ClearPass 6.2.5

Release Notes

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

About ClearPass 6.2.5

ClearPass 6.2.5 is a monthly patch release that introduces new features and provides fixes to previously outstanding issues. These release notes contain the following chapters:

- Chapter 2, "Upgrade Information" on page 13—Provides upgrade instructions and considerations.
- Chapter 3, "What's New in This Release" on page 15—Describes new features and issues introduced in this 6.2.5 release as well as issues fixed in this 6.2.5 release.
- Chapter 4, "Enhancements in Previous 6.2.x Releases" on page 19—Describes new features introduced in earlier 6.2 releases.
- Chapter 5, "Issues Fixed in Previous 6.2.x Releases" on page 23—Lists issues fixed in previous 6.2 releases.
- Chapter 6, "Known Issues Identified in Previous Releases" on page 33—Lists currently existing issues identified in previous releases.

Supported Browsers

For the best user experience, we recommend you update your browser to the latest version available. Supported browsers for ClearPass are:

- Mozilla Firefox on Windows XP, Windows Vista, Windows 7, and Mac OS
- Google Chrome for Mac OS and Windows
- Apple Safari 3.x and later on Mac OS
- Mobile Safari 5.x on iOS
- Microsoft Internet Explorer 7.0 and later on Windows XP, Windows Vista, Windows 7, Windows 8, and Windows 8.1.

The 6.2.5 patch cannot be uploaded on the Internet Explorer (IE) browser. For details, please see issue #19288 in "New Known Issues in the 6.2.5 Release" on page 17.

IE 10 is supported only in compatibility mode. For details, please refer to http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/compatibility-view.

Microsoft Internet Explorer 6.0 is now considered a deprecated browser. You might encounter some visual and performance issues when using this browser version.

System Requirements

ClearPass Guest and ClearPass Onboard are part of the ClearPass Policy Manager platform. ClearPass comes pre-installed when you purchase an appliance. ClearPass can also be installed on a virtual appliance.

Virtual Appliance Requirements

The following specifications are recommended in order to properly operate Aruba ClearPass Policy Manager in 64-bit VMware ESX or ESXi server environments. To ensure successful deployment and maintain sufficient performance, verify that your hardware meets the following minimum specifications.

ClearPass VMware ships with a 15 GB hard disk volume. This must be supplemented with an additional storage/ hard disk through the VMware's settings by adding a new hard disk before the VM is powered on. The additional space required depends on the ClearPass model purchased. Space requirements are described below.

Supported ESX/ESXi Versions

- 4.0 (Recommended minimum version of software for CP-VA-500 and CP-VA-5K. It does not support greater than 8 virtual CPUs required for the CP-VA-25K.)
- 5.0
- 5.1
- 5.5

CP-VA-500

- 2 Virtual CPUs
- 250 GB disk space (When you upgrade to a later version, a second drive of 250 GB will also be needed)
- 4 GB RAM
- 2 Gigabit virtual switched ports (Only one is needed if you do not use separate ports for data and management traffic)
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

An additional hard disk equal to the size of the new hard disk is required in order to upgrade to future versions. For more information, please refer to the section on upgrading in the Tech Note "Installing or Upgrading on a Virtual Machine".

CP-VA-5K

- 8 Virtual CPUs
- 250 GB disk space (When you upgrade to a later version, a second drive of 250 GB will also be needed)
- 8 GB RAM
- 2 Gigabit virtual switched ports (Only one is needed if you do not use separate ports for data and management traffic)
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

CP-VA-25K

- At least 12 Virtual CPUs (Aruba hardware appliances ship with 24 cores)
- 512 GB disk space (When you upgrade to a later version, a second drive of 512 GB will also be needed)
- At least 24 GB RAM (Aruba hardware appliances ship with 64 GB RAM)
- 2 Gigabit virtual switched ports (Only one is needed if you do not use separate ports for data and management traffic)

- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 350

In order for a CP-VA-25K virtual appliance to properly support up to 25,000 unique authentications with full logging capability, customers should configure additional hardware to match the number of CPUs and RAM that ship in our hardware appliances. If you do not have the VA resources to support a full workload, please consider ordering the ClearPass Policy Manager hardware appliance.

Evaluation version

- 2 Virtual CPUs
- 40 GB disk space
- 4 GB RAM
- 2 Gigabit virtual switched ports (Only one is needed if you do not use separate ports for data and management traffic)

An evaluation version can be upgraded to a later evaluation version in a manner similar to a production upgrade. An evaluation version cannot be upgraded to a production version.

VMware Player is not supported. Please contact Aruba customer support at support@arubanetworks.com with any further questions or if you need additional assistance.

ClearPass OnGuard Unified Agent Requirements

Be sure that your system meets the following requirements before installing the ClearPass OnGuard Unified Agent:

- 1 GB RAM recommended, 512 MB RAM minimum
- 200 MB Disk Space
- Mac OS X: Version 10.6 or higher (64-bit only)
- Windows XP: Service Pack 3 or higher
- Windows 2003: Service Pack 2 or higher

Windows 7, Windows 8, Windows Vista, and Windows Server 2008 are all supported with no Service Pack requirements.

Installing the Unified Agent will remove an existing VIA installation. To continue using VPN functionality, log in to CPPM as the administrator, go to **Administration > Agents and Software Updates > OnGuard Settings**, and select **Install and enable Aruba VPN component** from the **Installer Mode** drop-down list.

Supported Antivirus and Browser Versions, OnGuard

The browser and antivirus software versions shown in the following tables are supported for the ClearPass OnGuard dissolvable agent. Due to the large number of products available, this list may change at any time.

The ClearPass OnGuard dissolvable agent supports the following browsers:

- Firefox: 18 and above
- Chrome: 20 and above
- Internet Explorer (IE): 7 and above, but CPPM does not currently support IE 10
- Safari: 6 and above

In the lab, we use the following antivirus software for our validations.

- Kaspersky: IS-11 and above

- Sophos: 9 and above
- Avast
- COMODO
- MacAfee
- Microsoft Security Essentials
- Microsoft Forefront Endpoint Protection-2008
- AVG
- Trend Micro
- Windows Defender Firewall
- Microsoft Windows Firewall

Use of Cookies

Cookies are small text files that are placed on a user's computer by Web sites the user visits. They are widely used in order to make Web sites work, or work more efficiently, and to provide information to the owners of a site. Session cookies are temporary cookies that last only for the duration of one user session.

When a user registers or logs in via an Aruba captive portal, Aruba uses session cookies solely to remember between clicks who a guest or operator is. Aruba uses this information in a way that does not identify any user-specific information, and does not make any attempt to find out the identities of those using its ClearPass products. Aruba does not associate any data gathered by the cookie with any personally identifiable information (PII) from any source. Aruba uses session cookies only during the user's active session and does not store any permanent cookies on a user's computer. Session cookies are deleted when the user closes the browser.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com
End of Support information	www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Chapter 2

Upgrade Information

This chapter provides instructions and considerations for upgrading to the 6.2 release.

Upgrading to ClearPass Policy Manager 6.2

You can upgrade to ClearPass Policy Manager 6.2 from ClearPass Policy Manager 5.2.0 (non-VM), 6.0.x, or 6.1.x.

- Upgrade images are available within ClearPass Policy Manager from the Software Updates Portal at **Administration > Agents and Software Updates > Software Updates**.

To be able to see upgrade images in the Firmware & Patch Updates list in the UI, ClearPass Policy Manager versions 6.1.x and 6.2.x require a new patch. The 6.2.5 patch addresses this for all prior 6.2.x versions. A separate patch will be delivered to adress this for 6.1.x versions.

- For appliance upgrades from 5.2.0, the upgrade image is available on the Support site.
- Direct upgrades from versions prior to CPPM 5.2.0 are not supported. Customers with earlier versions of 5.x must upgrade to either ClearPass Policy Manager 5.2.0 or 6.x first before upgrading to 6.2.
- Direct upgrades from CPPM 5.2.0 VM are not supported. Customers must install the 6.2.x VM version and then migrate their data to this new version.

