Support MDMs (Mobile Device Managers) and device passwords

There may come a time in a testers experience when the powers that be (for example upper management or security) require cloud devices to need an MDM, or a password/passcode/pin. An MDM is a Mobile Device Manager. Device Management (MDM) and Device Locking explains a little more about MDM use, and how Perfecto can support passwords/passcodes/PIN.

If an MDM is absolutely required, Perfecto devices can work with an MDM. The MDM configurations would be done by whoever is supporting the MDM policies on the customer side.

Following are a few caveats to consider when working with an MDM:

- **Android devices using an MDM.** The MDM must not disable or restrict the following services:
  - Do Not disable ADB Debugging
  - Do Not disable the function to allow installation of unknown applications - (this is an android security setting)
  - Do Not disable data transfer over USB
  - Do Not disable video transfer over USB

- **iOS devices using an MDM.** The MDM must not disable or restrict the following services:
  - Any of the Perfecto iOS clients on the device
  - Do Not require a passcode lock less than 15 minutes,
  - Do Not disable data transfer over USB
  - Do Not disable video transfer over USB
  - Do Not disable installation of applications to the device

- **General Configuration.** The MDM must not force the following:
  - Immediate passcode lock - If required, set to no less than 15 minutes

As long as the MDM follows these requirements on the devices, using an MDM should not be a problem. Note that passwords/passcodes/pin use also falls under the same regulations.

Important

Perfecto is not responsible for installing, configuring or maintenance of any customer MDM or customer installed certificate(s).