# ClearPass 6.3.1


Release Notes

## Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include  , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

## Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

## Warranty

This hardware product is protected by an Aruba warranty. For details, see Aruba Networks standard warranty terms and conditions.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

# Contents

# Chapter 1

# About ClearPass 6.3.1

ClearPass 6.3.1 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 9—Provides upgrade instructions and considerations.
- Chapter 3, “What’s New in This Release” on page 11—Describes new features and issues introduced in this 6.3.1 release as well as issues fixed in this 6.3.1 release.
- Chapter 4, “Enhancements in Previous 6.3.x Releases” on page 21—Describes new features introduced in earlier 6.3 releases.
- Chapter 5, “Issues Fixed in Previous 6.3.x Releases” on page 31—Lists issues fixed in earlier 6.3 releases.
- Chapter 6, “Known Issues Identified in Previous Releases” on page 37—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

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.

#### 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
- 500 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)
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

### CP-VA-5K

- 8 Virtual CPUs
- 500 GB disk space
- 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)
- 1024 GB disk space
- 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-VM-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
- 80 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.

VMware Player is not supported. Please contact 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 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. A complete, current list is also available as an appendix in the CPPM online help.

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


Some third-party anti-malware products are not supported by ClearPass OnGuard. For a complete list of supported third-party products, in CPPM go to **Administration > Agents and Software Updates > OnGuard Settings**, click the **Help** link, and then click the **OnGuard Agent Support Charts** link.

## ClearPass Dissolvable Agent Requirements

The latest Java version is required in order to perform client health checks using the new Web login flow.

## 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

**Table 1** *Contact Information*

| | |
|---|---|
| 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)<br>1-408-754-1200 |
| International Telephones | http://www.arubanetworks.com/support-services/support-program/contact-support |
| Software Licensing Site | licensing.arubanetworks.com |
| End of Support information | http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/ |
| Wireless Security Incident Response Team (WSIRT) | http://www.arubanetworks.com/support-services/security-bulletins/ |
| Support Email Addresses | |
| Americas and APAC | support@arubanetworks.com |
| EMEA | emea_support@arubanetworks.com |
| WSIRT Email<br>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 6.3 release.

## Upgrading to ClearPass Policy Manager 6.3

You can upgrade to ClearPass Policy Manager 6.3 from ClearPass Policy Manager 5.2.0 (non-VM), 6.0.x, 6.1.x, or 6.2.x.

- Upgrade images are available within ClearPass Policy Manager from the Software Updates Portal at **Administration > Agents and Software Updates > Software Updates**.
- 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 6.3.
- 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.


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.

### Before You Upgrade

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

- Plan downtime accordingly. Upgrades can take longer (several hours) if you have a large log database. Upgrades can also take longer (several hours) if your number of audit records is large (hundreds of thousands) due to MDM integration with ClearPass.
- 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.
- 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 have two disks already loaded with previous ClearPass versions—for example, 6.1 on SCSI 0:1 and 6.2 on SCSI 0:2—then drop the inactive disk before upgrading. You must then add a newer disk that is twice the size of the old disk. The ClearPass installation will partition this disk into two logical volumes.


Never remove SCSI 0:0

# Chapter 3

# What's New in This Release

This chapter provides a summary of the new features and changes in the ClearPass 6.3.1 release.

This chapter contains the following sections:



## Release Overview

ClearPass 6.3.1 is a monthly patch release that introduces new features and provides fixes for known issues. The 6.3.1 cumulative patch update is available in Policy Manager under **Administration > Agents and Software Updates > Software Updates**.

### Before You Update

When you install the patch on a cluster, update the Publisher first before applying the update on Subscriber nodes.

When the patch installation is complete, the **Needs Restart** status is displayed on the Software Updates page. Log out and log in again to restart the system.


If you are installing the 6.3.1 patch through the Software Updates portal of the CPPM UI, the update progress indicator might stall. If this happens, refresh the browser window to show the updated progress.


In some cases, access to the ClearPass UI will not be available during the patch installation, but it will automatically recover. If this happens, wait for a few seconds, refresh the browser window, and then view the updated page to confirm the patch installation is complete.
After the patch installation is complete and the server has been rebooted once, you might experience errors in TACACS or WebAuth requests. If this happens, go to **Administration > Server Manager > Server Configuration > Services Control tab** and restart the **System auxiliary services** for the server.

## New Features and Enhancements in the 6.3.1 Release

### Policy Manager

- Support was added for the ability to add a banner to the ClearPass Policy Manager and ClearPass Guest login pages and the CLI. The banner can be used to notify users of any Web site access restrictions due to government regulations. (#13304)

- A Password Type attribute was added to the Generic SQL DB authentication sources to support RADIUS authentications when the authentication source contains passwords in cleartext, SHA, SHA256, NT Hash or LM Hash formats. (#19778)
- The Remote Assistance session feature now enables the TAC engineer to view the customer's ClearPass Administration UI as part of being able to login to arubasupport shell.(#20707)
- Support was added for redirection to a configured ClearPass Portal landing page when the user goes to https://CPPM-Server. This is in addition to the existing redirect support for http://CPPM-Server. (#20869)
- The Access Tracker will show an alert if more than two anti-malware products are detected on the client. (#20900)
- Palo Alto integration is now extended to Guest MAC Caching use cases. When the Session Restriction Enforcement Profile for a Palo Alto user ID update is configured with "Session-Check::Username = %{Endpoint:Username}", PostAuth will send the Guest username instead of the MAC Address in the user ID updates. (#20996)

## Dissolvable Agent

The OnGuard Web Agent help page now includes a section with recommendations and solutions to common problems. (#20751)

## Guest

- Support was added for the Twilio SMS gateway. (#21304)
- Arabic, German, and Dutch translation packs were added. (#21024, #21300, #21301)
- Support was added for languages that are written right-to-left (rtl). (#21302)

## Onboard

Two new attributes were added to the Certificate namespace. These attributes will contain the values of the mdpsCustomField and mdpsEmailAddress fields of an Onboard certificate: (20705)

Subject-AltName-DirName-OnboardCustomField

Subject-AltName-DirName-OnboardEmailAddress

## OnGuard

- Support was added for the following products: (#17996)
  - McAfee VirusScan 17.x
  - McAfee Personal Firewall 14.x
  - MacKeeper 2.x
  - ZoneAlarm Internet Security Suite 12.x
  - Bitdefender Antivirus Free Edition 1.x
  - Trend Micro Endpoint Encryption 5.x
  - McAfee All Access Internet Security 3.x
  - Dr.Web for Mac 9.X
  - Kaspersky PURE [HD Encryption] 13.x
  - Kaspersky Anti-Virus 14.x
  - Avira Server Security 14.x

  Support was enhanced for the following products:
  - Symantec Endpoint Protection 12.1.x

- Trend Micro OfficeScan Client 10.x
- Microsoft Windows Firewall 8
- Kaspersky Anti-Virus 13.x
- Symantec Encryption Desktop 10.x
- BitLocker Drive Encryption 6.x
- Norton AntiVirus 12.x
- Trend Micro OfficeScan Client 10.x
- AVG Internet Security 13.x
- AVG Internet Security 2012.xd on the report.

