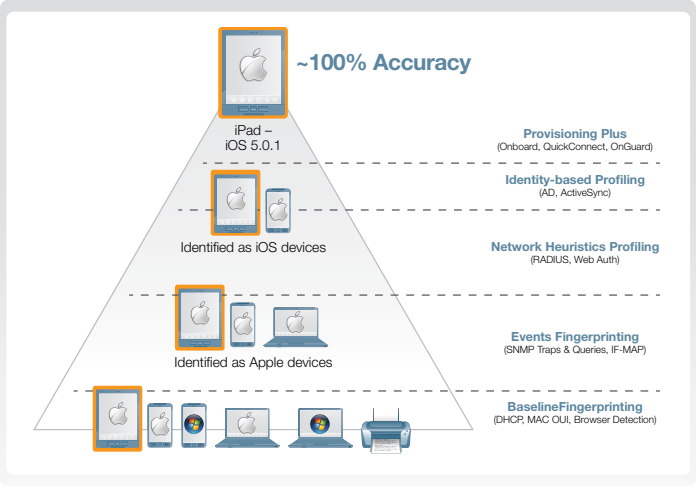
ARUBA CLEARPASS PROFILE

A software module for the ClearPass Policy Manager platform



The Aruba ClearPass five-tier profiling system.

KEY FEATURES

- Automated profiling of all BYOD and IT-managed endpoints.
- Creates a comprehensive whitelist of non-authenticating endpoints such as printers and IP cameras.
- Uses a five-tier profiling system to ensure near 100% device profiling accuracy.
- Works with ClearPass Onboard and ClearPass QuickConnect to ensure all devices are accurately categorized.
- Classifies and stores endpoint attributes within profiles that can be used for policy enforcement.
- View detailed device profiling data from the ClearPass Policy Manager.

ENTERPRISE-GRADE DEVICE PROFILING AND CLASSIFICATION

Aruba ClearPass Profile determines and identifies the unique characteristics of all endpoints that access enterprise networks. It ensures that endpoint attributes are always accurate and uses this information to validate device identity and enforce access privileges.

The collection of attributes for all endpoints is achieved through Aruba's unique five-tier profiling system, which performs baseline fingerprinting, events-centric fingerprinting, network heuristics profiling, identity-centric profiling and device provisioning.

Endpoint attributes are collected, classified by device type and stored within profiles. The profiles can then be used within role-based device policies that administer and enforce the appropriate network access.

THE CLEARPASS DIFFERENCE

In the bring-your-own-device (BYOD) era, it is difficult to keep up with the flurry of devices that connect to wireless and wired networks. Users routinely upgrade their mobile devices, purchase additional devices and replace lost or stolen ones.

This makes Aruba ClearPass Profile a critical part of your IT onboarding arsenal. Automated profiling ensures that current and accurate data is stored for all network devices, including laptops, tablets, smartphones, printers, phones and cameras.

ClearPass Profile delivers the industry's most extensive and accurate profiling system. It maintains a collective view of all devices, dynamically monitors new connections and automatically profiles newly-onboarded devices.

Known devices are reprofiled to update their identities each time that they connect to the network. Dynamic visibility into device types and their characteristics is a critical capability that enhances security, planning and helpdesk operations.

How it works

Aruba ClearPass Profile runs on the ClearPass Policy Manager hardware platform and virtual appliances, and can be deployed in standalone or cluster configurations. Profiling data is collected, stored and displayed through the ClearPass Policy Manager administrative dashboard.

Various profile collectors can be used to collect MAC organizational unique identifier (OUI), DHCP and HTTP fingerprinting data, Microsoft ActiveSync data and other forms of profiling information. A fingerprint of each device and its attributes are then compared with a known list of attributes in a dictionary that is maintained for each device type.

Aruba's five-tier profiling system lets organizations select the appropriate level of profiling based on their infrastructure and security requirements, which ensures superb profiling accuracy. The profile database is then used as a point of authorization for all policy decisions.

Profiling accuracy

Due to exceptional efficiency and accuracy, ClearPass Profile ensures that authorized devices are never denied access to the appropriate network resources. Device attributes are evaluated in two stages, which enable IT to set conditions that build upon baseline fingerprinting.

Stage two extends above baseline profiling and utilizes a collection of rules to match the appropriate policy and enforcement.

ARUBA networks

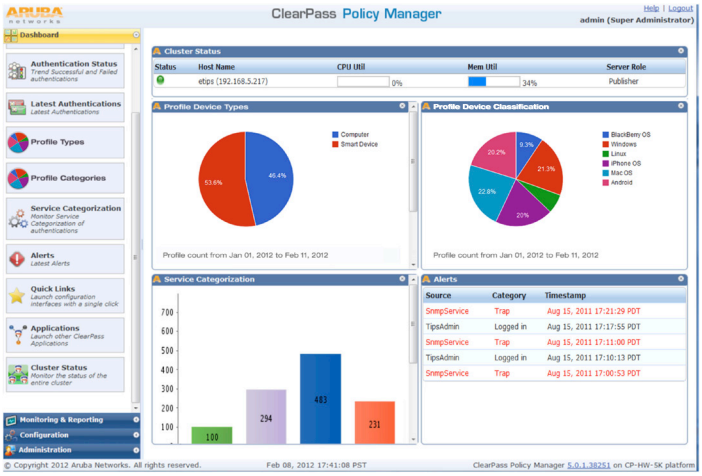
Real-time profiling and control

IT can easily spot classification conflicts that occur if a device is insufficiently categorized. RADIUS change-of-authorization (CoA) automatically requires a device to reauthenticate at the network access layer to initiate a new authentication.

When the user reconnects to the network, ClearPass reprofiles the device to ensure accurate profiling data. For example, if a printer is categorized as a laptop, but expected attributes for printers do not match, the device is automatically reprofiled without interfering with other devices that are connected to the same switch port.

ClearPass Profile visibility

ClearPass Profile gives IT access to a complete list of devices that contain details such as MAC address, device category, device type, device name, MAC vendor and time stamp. Filtering and sorting features make it easy to display device categories, classifications and device types.



Aruba ClearPass Profile offers real-time visibility into device classifications and device types.

Ordering Information	
Part Number	**Description**
LIC-CP-P-100	Profile License for Aruba ClearPass Policy Manager - 100 endpoints
LIC-CP-P-500	Profile License for Aruba ClearPass Policy Manager – 500 endpoints
LIC-CP-P-1K	Profile License for Aruba ClearPass Policy Manager – 1,000 endpoints
LIC-CP-P-2500	Profile License for Aruba ClearPass Policy Manager – 2,500 endpoints
LIC-CP-P-5K	Profile License for Aruba ClearPass Policy Manager – 5,000 endpoints
LIC-CP-P-10K	Profile License for Aruba ClearPass Policy Manager - 10,000 endpoints
LIC-CP-P-25K	Profile License for Aruba ClearPass Policy Manager – 25,000 endpoints
LIC-CP-P-50K	Profile License for Aruba ClearPass Policy Manager – 50,000 endpoints
Warranty	
Software	90 days**

** ClearPass Profile, a software license of the ClearPass Policy Manager system, requires a ClearPass Policy Manager server.*

*** Extended with support contract*

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