Extending BYOD with ClearPass

Aruba Network Services Team

June2013

AIRHEADS 2013

ARUBA networks

#airheadsconf

Agenda

- The Big Picture
- Onboarding with ClearPass
  - Technology Deployment
  - Detecting BYOD Devices
- Device Management with ClearPass
  - MDM Partners
  - Native ClearPass
- App Management with ClearPass
- Q&A

The Big Picture

BYOD Creating a New Set of Challenges

AIRHEADS 2013

- How do I get personal devices provisioned?
- How do I keep corporate data safe?
- How do I protect my network?
- What if a mobile device is lost?
- How do I maintain user privacy?

NETWORK: NAC?

DEVICE: MDM?

APP: MAM?

Policy Enforcement Options for BYOD

NAC / AAA

- VLAN
- ACLs
- QoS
- Authentication

MDM

- Device Provisioning & Onboarding
- Device Policy
- Device Level Encryption
- Passcode
- Full Wipe
- App blacklist / whitelist

MAM

- Authentication
- App Passcode
- App Wipe
- App Policies
- App SSO
- App VPN

First System to Combine All BYOD Tools

AIRHEADS 2013

ClearPass with Aruba WorkSpace

Who

What

When

Where

How

Network Control

1 Unified access management

NEW

Device Control

2 Built-in Onboarding & MDM

NEW

Application Control

3 Built-in mobile app management

4 Complete BYOD visibility and control

Onboarding with ClearPass

Technology Overview

BYOD Workflow

AIRHEADS 2013

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

1 Onboard Device

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

2 Join BYOD Domain

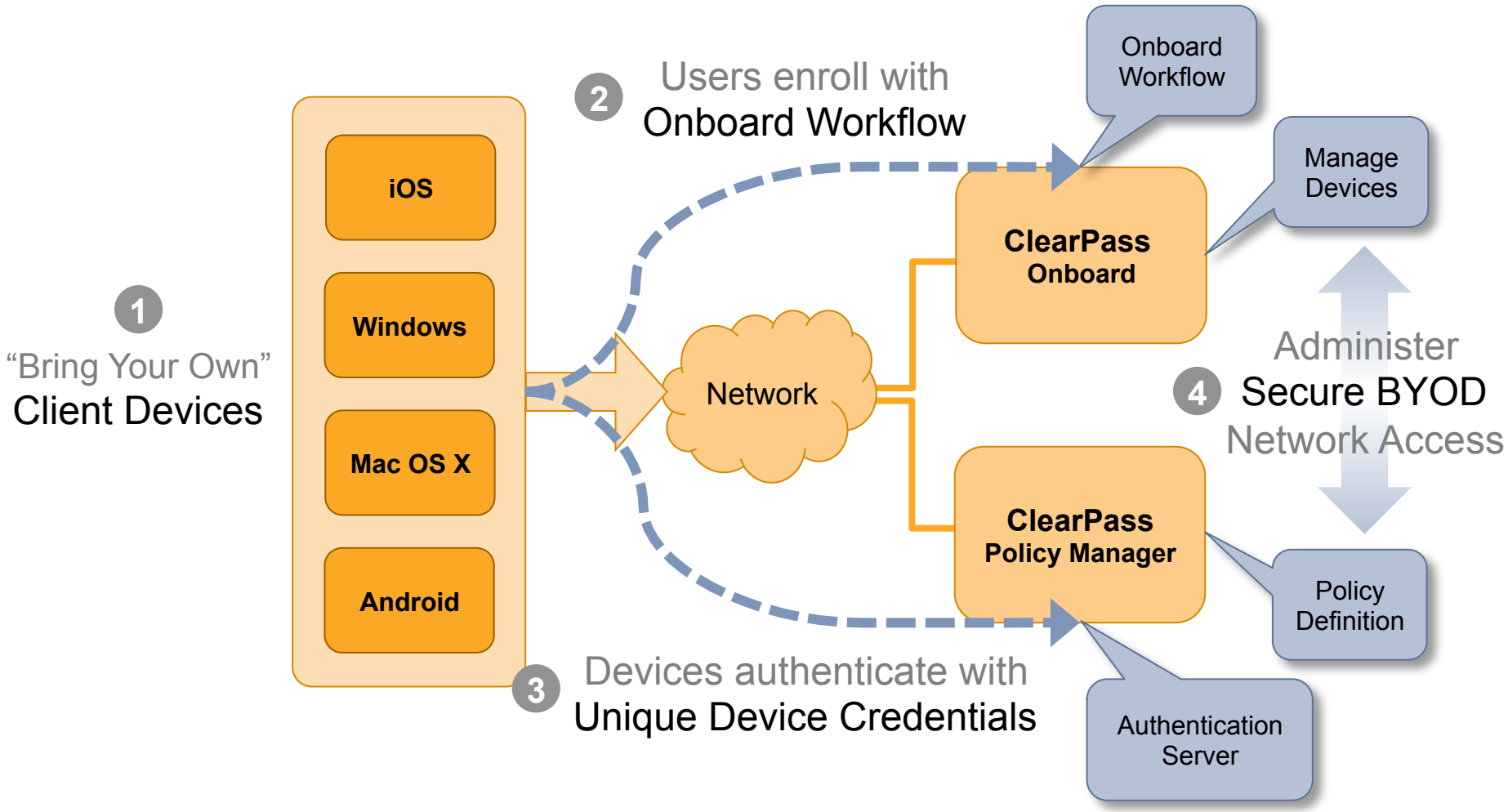
3 Device Access Controls

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

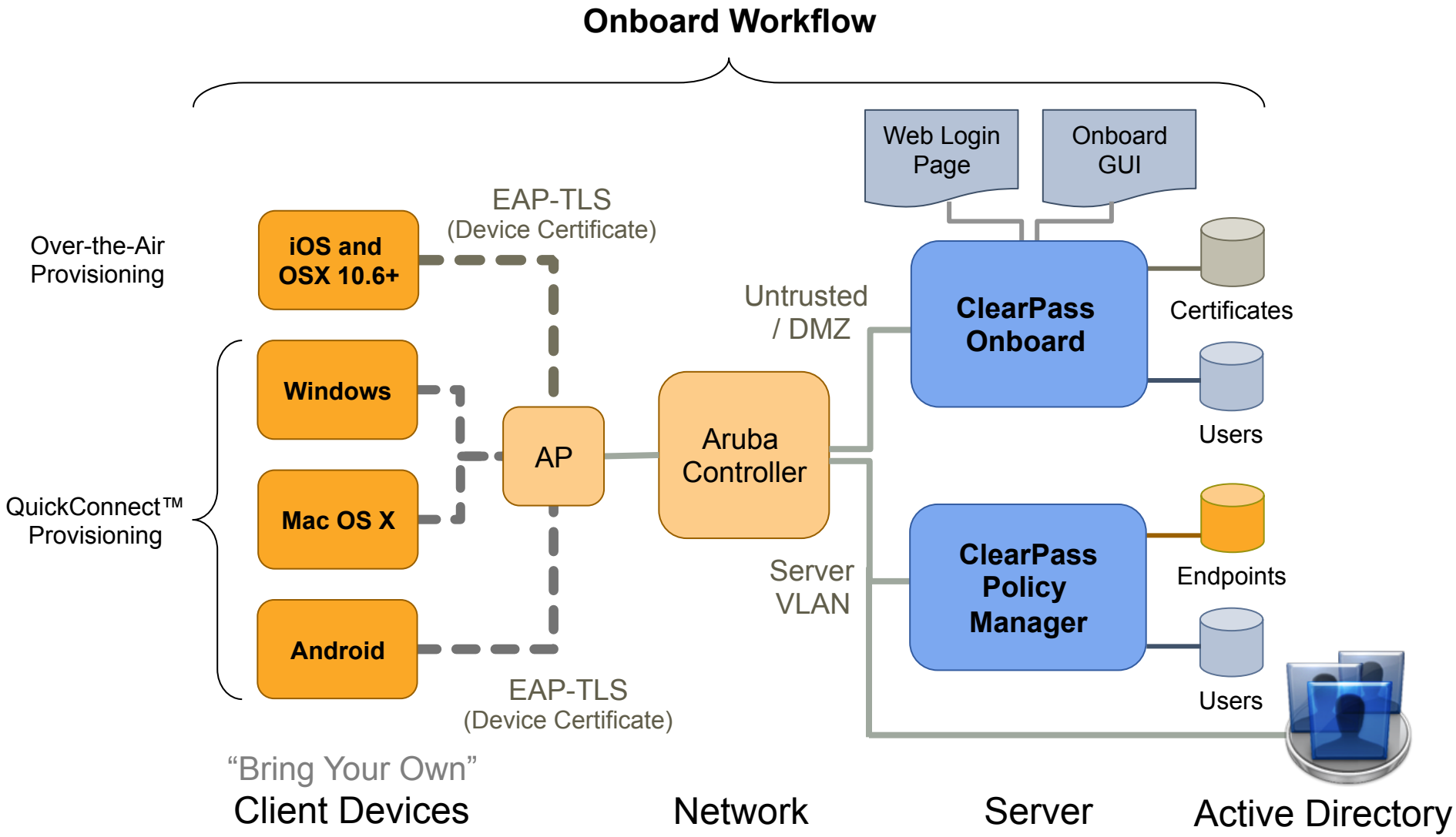
4 Visibility & Reporting

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

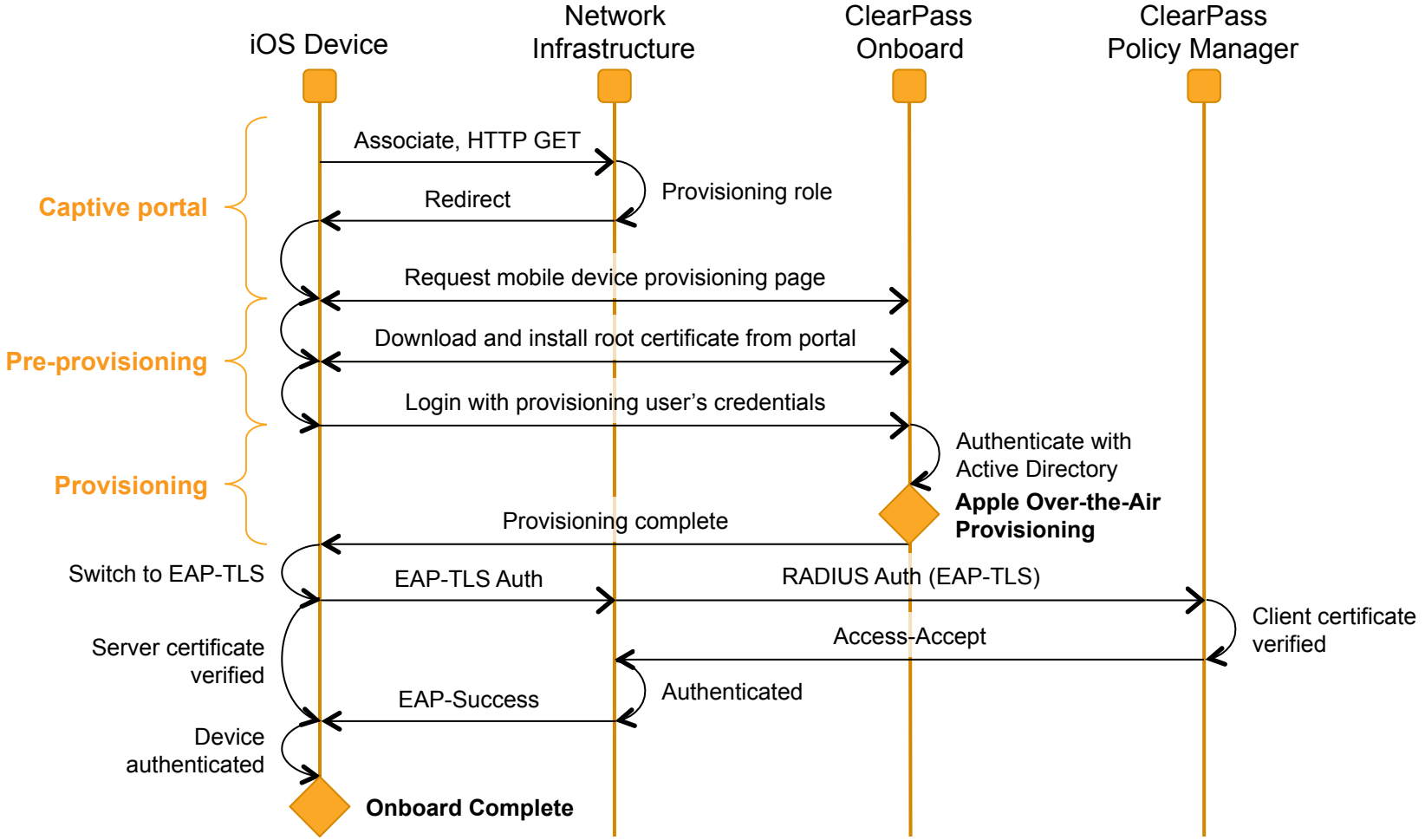
Deployment Architecture



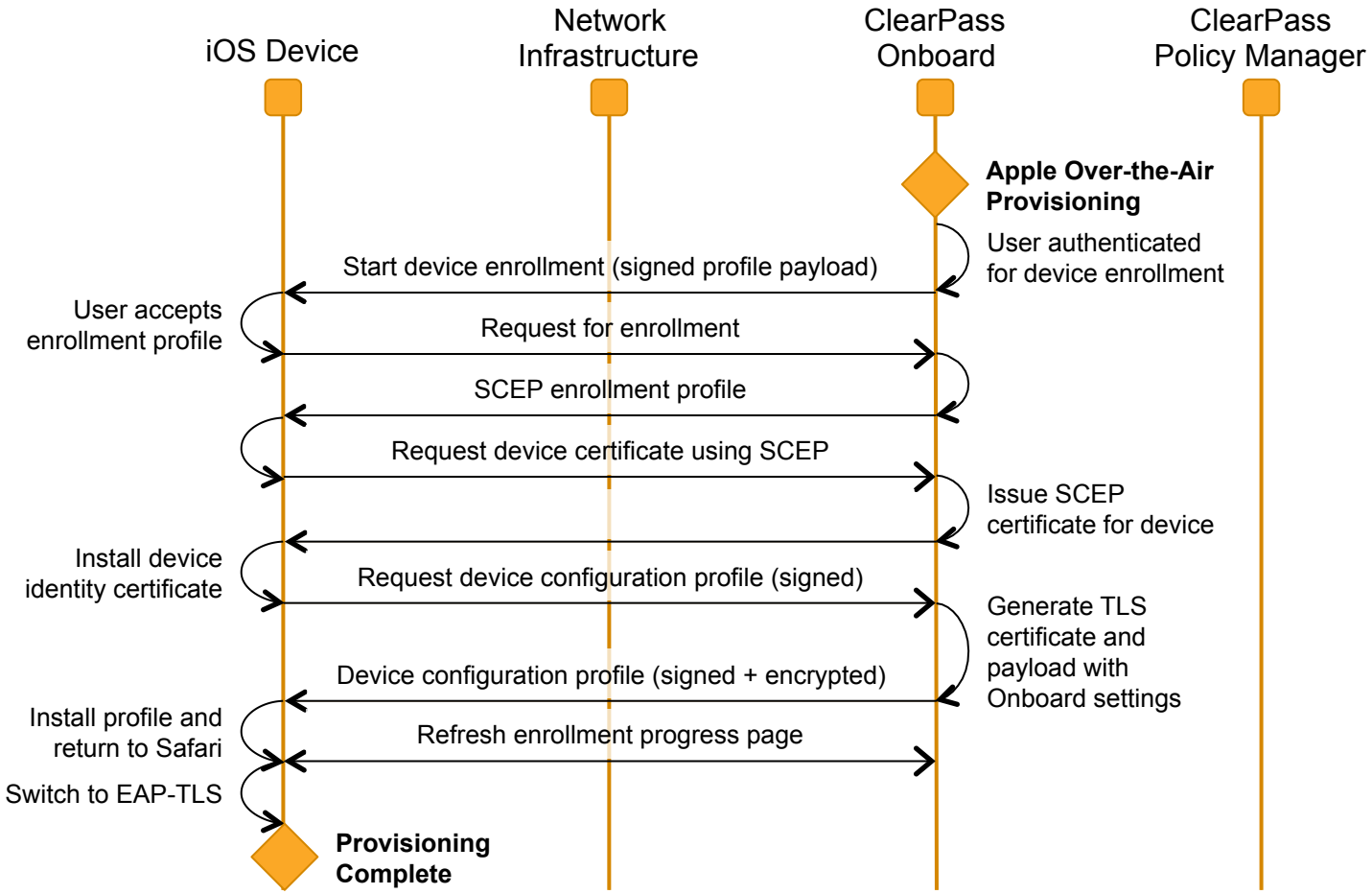