- A new **Health Check Interval (in hours)** attribute was added to the Onguard Agent enforcement profile. Administrators can use this attribute to define different Health Check Quiet Periods for different users, such as students or staff. The ClearPass OnGuard Unified Agent gives preference to the Health Check Quiet Period value received in the enforcement profile over the value configured in Global Agent Settings. If the Health Check Quiet Period value is not configured in the enforcement profile, the Global Agent Settings value is used instead. (#19371)
- A new **Health Logs** option was added under the **Diagnostic** tab. The health logs display diagnostic logs related to OnGuard health checks and CPPM server reachability on various network interfaces. This option is available on both Windows and Mac OS X. (#19385, #20898)
- The following items were added: (#20272)
  - A new field for Registry Keys to let you specify a custom message for failed Registry Key Checks
  - A Monitor Mode for the Registry Key Health Class
  - Registry Key Health Class Posture Check results in **Access Tracker > Output tab > Posture Evaluation Results** section
- In previous versions, the OnGuard Agent sent two WebAuth requests if any of the following health classes were configured: (#20896)
  - Installed Applications
  - Processes
  - Registry
  - Services
  - Windows Hotfixes

  Now the OnGuard Agent will send two WebAuth requests only the first time after installation. After that, the OnGuard Agent will send only one WebAuth request having information of the health classes listed above, and will do so only in the case of agent restart, machine restart, or user login/logout.

  For Mac OS X, this is applicable for the following health classes:
  - Installed Applications
  - Processes
  - Services
- OnGuard's backend service will not collect health if the OnGuard Agent (front end) is not running. This will reduce OnGuard CPU usage on client machines. (#20945)

# Issues Resolved in the 6.3.1 Release

The following issues have been fixed in the ClearPass 6.3.1 release.

## Policy Manager

The **Update** button has been removed from the **Monitoring > Live Monitoring > System Monitor** page. The System Monitor page will now be automatically refreshed every two minutes.

**Table 4** *Policy Manager Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 15253 | The swap space size in the **System Monitor** page reported an incorrect value after a restore and reset-database operation. |
| 17769 | During a patch installation through the user interface, the **Clear and Close** button was enabled before the installation was complete, and the error message “Install Error - Object Object” was displayed instead of the log file. |
| 18765 | The computed attribute Date:Date-Time was not populated for all WebAuth requests on Access Tracker. |
| 19983 | To avoid display of bulk response for Server Actions, the output of actions triggered for more than one Endpoint is suppressed in CPPM's Admin UI. |
| 20208 | Corrected an issue with onboarding Windows 8.1 clients. |
| 20289 | During upgrade, the SNMP settings for the CPPM server, including sysLocation and sysContact settings, were not retained and empty values were shown on the **Administration > Server Manager > Server Configuration** page. |
| 20292 | The **Last updated time** field on the **Monitoring > Live Monitoring > System Monitor** page displayed time based on the time zone of the CPPM node where the user was viewing the page. |
| 20414 | Links in Admin UI for import and export actions in all the summary pages now use simple “Import” and “Export All” text. |
| 20418 | When trying to integrate AirWatch with CPPM, the endpoint table was not updated with fetched information from AirWatch. This occurred if some AirWatch managed devices did not have a MAC address. |
| 20482 | Dashboard customization was lost after the dashboard page was refreshed. This sometimes occurred if multiple browser sessions or multiple sessions were accessing Dashboard simultaneously. |
| 20505 | Post Auth Simultaneous Session checks happened only once in the Guest MAC caching flow. This would happen if the session check was enforced for the user as a result of the Guest MAC caching service followed by MAC Authentication from the device. |
| 20517 | OpenSSL is upgraded to openssl-1.0.1e-6. This version fixes multiple security issues in OpenSSL, including CVE-2013-4353, CVE-2013-6449, and CVE-2013-6450. |
| 20597 | When trying to add a certificate to the trust list, the Chrome and Internet Explorer browsers sometimes produced the error “Content-type ‘application/x-pkcs7-certificates’ is not supported”. |
| 20626 | If a registered AirGroup device was removed from ClearPass Guest 6.3.0 and later added again, AirGroup functionality did not work for that device. |
| 20631 | With the introduction of AirWave integration with Policy Manager, the Access Tracker ‘s **Request Details** form included a link to open AirWave, but single sign-on was not available. |
| 20690 | Corrected integration issues in fetching endpoint details from MobileIron version 5.9 and higher. |
| 20806 | An incorrect license usage warning was displayed for application licenses in the CPPM Event Viewer. |
| 20814 | Corrected various issues to create better PostAuth performance. |
| 20815 | In the case of certain large backups, the Admin UI stalled at “migrate data” and the restore operation never completed. |

