enterprise Fully Managed.

#### MAM without enrollment

In this model, the device is not enrolled into MDM management. Instead, the device is Azure Active Directory registered and while doing this, MAM policies (application protection) can be enforced for managed applications specified in the policy.

**Design decision**: The use of MAM is used for specific company devices that currently are managed through a third-party MDM solution.

### Support for Apple devices

Intune supports the following deployment and management options for devices that run the iOS or iPadOS operating system. Within these options, Apple distinguishes between user owned (BYOD) or Company owned devices.

#### User Owned devices

For User owned devices, users can enroll the device using Device Enrollment or using User Enrollment. User Enrollment currently is in preview and therefore is not covered in this design.

To enroll a personal device into management with Intune, users need to install the Company Portal App from the App Store and follow the instructions. In these instructions, users have the option to secure the device (device enrollment) or secure work-related apps and data only (user enrollment). User enrollment only supports a subset of the configuration policies, device enrollment supports more policies.

When the use of personal owned devices is not allowed, the ability to enroll personal devices can be blocked using device restrictions in Intune.

After enrollment, configuration and compliance policies can be targeted to the enrolled device. When compliant, users can be granted access to company resources using conditional access policies which require a compliant device is to be used.

**Design decision**: The use of personal Apple devices (iOS/iPadOS) is not restricted. Users can enroll their device to access company resources. They need to be compliant before access to resources is granted.

#### Company owned devices

For company owned devices, Apple and Intune offer the following options:

* Apple's Device Enrollment Program (DEP)
* Apple School Manager
* Apple Configurator Setup Assistant enrollment
* Apple Configurator direct enrollment

Apple School manager is only for educational organizations and the use of Apple Configurator does not comply with the principle of Zero Touch deployment. Therefore, the chosen option for company owned devices is to use Apple’s device enrollment program (DEP).

**Design decision**: Company owned Apple Mobile devices will use DEP for enrollment.

In order to enable deployment with DEP, the following prerequisites must be met:

* Devices must be purchased in Apple DEP. This requires a reseller that supports this model and devices must be registered in Apple Business Manager.
* Apple DEP Token must be configured. This creates a connection between Intune and Apple Business Manager. Devices configured in Apple Business Manager will be imported into Intune.

**Design decision**: An Apple DEP token is created, and Intune is connected to Apple Business Manager to support enrollment using DEP

For enrollment, an enrollment profile needs to be created in Intune. This profile is assigned to devices that are enrolled in the organization and provides default settings for the devices. All settings will be described in a profile document, the important settings are in below table:

| Setting | Value | Rationale / Comments |
| --- | --- | --- |
| User Affinity | Enroll with User Affinity | Devices are personal, assigned to a specific user. Without user affinity, the Company Portal cannot be used. |
| Management Options | Supervised | Supervised devices give more management options and disabled Activation Lock by default. Microsoft recommends using DEP as the mechanism for enabling supervised mode, especially if you're deploying large numbers of iOS/iPadOS devices. |
| Locked enrollment | Yes | disables iOS/iPadOS settings that allow the management profile to be removed from the Settings menu |

The profile is synced with Apple Business manager and then assigned to devices. To circumvent no profile is assigned, a default profile can be selected. This is assigned to all devices enrolled with the specific token. Multiple tokens can be used, for instance when multiple resellers are used.

#### MAM without enrollment

In this model, the device is not enrolled into MDM management. Instead, the device is Azure Active Directory registered and while doing this, MAM policies (application protection) can be enforced for managed applications specified in the policy.

**Design decision**: The use of MAM is used for specific company devices that currently are managed through a third-party MDM solution.

