ARUBA networks

ClearPass: Understanding BYOD and today's evolving network access security requirements

ClearPass: Understanding BYOD and today's evolving network access security requirements

Chapter 1:

ARUBA networks

Introduction

You were asked to find a solution that would help your organization deploy a secure and effective way for employees, partners, and guests to use their personal devices on your wireless and wired networks. The solution needs to support laptops, smartphones and tablets, plus offer the flexibility to differentiate access by user role or device type. All of this without increasing ITs workload or cost.

After doing some research, you found Aruba's ClearPass Access Management solution, you read the datasheets, whitepaper, and even attended a webinar, but now you need more detail.

- If I already have a Wi-Fi infrastructure in-place that's not Aruba, will it still work?
- How does ClearPass Onboard support iPhones and Windows devices?
- Can I differentiate access by device type or ownership (Corporate vs. BYOD)?
- Where do MDM solutions play a part?

This chapter is intended to provide additional information about Aruba's ClearPass solution that goes beyond what is available in the datasheets. You'll learn how the ClearPass solution fits together, how device and user information can be used within policies to support BYOD and security compliance initiatives, and how you can implement ClearPass to solve an initial network access requirement as well as leverage additional solution capabilities as requirements grow.

The following diagram highlights the ability to deploy ClearPass within a DMZ for guest access and later add to the solution to solve employee BYOD onboarding needs, secure differentiated access of users and devices, and automatically profile all connected devices for visibility, troubleshooting, and wireless and wired infrastructure planning.

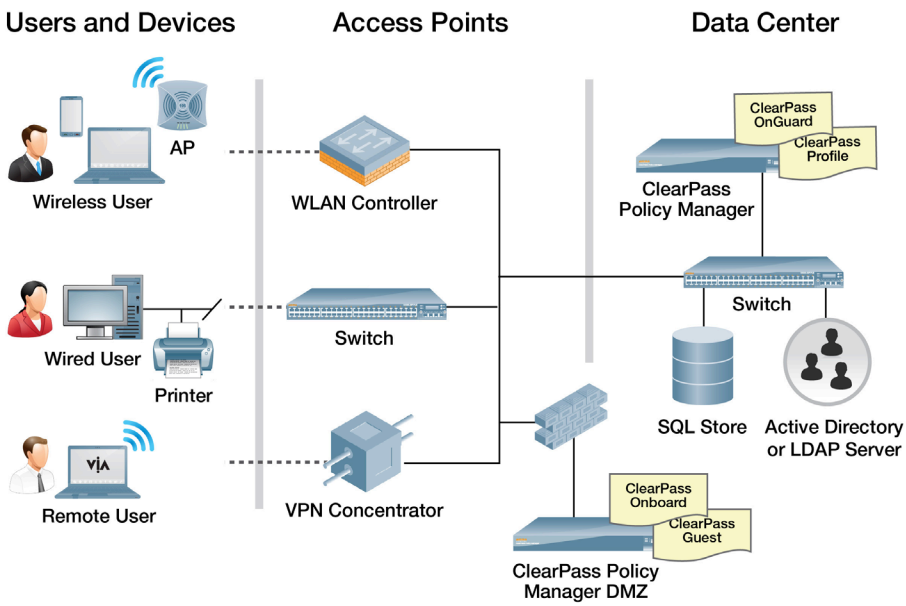

Figure 1: ClearPass Access Management System

Subsequent chapters will dive into each module in greater detail and will include examples and screenshots of how a policy is created, how an iPhone and Android device can be differentiated when onboarded, what you'll see when profiling devices, how posture checks on computers can be used to ensure a certain level of compliance, and how easy it is to implement guest access additional guest services.

Understanding Aruba ClearPass

Today's overwhelming demand for end-users to connect their IT issued as well as personally owned devices has led many IT organizations to adopt less secure policies or just saying no to BYOD. Both of which provide challenges that can lead to users implementing creative and unwanted workarounds as well as a loss of network control.

Aruba's ClearPass solution takes into consideration security, compliance, and IT workflow demands created when supporting BYOD and differentiated access. At the core of the ClearPass solution is the ClearPass Policy Manager which delivers policy enforcement and enterprise-class AAA features, while the following options solve onboarding, posture, and guest access challenges:

