W-ClearPass Access Management System

Real-time network access security and endpoint control for BYOD

The W-ClearPass Access Management System provides role- and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure.

Built-in RADIUS, TACACS+, profiling, onboarding, guest access and health checks – plus the ability to leverage third-party mobile device management solutions – ensure seamless policy enforcement across the entire network.

Centrally-managed network access policies provide the comprehensive authentication capabilities that are required for today's highly mobile workforce, regardless of device type or device ownership.

Automated services let users securely onboard their own devices, register AirPlay- and AirPrint-enabled devices for sharing, and create guest access credentials.

The result is a consistent and scalable network access control solution that exceeds bring-your-own-device (BYOD) and ITmanaged device security requirements.

The Clearpass Difference

The W-ClearPass Access Management System is the only network access control solution that centrally enforces all aspects of BYOD 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 and wired networking equipment which enables IT to easily rollout BYOD across any infrastructure.

With flexible deployment options, IT can start by providing sponsored guest access and also allow employees to onboard their own devices, and later add device profiling and application management. ClearPass is capable of scaling to support tens of thousands of devices and users.

Key features

- Role-based network access enforcement for 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 and Microsoft NAP posture and health checks.
- Single sign-on (SSO) and federated identity via SAML and Okta support.
- Advanced reporting of all user activity, authentications and failures.
- Comprehensive API integration with third-party MDM solutions.
- Device onboarding, profiling, guest access, and compliance reporting all included.

Unprecedented Simplicity

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

A simple-to-use template-based interface provides an efficient way to create network access and authentication services, regardless of the identity store currently in use, authentication method or enforcement model.

W-ClearPass Access Management System is also a valuable security operations and troubleshooting system that delivers unprecedented visibility to quickly identify network issues, and policy and security vulnerabilities.

Advanced Policy Management

Employee access

The Access Management System provides 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, and EAP-TTLS 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 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.

Mobile device and application management

The ClearPass MDM Connector makes it easy to use attributes collected by third-party MDM solutions to enforce network policies. A device can be denied Wi-Fi access if it is jailbroken, running blacklisted apps or if the owner does not appear in an authorization database.

Handling 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.

Built-in ClearPass profiling ensures that these devices are accurately fingerprinted and match the characteristics on subsequent profiling scans. Policies can be tailored to provide full or limited access to secure resources.

Secure device provisioning

ClearPass with Onboard fully automates the provisioning of any Windows, Mac OS X, iOS, and Android devices via a built-in captive portal. Users are re-directed to a template based interface to provision required SSID, 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 with Guest simplifies workflow processes, allowing receptionists, employees and other non-IT staff to create temporary accounts for Wi-Fi and wired network access.

Once registered, users receive account login credentials via SMS text messages or email. Guest network access accounts can be set to expire automatically after a specific number of hours or days.

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 with OnGuard and 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

Built-in device profiling

ClearPass is the only 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 also used to identify device profile changes and to dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, Access Management System can automatically deny access.

Extensive captive portal support

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

Also, built-in web-based device registration services let users self-register their devices, such as Apple Bonjour capable devices, game consoles, and other personal devices to automatically capture MAC address, device type and operating system version for IT.

W-ClearPass Access Management System appliances

The W-ClearPass Access Management System is available as hardware or virtual appliances that support 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 and 5.0.

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

W-ClearPass Access Management System

Specifications

Access Management System ClearPass Policy Manager

- Comprehensive identity-based policy engine.
- Posture agents for Windows, Mac OS X, Linux operating systems.
- Built-in AAA services – RADIUS, TACACS+, 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 – Access Management System AirGroup and unmanaged devices.

Framework and Protocol Support

- RADIUS, RADIUS CoA, TACACS+, web authentication
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1 and 2, EAP-MD5
- Wireless, wired, and VPN 802.1X
- 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 identity store
- Built-in static hosts list

RFC Standards

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

Internet Drafts

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

Appliance Specifications

	Access Management System-500	Access Management System-5000	Access Management System-25000
CPU	(1) Dual Core Pentium	(1) Quad Core Xeon	(2) Quad 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	(4) 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 (W x H x D)	16.8" x 1.7" x 14"	17.53" x 1.7" x 26.17"	17.53" x 1.7" x 26.17"
Weight (max config)	14 Lbs	39 Lbs	39 Lbs
Power			
Power consumption (maximum)	260 watts max	250 watts max	717 watts max
Power supply	Single	Single	Dual hot-swappable (optional)
AC input voltage	110/220 VAC auto-selecting	110/220 VAC auto-selecting	110/220 VAC auto-selecting
AC input frequency	50/60 Hz auto-selecting	50/60 Hz auto-selecting	50/60 Hz auto-selecting
Environmental			
Operating temperature	10º C to 35º C (50º F to 95º F)	10º C to 35º C (50º F to 95º F)	10º C to 35º C (50º F to 95º 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 Access Management System involves the following steps:

1. Determine the number of authenticated endpoints/devices in your environment. Additionally, select additional functionality, such as guests per day, total BYO devices being onboarded, 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	Access Management System 500 hardware platform supporting a maximum of 500 authenticated devices
CP-HW-5K or CP-VA-5K	Access Management System 5K hardware platform supporting a maximum of 5,000 authenticated devices
CP-HW-25K or CP-VA-25K	Access Management System 25K hardware platform supporting a maximum of 25,000 authenticated devices
Expandable application software*	
ClearPass Onboard – device onboarding and 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

*Select Dell Networking products carry an Extended Life Warranty with Basic Hardware Service. Warranty covers repair or replacement of the product for as long as it remains in use by the customer. In the event of discontinuance of product manufacture, Dell Extended Life Warranty extends until five (5) years after end of product model sales. Warranty limits any power supply, antennae or accessories to one (1) year from date of purchase. Warranty does not include troubleshooting, configuration, or other advanced service provided by Dell ProSupport.The Extended Life Limited Hardware Warranty is not transferrable. For more information see dell.com/warranty.

Learn more at Dell.com/Networking

November 2013 | Version 2.1
Dell_Networking_W-ClearPass Access Management System_Spec_Sheet