DATA SHEET

ARUBA CLEARPASS POLICY MANAGER

The most advanced policy management platform available

Aruba ClearPass Policy Manager provides role- and device-based network access control for employees, contractors and guests across any multivendor wired, wireless and VPN infrastructure.

With a built-in context-based policy engine, RADIUS, TACACS+ protocol support, device profiling and comprehensive posture assessment, onboarding, and guest access options, ClearPass is unrivaled as a foundation for network security in any organization.

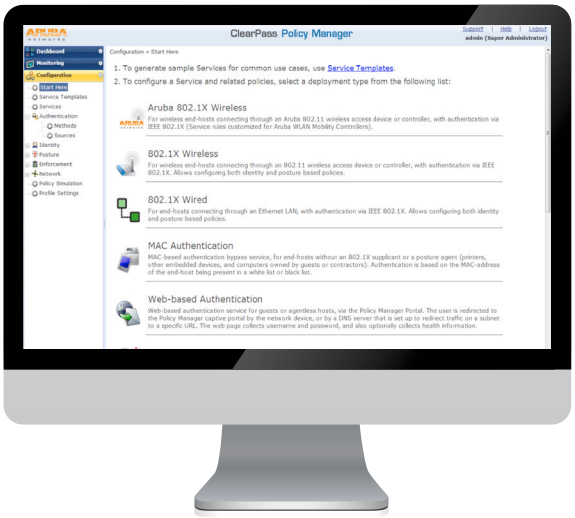
For wider security coverage, using firewalls, EMM and other existing solutions, ClearPass Exchange allows for automated threat protection and workflows to third-party security and IT systems that previously required manual IT intervention.

In addition, ClearPass supports secure self-service capabilities for end user convenience. Users can securely configure their own devices for enterprise use or Internet access. Aruba wireless customers can provide registration of AirPlay-, AirPrint-, DLNA-, and UPnP-enabled devices for sharing.

The result is a comprehensive and scalable policy management platform that goes beyond traditional AAA solutions to deliver extensive enforcement capabilities for IT-owned and bring-your-own-device (BYOD) security requirements.

KEY FEATURES

- Role-based network access enforcement for multivendor Wi-Fi, wired and VPN networks.
- Industry-leading performance, scalability, high availability and load balancing.
- Intuitive policy configuration templates and visibility troubleshooting tools.
- Supports multiple authentication/authorization sources (AD, LDAP, SQL dB) within one service.
- Self-service device onboarding with built-in certificate authority (CA) for BYOD
- Guest access with extensive customization, branding and sponsor-based approvals.



- Supports NAC and EMM/MDM integration for mobile device assessments.
- Comprehensive integration with third party systems such as SIEM, Internet security and EMM/MDM.
- Single sign-on (SSO) and Aruba Auto Sign-On support via SAML v2.0.
- Advanced reporting of all user valid authentications and failures.
- Built-in profiling using DHCP and TCP fingerprinting.
- Hardware and virtual support for ESXi and Hyper-V appliances.
- Automatic cluster upgrade.

THE CLEARPASS DIFFERENCE

The ClearPass Policy Manager is the only policy solution that centrally enforces all aspects of enterprise-grade mobility and NAC for any industry. Granular network access enforcement is based on a user's role, device type and role, authentication method, EMM/MDM attributes, device health, location, and time-of-day.

ClearPass offers extensive multivendor wireless, wired and VPN infrastructure support which enables IT to easily rollout secure mobility policies across any environment.

Deployment scalability supports tens of thousands of devices and authentications which surpasses the capabilities offered by legacy AAA solutions. Options exist for small to large organizations, from local to distributed environments.

ADVANCED REPORTING AND ALERTING WITH INSIGHT

Policy Manager includes advanced reporting capabilities that includes customizable dashboards for authentication, endpoint profiling, industry standards, and other information for guest, onboarding, and device health, all in an at-a-glance dashboard. InSight also includes granular alert capabilities.