- ClearPass Onboard
- ClearPass OnGuard
- ClearPass Guest

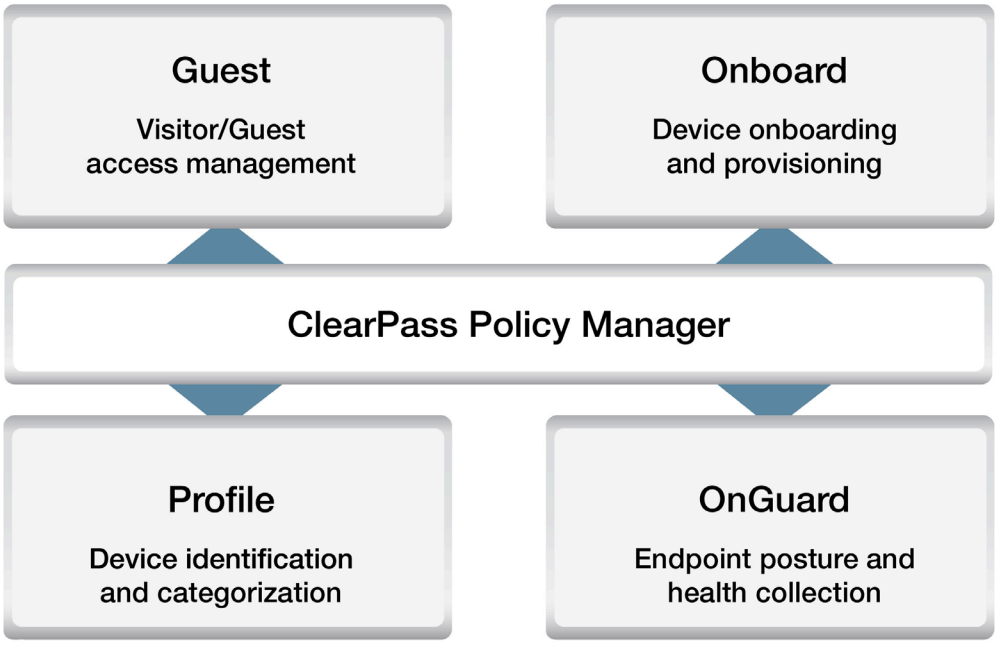

Figure 2: ClearPass Policy Manager and optional capabilities

ClearPass Policy Manager

The Policy Manager is a policy management engine, with full AAA functionality that includes RADIUS, device profiling, TACACS+, advanced reporting, and a comprehensive set of deployment and management tools. Policies can be created that differentiate users, corporate devices from BYOD, time-of-day and location attributes, and more.

While the use of Aruba controllers and switches provide the advantage of supporting per user role- based access, the Policy Manager has been designed to support multivendor environments that include Aruba, HP, Cisco, Juniper and more. VLAN and ACL enforcement is supported for any non-Aruba network access devices.

The following sections cover basic Policy Manager functionality:

- Policy management features
- AAA
- Device profiling
- AirPlay/AirPrint
- Reporting
- Appliance sizing
- Scalability

Policy management features

The Policy Manager provides a template based model to create and centrally manage user and device oriented wireless, wired, MAC authentication, web-based authentication, and network device administrator services from a single platform.

This provides the ability to leverage existing infrastructure while also providing the flexibility to support mixed 802.1X and non-802.1X authentication scenarios.

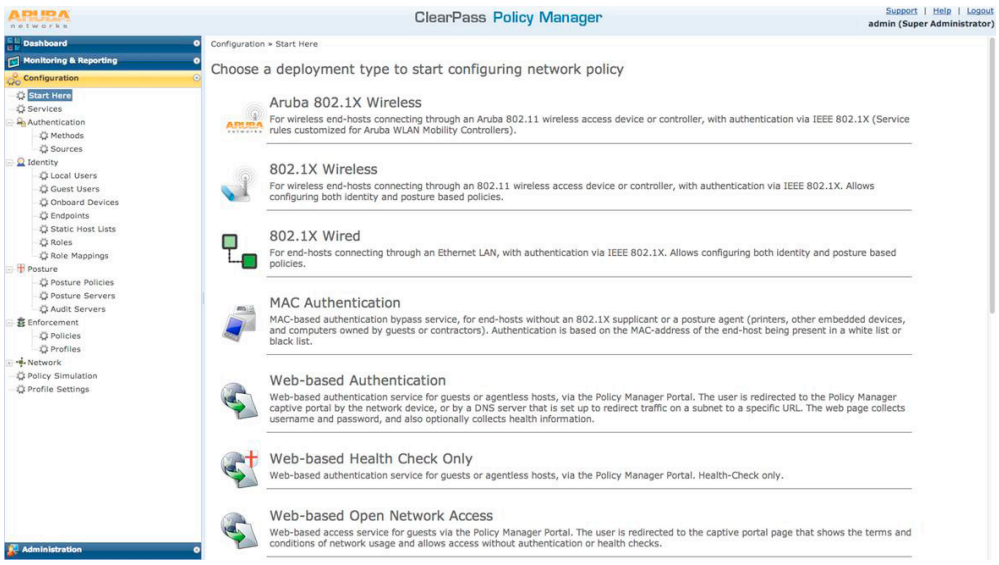

Figure 3: ClearPass and optional modules

Each service pre-populates associated RADIUS or TACACS+ attributes, and subsequently guides the administrator through a series of setup screens that assist in configuring the following service components:

- Authentication and Authorization sources
- User and device roles
- Computer posture/health rules and checks
- Enforcement policies
- Audit rules
- Profiler actions

A majority of the components or building blocks within a service can then be re-used when creating additional services. For example, the roles that were created for a wireless service can be re-used within a wired service to maximize time-savings and efficiency.