**Table 4** *Policy Manager Issues Fixed in 6.3.1 (Continued)*

| Bug ID | Description |
|---|---|
| 20847<br>20496 | If a CPPM configuration was modified under a high load, RADIUS authentication failures with SSL related errors and/or RADIUS server crashes sometimes occurred. |
| 20809 | The CPPM System Information summary did not show the correct disk usage. |
| 20870 | The **Default Service** template on the **Configuration > Start Here** screen could not be modified if the IE browser was used. |
| 20894 | Using the IPAddress or MACAddress type attributes in CPPM policy rule conditions produced an error. |
| 20899 | The Request Tracker logs now show logs for failed health checks in the INFO log level. |
| 21013 | Corrected an issue with migration of “GuestUser:[Role ID]” to “GuestUser:Role ID” when used in Enforcement Profiles. |
| 21036 | The process statistics of Stats Collection Service and Stats Aggregation Service were not displayed on the **System Monitor** page. |
| 21133 | A failure in copying data from the publisher caused subscriber setup to fail in some cases. |
| 21135 | Manual updates of unknown endpoints were not reflected in the endpoint database or at **Monitoring > Live Monitoring > Endpoint Profiler.** |
| 21191 | Unauthenticated read-only access was allowed to the Graphite tool in ClearPass. Although this tool does not have any sensitive data, it provides metrics of the various counters that are used to determine the performance of the ClearPass system. With this fix, access to Graphite and related resources is blocked by default, and the admin has to manually allow subnets or hosts to access the Graphite Web app in ClearPass. |
| 21294 | The password field would be cleared when editing the **Authentication Sources** configuration form. |
| 21297 | When validating a SQL query used in an authentication source filter, the error message “Invalid SWL syntax - FATAL: password authentication failed for user “appadmin” was displayed. |
| 21422 | Corrected an authentication failure issue in the selection of a domain controller used for MSCHAPv2 authentications when CPPM was joined to multiple domains with a trust relationship. |
| 21528 | Apache Tomcat is upgraded to the latest version, Tomcat 7.0.52. |
| 21546 | On the M**onitoring > System Monitor** page, the network counters now print more accurate values for the different protocols. |
| 21643 | MSCHAPv2 authentication failed if the password had non-ASCII characters and CPPM retrieved the cleartext password from a generic LDAP or external SQL authentication source or from an internal database. |
| 21695 | During a patch installation, although the installation was complete and the reboot was initiated, the corresponding entry in the **Updates** table incorrectly said “Install in Progress.” The entry now correctly says “Rebooting” instead of “install In Progress.” |
| 22015 | An administrator with read-only privileges could alter SSO SAML IdP data. |
| 22065 | When downloading the Guest skin or updates from the **Administration > Software Updates** page, the process would hang and the error message “Download is stuck or interrupted. Please run Check Status Now and retry” was displayed. The **Download** button is now correctly displayed when **Check Status Now** is clicked. |

## AirGroup

**Table 5** *AirGroup Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 21589 | Corrected an issue where editing the SSH Timeout for an AirGroup Controller did not take effect. |

## CLI

**Table 6** *CLI Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 20275 | Corrected an issue that allowed execution of commands when combined with certain special characters as a part of netjoin process. |
| 21098 | The CLI option to restore backups without passwords has been deprecated.<br>The usage for the “restore” command is updated to reflect this:<br>`[appadmin@venkat-dev-1]# restore`<br>Usage:<br>`restore user@hostname:/<backup-filename> [-l] [-i] [-b] [-c] [-r] [-n\|-N] [-s] [-u]`<br>`restore http://hostname/<backup-filename>[-l] [-i] [-b] [-c] [-e] [-n\|-N] [-s] [-u]`<br>`restore <backup-filename> [-l] [-i] [-b] [-c] [-r] [-n\|-N] [-s] [-u]`<br>Where:<br>`-b` = do not backup current config before restore<br>`-c` = restore CPPM configuration data<br>`-l` = restore CPPM session log data as well if it exists in the backup<br>`-r` = restore Insight data as well if it exists in the backup<br>`-i` = ignore version mismatch and attempt data migration<br>`-n` = retain local node config like certificates etc. after restore (default)<br>`-N` = do not retain local node config after restore<br>`-s` = restore cluster server/node entries from backup<br>The node entries will be in disabled state on restore<br>`-u` = upgrade process invoked restore command |
| 21592 | Corrected the message that is printed when the `configure fips-mode` command is executed without any parameters. It now correctly says `configure fips-mode` instead of `update-fipsmode`. |

## Guest

**Table 7** *Guest Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 21669 | Ampersand (&) characters in a password were not correctly escaped for server-initiated Web login (WebAuth) requests. |
| 21755 | Guest SAML IDP now looks for the sso_token parameter before checking the browser cookie. |
| 21594 | An issue prevented some debug-level Onboard messages from appearing in the Application logs. |
| 21307 | The XML-RPC method `amigopod.guest.list` previously returned both guests and devices. It is now updated to return only guests. To retrieve devices, use the `amigopod.mac.list` method. |
| 21363 | Corrected a database query error in data migration from 6.2 to 6.3. |
| 21311 | The {nwa_radius_query} function returned incorrect results for a valid MAC address. |
| 20746 | XML-RPC calls API calls to create MAC devices did not work in 6.3.0. |
| 21309 | The APIs used to retrieve a single user did not return the guest password although permissions allowed them to do so. |
| 21339 | A guest account set to not expire was displayed in Insight reports as having an expiration time of 1970-01-01 00:00 UTC. A blank value for the expiration time is now displayed for accounts that are set to not expire. |
| 21367 | Certain user account filter expressions specified in an operator profile sometimes resulted in a database query error. |

**Table 7** *Guest Issues Fixed in 6.3.1 (Continued)*

| Bug ID | Description |
|---|---|
| 20744 | Custom fields created with capitol letters in their names were exported as blank to CSV and TSV format. |
| 20745 | Auto-sending emails and SMS from a self-registration did not work correctly. |
| 21341 | The contents of a Zip file containing a directory did not show up in Content Manager after extraction. |

## Insight

**Table 8** *Insight Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 19507 | PDF & HTML Data Tables were not created if the CSV file size was larger than 1MB, although the generated PDF and HTML reports did include analytics if configured on the report. |
| 20860 | When a report that included a CPPM Node condition was edited, the IP address that was added did not appear in the report. The appropriate value is now shown. |
| 20930 | When the browser was set to the Chinese or Japanese language, the Insight report creation page did not display the **Column Type** or **Available Column** fields. |

## Onboard

**Table 9** *Onboard Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 20427 | id-kp-eapOverLAN extended key usage is now added when creating a trusted certificate in Onboard. |

## OnGuard

**Table 10** *OnGuard Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 18180 | Windows 8 clients failed to submit health information or took longer to submit because of the Windows Update service. |
| 19366 | To improve performance, the ClearPass OnGuard Unified Agent now collects health only for health classes which are configured on the server. |
| 19378 | When upgrading from VIA 2.1.1.3 to the ClearPass OnGuard Unified Agent, a known issue with uninstalling VIA launched a popup asking the user to select the VIA driver. |
| 20525 | The ClearPass OnGuard Unified Agent is unable to detect the Microsoft Windows firewall properly on Windows 8 if the endpoint has domain network settings in addition to Private/Public settings for enabling or disabling Wi-Fi. |
| 20717 | The OnGuard Persistent Agent on a Windows 7 client read the status of the floppy drive (A:) every minute even if the USB Devices health class was not configured. |
| 20856 | The Enabled status check did not work for the System Center Configuration Manager (SCCM) patch management application. |
| 21332 | On Mac OS X, a wireless interface was sometimes categorized as wired due to incorrect information reported by system configuration. |
| 21432 | Editing the Patch Management Health class configuration for “Any Supported Patch Agent” at **Configuration > Posture > Posture Policies** produced the error “InternalError: Null Element". |
| 21448 | On Mac OS X, logs were not sent if OnGuard’s backend service stopped. |

### QuickConnect

**Table 11** *QuickConnect Issues Fixed in 6.3.1*

| Bug ID | Description |
|---|---|
| 21020 | Windows 7 machines could not be onboarded to connect to a hidden SSID. |

## New Known Issues in the 6.3.1 Release

The following known issues were identified in the ClearPass 6.3.1 release.