Detailed Architecture



Onboard Workflow – iOS & OS X



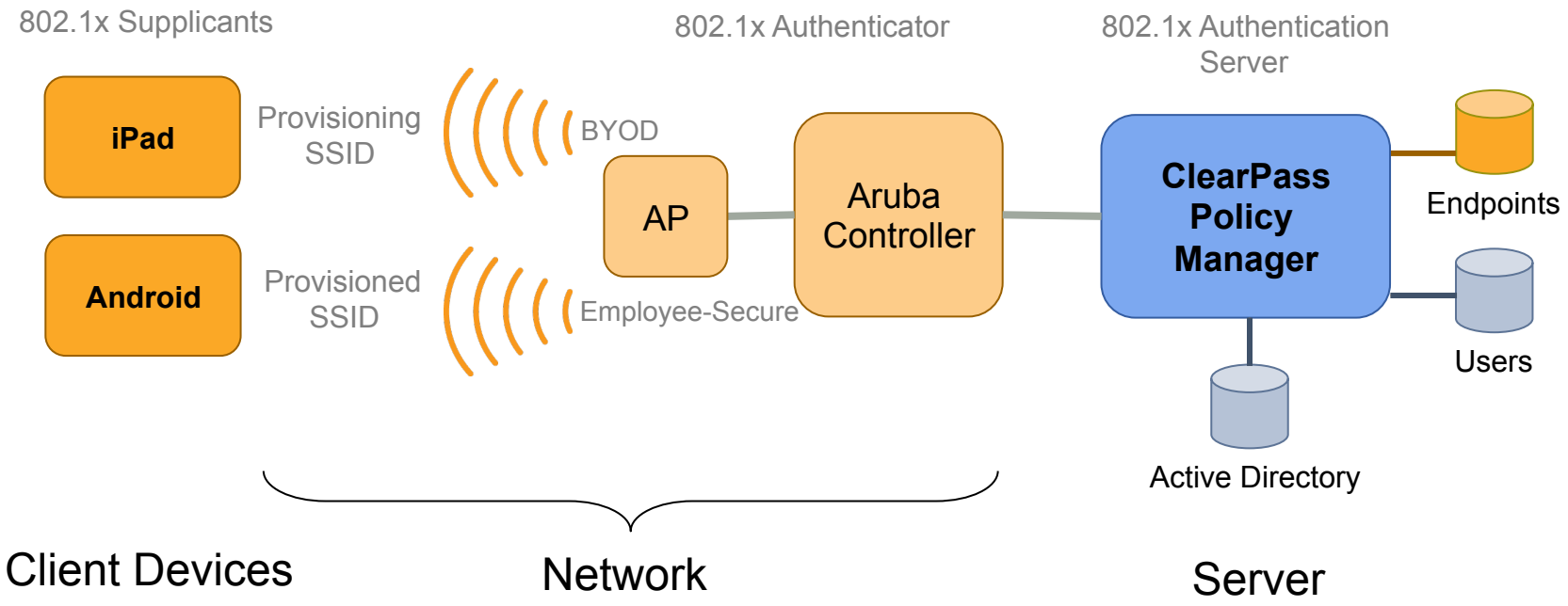
iOS “Over-the-Air Provisioning”



Onboard Workflow – other OS's

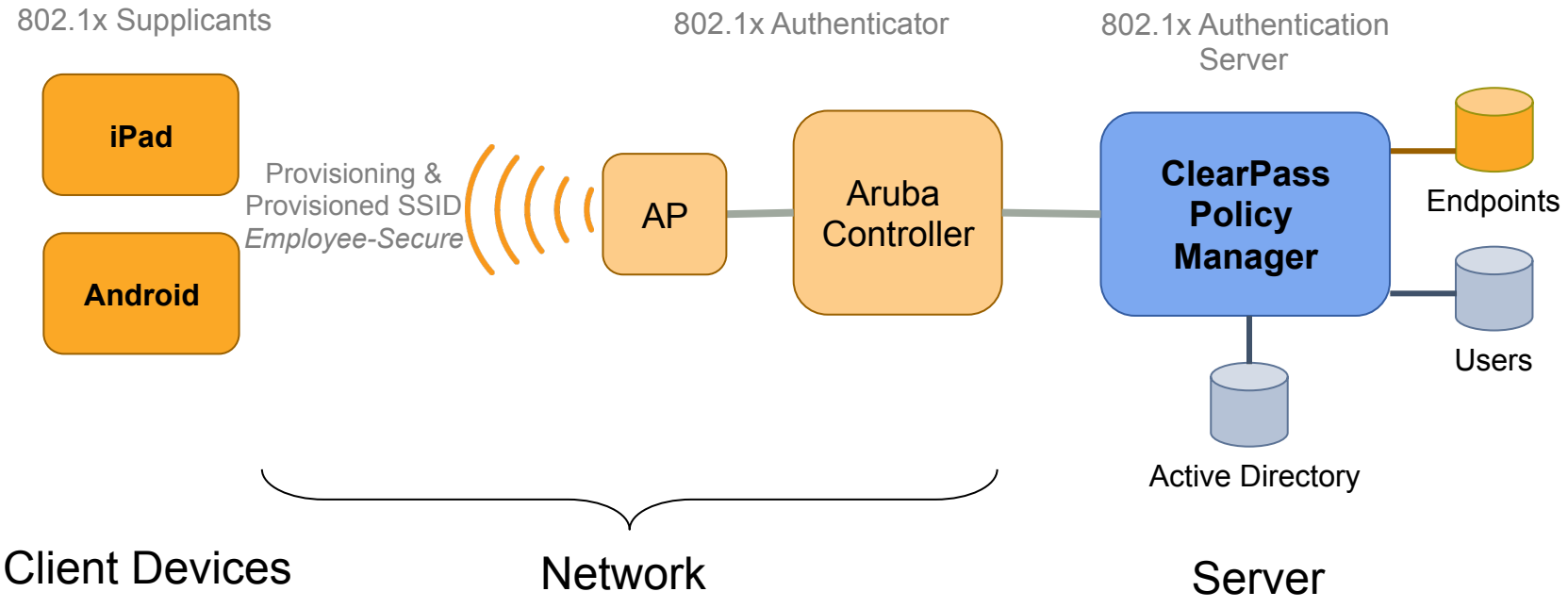
Onboarding Deployment Options

- **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



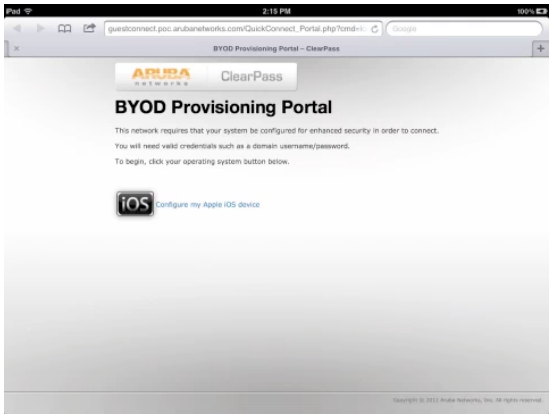
Onboarding Workflow

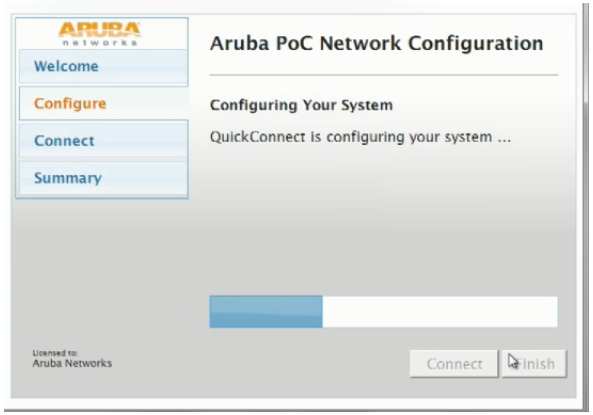
1. Device type automatically detected & redirected to portal

2. Settings & credentials are auto-configured after user enters domain credentials

3. User automatically placed on proper SSID & network segment

SSID = EnterpriseWPA2





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**

Sample Profile Dashboard

AIRHEADS 2013

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)

Switch Unknown Network Boot Agents
Game Console Storage Device
SmartDevice Access Points Computer
Printer Routers VoIP Phone