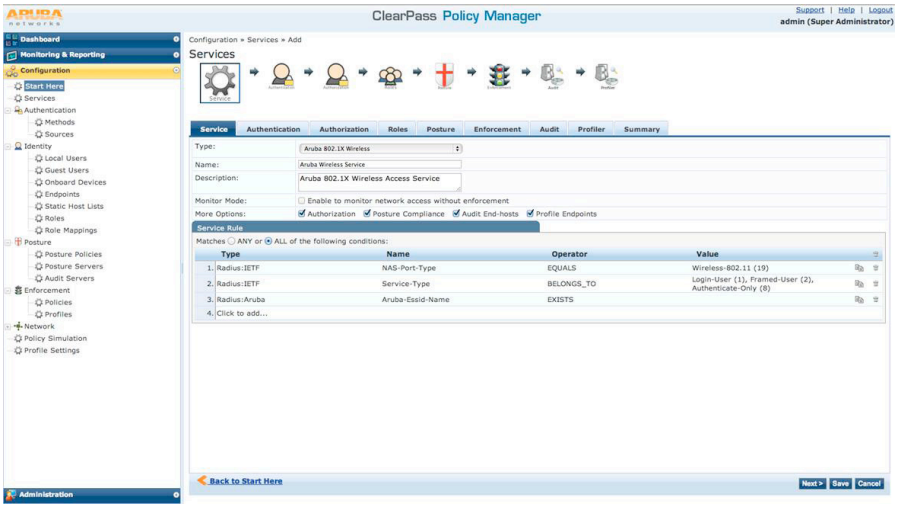

Figure 4: ClearPass and optional modules

The ClearPass Policy Manager includes an open API architecture that allows 3rd party solutions to populate the endpoints database with contextual information about the device. One example of this is MDM integration. For customers that have already deployed MDM for addressing corporate-issued mobile devices, ClearPass provides an MDM gateway that uses existing inbound API's from leading MDM solutions, and appends this data to the ClearPass endpoints table. This allows customers to set policies based on information gained from MDM agents such as the jailbroken status of a device.

AAA features

Enterprise-class RADIUS and TACACS+ services ensure full support for multiple user and device-based authentication use cases that include 802.1X as well non.1X authentication and authorization methods. Standards based RADIUS support for over 130 vendor specific attributes (VSAs) allow organizations to leverage a wide variety of legacy or planned wireless, wired, and VPN devices.

Supported EAP types include PEAP, FAST, TLS, TTLS, MSCHAPv2, and MD5. PAP and CHAP authentication is also available.

The use of AD, LDAP, SQL databases, token servers, and internal stores in the Policy Manager can be used as authentication sources. The Policy Manager also allows for the ability to join a single or multiple domains for situations where two organizations or groups have merged. Using a separate authorization method than what was selected for authentication is also supported.

Device Profiling

ClearPass Policy Manager includes real-time profiling and visibility for each endpoint connected to customers' wireless and wired networks which provide an effective method for differentiating access by endpoint type (laptop versus iPad), associating endpoints with an end-user or location, and securing access for non-user oriented devices like printers and IP cameras for wired port level security.

ClearPass' unique profiling model uses standard active and passive techniques as well as collectors (i.e. DHCP, SNMP and ActiveSync) to ensure highly accurate endpoint fingerprints. Granular data from Aruba's direct-touch technique directly captures data from ClearPass OnGuard and Onboard modules when deployed.

The fingerprinting data can automatically be used to provide some of following services:

- Real-time fingerprinting and visibility of all laptops, smartphones, APs, switches and more
- Authorization of printers, game consoles, VoIP phones as they connect to the network
- Associate users with devices, build asset registers, and gain a new level of device visibility

The Policy Manager maintains an interactive representation of device data that provides a visual perspective as well as means to differentiate access per device type or attribute. Dynamic access policies based on endpoints that are known and unknown (fingerprinted for the first time) are now easily applied and managed regardless of endpoint type or user's role.

