April 2012 ClearPass Policy Manager Software Release

New features added in this release

- **ClearPass Profile** – Aruba's ClearPass Profile is a software module designed to provide automated profiling for each device that accesses a network running the ClearPass Policy Manager (CPPM) platform. By capturing and storing unique characteristics of all endpoints. The ClearPass solution ensures that endpoint attributes are consistently fingerprinted for validity upon authentication, which allows IT administrators to use this data to enforce granular and accurate access privileges based on device categories.

- **Support for Multiple Active Directory Domains:** ClearPass Policy Manager can now be joined to multiple Active Directory domains that do not share a trust relationship. This allows the Policy Manager to authenticate users from multiple ADs. For example, after two companies merge and retain separate AD domains for an indefinite amount of time.

- **Policy Manager Zones:** CPPM shares a distributed cache that consists of:

    - runtime state such as role and posture of connected entities
    - connection status of all endpoints running ClearPass OnGuard
    - and endpoint details gathered by Profile, across all nodes in a cluster

  CPPM uses this information to make policy decisions across multiple transactions. In a deployment where a cluster spans WAN boundaries and multiple geographic zones, it is not necessary to share all of this runtime state across all nodes in the cluster. Zones can be defined to restrict the sharing of such runtime information.

- **Granular Multilevel Administration:** CPPM now supports full role based granular control of Read, Write and Delete operations from the administration UI and the configuration API.

- **Modified Service Creation Workflow:** Authorization, Audit, and Posture steps are now optional within the service creation workflow. These can be turned on for more advanced use cases.

- **Custom tags:** Administrators can now create custom tags, which can be assigned to entities such as endpoints, network devices, and domain and guest users. Custom tags allow administrators to specify policies based on arbitrary attributes associated with these different entities. For example, Endpoint Status for an endpoint.

ClearPass OnGuard

New Features added in this release

- New Windows health checks
  - Detection of VM clients
  - Detection of bridged interfaces

Known issues with this release

1. Upgrading ClearPass Policy Manager from version 5.0.1 to 5.1.0 does not migrate the existing OnGuard License.
   Workaround: Copy the OnGuard license installed on version 5.0.1 and re-use that license after upgrading to version 5.1.

2. You cannot join a subscriber to a cluster if the cluster password on the Publisher contains special characters such as the '$' character

3. Joining a subscriber to a cluster fails if "Restore local database after this operation" is selected.

4. Dissolvable agent does not collect health data on 64-bit Java 7 versions on Windows 64 bit operating systems.

5. Online Help documentation for the 5.1 release will be available in the first service release in mid May

6. The ActiveSync plugin for the Profile module will be available in the first service release of 5.1 in mid May

7. ClearPass Profile: You can only configure a single CPPM node with Profile per Zone. ClearPass Profile does not currently support redundancy within a Zone.

8. RADIUS CoA does not work if NAD groups are associated with an Enforcement Profile.
Workaround: Create multiple Enforcement Policy rules for each NAD group

Known issues with ClearPass OnGuard 5.1 release

1. Upgrading OnGuard from the following versions 3.5/4.0/5.0/5.0.1 to 5.1 will fail if the OnGuard installer is invoked without admin privileges on the client.
   Workaround: Execute the "msciexec/I ClearPassOnGuardInstall.msi" command from the windows command prompt as the Admin user

2. Migration of Posture Policies from earlier versions of ClearPass Policy Manager to 5.1 is not supported.
   Workaround: Please add/configure posture policies on the CPPM again

3. The quarantine messages on the OnGuard agent user interface are not properly formatted for MAC OS X.

4. On Windows XP SP2 operating systems, the OnGuard agent exits when you switch between users on the same machine

5. Support for health checks on Windows 2000 is discontinued with this release

6. Hosted Networks health checks will be supported only on the Windows 7 operating system. This feature is unavailable for Windows XP, Vista, 2003 and2008

7. Disabling of USB storage devices on Windows 2008 Server (64 bit) is not supported

ClearPass USHA

Known issues with ClearPass USHA 5.1 release

1. Wireless or wired end points will not be able to connect to the network with USHA enabled to collect health when the health information payload (SoH /SoHR) size is greater than 800 bytes.

2. Do not install ClearPass OnGuard and ClearPass USHA on the same client. Once installed, uninstallation of either of them can fail.

Aruba Networks
1344 Crossman Avenue
Sunnyvale, CA 94089-1113
Phone: +1-408-227-4500
Fax: +1-408-227-4550