Device Family

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

Windows Symbian Android
BlackBerry Apple Nokia

Device Name

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

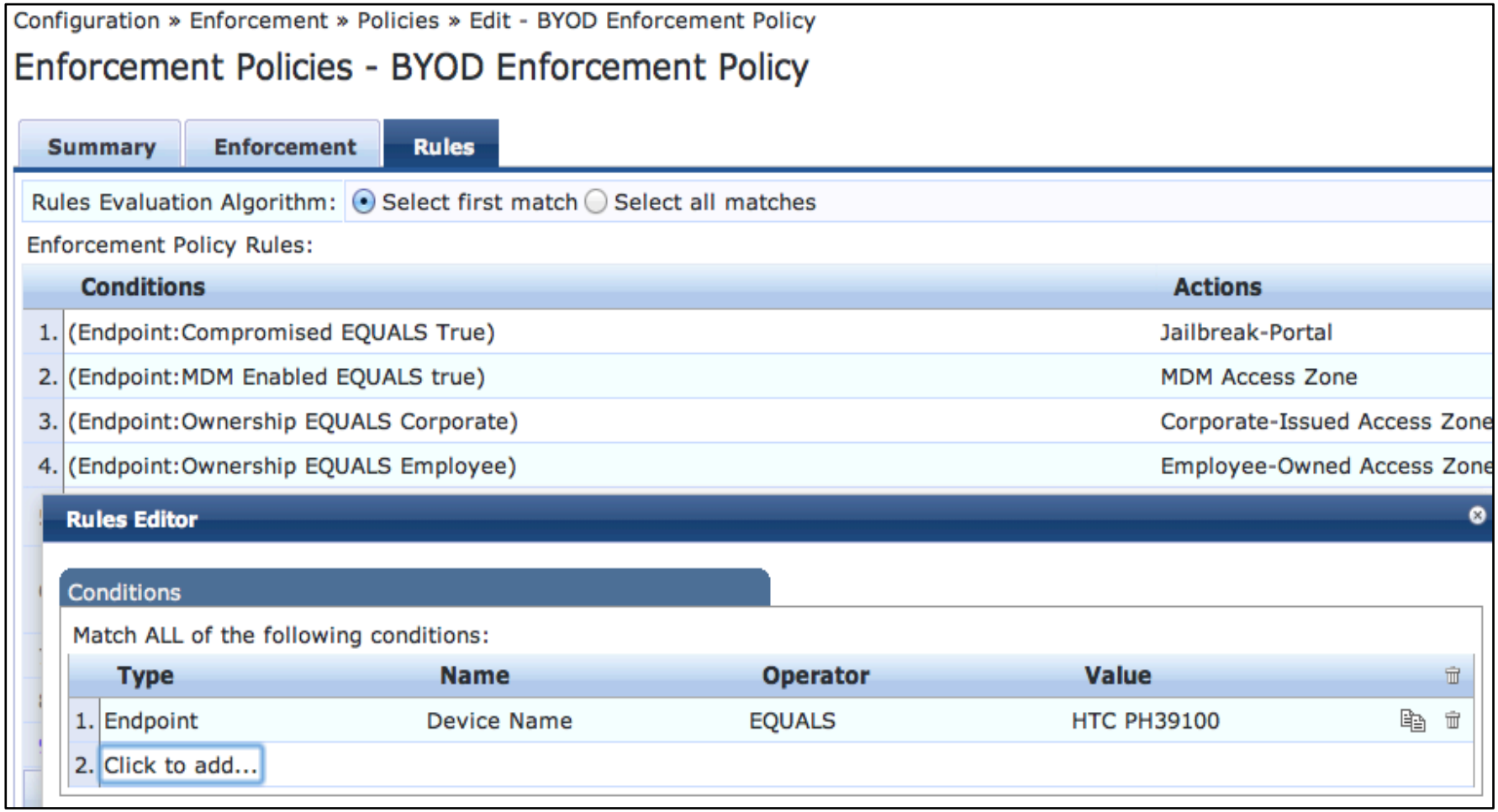
Sony Ericsson Android Samsung Android
Android HTC Android Motorola Android
AsusTek Android

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



Device Management with ClearPass

MDM Partners or Native ClearPass

AIRHEADS 2013

MDM Partners

airwatch
CITRIX
JAMF software
ZENPRISE
MaaS360 by Fiberlink
MobileIron
SOTI We Manage Mobility

Multi-Platform Support

iOS
BlackBerry
Windows Mobile
Windows Phone 8
symbian OS
Mac

★ Coming in CPPM 6.2

ClearPass with WorkSpace

iOS Only Support for Corporate Issued Devices

iOS

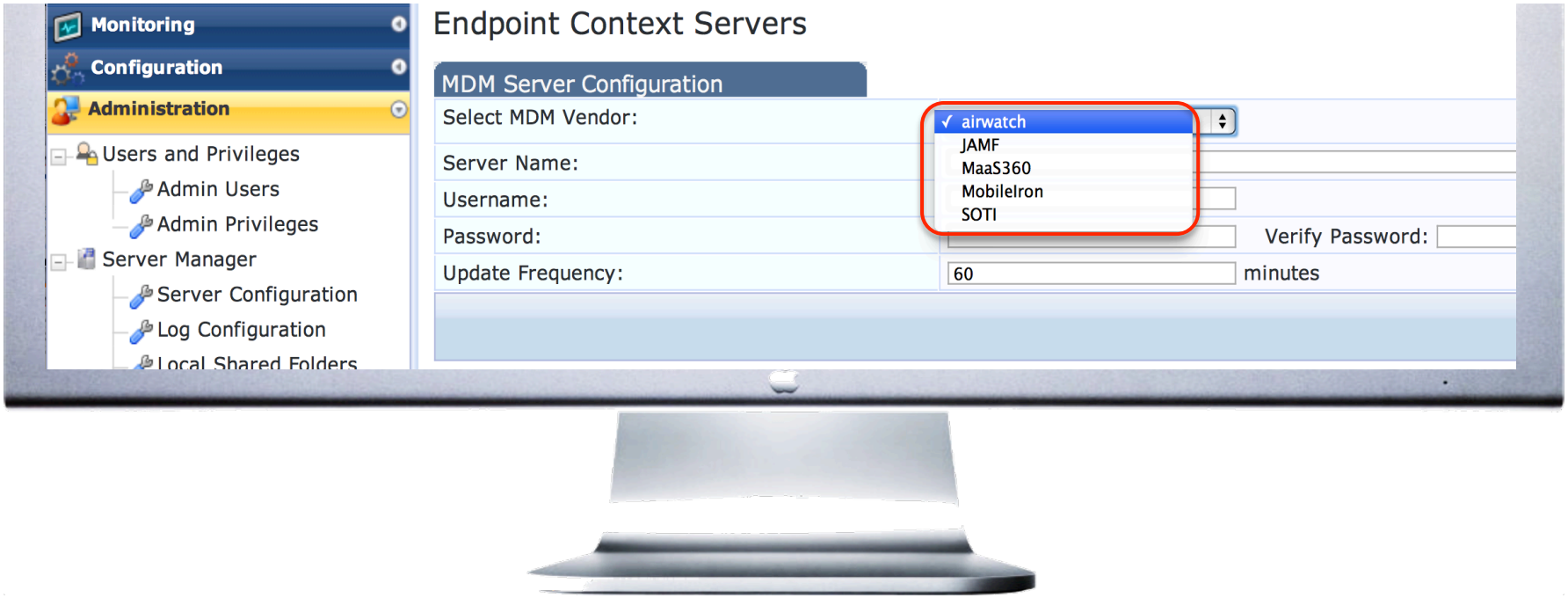
MDM Partners

Integrating Leading MDM Vendors

- **ClearPass uses public APIs for:**

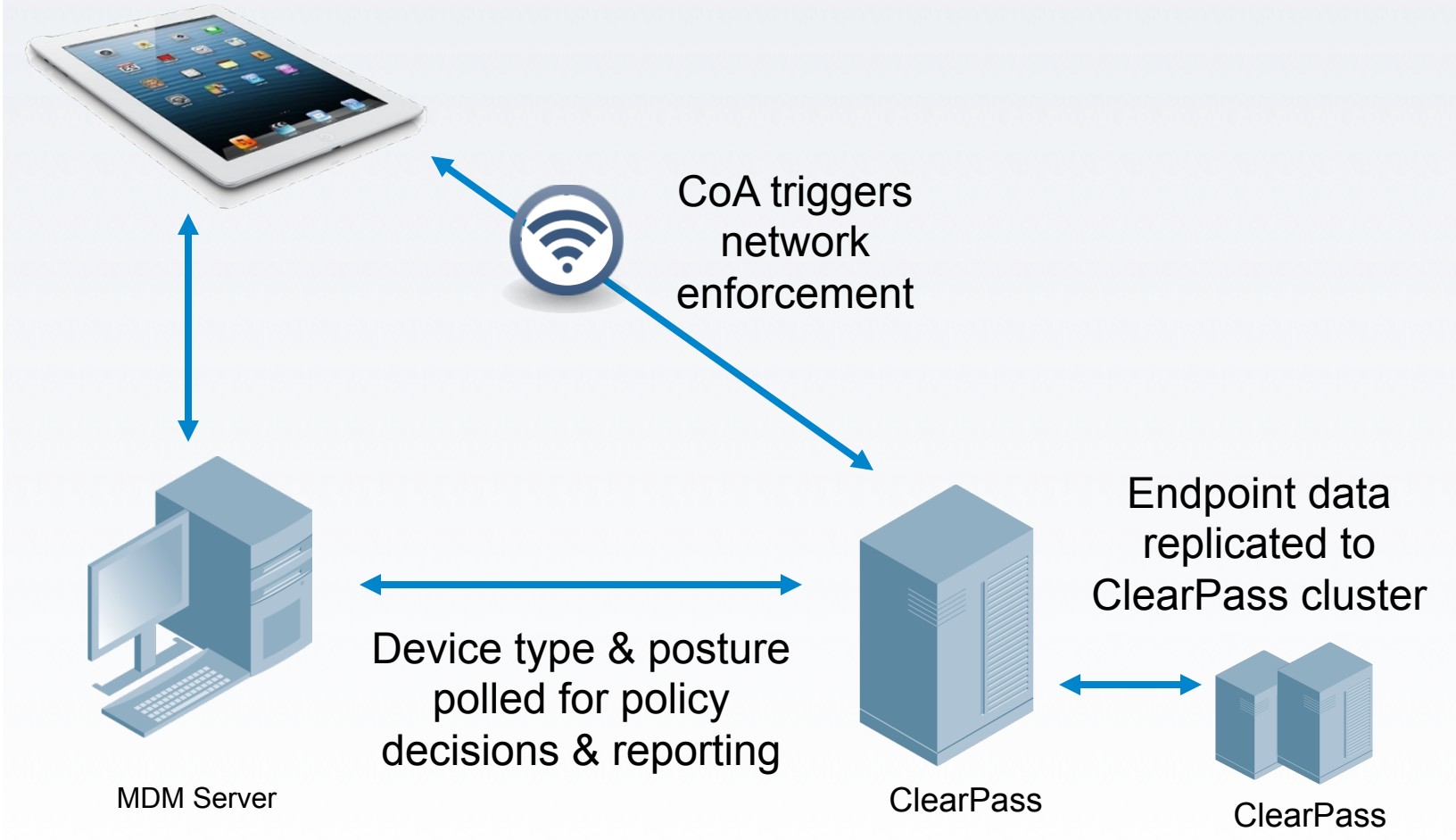
airwatch SOTI MobileIron MaaS360 by Fiberlink JAMF software

