Správa mobilních zařízení (MDM) Příklad použití v praxi

20.10.2022

T Business

Ukázkové nastavení politik a restrikcí

Než začnete s centrální správou vašich firemních mobilních zařízení, je třeba se rozhodnout, v jakém režimu budou vaše zařízení nastavena. Nejčastěji se rozhodujeme mezi režimem plné správy nebo režimem BYOD.

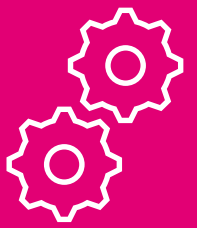
01

V režimu plné správy (Fully Managed, Supervised) organizace může plně ovládat všechny dostupné vlastnosti zařízení. K dispozici je více vlastních nastavení než v jiných režimech. Tento režim má však dvě zásadní vlastnosti:

- Administrátor může ovládat všechny dostupné vlastnosti zařízení a zasahovat do veškerého obsahu na zařízení. To nemusí být vždy vhodné z pohledu ochrany soukromí v případě, že zaměstnanci mohou využívat zařízení i pro soukromé účely.
- Zařízení je možné do tohoto režimu přepnout jen po uvedení do továrního nastavení. Tedy po smazání všech dat. V případě iOS je možné zařízení do tohoto režimu uvést jen pomocí Apple DEP.

02

Režim BYOD umožňuje oddělení firemního a soukromého prostoru. Organizace má možnosti zasahovat a nastavovat pravidla pro firemní prostor a v určitých případech omezeně pro celé zařízení. Tento režim je proto častěji využíván v případě, že zaměstnanci mohou využívat zařízení i pro soukromé účely.



V rámci firemní flotily mobilních zařízení je možné spravovat zařízení v různých režimech.

Příklad použití režimu BYOD

01

Telekomunikační operátor / finanční instituce.

02

Potřebuje efektivně spravovat velké množství telefonů přidělených zaměstnancům a minimalizovat nároky na vytížení IT oddělení. Musí také zajistit, aby firemní data zpracovávaná v zařízeních neunikla, čímž by došlo k porušení zákonných povinností. Na druhé straně ale chce umožnit zaměstnancům využívat telefony i k osobním účelům a musí tedy chránit jejich soukromí.

