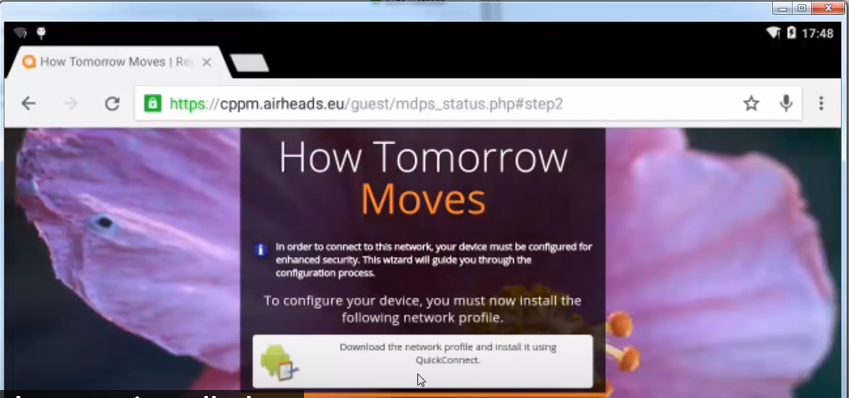
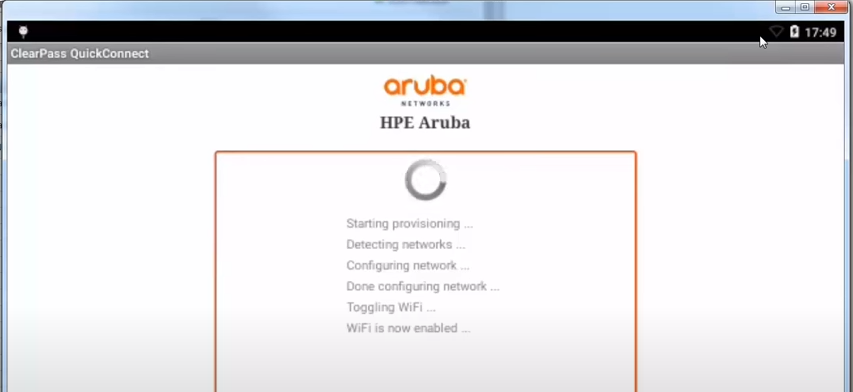
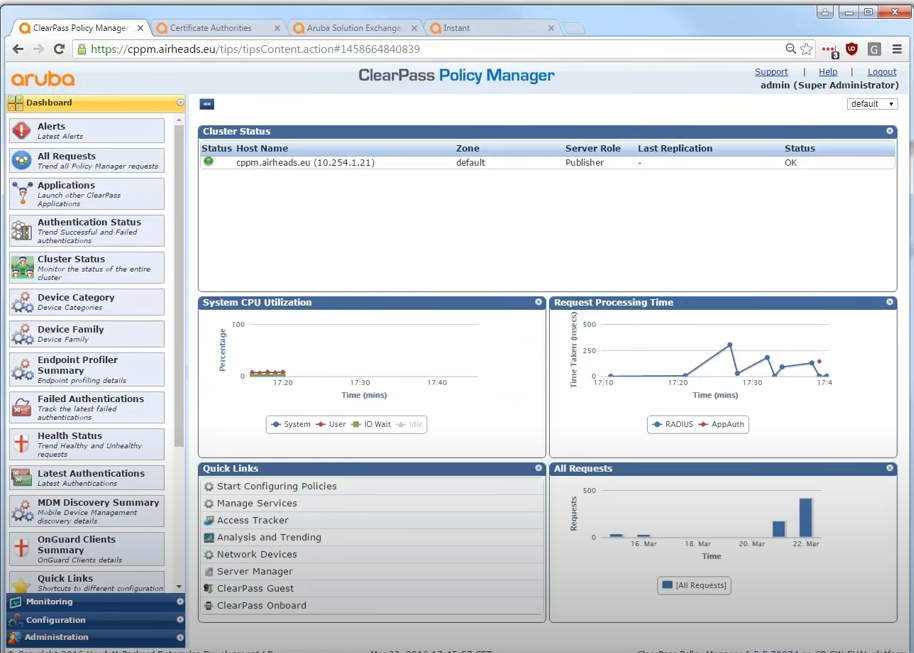
ARUBA CLEARPASS

Features

* It is a policy platform
* ClearPass works with any multivendor network and can be extended to business and IT systems that are already in place.
* ClearPass delivers a wide range of unique self-service capabilities. Users can securely onboard their own devices for enterprise use or register AirPlay, AirPrint, Digital Living Network Alliance (DLNA), and Universal Plug and Play (UPnP) devices that are enabled for sharing, sponsor guest Wi-Fi access, and even set up sharing for Apple TV and Google Chromecast.
* The power of ClearPass comes from integrating ultra-scalable AAA (authentication, authorization, and accounting) with policy management, guest network access, device onboarding, and device health checks with a complete understanding of context.
* The criteria on determining the appropriate access privileges for any user is their contextual data that is leveraged across the network to ensure that users and devices are granted the appropriate access privileges.
* ClearPass can be extended to third-party security and IT systems using REST-based APIs to automate work flows that previously required manual IT intervention.

