

Android Randomized MAC Address - Capture for Aruba ClearPass

Proposed workaround:

1. In Certificate Authority - build a certificate template for Intune users (named IntuneUser)
2. In Intune - create a PKCS certificate configuration profile using the **User** certificate template, but then used certificate type **Device**

Basics [Edit](#)

Name	██████████ PKCS_CN_MACaddress
Description	User certificate for android phones that use MAC randomization and connect to ClearPass
Platform	Android Enterprise
Profile type	PKCS certificate

Configuration settings [Edit](#)

Renewal threshold (%)	20
Certificate validity period	1 Years
Certification authority	████████████████████
Certification authority name	████████████████
Certificate template name	IntuneUser
Certification authority type	microsoft
Certificate type	Device
Subject alternative name	Attribute
	DNS
	Email address
	User principal name (UPN)
Subject name format	CN={{WiFiMacAddress}}

3. In Intune - created a WIFI configuration profile type using the PKCS for the certificate

Wifi Test | Properties ...
Device configuration profile

Search (Ctrl+ /) <<

Overview

Manage

- Properties

Monitor

- Device status
- User status
- Per-setting status

Basics [Edit](#)

Name: Wifi Test

Description: [Redacted]

Platform: Android Enterprise

Profile type: Wi-Fi

Configuration settings [Edit](#)

SSID: MOBILE-test

Hidden network: Enable

EAP type: EAP - TLS

Root certificate for server validation: Root Cert

Authentication method: Certificates

Certificates: PKCS CN_MACAddress

Scope tags [Edit](#)

Default

Assignments [Edit](#)