AIRHEADS 2013

Enabling BYOD Workshop

Aruba Network Services Team

March 2013

#airheadsconf

Agenda

AIRHEADS 2013

- Deploying ClearPass Onboard
    - BYOD Policy
- Technology Overview
    - Profiling BYO Devices
    - Integrating ClearPass with MDM
    - Onboard Provisioning
- Troubleshooting
- Q&A

Onboarding with ClearPass

Deploying ClearPass Onboard

- **Planning**
  - BYOD Policy
- **Configuring**
  - CA settings
  - Network Settings
  - Provisioning Settings
  - Advanced Settings
- **Lifecycle Management**
  - User experience
  - Lost, expired, revoked devices
  - Troubleshooting

BYOD Policy

Building a BYOD Policy (Gartner)

- Device diversity
- Policy enforcement
- Security and compliance
- Containerization
- Inventory management
- Software distribution
- Administration and reporting
- IT service management
- Network service management

Technology Overview

Technology Overview

- **Detecting new BYO Devices**
  - Lack of Provisioned Credential
  - Device Profiling
  - MDM Integration
- **User Managed Provisioning Workflow**
  - Setup PKI for device credentials
  - Provisioning Settings
  - Network Settings
  - Advanced Settings
  - Troubleshooting

BYOD Workflow

1 Onboard Device

- Supplicant Config
- Push Trusted Cert
- Enable Posture
- Set Auth type

2 Join BYOD Domain

- Enrolment workflow
- Authorize User to provision device
- Device credential push
- Link User to Device

3 Device Access Controls

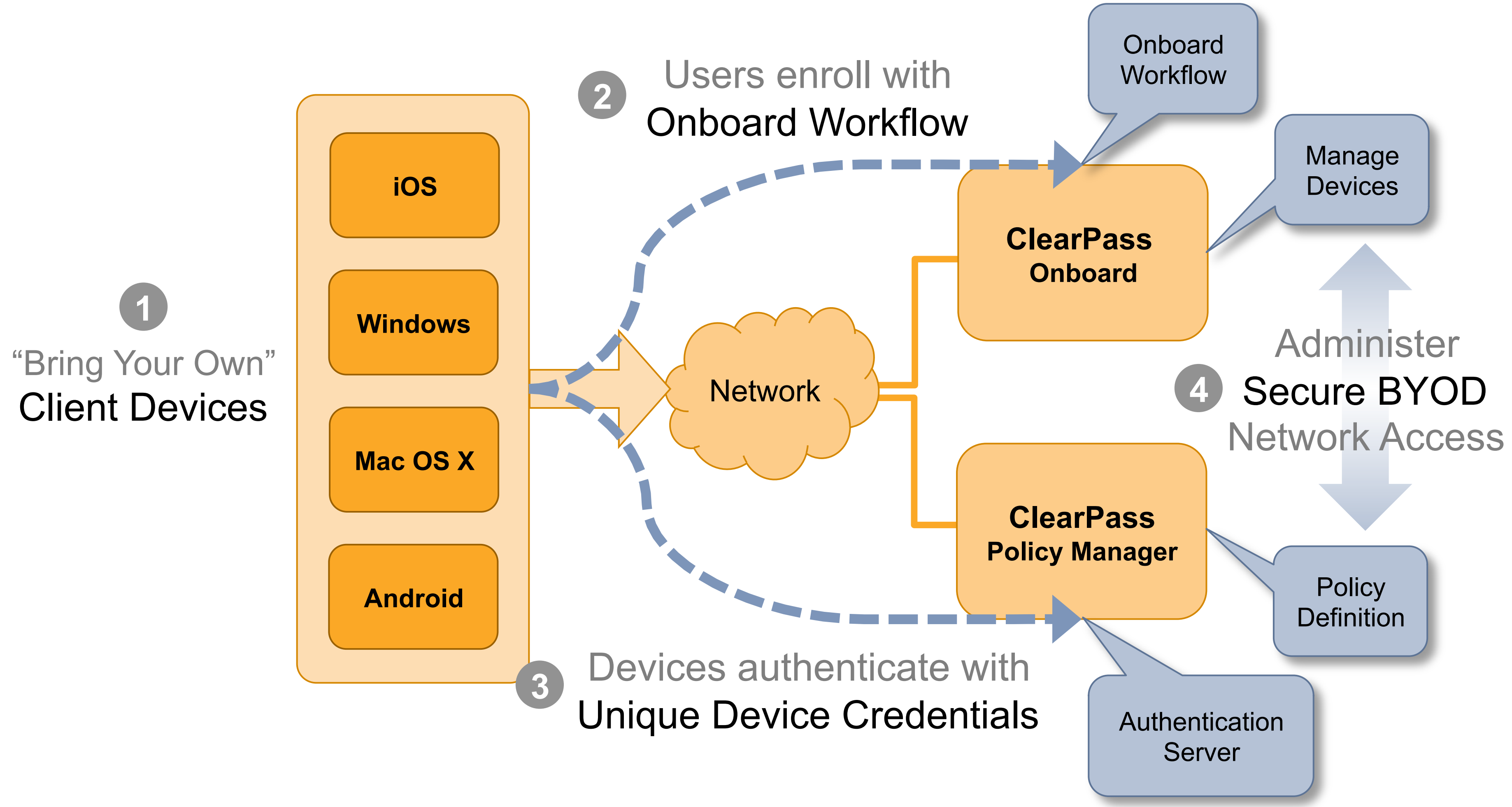
- Revoke Device Access
- Device Profiling
- Role Derivation
- Corp vs Employee Liable

4 Visibility & Reporting

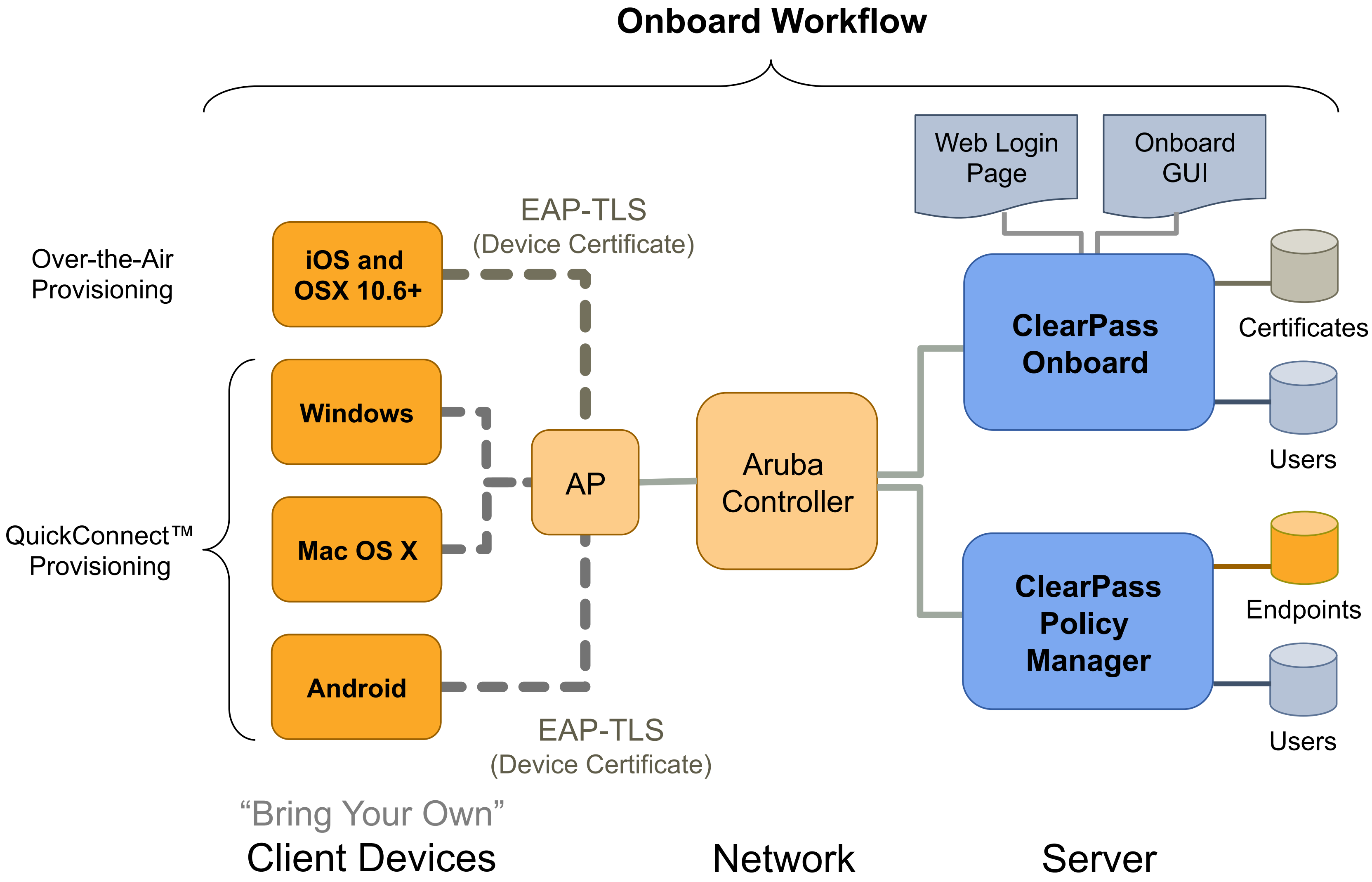
- Complete view device & network
- Command & Control
- Inventory
- Diagnostics