Before You Upgrade

Before you begin the upgrade process, please review the following important items:

- User modifications on default services (dynamically received data such as Guest SSIDs) will not be carried forward after the upgrade. You must configure these inputs again after you upgrade.
- Data filter and Syslog Export filter configurations will be removed after the upgrade. You may have to reconfigure them.
- If you are upgrading a ClearPass Policy Manager 6.1.2 production virtual machine, you must add an additional hard disk (SCSI 0:2) to the VM before you upgrade. Please refer to the ClearPass VMware installation instructions Tech Note available in the Deployment Guides section at support.arubanetworks.com.
- Any log settings that were modified prior to the upgrade are not retained, and are reset to the default. The administrator should configure any custom log settings again after the upgrade.
- If you upgrade to ClearPass 6.2 after installing the 6.1.3 patch:
  - For offline upgrades from 6.1.3 to 6.2, please use the 6.2 signed upgrade image posted on the Support Web site.
  - For upgrading to 6.2 from versions prior to 6.1.3, please use the 6.2 unsigned upgrade image.

MySQL is supported in CPPM 6.0.x and greater. Aruba does not ship drivers for MySQL by default. Customers who require MySQL can contact Aruba support to get the required patch. Users should be aware that this patch does not persist across upgrades, so customers using MySQL should contact support before they upgrade.

After You Upgrade

The following actions might be required after upgrading to Policy Manager 6.2.0:

- If Guest Access with MAC caching service was configured prior to the 6.2 or 6.1 release, then after upgrading to the current release, the service must be recreated from the Service Template “Guest MAC Authentication”. The new enforcement profiles “Guest Expire Post Login” and “Guest Do Expire” will then be included in the enforcement policies. (#16270)
- The **Configuration > Authentication > Sources** filters might show duplicate filters. This may be seen after migration or upgrade if the backup included user-modified attributes. To ensure that user-modified attributes are not overwritten during the upgrade, both the default attributes and the modified attributes in the backup are loaded during the migration/upgrade. Users should manually remove the unused attributes after the migration/upgrade. (#16430)
- System Monitoring Information is not migrated when upgrading from previous versions of 6.X to 6.2, and the system monitoring node table will be empty after the upgrade. Users should manually add these values. (#16431)

Chapter 3

What's New in This Release

This chapter provides a summary of the new features and changes in the ClearPass 6.2.5 release.

This chapter contains the following sections:

Release Overview

ClearPass 6.2.5 is a monthly patch release that offers new features and provides fixes for known issues. The 6.2.5 cumulative update patch is available in ClearPass Policy Manager under **Administration > Agents and Software Updates > Software Updates**.

New Features and Enhancements in the 6.2.5 Release

Policy Manager

- **Monitoring > Live Monitoring > Access Tracker** now shows an alert if more than two anti-malware products are detected on a client. (#19661)
- The Request Tracker logs now show logs for failed health checks in the INFO log level, letting administrators see which health checks failed in this default log level. (#20688)

Onboard

Onboard now includes id-kp-eapOverLAN when creating trusted certificates. (#20423)

OnGuard

- Support was added for the following new Patch Management product: (#17796)
  - McAfee Epolicy Agent 4.x

  Support was added for the following new AV/AS products:
  - McAfee All Access Internet Security 3.x
  - Kaspersky Anti-Virus 14.x
- The following new Registry Key items were added: (#19031)
  - New field to specify a custom message for failed Registry Key checks.
  - Monitor Mode for Registry Key Health Class.
  - Registry Key Health Class Posture Check results in the **Posture Evaluation Results** section on the **Output** tab of the Access Tracker.
- In previous versions, the OnGuard Agent sent two WebAuth requests if any of the following health classes were configured: Registry, Processes, Services, or Windows Hotfixes. To improve performance, the OnGuard Agent now will only send two WebAuth requests the first time after installation. After that, the OnGuard Agent will send only one WebAuth request with information of the above-mentioned health

classes in the following cases: Agent restart, Machine restart, or User Login/Logout. For Mac OS X, this is applicable for the following health classes: Processes and Services. (#19032)

- A new **Health Logs** option was added to the **Diagnostics** tab. Health logs display diagnostic logs related to OnGuard health checks. (#19384)

Issues Resolved in the 6.2.5 Release

The following issues have been fixed in the ClearPass 6.2.5 release.

Policy Manager

Table 1 *Policy Manager Issues Fixed in 6.2.5*

Bug ID	Description
15953	An incorrect license usage warning was displayed for application licenses in the CPPM Event Viewer.
17769	During installation of the monthly patch, the **Clear and Close** button was enabled before the installation was complete. If the button was clicked, the log file was not displayed when the **Needs Restart** link was clicked and an error message was displayed.
18483	Although a username could be created with an apostrophe and a password could be created with a British pound sign, trying to log in with them failed and an error message was displayed.
19760	Corrected an issue where the Access Tracker on the publisher did not show RADIUS request attributes, computed attributes, or RADIUS response attributes.
19966	The Do_Expire and Expire_post_login features now work correctly for the entities that are authenticated against CPPM subscriber nodes.
20112	Corrected an issue where the CPU usage was very high (300%), causing the ClearPass user interface to become unresponsive and need to be restarted.
20340	Application licenses are no longer counted toward base AAA licenses.
20437	The CLI command "`system boot-image -l`" is enhanced to provide information about the SCSI disk in use for VM installations.
20606	Post Auth is now optimized to send Enforcement Profile attributes in Entity Updates only of they are required to be updated.
20618	Corrected an issue that allowed execution of commands when combined with certain special characters as a part of the netjoin process.
20629	Corrected an issue where authentications sometimes failed due to SSL session-related errors like 'decrypt_error' or 'close_notify'.

Guest

Table 2 *Guest Issues Fixed in 6.2.5*

Bug ID	Description
20467	Corrected an issue where guests could not log in to a Motorola WiNG4 controller.
20701	PHP is upgraded to version 5.4.23. This version includes fixes for CVE-2013-6420.
20702	Custom fields created with uppercase letters in their names were exported as blank to CSV and TSV format.

Onboard

Table 3 *Onboard Issues Fixed in 6.2.5*

Bug ID	Description
20610	Corrected an issue that caused the Mac OS X 10.6 client to display the error message “No networks identified for this OS” during device enrollment.
20699	The error message “Failed to connect to <network>” was displayed unnecessarily.
20704	XP Credentials and Vista Credentials were removed from **Network Settings > Authentication**, as these settings had no actual effect on device provisioning.

OnGuard

Table 4 *OnGuard Issues Fixed in 6.2.5*

Bug ID	Description
13556	OnGuard failed to read the last scan time for MAC Keeper Antivirus and Kaspersky Antivirus in MAC 10.8.
13557	Auto-Remediation (Enable Real Time Protection) for MacKeeper did not work with MAC OnGuard. MAC OnGuard indicated that the Real Time Protection for MacKeeper was enabled, but on the backend the RTP was still disabled.
19777	The ClearPass OnGuard Unified Agent now supports bouncing Cisco AnyConnect Version 3.1.04074 VPN Interface on Mac OS X.
20133	OnGuard failed to collect health information on Windows if the “Windows Management Instrumentation” (WMI) setup was corrupted.
20278	Corrected an issue on Mac OS X where OnGuard set the Interface type for a Wired, Wireless, or VPN Interface as OTHER.

New Known Issues in the 6.2.5 Release

The following known issues were identified in the ClearPass 6.2.5 release.

The 6.2.5 patch cannot be uploaded on the Internet Explorer (IE) browser. For details, please refer to #19288.

Policy Manager

Table 5 *Policy Manager Known Issues in 6.2.5*

Bug ID	Description
18765	**Symptom:** In Access Tracker, the Date:Date-Time attribute is blank for all Web Auth requests. **Scenario:** On the **Monitoring > Live Monitoring > Access Tracker > Input tab > Computed Attributes** section, the value for **Date: Date-Time** is blank for all Web auth requests. This may occur after changing CPPM’s DNS hostname or DNS server. **Workaround:** None.
#18947	**Symptom/Scenario:** During a patch installation through the user interface, CPPM might occasionally hang for a long time when the installation is almost complete, and the “need to restart” message is not displayed. **Workaround:** Refresh ClearPass or log out and log in again.

Table 5 *Policy Manager Known Issues in 6.2.5 (Continued)*

Bug ID	Description
20334	**Symptom:** The Syslog filter prevents the subscriber from being dropped. **Scenario:** This occurred where a syslog export filter was configured that contained both the publisher and subscriber under the the ClearPass servers. This prevented ClearPass from dropping the subscriber even using the force message. **Workaround:** Remove the cluster node entries wherever they are referenced and then drop the node.
20496	**Symptom:** Users are unable to connect to the wireless network. Authentication fails with the error “EAP-PEAP: fatal alert by client - decrypt_error” or “EAP-PEAP: fatal alert by client - close_notify”. **Scenario:** The issue has been observed on all platforms. **Workaround:** There is no workaround at this time. The issue may be temporarily addressed by clearing the cache for the AD source at **Configuration > Authentication > Sources > AD**, or by restarting the RADIUS service.
20765	**Symptom/Scenario:** Upgrade images do not appear in the Firmware & Patch Updates list. **Workaround:** To be able to see upgrade images in the list at **Administration > Agents and Software Updates > Software Updates > Firmware & Patch Updates**, ClearPass Policy Manager versions 6.1.x and 6.2.x require a new patch. The 6.2.5 patch addresses this for all prior 6.2.x versions. A separate patch will be delivered to address this for 6.1.x versions.