### Policy Manager

**Table 12** *Policy Manager Known Issues in 6.3.1*

| Bug ID | Description |
|---|---|
| | If you are installing the 6.3.1 patch through the Software Updates portal of the CPPM UI, the update progress indicator might stall. If this happens, refresh the browser window to show the updated progress. |
| | In some cases, access to the Administration UI will not be available during the patch installation, but it will automatically recover. If this happens, wait for a few seconds, refresh the browser window, and then view the updated page to confirm the patch installation is complete.<br>After the patch installation is complete and the server has been rebooted once, you might experience errors in TACACS or WebAuth requests. If this happens, go to **Administration > Server Manager > Server Configuration > Services Control tab** and restart the **System auxiliary services** for the server. |
| 20943 | **Symptom/Scenario:** After upgrading from 6.2.0 to 6.3.0, the WorkSpace Attributes under Service Rules, Role Mapping, and Enforcement Policy Rules are not updated. In 6.2, under **Enforcement Policy > Rules**, the WorkSpace Dictionary Items are used with Application:WorkSpace:<Attribute>. In 6.3 this is changed to Application:ClearPass:<Attributes>. |
| 21015 | SNMP v3 read with non-privileged security levels (NOAUTHNOPRIV and AUTHNOPRIV) is allowed even if the AUTHPRIV security level is selected. |
| 21334 | **Symptom/Scenario:** If ClearPass is signed with an EC-based HTTPS server certificate and accessed from the FireFox browser or older versions of Internet Explorer (IE), the UI does not launch.<br>**Workaround:** Use the latest version of IE, or the Chrome browser instead. |
| 21444 | **Symptom:** The CPPM Administrator UI is not accessible after upgrading to 6.3.0.<br>**Scenario:** This occurs only if the private key provided for the CPPM Server Certificate in the earlier version is not PKCS12 format, or if the key length is less than 1024 bits.<br>**Workaround:** Follow these steps:<br>1. Before upgrading to 6.3.0, export the Server Certificate and save it.<br>2. Create a new self-signed certificate and make sure the key length is at least 1024 bits long, and then update the Server Certificate.<br>3. Proceed with the upgrade.<br>4. After the upgrade, log in to the Admin UI and import the Server Certificate that was saved in step 1.<br>In case these steps were not done before the upgrade, boot back to the older version partition and follow these steps. |
| 22023 | **Symptom/Scenario:** Launching the customer's ClearPass user interface through Proxy does not work on the Internet Explorer or Safari browsers.<br>**Workaround:** Use the Chrome or Firefox browser instead. |
| 22036 | After the Aruba Support SSH session (established by TAC engineer) is terminated, the TAC engineer must manually exit the SSH tunnel session established between the TAC engineer's host and the Remote Assistance Server. |
| 22068 | The SSO flow with certificate check only works using the CPPM RADIUS server certificate; at this time it does not work with the Web server certificate. |

**Table 12** *Policy Manager Known Issues in 6.3.1 (Continued)*

| Bug ID | Description |
|---|---|
| 22132 | EAP-MSCHAPv2 fails with Oracle DB as the authentication source if the password contains Non-ASCII characters. |
| 22097 | **Symptom:** When adding or editing external databases as authentication sources, error messages are displayed.<br>**Scenario:** This has been observed for two different conditions. In both cases, the message is benign:<br>• For any authentication source that is using an external database, adding or editing filters sometimes displays errors such as “Invalid SQL syntax - The server does not support SSL.” This message simply indicates that the external server that is set up as the authentication source is not set up for communication over SSL. Authentications are happening correctly over the non-SSL port.<br>• Using the Oracle DB as an external authentication source produces errors such as “Invalid SQL syntax - Connection refused. Check that the hostname and port are correct and that the postmaster is accepting TCP/IP connections”. This message is benign; there is no actual problem with the backend communication to the Oracle DB.<br>**Workaround:** Save the filter queries and authentication source after adding or editing it. The backend authentications should not be blocked or affected in any way. |

## Onboard

**Table 13** *Onboard Known Issues in 6.3.1*

| Bug ID | Description |
|---|---|
| 23287 | **Symptom:** Embedding Admin credentials for onboarding does not work in Windows 8 and above. The system hangs and there is no error message.<br>**Scenario:** When onboarding Windows systems with Windows 8 and above, if operations requiring admin privileges are configured, then the end user doing the onboarding needs to have admin privileges on the system. These operations include installing applications, configuring wired network,s installing certificates in the machine certificate store, and so on. Embedding admin credentials along with the QuickConnect wizard for this purpose does not work for Windows 8 and above.<br>**Workaround:** There is no workaround. This is a Windows system limitation. |

## OnGuard

**Table 14** *OnGuard Known Issues in 6.3.1*

| Bug ID | Description |
|---|---|
| 21077 | The ClearPass OnGuard Unified Agent does not support Parallels Desktop 9 on Mac OS X. |

# Chapter 4

# Enhancements in Previous 6.3.x Releases

This chapter provides a brief summary of the features and enhancements introduced in previous ClearPass 6.3.x releases.