ADVANCED POLICY MANAGEMENT

Enforcement and visibility for wired and wireless

With ClearPass, organizations can deploy wireless using standards-based 802.1X enforcement for strong authentication. ClearPass also offers a way to create non-.1X policies on wired networks with OnConnect – for those organizations not ready to go full 802.1X and AAA throughout their wired infrastructure. ClearPass allows for a hybrid approach to enable IT to gain insights about all devices – computers, smartphones and IoT – accessing the network.

Concurrent authentication methods can be used to support a variety of use-cases. It also includes support for multi-factor authentication based on login times, posture checks, and other context such as new user, new device, and more.

Attributes from multiple identity stores such as Microsoft Active Directory, LDAP-compliant directory, ODBC-compliant SQL database, token servers and internal databases across domains can be used within a single policy for fine-grained control.

Contextual data from these profiled devices allows for IT to define what devices can access either the wired, VPN, or wireless network.

Device profile changes are dynamically used to modify authorization privileges. For example, if a Windows laptop appears as a printer, ClearPass policies can automatically revoke or deny access.

Secure device configuration of personal devices

ClearPass Onboard provides automated provisioning of any Windows, Mac OS X, iOS, Android, Chromebook, and Ubuntu devices via a user driven self-guided portal. Required SSIDs, 802.1X settings and security certificates are automatically configured on authorized devices.

Customizable visitor management

ClearPass Guest simplifies workflow processes so that receptionists, employees and other non-IT staff can create temporary guest accounts for secure Wi-Fi and wired Internet access. Self-registration, sponsor and bulk credential creation supports any guest access need – enterprise, retail, education, large public venue.

Device health checks

ClearPass OnGuard, leveraging OnGuard persistent and dissolvable agents, performs advanced endpoint posture assessments over wireless, wired and VPN connections. OnGuard health-check capabilities ensure compliance and network safeguards before devices connect.

ADDITIONAL POLICY MANAGEMENT CAPABILITIES

Integrate with security and workflow systems

ClearPass Exchange interoperability includes REST-based APIs, and forwarding of syslog data flows to and from ClearPass on-demand; that can be used to facilitate workflows with MDM, SIEM, firewalls PMS, call centers, admission systems, and more. For faster, flexible interoperability, ClearPass can allow end users to integrate container based extensions in real time for extremely fast interoperability with new partners or new features on-demand. Context is shared between each component for end-to-end policy enforcement and visibility.

Connect and work apps are good to go

ClearPass Auto Sign-On capabilities make it infinitely easy to access work apps on mobile devices. A valid network authentication automatically connects users to enterprise mobile apps so they can get right to work.

Single sign-on (SSO) support works with Ping, Okta and other identity management tools to improve the user experience to SAML 2.0-based applications.

SPECIFICATIONS

ClearPass Policy Manager Appliances

ClearPass Policy Manager is available as hardware or a virtual appliance that supports 500, 5,000 and 25,000 authenticating devices. Virtual appliances are supported on VMware ESX/i and Microsoft Hyper-V.

- ESX 4.0, ESXi 4.1, up to 6.0
- Hyper-V 2012 R2 and Windows 2012 R2 Enterprise

Virtual appliances, as well as hardware appliances, can be deployed within an active cluster to increase scalability and redundancy.

Platform

- Built-in AAA services – RADIUS, TACACS+ and Kerberos
- Web, 802.1X, non-802.1X, RADIUS authentication and authorization
- Advanced reporting, analytics and troubleshooting tools
- External captive portal redirect to multivendor equipment
- Interactive policy simulation and monitor mode utilities
- Multiple device registration portals – Guest, Aruba AirGroup, BYOD, un-managed devices
- Deployment templates for any network type, identity store and endpoint
- Admin/Operator access security via CAC and TLS certificates
- IPSec tunnels

Framework and protocol support

- RADIUS, RADIUS CoA, TACACS+, web authentication, SAML v2.0
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1 and 2, EAP-MD5
- NAC, Microsoft NAP
- Windows machine authentication
- MAC auth
- Audit (rules based on port and vulnerability scans)
- Online Certificate Status Protocol (OCSP)
- SNMP generic MIB, SNMP private MIB
- Common Event Format (CEF), Log Event Extended Format (LEEF)
- TLS 1.2

