AIRWATCH AND ARUBA CLEARPASS WORKING TOGETHER

Network security is now more relevant for mobile devices

- For strong network policy enforcement, AirWatch shares contextual information about devices with ClearPass.
- Jailbreak/root-kit detection – Unhealthy devices detected by AirWatch are denied access or quarantined by ClearPass.
- ClearPass posture assessments for missing EMM agents or denylisted apps can trigger appropriate access enforcement, remediation and notifications.

Easily tie mobile security enforcement to the rest of your business

- Create business-relevant network rules – location and denylisted apps can trigger relevant security actions on mobile devices and change network privileges accordingly.
- Invoke critical non-network device actions – ClearPass Exchange APIs let IT automate and improve common business workflows such as IT helpdesk ticketing and device notifications.

Streamlined certificate enrollment with integrated network policy enforcement

- Built-in ClearPass certificate authority eliminates login and passwords on mobile devices for improved security and user experience.
**FREQUENTLY ASKED QUESTIONS**

Q: Why should I allow mobile devices to connect to Wi-Fi?  
• Superior indoor coverage, speed and app security.  
• Cost avoidance: Data overage and roaming charges.

Q: Why ClearPass for enterprise Wi-Fi connectivity?  
• Network access enforcement that builds on AirWatch’s device and app policies.  
• Policies based on user role, device and location attributes.

Q: How does AirWatch/ClearPass integration differ from competing solutions?  
• A major difference lies in the ability to trigger customer-defined policies that broaden enforcement and notification capabilities. Other NAC solutions only enforce policies at the network layer.  
• ClearPass offers a fully integrated certificate authority for 802.1X certificate provisioning, management and revocation.

**END-TO-END ACCESS AND NOTIFICATION WORKFLOW WITH AIRWATCH**

1. **Jail-Broken Device Detected**  
2. **Helpdesk Ticket Auto Generated**  
3. **Message to Device Auto Generated**