Deployment Architecture

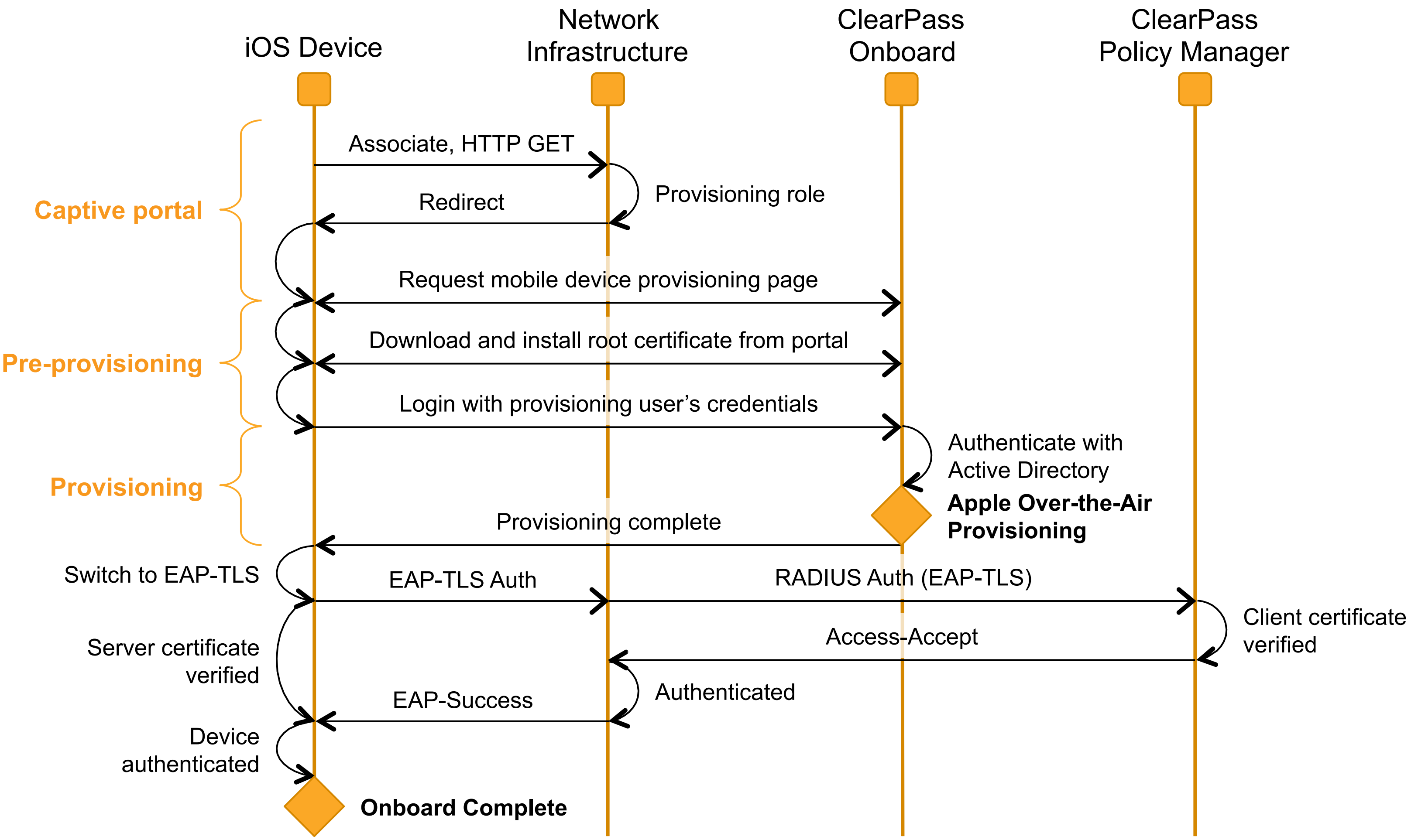
AIRHEADS 2013



Detailed Architecture



Onboard Workflow – iOS & OS X



iOS Device

Network Infrastructure

ClearPass Onboard

ClearPass Policy Manager

Captive portal

Associate, HTTP GET

Provisioning role

Redirect

Pre-provisioning

Request mobile device provisioning page

Download and install root certificate from portal

Login with provisioning user's credentials

Provisioning

Authenticate with Active Directory

Apple Over-the-Air Provisioning

Provisioning complete

Switch to EAP-TLS

EAP-TLS Auth

RADIUS Auth (EAP-TLS)

Client certificate verified

Access-Accept

Server certificate verified

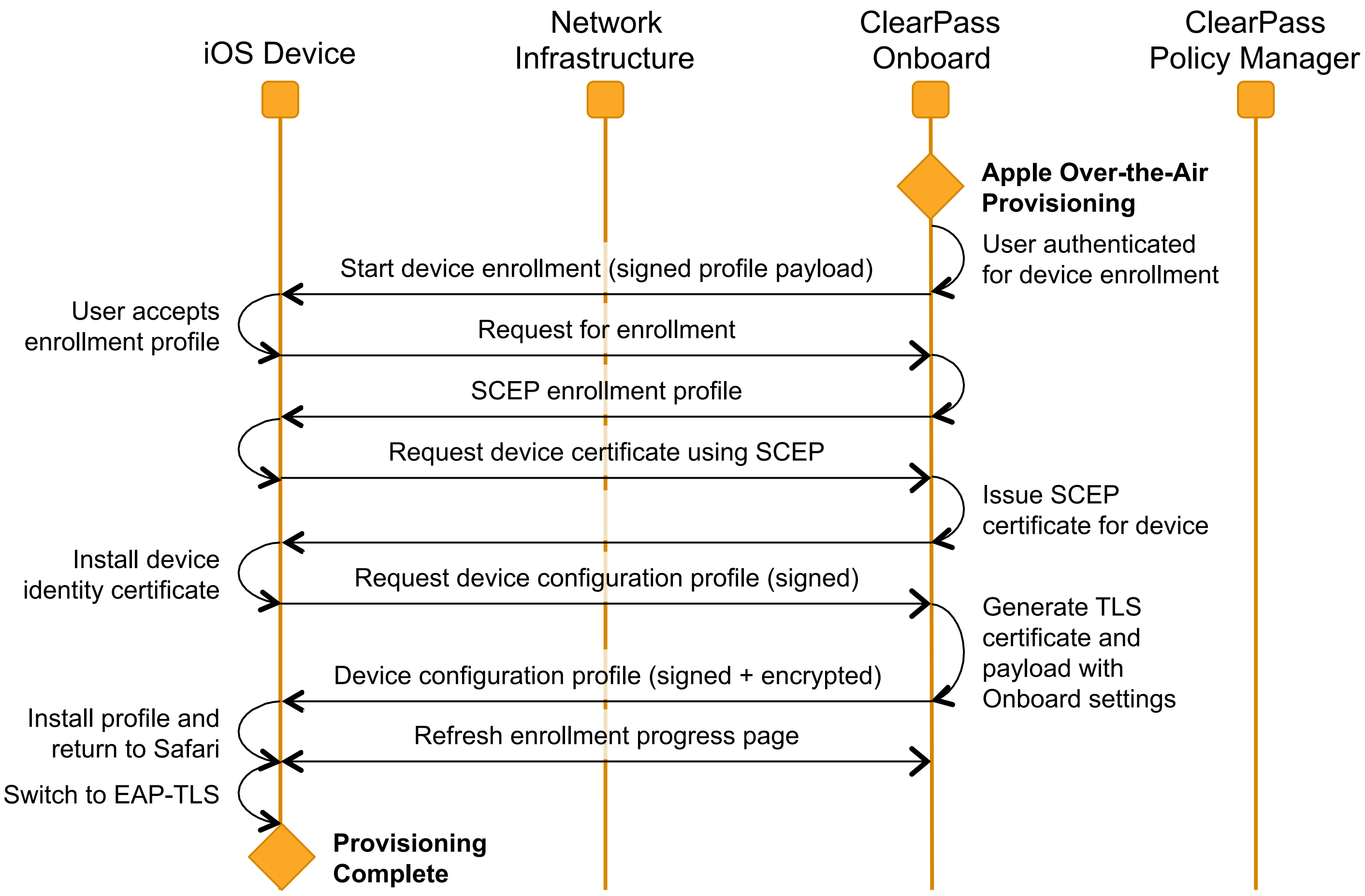
Authenticated

EAP-Success

Device authenticated

Onboard Complete

iOS “Over-the-Air Provisioning”



iOS Device

Network Infrastructure

ClearPass Onboard

ClearPass Policy Manager

Apple Over-the-Air Provisioning

User authenticated for device enrollment

Start device enrollment (signed profile payload)

User accepts enrollment profile

Request for enrollment

SCEP enrollment profile

Request device certificate using SCEP

Issue SCEP certificate for device

Install device identity certificate

Request device configuration profile (signed)

Generate TLS certificate and payload with Onboard settings

Device configuration profile (signed + encrypted)