- **Normalize MDM endpoint data across vendors**



ClearPass MDM Integration

Using MDM device information for Policy



Use MDM Attributes for Network Policy

AIRHEADS 2013

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

Policy Example

Permit / Deny

Whitelist / Blacklist

Remediate

Quarantine

Redirect

Role-based Security

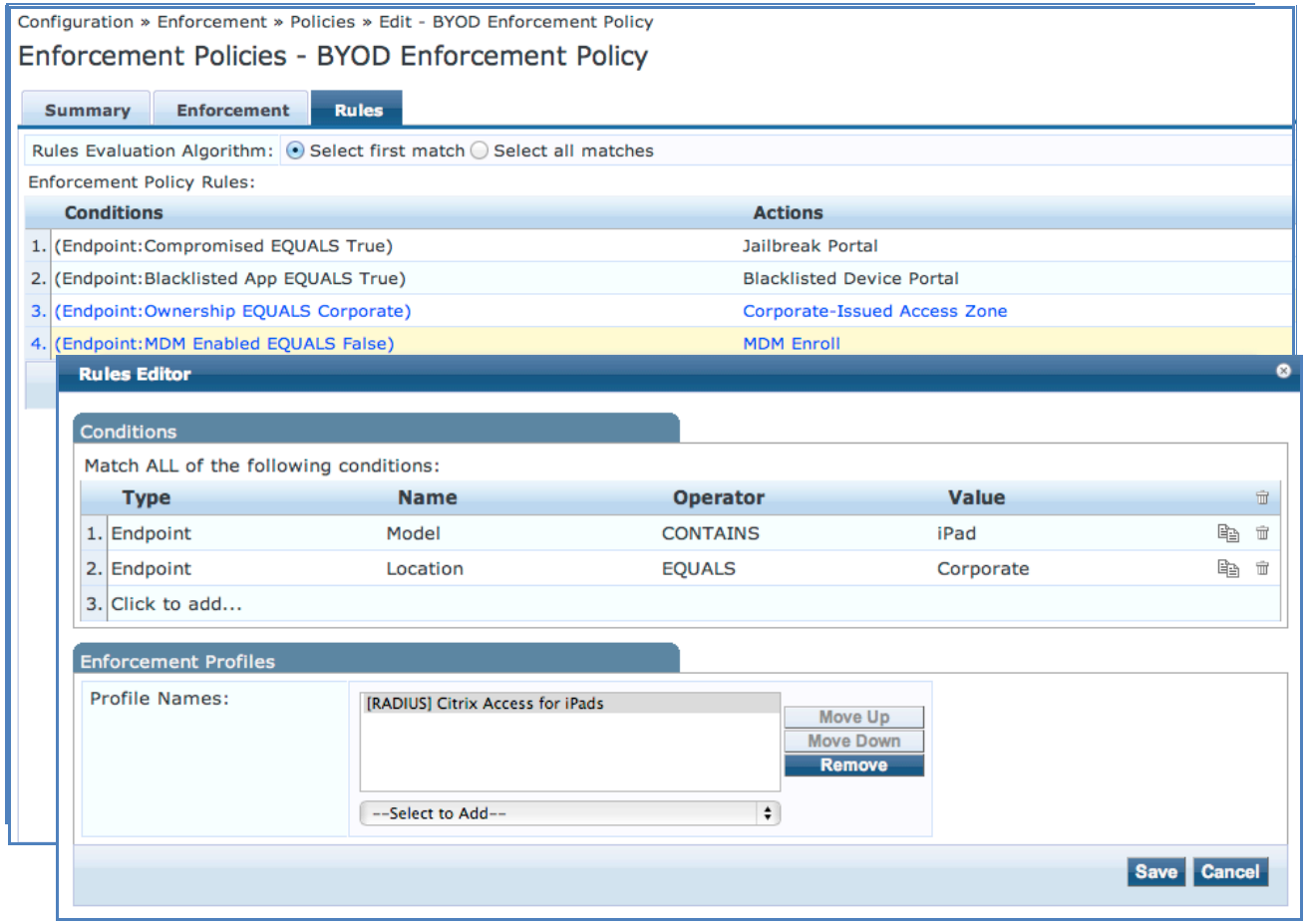
Bandwidth Mgmt

Optimize Multimedia

Use context from ClearPass + MDM to set network policy

WHO	WHAT	WHEN	WHERE	HOW
• User/group membership	• Device Profile • OS version • Endpoint health • Jailbreak status • Pincode/encryption	• Time/Date • eg. in semester	• Location • Trusted or untrusted network	• Application installed • blacklisted

Sample network policies based on MDM



- Jailbreak
- Blacklisted App
- Corporate Issued vs Employee Owned
- MDM Enabled
- iPad vs iPhone

Native ClearPass iOS MDM

Enforce iOS Device Policy with MDM

AIRHEADS 2013

Aruba WorkSpace helps organizations reduce the cost and risk of managing corporate-issued mobile devices

Monitor:

Monitor device inventory
Audit devices to ensure compliance

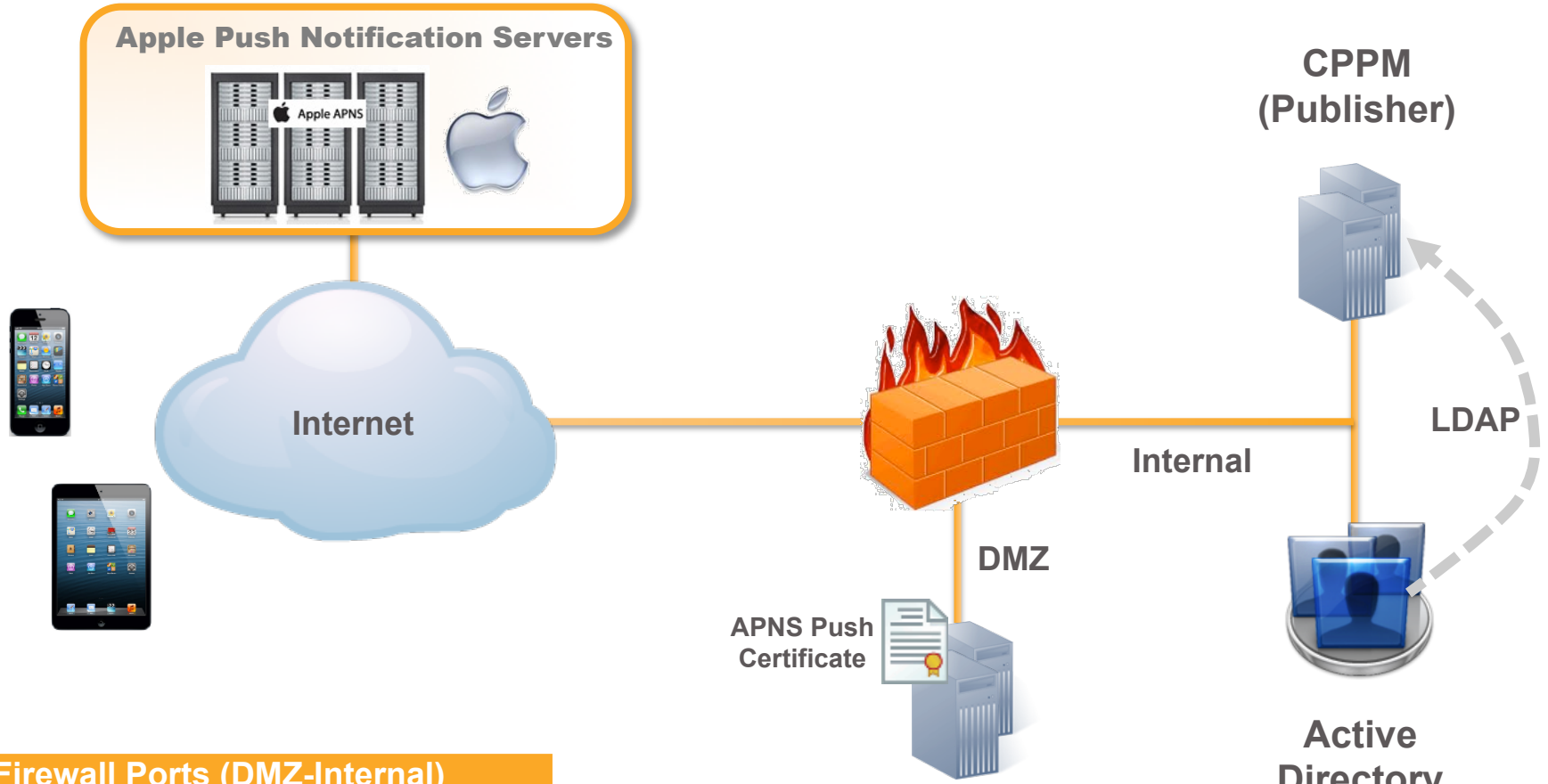
Control:

Configure security settings
Over the air remote provisioning

Protect:

Lock and wipe devices
Passcode enforcement

Enabling ClearPass for MDM



Firewall Ports (DMZ-Internal)	
Inbound	**Outbound**
HTTPS (TCP 443)	HTTPS (TCP 443)
SQL (TCP 5432)	SQL (TCP 5432)
NTP (UDP 123)	NTP (UDP 123)

Managing iOS devices over the air

AIRHEADS 2013

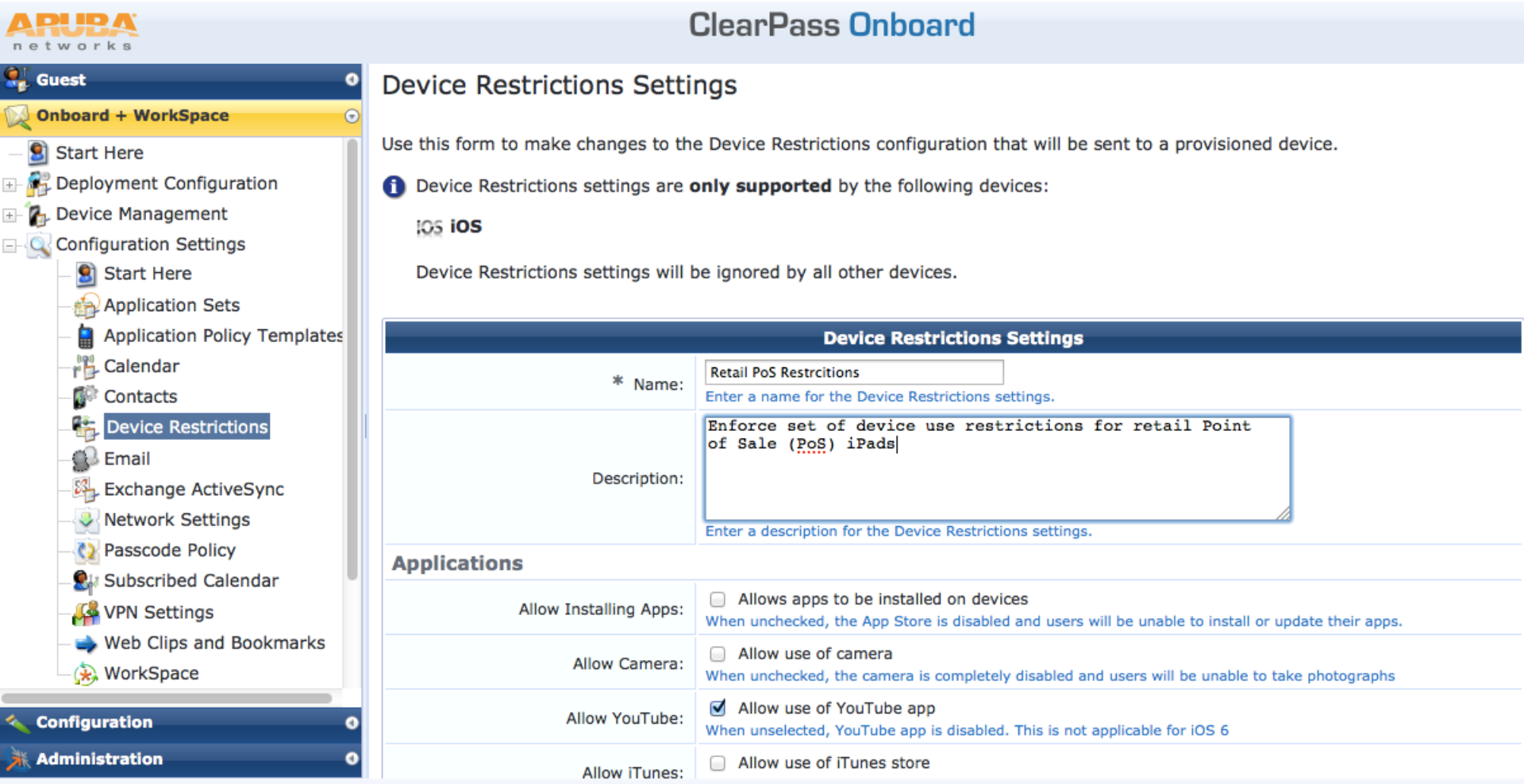
MDM Enrollment

Generate MDM Profile → OTA Enrollment → Install MDM Profile → Bind to WorkSpace Server

Execute Command / Queries ← Device connects to WorkSpace ← Send Push Notification ← Policy Change on WorkSpace