## Configuration and compliance policies

Both Android and Apple devices in Intune, support different types of policies, depending on the type of configuration you need to make:

* Compliance policies

These conditions determine the state of a device compared to company requirements. If the device meets conditions, it will be marked as compliant. Compliant devices can be given access to company resources in conditional access rules

* Configuration, or device restriction policies

Used to configure and restrict the device features and settings

* Wi-Fi profile

Used to preconfigure a Wi-Fi profile on the device

* Trusted certificate

Enroll a trusted certificate, for example a Root certificate for the organization’s PKI (Public Key Infrastructure)

* VPN

Configure settings for VPN connections

* PKCS or SCEP certificate enrollment configuration

This controls certificate enrollment using the Intune connector to the companies PKI infrastructure

This paragraph describes the compliance and device restrictions policies. The other policies are self-explaining or fill in a functional requirement, depending on the country or business unit within Securitas.

### Compliance policies

Compliance policies are used to fulfill the following needs:

* Provide insight in the state of enrolled devices in relation to company specified conditions
* Grant access to company resources only for devices that are compliant with company specified conditions

Devices can only become compliant when they are enrolled into Intune management. Unenrolled devices are non-compliant by default.

With above statement in mind, compliance policies have the following limitations:

* Only predefined conditions can be checked in compliance policies. You determine which of them are included in your checks, but you cannot add custom conditions;
* To use device compliancy in conditional access, the company resource needs to use Azure Active Directory for authentication. For example, this is the case for Office 365 applications like Exchange Online and SharePoint Online;

For both Apple and Android devices, compliance policies differ in capabilities for the enrollment scenario that is chosen for the device. The policies described in this paragraph only detail the settings which are actually set or configured which means those settings which do not have a value of ‘not configured’.

#### Compliance policy for Apple devices (iOS and iPadOS)

The following settings are configured in the compliance policy for devices running iOS or iPadOS:

| Category | Setting | Default Value | Proposed Value |
| --- | --- | --- | --- |
| Device Health | Jailbroken Device | Not Configured | Block |
|  | Require the device to be at or under the Device Threat Level | Not Configured | Not Configured (requires third party product) |
| Device Properties | Minimum OS version | Not Configured | 12 |
| System Security | Require a password to unlock mobile devices1 | Not Configured | Required |
|  | Simple passwords | Not Configured | Block |
|  | Minimum password length | 4 | 6 |
|  | Required password type | Not Configured | Numeric |
|  | Maximum minutes after screen lock before password is required | Not Configured | 5 minutes |

1. The settings for password only apply for devices using device enrollment or automated device enrollment (DEP). On devices that are enrolled with user enrollment, the password is set to a minimum of 6 characters and simple passwords are blocked, regardless the settings configured in the policy.

The compliance policy is targeted to all users with an Apple mobile device.

#### Compliance policy for Android devices

For Android devices, the following compliance are possible:

* Android Device Administrator
* Android Enterprise Device Owner (Dedicated and Fully Managed)
* Android Enterprise Work Profile

In SSW, we will not enroll new devices with the Device Administrator model, a policy is kept as support for existing devices in the production environment.

**Policy for Android Enterprise Work Profile**

| Category | Setting | Default Value | Proposed Value |
| --- | --- | --- | --- |
| Device Health | Rooted Devices | Not Configured | Block |
|  | Google Play Services is configured | Not Configured | Require |
|  | Up-to-date security provider | Not Configured | Require |
|  | SafetyNet device attestation | Not Configured | Check Basic Integrity |
| System Security | Require a password to unlock mobile devices | Not Configured | Required |
|  | Required password type | Not Configured | Numeric Complex |
|  | Minimum password length | Not Configured | 6 |
|  | Maximum minutes of inactivity before password is required | Not Configured | 5 minutes |
|  | Encryption of data storage on device | Not Configured | Require |

**Policy for Android Enterprise Fully Managed**

| Category | Setting | Default Value | Proposed Value |
| --- | --- | --- | --- |
| Device Health | Require the device to be at or under the Device Threat Level | Not Configured | Not Configured (requires third party product) |
|  | SafetyNet device attestation | Not Configured | Check Basic Integrity |
| Device Properties | Minimum OS version | Not Configured | 9 |
| System Security | Require a password to unlock mobile devices | Not Configured | Required |
|  | Required password type | Not Configured | Numeric Complex |
|  | Minimum password length | Not Configured | 6 |
|  | Maximum minutes of inactivity before password is required | Not Configured | 5 minutes |
|  | Encryption of data storage on device | Not Configured | Require |

