SOLUTION OVERVIEW

MANAGING SMART DEVICES FOR SECURE ENTERPRISE MOBILITY

MobileIron and Aruba ClearPass Integration

INTRODUCTION

In today's mobility-centric environment – where smartphones and tablets are a common fixture at work, home and at social events – it's inevitable that they will contain a combination of personal and enterprise data.

Infrastructure-wide policies that automate how mobile devices can be configured, remotely managed and then used on wireless and wired networks are now a best practice for any enterprise IT organization.

Aruba Networks® and MobileIron work together to manage device and network policies that protect enterprise data and network resources. Enterprises with IT-managed and BYOD initiatives can ensure that work apps and data are protected across cellular and Wi-Fi networks.

- MobileIron mobile device management (MDM)
- The Aruba ClearPass network access management platform

Because these mobile devices are used everywhere, it is also important to ensure that network policies are in place for smartphones and tablets that are lost or stolen. In the past, losing a wallet was the beginning of a long day.

Personal data was inevitably there for anyone to see and use until phone calls were made to cancel accounts. Today, a lost or stolen device can mean a long day for the user, the IT team, and depending on how the organization, even a public relations department.

MANAGING DEVICE, DOC AND APP SECURITY

MobileIron provides end-to-end security and management for apps, docs and devices as a foundation of implementing a mobile strategy. As a result, IT can setup a virtual mobile perimeter that enables device security and business data and app protection, while still delivering an excellent user experience, even on employee-owned smartphones and tablets.

A broad level of support for mobile operating systems gives users the ability to choose their own device type. MobileIron's commitment to a multi-OS environment means users get what they want (whether enterprise or employee-owned), and IT gets what it needs (features that protect enterprise data, regardless of device type).

WHERE MOBILEIRON HELPS

- Privacy policy and selective wipe to secure corporate data while protecting personal data.
- Sophisticated posture monitoring and automated policy workflow.
- Self-service enterprise app store for employees.
- Secure network access and plan management for cellular.

SECURE NETWORK ACCESS POLICIES

Aruba ClearPass provides ultra-scalable network access security using built-in policy management and AAA for mobile environments. IT can leverage a user's role, device type, location, time-of-day and other attributes to execute custom policies for enterprise-wide wireless, wired and VPN access.

Complete views of all users and devices give IT total control over what internal resources can be accessed and when. To improve the end-user experience, ClearPass delivers a wide range of unique self-service capabilities that let users securely onboard their own devices, sponsor guest Wi-Fi access and setup sharing of Apple TV and Google Chromecast.

WHERE ARUBA HELPS

- Network policy and authentication services for secure Wi-Fi access.
- Automated device onboarding and guest self-service portals.
- Comprehensive network-wide profiling, device visibility and reporting.
- Support for multivendor network environments.

MDM AND NETWORK POLICY INTEGRATION

For IT organizations that wish to take advantage of MDM controls and network access security for mobile deployments, it's as simple as leveraging the Aruba ClearPass Exchange API and MDM Connector.

Whether IT-issued or BYOD, ClearPass can pull a normalized set of data tags from MobileIron to create an extensive table of endpoints. These data tags can then be referenced within policies to enforce various business rules using a device's state information.

Examples of MDM-derived attributes that can be pulled into the ClearPass endpoint database are shown below.

