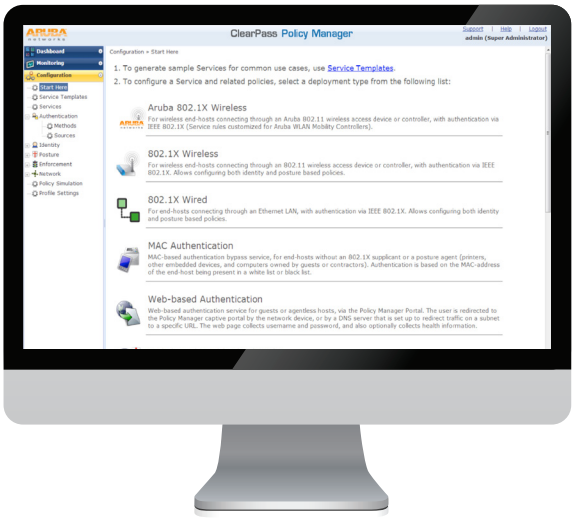
产品说明书

ARUBA CLEARPASS POLICY MANAGER

现有最先进的策略管理平台



Aruba ClearPass Policy Manager 平台跨任意多供应商的有线、无线和 VPN 基础设施，为员工、合同工和访客提供基于角色和设备的网络访问控制。

通过基于具体环境的内置策略引擎、RADIUS、TACACS+ 协议支持、设备分析和全面的安全状况评估、登录以及访客接入选项，ClearPass 无可匹敌的功能使其能够为任意机构打造网络安全平台。

为了实现更广泛的安全覆盖，通过使用防火墙、EMM 和其他现有解决方案，ClearPass Exchange 实现了与第三方安全和 IT 系统之间的自动化威胁防护和工作流，而这以前都需要手动 IT 干预。

此外，为了方便最终用户，ClearPass 支持安全自助服务功能。用户可以针对企业使用或互联网访问安全地配置自己的设备。Aruba 无线客户可以为支持 AirPlay、AirPrint、DLNA 和 UPnP 的设备提供注册，用于分享功能。

由此可以得到全面且可扩展的策略管理平台，其功能远超传统 AAA 解决方案，可以针对 IT 拥有和自带设备 (BYOD) 安全要求提供广泛的实施功能。

主要特色

- 针对多供应商 Wi-Fi、有线和 VPN 网络的基于角色的网络访问权限实施。
- 行业领先的性能、可扩展性、高可用性和负载平衡。
- 直观的策略配置模板和监控故障排除工具。
- 支持一个服务中的多种身份验证/授权来源（AD、LDAP、SQL dB）。
- 自助服务设备登录，具备适用于 BYOD 的内置证书颁发机构 (CA)
- 访客接入功能，具备全面的定制、品牌和基于发起人的审批方法。
- 支持 NAC 和 EMM/MDM 集成，用于移动设备评估。
- 与 SIEM、互联网安全性和 EMM/MDM 第三方系统的全面集成。
- 通过 SAML v2.0 的单点登录 (SSO) 和 Aruba 自动登录支持。
- 先进的报告功能，可以报告所有用户的有效身份证明和失败。
- 使用 DHCP 和 TCP 指纹的内置分析。
- 面向 ESXi 和 Hyper-V 设备的硬件和虚拟支持。
- 自动集群升级

CLEARPASS 的与众不同之处

ClearPass Policy Manager 是唯一一款面向所有行业，在各个层面实施企业级移动性和 NAC 的策略解决方案。细粒度网络访问实施基于用户的角色、设备类型和角色、身份验证方法、EMM/MDM 属性、设备健康状况、位置和一天中的时间。

ClearPass 具备前所未有的互操作性，提供了广泛的多供应商无线、有线和 VPN 基础设施支持，使得 IT 可以轻松地跨任意环境推出安全移动策略。

部署可扩展性支持上万台设备及身份验证，将旧式 AAA 解决方案提供的功能远远抛在身后。不论企业规模大小，也不论是本地环境还是分布式环境，都有合适的选项。

INSIGHT 提供的高级报告和警报功能

Policy Manager 包括高级报告功能，提供了可定制的面板，用于身份验证、端点分析、行业标准，以及访客、登录和设备健康状况等其他信息，所有这些都在一个可快速查看的面板中。InSight 还包括细粒度警报功能。