Supported identity stores

- Microsoft Active Directory
- RADIUS
- Any LDAP compliant directory
- Any ODBC-compliant SQL server
- Token servers
- Built-in SQL store, static hosts list
- Kerberos

RFC standards

- 2246, 2248, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3576, 3579, 3580, 3748, 4017, 4137, 4849, 4851, 5216, 528, 7030

Internet drafts

- Protected EAP Versions 0 and 1, Microsoft CHAP extensions, dynamic provisioning using EAP-FAST, TACACS+

Information assurance validations

- FIPS 140-2 – Certificate #2577

Profiling methods

- DHCP, TCP, MAC OUI, ClearPass Onboard, SNMP, Cisco device sensor

	ClearPass Policy Manager-500	ClearPass Policy Manager-5K	ClearPass Policy Manager-25K
APPLIANCE SPECIFICATIONS			
CPU	(1) Eight Core 2.4GHz Atom C2758	(1) Quad Core Xeon 3.4 GHz E3-1231_V3	(2) Six Core Xeon 2.4GHz E5-2620_V3
Memory	8 GB	8 GB	64 GB
Hard drive storage	(1) SATA (7.3K RPM) 1TB hard drive	(2) SATA (7.2K RPM) 1TB hard drives, RAID-1 controller	(6) SAS (10K RPM) 600GB Hot-Plug hard drives, RAID-10 controller
APPLIANCE SCALABILITY			
Maximum endpoints	500	5,000	25,000
FORM FACTOR			
Dimensions (WxHxD)	17.2" x 1.7" x 11.3"	17.09" x 1.67" x 15.5"	18.98" x 1.68" x 27.57"
Weight (Max Config)	8.5 Lbs	16.97 Lbs	Up to 37 Lbs
POWER			
Power supply	200 watts max	250 watts max	750 watts max
Power redundancy	N/A	N/A	optional
AC input voltage	100/240 VAC auto-selecting	100/240 VAC auto-selecting	100/240 VAC auto-selecting
AC input frequency	50/60 Hz auto-selecting	50/60 Hz auto-selecting	50/60 Hz auto-selecting
ENVIRONMENTAL			
Operating temperature	5° C to 35° C (41° F to 95° F)	10° C to 35° C (50° F to 95° F)	10° C to 35° C (50° F to 95° F)
Operating vibration	0.25 G at 5 Hz to 200 Hz for 15 minutes	0.26 G at 5 Hz to 350 Hz for 15 minutes	0.26 G at 5 Hz to 350 Hz for 15 minutes
Operating shock	1 shock pulse of 20 G for up to 2.5 ms	1 shock pulse of 31 G for up to 2.6 ms	1 shock pulse of 40 G for up to 2.3 ms
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)	-16 m to 3,048 m (-50 ft to 10,000 ft)	-16 m to 3,048 m (-50 ft to 10,000 ft)

* Virtual appliance sizing must match hardware appliance specifications

ORDERING GUIDANCE

Ordering the ClearPass Policy Manager involves the following steps:

1. Determine the number of authenticated endpoints/devices in your environment. Additionally, select optional functionality, such as guests per day, total BYO devices being configured for enterprise use, and total number of computers requiring health checks.
2. Choose the appropriate platform (either virtual or hardware appliance) sized to accommodate the total number of devices and guests that will require authentication for your deployment.

ORDERING INFORMATION

Part Number	Description
CP-HW-500 or CP-VA-500	Aruba ClearPass Policy Manager 500 hardware platform supporting a maximum of 500 authenticated devices
CP-HW-5K or CP-VA-5K	Aruba ClearPass Policy Manager 5K hardware platform supporting a maximum of 5,000 authenticated devices
CP-HW-25K or CP-VA-25K	Aruba ClearPass Policy Manager 25K hardware platform supporting a maximum of 25,000 authenticated devices
Expandable application software*	
ClearPass Onboard – device configuration and certificate management	
ClearPass OnGuard – endpoint device health	
ClearPass Guest – visitor access management	
Warranty	
Hardware	1 year parts/labor**
Software	90 days**

* Expandable application software is available in the following increments: 100, 500, 1,000, 2,500, 5,000, 10,000, 25,000, 50,000 and 100,000.

** Extended with support contract

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com