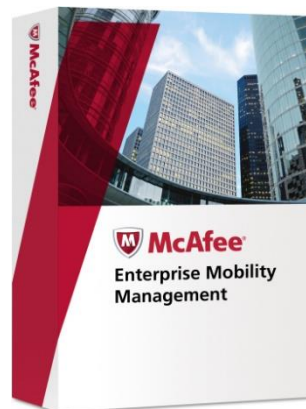


# McAfee® EMM 11.0



Jan Pergler  
Pre-Sales Engineer  
[j.pergler@pcs.cz](mailto:j.pergler@pcs.cz)  
[www.dataguard.cz](http://www.dataguard.cz) |  
[www.pcs.cz](http://www.pcs.cz)

## Bezpečná jednotná správa všech koncových zařízení

- Stejně zabezpečení a vynucení pravidel
- Využití současného nastavení politik
- Stejní uživatelé, aplikace a data



## Ochrana mobilních zařízení

- Správa zařízení (MDM)
- Anti-malware
- Blokování Jailbroken a Rooted zařízení
- Vynucení minimální verze iOS



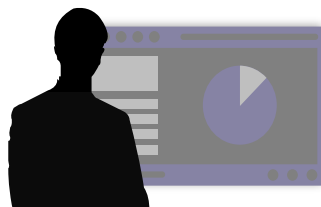
## Ochrana dat v mobilu

- Správa firemních dat, nezávislost na vlastníkovvi zařízení
- Vynucování šifrování zařízení
- Zamknutí, wipe, resetování do továrního nastavení
- McAfee aplikace: Secure Container, McAfee Web Gateway



## Ochrana aplikací

- McAfee App Alert™
- Firemní úložiště aplikací
- Reputace instalovaných aplikací s GTI



ePO

## McAfee App Alert zabezpečuje a chrání data pomocí přehledných oprávnění aplikací na platformě Android

- Skenování všech aplikací v zařízení
- Hodnocení aplikací dle požadovaných oprávnění
- Ověřování URL odkazů v  
Global Threats Inteligence (GTI)
- Přehledné zobrazení oprávnění  
jednotlivých aplikací
- Reporty do ePO