高级策略管理

员工访问

ClearPass Policy Manager 提供基于角色和设备的身份验证，这些验证基于 802.1X、MAC 验证和 Web 门户访问方法。可以使用并行身份验证方法来支持各种使用案例。还可以包括对基于登录时间、安全状况检查和其他具体环境信息（例如新用户、新设备等）的多重身份验证的支持。

来自跨域的 Microsoft Active Directory、LDAP 兼容目录、ODBC 兼容 SQL 数据库、令牌服务器和内部数据库的多种身份存储可以用于单个策略中，实现精细控制。

内置分析服务可搜索和分类所有网络元件，包括交换机、控制器和传统互连端点（智能手机、平板电脑等），同时允许自行定义用于非传统端点但对物联网 (IoT) 和其他无外设设备至关重要的网络元件，例如 IP 摄像机、电话和打印机。来自这些已建档设备的具体环境数据使得 IT 可以定义哪些设备可以访问有线、VPN 或是无线网络。

设备配置文件更改可用于动态修改授权权限。例如，如果 Windows 笔记本电脑显示为打印机，则 ClearPass 策略可以自动撤消或拒绝访问。

个人设备上的安全设备配置

ClearPass Onboard 为任意 Windows、Mac OS X、iOS、Android、Chromebook 和 Ubuntu 设备提供了通过用户驱动的自动导向门户进行自动化预配。自动在已授权设备上配置所需的 SSID、802.1X 设置以及安全证书。

可定制的访客管理

ClearPass Guest 简化了工作流程，这样前台接待人员、员工和其他非 IT 员工可以创建临时访客帐户，用于安全 Wi-Fi 和有线互联网接入。自行注册、发起人和批量凭据创建等功能可以支持企业、零售商、教育以及大型公共场所等任何类型的访客接入需求。

设备健康状况检查

ClearPass OnGuard 利用 OnGuard 的永久和临时代理，在无线、有线和 VPN 连接上执行高级端点安全状况评估。OnGuard 健康检查功能确保了合规性和网络安全，然后才允许设备连接。

其他策略管理功能

与安全和工作流系统集成

ClearPass Exchange 互操作性包括基于 REST 的 API，以及往返于 ClearPass 上的按需系统日志事件流转发，可用于协调与 MDM、SIEM、防火墙 PMS、呼叫中心、管理系统等的工作流。具体环境信息在各个组件之间共享，实现端到端的策略实施和监控。

只需连接，工作应用程序即刻可用

ClearPass 自动登录功能使得在移动设备上访问工作应用程序空前简单。有效的网络身份验证可以自动将用户连接到企业移动应用程序，这样用户就可以立即开展工作。

单点登录 (SSO) 支持用于 Ping、Okta 和其他身份管理工具，改善用户在基于 SAML 2.0 的应用程序上的体验。

规格

ClearPass Policy Manager 设备

ClearPass Policy Manager 以硬件设备或虚拟设备的形式提供，支持 500、5,000 和 25,000 台通过身份验证的设备。支持 VMware ESX/i 和 Microsoft Hyper-V 的虚拟设备。

- ESX 4.0，ESXi 4.1，最高 6.0
- Hyper-V 2012 R2 和 Windows 2012 R2 Enterprise

虚拟设备，以及所有硬件设备，可以部署在活动/活动集群中，用于提升可扩展性和冗余度。

平台

- 内置 AAA 服务 – RADIUS、TACACS+ 和 Kerberos
- Web、802.1X、非 802.1X、RADIUS 身份验证和授权
- 高级报告、分析和故障排除工具
- 外部强制网络门户，重定向到多供应商设备
- 交互式策略模拟和监视模式实用工具
- 多设备注册门户 – Guest、Aruba AirGroup、BYOD、不受管设备
- 针对任意网络类型、身份存储和端点的部署模板
- 通过 CAC and TLS 证书实现管理员/操作员访问权限安全性
- IPSec 隧道

框架和协议支持

- RADIUS、RADIUS CoA、TACACS+、Web 身份验证、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 和 2, EAP-MD5
- NAC, Microsoft NAP
- Windows 计算机身份验证
- MAC 验证
- 审计（基于端口的规则和漏洞扫描）
- 在线证书状态协议 (OCSP)
- SNMP 通用 MIB，SNMP 专用 MIB
- 通用事件格式 (CEF)，日志事件扩展格式 (LEEF)