## Features and Enhancements in Previous 6.3.x Releases

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

### Policy Manager

- CPPM 6.x changed the format of the configuration files written when CPPM is joined to an AD Domain. Migration of these files from the 5.x format to the 6.x format is not possible because administrator credentials are required, and these are not stored on CPPM. If you are upgrading from 5.x to 6.3, then you must leave the AD domain and then re-join after the upgrade is complete. (#10516)
- End-to-end RADIUS authentication testing capability was added at **Configuration > Policy Simulation** to aid in troubleshooting and diagnostics. It includes Basic RADIUS auth via radclient, EAP-TLS RADIUS auth via eapol_test, and Active Directory/MSCHAPv2 tests. (#10571)
- The **Monitoring > Live Monitoring > System Monitor** page now includes additional I/O performance graphs. (#11980)
- Added support for ClearPass to act as a SAML identity provider (IdP). (#12195)
- A new tab, **ClearPass**, was added to the **Monitoring > Live Monitoring > System Monitor** page. The graphs on this tab provide statistics on time taken and counts for service categorization, authentication, authorization, role mapping, posture validation, audit scan, enforcement, and end-to-end request processing. (#12329)
- You can now use the Access Tracker to select the node zones as a selection server/domain field and restrict search on the nodes in the zone. At **Monitoring > Live Monitoring > Access Tracker**, click the session's row in the list and click **Edit**. In the **Select Server/Domain** field, select the default (2 servers). (#12332)
- Separate certificates can now be used for Web logins and RADIUS 802.1x. (#12383)
- The system Monitor page is enhanced to provide system monitoring information for various network services and ClearPass performance. The information includes: (#12393)
  - Authentication and authorization counters
  - Authentication and authorization delays
  - Request processing delays
  - Network traffic information (RADIUS, TACACS+, Database, SSH, NTP, HTTP/HTTPS, OnGuard, etc.)
  - CPU load information
- ClearPass Policy Manager now supports Suite B cryptographic algorithms. (#12635, #17075, #17454)
- An IETF CoA template was added to allow an IETF profile to be associated with and dispatched from the CoA module, with no dependencies on the selected NAS vendor. (#12923, #18751)
- The **Monitoring > Blacklisted Users** page allows users to view the list of users who are no longer eligible to access your network. This monitoring page also shows whether the following attributes have been exceeded: - Bandwidth limit - Session count - Session duration. (#13029)

- An online/offline status indicator for endpoint devices was added to **Configuration > Identity > Endpoints > Edit Endpoint** and to **Monitoring > Live Monitoring > Access Tracker > Request Details**. (#13550)
- New templates were added to the **Configuration > Service Template** page. (#14177)
- This version of Policy Manager includes an improved method for fetching data from MDM vendors. The Policy Manager Endpoint Context Server (MDM) integration now includes the following additional support: (#14392)
  - Data retrieval via paging
  - Ability to change URLs used for API calls to MDM vendors
  - Refresh data from a specific MDM vendor
- Evaluation customers can now convert their evaluation VMs to a production SKU. This migration upgrades using a single disk. In addition, any configurations made during the evaluation period will be retained after converting to a production SKU. (#14509, #16631)
- The **Event Viewer** now includes events related to the RAID controller state. Note that this feature is only available for CP-HW-5K and CP-HW-25K SKUs. (#14706)
- An advanced option in the domain joining interface can provide explicit domain controller information to Samba, assisting the user to control what domain controllers CPPM will use for authentications. (#14738)
- When editing the **Server Configuration** page, the **Keep Alive Configuration** default values now display on the **Service Parameters** page for the ClearPass system services. (#15018)
- CPPM can now disconnect the client from the network when connectivity with OnGuard is lost, and a Change of Authorization (CoA) will be sent. (#14079)

  This is accomplished through the Post Auth Session Restriction Enforcement Profile and by adding: **Session-Check::Agent-Connection = Down Post-Auth-Check::Action = Disconnect**. This Enforcement Profile should be sent as a part of OnGuard authentication and will take effect when the OnGuard session ends.
- Added the ability to verify whether an Active Directory account has expired. (#15552)
- Usernames are now case-insensitive. (#15809)
- A new option was added to the **Collect Logs** feature in the UI and CLI. When selected, a backup of the configuration without password fields is generated as part of the logs generated. (#15985)
- Users can now perform backup and restore operations on just the data within Insight or another application without affecting other CPPM configurations. (#15987)
- CPPM now includes new App Auth templates for ClearPass Onboard and ClearPass Guest (App Auth is now the default for guest Web login pre-authentication checks and Onboard authorization checks). (#16018, #16019)
- The **Identity > Onboard Devices** and I**dentity > Guest Users** pages have been removed from Policy Manager. These features are now exclusively managed through ClearPass Guest. (#16023)
- The attributes Aruba-AirGroup-Shared-Group and Aruba-User-Group were added to the Aruba RADIUS dictionary. (#16083)
- Time zone settings now account for daylight savings time (DST) changes in Morocco and Israel. Morocco does not observe DST during Ramadan. Therefore, Morocco switches to Western European Time (WET) on July 7, and then reverts to Western European Summer Time (WEST) on August 10. Also, the period of DST in Israel has been extended until the last Sunday in October beginning in 2013. (#16103)
- To support more user, group, role, and location attributes, long values (greater than 247 characters) for RADIUS attributes can now be split across multiple consecutive AirGroup vendor-specific attributes. This applies to the following Aruba vendor-specific attributes: (#16116, #16110)

- Aruba-Location-Id (string)
- Aruba-AirGroup-Shared-User (string)
- Aruba-AirGroup-Shared-Role (string)
- Aruba-AirGroup-Shared-Group (string)

- Administrators can now control whether Guest account passwords are displayed in CPPM. The Admin privileges supports the allowPasswords setting to be set to either true or false. The default is false, which hides passwords for Guest accounts already configured in the Guest Users UI. This administrator privilege can also create and update Guest accounts with new passwords. (#16122)
- Policy Manager now supports receiving device profile information directly from supported Cisco infrastructure. Leveraging the Cisco device sensor technology requires HW running IOS 15.0 (SE1) (#16326
- Policy Manager now supports connecting one of its network interfaces into a network SPAN/Mirror port enabling device profiling based on DHCP traffic. (#16328)
- Security enhancements ensure that no Admin user can view users' credentials. Additionally, the Guest Users page has been removed from **Policy Manager > Configuration > Identity**. (#16337)
- Added the ability for administrators to override some attributes of the profiled status of an endpoint. On the **Configuration > Identity > Endpoints > Edit Endpoint** form, the user can edit the device category, family, and name. This can be used in the occasional situations where multiple device types share the same DHCP fingerprint and might be miscategorized. (#16364)
- Support was added for real-time services for asynchronous events in ClearPass, providing users faster access in situations such as integration with third-party firewalls. (#16392)
- For Palo Alto Networks Devices, the **External Context Servers** configuration page includes a new check box to indicate whether the GlobalProtect license is installed on them. If this check box is selected, CPPM sends an HIP report for the logged-in users to the configured Palo Alto Network Devices. (#16455)
- As part of support for Single Sign-On (SSO) based on Layer 2 network authentication through AOS, Policy Manager now supports SSO using the Secure Assertions Markup Language (SAML) standard. Integration with AOS version 6.4 is required. In the UI, SSO can be configured from the **Configuration > Identity** menu. (#16548)
- The Virtual IP Settings configuration form now includes an indicator to identify which CPPM node is the active VIP. (#16598)
- In the Aruba Downloadable Role configuration, support was added for Time Range and Session ACLs. (#16645)
- At **Administration > External Servers > Endpoint Context Servers**, support was added for validating the identity of the server certificate's server. The certificate must be uploaded through CPPM's standard certificate trust list. (#16734)
- Since OnGuard health checking through the dissolvable agent is now integrated with the Guest Web login workflows, the user interface at **Administration > Agents and Software Updates > OnGuard Portal** was removed from the OnGuard health-checking applet. (#16744, #16748, #10139)
- Default RADIUS COA enforcement profiles are now available for Aerohive, Motorola, and Trapeze. (#16745)
- The **Endpoint Context Server Actions** form now includes the ability to specify the HTTP enforcement actions (headers, content, and so on). METHOD types are supported, with allowed values of POST, PUT, GET, and DELETE. (#16827)
- A new Aruba vendor-specific attribute, Aruba-AirGroup-Version, was added. This VSA specifies the AirGroup protocol version currently used by the RADIUS client or RADIUS server. Enumerated values are as follows: (#16865)

- AirGroup-v1 (1): Indicates the message is AirGroup protocol version 1. This value should not be used; it is included only for completeness.
- AirGroup-v2 (2): Indicates the message is AirGroup protocol version 2.