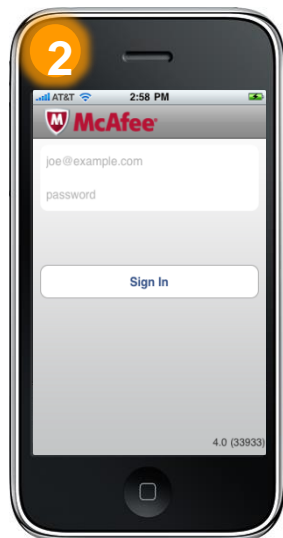




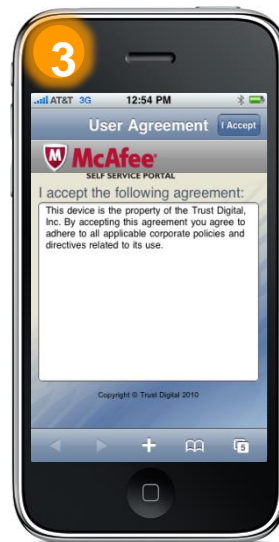
# Instalace EMM klienta iOS, Android



**Spustit aplikaci  
z App Store,  
Google Play**



**Vložit  
emailové  
autentizační  
údaje**



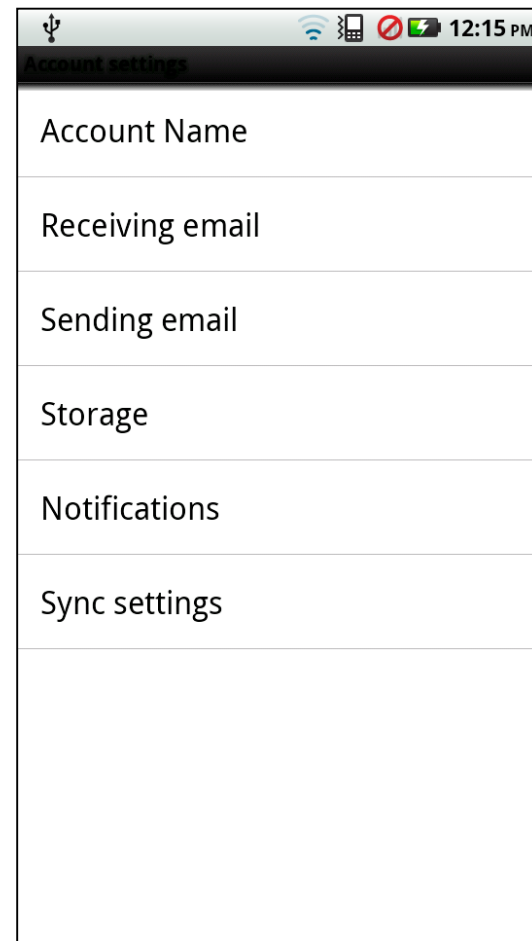
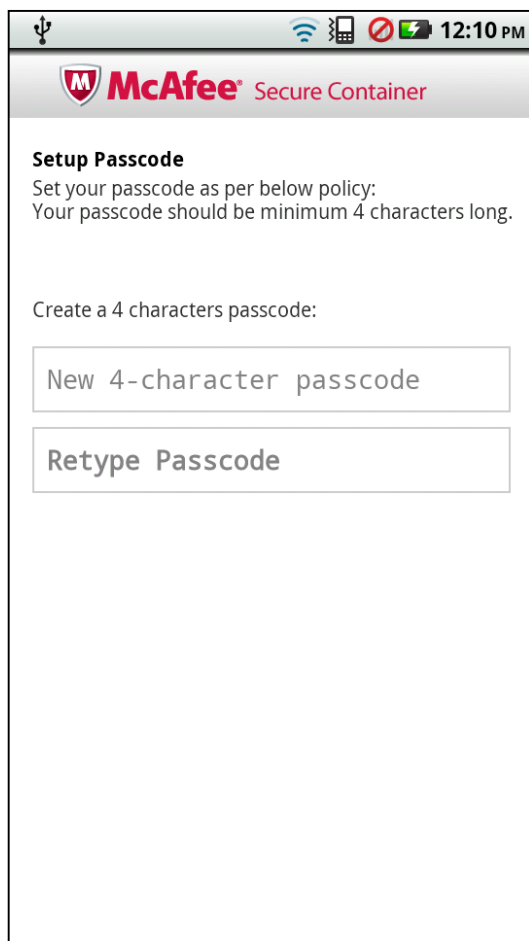
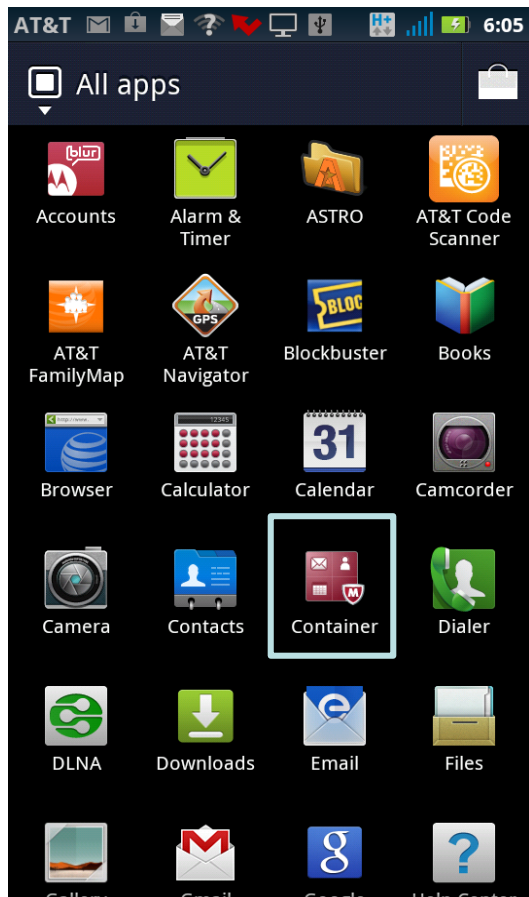
**Odsouhlasit  
politiku**



**IT služba je  
automaticky  
nainstalována  
a spuštěna**

## Snadná, bezpečná, automatická





- Secure Container pro všechny mobilní platformy
- Šifrovací standard FIPS 140-2
- S/MIME šifrovaný email
- Editor dokumentů / Správce souborů
- Zabezpečený webový prohlížeč
- Management aplikací