TLS 1.2

支持的身份存储

- Microsoft Active Directory
- RADIUS
- 任意 LDAP 兼容目录
- 任意 ODBC 兼容 SQL Server
- 令牌服务器
- 内置 SQL 存储，静态主机列表
- Kerberos

RFC 标准

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

互联网草案

- 受保护的 EAP 版本 0 和 1，Microsoft CHAP 扩展，使用 EAP-FAST 的动态预配，TACACS+

信息保障验证

- FIPS 140-2 – 证书 #2577

分析方法

- DHCP，TCP，MAC OUI，ClearPass Onboard，SNMP，Cisco 设备传感器

	ClearPass Policy Manager-500	ClearPass Policy Manager-5K	ClearPass Policy Manager-25K
设备规格			
CPU	(1) 八核 2.4GHz Atom C2758	(1) 四核 Xeon 3.4 GHz E3-1231_V3	(2) 六核 Xeon 2.4GHz E5-2620_V3
内存	8 GB	8 GB	64 GB
硬盘驱动器存储	(1) SATA (7.3K RPM) 1TB 硬盘驱动器	(2) SATA (7.2K RPM) 1TB 硬盘驱动器，RAID-1 控制器	(6) SAS (10K RPM) 600GB 热插拔硬盘驱动器，RAID-10 控制器
设备可扩展性			
最大端点数	500	5,000	25,000
形状因数			
尺寸（长x高x宽）	17.2 x 1.7 x 11.3 英寸	17.09 x 1.67 x 15.5 英寸	18.98 x 1.68 x 27.57 英寸
重量（最高配置）	8.5 磅	16.97 磅	最高 37 磅
电源			
电源	最高 200W	最高 250W	最高 750W
电源冗余	N/A	N/A	可选
AC 输入电压	100/240 VAC 自动选择	100/240 VAC 自动选择	100/240 VAC 自动选择
AC 输入频率	50/60 Hz 自动选择	50/60 Hz 自动选择	50/60 Hz 自动选择
环境			
工作温度	5° C 到 35° C（41° F 到 95° F）	10° C 到 35° C（50° F 到 95° F）	10° C 到 35° C（50° F 到 95° F）
工作震动	5 Hz 到 200 Hz 下，0.25 G 15 分钟	5 Hz 到 350 Hz 下，0.26 G 15 分钟	5 Hz 到 350 Hz 下，0.26 G 15 分钟
工作冲击	1 次最高 2.5 毫秒内 20 G 的冲击	1 次最高 2.6 毫秒内 31 G 的冲击	1 次最高 2.3 毫秒内 40 G 的冲击
工作高度	-16 米到 3,048 米（-50 英尺到 10,000 英尺）	-16 米到 3,048 米（-50 英尺到 10,000 英尺）	-16 米到 3,048 米（-50 英尺到 10,000 英尺）

* 虚拟设备规模必须与硬件设备规格相符

产品说明书
ARUBA CLEARPASS POLICY MANAGER

订购指南

订购 ClearPass Policy Manager 涉及到以下步骤：

1. 确定环境中通过身份验证的端点/设备数量。此外还提供可选功能，例如每日访客数、配置为企业用途的 BYO 设备总数以及需要健康状况检查的计算机总数。
2. 根据您的部署需要身份验证的设备和访客总数，选择合适的平台（虚拟或硬件设备）规模。

订购信息	
部件号	**说明**
CP-HW-500 或 CP-VA-500	Aruba ClearPass Policy Manager 500 硬件平台，支持最高 500 台通过验证的设备
CP-HW-5K 或 CP-VA-5K	Aruba ClearPass Policy Manager 5K 硬件平台，支持最高 5,000 台通过验证的设备
CP-HW-25K 或 CP-VA-25K	Aruba ClearPass Policy Manager 25K 硬件平台，支持最高 25,000 台通过验证的设备
可扩展应用程序软件*	
ClearPass Onboard – 设备配置和证书管理	
ClearPass OnGuard – 端点设备健康状况	
ClearPass Guest – 访客接入管理	
质保	
硬件	1 年期部件/人工保修**
软件	90 天**

* 可扩展应用程序软件按以下增量提供：100、500、1,000、2,500、5,000、10,000、25,000、50,000 和 100,000。

** 可根据支持合同延长

a Hewlett Packard Enterprise company

www.arubanetworks.com

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