03

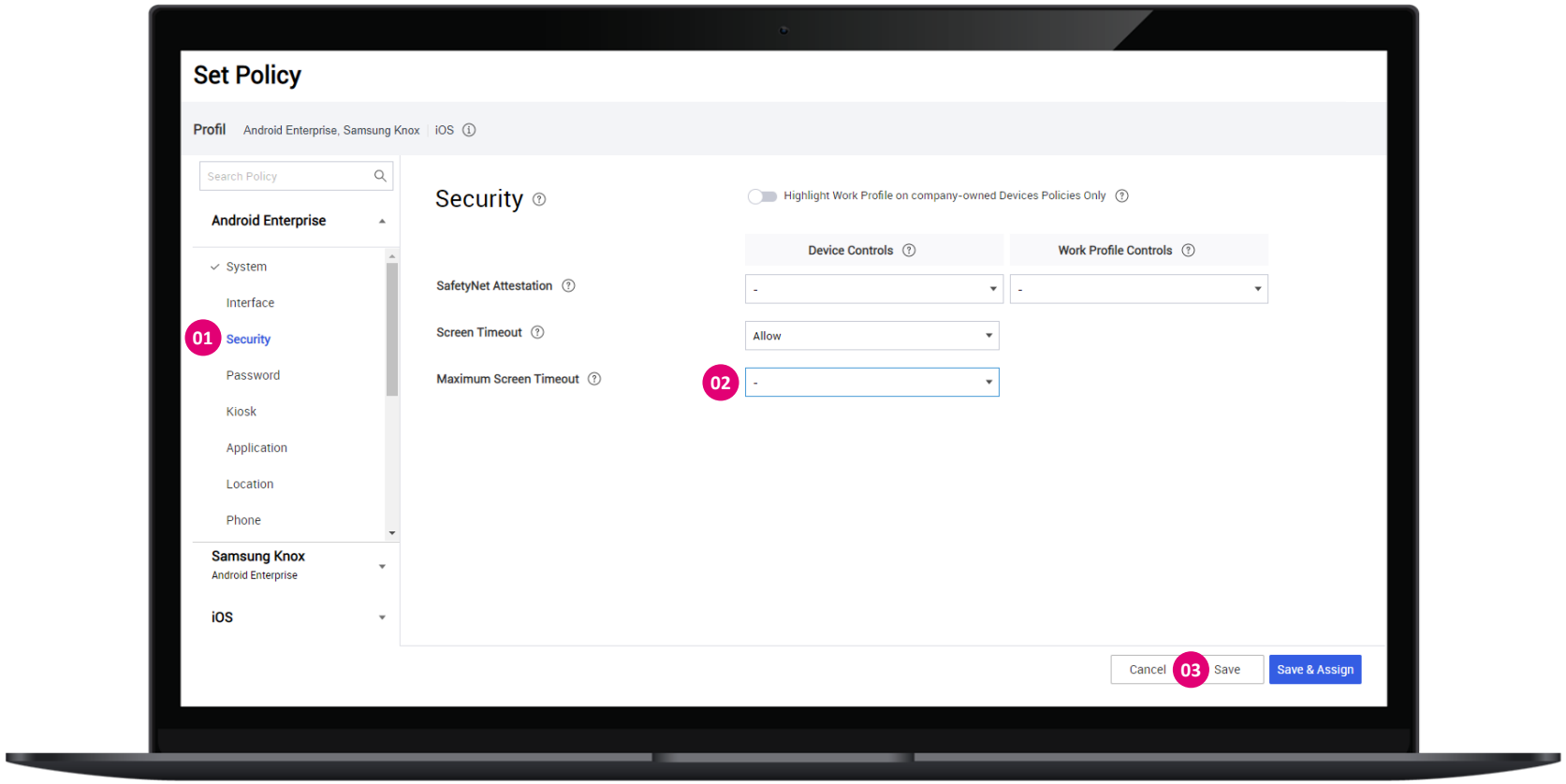
Řešení pro správu mobilních zařízení umožňuje oddělit v telefonu soukromý a firemní prostor. Soukromý prostor využívá zaměstnanec dle svého uvážení. Na firemní prostor jsou však uplatněna podniková bezpečnostní pravidla včetně ochrany přístupu heslem či zákazu kopírování dat. V tomto prostoru se také automaticky nainstalují veškeré aplikace, které pro svou práci zaměstnanec potřebuje. IT oddělení definuje pravidla pro nastavení telefonů, která se pak automaticky aplikují na celé určené skupiny zařízení. Zatížení správce je tak minimalizováno. V případě potřeby může správce zaměstnanci poskytnout vzdálenou pomoc nebo při ztrátě zařízení vzdáleně smazat firemní data.

