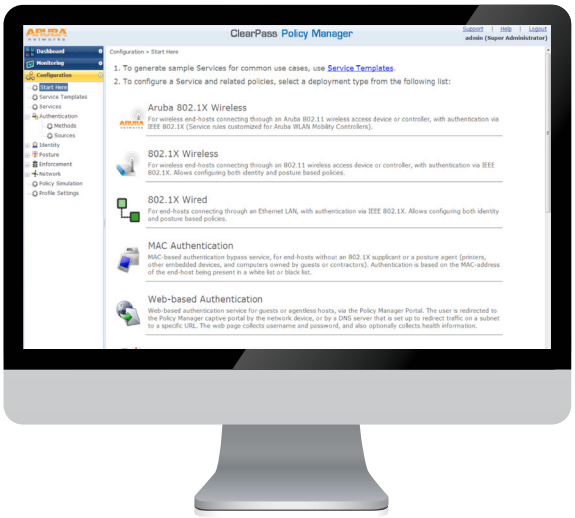
DATA SHEET

ARUBA CLEARPASS POLICY MANAGER™

The most advanced policy management platform available



The Aruba ClearPass Policy Manager™ platform 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, Microsoft NAP, 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.

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.

Offering unsurpassed interoperability, 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.

UNPRECEDENTED SIMPLICITY

Centrally-defined policies and enforcement eliminates the need for multiple AAA and policy management systems, which strengthens an organization's overall security architecture. A host of built-in capabilities lets IT quickly adapt to changing network access challenges.

ClearPass is also a valuable security operations and troubleshooting tool that delivers unprecedented visibility to quickly identify network issues, and policy and security vulnerabilities.

ADVANCED POLICY MANAGEMENT

Employee access

ClearPass Policy Manager offers role-based user and device authentication based on 802.1X, non-802.1X and web portal access methods. Concurrent authentication methods can be used to support a variety of use-cases.

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.

Enhanced device profiling

A built-in profiling service discovers and classifies all endpoints, regardless of device type or access method – wired, wireless or VPN. Contextual data from smart phones and tablets, to IP cameras can be obtained using DHCP, TCP, and other fingerprinting methods to define policies.

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.

Access for unmanaged endpoints

Unmanaged non-802.1X devices – printers, IP phones and other Internet of Things (IoT) – can be identified as known or unknown upon connecting to the network. MAC authentication and profiling validate network access privileges and authorization.

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 to 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 or Microsoft NAP*, 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 that can be used to facilitate workflows with MDM, SIEM, firewalls PMS, call centers, admission systems and more. 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

The 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 5.5
- Hyper-V 2012 R2 and Windows 2012 R2 Enterprise

Virtual appliances, as well as hardware appliances, can be deployed within an active/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 (non-802.1X devices)
- 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)

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 #1747

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) Dual Core Pentium	(1) Quad Core Xeon	(2) Six Core Xeon
Memory	4 GB	8 GB	64 GB
Hard drive storage	(1) 3.5" SATA (7K RPM) 500GB hard drive	(2) 3.5" SATA (7.2K RPM) 1TB hard drives, RAID-1 controller	(6) 2.5" SAS (10K RPM) 600GB Hot-Plug hard drives, RAID-10 controller
APPLIANCE SCALABILITY			
Maximum devices	500	5,000	25,000
FORM FACTOR			
Dimensions (WxHxD)	16.8" x 1.7" x 14"	17.53" x 1.7" x 16.8"	17.53" x 1.7" x 27.8"
Weight (Max Config)	14 Lbs	18 Lbs	Up to 39 Lbs
POWER			
Power consumption (maximum)	260 watts max	250 watts max	750 watts max
Power supply	Single	Single	Dual hot-swappable (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	10° C to 35° C (50° 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	0.26 G at 5 Hz to 350 Hz for 5 minutes	0.26 G at 5 Hz to 350 Hz for 5 minutes	0.26 G at 5 Hz to 350 Hz for 5 minutes
Operating shock	1 shock pulse of 31 G for up to 2.6 ms	1 shock pulse of 31 G for up to 2.6 ms	1 shock pulse of 31 G for up to 2.6 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

aruba NETWORKS an HP company

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