**Policy for Android Device Administrator devices**

| Category | Setting | Default Value | Proposed Value |
| --- | --- | --- | --- |
| Device Health | Rooted Devices | Not Configured | Block |
| System Security | Require a password to unlock mobile devices | Not Configured | Required |
|  | Required password type | Not Configured | Numeric Complex |
|  | Minimum password length | Not Configured | 6 |
|  | Maximum minutes of inactivity before password is required | Not Configured | 5 minutes |
|  | Encryption of data storage on device | Not Configured | Require |

### Device configuration Policies

Device restriction policies configure or restrict settings and features on the mobile devices to fulfill the following needs:

* Protect against service calls because users misconfigure their device;
* Protect against unwanted configurations which can cause security issues;
* Protect users to make use of undesired features or services on company owned devices. This includes but is not limited to security related features.

As with the compliance policies, different restriction policies exist based on make (Apple vs Android) and deployment model. This paragraph details the proposed policies for configured settings. Please bear in mind that available policies can change over time because of new capabilities in the devices/OS and new features that Intune supports in the future.

#### iOS and iPadOS

For iOS/iPadOS Device Features and Device Restrictions can be configured in separate policies. In the production environment, no policy is configured at this moment in time (March 2020). Below mentioned policies are proposed values and need confirmation.

| Category | Setting | Default Value | Proposed Value |
| --- | --- | --- | --- |
| General | Share usage data | Not Configured | Block |
|  | Untrusted TLS certificates | Not Configured | Block |
|  | Limit ad tracking | Not Configured | Limit |
| App Store, Doc Viewing, Gaming | Download content from iBook store flagged as 'Erotica' | Not Configured | Block |
|  | Explicit iTunes music, podcast, or news content | Not Configured | Block (requires iOS 13) |
|  | Adding Game Center friends | Not Configured | Block (requires iOS 13) |
|  | Game Center | Not Configured | Block |
|  | Multiplayer gaming | Not Configured | Block (requires iOS 13) |

| Built in Apps | Siri | Not Configured | Block |
| --- | --- | --- | --- |
|  | Siri while device is locked | Not Configured | Block |
|  | Siri profanity filter | Not Configured | Block |
|  | Block removal of system apps from device | Not Configured | Block |
| Wireless | Personal Hotspot | Not Configured | Block |
| Connected Devices | Apple Watch pairing | Not Configured | Block |
|  | Block setting up new nearby devices | Not Configured | Block |
| Cloud and Storage | Encrypted backup | Not Configured |  |
|  | Managed apps sync to cloud | Not Configured |  |
|  | Block Enterprise Book Backup | Not Configured |  |
|  | Block enterprise book metadata sync (notes and highlights) | Not Configured |  |
|  | Photo stream syncing to iCloud | Not Configured |  |
|  | iCloud Photo Library | Not Configured |  |
|  | Shared photo stream | Not Configured |  |
|  | Handoff | Not Configured | Block |
|  | Backup to iCloud | Not Configured |  |
|  | Block iCloud Document sync | Not Configured | Block |
|  | Block iCloud Keychain sync | Not Configured | Block |

**Android Enterprise – Work profile**

| Category | Setting | Default Value | Proposed Value |
| --- | --- | --- | --- |
| Work profile settings | Copy and paste between work and personal profiles | Not Configured | Block |
|  | Data sharing between work and personal profiles | Device Default | Apps in work profile can handle sharing request from personal profile |
|  | Work profile notifications while device locked | Not Configured | Block |
|  | Default app permissions | Device Default | Prompt |

|  | Add and remove accounts | Not Configured | Block |
| --- | --- | --- | --- |
|  | Screen capture | Not Configured | Block |
|  | Require Work Profile Password | Not Configured | Require |
|  | Minimum password length | Not Configured | 6 |
|  | Maximum minutes of inactivity until work profile locks | Not Configured | 5 Minutes |
|  | Required password type | Not Configured | Numeric Complex |
| System security | Threat scan on apps | Require | Require |