Nastavení uzamčení obrazovky

01 V nastavení politik profilu přejděte na položku Security.

02 U Screen Timeout nastavte hodnotu na Allow.

03 Nastavení uložte tlačítkem Save.



Nastavení kódu pro zamčení obrazovky

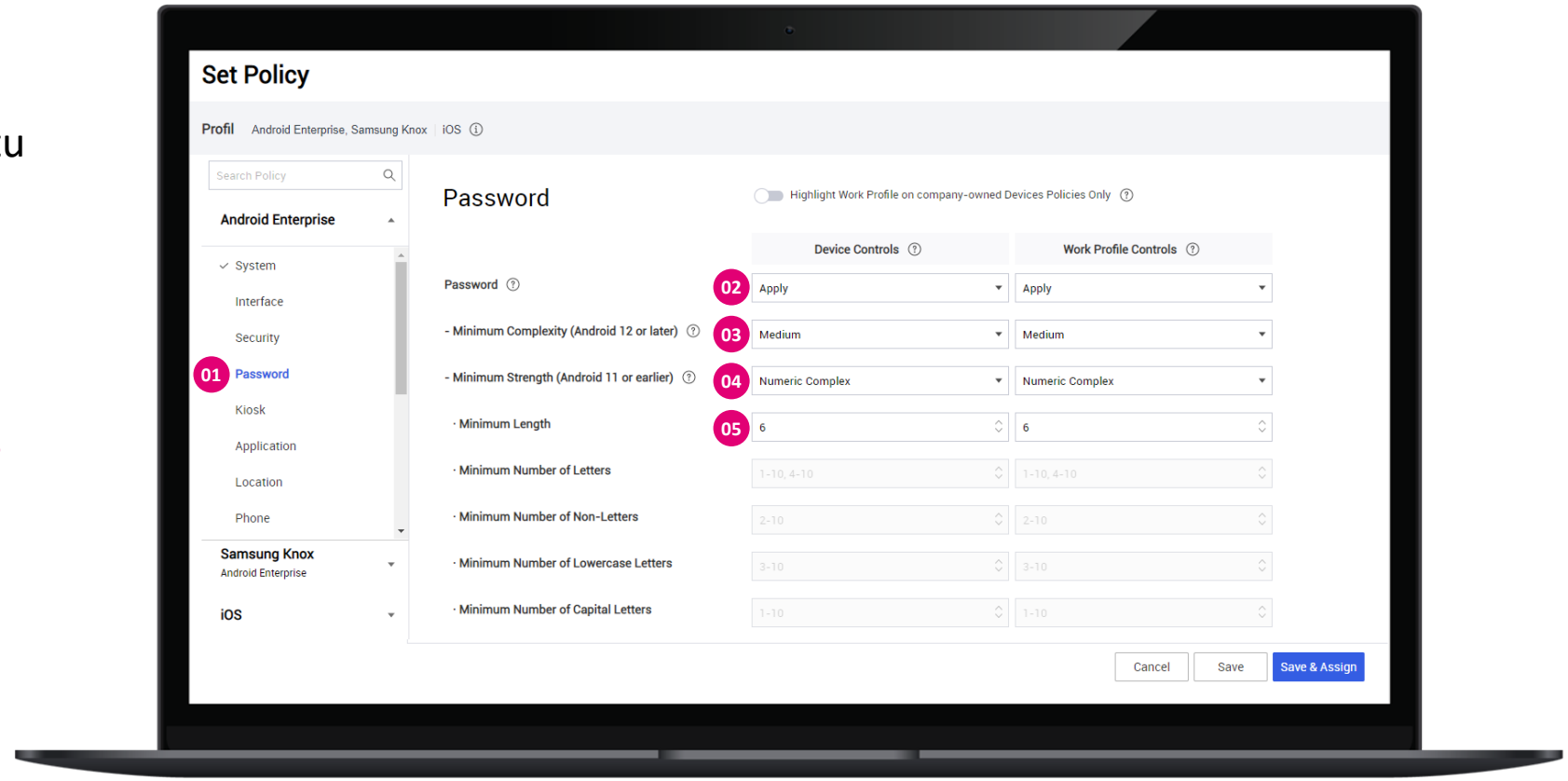
01 Následně přejděte na položku Password.