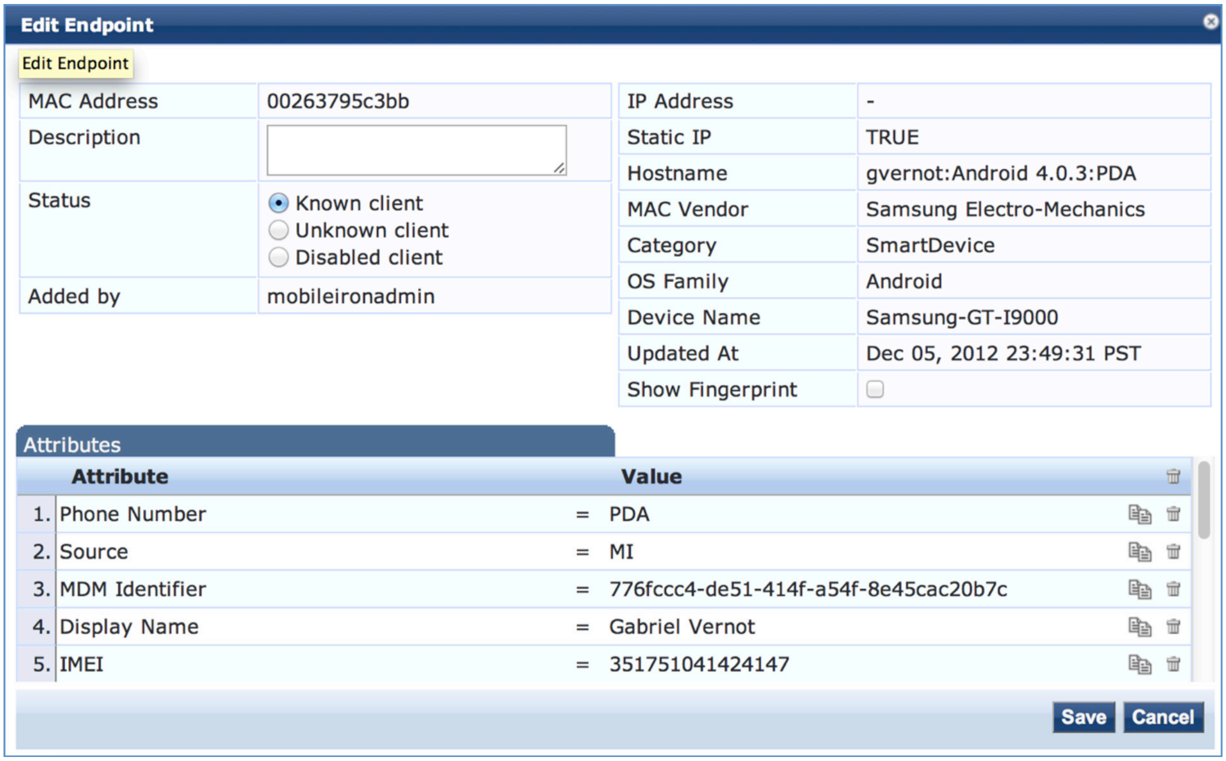
MOBILEIRON AND ARUBA WORKING TOGETHER

Jailbreak status – A common use case is to leverage the presence of the MDM agent to detect if a device has been jailbroken (Apple iOS) or a root-kit installed (Android). ClearPass lets IT create a policy that automates how these compromised devices are handled when users try to connect to the enterprise network. Access can be denied or limited.

Blacklisted apps – To strengthen compliance policies, blacklisted apps can be defined and checked via MobileIron. ClearPass knows when MobileIron detects blacklisted apps and redirects users to a remediation portal, where the policy breach is explained. Optionally, network access can be restricted to the Internet, for example.

MDM agent removed – Sometimes users will deliberately or accidentally remove an MDM agent or profile from their devices. This severs device management and prevents MobileIron from enforcing policies. Fortunately, ClearPass knows when a device is not under management and redirects it through the provisioning process.

The above examples represent only a small number of possible scenarios in which IT organizations can utilize MDM and network access security to ensure that mobile device policies are enforced across cellular and wireless networks.



Edit Endpoint

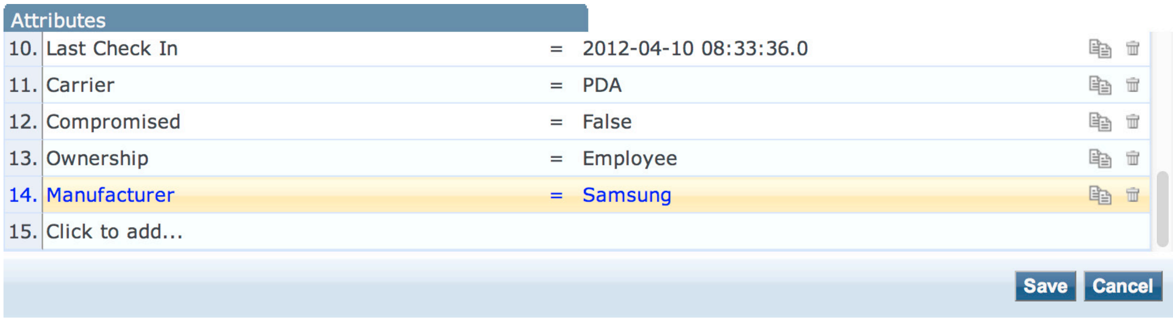
Edit Endpoint

MAC Address	00263795c3bb
Description	
Status	● Known client ○ Unknown client ○ Disabled client
Added by	mobileironadmin

IP Address	-
Static IP	TRUE
Hostname	gvernot:Android 4.0.3:PDA
MAC Vendor	Samsung Electro-Mechanics
Category	SmartDevice
OS Family	Android
Device Name	Samsung-GT-I9000
Updated At	Dec 05, 2012 23:49:31 PST
Show Fingerprint	□

Attributes

	Attribute		Value
1.	Phone Number	=	PDA
2.	Source	=	MI
3.	MDM Identifier	=	776fccc4-de51-414f-a54f-8e45cac20b7c
4.	Display Name	=	Gabriel Vernot
5.	IMEI	=	351751041424147



	Attributes		
10.	Last Check In	=	2012-04-10 08:33:36.0
11.	Carrier	=	PDA
12.	Compromised	=	False
13.	Ownership	=	Employee
14.	Manufacturer	=	Samsung
15.	Click to add...		

ENHANCED INTEGRATION CAPABILITIES

Using two-way interaction, MobileIron uses network events to prompt ClearPass Exchange into action regarding devices under MDM control. If a policy is violated, a notification is automatically sent to the user explaining why the device was quarantined.

When certificates are distributed for authentication, ClearPass acts as a certificate authority to ensure that each device contains a unique certificate that includes device information and user data, not just data about the organization for which the certificate was issued.

SUMMARY

Together, Aruba and MobileIron provide enterprises with policy management that does it all – a complete solution for mobile device and network access security, from optimized policies to complete AAA services for any BYOD or IT-managed deployment.

IT organizations can now maintain real-time data about users, device attributes and status, application use, and location. This gives IT unrivaled network visibility, workflow automation, and security for personal and corporate-owned mobile devices.

Document developed in collaboration with MobileIron

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com