- The AirGroup protocol version is now detected and sent in response to an AirGroup authorization request. (#16975, #16981)
- Support was added for importing Elliptic Curve (EC) Certificates into CPPM. (#17040, #17047)
- A new **Details** button on the **Administration > Certificates > Server Certificate** page displays the complete details for the certificate. (#17126)
- When viewing a record in the **Access Tracker**, users now have the ability to scroll to the previous or next records. In prior versions, users had to close the popup window to view another record. (#17221)
- AirWave was added as an external content server. (#17231)
- The Wi-Fi RADIUS dictionary is updated with attributes supporting Hotspot 2.0. (#17247)
- The maximum number of database connections can now be set as a Service Parameter. The default values for the different hardware types are: (#17392)
  - CP-HW-500 = 400 connections
  - CP-HW-5K = 700 connections
  - CP-HW-25K = 1000 connections
- ClearPass can now generate Elliptic Curve (EC) cryptography certificate signing requests. An **Algorithm** field was added to the **Certificate Signing Request** and **Create Self-Signed Certificate** forms, and includes three types of RSA and two types of EC Private Key algorithms. (#17406)
- The Access Tracker's columns can now be customized. The user can now choose columns to add or remove and change their order. (#17426)
- **Configuration > Policy Simulation** now includes support for Authentication Simulation. Options are available for the Active Directory Authentication, Application Authentication, and RADIUS Authentication types. (#17574)
- New attributes were added to the Onboard dictionary. This is a combined dictionary used for both Onboard and WorkSpace. (#17621)
- Support was added for Remote Assistance. This feature enables the ClearPass Policy Manager administrator to allow an Aruba Networks support engineer to remotely login (via SSH) to the ClearPass Policy Manager server for the purpose of debugging any issues the customer is facing or for any proactive monitoring of the server. (#17673)

  The following is a typical Remote Assistance flow:

  - The administrator schedules a Remote Assistance session for a desired duration.
  - The Aruba Networks support contact receives an email with instructions and credentials to log in.
  - The session is terminated at the end of the stipulated duration.
  - The Administrator can terminate a session before its stipulated duration from the user interface. The Support contact can terminate the session before its stipulated duration from the logged-in session.

  This feature is accessible from A**dministration > Support > Remote Assistance**.
- The Publisher and the Dedicated Publisher can now be in different subnets for publisher redundancy, accommodating environments where they might be in separate data centers. (#17815)
- The Brocade RADIUS dictionary was added. (#18204)
- License expiration warning alerts that indicate the number of days remaining for a subscription or evaluation license were added to the **Event Viewer**. Administrators can also configure notification by email alerts or the **Syslog Filter**. The alert counter starts at 120 days. (#18305)
- Users can configure the default landing page from the **Administration > Agents and Software Updates > ClearPass Portal** page. (#18635)

- The **Policy Server** now supports distributed AirGroup CoA operations across the publisher and subscribers. (#18838)
- Administrators can now use the health status of individual health classes in posture policies to tailor the enforcement profile that will be applied. The value of the attributes will be either Healthy or Unhealthy based on pass/fail checks. These attributes are then added to an internal dictionary and can be used along with Tips:Posture or independently to arrive at the appropriate enforcement profile to be sent to the client. (#18995)
- The following new attributes were added in the Certificate namespace, and are populated when clients authenticate using the EAP-TLS authentication method: (#19102)
  - Public Key Algorithm
  - Public Key Length
  - Signature Algorithm
- New system start-rasession and system terminate-rasession commands were added in 6.3. These commands allow administrators to configure and terminate a Remote Assistance session through the CLI. (#19220)
- The ClearPass Portal page was moved in the navigation hierarchy, and is now at **Administration > ClearPass Portal**. (#19363)
- Support was added for VMware ESXi 5.5. (#19541)
- ClearPass Policy Manager is FIPS 140-2 compliant through incorporation of a FIPS-validated module which provides all cryptography functions for the application. Policy Manager incorporates the OpenSSL FIPS Object Module. The OpenSSL FIPS Object Module has obtained FIPS 140-2 certificate number 1747, listed at:
  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747(#12634)

## AirGroup

- Added the ability to create user groups, and to define recurring time-based access schedules for shared devices. The user group can be assigned to users as attributes, who then have access to the shared devices only when the schedule allows access for that group attribute. (#15566)
- Limits were set on the lengths of some values. The lengths for shared user, role, location, and group name are limited to 64 characters, count to 100, and total length to 1000. (#16352)
- Added support for sending AirGroup notification messages from the CPPM server's virtual IP address, if one is configured. To enable this feature, select the appropriate network interface under **Administration > AirGroup Services > Configuration > Network Interface**. (#19938)

## Guest

- **Content Manager** now organizes content into a **Private Files** directory and a **Public Files** directory. The Private Files directory allows users to upload files that will not be accessible through HTTP or HTTPS. (#8402)
- OnGuard dissolvable agent health checking is now integrated with ClearPass Guest's Web login workflows. (#10139)
- ClearPass Guest now includes Advertising Services, letting you deliver marketing promotions and advertisements on a variety of Guest Management registration, receipt, and login pages. To use this feature, go to **ClearPass Guest > Configuration > Advertising**. (#10613)
- User interface changes in the **Edit Web Logins** page reflect added support for Wired Cisco and for generic ClearPass WebAuth. A **Login Method** drop-down list lets you select how a user's network login will be handled. (#15277)