- Plná integrace EMM do ePO
  - EMM Proxy zůstane komunikačním prostředníkem, který oddělí vnitřní a vnější komunikaci
- Jednotná konzole pro koncová zařízení
- ePO reporty, upozornění a automatizace
- Tagování jednotlivých zařízení
- Zvýšení kvality a výkonu celého řešení





- Jednotné sledování koncových zařízení a výkonná automatizace v ePO dramaticky zvyšuje bezpečnost zařízení
  - Přehledné sledování povolených a zakázaných aplikací
- Jednotnost snižuje nároky na administraci a tím i náklady na správu



Server: EMM-DMZ-DHUB | Time: 1/11/13 6:52:01 AM PST | User: admin | Log\_Off

Menu System Tree Dashboards System Tree Queries & Reports Policy Catalog Extensions Server Tasks Registered Servers

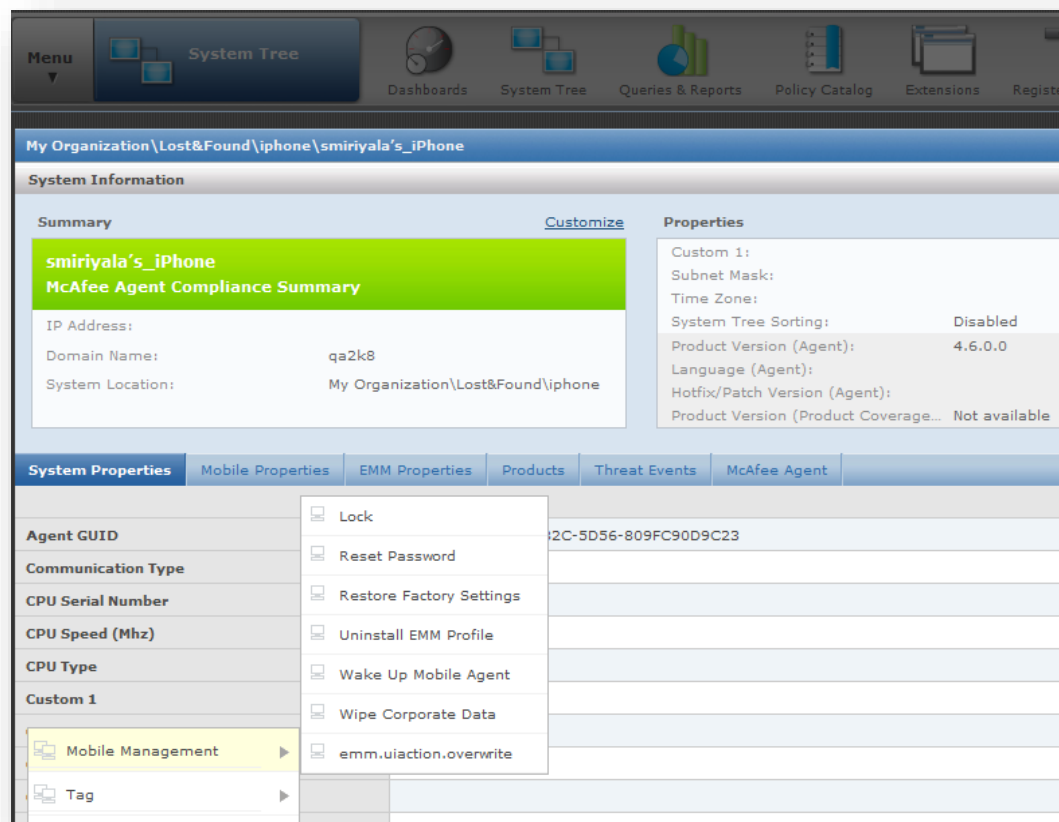
System Tree My Organization Lost&Found QA2K8 Test