Onboard

Table 6 *Onboard Known Issues in 6.2.5*

Bug ID	Description
20867	**Symptom/Scenario:** Android 4.3 and above fails to install self signed certificate for the CA certificate. **Workaround:** For onboarding Android version 4.3 and above, CPPM must have a RADIUS server certificate issued by a proper Certificate Authority and not a self signed certificate. This is a requirement of Android’d API for Wi-Fi management. In Onboard network settings, the CA certificate that issued the server's certificate has to be selected as the trusted root certificate to be installed on Android.
20983	**Symptom:** HTC Android asks the user to enter a certificate name to be installed when onboarding. **Scenario:** HTC Androids running Android version less than Android 4.3 and greater than Android 2.3 would ask the user to enter a name for the certificate to be installed while onboarding. Authentication will fail if the user does not enter the exact certificate name as QuickConnect application instructs in a message prior to the certificate installation dialog. **Workaround:** None. This issue is due to a limitation in the Android phone’s firmware.

OnGuard

Table 7 *OnGuard Known Issues in 6.2.5*

Bug ID	Description
20525	**Symptom:** The unified agent Onguard is unable to detect Microsoft windows firewall properly on Windows 8 OS. **Scenario:** This has occurred with a specific configuration, where the endpoint has domain network settings in addition to Private/Public settings for enabling/disabling the firewall. **Workaround:** None.

Chapter 4

Enhancements in Previous 6.2.x Releases

This chapter provides a brief summary of the features and enhancements introduced in previous ClearPass 6.2.x releases.

Features and Enhancements in Previous 6.2.x Releases

This section provides detailed information about changes to each functionality area. Issue tracking IDs are included when available.

Policy Manager

- A "Monitor Mode" option was added for the Windows Hotfixes health class. When Monitor Mode is enabled, the health status of the Windows Hotfixes health class is always set to Healthy. This allows administrators to collect information related to missing hotfixes but not have the client treated as unhealthy if some hotfixes are missing. The option is similar to the Monitor Mode option for Service. After the Monitor Mode option is enabled, the **Output** tab for a session on the **Monitoring > Live Monitoring > Access Tracker** list will display the list of missing hotfixes, and will also display "Hotfixes:MonitorMode = Enabled" to indicate why the client is marked Healthy.
- ClearPass WorkSpace lets IT secure, distribute, and manage enterprise apps on mobile devices. A companion WorkSpace mobile app enforces policies, encrypts data, and provides a single sign-on for all work apps. WorkSpace supports an ecosystem of enterprise mobile apps and application partners across key categories. An organization's IT department can use WorkSpace to easily secure, distribute, and manage more than 40 leading third-party enterprise productivity apps as well as internally-developed apps. WorkSpace features are part of ClearPass Onboard, which is now labeled **Onboard + WorkSpace** in the left navigation.
- CPPM can now send syslog messages to the Syslog server over TCP. (#11755)
- New ClearPass WorkSpace licensing was implemented in ClearPass. Starting with the 6.2.0 release, ClearPass includes a production WorkSpace license for 25 endpoints by default. Users should be aware that to run WorkSpace, a corresponding Onboard or Enterprise license is required.(#12639)
- Users can configure a downloadable access control list (dACL) through the new **Role Configuration** tab in the Aruba Downloadable Role Enforcement Profile for Aruba Mobility Access switches. (#12825)
- The Clearpass OnGuard Unified Agent now supports health checks over VPN connections (IPSec) terminated on the Aruba Controller. (#13010)
- ClearPass now supports a framework for sending outbound http based enforcement actions to external context servers. This could include sending a message to an MDM server to trigger a remote wipe or remote lock. Example enforcement actions are listed for the various endpoint context servers supported and will be updated in future releases. (#13450)
- On the **Administration> Create Certificate Signing Request** form, the **Common Name** (CN) is now prepopulated with the fully-qualified domain name, and the default value for **Key Length** is increased to 2048. (#13551)
- CPPM can now make authorization decisions using the **Enhanced Key Usage** (EKU) field. (#14183)
- CPPM's integration with Palo Alto Networks firewall is enhanced to reduce the delay in notification updates. The polling timeout interval may now be set to a default value of as little as 30 seconds, supporting near-realtime updates of external entities. (#14270, 15194)

- CPPM's integration with Active Directory (AD) servers is enhanced. This also corrects an issue where, under certain conditions, a winbind/AD connection caused Active Directory authentications to fail. (#14273)
- CPPM now supports sending logs to multiple syslog servers. (#14391)
- CPPM's external context server (MDM) integration is enhanced to support the following operations, strengthening the ability to fetch data from MDM vendors for use in ClearPass policies (#14392):
  - Data retrieval via paging
  - Ability to change URLs used for API calls to MDM vendors (already supported in 6.1)
  - Ability to "refresh" data from a specific MDM vendor
- CPPM now supports Citrix XenMobile as an external context server. (#14511)
- CPPM can now make authorization decisions based on the "Not Valid After" attribute in a certificate. This enables ClearPass to put up a captive portal page that warns the user that their Onboarded client certificate is about to expire. (#14772)
- CPPM now has Cisco NCS (Prime) TACACS Service Dictionary included. (#15082)
- The new VSA "Aruba-AP-IP-Address" was added to the Aruba RADIUS dictionary. This VSA downloads the IP address from the RADIUS server to be used as a static inner IP for the RAP. (#15371)
- Audit records older than 30 days or the configured number of days are now automatically deleted, improving efficiency when performing administrator operations. (#17330)
- Support was added for detecting the iOS 7 Captive Network Assistant. This capability may be required in certain circumstances, especially if a captive portal is used for onboarding iOS 7 devices. For full details, see the App Note "Apple Captive Network Assistant Bypass with Guest" in the Tech Notes section of the Support site. The App Note includes instructions for successfully implementing the Guest captive portal instead of the Apple Captive Network Assistant to onboard iOS 7 devices. (#17749, #17820)
- Support was added for the Windows 8.1 Network Access Protection (NAP) Agent. RADIUS requests from the Windows 8.1 NAP Agent are now categorized as Windows 8. (#18775)
- Support was added for handling bulk imports for Endpoints. (#19254)
- Additional database indexes were added, improving loading times for pages when listing guest users. (#19453)
-

AirGroup

- A new configuration option for the AirGroup controller allows the timeout value to be specified when getting configuration information from the device. The default value is 15 seconds (increased from 5 seconds in previous releases). If the controller is a master controller with many APs configured, or if network conditions require an additional delay, you might need to further increase the value. (#18454)

Guest

- Updated French translation packs are available. (#16634)
- Support was added to allow Web logins and guest registrations behind wired Cisco switches. Guests can also log in via server-initiated RFC-3576 calls in addition to the standard HTTP POST. (#17175)
- Auto-complete options for sponsor lookups were added to guest self-registrations. (#9446)
- ClearPass Guest now supports HigherOne CASHnet as a credit card transaction processor. (#9363)
- Support for Meru Networks controllers was added to Web Login pages. (#10480)
- The sponsorship confirmation email now includes the ability to let the sponsor change the account expiration time.(#11292)
- The application log viewer is enhanced to allow viewing of logs for other servers in a cluster. (#12044)

- When customizing forms, you can now add static text rather than having to base the addition on an existing field. (#13514)
- The **Translation** section in ClearPass Guest's Configuration module, in conjunction with Translation Assistant plugins, let you define and edit language translation packs and enable application features that provide assistance with translation. (#15998, #15102)
- The Japanese translations language pack is updated. (#16266)

Insight

- Clearpass Insight now has two new templates (#15032):
  - Endpoint—New template to generate reports on endpoints
  - Unique sessions—New template to generate unique mac and user details
- The Session and NAS template has been modified to include session statistics, such as Average Session and Average Traffic.