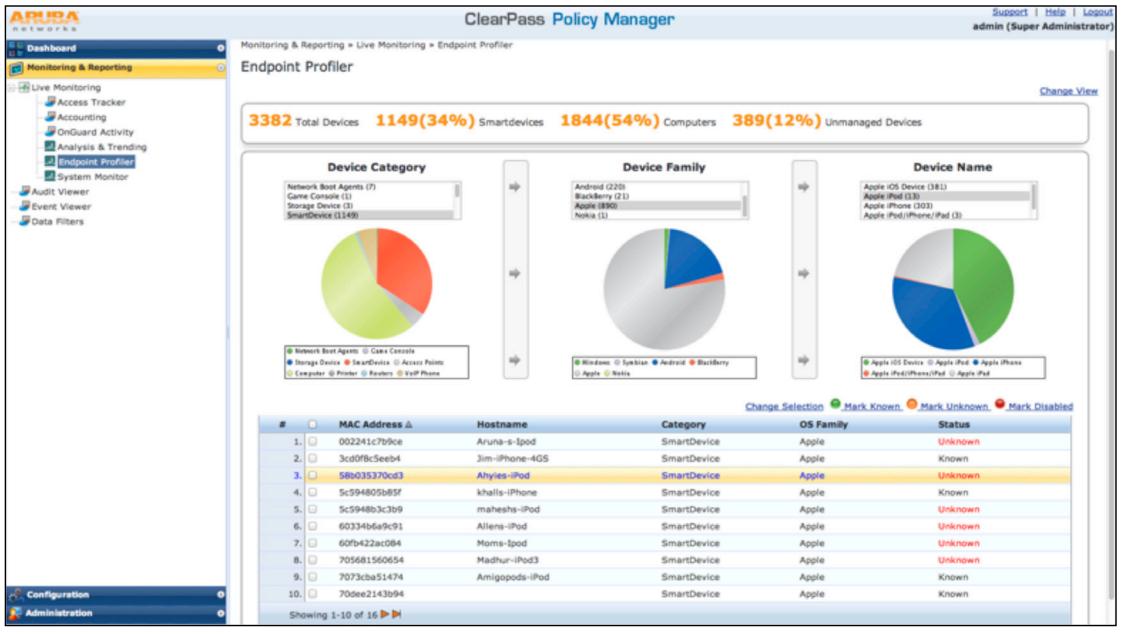

Figure 5: Comprehensive view of all connected devices

Each time that a device authenticates the endpoints database is updated to ensure that device changes are captured; OS updates, etc.

RADIUS change of authorization (CoA) can be used to act on devices that do not meet fingerprint or expected categorization. For example, a device that once looked like a printer but now returns computer attributes can be pushed into a quarantined VLAN.

The IT organization also has the ability to initiate fingerprinting of devices (such as printers) that are configured with a static IP by using a combination of an NMAP scan (looking for open SNMP ports) and SNMP.

AirPlay/AirPrint

AirGroup is an Aruba feature that's included within the ClearPass Policy Manager that improves the performance and usability of Apple Bonjour capable devices like printers, Apple TVs and projectors over services like AirPlay and AirPrint. AirGroup functionality is shared between an Aruba wireless LAN (WLAN) and the Aruba ClearPass Policy Manager.

The WLAN centralizes and optimizes Bonjour-based mDNS messages in the network while ClearPass adds ownership and location-based traffic control and policy-based access control for Bonjour by restricting visibility of devices based on user role, device ownership and location. ClearPass allows for self-registration of a user's personal devices onto the local network with the option to define a group of friends or associates who are allowed to share use of the devices.

Compliance Reports

The Policy Manager includes a complete set of IT and helpdesk reporting tools that display per user/session statistics that include AAA authentication and authorization data. Long-term archiving is also supported for compliance and audit purposes.

Customizable reports deliver the information that is most important for your team, managers, and organization. Easy to complete report templates help you narrow down the data to what you need, what the report will look like, and how and when you share the information.