**Android Enterprise – Fully managed**

| Category | Setting | Default Value | Proposed Value |
| --- | --- | --- | --- |
| General | Factory reset | Not Configured | Block |
|  | Safe boot | Not Configured | Block |
|  | Tethering and access to hotspots | Not Configured | Block |
|  | System update | Device Default | Maintenance Window |
|  | Start time | Not Configured | 7 PM |
|  | End time | Not Configured | 7 AM |
| System security | Threat scan on apps | Require | Require |
| Device Password | Required password type | Not Configured | Numeric Complex |
|  | Minimum password length | Not Configured | 6 |
| Power Settings | Time to lock screen | Not Configured | 5 minutes |
| Users and Accounts | Add new users | Not Configured | Block |
|  | User removal | Not Configured | Block |
|  | Personal Google Accounts | Not Configured | Block |
|  | User can configure credentials | Not Configured | Block |
| Applications | App auto-updates | Not Configured | Wi-Fi Only |
|  |  |  |  |

## Applications: provisioning and protection

Configuration for applications falls into two parts:

* Provisioning of applications, including black- and/or whitelisting of apps
* Application protection policies to secure company data used in apps on mobile devices

### Application provisioning

In Intune, client apps can be configured for installation to offer the following types of apps:

* Apps from the Apple Store or Google Play store;
* A Web link to an app on the internet;
* A Line of Business App (app needs to be available as an apk or ipa package);

After configuration in the Intune console, the app is assigned to users or devices, with the ability to push the app (make it Required) or offer it for users to install the app at their convenience (Available).

Apart from app installation from Intune, Apple and Android devices use their own app stores where users can select and install (purchase) apps. On personal devices, users may be used to search for any application they like or want to use, select it, install it and use it. For company owned devices, we typically want to have more control to make sure only trusted and approved apps are used. Furthermore, we might want to push certain apps to these devices in order them to be ready for use, right after configuration of the device.

There are several ways to achieve the goals of the company’s policy, depending on the device and deployment model.

* Android Enterprise Work profile:
  + Users can install all apps in the personal profile, users can only install (approved) apps from the managed Google Play Store
  + The feature ‘Threat scan on apps​’ scans apps and when a threat is found, a warning is sent to the user to remove the app. This feature is turned on by default.
* Android Enterprise fully managed:
  + By default, users can only install (approved) apps from the managed Google Play Store. There is a policy which allows the install all apps in the Google Play Store.
  + The feature ‘Threat scan on apps​’ scans apps and when a threat is found, a warning is sent to the user to remove the app. This feature is turned on by default.
* iOS and iPadOS:
  + By default, users can install apps from the app store. The store can be blocked with a policy;
  + Restricted apps can be added to the compliance policy. If one or more restricted apps are found on a device, the device is marked as non-compliant. Users need to uninstall the restricted app before the device can be marked compliant again.
  + Using a Device Restriction policy, a list of Approved Apps or Prohibited Apps can be configured to get insight in the use of those apps on managed devices.
  + With the Show or Hide Apps policy, a list of apps can be configured that users can or cannot see or launch.

**Design decision**: No restrictions will be configured on the installation or use of apps.

### Application protection policies

With application protection policies, rules and conditions can be specified and pushed to devices, in order to protect company data that is used in (managed) apps on mobile devices. Application protection policies, in combination with Conditional Access, contribute in Mobile Application Management (MAM). The policies can be configured for use on devices with – or devices without enrollment or for both. The default policy in SSW will be that there is no differentiation in enrollment.

On high level, application protection policies force that company data is stored in an encrypted container on the device and can be used only from managed applications. Data cannot be copied or shared with unmanaged applications. Next to this, requirements are configured for the device, similar to the device compliancy checks.

Before an apps can make use of the protection policies, it needs to be integrated with the Intune SDK or wrapped with the Intune App Wrapping tool. A list of apps is available from Intune that already is integrated and ready for use.

