DEPLOYING BYOD:
ONBOARDING, PROVISIONING, POLICY, REPORTING
The BYOD Challenges

Requirement: Securely Onboard Mobile Devices

Corporate Liable

- Trusted
  - Company-owned
  - Fully managed
  - Fully controlled

Employee Liable

- Tolerated
  - Company or Employee owned
  - Limited visibility
  - Limited control

How do I:
- Maintain visibility & control?
- Deliver secure, differentiated access?
- Simplify device provisioning?
Is your Network ready for BYOD?

- **The buzz is uncontrollable**
  - Any device, any user, any time

- **What have we learnt from the originators of BYOD…?**

- **Education has been doing BYOD for years**
  - Lots of diverse devices to manage = lots of helpdesk calls
  - Securing the network and the application is key
  - Expand cloud applications or VDI

- **So from a security perspective**
  - BYOD is driving the need for a more intelligent access control network
Join the BYOD Domain

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
BYOD Building Blocks
Foundation Technologies for BYOD

- **Device Profiling**
  - Accurately determine device, force enrollment or deny access

- **Enrollment and Provisioning Workflow**
  - Clean user self managed onboarding process, no IT involvement

- **Context Aware Policy Definition Point (PDP)**
  - Implement business policy for BYOD access, multi-contextual

- **Granular Policy Enforcement at the Access Layer**
  - Stateful firewalling, Application Aware, Bandwidth Constraints

- **BYOD lifecycle management**
  - Device inventory, revoke network access, more to come . . .
User and Device Policy Example

1. All devices auto profiled
2. Device information mapped to classification for policy and proper access
3. Granular access based on device type and identity

Example: Executive level user connects to network with iPad 2, and ClearPass Profile matches device to category, family and type to apply full access policy
Enrollment & Provisioning Workflow

1. Authorize BYOD enrollment based on AD credentials
2. Register device type & ownership
3. Provision a unique device credential for that user & device
4. Revoke access for devices that are lost or stolen
Onboard Provisioning

Wi-Fi Network Settings » Windows Network Settings

Windows Networking Settings
These settings are only applicable to Windows devices.

- NAP Services: [ ] Enable NAP services
- Admin Username: Enter if configuration of networking requires administrator credentials.
- Admin Password: Enter if configuration of networking requires administrator credentials.
- IP Address: [ ] Assign IP address using DHCP
- DNS: [ ] Assign DNS using DHCP
- DNS Registration: [ ] Register IP address with DNS

Windows XP Networking

- Configure Using: [ ] Use Windows to configure wireless
- Notification Icon: [ ] Show icon in notification
- Notify Connectivity: [ ] Notify when connectivity is limited

Network Access
Options for basic network access.

- * SSID:
- Wireless:
- Auto Join:
- * Security Type:
- * Security Version:

Enterprise Protocols
Options for 802.1x protocols supported on the wireless network.

- IOS & OS X EAP:
  - Accepted EAP Types:
    - [ ] TLS
    - [ ] PEAP
    - [ ] TTLS
    - [ ] EAP-Fast
- Legacy OS X EAP:
  - PEAP with MSCHAPv2: The authentication protocol to use with OS X 10.5/6 (Leopard/Snow Leopard)
- Android EAP:
  - PEAP with MSCHAPv2: The authentication protocol that will be used for Android devices
- Windows EAP:
  - PEAP with MSCHAPv2: The authentication protocol that will be used for Windows devices
- Fast Reconnect: [ ] Enable Fast Reconnect
- Quarantine: [ ] Enable Quaranlime checks
- Cryptobinding: [ ] Enforce Cybnto binding

#airheadsconf
1. Device type is auto detected and user prompted to commence workflow

2. Settings and credentials are auto configured on device

3. User is automatically placed on secure SSID or network segment upon completion of onboarding
Context Aware Policy Definition Point

Policy

User

Device

Location

Application

Employees
Contractors
Guests
Students
Faculty

Personal

Corporate

Device Type

Health

VPN

Cloud

HQ
Branch
Home
Remote

Media

Time of day

Virtual Desktop

Video

Voice
Intuitive Policy Definition

- Service
- Authentication
- Authorization
- Roles
- Posture
- Audit
- Enforcement
Granular Policy Enforcement at the Access Layer

Policy Enforcement Firewall (PEF)

- Identify the Connection
- Classify the Traffic
- Control Access per Packet
- Optimize the Air
- Follow the User

Instant AP
Mobility Access Switch
Mobility Controller
Enforce on any Network!

POLICY DECISION

ClearPass Policy Manager

POLICY ENFORCEMENT:

Any Network

Permit | Deny | Whitelist | Blacklist | Redirect | NAT | Bandwidth Mgmt | Optimize Multimedia

Policy Enforcement Optimized for Mobility

#airheadsconf
BYOD lifecycle management

- Revoke Device Network Access
- Realtime Dashboard of BYOD Access
- Device Inventory Data
- Enforcement of BYOD Access Policies
Distributed Architecture

- Centralized/Distributed Administrative Domains
- Redundancy/Load Balancing
- Cluster wide licenses
5 Tips for BYOD

• Define your BYOD Access Policy
  – Limited Access Zone, Which devices, Bandwidth Contracts

• Device Aware Access Network
  – Device Profiling, ability to force enrollment workflow

• Granular Policy Definition & Enforcement
  – Centralized policy creation, role based enforcement

• User Managed Onboarding Process
  – Avoid Help Desk load, install trusted certs, profile device details

• Method to Revoke Device Access Critical
  – Unique device credential, lost device or employee leaves
Thank You