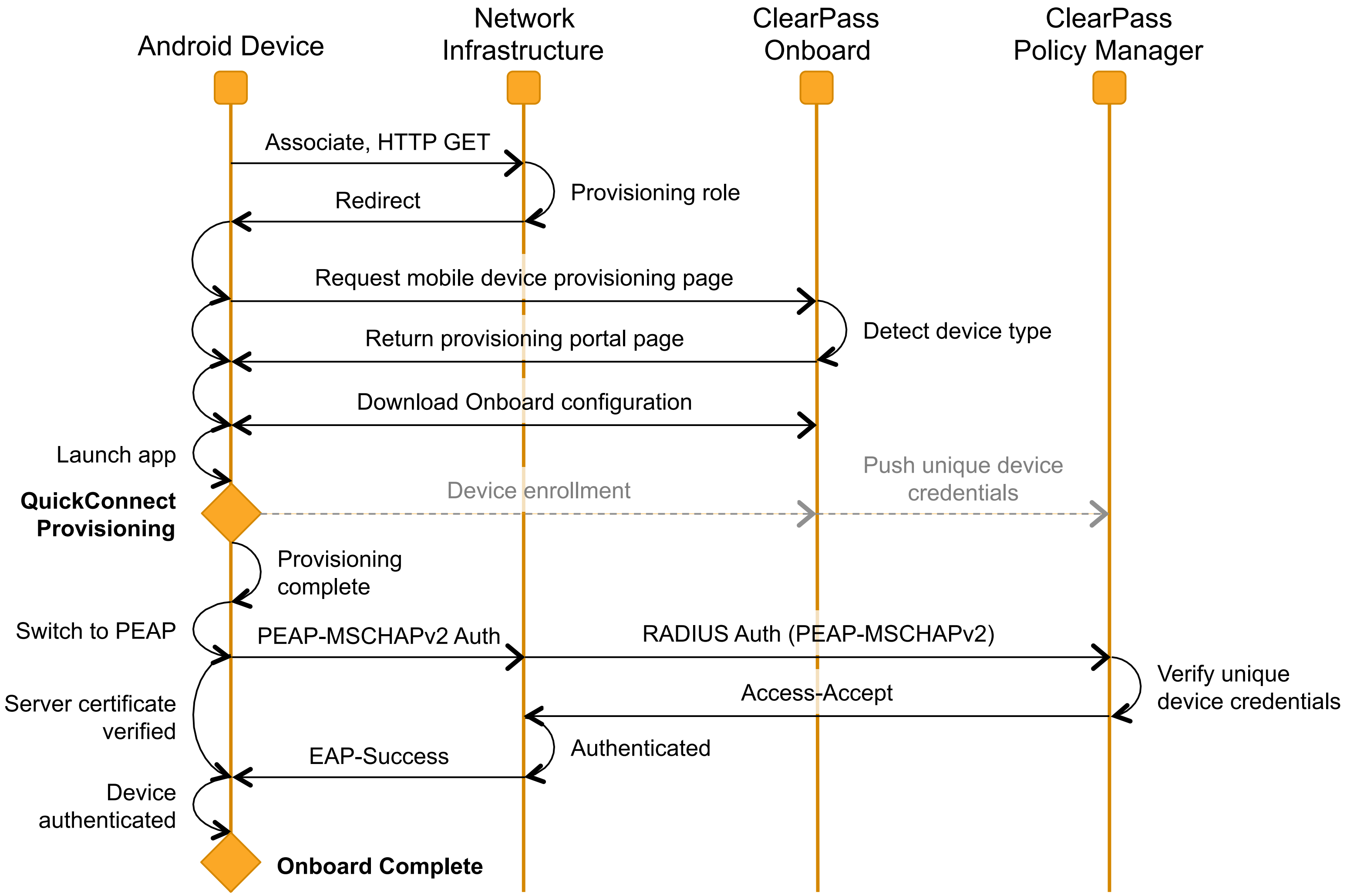
Install profile and return to Safari

Refresh enrollment progress page

Switch to EAP-TLS

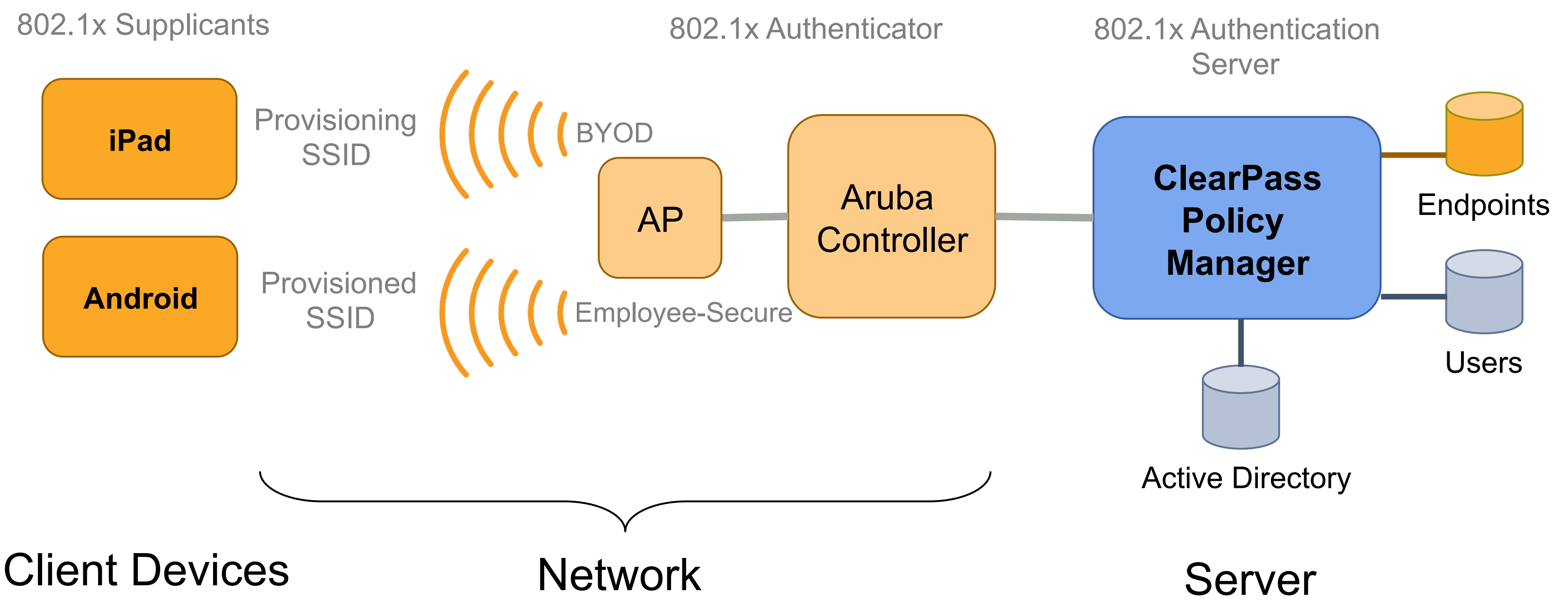
Provisioning Complete

Onboard Workflow – other OS's



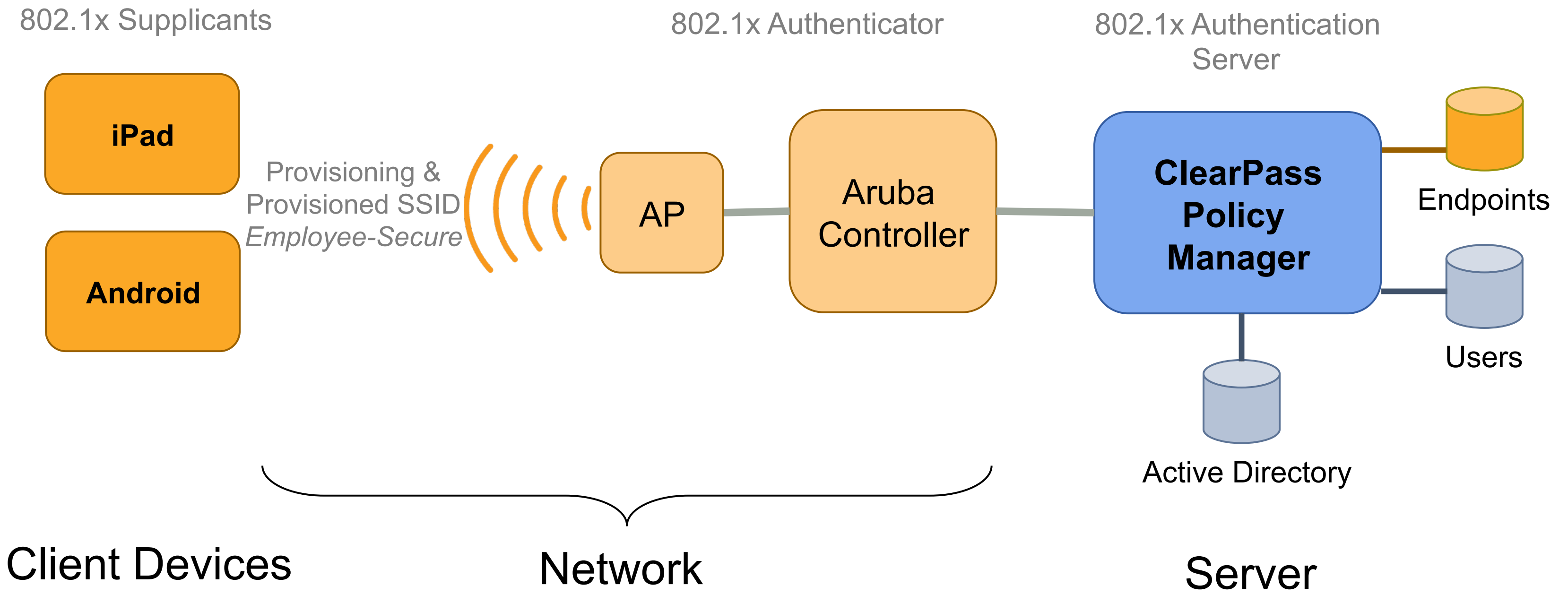
Onboarding Deployment Options

- **Different SSID for Provisioning & Provisioned**
  - Standalone SSID
  - Linked from Guest Access Portal



Onboarding Deployment Options

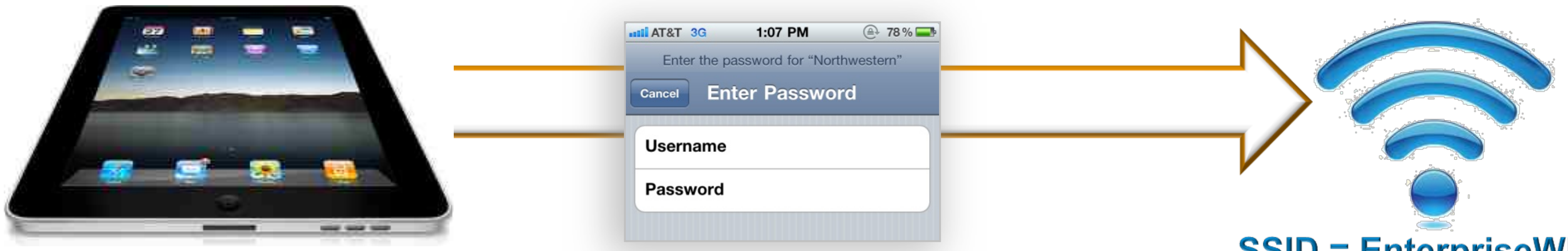
- **Same SSID for Provisioning & Provisioned**
  - Device Profiling
  - Lack of provisioning credential
  - MDM integration



Onboarding Workflow

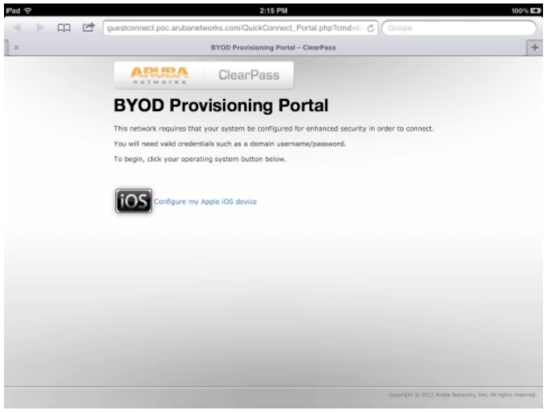
AIRHEADS 2013

1. Device type automatically detected & redirected to portal
2. Settings & credentials are auto-configured after user enters domain credentials
3. User automatically placed on proper SSID & network segment



Enter the password for “Northwestern”

SSID = EnterpriseWPA2


iPad 2:15 PM 100%

guestconnect.poc.arubanetworks.com/QuickConnect_Portal.php?cmd=lo

BYOD Provisioning Portal – ClearPass

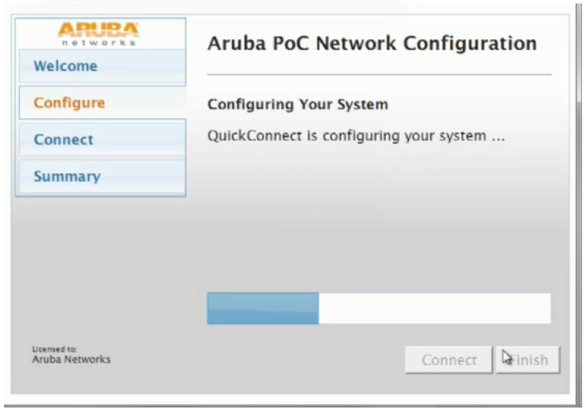
BYOD Provisioning Portal

This network requires that your system be configured for enhanced security in order to connect.

You will need valid credentials such as a domain username/password.

To begin, click your operating system button below.

iOS Configure my Apple iOS device

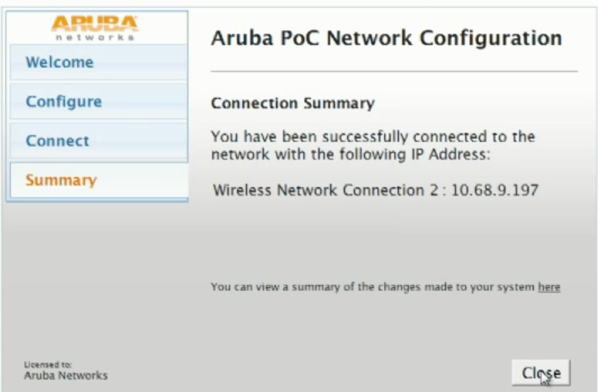


Aruba PoC Network Configuration

Configuring Your System

QuickConnect is configuring your system ...