Onboard

- Onboard includes the ability to provision a TLS certificate in the Windows computer store. (#12166)
- For OS X and iOS, added the ability to define custom fields that appear in Onboard device provisioning login forms and are included in TLS client certificates. This feature is not supported on Windows or Android yet. (#14327)
- Added the ability for the configuration profile provisioned to devices to be dynamically specified via returned RADIUS attributes. (#14357)
- Added an option to have device TLS certificates issued by Active Directory Certificate Services. (#14492)
- SHA 256 is now supported as a digest algorithm for the Onboard Certificate Authority. (#14565)
- Added a BYOD self-service portal through which users can view, enable, disable, and delete their own Onboard devices. (#14911)
- Support was added for onboarding devices running Mac Mavericks (OS X 10.9). (#18630)

OnGuard

- The Clearpass OnGuard Unified Agent for MAC OS X now supports Patch Management application checks. (#7161)
- The Clearpass OnGuard Unified Agent now has a new health class to check disk encryption on MAC OS X. (#14025)
- The Clearpass OnGuard Unified Agent now has a new health class to check running/stopped processes on MAC OS X. (#14026)
- The Clearpass OnGuard Unified Agent now has a new health class to check running/stopped services on MAC OS X. (#14028)
- The Clearpass OnGuard Unified Agent now has a new health class to check Peer to Peer (P2P) applications on MAC OS X. (#14029)
- The Clearpass OnGuard Unified Agent now has a new health class to check USB mass storage devices on MAC OS X. (#14031)
- The Clearpass OnGuard Unified Agent now has a new health class to check disk encryption on Windows OS. This feature has been tested using BitLocker Drive Encryption, and is supported for Windows 7, and Windows 8 Pro and Enterprise editions. (#14035)
- The Clearpass OnGuard Unified Agent now supports Active Directory Single Sign On (SSO) on Windows Platforms. (#14421)

- Clearpass administrators can now configure a default email address on Clearpass OnGuard settings. This email address will be used by clients to send the logs when user clicks Send Logs. (#14917)

Installing Unified Client will remove an existing VIA installation. To continue using VPN functionality, log in to CPPM as the administrator, go to **Administration > Agents and Software Updates > OnGuard Settings**, and select **Install and enable Aruba VPN component** from the **Installer Mode** drop-down list.

- Support was added for non-English characters in usernames and passwords for the Clearpass OnGuard Unified Agent running on MAC OSX. (#13840, #13841)
- Support was added for Data File Time check for antivirus and antispyware health classes for Mac OS X. (#17532)
- Support was added for Mac Mavericks (OS X 10.9). (#18614)
- Support was added for detecting newer antivirus and antispyware products on Windows OS using Windows Security Center (WSC). (#18582)
- The logic for selecting an antivirus/antispyware application was changed to 'Any Supported Product'. An antivirus/antispyware application that has RTP Enabled is now given higher preference than one that has RTP disabled. (#18208)
- Support was added for the following new products: (#17996, #18381)

Table 8 *OnGuard Added Product Support*

Product Category	Product
Anti-Virus/Anti-Spyware	avast! Pro Antivirus 9.x (Windows) avast! Free Antivirus 8.x (Mac) avast! Free Antivirus 9.x avast! Internet Security 9.x avast! Premier Antivirus 9.x AVG AntiVirus Free Edition 2014.x (Windows) AVG AntiVirus 2014.x (Windows) AVG Premium Security 2014.x (Windows) Avira Free Antivirus 14.x Malwarebytes Anti-Malware 1.x (Windows) Malwarebytes Anti-Malware Pro 1.x (Windows) Panda Antivirus Pro 13.x (Windows) Quick Heal Total Security 15.x (Windows) Quick Heal AntiVirus Pro 15.x
Firewall	Mac OS X Built-in Firewall 10.9.x (Mac)
Disk Encryption	FileVault 10.9.x (Mac)
Patch Management	DELL Kace Agent 5.x (Mac and Windows) Software Update 10.9.x (Mac)

The following issues were fixed in previous 6.2.x releases. For a list of issues resolved in the 6.2.5 release, see the What's New in This Release chapter.

Fixed in 6.2.4

Policy Manager

Table 9 *Policy Manager Issues Fixed in 6.2.4*

Bug ID	Description
#18350 #19229	EAP-TLS with OCSP authentication failed if a certificate revocation list existed in the system.
#18967	The values provided by the MDM servers were not as expected. This caused issues with determining device profile information, and the warning message "Ignore incomplete Profile entry" was displayed in the mdm.log file. All device profile details are now correctly discovered.
#19024	CPPM lost the PostgreSQL database connection if the cluster password included any of the following special characters: ! @ # The following special characters are now supported: **! @ # $ % ^ & * ? / - _ + = . ,**

Guest

Table 10 *Guest Issues Fixed in 6.2.4*

Bug ID	Description
#19248	Corrected an issue where Xirrus could not be properly configured as a vendor for a self-registration.
#19249	Corrected an issue with the Account Expiration Time field's calendar button when the browser's language settings were set to Japanese or Korean.
#19270	Connecting to an LDAP server from ClearPass Guest failed with an error such as 'certificate verify failed (unable to get local issuer certificate)'. SSL connections to LDAP servers from Guest now use the CPPM Trust List to verify the identity of the LDAP server. Users should be aware that for correct validation of the LDAP server's identity, all certificates from the LDAP server – including the server's certificate, any intermediate certificates and the root CA certificate – must be present in the CPPM trust list.
#19405	Corrected a performance issue where user-list searches were slow if multiple fields were enabled for searching.

Onboard

Table 11 *Onboard Issues Fixed in 6.2.4*

Bug ID	Description
#19474	When onboarding for secure wired access, the client machine had to be unplugged and then reconnected after onboarding in order to use the onboarded credentials for network access.

OnGuard

Table 12 *OnGuard Issues Fixed in 6.2.4*

Bug ID	Description
#11319	Live updates for Windows Defender Antivirus software are now supported on the Windows 8 OS.
#15360	ClearPass OnGuard Unified Agent for Mac OS X reported BitTorrent 7.x Peer To Peer Application as Running even after terminating/closing BitTorrent 7.x.
#18427	The ClearPass OnGuard dissolvable agent selected the Virtual Network Interface's MAC address as the username in a WebAuth request.
#18904	When the ClearPass OnGuard Web agent applet was launched, the Java plugin on the client browser displayed the warning message "This application will be blocked in a future Java security update because the JAR file manifest does not contain the permissions attribute".
#18924	Corrected an issue where, on a Mac OS with the .DAT file's update interval configured, the ClearPass OnGuard Unified Agent failed to print AntiVirus remediation messages.
#18960	If both wired and wireless interfaces were managed, OnGuard did not trigger WebAuth when a system came out of hibernation on a wired interface.
#19456	If a Mac OS X with a wireless connection lost that connection immediately after establishing a wired connection, OnGuard could not send a soft reauthorization and displayed the message "sending WebAuth request failed".
#19457	The link to Java Installer download page now works correctly. This link is displayed on the WebAgent help page if Java is not installed on the machine.

WorkSpace

Table 13 *WorkSpace Issues Fixed in 6.2.4*

Bug ID	Description
#19115	Corrected an issue where MDM Profile installation failed with certain Certificate Authorities if there were i18n characters in the CA.

Fixed in 6.2.3

Policy Manager

Table 14 *Policy Manager Issues Fixed in 6.2.3*

Bug ID	Description
#17331	High memory usage of the Admin UI occurred when there was a continuous heavy load of TipsAPI requests, which resulted in errors in Access Tracker and in Analysis and Trending.
#17743	CPPM did not send a RADIUS CoA when changes were made to an AirGroup shared device.

Table 14 *Policy Manager Issues Fixed in 6.2.3 (Continued)*

Bug ID	Description
#18153	The WorkSpace license count in a cluster is now shown correctly. Before the fix, for a two-node cluster with default licenses, the Enterprise license count correctly showed 50 (25 per node) but only 25 were shown for the WorkSpace license.
#18185	Access Tracker was hanging and not showing information from the subscriber CPPM node. This occurred on nodes where there were multiple syslog queries that each took hours to complete. The fix now ensures that syslog queries never scan more than 10 minutes of data at a time.
#18216	Restoring the database from 6.2.1 to 6.2.2 produced a migration error for Policy Manager.
#18380	A failed publisher would re-acquire the VIP in the case of a split-brain network condition. The failed publisher now correctly releases the VIP and stops its VIP service when it detects that the secondary has taken over as publisher.
#18477	In some cases, Access Tracker requests were not seen in the Admin UI if multiple requests were made while loading was in progress.
#18595	Upgrading VMware tools from the vSphere console made CPPM unusable. Note: Although the issue is fixed, we recommend that customers do not update VMware tools without confirming compatibility with Aruba documentation/support.
#18620	Security enhancements ensure that no Admin user can view users' credentials. Prior to the fix, passwords could be shown in clear text to some Admin users if inspected through browser developer tools.
#18639	The CLI commands **`krb auth`** and **`krb list`** now work correctly. Prior to the fix, some clients were unable to authenticate users across a Kerberos authentication source.
#18699	Corrected an issue with the Direct Web Remoting (DWR) interface in CPPM that made it possible for an authenticated user to reuse the session cookie of another authenticated user.
#18898	Optimized the SQL query used in the Post Authentication module to fetch the list of active users.