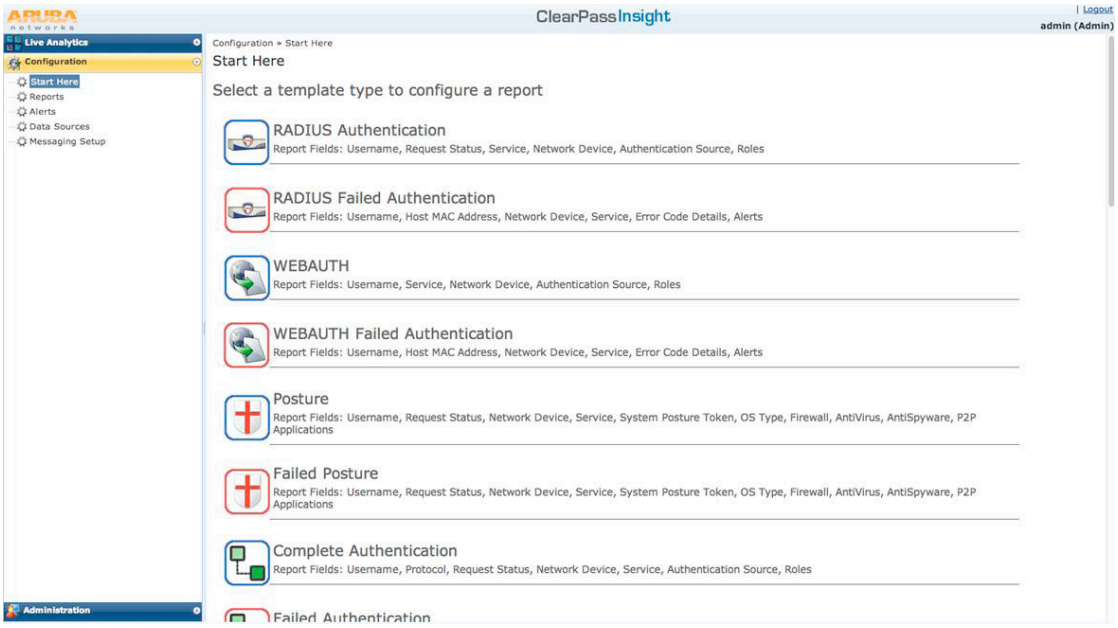

Figure 6: Comprehensive ClearPass Reporting Templates

Appliance sizing

The ClearPass Policy Manager is available as a hardware or virtual appliance and is required for any use case where user or device based authentication and authorization will be performed to grant network access. This includes guests, employees, BYOD and the authentication of unmanaged devices (printers, IP Phones, etc.).

The base platform currently ships in hardware or virtual machine formats and provides support for up to:

- 500 unique devices
- 5,000 unique devices
- 25,000 unique devices

Licensing for the Policy Manager is embedded, which means that correctly sizing the base platform is important as an additional appliance will be required to support a larger number of unique authentications. For example, if a CP-HW-5K appliance is installed and authentications exceed 5,000 unique authentications by 2,000 on a consistent basis, a second CP-HW-5K must be installed in a cluster configuration to add extra capacity (up to 10,000 unique authentications).

ClearPass clustering supports local and distributed deployments, as well as the ability to mix hardware and virtual appliances within a cluster. When compared to other solutions, ClearPass offers the flexibility to authenticate up to 100,000 unique devices using only four (4) appliances without the need for additional or dedicated management appliances. Additional appliances support larger deployments or growth.

A Publisher/Subscriber model easily allows for needed redundancy and backup capabilities.

Modular scalability

Each additional ClearPass software component requires the Policy Manager as the base platform. Licensing is dependent on the number of guests or devices that a customer requires to either onboard, profile, perform a health check, or register a guest user.

The following visual provides an example of licensing across a ClearPass Policy Manager cluster that consists of two (2) CP-HW-5K appliances with a complete ClearPass feature set. Licenses for the additional features are applied and tracked across the cluster and do not require per Policy Manager licensing when deployed in a cluster.

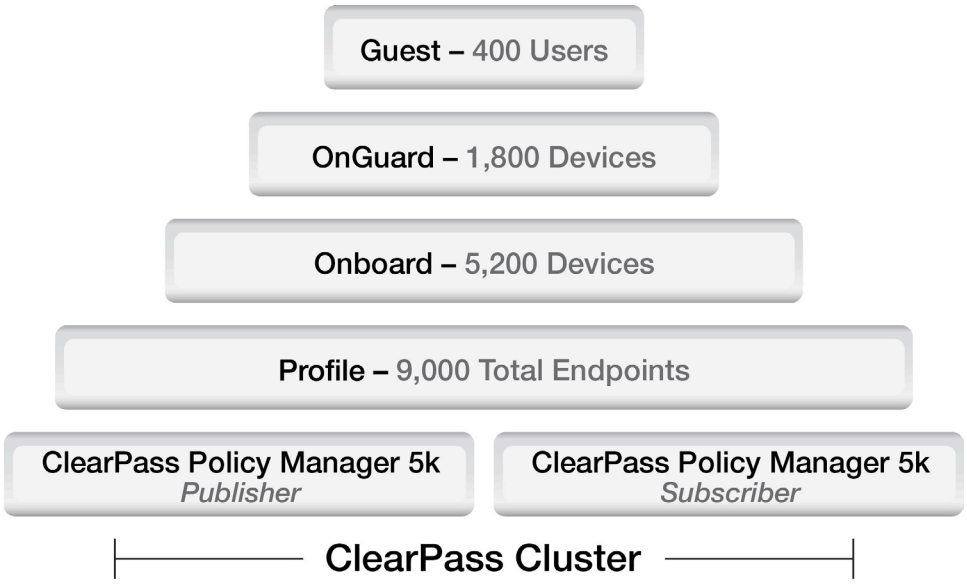

Figure 7: Cluster-wide scalability and licensing

Additional Policy Manager appliances or feature licenses allow for growth or the distribution of resources. Appliances that are not deployed within a cluster do require separate feature licenses.

