

Overview

Aruba ClearPass Policy Manager Platform

The most advanced Secure NAC platform available



Product overview

Aruba's ClearPass Policy Manager, part of the Aruba 360 Secure Fabric, provides role- and device-based secure network access control for IoT, BYOD, Corporate devices, the employees, contractors and guests across any multivendor wired, wireless and VPN infrastructure that use them.

With a built-in context-based policy engine, RADIUS, TACACS+, non-RADIUS enforcement using OnConnect, device profiling, posture assessment, onboarding, and guest access options, ClearPass is unrivaled as a foundation for network security for organizations of any size.

For comprehensive integrated security coverage and response using firewalls, EMM/MDM and other existing solutions, ClearPass supports the Aruba 360 Security Exchange Program. This allows for automated threat detection and response workflows that integrate with third-party security vendors and IT systems previously requiring manual IT intervention.

In addition, ClearPass supports secure self-service capabilities making it easier for end users trying to access the network. Users can securely configure their own devices for enterprise use or Internet access. Aruba wireless customers in particular can take advantage of the enhanced security of their AirGroup environment as well as ClearPass Auto Sign-On. This enables a user's network authentication to pass automatically to their enterprise mobile apps so they can get right to work.

The result is detailed visibility of all wired and wireless devices connecting to the enterprise, increased control through simplified and automated authentication or authorization of devices, and faster, better incident analysis and response through the integration of Aruba IntroSpect UEBA and third-party partner ecosystems. This is achieved with 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 multi-vendor Wireless, wired and VPN networks.
- Virtual and hardware appliances that can be deployed in a cluster to increase scalability and redundancy.
- Intuitive policy configuration templates and visibility troubleshooting tools.
- Supports multiple authentication/authorization sources (AD, LDAP, SQL dB).
- Self-service device onboarding with built-in certificate authority (CA) for BYOD

Overview

- Guest access with extensive customization, branding and sponsor-based approvals.
- Supports NAC and EMM/MDM integration for mobile device assessments.
- Comprehensive integration with the Aruba 360 Security Exchange Program.
- Single sign-on (SSO) support works with Ping, Okta and other identity management tools to improve user experience to SAML 2.0-based applications.
- Advanced reporting and granular alerts
- Active and passive device fingerprinting
- Support for popular virtualizations platforms such as VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, CentOS KVM & Amazon EC2.

The ClearPass Difference

ClearPass is the only policy platform that centrally enforces all aspects of enterprise-grade access security for any industry. Granular policy enforcement is based on a user's role, device type and role, authentication method, EMM/MDM attributes, device health, traffic patterns, location, and time-of-day.

ClearPass offers extensive multi-vendor 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 centralized to distributed environments.

Advanced Policy Management

Enforcement and visibility for wired and wireless

With ClearPass, organizations can deploy wired or wireless using standards-based 802.1X enforcement for secure authentication. ClearPass also supports MAC address authentication for IoT and headless devices that may lack support for 802.1X. For wired environments where RADIUS based authentication cannot be deployed, OnConnect, offers an alternative using SNMP based enforcement.

Authentication methods can be used to concurrently support a variety of use-cases. It also includes support for multi-factor authentication based on log-in 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

ClearPass Onboard provides automated provisioning of any Windows, macOS, iOS, Android, Chromebook, and Ubuntu devices via a user driven self-guided portal. Network details, security settings and unique device identity certificates are automatically configured on authorized devices. Cloud identity services like Microsoft Azure Active Directory, Google G Suite and Okta can also be leveraged as identity providers with Onboard for secure certificate enrollment.

Device health checks

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

Customizable Visitor Management

ClearPass Guest simplifies visitor workflow processes to enable employees, receptionists, and other non-IT staff to create temporary guest accounts for secure wireless and wired access. Highly customizable, mobile friendly portals provide easy-to-use login processes that include self-registration, sponsor approval, and bulk credential creation support any visitor needs ### enterprise, retail, education, large public venue. Credentials can be delivered by SMS, email, printed badges, or input directly through cloud identity providers such as Facebook or Twitter.

Built in support for commercial oriented guest Wi-Fi hotspots with credit card billing and 3rd party advertising driven workflows make it simple to integrate into a wide variety of environments.

Overview

Aruba 360 Security Exchange Program

Integrate with security and workflow systems

Support for the Aruba 360 Security Exchange Program is an integrated component of ClearPass. Using features like REST-based APIs, RADIUS Accounting Proxy, and Syslog ingestion help facilitate workflows with EMM/MDM, SIEM, firewalls, help-desk systems and more. Context is shared between each component for end-to-end policy enforcement and visibility.

The ClearPass Ingress Event Engine provides 3rd party systems the means to share information in real-time using Syslog. This enables ClearPass to respond to changing threats for users and devices after they have authenticated to the network. By utilizing an open dictionary approach, anyone can write a parsing ruleset without the need for costly add-ons or locked in 3rd party ecosystems.

Advanced Reporting and Alerting

ClearPass Insight provides advanced reporting capabilities via customizable reports. Information about authentication trends, profiled devices, guest data, on-boarded devices, and endpoint health can also be viewed in an easy to use dashboard. Insight also has support for granular alerts and a watchlist to monitor specific authentication failures.

Specifications

Appliances

ClearPass is available as hardware or as a virtual appliance.

Virtual appliances are supported on VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, CentOS KVM & Amazon EC2.

