

## DATA SHEET

## CLEARPASS ONBOARD

A ClearPass Policy Manager Application

# Automated mobile device provisioning and configuration for secure BYOD

ClearPass Onboard automatically configures and provisions mobile devices – Windows, Mac OS X, iOS, Ubuntu, Chromebook and Android 2.2 and above – enabling them to securely connect to enterprise networks in support of BYOD initiatives.

Employees, contractors and partners are automatically given permission to self-configure their own devices. The ClearPass Onboard portal dynamically detects a device's operating system and guides the user through the appropriate configuration package.

This provides an incredibly simple way to configure wireless, wired and VPN settings, apply unique per device certificates and profiles, and ensure that users can securely connect their devices to 802.1X- enabled networks with minimal IT interaction.

ClearPass Onboard also increases the amount of usable data for troubleshooting, user- and device-based policies, and collected compliance reporting per each device.

The result is a streamlined workflow that allows IT helpdesk personnel to efficiently automate multiple processes that are required to successfully carry out BYOD initiatives while improving the user experience.

### THE CLEARPASS ADVANTAGE

With the industry's most advanced auto-provisioning features, onboarding thousands of devices is amazingly simple via integrated policy management, customizable user-facing portal, and built-in CA.

#### Automated policy management

With ClearPass, IT can use profiling data collected during onboarding to enforce device categorization and role-based network access policies. Centrally-defined policies also limit the types of devices that can be onboarded and which users can onboard them.

#### **KEY FEATURES**

- Enables users to self-register and securely onboard multiple devices
- Supports Windows, Mac OS X, iOS, Android, Chromebook and Ubuntu operating systems
- Automates the configuration of network settings for wired and wireless endpoints
- Unique provisioning and revocation of devicespecific credentials
- · Contains built-in certificate authority
- Uses profiling to identify device type, manufacturer and model
- Provides BYOD visibility and centralized policy management capabilities

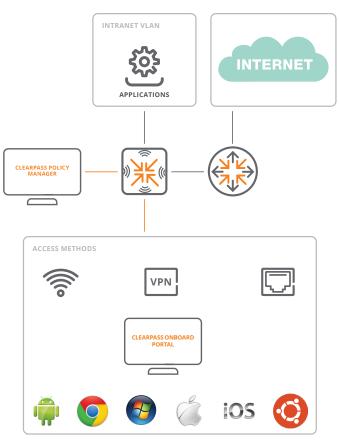


figure 1.0\_09.26.14\_cp-onboard-ds

ClearPass Onboard lets users securely configure their own smartphones, tablets and laptops.

APUBA networks	ClearPass Onboard		Support   Help   Logout admin (IT Administrators)
Guest O	Onboard * Network Settings Network Settings		
<ul> <li>Start Here</li> <li>Applications</li> </ul>	Use this form to make changes to the network settings that will be sent to a provisioned device.		
Certificate Authority Sett	🕹 Access 🦞 P	Network Settings » Network Access	
	Network Access Options for basic netwo		
	* Name:	Example Network Enter a name for the network that will be shown to the user.	
	Enabled:	Provision the network profile Select this option to include this network in the device profile.	
	Description:	Connect to the example network.	E
	* Network Type:	Wireless only Select which types of network will be provisioned. Enterprise security (802.1X) will be selected if wired networks are to be supported.	
	* Security Type:	Enterprise (802.1X) Select the authentication method used for the network. Enterprise security (802.1X) will be selected if wired networks are to be supported.	
	Wireless Network Settings Options for wireless network access.		
	* Security Version:	WPA2 with AES (recommended) Select the WPA encryption version for the wireless network. This setting is used for Windows, Android and Legacy OS X (10.5/6) devices only. IOS and OS X 10.7+ (Lion or later) devices audo-detect the WPA version.	
	* SSID:	Example-TLS Enter the SSID of the wireless network to connect to.	
	Wireless:	Hidden network Select this option if the wireless network is not open or broadcasting.	
	Auto Join:	Automatically join network Select this option to automatically join the wireless network.	
Configuration O		Next Save Changes Cancel	

ClearPass Onboard administrator interface features customizable settings per network type.

#### Customized device provisioning

A centrally managed administrator portal allows IT to configure device certificates and trust details, network access, VPN, and health check settings, and authentication protocols for wireless and wired networks.

The IT staff can also define the number of devices that can be onboarded per user and how long their certificates are valid.

#### **ADVANCED ONBOARDING CAPABILITIES**

#### Managing unique device credentials

The distribution of published device credentials through ClearPass Onboard's built-in CA safeguards organizations that want to adopt BYOD initiative's without requiring the implementation of an external certificate authority. ClearPass Onboard leverages the certificate authority within the Policy Manager platform to publish unique certificates that also include specific user and device data.

ClearPass also supports the distribution of Onboard generated certificates requested by third-party applications – mobile device management (MDM) or enterprise mobility management (EMM) – through SCEP and EST (RFC 7030) protocols.