Introduction to ClearPass Guest

In the past guest access was primarily focused on supporting in-office visitors and allowing users to connect to open networks. Today, requirements dictate that a solution allow for a variety of guest types based on the venue; day visitors, contractors, and vendors at the enterprise, hospital, or educational campus, shoppers at the retail store or mall, fans attending a large public venue.

ClearPass Guest is a dedicated application for differentiating visitor access, and streamlining the IT management functions associated with creating, distributing and terminating account credentials, determining access privileges, and branding requirements.

Functions associated with registration tasks can be securely shared with sponsors which include receptionists or other non-IT staff in order to create temporary visitor accounts. Sponsors can also be assigned separate privileges and reporting capabilities.

Guests, contractors, and temporary employees with mobile devices can also self-register for network access. Once registered, ClearPass Guest delivers account login credentials to users via SMS text messages, email or printed receipts. These temporary visitor accounts can be setup per location and to expire automatically after a specific number of hours or days.

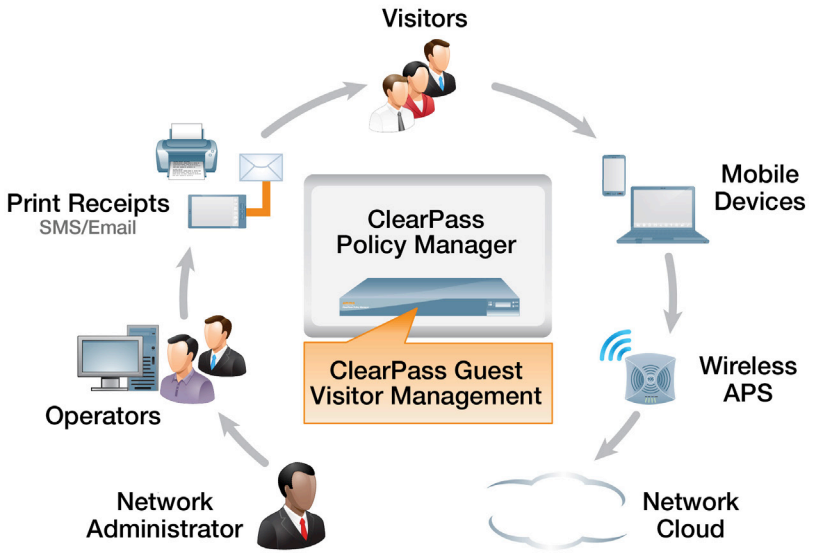

Figure 8: Visitor access using ClearPass Guest

To satisfy the needs of large enterprises and multisite networks, ClearPass Guest scales to support thousands of concurrent visitors on any given day. Customers only need to purchase licensing that allows for the largest number of expected concurrent users. Users that have credentials, but are not currently connected to a network do not count against the license limit.

Integration within Aruba and any existing multivendor networks allow ClearPass Guest to be deployed within any environment to meet diverse security and compliance mandates.

- Customizable captive portal supports branding and usage messaging
- Offers complete self-registration and sponsor capabilities
- Seamlessly integrates with existing wired / wireless infrastructure

Introduction to ClearPass Onboard

ClearPass Onboard provides the ability for trusted end-users to automatically register and configure personal devices on secure networks for uninterrupted email and Internet access. A self-contained captive portal allows users to provision Windows, Mac OS X, iOS, and Android devices without involving IT or the helpdesk. The IT department simply pre-configures download packages built for their networks and device types.

Users simply follow instructions presented on the captive portal to configure the preset 802.1X wireless and wired settings. The portal automatically detects the type of device being onboarded to ensure that the proper configuration is applied. A request for active directory credentials and permission to install a unique credential or certificate ensure that the user can perform the entire onboarding process securely and without any help.

As ClearPass Onboard is a certificate authority it allows for the distribution of unique device certificates for iOS devices during the onboarding process that provide a new level of security as the certificate also contains user and device information that is not provided in normal TLS based certificates.

The onboarding process can also define which users can onboard devices, as well as:

- The types of devices that can be onboarded
- How many devices per user
- What form of certificates are to be used, and more.