AirGroup

Table 15 *AirGroup Issues Fixed in 6.2.3*

Bug ID	Description
#18454	A new configuration option for the AirGroup controller allows the timeout value to be specified when getting configuration information from the device. The default value is 15 seconds (increased from 5 seconds in previous releases). If the controller is a master controller with many APs configured, or if network conditions require an additional delay, you might need to further increase the value.

Guest

Table 16 *Guest Issues Fixed in 6.2.3*

Bug ID	Description
#18455	The plain text format used when exporting the application log is updated. In addition to the existing fields, the generated text file now includes any arguments that were logged.
#18457	Creating multiple guest accounts now attempts to find a username that isn't in use when it generates an existing username. Prior to the fix, multiple account creation would stop before completing.

Onboard

Table 17 *Onboard Issues Fixed in 6.2.3*

Bug ID	Description
#18922	Onboard was not recording multiple MAC addressed in the TLS client certificate.

OnGuard

Table 18 *OnGuard Issues Fixed in 6.2.3*

Bug ID	Description
#13841	Non-English characters are now supported in usernames and passwords for the Clearpass OnGuard Unified Agent running on MAC OSX.
#15176	Remediation tasks for Set RTP now work correctly in AVG Free Antivirus (2013).
#17193	An issue caused the ClearPass Unified OnGuard Agent service to crash. The issue was rare, and occurred when the backend service attempted to contact the front end before it was running.
#17489	An issue caused the Clearpass OnGuard Unified Agent to be displayed every 5-10 seconds.
#18180	Windows 8 clients sometimes took too long to submit health information (5 to 6 minutes) or would fail to submit it, although on retry the information was submitted and the client was marked healthy.
#18430	On slower systems, the OnGuard health check took two or three hours to run. Slow systems sometimes caused the backend service to take more than three minutes to perform the health check. This in turn caused the OnGuard Agent to time out, and the health check would run for two or three hours. The health collection timeout limit is now increased from three minutes to 20 minutes to accommodate slow conditions, and the cache is not automatically cleared.
#18459	Starting Onguard would open two instances of OnGuard on the same client. This was observed on MAC OSX.
#18849	The warning message “”ClearPassOnGuard.pkg” is from an unidentified developer” was displayed when the user tried to open the ClearPass Unified OnGuard installer package on a Mac OS X.

WorkSpace

Table 19 *WorkSpace Issues Fixed in 6.2.3*

Bug ID	Description
#15126	Enforcement of an app’s geo-fencing policy is now immediate. Prior to the fix, when a geo-fencing policy was enabled for an app and that app (instead of WorkSpace) was active, enforcement of the geo-fencing policy was sometimes delayed until the next WorkSpace configuration poll was run.
#18846	The latest WorkSpace dylib-1.2.57770 was updated with fixes.
#18847	The Aruba new overlay icon was updated.

Fixed in 6.2.2

Policy Manager

Table 20 *Policy Manager Issues Fixed in 6.2.2*

Bug ID	Description
17938	AirGroup MAC Auth against Guest devices was counted towards the ClearPass Guest License.

Guest

Table 21 *Guest Issues Fixed in 6.2.2*

Bug ID	Description
17817	Corrected a potential security issue regarding the redirect functionality of the “target” field in Amigopod login page authentication. Redirect behavior is restricted to internal addresses.
17820	Added support for iOS 7 to the Apple Captive Network Assistant bypass feature (landing.php). Refer to the App Note “Apple Captive Network Assistant Bypass with Amigopod” for details.

Onboard

Table 22 *Onboard Issues Fixed in 6.2.2*

Bug ID	Description
17980	Mac OS X “System” profiles did not keep the 802.1X connection alive when no users were logged in.

OnGuard

Table 23 *OnGuard Issues Fixed in 6.2.2*

Bug ID	Description
17688 17712	The Onguard Process Check on Windows failed for a non-English Windows OS.

WorkSpace

Table 24 *WorkSpace Issues Fixed in 6.2.2*

Bug ID	Description
17881	The “role enforcement based on WS app auth” functionality was added.
17903	The WorkSpace dylib-1.2.56304 was updated.
17953	Users were not able to reinstall the configuration profile.
18032	The error message “Invalid Client Certificate” was displayed when provisioning the workspace with certain certificate authorities.

Fixed in 6.2.1

Policy Manager

Table 25 *Policy Manager Issues Fixed in 6.2.1*

Bug ID	Description
15382	The 6.2.1 patch addressed a known vulnerability in Struts CVE-2013-2251 that could be introduced by manipulating parameters prefixed with “action:”/”redirect:”/”redirectAction:”, allowing remote command execution.
16498	Support was added for the vendor-specific attribute Aruba-Essid-Name.
16586	Corrected an issue with netevents generation where more than 10,000 audit entries within two minutes would cause high CPU and memory usage, affecting CPPM functionality.
16712	The CPPM 6.2 Dissolvable Agent did not work if a Virtual IP FQDN was used to load the Clearpass Onguard portal.
16803	After upgrading to 6.2.0, a configuration file was deleted. This caused the Dissolvable Agent to not load the Clearpass Onguard portal page, and a “Cache entry not found” Java error was displayed.
16825	VIP service restart on the nodes is no longer required when VIP failover wait time is changed in cluster-wide parameters.
17130	The cpass-async-netd service sometimes failed to start. This issue was seen on low-power virtual machines (VMs) when most of the services were activated, causing a high load.
17145	The AD recovery section of Radius Service Parameters now includes an option to restart Winbind Service.
17280	When installing certificates in the machine store, onboarding did not work for usernames that contained a period character (.).
17283	The MaxClients limit for the Apache httpd Web server could not be set to a value greater than 256.
17321	CPPM now supports using Radius CoA for Network Access Devices (NAD) that use Classless Inter-Domain Routing (CIDR) addresses.
17531	The “Not Valid After” attribute did not return a proper value. This caused authorization decisions based on that attribute in a certificate to not work properly.
17645	The HTTP authorization source feature now supports talking to HTTPS servers and servers that require authentication. Nested elements in the JSON payload returned by the server are ignored.
17648	Disabled support for AECDH ciphers to prevent a possible man-in-the-middle attack against the SSL protocol.

Guest

Table 26 *Guest Issues Fixed in 6.2.1*

Bug ID	Description
17132	Corrected an issue in self-registrations where, if the user logged in after looking up a sponsor, the error message “NwaLdapSponsorUserSearchAjax not callable” was displayed.
17165	Users were able to log in without sponsor approval if MAC caching was enabled.
17173	The custom **CSS Class** field was ignored when rendering the **Submit** button on a registration form. The class is now included as expected.
17188	Corrected the import of Amigopod 3.9 “Network Login Access Setup” settings. Operator login “allowed” and “denied” networks are now ignored as they are obsolete.

Table 26 *Guest Issues Fixed in 6.2.1 (Continued)*

Bug ID	Description
17190	The list of accounts and devices shown on the **List Accounts** and **List Devices** pages became faulty whenever an invalid condition was added to the **"**[Guest Roles]**"** role mapping policy. Invalid conditions in the "[Guest Roles]" role mapping policy are now ignored and they no longer affect the **List Accounts** or **List Devices** pages.
17204	User search and autocomplete in the **LDAP Sponsor Lookup** field failed with a JavaScript error for certain skins.
17211	Onboard device provisioning pages were imported as Web login pages.
17242	Added reporting capabilities for up to 20 custom fields defined in Guest.
17302	The PHP version was upgraded to 5.4.19. This version includes fixes for the CVE-2013-4248, CVE-2013-4113, CVE-2013-2110, CVE-2013-1635, CVE-2013-1643, CVE-2013-1824 vulnerability issues.

