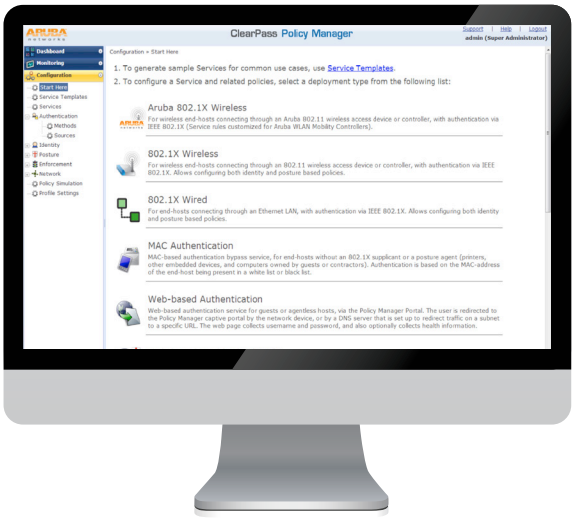
DATA SHEET

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 wired, wireless and VPN infrastructure.

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

ClearPass can be extended to third-party security and IT systems using REST-based APIs to automate workflows 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.

In addition to automating mobility services, ClearPass supports self-service capabilities for end users. Users can securely configure their own devices for enterprise use and register AirPlay-, AirPrint-, DLNA-, and UPnP-enabled devices for sharing.

The result is a comprehensive and scalable access management platform that goes beyond traditional AAA solutions to deliver consistent policies 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.
- Web-based interface simplifies policy configuration and troubleshooting.
- Supports NAC, Microsoft NAP posture and health checks, and MDM integration for mobile device posture checks.
- Auto Sign-On and single sign-on (SSO) support via SAML v2.0.
- Advanced reporting of all user authentications and failures.
- HTTP/RESTful APIs for integration with third party systems such as SIEM, Internet security and MDM.
- Device profiling and self-service onboarding.
- Guest access with extensive branding and customization and sponsor-based approvals.
- IPv6 administration support

THE CLEARPASS DIFFERENCE

The ClearPass Policy Manager is the only NAC solution that centrally enforces all aspects of enterprise mobility from a single platform. Granular network access privileges are granted based on a user's role, device type, MDM attributes, device health, location, and time-of-day.

Offering unsurpassed interoperability, ClearPass supports an extensive collection of multivendor wireless, wired and VPN networking equipment which enables IT to easily rollout secure mobility policies across any infrastructure.

With flexible deployment options, IT can start by providing sponsored guest access and let employees self-configure their own devices, and later add MDM. ClearPass scales to support tens of thousands of devices and users.

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.

An easy-to-use template-based interface provides an efficient way to create network access and authentication services, regardless of current identity stores, authentication methods or enforcement models.

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

ADVANCED POLICY MANAGEMENT

Employee access

ClearPass Policy Manager offers user and device authentication based on 802.1X, non-802.1X and web portal access methods. Multiple authentication protocols like PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public can be used concurrently to strengthen security in any environment.

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.

Additionally, posture assessments and remediation can be added to existing policies at any time.

Built-in device profiling

ClearPass has the only built-in profiling service that discovers and classifies all endpoints, regardless of device type. A variety of contextual data – MAC OUIs, DHCP fingerprinting and other identity-centric device data – can be obtained and used within policies.

Stored profiling data is used to identify device profile changes and to dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, ClearPass Policy Manager can automatically deny access.

Access for unmanaged endpoints

Unmanaged non-802.1X devices – printers, IP phones and IP cameras – can be identified as known or unknown upon connecting to the network. The identity of these devices is based on the presence of their MAC address in an external or internal database.

Secure device configuration of personal devices

ClearPass Onboard fully automates the provisioning of any Windows, Mac OS X, iOS, Android, Chromebook, and Ubuntu devices via a built-in captive portal. Valid users are redirected to a template-based interface to configure required SSIDs, 802.1X settings, and download unique device credentials.

Additional capabilities include the ability for IT to revoke and delete credentials for lost or stolen devices, and the ability to configure mobile email settings for Exchange ActiveSync and VPN clients on some device types.

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 network access. Self-registration allows guests to create their credentials.

Customizable captive portal capabilities let IT and marketing organizations create a branded guest login experience with targeted advertising and user code-of-conduct messaging. Self-registration and automated credential delivery also streamlines IT operations.

Device health checks

ClearPass OnGuard, as well as separate *OnGuard persistent or dissolvable agents*, perform advanced endpoint posture assessments. Traditional NAC health-check capabilities ensure compliance and network safeguards before devices connect.

Information about endpoint integrity – such as status of anti-virus, anti-spyware, firewall, and peer-to-peer applications – can be used to enhance authorization policies. Automatic remediation services are also available for non-compliant devices.

ADDITIONAL POLICY MANAGEMENT CAPABILITIES

Integrate with security and workflow systems

ClearPass Exchange offers a set of syslog data flows and REST-based APIs that can be used to facility interoperability with MDM, SIEM like Splunk, PMS, call centers, admission systems and more.

Built-in integration with MobileIron, AirWatch, SAP Afaria, Citrix, JAMF, SOTI and IBM/MaaS360 makes it easy to use attributes collected by an MDM agent to enforce network policies. A device can be denied Wi-Fi access if it's jailbroken, running blacklisted apps or the owner isn't in an authorization database.

Connect and work apps are good to go

ClearPass Auto Sign-On capabilities make it infinitely easy to access work apps on mobile devices. Instead of a single sign-on, which requires everyone to manually login to the network *and* apps, ClearPass Auto Sign-On leverages the network login and automatically authenticates users to enterprise mobile apps so they can get right to work.

ClearPass can be configured as an Identity Provider (IdP) to work with Ping, Okta and other identity management tools so that users can access SAML-based applications for an improved and secure mobility experience.

Extensive captive portal support

ClearPass provides a central captive portal for authentication that works on Aruba and any other multivendor wired and wireless network. This eliminates the need for separate Wi-Fi and wired captive portals.

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 and ESXi platforms, versions ESX 4.0, ESXi 4.0, 5.0 and 5.5.

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

SPECIFICATIONS

Aruba Clearpass Policy Manager

- Comprehensive identity-based policy engine.
- Posture agents for Windows, Mac OS X, Linux operating systems.
- Built-in AAA services – RADIUS, TACACS+ and Kerberos.
- Web, 802.1X, non-802.1X authentication and authorization.
- Reporting, analytics and troubleshooting tools.
- External captive portal redirect to multivendor equipment.
- Interactive policy simulation and monitor mode utilities.
- Deployment templates for any network type, identity store and endpoint.
- User-initiated device registration – Aruba AirGroup and unmanaged devices.

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)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1 and 2, EAP-MD5
- Wireless and wired 802.1X and VPN
- Microsoft NAP, NAC
- Windows machine authentication
- MAC auth (non-802.1X devices)
- Audit (rules based on port and vulnerability scans)

Supported identity stores

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

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 compliant – Certificate #1747

	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) 500GB 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)

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

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