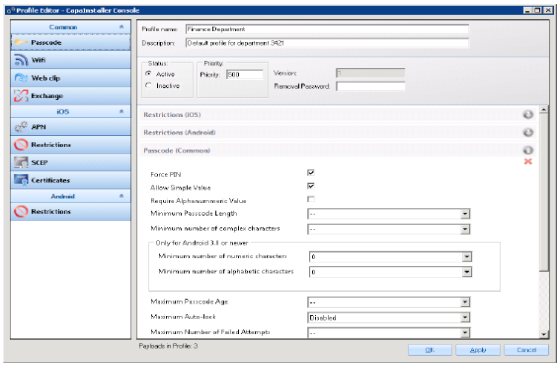
CapaInstaller

Mobile Device Management

Mobile Device Management is seamlessly integrated in CapaInstaller and offers centralized configuration and monitoring of Apple iOS, Apple macOS and Android based devices. The solution enables the IT Department to take control of users' mobile devices using the same management console as used for Windows computers.



ENROLLMENT

End-users or IT staff enroll devices Over-the-air (OTA) using different authentication methods, including Active Directory. They are also able to create simple-to-use enrollment configurations that simplify this process across the mobile device platforms. The system offers customized Terms of Use and require acceptance during enrollment to prevent any legal issues afterwards.

SECURITY MANAGEMENT

To raise the security level of the devices, it is possible to require a passcode with configurable complexity, length, age and other parameters. In case of misplaced or stolen devices, IT staff are able to lock a device with current passcode to protect access to the device or perform a complete wipe (factory reset) of the device to delete user data.
IT staff can lock down an end-user's ability to use specific features such as camera usage to e.g. allow physical access to restricted areas with the device.

CONFIGURATION MANAGEMENT

To manage the devices profiles containing configurations, restrictions or apps can be applied. These profiles are assigned to individual devices or groups of devices to target specific requirements. Deployment of apps using profiles allows remote install and uninstall of enterprise, Apple App Store and Google Play apps. The most commonly used settings are configuration of WiFi access points and Microsoft Exchange configuration. In addition, distribution of certificates for use with applications and publishing URL shortcuts (webclips) to home screen of the devices are available.

ASSET MANAGEMENT

On request, the devices scan and upload hardware and software inventory details including manufacturer, model, UDID, serial number, IMEI, host name and a full commercial descriptive name e.g. "iPhone XR 64GB". Hardware information lists Wi-Fi MAC address, Bluetooth MAC, IP addresses, subscriber carrier, current carrier, roaming status, SIM serial number, phone number, current battery level and device storage capacity as well as used capacity. The software inventory contains information about operating system, version, build and installed applications and their version.

REAL-TIME REPORTS

Query & Reporting makes it possible to create reports based on any type of data, or to use some of the predefined reports. By choosing precisely which data to include, using both static and/or dynamic criteria, each report can be extremely concise and focused. CapaInstaller integrates with Microsoft SQL Server Reporting Services, which makes it possible to view the reports in a browser without even having CapaInstaller installed.

DEVICE MANAGEMENT

It is possible to set the frequency intervals at which the system collects device information. Perform bulk management of groups containing Windows, Apple macOS computers and iOS as well as Android devices to simplify administration of these. Retire the devices by un-enrolling them from the management system.

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup
(+45) 70 10 70 55
sales@capasystems.com

CapaInstaller

Mobile Device Management

Feature Overview

- **Self Service Portal**
  Enterprise App Store for users. Let users manage their own devices
- **Passcode**
  Require a device passcode with configurable complexity, length, age, history
- **Encryption**
  Enforce full device encryption according to industry standards
- **Lock/Wipe Device**
  Lock device to protect a lost device, complete wipe (factory reset) of stolen device
- **Restrictions**
  Lock down the ability to use specific device features, apps and web browsing
- **App Deployment**
  Remote install and uninstall of enterprise, Apple App Store and Google Play apps.
- **Certificates**
  Integrate with certificates for secure applications usage
- **Network**
  Configure access to Wi-Fi networks
- **Microsoft Exchange Support**
  Set up access to corporate Microsoft Exchange mailbox using one configuration for all users
- **Shortcuts**
  Publish URL shortcuts (webclips) to home screen
- **Device identification**
  Manufacturer, model, UDID, serial number, IMEI, host name
- **Device signature**
  Full commercial descriptive name e.g. “iPhone XR 64GB”
- **Device platform**
  Operating system, version, build
- **Network Information**
  Wi-Fi MAC address, Bluetooth MAC, IP addresses
- **Certificate**
  Use device and user certificates for WiFi and exchange using your existing on-premises infrastructure
- **Carrier Information**
  Subscriber/current carrier, roaming status, SIM serial number, phone number
- **Device Storage**
  Primary capacity and space available
- **Installed Applications**
  List installed applications and their version
- **Reporting**
  Generate reports with automated distribution without console access
- **Queries**
  Determine the frequency intervals at which the console captures device information
- **Commands**
  Send commands on-demand to devices to request info, lock or wipe a device
- **Bulk Management**
  Perform cross platform actions to groups of devices
- **Over-the-air (OTA) enrollment**
  Enroll device without the need to install agent
- **Whitelist**
  Enhance security by whitelisting application as safe to use
- **Blacklist**
  Prevent selected application from being used
- **Lock Single App**
  Lock a device so it can only run one app. This is also known as kiosk mode
- **Apple Volume Purchase Program**
  Automatically assign and withdraw licenses to IOS devices or Apple ID
- **Apple Device Enrollment Program**
  Provides a fast, streamlined way to deploy your corporate-owned iOS devices, whether purchased directly from Apple or through participation Apple Authorized Resellers
- **Samsung Knox Enrollment**
  Knox Mobile Enrollment makes deploying thousands of devices quick and easy
- **Chromebooks**
  With Chromebook inventory, you can collect information about all your devices and the software versions they are using. Useful for having a full overview of all your devices and enough information to make sure there is no security breach in your environment because of missing updates to the operating system or software.