Licensed to:
Aruba Networks



Aruba PoC Network Configuration

Connection Summary

You have been successfully connected to the network with the following IP Address:

Wireless Network Connection 2 : 10.68.9.197

You can view a summary of the changes made to your system here

Licensed to:
Aruba Networks

ARUBA networks

#airheadsconf

Detecting BYO Devices

Power of context aware policies

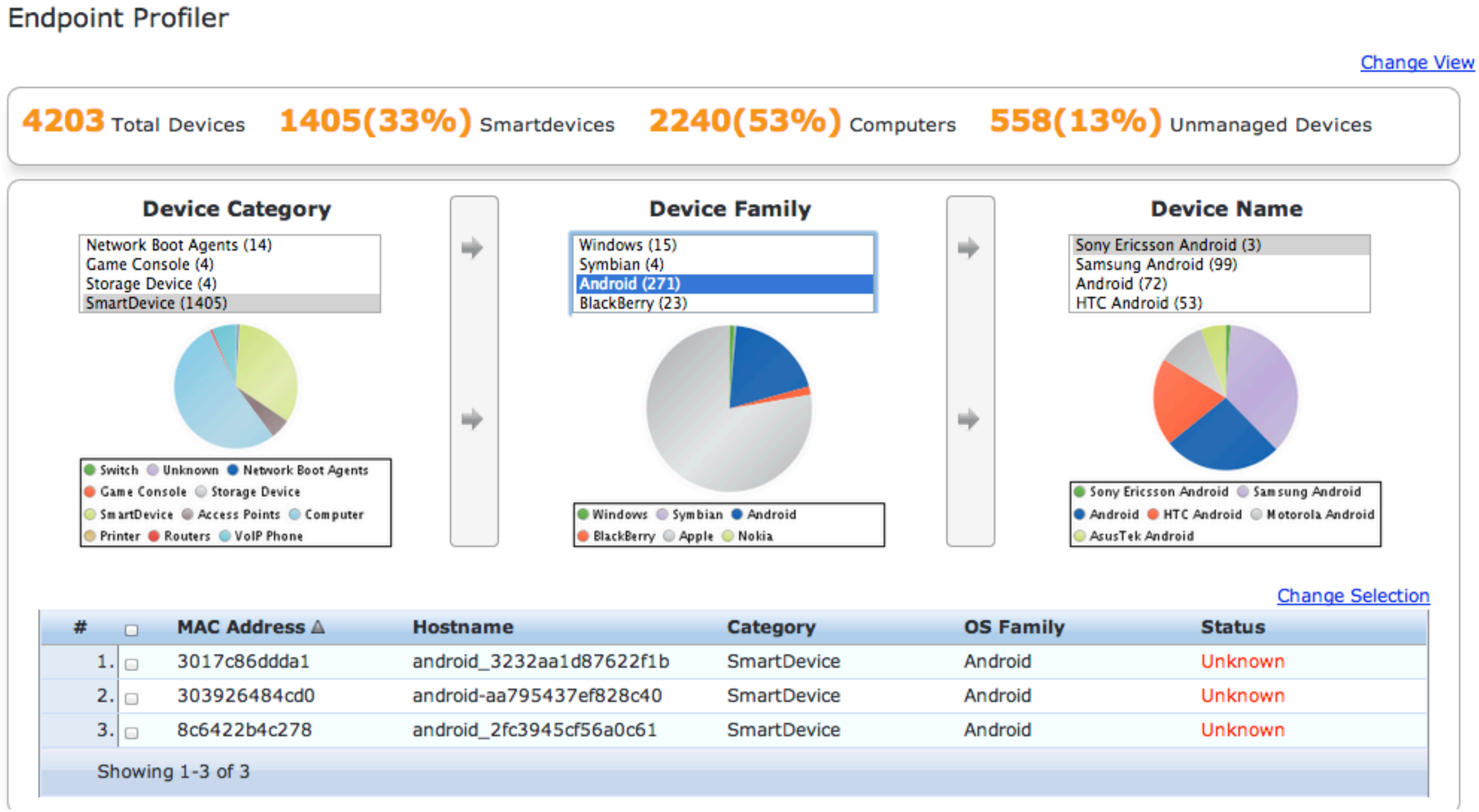
- **No longer a binary decision**
- **Leverage context sources to determine enforcement**
  - Active Directory Group Membership
  - Machine authentication for domain joined devices
  - Device Type / Posture of the device
  - Managed by MDM / context from MDM
  - Lack of provisioned credential
- **Differentiate Corporate Managed / Provisioned devices**
  - Enforce Machine Authentication differently
  - Enforce MDM managed differently
  - Enforce Onboard provisioning differently
  - Redirect unmanaged / un-provisioned device to provisioning workflow (for example – only using PEAP AD credentials)

Sources of Profile Data

- **Native**
  - MAC OUI
  - HTTP User Agent (Captive Portal Services)
  - Onboard (explicit knowledge from client OS interactions)
  - OnGuard (explicit knowledge from client OS interactions)
- **Network Sourced**
  - DHCP Option fingerprinting (DHCP relay)
  - Subnet scan with SNMP profiling (CDP, LLDP, sysDescr)
  - AOS Controller 6.3 export (DHCP, HTTP, mDNS)
- **Agent / Server Integration**
  - MS Exchange (Active-Sync device type)
  - MDM Deployments
- **Fingerprints updated automatically over the net**

CONFIDENTIAL

Sample Profile Dashboard



Endpoint Profiler

Change View

4203 Total Devices **1405(33%)** Smartdevices **2240(53%)** Computers **558(13%)** Unmanaged Devices

Device Category

Network Boot Agents (14)
Game Console (4)
Storage Device (4)
SmartDevice (1405)

Device Family

Windows (15)
Symbian (4)
Android (271)
BlackBerry (23)

Device Name

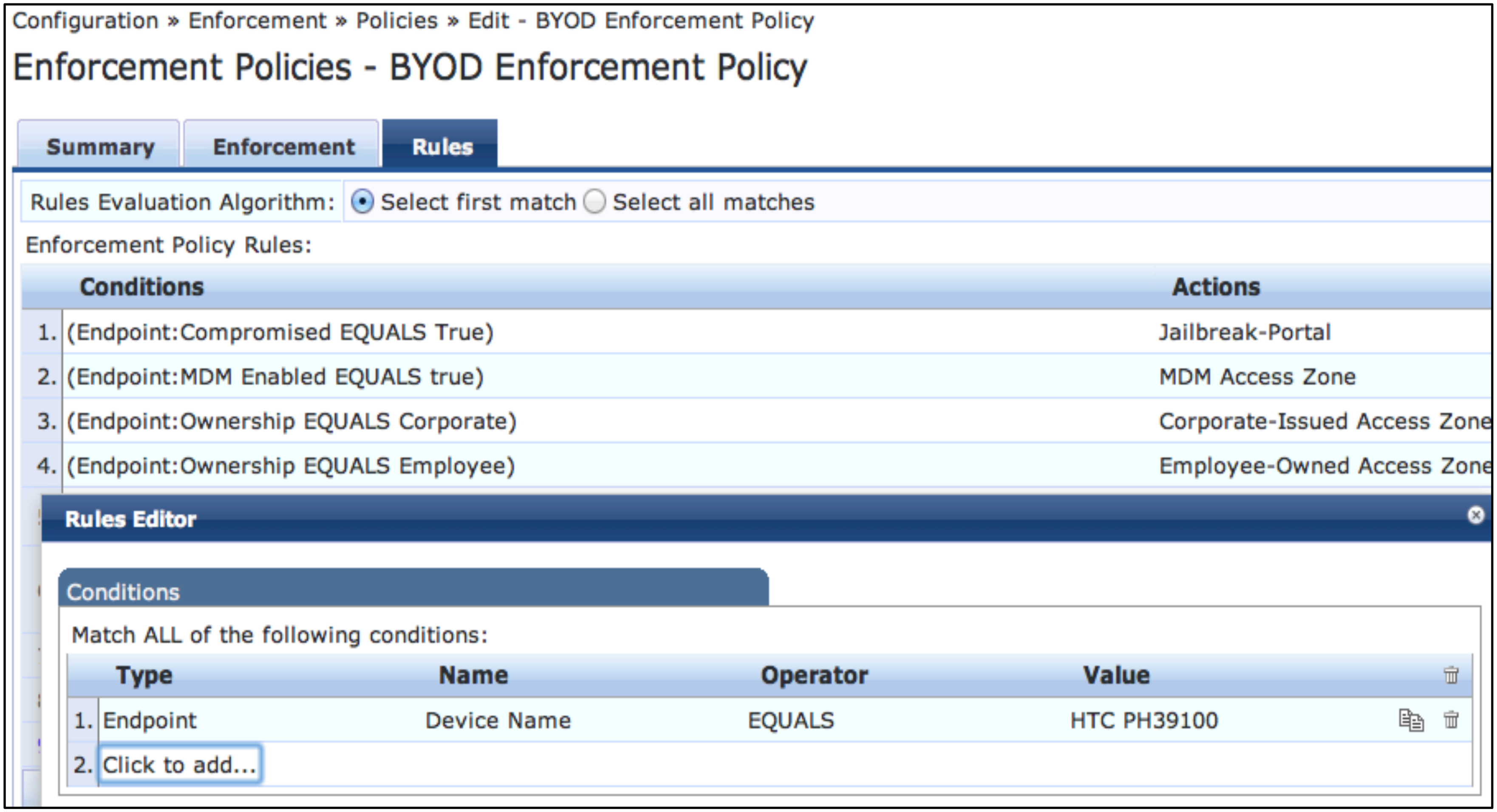
Sony Ericsson Android (3)
Samsung Android (99)
Android (72)
HTC Android (53)

Change Selection

#	□	MAC Address △	Hostname	Category	OS Family	Status
1.	□	3017c86ddda1	android_3232aa1d87622f1b	SmartDevice	Android	Unknown
2.	□	303926484cd0	android-aa795437ef828c40	SmartDevice	Android	Unknown
3.	□	8c6422b4c278	android_2fc3945cf56a0c61	SmartDevice	Android	Unknown

Showing 1-3 of 3

Example Enforcement Policy



Configuration » Enforcement » Policies » Edit - BYOD Enforcement Policy

Enforcement Policies - BYOD Enforcement Policy

Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Enforcement Policy Rules:

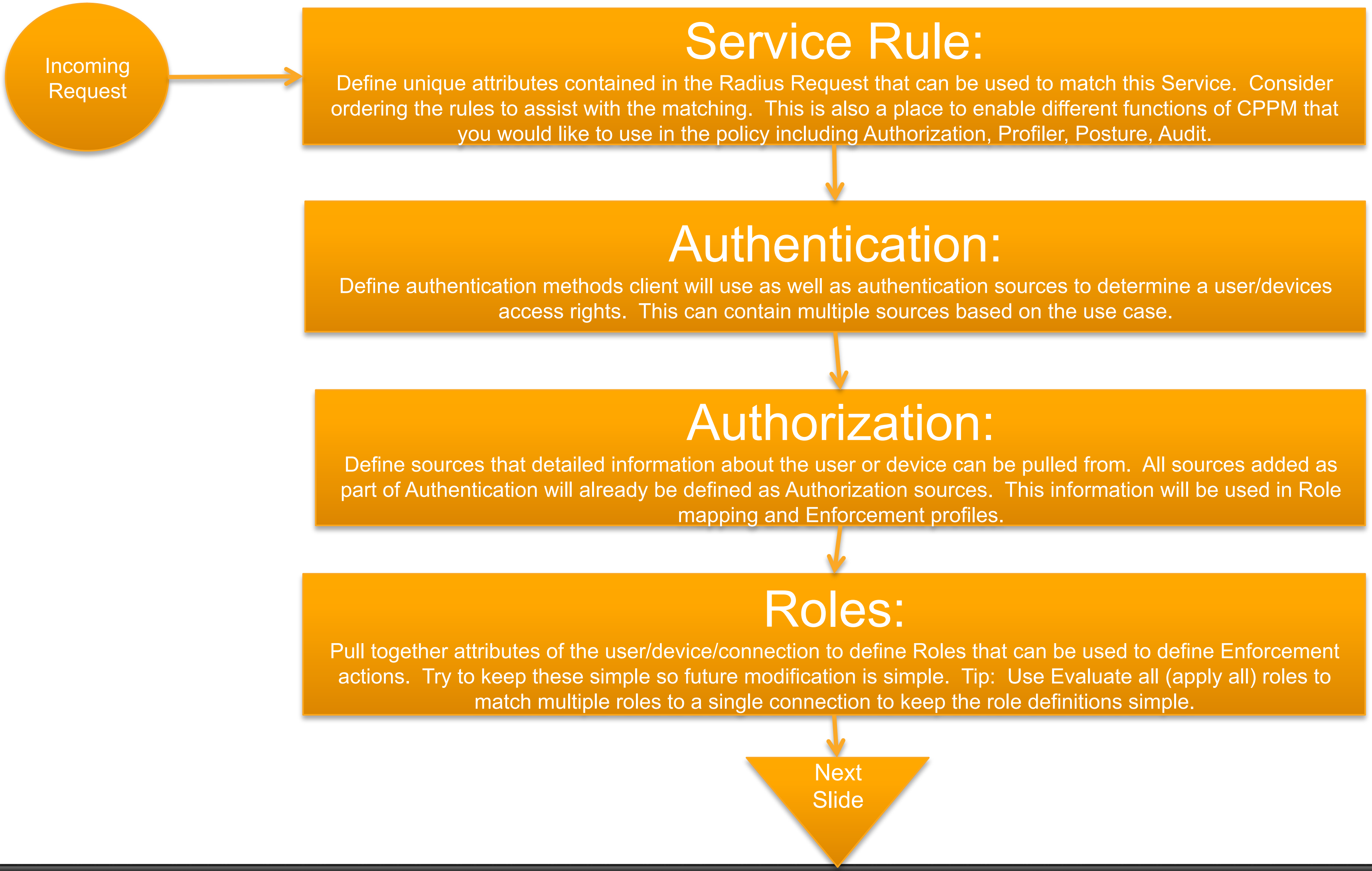
	Conditions	Actions
1.	(Endpoint:Compromised EQUALS True)	Jailbreak-Portal
2.	(Endpoint:MDM Enabled EQUALS true)	MDM Access Zone
3.	(Endpoint:Ownership EQUALS Corporate)	Corporate-Issued Access Zone
4.	(Endpoint:Ownership EQUALS Employee)	Employee-Owned Access Zone

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Endpoint	Device Name	EQUALS	HTC PH39100
2.	Click to add...			