Details about 1	e Details the certificate and its owner.		
Issued To:	💱 kaveh		
Valid From:	Wednesday, 24 October 2012, 10:36 AM		
Valid To:	S Thursday, 24 October 2013, 11:06 AM		
Subject:	Country US		
	State California		
	Locality Sunnyvale		
	Organization Example Organization		
	Common Name kaveh		
	mdpsDeviceType iOS		
	mdpsDeviceUdid cf3baa22372a497013b94e82e0263a47e39b92e		
	mdpsDeviceImel 01 321200 804473 3		
	mdpsProductName iPad3.3		
	mdpsProductVersion 10A403		
	mdpsUserName kaveh		
	mdpsDeviceSerial DMPHV6ZUDVGG		
Issuer De	tails the certificate authority that issued the certificate.		
	ClearPass Onboard Local Certificate Authority (Signing)		
	🔝 ClearPass Onboard Local Certificate Authority (Signing)		
	ClearPass Onboard Local Certificate Authority (Signing) Country US		
	ClearPass Onboard Local Certificate Authority (Signing) Country US State California		
Issued By:	ClearPass Onboard Local Certificate Authority (Signing) Country US		
Issued By:	ClearPass Onboard Local Certificate Authority (Signing) Country US State California Locality Sunnyvale		
Issued By: Issuer: Advanced	ClearPass Onboard Local Certificate Authority (Signing) Country US State California Locality Sunnyvale Organization Aruba Networks Common Name ClearPass Onboard Local Certificate Authority (Signing)		
Issued By: Issuer: Advanced	ClearPass Onboard Local Certificate Authority (Signing) Country US State California Locality Sunnyvale Organization Aruba Networks Common Name ClearPass Onboard Local Certificate Authority (Signing)		

#### **Revocation of unique credentials**

Easy-to-use search and menu-driven capabilities ensure the rapid revocation and deletion of certificates for specific mobile devices if a user leaves an organization or the mobile device is lost or stolen.

Supported EAP methods:

- PEAP EAP-MSCHAPv2
- EAP-TLS

## **ORDERING GUIDANCE**

ClearPass Onboard can be ordered via perpetual license or subscription that includes ArubaCare for the length of the subscription. Available Enterprise options provide the ability for organizations to flexibly use the licenses for ClearPass Onboard, Guest or OnGuard.

Ordering ClearPass Onboard involves the following three steps:

- 1. Determine the number of unique endpoints that users will provision within your environment.
- Select the total number of Onboard Part Numbers.
   Anything over the capacity of a base appliance will require the purchase of a second Policy Manager appliance.
- 3. Choose the appropriate ClearPass Policy Manager hardware or virtual appliances to accommodate the total number from above.

Example – To support the provisioning of 2000 total devices, ensure that the Policy Manager platform is sized to accommodate the 2000 devices and any other endpoints that will authenticate via 802.1X, MAC auth, etc.

Purchase the following:

- ClearPass Hardware Appliance CP-HA-5K
- ClearPass Onboard 2 X LIC-CP-OB-1K

Additional Onboard capacity can be purchased at any time to meet growth demands.

## **ORDERING INFORMATION\***

Part Number	Description
LIC-CP-OB-100	Onboard for Aruba ClearPass Policy Manager – 100 endpoints
LIC-CP-OB-500	Onboard for Aruba ClearPass Policy Manager – 500 endpoints
LIC-CP-OB-1K	Onboard for Aruba ClearPass Policy Manager – 1,000 endpoints
LIC-CP-OB-2500	Onboard for Aruba ClearPass Policy Manager – 2,500 endpoints
LIC-CP-OB-5K	Onboard for Aruba ClearPass Policy Manager – 5,000 endpoints
LIC-CP-OB-10K	Onboard for Aruba ClearPass Policy Manager – 10,000 endpoints
LIC-CP-OB-25K	Onboard for Aruba ClearPass Policy Manager – 25,000 endpoints
LIC-CP-OB-50K	Onboard for Aruba ClearPass Policy Manager – 50,000 endpoints
LIC-CP-OB-100K	Onboard for Aruba ClearPass Policy Manager – 100,000 endpoints
Enterprise Perpetual Part Number	
LIC-CP-EN-xxx*	Enterprise license for ClearPass Policy Manager
<b>Onboard Subscription Part Numbers</b>	
SUB1-CP-OB-xxx*	1 Year Onboard Subscription License for ClearPass Policy Manager
SUB3-CP-OB-xxx*	3 Year Onboard Subscription License for ClearPass Policy Manager
SUB5-CP-OB-xxx*	5 Year Onboard Subscription License for ClearPass Policy Manager
Enterprise Subscription Part Number	5
SUB1-CP-EN-xxx*	1 Year Enterprise Subscription License for ClearPass Policy Manager
SUB3-CP-EN-xxx*	3 Year Enterprise Subscription License for ClearPass Policy Manager
SUB5-CP-EN-xxx*	5 Year Enterprise Subscription License for ClearPass Policy Manager
Warranty	
Software	90 days**

\* Subscription and enterprise licenses can be purchased in 1-, 3- or 5-year increments for 100, 500, 1,000, 2,500, 5,000, 10,000, 25,000, 50,000, and 100,000 endpoints

\*\* Extended with support contract



For more information, contact one of our Howard Medical representatives:

36 Howard Drive | Ellisville, MS 39437 877.856.6441 | Fax: 601.399.5060 | www.howard-medical.com