Systems Assigned Policies Assigned Client Tasks Group Details

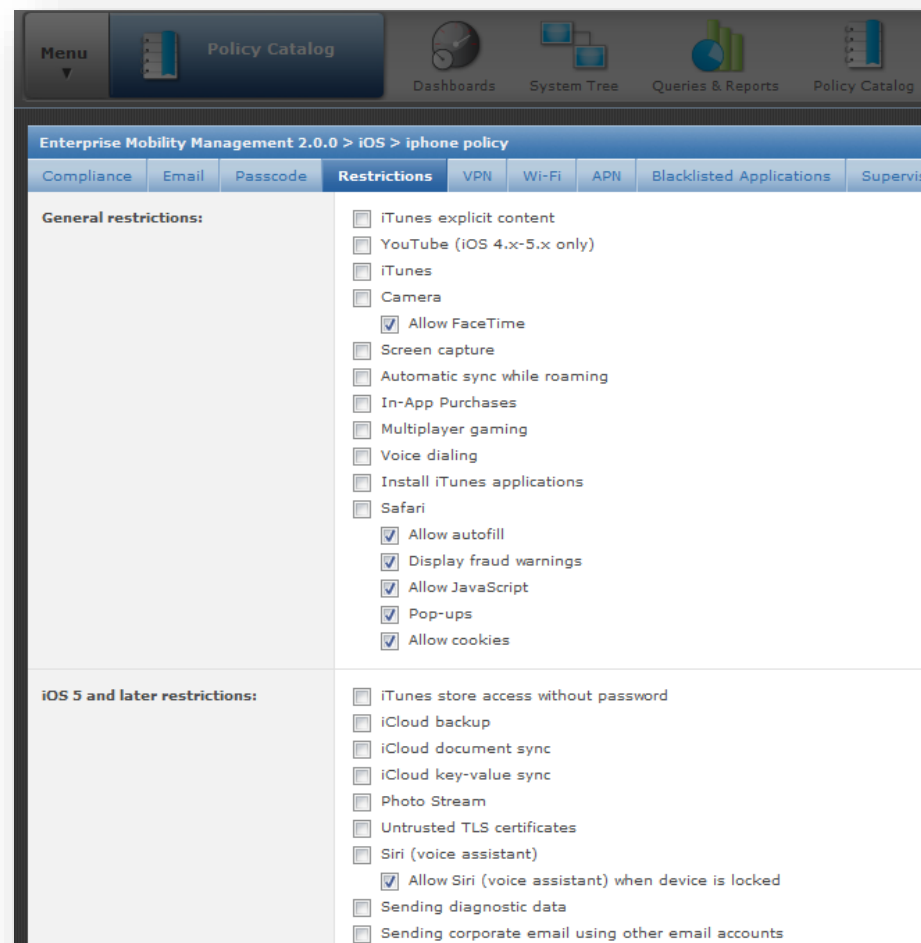
Preset: This Group Only Custom: None Quick find: Apply Clear Show selected rows

	System Name ▲	Managed State	Compliant	Tags	IP Address	User Name	Last Communication	Model	Model Version
	androidc145481145	Managed				gc07	1/10/13 10:30:00	HTC One X+	HTC One X+
	androidc213337785	Managed				gc07	1/4/13 1:22:26 PM	HTC VLE_U	HTC VLE_U
	Appl88923YCU3NQ	Managed				dgarg1	1/3/13 1:55:34 PM	iPhone2,1	MC136LL
	WP000000011	Managed				tj10	1/3/13 3:22:01 PM		

- Ovládání ze System Tree
  - Uzamknutí zařízení
  - Reset hesla
  - Reset do továrního nastavení
  - Odinstalace EMM agenta
  - Vynucení komunikace agenta
  - Smazání firemních dat
  
- Upozornění
  - Upozornění na viry, soulad s politikou, nová zařízení, ...



- Účinné a snadné vytvoření politik v ePO katalogu politik a jejich snadné aplikování na uživatele nebo na zařízení v závislosti na stanovených podmínkách (typ zařízení, VIP uživatel).
- Sestavení politik
  - V celém System Tree
  - Na základě mobilního OS (iOS, Android, Windows Phone)
  - Na skupinu
  - Na uživatele
  - Na specifické zařízení



## Sestavení politik dle nebezpečnosti OS: Oddělení politik na základě OS mobilního zařízení

- Příklad:
  - iOS 5 Policy – Ponechání nativního šifrování emailu, vynucení delšího hesla k odemknutí, blokování zálohy do iTunes, blokování přesunu firemních emailů do soukromé schránky.
  - Android 4.0 a novější – Zakázání nativního email klienta, vynucení šifrování celého zařízení a delšího hesla k odemknutí
  - Android 3.x a starší – Vynucení používání Secure Containeru a komplexního hesla k jeho odemčení