Service Definition workflow



Incoming Request

Service Rule:

Define unique attributes contained in the Radius Request that can be used to match this Service. Consider ordering the rules to assist with the matching. This is also a place to enable different functions of CPPM that you would like to use in the policy including Authorization, Profiler, Posture, Audit.

Authentication:

Define authentication methods client will use as well as authentication sources to determine a user/devices access rights. This can contain multiple sources based on the use case.

Authorization:

Define sources that detailed information about the user or device can be pulled from. All sources added as part of Authentication will already be defined as Authorization sources. This information will be used in Role mapping and Enforcement profiles.

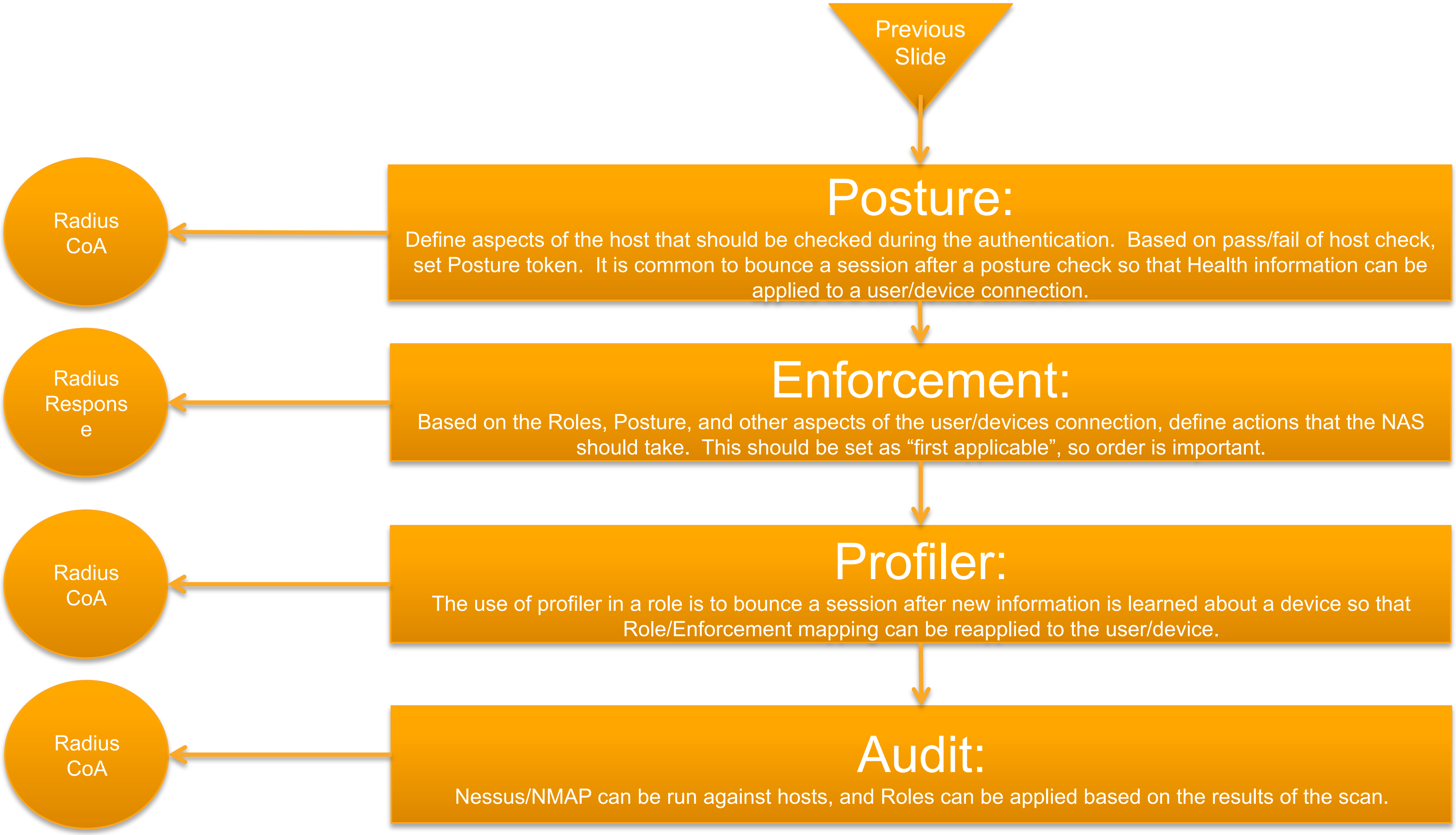
Roles:

Pull together attributes of the user/device/connection to define Roles that can be used to define Enforcement actions. Try to keep these simple so future modification is simple. Tip: Use Evaluate all (apply all) roles to match multiple roles to a single connection to keep the role definitions simple.

Next Slide

Service Definition workflow

AIRHEADS 2013



Previous Slide

Posture:

Define aspects of the host that should be checked during the authentication. Based on pass/fail of host check, set Posture token. It is common to bounce a session after a posture check so that Health information can be applied to a user/device connection.

Radius CoA

Enforcement:

Based on the Roles, Posture, and other aspects of the user/devices connection, define actions that the NAS should take. This should be set as “first applicable”, so order is important.

Radius Response

Profiler:

The use of profiler in a role is to bounce a session after new information is learned about a device so that Role/Enforcement mapping can be reapplied to the user/device.

Radius CoA

Audit:

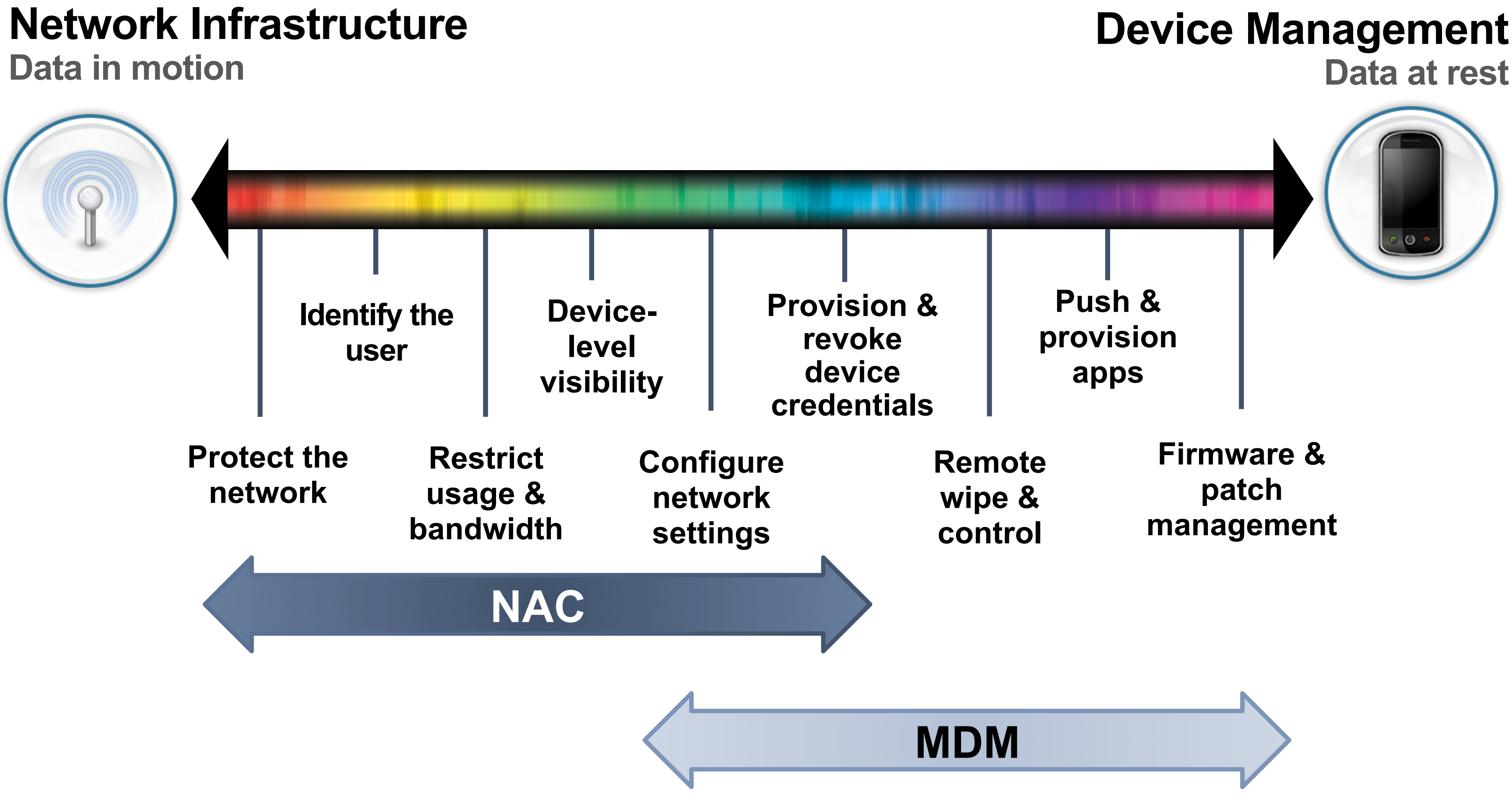
Nessus/NMAP can be run against hosts, and Roles can be applied based on the results of the scan.