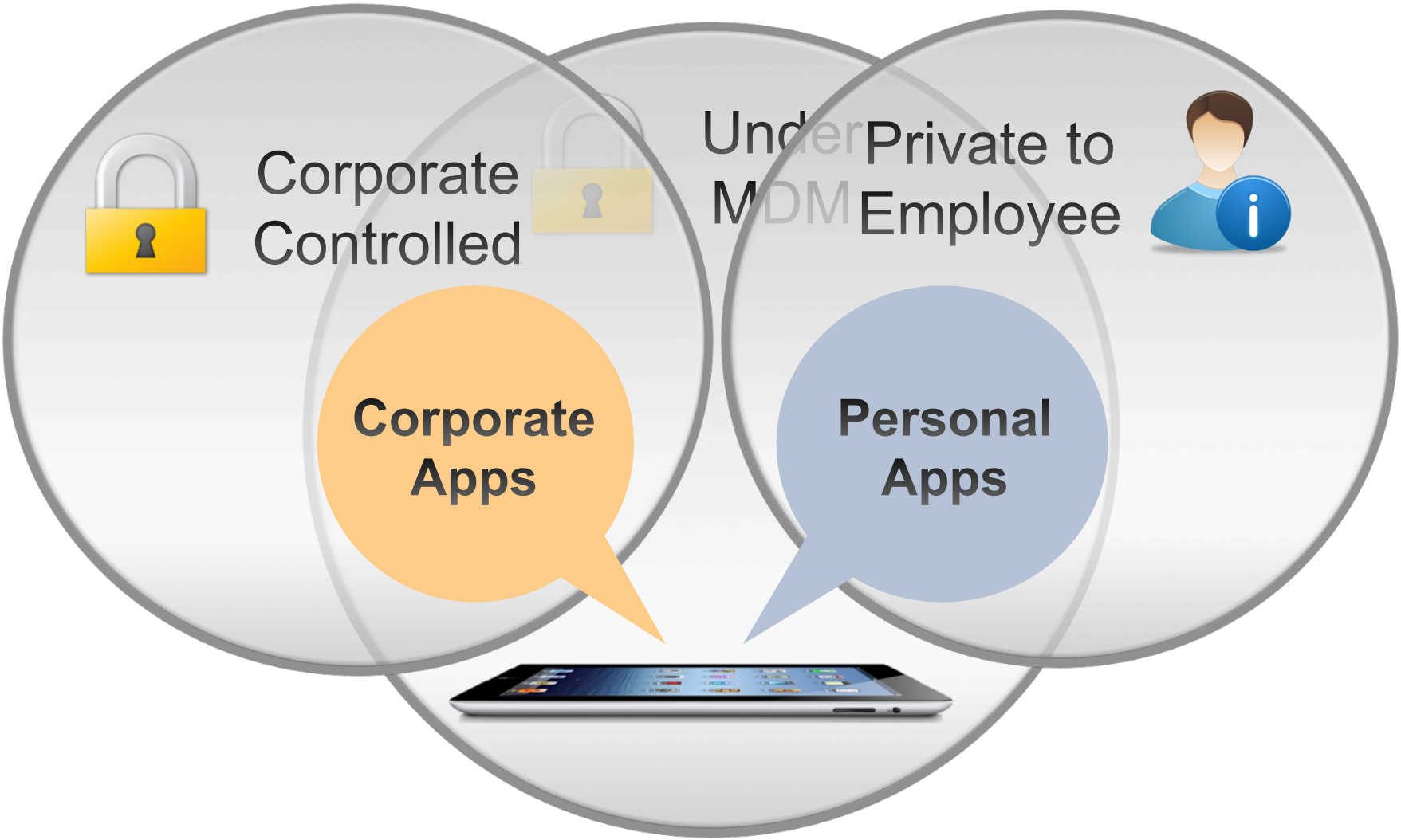
MDM Management

Example Configuration for MDM



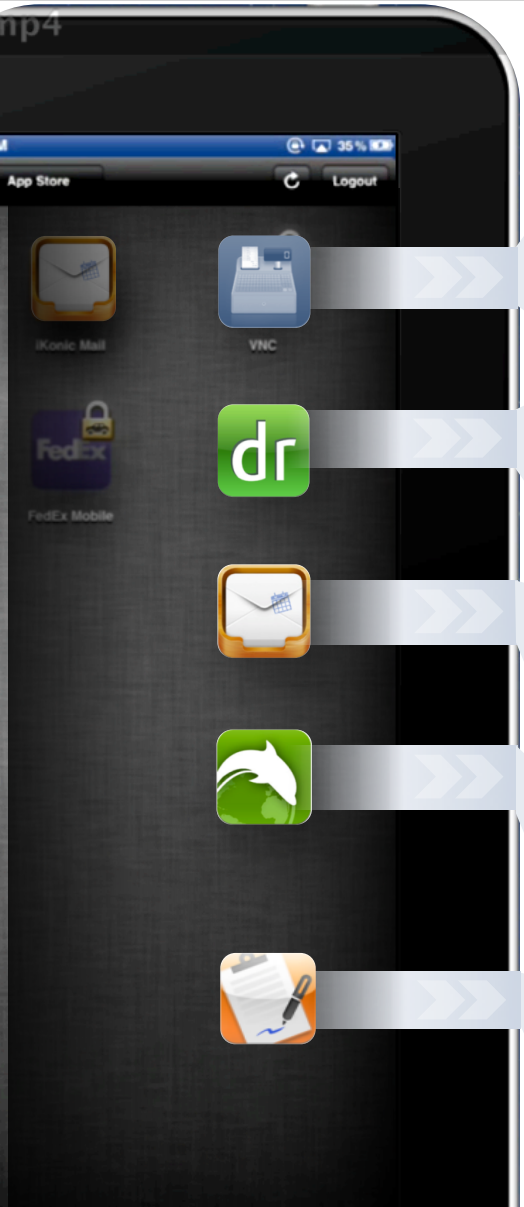
App Management with ClearPass

Separating Corporate and Personal Data



Create App Policy based on context

AIRHEADS 2013



Mobile Context

TIME-FENCING

Point of Sale App:
Must be used during store hours

GEO-FENCING

EMR Apps:
Must be used at hospital or member facilities

MOTION SENSING

Email App:
Can not be used while driving/ moving

CONTENT CONTROL

Browser App:
Can not access torrent sites

DEVICE CONTROL

Device Status:
Cut & paste restrictions, Jailbreak / Root detection, Cloud backup

One App for Employee Self-Service

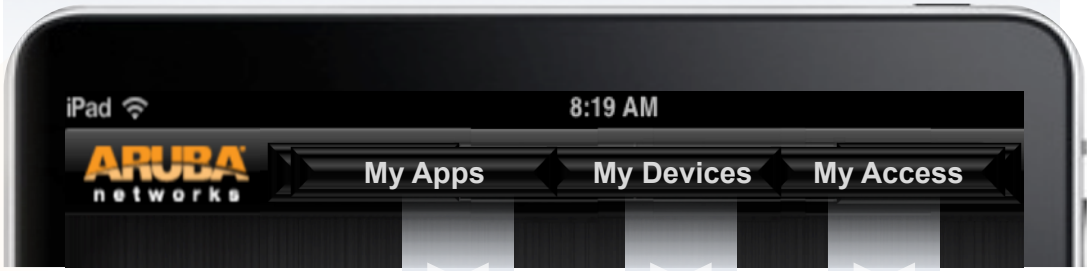
AIRHEADS 2013

Personal

- WorkSpace App provisioned to device

Corporate

- Employee self-service mobility
- Personalized portal with Single Sign-On



ClearPass with Aruba WorkSpace

First Integrated BYOD System

- **Simplify BYOD Rollout**: No need to onboard multiple vendors and integrate multiple systems
- **Faster Service Delivery**: automate BYOD provisioning across network, device and app
- **Stronger Security**: More options to control BYOD use

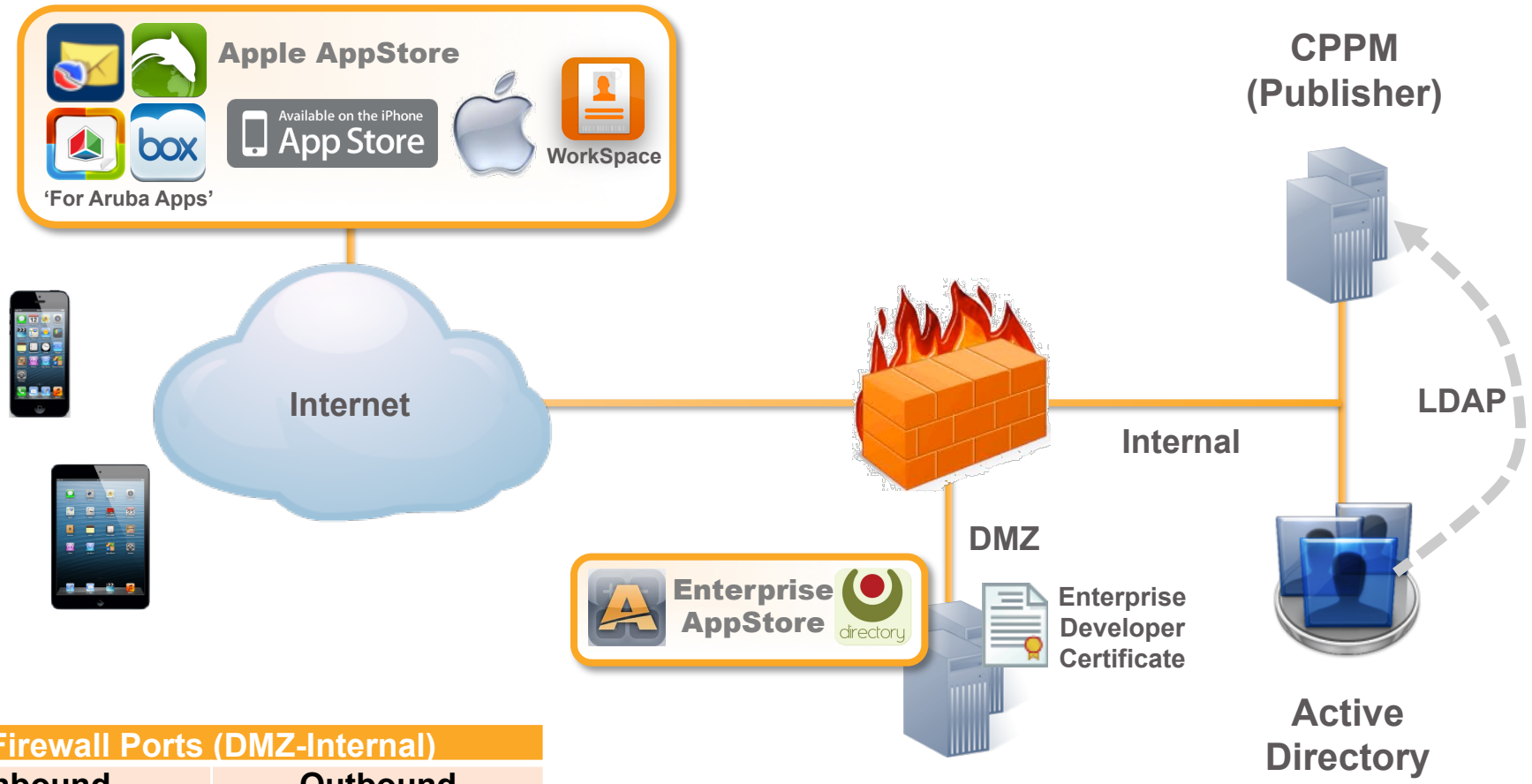
Most Comprehensive Self-Service Portal

- **Personalized BYOD**: Employees get visibility and are empowered to customize their BYOD experience