For example, the flexibility provided via the onboarding process can allow for an executive to onboard three devices, but limit others to two devices. Or if support is provided to only iOS devices for a specific user group, Android devices can be restricted from onboarding.

The solution also provides the ability to selectively revoke a credential of a device that has been lost or stolen, or where a user's role has changed. Revoking a credential for a device versus changing a user's active directory account does not hamper the user's ability to login with other devices.

Access privileges
The information gathered during the onboarding process can be used for device inventory and for policies that provide very granular differentiation based on some of the following criteria:

- Does the device contain an onboarding credential or not?
- Is the certificate/credential bound to AD/LDAP attributes?
- Does the device type contain specific characteristics, etc.?

Unique device credentials for Windows and Android devices are a combination of device ID and strong password provisioned into the device by the onboarding process. Onboard provisions these credentials and certificates into the Policy Manager (along with device-specific authorization attributes) for use within policies

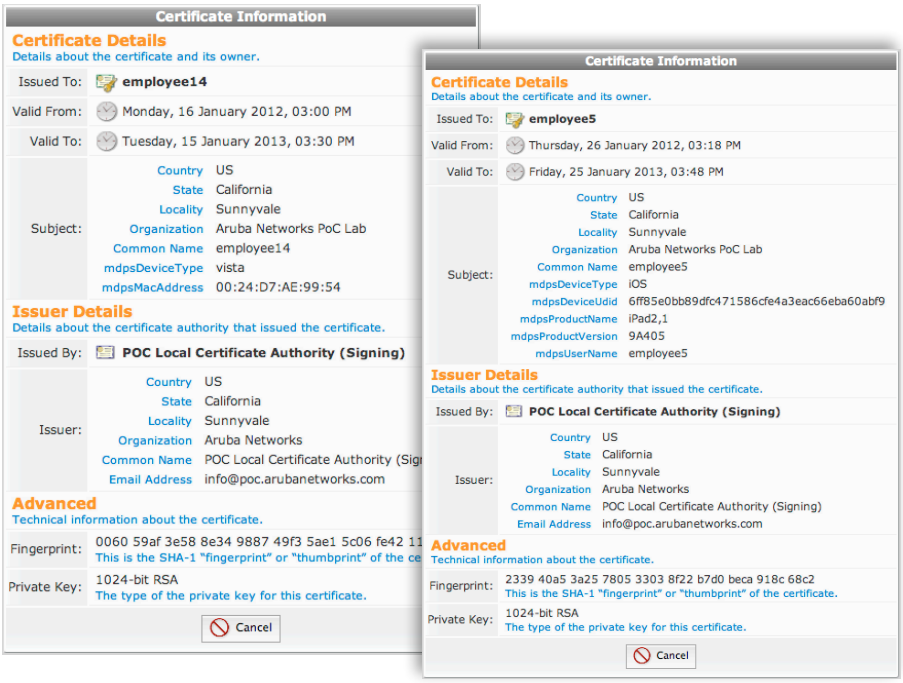

Figure 9: Onboard certificate details

Supported BYOD devices include the iPhone, iPad, MacBook, all major computers running Microsoft Windows 7, and Windows XP, and Android devices.

Manufacturer	Model	Type	OS Versions
Google	Nexus 7	Tablet	4.1.1
Samsung	Galaxy-S	Smartphone	Android 4.0.3
HTC	One X	Smartphone	Android 4.0.3
Kindle	Fire	Tablet	Customized Android 2.3

Figure 10: A sample of supported Android devices

Customers only need to purchase licensing that allows for the total number of expected devices that will be provisioned via the Onboard feature (normally user-owned devices). Devices that are lost or stolen and have their credential revoked automatically free up that license for re-use.

Introduction to ClearPass OnGuard

ClearPass OnGuard performs advanced endpoint posture assessments as well as enterprise-grade network access control (NAC) to ensure that all laptops and computers meet required compliance and safeguards.

Posture and health check policies are created and managed on the ClearPass Policy Manager platform for Windows, Macintosh and Linux operating systems. Persistent and dissolvable agents support 802.1X, non-802.1X, and captive portal access.

All endpoints are checked before granting network access. Endpoints that are identified as at risk can be securely quarantined while IT initiates auto-remediation or requires users to manually remediate without help desk or IT intervention.

Policies can be created to perform:

- Wireless and wired network access
- Automatic and manual quarantine of non-compliant endpoints
- Captive portal and non-captive portal access for employees and guests

Types of assessments include checks for running anti-virus, anti-spyware, and firewall applications for each operating system. Additional windows checks can allow P2P applications, USB storage devices, network interface bridging, registry keys and more.