02 V obou sloupcích nastavte hodnotu na Apply.

03 Minimum Complexity (Android 12 or later) nastavte na Medium.

04 Minimum Strength (Android 11 or earlier) nastavte na Numeric Complex.

05 Minimum Length nastavte minimálně na 6 znaků.



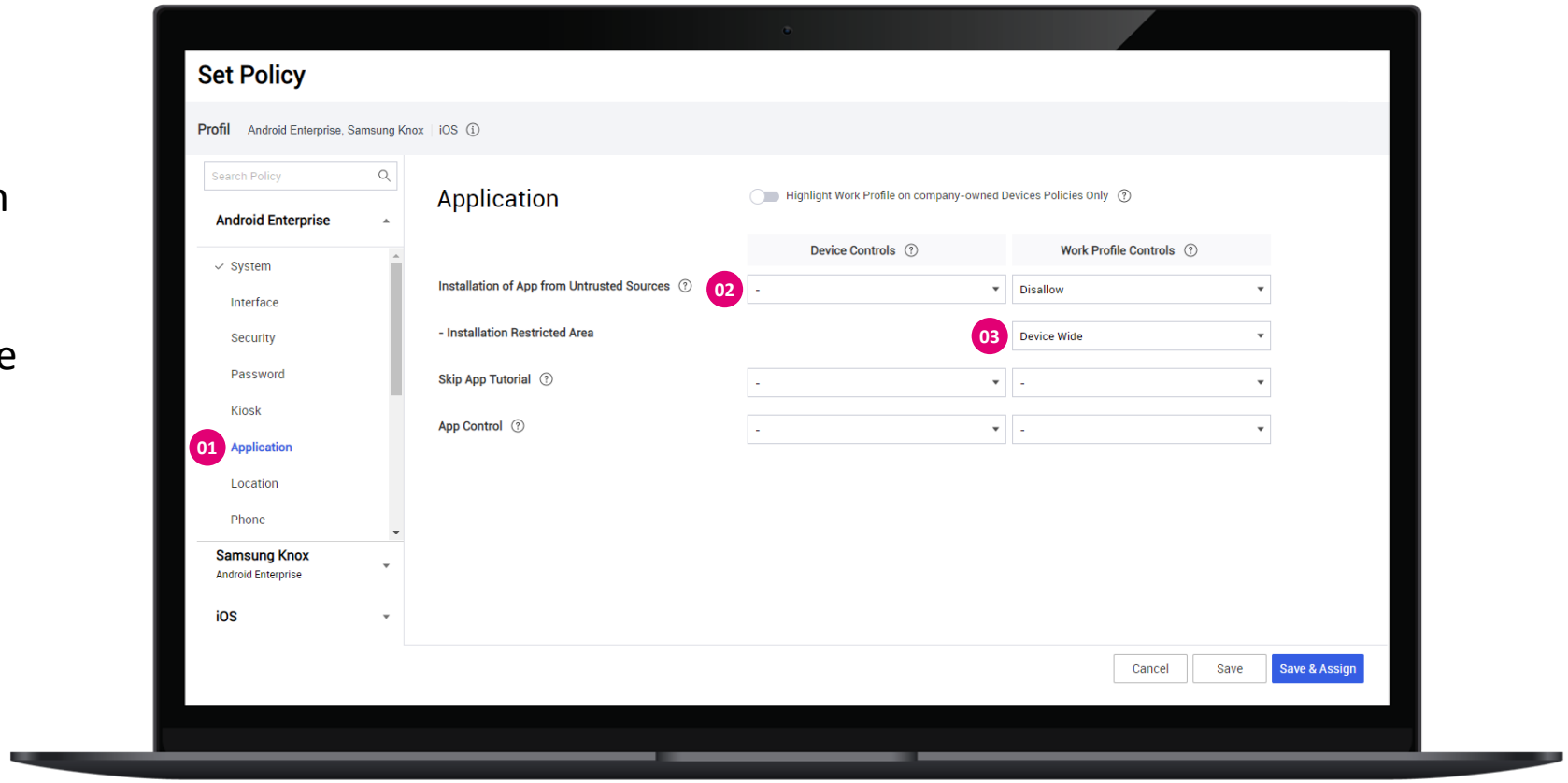
T Business

Zamezení instalace aplikací z neoficiálních zdrojů

01 Další krok se nachází pod položkou Application.

02 U Installation of App from Untrusted Sources zvolte v pravém sloupci Disallow.