Also, for this type of policies, the ability depends on the device type:

#### Android

| Category | Item | Proposed Value |
| --- | --- | --- |
| Apps | Public Apps | All available apps are protected |
|  | Custom Apps | com.adobe.reader.intune  com.microsoft.o365smb.connections |
| Data protection | Prevent backups | Block |
|  | Send org data to other apps | Policy managed apps |
|  | Save copies of org data | Block |
|  | Allow user to save copies to selected services | OneDrive for Business  SharePoint |
|  | Receive data from other apps | All apps |
|  | Restrict cut, copy, and paste between other apps | Any App |
|  | Screen capture and Google Assistant | Enable |
|  | Encrypt org data | Require |
|  | Encrypt org data on enrolled devices | Require |
|  | Sync app with native contacts app | Allow |
|  | Printing org data | Allow |
|  | Restrict web content transfer with other apps | Allow |
|  | Org data notifications | Allow |
| Access requirements | PIN for access | Require |
|  | PIN type | Numeric |
|  | Simple PIN | Block |
|  | Select minimum PIN | 6 |
|  | Fingerprint instead of PIN for access (Android 6.0+) | Allow |
|  | App PIN when device PIN is set | Require |
|  | Recheck the access requirements after (minutes of inactivity) | 30 |

#### iOS and iPadOS

| Category | Item | Proposed Value |
| --- | --- | --- |
| Apps | Public Apps | All available apps are protected |
|  | Custom Apps | com.adobe.reader.intune  com.microsoft.o365smb.connections |

| Data protection | Prevent backups | Block |
| --- | --- | --- |
|  | Send org data to other apps | Policy managed apps |
|  | Select apps to exempt | Default: tel;telprompt;skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services; |
|  | Save copies of org data | Block |
|  | Allow user to save copies to selected services | OneDrive for Business  SharePoint |
|  | Receive data from other apps | All apps |
|  | Restrict cut, copy, and paste between other apps | Any App |
|  | Screen capture and Google Assistant | Enable |
|  | Encrypt org data | Require |
|  | Encrypt org data on enrolled devices | Require |
|  | Sync app with native contacts app | Allow |
|  | Printing org data | Allow |
|  | Restrict web content transfer with other apps | Allow |
|  | Org data notifications | Allow |
| Access requirements | PIN for access | Require |
|  | PIN type | Numeric |
|  | Simple PIN | Block |
|  | Select minimum PIN | 6 |
|  | Touch ID instead of PIN for access (iOS 8+/iPadOS) | Allow |
|  | Face ID instead of PIN for access (iOS 11+/iPadOS) | Allow |
|  | App PIN when device PIN is set | Require |
|  | Recheck the access requirements after (minutes of inactivity) | 30 |
| Conditional Launch | Max PIN attempts | 5, then reset PIN |
|  | Offline grace period | 720 minutes, then block access |
|  | Offline grace period | 90 days, then wipe data |
|  | Jailbroken/rooted devices | Block Access |

## OS Updates

For devices running **iPadOS** or **iOS** that are enrolled using an Apple Enrollment program (DEP in this case) policies can be created and assigned to automatically force software updates. This will makes sure managed devices are kept up to date. Users still can update their devices manually.

**Design decision**: Software updates for iOS and iPadOS are forced on DEP enrolled devices using a software update policy.

The policy is configured with the following settings:

| Category | Item |
| --- | --- |
| Version to install | Latest version |
| Schedule type | Update outside of scheduled time |
| Time Zone | <depends on the users region> |
| Start Day | Monday |
| Start Time | 7 AM |
| End Day | Friday |
| End Time | 5 PM |

For devices running the **Android Enterprise Fully managed**, update behavior can be configured in the device restrictions policy.

**Design decision**: Software updates for Android are configured for Android Enterprise Fully Managed devices using a Device Restriction policy.

The following settings are added in the policy:

| Category | Item |
| --- | --- |
| System update | Maintenance Window |
| Start Time | 7 PM |
| End Time | 7 AM |