Insight

Table 27 *Insight Issues Fixed in 6.2.1*

Bug ID	Description
17150	The message "Internal Server Error" was displayed when the user tried to log in to Insight after Network Restrictions was configured.

Onboard

Table 28 *Onboard Issues Fixed in 6.2.1*

Bug ID	Description
16707	Corrected an issue that prevented migrating Onboard backups that contain multiple copies of the same certificate.
17177	In cases where the profile signing certificate trust chain is incomplete, the error message now more clearly describes the problem.
17210	Corrected an issue that prevented signing a previously-created certificate signing request (CSR).
17658	A "profile installation failed" error was displayed when retrieving certificates that were generated by ADCS during enrollment.

OnGuard

Table 29 *OnGuard Issues Fixed in 6.2.1*

Bug ID	Description
16032	ClearPass OnGuard failed to read the encryption state of drives using Symantec Endpoint Encryption 8.2.1 (Full Disk).
16829	The Windows update check failed on a Windows XP non-English system, and displayed the error message "The periodic scan of this system for security updates failed. Please try again."
17313	Support was added for the Clearpass Onguard Unified Agent to detect Virtual Machine checks for Hyper-V Manager.
17357	The Dissolvable Agent did not work on client machines that had Java 6 installed, and the error message "Starting applet clearpass OnGuard" was displayed.
17582	Support was added for Kaspersky Internet Security 14.0.

WorkSpace

Table 30 *WorkSpace Issues Fixed in 6.2.1*

Bug ID	Description
16479	The WorkSpace banner was not shown on the iPhone or iPod, and the **WorkSpace > Preferences > Notifications From Admin** page was blank.
17268	After the user upgraded, a License error message was displayed on the **Onboard + WorkSpace > WorkSpace Configuration** pages.
17269 17270	The database query error “invalid input syntax” was displayed if the user tried to save an App Set or an App Policy Template without a name.
17271	The Application Log displayed the error message “Invalid argument supplied for foreach ()” if the user tried to add “Device Restrictions” to a configuration profile after migrating from 6.1.2 to 6.2.0.
17272	The WorkSpace Dynamic Library (dylib) file was updated to version 1.1.54873.
17273	WorkSpace authentication failed if the password included an ampersand character (&).
17274	If a user initiated the MDM “wipe device” Option, it remained stuck in the queue and subsequent MDM actions were also queued and not sent to the device.

Fixed in 6.2.0

Policy Manager

Table 31 *Policy Manager Issues Fixed in 6.2.0*

Bug ID	Description
11593	After a restore operation, the EAP-FAST master keys are generated and updated in 30 minutes on the restored machine. Corrected an issue where, during this period, authentications using EAP-FAST mechanism might fail.
14297	When a cluster password was changed, users had to restart the async-netd service in order to start sending events to Insight.
14448	The list of IdP Certificates on the **Configuration > Identity > SSO** page included certificates which were not enabled in the trust list. A note was added with an alert stating that only trusted certificates which are enabled in the trust list will be shown under the IdP certificate List.

AirGroup

Table 32 *AirGroup Issues Fixed in 6.2.0*

Bug ID	Description
14342	Adding an Aruba Instant AP to the list of AirGroup Controllers failed with a message similar to “Could not read configuration from controller (error 4: State not matched in expect)”.
14771	Added support for reading roles from Aruba Instant access points when using the **AirGroup Controllers > Read Configuration** command.
15472	Reading the configuration from an AirGroup Controller would not read the details of more than 32 access points.
15656	Using the Read Configuration command with an AirGroup controller did not always obtain the list of AP Groups and the list of access points.

Guest

Table 33 *Guest Issues Fixed in 6.2.0*

Bug ID	Description
13876	If the sponsor overrode the guest's role with a new setting, after the guest logged in with the new role and logged out again, Active Sessions still showed the original role instead of the expected role.
14207	After migrating from 6.0.1 or 6.0.2 to 6.1, users that were created in 6.0.x with "No Expiry" showed an expiration date in 2038.
14274	Users could not be disconnected from the **Guest > Active Sessions** page when using Cisco WLC.
14426	Selecting specific guest roles in the operator profile caused a "Database query error" on the **Guest > Active Sessions** list view.
15057	If the language was set to certain European languages, hotspot sign-ups displayed values in Euros instead of US dollars.
15213	SMS notification email messages were sent using the SMTP settings configured for email notifications, instead of the SMS notification settings, when the **CPPM > Administration > External Servers > Messaging Setup** option "Use the same settings for sending both emails and SMSes" was unchecked.
15427	A trailing space was added to the MAIL FROM: header line in an outbound SMTP connection, even when no mail parameters were specified. This behavior was in violation of the SMTP protocol specified in RFC 2821 and could lead to issues with certain SMTP gateways.
15473	Disabling or deleting a guest account did not always generate a corresponding RFC 3576 Disconnect-Request for other active sessions associated with the guest account using MAC caching.
15545	A guest form configured with a Captcha field displayed the message "The security code is incorrect" on a ClearPass server configured as a subscriber node.

Insight

Table 34 *Insight Issues Fixed in 6.2.0*

Bug ID	Description
11818	PDF and HTML data tables were not created when a CSV file size was greater than 1MB.

Onboard

Table 35 *Onboard Issues Fixed in 6.2.0*

Bug ID	Description
14244	Clicking the **Cancel** button of an export certificate form on the subscriber threw an exception. Also fixed the issue where on the trust chain page of a certificate, clicking the **Cancel** button of an export certificate form would log out the user.
14249	A new TLS client certificate is generated for devices that re-enroll when their previous certificate has less than 25% of its lifetime remaining. This corrects an issue where the existing client certificate was reissued to a device that re-enrolled even if the certificate was about to expire.
14305	Corrected the default reconnect settings for iOS devices when importing a version 3.9 backup. The **Allow Automatic Reconnect** and **Allow Manual Reconnect** check boxes under **Provisioning Settings > iOS and OS X** are now selected by default.
14312	For wired configurations, the client did not respond to a new authorization attempt and remained in MAC or EAP-PEAP instead of switching over to EAP-TLS. The wired zero configuration is now correctly restarted and the role authorized.
14363	Trying to provision Android 4.2.2 produced the error "There was a problem in connecting to the network, please retry".

Table 35 *Onboard Issues Fixed in 6.2.0 (Continued)*

Bug ID	Description
14364	Android devices could not be connected after provisioning if there was a period character (.) in the SSID.
14677	Corrected errors in migration of Onboard configuration from 6.0.2 and earlier systems.
14932	Corrected an issue that could result in the message “Onboard provisioning can not be performed at this host address. If you were redirected here, please contact a network administrator” when attempting to provision a device.
14965	Increased the default “Reconnect Timeout” used by iOS and OS X devices during Onboard device provisioning from 15 seconds to 20 seconds. Also fixed an issue where the administrator-specified “Reconnect Timeout” was being ignored. These changes will reduce the likelihood of a “Failed to connect to...” error message being shown to the user during device provisioning.
15443	Corrected the auto-reconnect when “switchip” and “mac” are provided to an earlier login page in a multi-page sequence.
15486	The per-user limit for the number of Onboard devices was only applied using case-sensitive matching. This allowed users to bypass the limit by specifying usernames that varied only by case.
15522	Onboard error messages for iOS/OS X were not displayed to the client on the provisioning page.
15598	Corrected an issue that could cause the root certificate download link to not display even when the user required the root certificate for the profile to show as Trusted.
15652	Corrected the device password generation for repeat enrollments when using certificates created by the device.
15681	Automatic reconnect after device provisioning failed if multiple links were used to reach the device provisioning page.
15891	The **Delete Client Certificates** option on a Certificate Authority did not delete the corresponding device accounts under **Onboard Devices** in Policy Manager.
16075	Removed hostname checking in Onboard that could result in “Onboard provisioning can not be performed at this host address” error being displayed.

OnGuard

Table 36 *OnGuard Issues Fixed in 6.2.0*

Bug ID	Description
10671	The HideLogoutButton parameter for OnGuard only applied to the Windows OS. The HideLogoutButton parameter now applies to all operating systems, and is included in the global settings options at A**dministration > Agents and Software Updates > OnGuard Settings > Global Agent Settings**.
13508	OnGuard did not support the **Cache Credentials For Days** option under **Global Agent Settings**.
14279	Mac OS X ClearPass OnGuard categorized 3G USB Data Cards as VPN type instead of OTHERS.
14886	OnGuard failed to enable RTP of Malwarebytes Anti-Malware Pro (1.75.0.1300) anti-spyware application on Windows.
15259	High memory usage was seen on the Clearpass OnGuard Unified Agent if the client PC had AVG Antivirus.