Radius CoA

MDM Integration

Managing Mobility

AIRHEADS 2013

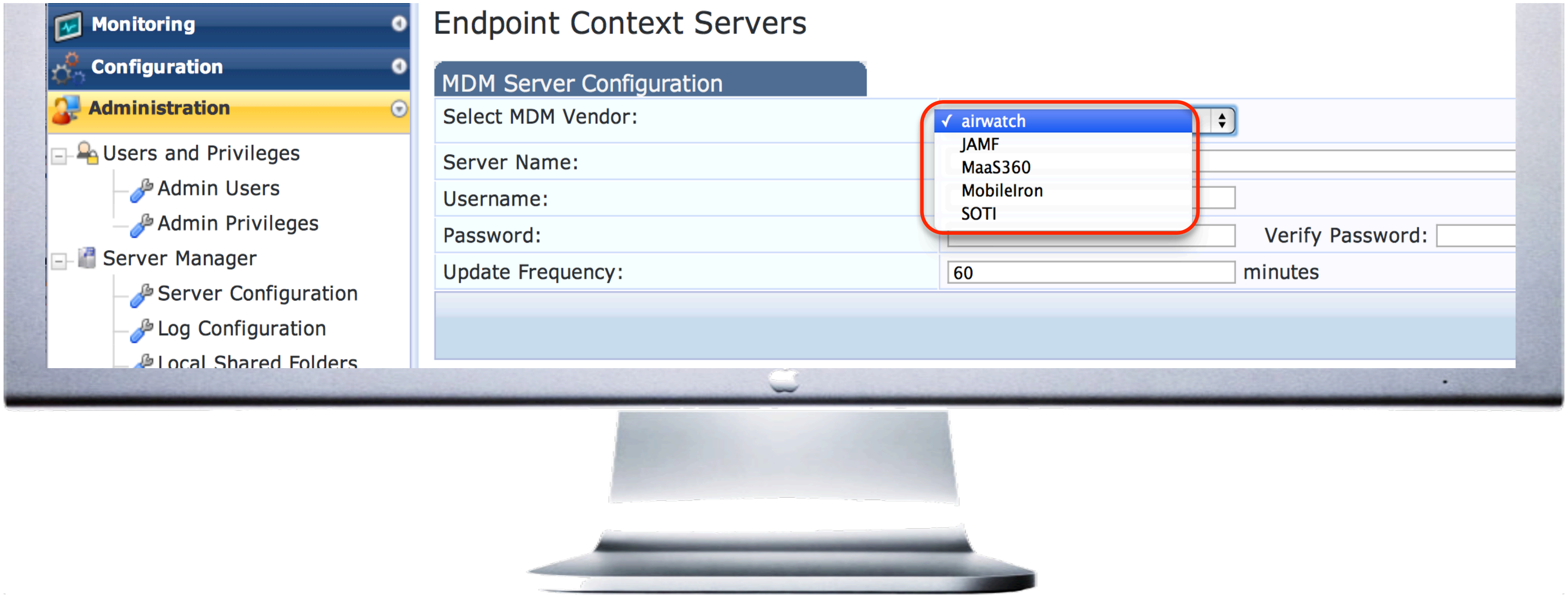


Integrating Leading MDM Vendors

- ClearPass uses public APIs for:

airwatch SOTI MobileIron MaaS360 by Fiberlink JAMF software

- Normalize MDM endpoint data across vendors



Endpoint Context Servers

MDM Server Configuration

Select MDM Vendor:	✓ airwatch JAMF MaaS360 MobileIron SOTI
Server Name:	
Username:	
Password:	Verify Password:
Update Frequency:	60 minutes

Mutually Leverage Context

Exchange endpoint context & trigger policies

SOTI
airwatch
MaaS360 by Fiberlink
MobileIron
JAMF software

Network Policies

Device Policies

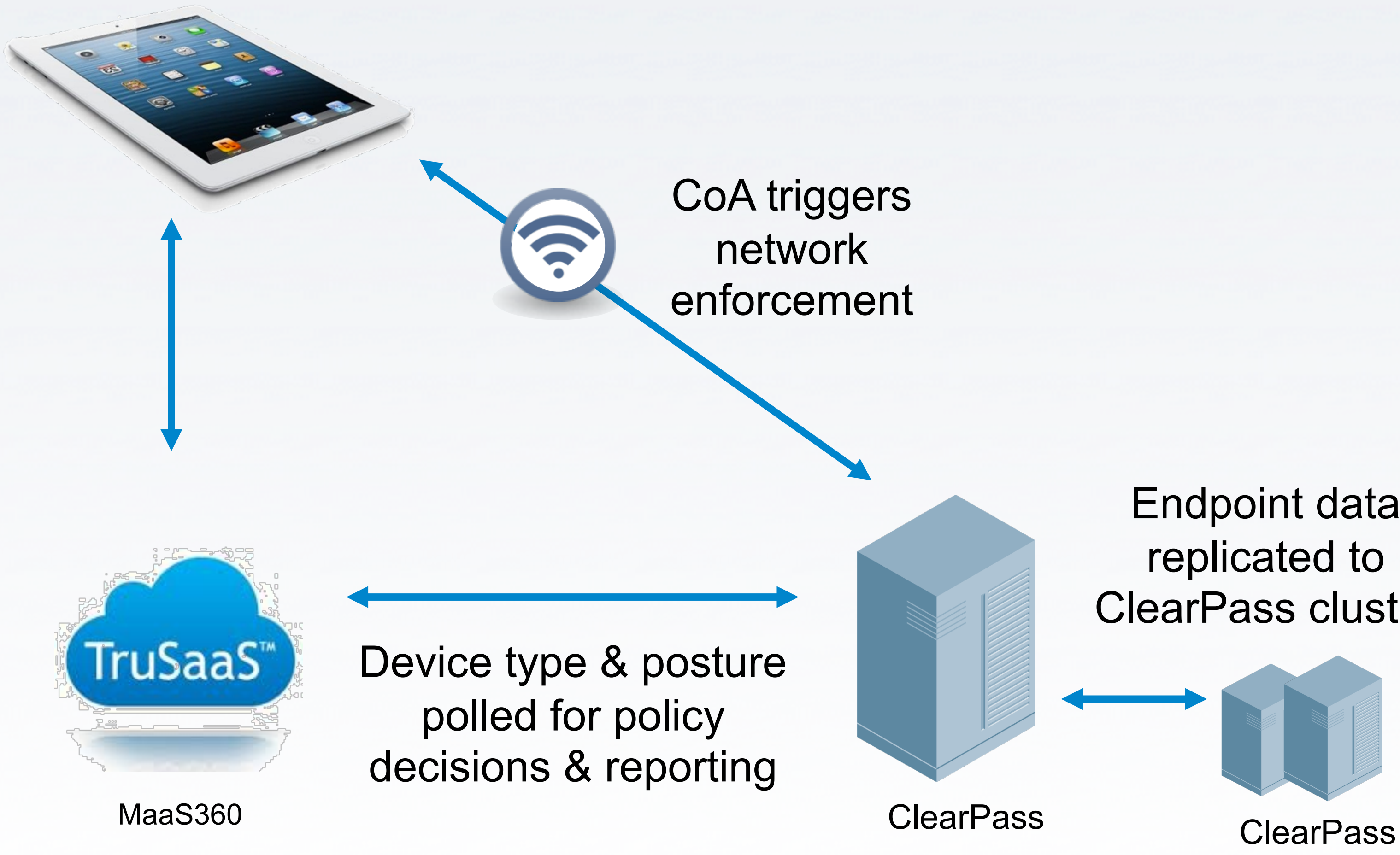
- Firewall Policies
- Redirect to enroll
- Quarantine devices
- Bandwidth Prioritization

- Device restrictions
- Remote Lock & Wipe
- Install Application
- Black list Apps

ClearPass MDM Integration

AIRHEADS 2013

Using MDM device information for Policy



CoA triggers network enforcement
TruSaaS™
MaaS360
Device type & posture polled for policy decisions & reporting
ClearPass
Endpoint data replicated to ClearPass cluster
ClearPass

Use MDM Attributes for Network Policy

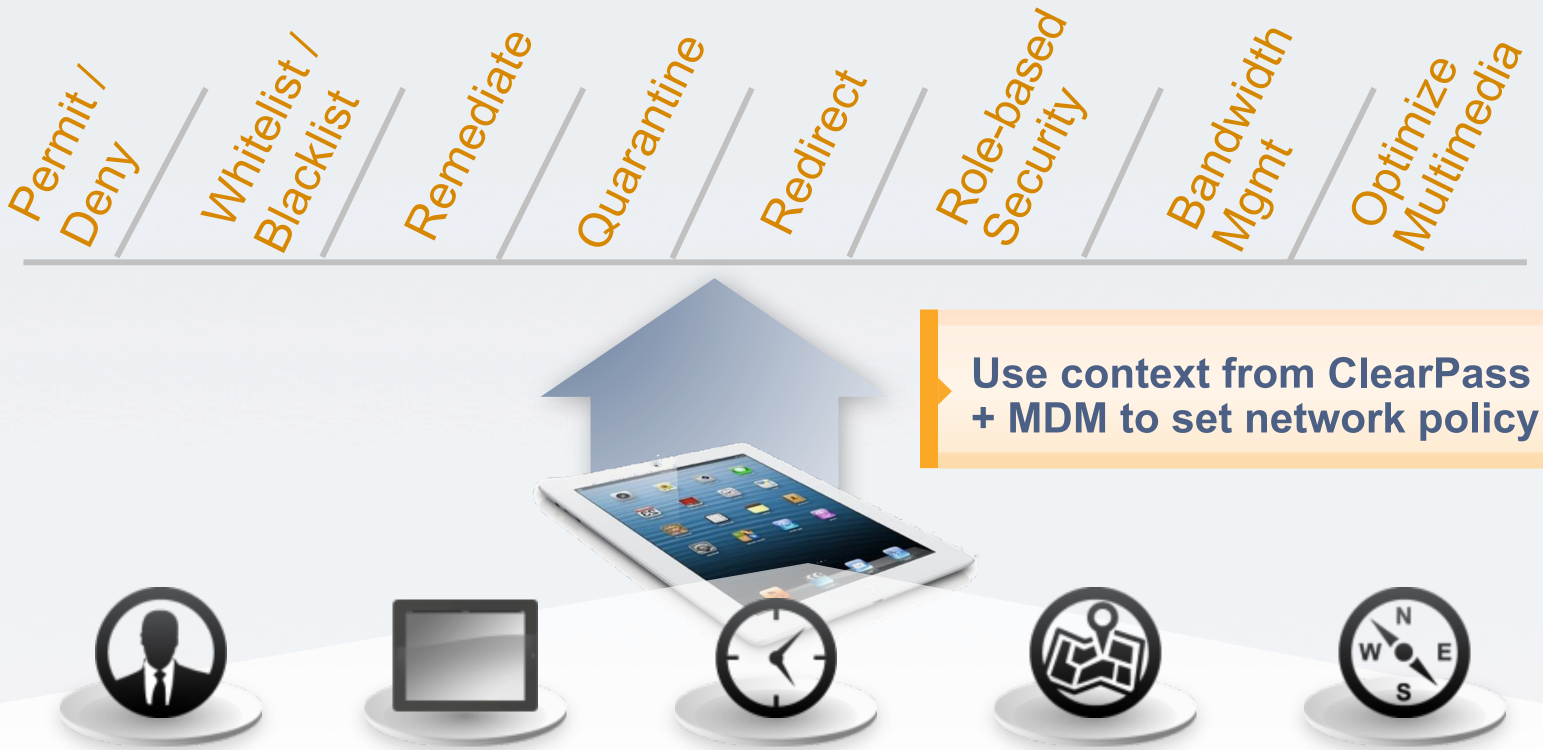
MDM Attributes

Inventory	**Manufacturer:**	Apple
	Model:	iPad2
	OS Version:	iOS 6.1
	UDID	1730235f564094186
	Serial Number	79049XXXA4S
	IMEI	012416009780168
	Phone Number	408-534-2819
	Carrier	Verizon
	MDM Id	130d0f992t34
	Owner	jhoward
	Display Name	John Howard
	Ownership	Employee Liable
Posture	**MDM Enabled**	Yes
	Compromised	Not Jailbroken
	Encryption Enabled	Yes
	Blacklisted Apps	No
	Required Apps	Yes
	Last Check in	01/30/2012 9:03am

Setting Network Policy

AIRHEADS 2013

Policy Example



Use context from ClearPass + MDM to set network policy

WHO

- User/group membership

WHAT

- Device Profile
- OS version
- Endpoint health
- Jailbreak status
- Pincode/encryption

WHEN

- Time/Date
- eg. in semester

WHERE

- Location
- Trusted or untrusted network

HOW

- Application installed
- blacklisted

Integrated User Onboarding

Provisioning Workflow

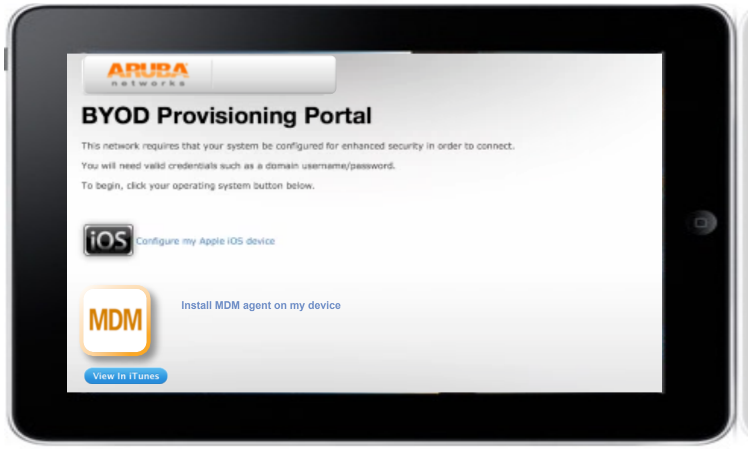
- Detect un-enrolled device connected to the network

- Redirect to MDM self-service portal

  or

  Prompt user to download MDM agent

- Host MDM application, from network captive portal



BYOD Provisioning Portal

This network requires that your system be configured for enhanced security in order to connect.