- Support was added for secure hash-based verification of parameters passed to the captive portal during user redirection. New options for security hash and the shared secret are available on the **Edit Web Logins** page. (#15810)
- Added support for Web login pages to act as a SAML identity provider (IdP). (#15899)
- The default forms for creating guests and devices are improved. MACTrac and AirGroup Operator forms are combined, providing a single place for all user-based device registration. Administrators can now create personal AirGroup devices as well as shared AirGroup devices. (#15900)
- Guest Web logins now support Aruba Application Authentication. App Auth is now the default for guest Web login pre-authentication checks and Onboard authorization checks. (#15921, #16005, #16006)
- FIPS support was added for Guest and Onboard. (#16078)
- The PHP version was upgraded to 5.4.20. This includes fixes for CVE-2013-4248, CVE-2013-4113, CVE-2013-2110, CVE-2013-1635, CVE-2013-1643, and CVE-2013-1824. (#16108, #18267)
- Added the ability to download a guest receipt as an Apple Passbook pass. The layout and content of the pass is defined by a "pass template". (#16588)
- Guest usernames are now always handled as not case-sensitive. During migration, guest usernames that are identical except for case differences will be renamed. To find these strings after migrating to 6.3, search for the string "-renamed-". (#16593)
- Updated French translations are available. (#16632)
- Access is now available to the {$_endpoint} variable on Guest page loads. This variable holds information about the endpoint and is populated with information taken from ClearPass Profile. You can add {dump var=$_endpoint export=html} to a Web login or other guest-facing page to see the kind of information that is available. (#16648)
- Added support for the special keyword _admin in an email CC list. This enables the use of the current operator's email address as the target of an email receipt. (#17030)
- Added built-in support for bypassing the Apple Captive Network Assistant. (#17672)
- Provisioning of a device profile without network settings is now supported. (#17758)
- The **SMS Gateway** editor is updated. New capabilities include message URL encoding, HTTP Basic authentication, and support for additional success response codes. (#17936)
- Added the ability to specify the flag icon used for a translation pack in the user interface. (#19139)
- A Dutch translation pack was added. (#19172)
- Added the ability to export any overrides made to a translation pack. This file can be shared with Aruba Networks and is compatible with the translation tools. (#19261)
- Customers converting from Amigopod can now continue to use their existing page URLs without modification—for example, `/guest_register.php` does not need to be modified to `guest/guest_register.php`. (#19277)

## Insight

- Insight's alert emails are enhanced to make it easier to identify event details. At **Search > Search Alerts**, new columns match the alert conditions to the body of the email message, making it easier to

find details such as when the alert was triggered or how many failures were seen within a time window. (#11055)

- Insight is enhanced to customize columns when searching records. You can drag and drop the **Available Columns** to **Selected Columns** to get the desired search results. For administrators, the search options selected on each template are saved and can be viewed at the next login. (#11110)
- The Insight UI is enhanced to provide an option to import a report/alert template on a running system. This is useful to provide new reports without waiting for CPPM releases. A new **Select file to import** parameter is added under the **Import Insight Template** container in the **Administration** tab. (#15988)
- Insight introduced a master-slave cluster model for replicating configuration. If multiple nodes have Insight enabled, one node can be configured as a master and others can be configured as slaves. If no node is configured as master, replication will be turned off. A new **Replicate** button is introduced in the **Administration** tab to configure across the cluster nodes. Only a single node can be configured as a master. (#16456)
- Insight provides the capability to run a search and filter the reports without creating new reports or adding new fields to an existing report. Now you can filter the search results by NAD IP, CPPM node IP, and hostnames. (#16837)
- Insight is enhanced to provide search results listed in rows to view additional information that is retrieved from the database for a selected user, device, or session in the popup window. The popup window displays the following information based on the selected template: (#16860)
  - User Information
  - Device Information
  - Session Information
  - Network Information
  - Policy Information
- The Insight Dashboard is enhanced to make it more interactive, and it provides an aggregated view of authentication events for a cluster. New widgets are introduced with the option to select and unselect. Insight stores the widget display settings and location and displays them when the administrator logs in the next time. (#16907)
- The Insight Customize widget now allows you to select the graphs that display by default on your Insight Dashboard. (#19221)

## Onboard

- Support was added for installing multiple network configurations automatically using QuickConnect. (#12399)
- Added the ability to send a warning email before a user's Onboard device credentials expire. This is configured at **Onboard > Provisioning Settings > General tab > Actions > Notify users before their credentials expire**. (#12625)
- The custom fields specified on the **Provisioning Settings > Web Logins** tab are now also used when QuickConnect is used to perform device provisioning. (#14328)
- The QuickConnect client for Android and Windows has been updated to follow a similar workflow to the iOS enrollment process. (#14358)
- Implemented generic SCEP server support for Onboard Certificate Authorities. This enables Onboard to be used as a CA with third-party products that use SCEP to enroll certificates; for example, MobileIron, AirWatch, and others. (#16368)
- Corrected an issue where Mac OS X "System" profiles did not keep an 802.1x connection alive when no users were logged in. (#17036)
- Added support for SHA-384 and SHA-512 signature algorithms. (#18473)