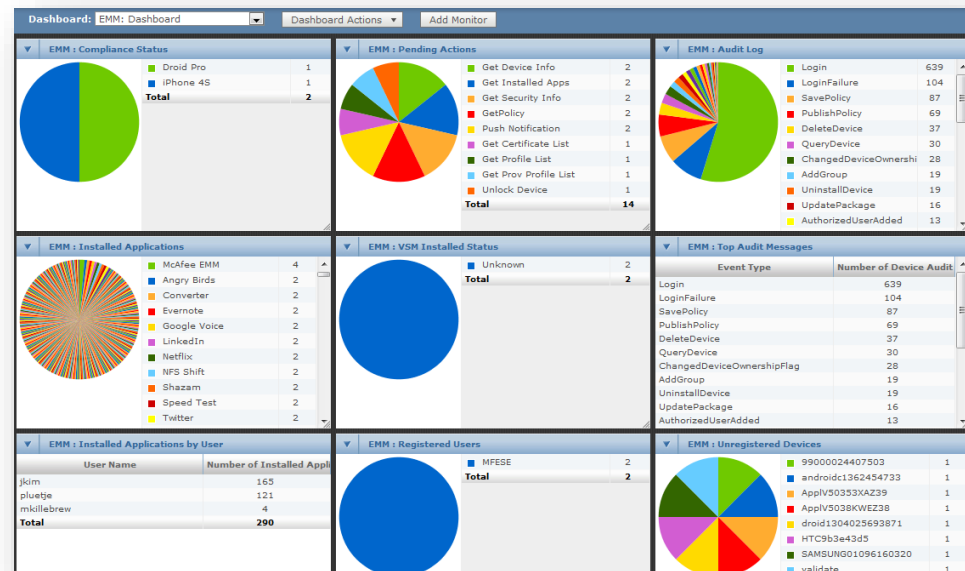




Jednoduché rozdělení politik dle vlastníka zařízení: Oddělení politik pro firemní a vlastní zařízení dovoluje nastavit dostatečně bezpečné prostředí pro firemní data a snížení nákladů na mobilní zařízení které je vlastnictvím uživatele (BYOD)

- Příklad:
  - Firemní zařízení: Pokud je v zařízení proveden Root/Jailbreak , automaticky je zařízení otagováno a následně přesunuto do karantény, administrátor je upozorněn emailem, že zařízení v stavu Root/Jailbreak a je resetováno do továrního nastavení
  - Zařízení uživatele: Pokud je v zařízení proveden Root/Jailbreak , automaticky je zařízení otagováno a následně přesunuto do karantény, administrátor rozhodne (nebo automaticky) o smazání **pouze firemních dat**

- **Dashboardy**
  - Rychlý přehled připojených zařízení a jejich stavu
  - Zařízení, operátor, hrozby, IMEI, aplikace, status, OS, tel.číslo
- **Reporty**
  - Vestavěné reporty, které pokrývají běžné požadavky administrátorů
  - možnost tvorby vlastních
- **Akce**
  - Přímý proklik na ohrožená zařízení
  - rychlý přehled a možnost upozornění uživatele, případně smazání zařízení



## System Device Tree

Mobilní zařízení jsou nyní v ePO System Tree a je možné snadné využívat seskupování výjimek s jednotnou politikou

Řazení / Filtrování

## Ovládání zařízení

Kontrola zařízení přímo ze System Tree (Wipe, Uninstall, Lock, SMS, Wakeup, Override, ..)

Zamezení komunikace zařízení, které nesplňuje požadavky na zabezpečení.

## ePO správa politik

Snadné a přehledné nastavení politik pro Android, iOS, Windows Phone v ePO známé z ostatních McAfee produktů

Flexibilní nastavení politik v ePO

## Akce / Reakce

Přednastavené query na očekávané prohřešky uživatelů

Upozorňování na jailbreak/root, nepovolené aplikace

ePO automatické úkoly v případě detekce ohrožení dat

## Přehledy

Zařízení

Bezpečnost (detekce virů)

Aktivity uživatele

Aplikace

## Ostatní

Přechod na ePO licencing

Vylepšené portálové certifikáty SSL

# Schéma EMM 9.x a 10.x