You will need valid credentials such as a domain username/password.

To begin, click your operating system button below.

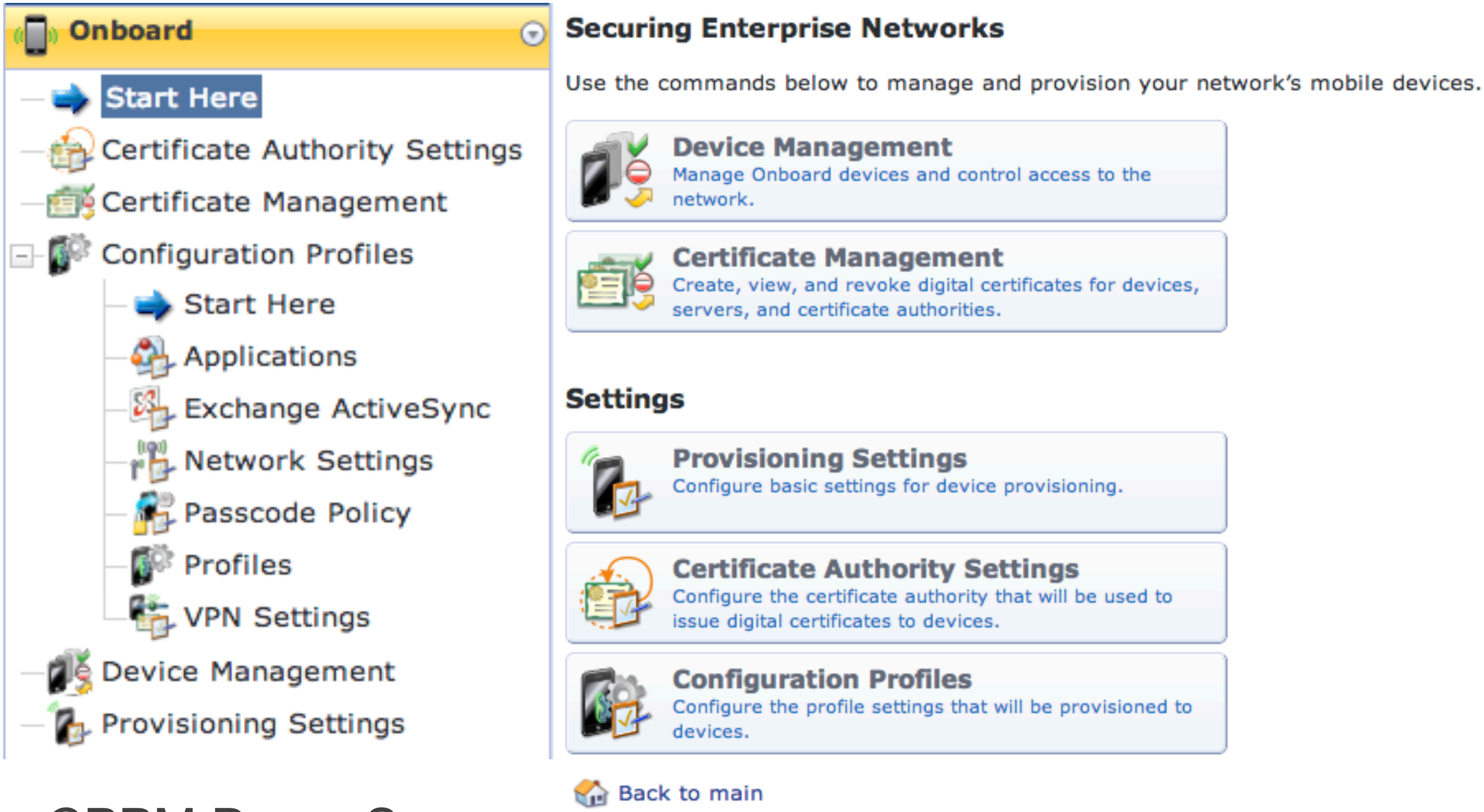
Onboard Setup

Certificate Authority Setup

- **TLS client certificate provisioned per device**
- **Onboard using built in CA**
  - Act as standalone Root CA
  - Integrate with existing PKI as Intermediate CA
  - SCEP Proxy options coming soon
- **Certificates replicated throughout cluster**
  - Onboard proxied to publisher node (http proxy)
  - Proxy process transparent to client device
  - Client certificates available on replicated to subscribers
- **OSCP Responder available from subscribers**
  - Locally check for revocation of client certificates
  - OSCP configured to override to localhost

Configuring Onboard - Walkthrough

AIRHEADS 2013



Securing Enterprise Networks

Use the commands below to manage and provision your network's mobile devices.

Device Management
Manage Onboard devices and control access to the network.

Certificate Management
Create, view, and revoke digital certificates for devices, servers, and certificate authorities.

Settings

Provisioning Settings
Configure basic settings for device provisioning.

Certificate Authority Settings
Configure the certificate authority that will be used to issue digital certificates to devices.

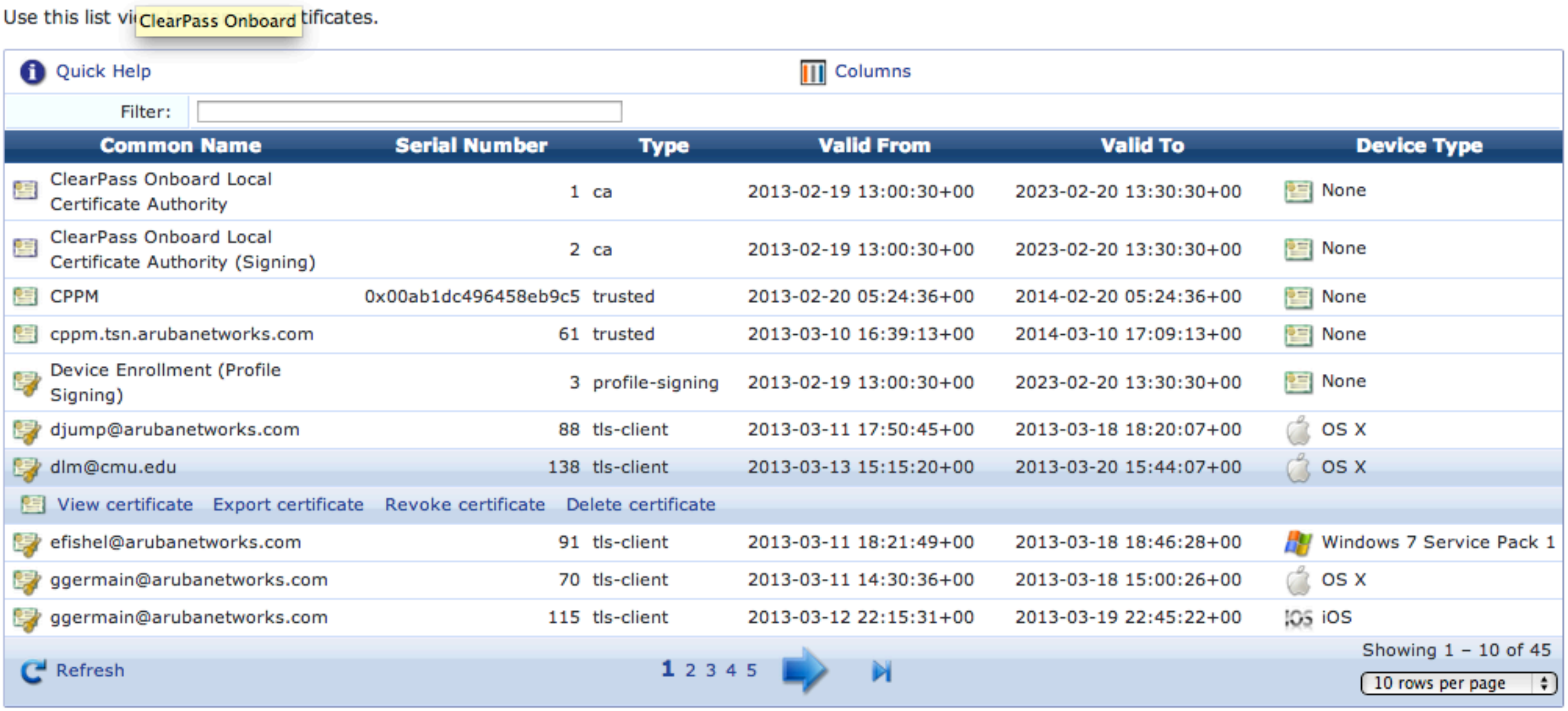
Configuration Profiles
Configure the profile settings that will be provisioned to devices.

Back to main

CPPM Demo Server

Troubleshooting

Managing client certificates



Use this list vi ClearPass Onboard tificates.