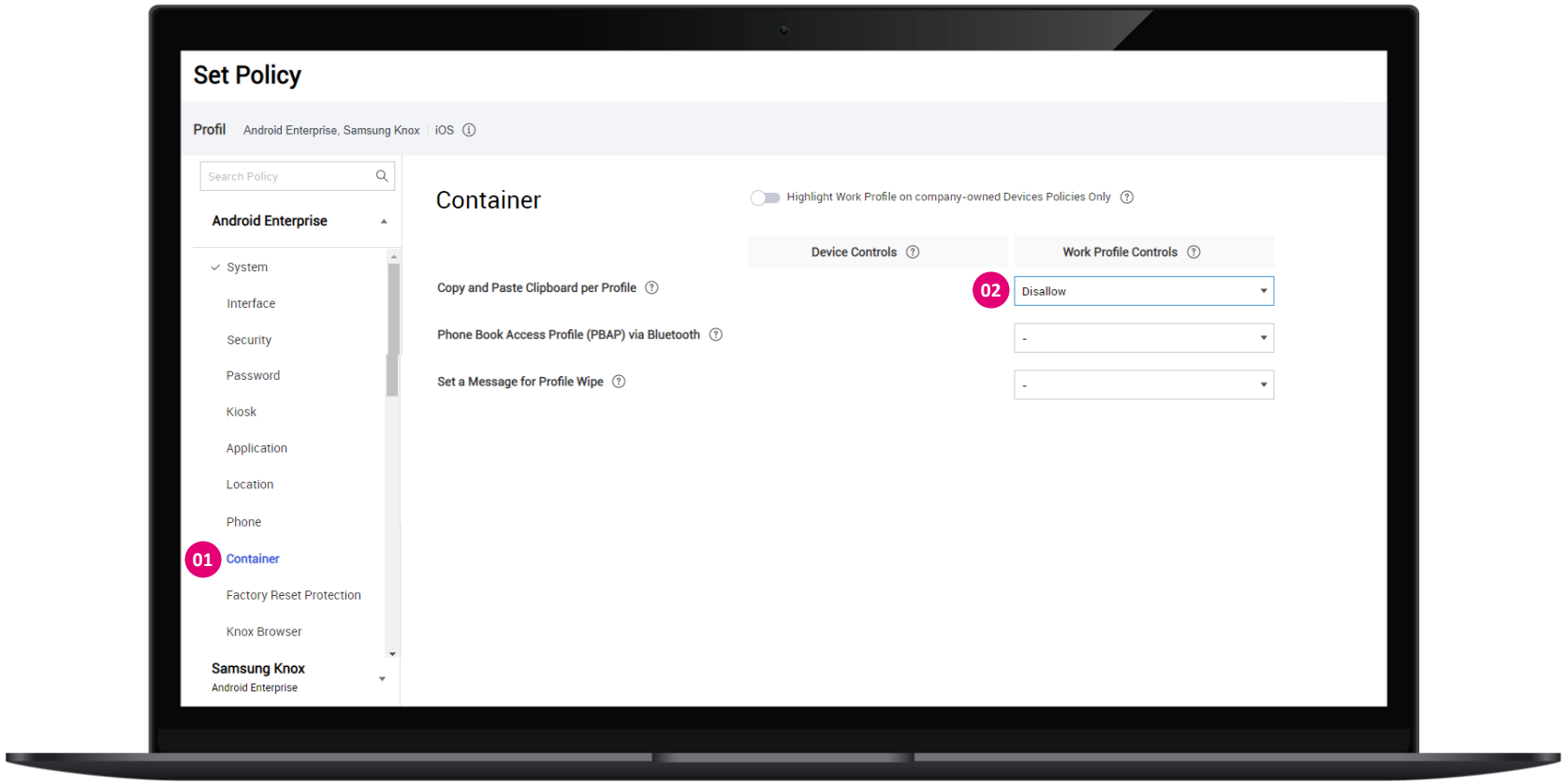
03 Installation Restricted Area vyberte hodnotu Device Wide.



Zakázání kopírování dat mezi profily

01 Jako poslední klikneme na položku Container.

02 U Copy and Paste Clipboard per Profile zvolíme Disallow.



Nastavení kódu pro zamčení obrazovky

01 V levém sloupci rozklikněte položku iOS.

02 Následně klikněte na položku Security.

03 Passcode Policies přepněte na Apply.

04 Passcode Strength vyberte Numeric.

05 Minimum Length nastavte nastavte alespoň na 6 znaků.