Periodic compliance checks are performed in the event that users try to circumvent policies after being provided access. Auto-remediation will then be performed again to bring the device back into compliance.

Reports can be used to identify how many devices meet compliance requirements and if adjustments are required. Policies without enforcement can also be performed to allow the tuning of policies prior to enforcement.

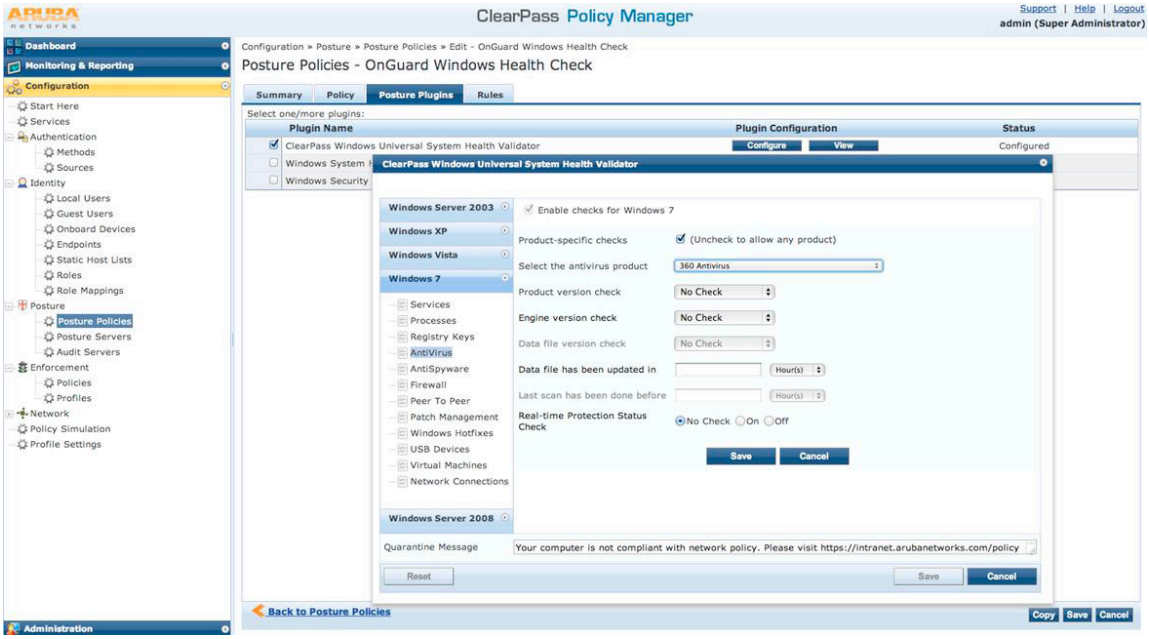

Figure 11: In-depth anti-virus health checks

Customers only need to purchase licensing that allows for the total number of expected laptops or computers that will have posture or health checks performed via the OnGuard feature either using an Aruba persistent or dissolvable agent, or a native Microsoft agent.

Frequently Asked Questions

Q. How do know what devices my employees are connecting to the network?

A. The use of ClearPass Policy Manager and ClearPass Profile provide visibility into each device that connects using either DHCP or has been statically addressed. User information such as device attributes are stored each time a device is connected or a profiling scan is performed.

Q. What do I use if I'm looking for access and application management of smart devices?

A. While ClearPass helps organizations control Wi-Fi access of smart devices and computers, the ability to manage smart devices for remote wipe, location tracking, or controlling the use of applications is dependent on Aruba's MDM partners.

Q. Where does the Amigopod product fit into the ClearPass solution?

A. The former Amigopod products are now ClearPass Guest and ClearPass Onboard. Guest and Onboard currently reside on the same platform and use the Policy Manager for RADIUS services, policy management, visibility and reporting.

Q. Can devices be put into different VLANs depending on type or user role?

A. ClearPass uses the capabilities of the controllers and switches within the infrastructure. In Aruba deployments role-based access enforcement or VLAN steering provided by the controller is utilized. VLAN steering and ACLs are used in environments where Cisco, HP, Juniper, and other vendors are deployed.

Q. Can I purchase the ClearPass Policy Manager without purchasing any modules?

A. Yes. The Policy Manager provides enterprise-class RADIUS and TACACS+ features, with the ability to handle differentiated access use-cases for users and devices. Modules can be added at a later time as requirements dictate.

Q. How do I use ClearPass with MDM (mobile device management) solutions?

A. ClearPass policies will have the ability to leverage information about smart devices and tablets made available by corporate managed MDM solutions, like MobileIron, MaaS360, SOTI,, and other Aruba partners. For example, devices that are detected to be jailbroken can be denied corporate network access.

www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com