Quick Help   Columns

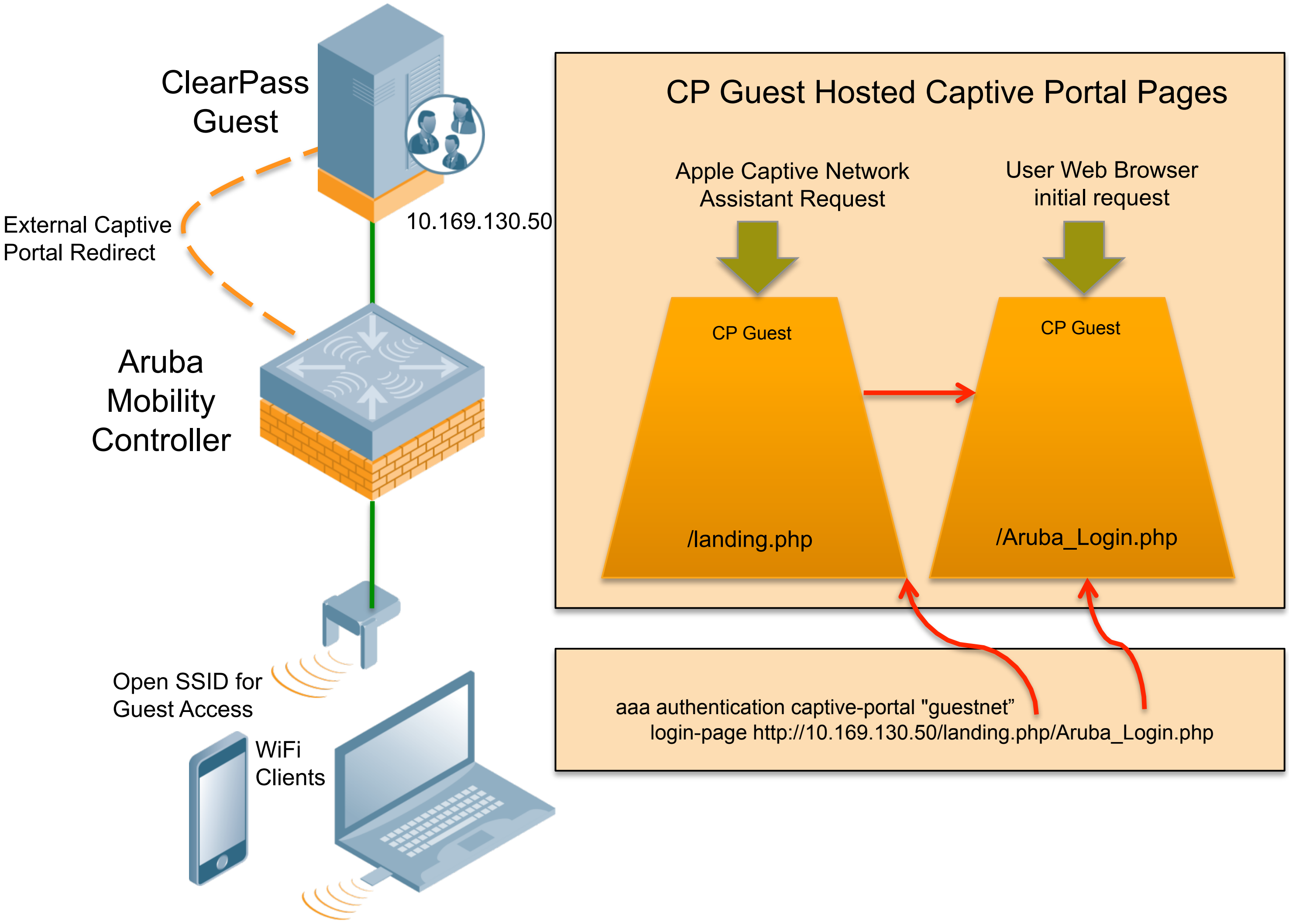
Filter:

Common Name	Serial Number	Type	Valid From	Valid To	Device Type
ClearPass Onboard Local Certificate Authority	1	ca	2013-02-19 13:00:30+00	2023-02-20 13:30:30+00	None
ClearPass Onboard Local Certificate Authority (Signing)	2	ca	2013-02-19 13:00:30+00	2023-02-20 13:30:30+00	None
CPPM	0x00ab1dc496458eb9c5	trusted	2013-02-20 05:24:36+00	2014-02-20 05:24:36+00	None
cppm.tsn.arubanetworks.com	61	trusted	2013-03-10 16:39:13+00	2014-03-10 17:09:13+00	None
Device Enrollment (Profile Signing)	3	profile-signing	2013-02-19 13:00:30+00	2023-02-20 13:30:30+00	None
djump@arubanetworks.com	88	tls-client	2013-03-11 17:50:45+00	2013-03-18 18:20:07+00	OS X
dlm@cmu.edu	138	tls-client	2013-03-13 15:15:20+00	2013-03-20 15:44:07+00	OS X
View certificate Export certificate Revoke certificate Delete certificate					
efishel@arubanetworks.com	91	tls-client	2013-03-11 18:21:49+00	2013-03-18 18:46:28+00	Windows 7 Service Pack 1
ggermain@arubanetworks.com	70	tls-client	2013-03-11 14:30:36+00	2013-03-18 15:00:26+00	OS X
ggermain@arubanetworks.com	115	tls-client	2013-03-12 22:15:31+00	2013-03-19 22:45:22+00	iOS

Refresh   1 2 3 4 5   Showing 1 – 10 of 45   10 rows per page

- **Revoke/Delete client certificates**
- **Quick search to find specific users/devices**

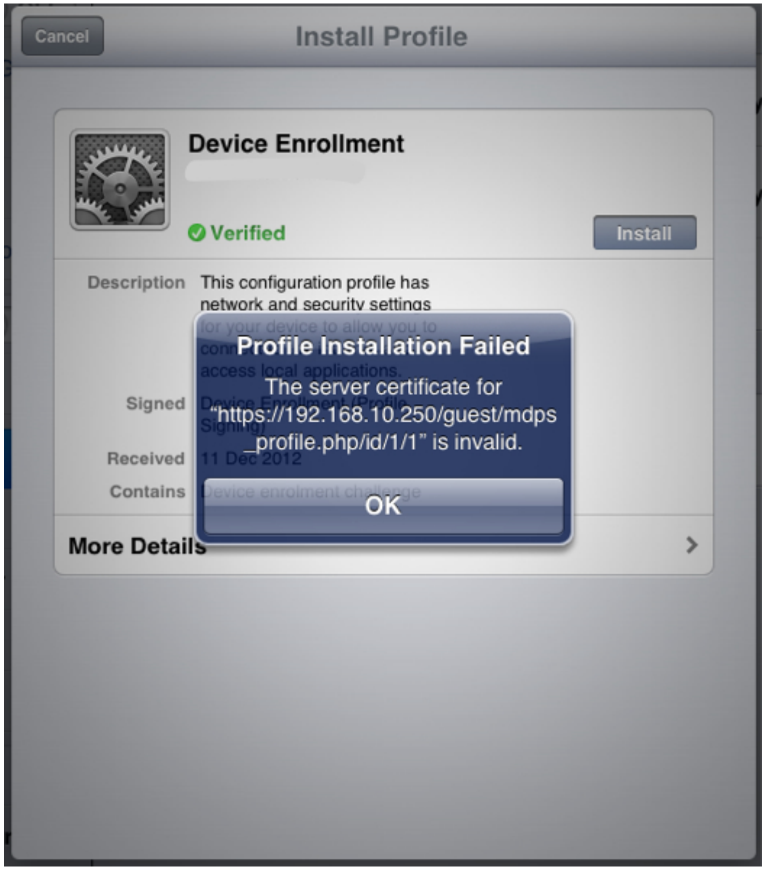
Apple Captive Network Assistant



```
aaa authentication captive-portal "guestnet”
   login-page http://10.169.130.50/landing.php/Aruba_Login.php
```

Invalid Profile when Onboarding

- **iOS expects to trust the web server hosting the profiles being pushed**
- **Multiple options to resolve**
  - Use HTTP if using L2 WiFi encryption
  - Install publically signed web server cert
  - Sign web server cert from Onboard CA
- **Its all about iOS server trust**



Device Enrollment

✓ Verified

Description: This configuration profile has network and security settings for your device to allow you to conn… access local applications.

Signed: Device Enrollment (Profile Signing)

Received: 11 Dec 2012

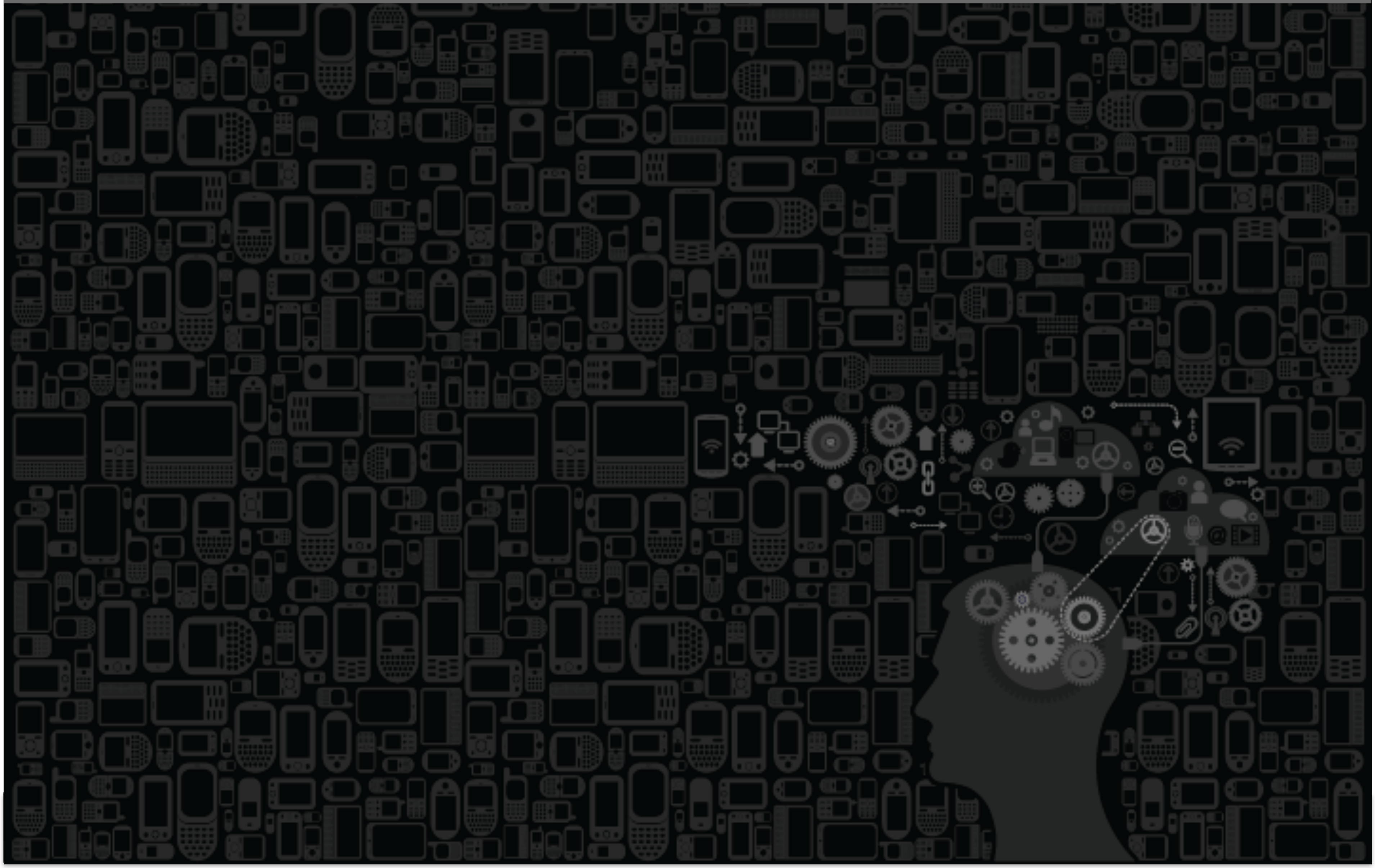
Contains: Device enrolment challenge

Profile Installation Failed

The server certificate for "https://192.168.10.250/guest/mdps_profile.php/id/1/1" is invalid.

Q&A

AIRHEADS 2013



AIRHEADS 2013

The Airheads Challenge

Use Unlock Code “ONBOARD”

To get the quiz for this session

Login to play at

community.arubanetworks.com

ARUBA networks

#airheadsconf

Thank You

AIRHEADS
LAS VEGAS 2013

JOIN: community.arubanetworks.com

FOLLOW: @arubanetworks

DISCUSS: #airheadsconf