Chapter 6

Known Issues Identified in Previous Releases

The following known issues for this release were identified in previous releases. Workarounds are included when possible. For a list of known issues identified in the 6.2.5 release, see the What's New in This Release chapter.

Policy Manager

Table 37 *Known Issues in Policy Manager*

Bug ID	Description
	The subscription ID is not retained when you upgrade to CPPM 6.0.2. After you upgrade, you must re-enter the subscription ID at **Administration > Agents and Software Updates > Software Updates**. This is the same subscription ID that was used for 6.0.1, and is required in order to receive software updates.
	Alert messages in the access tracker might be missing for some failed RADIUS authentication requests.
	OCSP URLs cannot be accessed through HTTP proxy from CPPM.
	Upgrading from previous versions to 6.0.1 will fail if ClearPass Policy Manager is already joined to the domain. **Workaround**: Perform a "leave domain" before starting an upgrade.
	If Profile is enabled, cleanup intervals for Known/Unknown/Disabled endpoints in the Cluster Wide Parameters must not be configured. This is known to cause issues with the cleanup process.
	Domain join operations will fail if the domain password contains special characters such as a space, quotation marks, or a "$" symbol.
10447	Internet Explorer 10 is supported only in compatibility mode. For details, please refer to http://windows.microsoft.com/en-US/ internet-explorer/products/ie-9/features/compatibility-view.
10881	Entity updates with PostAuth enforcement fail if publisher is down.
11744	Upgrading from 5.2 to 6.x will fail if CPPM is joined to a domain. This issue does not exist for customers who have installed the latest cumulative patch.
11906	The Aruba dictionary becomes disabled by default after upgrading from Policy Manager 4.x to 6.0.1. **Workaround:** Customers who run into this issue must enable the Aruba dictionary manually from the **Administration > Dictionaries** page.
12316	Syslog Filters and Data Filters configuration will be removed after an upgrade. Policy Manager does not carry forward Syslog Filters and Data Filters configuration. Only default data is migrated.
13645	Authorization attributes are not cached for the Okta authentication source.
13781	In the 6.1 release, the default unit for the CRL update interval is now "hours" instead of "days." When restoring a 5.x backup on 6.x CPPM, this default unit will update to "hours."
13999 13975	In order to add or update a PostAuth profile configuration, the admin must first delete old profiles from CPPM, and then add the new/updated profiles.
14186	PostAuth will fail in MAB flow if a user tries to connect using an endpoint that is UNKNOWN to CPPM.
14190	In order for PostAuth to work in MAC Authentication Bypass (MAB) flow, users must add a new blacklist repository with a custom filter.
#19288	**Symptom:** The 6.2.3, 6.2.4, or 6.2.5 patch cannot be uploaded on the Internet Explorer (IE) browser. **Scenario:** On Internet Explorer, uploading the patch through the Admin UI fails with the message "Content-Type "Text/plain" is not supported". **Workaround:** Use the Firefox or Chrome browser instead of IE.

Guest

Table 38 *Known Issues in Guest*

Bug ID	Description
9967	Unicode SMS messages are limited to 70 Unicode characters. The ClearPass Guest user interface still displays 160 characters as the limit. Sending a Unicode SMS message over 70 characters may fail if the SMS service provider does not support multi-part SMS messages. **Workaround**: If you plan to use Unicode SMS messages, check your SMS receipt carefully to ensure it is not over 70 characters in length.
10334	Filtering on the Guest Manager List Accounts page (guest_users) might not work when non-standard columns are displayed. You might see the message “Internal error: NwaClearPassApi does not support this query: Complex queries using _Build are not supported”. **Workaround**: Use default columns, or disable searching on additional columns that are added to the view (customize the view, edit the column, and deselect the **Include values when performing a quick search** check box).
10613	Advertising Services is not available in this version of ClearPass Guest.
15684	**Symptom/Scenario:** If the MAC delimiter for the Mac Auth profile is not set to **“**dash**”** (-) in the controller, CoA is not sent to the active MAC connection. **Workaround:** Ensure that the MAC delimiter character for the Aruba controller's Mac Auth profile is set to “dash” (-).
15809	User names are treated case-sensitively by ClearPass Policy Manager. **Workaround**: Be aware that authentication is always case-sensitive and enter your username accordingly.

Insight

Table 39 *Known Issues in Insight*

ID	Description
	The previous configuration for the Report Analytics selection is not retained when a report is edited. **Workaround:** Select the appropriate Analytics columns again before you click Save.
11696	Generated reports for missing hotfixes do not display properly.
11827	Insight is not supported in Internet Explorer 8 (IE8) or earlier.
12096	Editing a report to select some columns for analytics overwrites/replaces the chosen columns for the corresponding report.
12159	Insight reports do not immediately display License changes. These changes may take up to 24 hours, depending on when the changes were completed.
12315	When editing a report, the new report does not retain the previously configured Report Analytics selection.
12414	Insight HTML reports that are accessed from inside the Insight UI do not show images that are attached to the report. Note that PDF reports correctly display the images.
13980	Columns with non-ascii values do not display in PDF reports.
14420	In 6.1, Insight is disabled by default. New customers as well as customers who upgrade must enable Insight on the desired server. To enable Insight, navigate to the Policy Manager **Administration > Server Manager > Server Configuration** page, select the server on which to enable Insight, and then select the **Enable Insight** check box.

Onboard

Table 40 *Known Issues in Onboard*

Bug ID	Description
9897	ClearPass Onboard does not update the Policy Manager endpoints table with an endpoint record when provisioning an iOS 5 device. This is because the iOS 5 device does not report its MAC address to ClearPass Onboard during device provisioning.
10127	Auto-reconnect does not work for Mac OS X 10.7. This client will reconnect using the original credentials that were used to connect to the SSID (PEAP instead of TLS). This happens even if the “Remember this Network” option is NOT selected when connecting to the provisioning network.
10667	When using Onboard to provision a OS X system with a system profile, an administrator user must select the appropriate certificate when connecting to the provisioned network for the first time. The administrator should also ensure that the system's network settings are configured to automatically prefer connecting to the provisioned network, if the intent is for non-administrator users to always use that network. The process to provision an OS X system with a system profile is: • The administrator should log in to the OS X system and connect to the provisioning SSID. Do not select “Remember this network.” • Use Onboard to provision the device with an EAP-TLS profile, ignoring the username/password prompt. • Connect to the provisioned network, selecting EAP-TLS as the mode and selecting the provisioned certificate, but ignoring the username field. • When the system connects and authorizes to the network, use Network Preferences to place the EAP-TLS network first in the priority list. • After the administrator logs out, users logging in are connected by EAP-TLS and cannot modify those settings.

OnGuard

Memory utilization for ClearPass OnGuard depends on the Health Classes configured and the type of Windows OS; however, the minimum requirement for ClearPass OnGuard running on a Windows platform is 90 MB.

Table 41 *Known Issues in OnGuard*

ID	Description
	OnGuard fails to collect health on Windows 8 OS if VMWare Server 2.0.2.X is installed.
	Symptom: Upgrading ClearPass OnGuard from versions 3.5, 4.0, 5.0, 5.0.1, 5.1.1, and 5.2 to 6.0 will fail if the OnGuard installer is invoked without administrative privileges on the client. **Scenario:** This applies to the MSI version only. **Workaround**: Execute the `msiexec/I ClearPassOnGuardInstall.msi` command from the windows command prompt as the administrator user.
	Disabling USB storage devices on Windows 2008 server (64-bit) is not supported.
	Migration of Posture Policies from earlier versions of ClearPass Policy Manager to 5.1.x/5.2.0/6.0 is not supported. **Workaround**: Add/configure posture policies directly on the upgraded version of CPPM again.
	Live updates for Windows Defender is not supported on Windows 8, and users cannot browse the URL provided in the OnGuard remediation messages.