- VMware ESXi 5.5 up to 6.5 Update 1
- Microsoft Hyper-V 2012/2016 R2 and Windows 2012/2016 R2 Enterprise
- KVM on CentOS 6.6, 6.7 and 6.8
- Amazon EC2

Platform

- 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, and un-managed devices
- Admin/operator access security via CAC and TLS certificates

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
- OAuth2
- Windows machine authentication
- SMB v2/v3
- 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

Overview

- MySQL, Microsoft SQL, PostGRES and Oracle 11g ODBC-compliant SQL server
- Token servers
- Built-in SQL store, static hosts list
- Kerberos
- Microsoft Azure Active Directory
- Google G Suite

RFC standards

- 2246, 2248, 2407, 2408, 2409, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3576, 3579, 3580, 3748, 3779, 4017, 4137, 4301, 4302, 4303, 4308, 4346, 4514, 4518, 4809, 4849, 4851, 4945, 5216, 5246, 5280, 5281, 5282, 5755, 5759, 6818, 6960, 7030, 7296, 7321, 7468, 7815, 8032, 8247

Internet drafts

- Protected EAP Versions 0 and 1, Microsoft CHAP extensions, dynamic provisioning using EAP-FAST, TACACS+, draft-ietf-curdle-pkix-00 EdDSA, Ed25519, Ed448, Curve25519 and Curve448 for X.509, draft-nourse-scep-23 (Simple Certificate Enrollment Protocol)

Profiling methods

- Active: Nmap, WMI, SSH, SNMP
- Passive: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, 'SPAN' Port, HTTP User-Agent, IF-MAP
- Integrated & 3rd Party: Onboard, OnGuard, ArubaOS, EMM/MDM, Rapid7, Cisco device sensor

IPv6 Support

- 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

Information assurance validations

- FIPS 140-2 - Certificate #2577
-

Configuration

Ordering Guidance

Please refer to the ClearPass Scaling & Ordering Guide for detailed information on appropriate sizing and required licensing to deploy ClearPass. This can be found on the Aruba support website in the [ClearPass documentation section](#).

Ordering Information

Description	Part Number
Hardware Appliances	
Aruba ClearPass C1000 S-1200 R4 HW-Based Appliance	JZ508A
Aruba ClearPass C2000 DL20 Gen9 HW-Based Appliance	JZ509A
Aruba ClearPass C3000 DL360 Gen9 HW-Based Appliance	JZ510A
Virtual Appliances	
Aruba ClearPass Cx000V VM-Based Appliance E-LTU	JZ399AAE
Power Supplies	
Aruba ClearPass DL20 Spare Power Supply	JX923A
Aruba ClearPass-Airwave DL360 500W Spare Power Supply	JX922A
Software Licenses*	
ClearPass Access– 802.1X, MAC-Auth, Guest, TACACS+, OnConnect, Endpoint Profiling & ClearPass Exchange (Licensed per maximum number of endpoints concurrently connected per day)	
ClearPass OnBoard – Network details, security settings and unique device identity certificates (Licensed per maximum number of users with active certificates)	
ClearPass OnGuard – Endpoint device health (Licensed per number of endpoints using OnGuard per day)	
Warranty	
1 year parts**	Hardware
90 days**	Software

*Software licenses are available in the following increments: 100, 500, 1,000, 2,500, 5,000, and 10,000

** Extended with support contract

Technical Specifications

	C1000 Appliance (JZ508A)	C2000 Appliance (JZ509A)	C3000 Appliance (JZ510A)
Hardware Model	Unicom S-1200 R4	HPE DL20 Gen 9	HPE DL360 Gen 9
CPU	(1) Eight Core 2.4GHz Atom C2758	(1) Xeon 3.5Ghz E3-1240v5 with Four Cores (8 Threads)	(2) Xeon 2.4GHz E5-2620_V3 with Six Cores (12 Threads)
Memory	8 GB	16 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
Out of Band Management	N/A	HPE Integrated Lights-Out (iLO) Standard	HPE Integrated Lights-Out (iLO) Advanced
Serial Port	Yes (RJ-45)	Yes (Virtual Serial via iLO)	Yes (DB-9)
Performance & Scale	Please refer to the ClearPass Scaling & Ordering Guide	Please refer to the ClearPass Scaling & Ordering Guide	Please refer to the ClearPass Scaling & Ordering Guide
Form Factor			
Dimensions (WxHxD)	17.2" x 1.7" x 11.3"	17.11" x 1.70" x 15.05"	17.1" x 1.7" x 27.5"
Weight (Max Config)	8.5 Lbs	Up to 19.18 Lbs	Up to 33.3 Lbs
Power			
Power supply	200 watts max	HPE 900W AC 240VDC Power Input FIO Module*	HPE 500W Flex Slot Platinum Hot Plug Power Supply
Power redundancy	N/A	Optional	Optional

Technical Specifications

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	Random vibration at 0.000075 G ² /Hz, 10Hz to 300Hz, (0.15 G's nominal)	Random vibration at 0.000075 G ² /Hz, 10Hz to 300Hz, (0.15 G's nominal)
Operating shock	1 shock pulse of 20 G for up to 2.5 ms	2 G's	2 G's
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)	3,050 m (10,000 ft)	3,050 m (10,000 ft)

*The HPE 900W Redundant Power Supply supports 100VAC to 240VAC and also supports 240VDC..

Summary of Changes

Date	Version History	Action	Description of Change
18-Dec-2017	From Version 3 to 4	Changed	Minor edit on Configuration section
04-Dec-2017	From Version 2 to 3	Added	SKUs added: JZ508A, JZ509A, JZ510A, JZ399AAE, JX923A
		Changed	All document sections updated
07-Nov-2016	From Version 1 to 2	Added	SKUs added: JW771A, JW772A
01-Nov-2016	Version 1	Created	Document creation.



Sign up for updates



© Copyright 2017 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

To learn more, visit: <http://www.hpe.com/networking>

c05272683 - 15701 - Worldwide – V4 - 18-December-2017