Extensive Partner Ecosystem

- **More than 40 3rd-Party ISV Apps:** Extensive list of productivity and collaboration tools

Enabling ClearPass for WorkSpace



Firewall Ports (DMZ-Internal)	
Inbound	**Outbound**
HTTPS (TCP 443)	HTTPS (TCP 443)
SQL (TCP 5432)	SQL (TCP 5432)
NTP (UDP 123)	NTP (UDP 123)

Managing App Policy over the air

AIRHEADS 2013

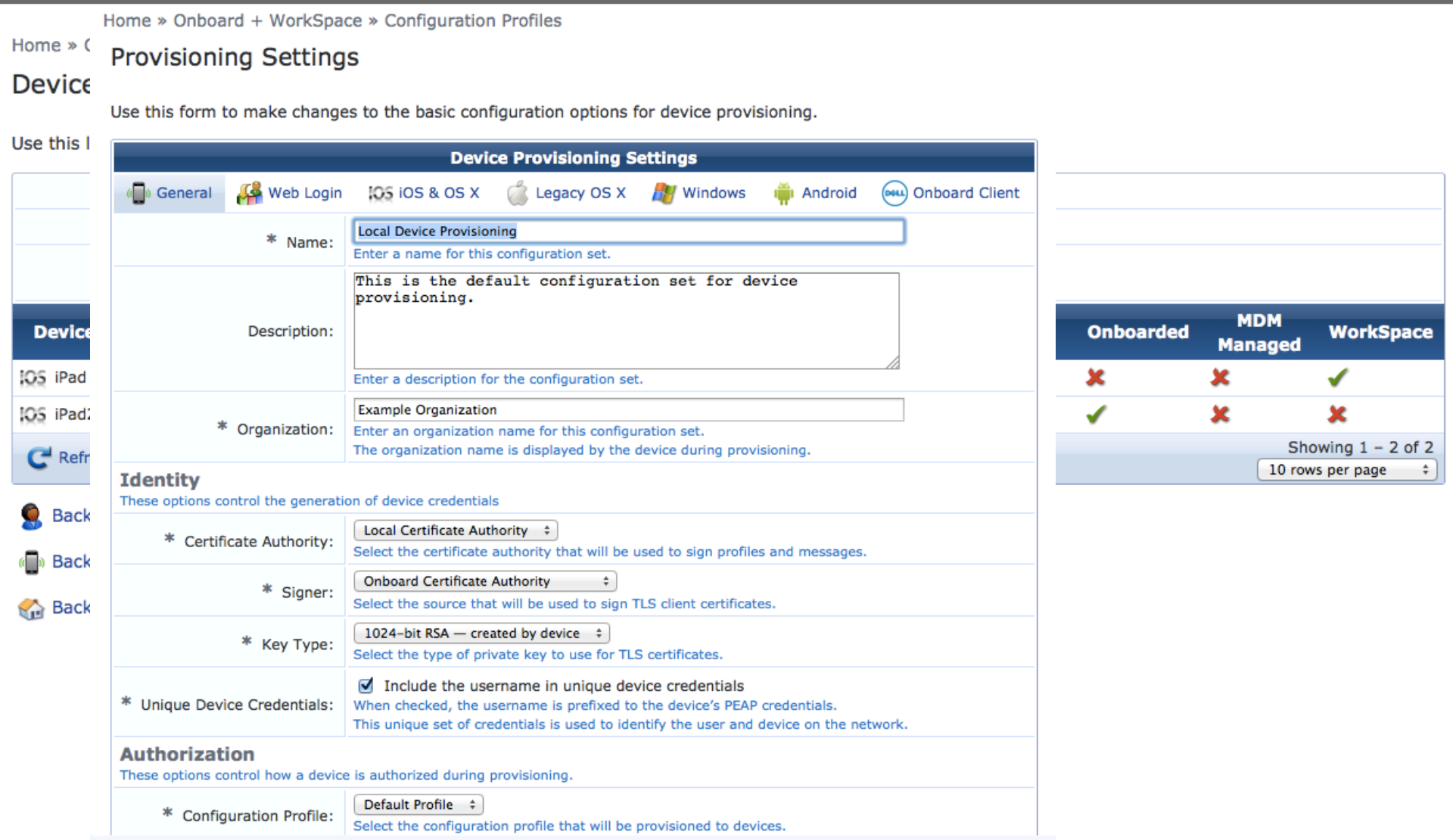
WorkSpace Enrollment

OTA Enrollment → Trigger WorkSpace App Install → Authenticate User & Provision App → Install Policy Managed Apps

Execute Policy / Update App ← Device connects to WorkSpace ← WorkSpace or App Launch ← Policy Change on WorkSpace

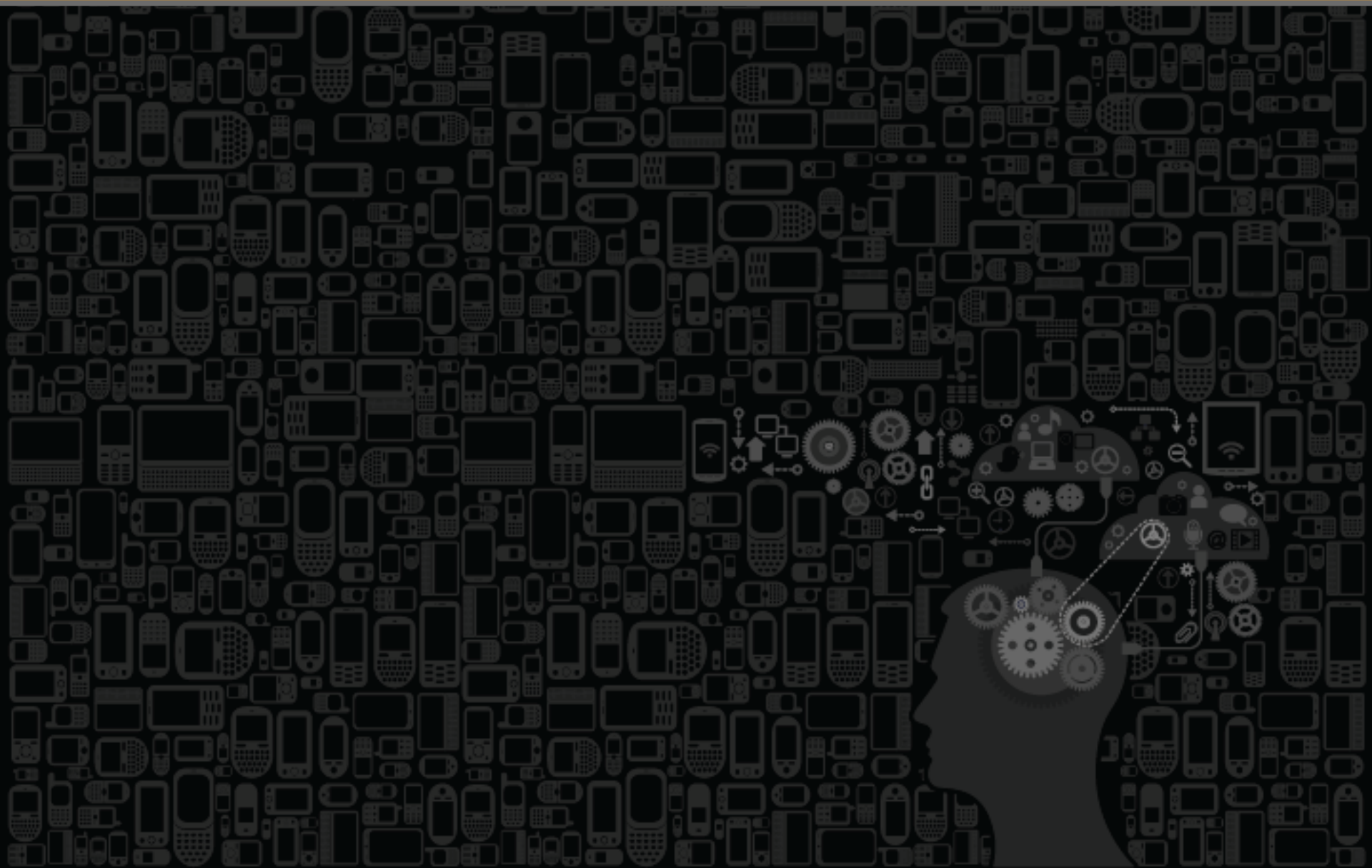
App Policy Management

Example configuration for WorkSpace



Q&A

AIRHEADS 2013



AIRHEADS
ALICANTE 2013

JOIN: community.arubanetworks.com

FOLLOW: @arubanetworks

DISCUSS: #airheadsconf

Thank You