Table 41 *Known Issues in OnGuard (Continued)*

ID	Description
	Auto-Remediation fails if the OnGuard agent is installed by a domain user (non-administrator). Two workarounds are available: **Workaround 1**: Install OnGuard using administrator privileges from the command prompt. Command to execute: `msiexec /i ClearPassOnGuardInstall.msi` **Workaround 2**: Use the EXE version of the installer (ClearPassOnGuardInstall.exe) to install OnGuard.
10165	**Symptom:** ClearPass OnGuard cannot restrict the clients based on Windows service packs. **Scenario:** If any of the Windows System Health Validator check fails, the health status of client is set to unhealthy but no SoHR is send to OnGuard. OnGuard cannot display a specific remediation message; however, the icon is set to Red shield to indicate the client is Unhealthy. **Workaround:** There is no workaround at this time.
11806	**Symptom:** ClearPass OnGuard 6.1 does not support Sophos 10.0.4 on Windows XP SP3. **Scenario:** The ClearPass OnGuard/VIA+Onguard crashes on Windows XP SP3 if Sophos AV is configured with full scan time. **Workaround:** There is no workaround at this time.
12342	The OnGuard agent fails to collect health on Windows 8 if VMware Server 2.0.2.X is installed.
13164	**Symptom:** The hardware installation pop-up dialog appears to stop installing the ClearPass OnGuard Unified Agent for VIA+Onguard mode. A warning message similar to “The software you are installing... has not passed Windows Logo testing” might be displayed during installation. **Scenario:** This might occur during the installation of the ClearPass OnGuard Unified Agent on WinXP and Windows 2003 SP2. **Workaround:** Users should click **“**Continue Anyway**”** to proceed.
13363	**Symptom/** On MAC OS, The current version of the ClearPass OnGuard Unified Agent VPN component does not show some VPN related information—for example, tunnel IP assigned by the controller, packet count, or diagnostic details. **Scenario:** This occurs on MAC OS. It does not occur on Windows OS.
13379	Uninstalling OnGuard is not supported from the UI. Users must currently run the following script from the CLI for in order to remove OnGuard from the system completely: `/usr/local/bin/clearpassonguarduninstaller.sh`
13676	OnGuard no longer supports the Client Certificate Check feature, which was available in prior versions.
13677	OnGuard does not support the External Captive Portal Support feature.
13929	At times, OnGuard may fail to detect peer-to-peer applications, such as Bittorrent/uTTorrent, on Windows 2008 R2
13935	OnGuard does not support enabling/disabling the Windows Update Agent Patch Management Application.
13970	After anti-virus software is installed, the system must be rebooted before using ClearPass OnGuard.
14196	ClearPass OnGuard will not be able get the correct status of 'Software Update' PM application on Mac OS X, if “Check for updates” and “Download updates automatically” are not toggled at least once.
14673	The Mac OnGuard Agent does not support bouncing of a VPN Interface other than the Aruba VPN Interface (version 6.1).
14760	In some cases, OnGuard fails to connect to the CPPM server from a wired interface if the VPN is connected from a trusted network.
14842	Installing the ClearPass OnGuard Unified Agent removes an existing VIA installation. To continue to use VPN functionality, go to **Administration > Agents and Software Updates > OnGuard Settings** and select **Install and enable Aruba VPN component** from the drop-down list.
14996	If McAfee VE is running on Windows XP, the ClearPass OnGuard Unified Agent VPN will not work.
15072	VIA connection profile details are not carried forward after upgrade from VIA 2.0 to ClearPass OnGuard Unified Agent 6.1.1.
15097	The ClearPass OnGuard Unified Agent does not support installation of a VPN component on Mac OS X 10.6.

Table 41 *Known Issues in OnGuard (Continued)*

ID	Description
15156	VPN configuration is not retained after upgrading to the ClearPass OnGuard Unified Agent using MSI Installer on a 64 bit Windows system.
15233	On Win 7 (64 Bit), upgrading an existing VIA 2.1.1.X to the ClearPass OnGuard Unified Agent can lead to an inconsistent state. Users should first uninstall VIA and then proceed with the ClearPass OnGuard Unified Agent installation.
15362	Portable versions of applications and antivirus (AV) cannot be detected by OnGuard.
15586	**Symptom:** The ClearPass OnGuard 6.2 Dissolvable agent does not support the following new health classes on Mac OS X: Processes, Patch Management, Peer-To-Peer, Services, USB Devices, and Disk Encryption. The Dissolvable Agent (DA) does not display these health classes as remediation messages in the user interface because java binary sdk support is not included. **Scenario:** The client will be unhealthy if any of the health classes listed above are configured and performing a health scan via the DA.
15956	ClearPass OnGuard does not support enabling RTP and start Full System Scan for Microsoft Forefront Endpoint Protection 2010 Antivirus.
15986	ClearPass OnGuard returns the product name of Microsoft Forefront Endpoint protection AntiVirus as “Microsoft Security Essential”.
16181	**Symptom:** The command level process can be detected using the path **“**none**”**, but the application level process can't be detected by setting the path to “none”. **Scenario:** This applies to MAC OS. **Workaround:** The application-level process health should be configured with the path set to **Applications > Firefox.app**.
16550	**Symptom/Scenario:** The ClearPass OnGuard Unified Agent does not support checking of disk encryption state using the Mackeeper (ZeoBIT LLC) Disk Encryption Product on MAC OS X. This causes the client to be treated as healthy even if none of the disk is encrypted. **Workaround:** There is no workaround at this time.

WorkSpace

Table 42 *WorkSpace Known Issues in 6.2.5*

Bug ID	Description
11152 12541	**Symptom/Scenario:** The WorkSpace app uses the native iOS email app for sending debug logs. **Workaround:** Users must configure their native iOS email client in order to send debug logs to the administrator.
11315	**Symptom/Scenario:** If **“**Allow app to email the document**”** is not enabled, then users cannot send the document using the e-mail option in Open-IN. **Workaround:** Select the e-mail application (Ikonic or TouchDown) from the list of applications shown in the open-IN dialog.
12095	**Symptom:** Dolphin displays a blank page when a Network Access Policy is applied. **Scenario:** In a Network Access Policy, the type of value specified in the **“**Hostname/IP/range**”** field must match that of the “Redirect to Server” field. **Workaround:** If a hostname is used in the **“**Hostname/IP/range**”** field, then a hostname must be used in the “Redirect to Server” field. Similarly, if IP/range is used, it must be used in both fields.
12683	Insight reporting is not supported for WorkSpace in 6.2.
12726	**Symptom/Scenario:** A user search for a location on a map might appear to give the wrong coordinates. In fact, for geo-fencing co-ordinates, when multiple results are returned for a search string, the first result returned is used.

Table 42 *WorkSpace Known Issues in 6.2.5 (Continued)*

Bug ID	Description
12739	**Symptom/Scenario:** Accessing self-signed certificate Web sites via https does not work with Dolphin for the Aruba App. If the user clicks to accept the certificate when prompted, the page loading process goes into a loop and the screen flickers. **Workaround:** Add the certificate to the trusted store before accessing the resource.
12752	**Symptom:** On some devices, the Box app might not show the 'Use' option after capturing a video. **Scenario:** This situation can occur with policy-enabled apps. It does not occur with personal apps. **Workaround:** There is no workaround at this time.
14654	**Symptom:** WorkSpace cannot detect and prevent cloud apps such as Box from providing the option to email a document within the application that uses email on the server. **Scenario:** If sharing is not disabled, files can be sent to any outside users from the registered email account. **Workaround:** The IT administrator should disable the Share option in Box.
14758	**Symptom:** An error page or a Google search page is displayed when a URL is tapped in an email application. **Scenario:** This occurs if Dolphin is configured as the default browser and the hostname URL is selected from a policy-enabled app. When a URL is tapped in a policy-enabled email application, WorkSpace opens the link in the policy-enabled browser. If the destination is an internal resource and if the VPN is not connected, then an error page or a Google search page is displayed. **Workaround:** Refresh the page after the VPN connection is established.
14992	**Symptom/Scenario:** When a File is uploaded to Box from another application, the preview for the file may not be displayed correctly. **Workaround:** There is no workaround at this time.
15228	**Symptom:** The **"**Enforce Apps up to date**"** option does not work on the client in this version. **Workaround:** The user should manually check for updates to third-party applications.
16123	**Symptom:** Devices and users cannot be deleted from WorkSpace. **Scenario:** The Delete button removes the device or user from the page but not from the database, and the device or user is displayed again when the page is reloaded. **Workaround:** There is no workaround at this time.
16428	**Symptom:** Changing the value of "Minimum SDK version for partner apps" in a WorkSpace Policy will make all provisioned WorkSpace apps unusable. **Scenario:** This situation occurs in all WorkSpace apps assigned the WorkSpace policy in which the Minimum SDK version for partner apps" field is changed. This field is in **WorkSpace Configuration > WorkSpace > [WorkSpace Settings] > Edit > iOS Devices**. **Workaround:** Delete and reinstall WorkSpace to update the user device ID.
17160	ADCS is currently not supported for MDM and WorkSpace.