* It integrates with mobile device management to leverage device inventory and posture information, which enables better-informed policy decisions.
* Onboarding in ClearPass is as follows, People bring their own devices instead of the organization giving their devices to people. While people are getting their devices on the network, they are guided through a provisioning as cycle in clear pass where they can request a client certificate it will be automatically configured on the device and they get access. So, they don’t know they get certificates but organization is handing out the certificates.
* In Abura ClearPass, devices use a client certificate instead of using username and a password.
* It has an access tracker which is where we see coming in all our requests as soon as they start coming on.
* It has a provisioning portal web page such as Pfsense landing page, and in this page, there are some warnings and besides there is a link for downloading the ClearPass QucikConnect which is the self-service device onboarding. In the following image there is an example;
* The onboarding process is allowed via an application called ClearPass QuickConnect. Then the next step is managing these devices onboarded over wireless connection and this done with ClearPass Policy Manager.





**ClearPass Policy Manager Hardware and Virtual Appliances**

ClearPass Policy Manager is available as a hardware or a virtual appliance. To increase scalability and redundancy, you can deploy virtual appliances, as well as the hardware appliances, within a cluster.

For hardware and virtual appliance installation and deployment procedures, see [This describes the procedures for installing and configuring ClearPass Policy Manager on a hardware appliance, as well as how to install ClearPass on a VMware vSphere Hypervisor host and on a host that runs Microsoft's hypvervisor, Hyper-V™. This guide also describes how to install a ClearPass virtual appliance on a host that runs the CentOS KVM (Kernel Virtual Machine) hypervisor.](https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/Hardware%20and%20Virtual%20Appliances/Intro_Appliances.htm).

Virtual appliances are supported on the following platforms:

VMware ESX and ESXi

For installation and deployment procedures, see [Using the VMware vSphere Hypervisor Web Client to Install ClearPass on a Virtual Machine](https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/Hardware%20and%20Virtual%20Appliances/ESX_virtual_applicance.htm).

Microsoft Hyper-V

For installation and deployment procedures, see [Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance](https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/Hardware%20and%20Virtual%20Appliances/HyperV_virtual_applicance.htm).

**ClearPass Specifications**

The ClearPass Policy Manager specifications are as follows:

[[Open](javascript:void(0))Hardware and Virtual Appliances Support](javascript:void(0))

ClearPass is available as hardware or as a virtual appliance. Virtual appliances are supported on VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, and Amazon EC2.

* VMware ESXi 5.5 to 6.7
* Microsoft Hyper-V Server 2012 R2 and 2016, and Windows Server 2012 R2 with Hyper-V
* KVM on CentOS 6.6, 6.8
* Amazon EC2

[[Open](javascript:void(0))ClearPass Platform](javascript:void(0))

* Deployment templates for any network type, identity store, and endpoint
* 802.1X, MAC authentication, and captive portal support
* ClearPass OnConnect for SNMP-based enforcement on wired switches
* Advanced reporting, analytics, and troubleshooting tools
* Interactive policy simulation and monitor mode utilities
* Multiple device registration portals—Guest, Aruba AirGroup, BYOD (bring your own device), and unmanaged devices
* Admin/Operator access security via CAC (Common Access Card) and TLS (Transport Layer Security) certificates

[[Open](javascript:void(0))Framework and Protocol Support](javascript:void(0))

* RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
* EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
* PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
* EAP-TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
* EAP-TLS
* PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
* Wireless and wired 802.1X and VPN
* OAuth .02
* Microsoft NAP and NAC
* Active Directory machine authentication
* Online Certificate Status Protocol (OCSP)
* SNMP generic MIB, SNMP private MIB
* Common Event Format (CEF), Log Event Extended Format (LEEF)
* Simple Certificate Enrollment Protocol (SCEP)
* Enrollment over Secure Transport (EST)

[[Open](javascript:void(0))Supported Identity Stores](javascript:void(0))

* Microsoft Active Directory
* Kerberos
* Any LDAP-compliant directory
* Microsoft SQL, PostgreSQL, MariaDB, and Oracle 11g ODBC-compliant SQL server
* Built-in SQL store
* Built-in static-hosts list
* Token servers
* Built-in SQL store, static hosts list
* Microsoft Azure Active Directory (via SAML and OAuth 2.0)
* Google G Suite (via SAML and OAuth 2.0)

[[Open](javascript:void(0))IPv6 Support](javascript:void(0))

* Web and CLI based management
* IPv6 addressed authentication & authorization servers
* IPv6 accounting proxy
* IPv6 addressed endpoint context servers
* Syslog, DNS, NTP, IPsec IPv6 targets
* IPv6 Virtual IP for high availability
* HTTP Proxy
* Ingress Event Engine Syslog sources

[[Open](javascript:void(0))Profiling Methods](javascript:void(0))

* Active: Nmap, WMI, SSH, SNMP
* Passive: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, ‘SPAN’ Port, HTTP User-Agent, IF-MAP
* Integrated and Third-Party: Onboard, OnGuard, ArubaOS, EMM/MDM, Rapid7, Cisco device sensor

Advantages

* ADVANCED POLICY MANAGEMENT
  + Enforcement and visibility for wired and wireless
  + Secure device configuration of personal devices
  + Device health checks
  + Customizable visitor management
* ARUBA 360 SECURITY EXCHANGE PROGRAM
* Integrate with security and workflow systems
* ADVANCED REPORTING AND ALERTING

Source: <https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/About%20ClearPass/About_ClearPass.htm>