## OnGuard

- The ClearPass OnGuard Unified Agent introduced a new **Virtual Machine** health class for Mac OS X. (#14027)
- The ClearPass OnGuard Unified Agent introduced a new **Network Connections** health class for Mac OS X that provides configuration to control network connections based on connection type. (#14030)
- The ClearPass OnGuard Unified Agent introduced a new **Installed Applications** health class on Mac OS X and Windows OS. With the introduction of this new health class, an administrator can configure what applications should be present or not present on clients. Auto-remediation is not supported for the Installed Applications health class. (#14033, #14036)
- The Enforcement Policy rules now include Per-Application-Based posture enforcement policies, based on the results of the individual Application Posture Tokens (APTs) of the health classes configured in the Internal Posture Policy. (#14080)
- The ClearPass OnGuard Unified Agent now supports detection and installation of missing patches for patch management agents such as System Center Configuration Manager (SCCM) or Microsoft Windows Update Agent on Windows. A new option, “Install Level Check,” was added for Patch Management Health Class having the values “No Check,” “All,” “Selected on Server,” and “Security.” Based on the value of the “Install Level Check,” OnGuard Agent checks missing patches and, if auto-remediation is enabled, OnGuard downloads and installs missing patches. Note: This feature is verified with Microsoft Windows Update Agent. (#15737, #12616)
- Currently, when a user clicks **Retry/Logout**, that user stays in a healthy VLAN; however, OnGuard stops monitoring the client health. To avoid this, OnGuard bounces the interface after a default of 5 minutes from when the user quits the OnGuard Agent. Now OnGuard provides the ablility to configure the number of minutes that should elapse before OnGuard bounces interfaces when OnGuard remains disconnected after Logout/Quit. A new parameter, **Delay to bounce after Logout (in minutes)**, is introduced in **Global Agent Settings**. (#15738)
- The ClearPass OnGuard Unified Agent can automatically upgrade when a newer version is available on the CPPM server. A new Agent action is introduced to determine what the OnGuard Agent should perform when an update is available. The options **Ignore**, **Notify User**, and **Download and Install** are available. This feature is only available with OnGuard Agent versions 6.3 and above. (#16756)
- Currently, all the configured health classes in a posture policy are evaluated and the evaluation result is used in determining the overall health state of the posture policy. In some cases, the administrator might want to collect information for these health classes but not want the clients to be treated as unhealthy. A new **Monitor Mode** option is added for the **Windows Hotfixes** health class to fix this issue. If Monitor Mode is enabled, then the health status of the **Windows Hotfixes** health class is set to healthy. (#16898)
- The ClearPass OnGuard Unified Agent provides the ability for an administrator to configure the desired period (in hours) for OnGuard to avoid health checks after a client is deemed healthy. The roles and client health status are cached separately, ensuring that the client health status is not deleted if RADIUS authentication fails. A new parameter, **OnGuard Health Check Interval (in hours)**, is introduced in Global Agent Settings. The default value is 0 to make sure that the health checks are not avoided. This parameter is supported only by the OnGuard Agent in Health Only mode for wired and wireless interfaces. It is not supported by the dissolvable agent or for VPN-type interfaces. (#17662, #12517)
- The ClearPass OnGuard Unified Agent for Mac OS X and for Windows is now localized in Japanese. The OnGuard UI can display text in the language that is selected during installation. (#17899, #13136)
- The online help now includes links to charts of the third-party software OnGuard supports. Charts are included for antivirus, antispyware, firewall, disk encryption, peer-to-peer, patch management, and virtual machine products. To access the support charts, go to **Administration > Agents and Software Updates > OnGuard Settings**, click the **Help** link to open the OnGuard Settings topic, and then click the right arrow to navigate to the OnGuard Agent Support Charts subtopic. (#18228)

## WorkSpace

- Added iOS 7 support for ClearPass WorkSpace. (#16416)
- The BYOD Self-Service portal supports the following MDM/WorkSpace tasks for end users. End users can perform the following actions when a device is lost or stolen: (#17442, #16271)
  - Locking a device
  - Unlocking a device
  - Wiping device data
  - App management actions such as installing or uninstalling an app
- Added support for Web apps for WorkSpace in iOS App types. All the Web apps configured in WorkSpace use the Aruba proprietary browser published in the app store. (#16757)
- Added an ability to check if a device is actively managed by MDM before allowing access to WorkSpace and WorkSpace managed apps. If the device is not MDM managed, it will be blocked from using WorkSpace or the WorkSpace managed apps. (#17445)
- Added single sign-on (SSO) login support for Enterprise apps in Aruba WorkSpace. With SSO enabled, the user can log in to WorkSpace and gain access to all WorkSpace apps without being prompted to log in again. WorkSpace uses an NTLM/Basic or form-based authentication for SSO. With NTLM/Basic authentication, users can authorize with the servers without using a password. With form-based authentication, users must enter their username, password, and/or domain name in the HTML form. (#18143)
- The following preconfigured MDM actions are available on AW and MI devices: (#20056)
  - Send Message
  - Send Message (Parameterized)
  - Lock Device
  - Unlock Device
  - Clear Passcode
  - Get Application
  - Get Labels

  To configure these actions in ClearPass Policy Manager, go to **Configuration > Identity > Endpoints**.

# Chapter 5

# Issues Fixed in Previous 6.3.x Releases

The following issues were fixed in previous 6.3.x releases. For a list of issues resolved in the 6.3.1 release, see the What's New in This Release chapter.

## Fixed in 6.3.0

### Policy Manager

**Table 15** *Policy Manager Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 10447 | Corrected an issue where IE 10 was supported only in compatibility mode. |
| 16325 | The RADIUS/TACACS shared secret size was increased from 32 characters to 128 characters. |
| 16430 | Insight Repository Filters were duplicated after upgrading or migrating to 6.2, producing two sets of the same filters in the Insight authentication source. |
| 16719 | The VIP could not be moved back to the publisher after failing over to the subscriber. When using CPPM VM deployments on a VMWare distributed switch, forged transmits should be enabled on the switch in order for the VIP feature to work properly. |
| 17320 | If the **Check Status Now** button was clicked in the **Firmware and Patch Updates** section of the **Administration > Agents and Software Updates > Software Updates** page, instead of displaying the Download button, all patches and updates were automatically downloaded. This issue was observed on 6.1.x. |
| 17333 | Onboarding users with usernames in the format DOMAIN/user did not work. |
| 17343 | The SNMP capabilities in the **Access Tracker > Change Status** feature is deprecated. This is now controlled by a new service parameter. |
| 17865 | The Receptionist admin privilege role in CPPM now maps to the Help Desk privilege role. Management of guest users is now handled through the ClearPass Guest user interface, so the no UI is needed for the Receptionist role after ClearPass login. |
| 17886 | Machine authentication failed if the machine name exceeded 15 characters. |
| 18066 | The Send Message HTTP action from AW MDM failed for JSON. |
| 18125 | RADIUS CoA enforcement profiles can now be used in Application type Enforcement Policies. |
| 18224 | In tunneled EAP methods, having different valid inner and outer identities could result in incorrect authorization handling. |
| 18438 | Additional database indexes were added to improve page load times when listing guest users. |
| 18734 | RADIUS CoA failed if an NAD IP address was configured with a 32-bit mask —for example, as a.b.c.d/32. |
| 18777 | RADIUS Auth-Sim test for TLS client certificate failed in FIPS mode. |
| 18779 | The RADIUS server stopped running if EAP-MD5 was added to a service as an authentication method along with EAP-PEAP. |
| 19650 | The CPPM 6.2.X guest portal flow has been replaced by the ClearPass Guest Web login flow. The 6.2 portal URL will redirect to tips/welcome.action page from 6.3 onwards. |

**Table 15** *Policy Manager Issues Fixed in 6.3.0 (Continued)*

| Bug ID | Description |
|---|---|
| 20277 | Corrected an issue that caused Admin UI to be slow when there was heavy Post-Auth activity to update Endpoint details. |
| 20411 | CPPM did not get updates from Aruba Activate when some device attributes were not present. |
| 20436 | The CLI command "`system boot-image -l`" is enhanced to provide information about the SCSI disk in use for VM installations. |
| 20622<br>20719 | Some user interface elements were not properly formatted or right-aligned on the Chrome browser (version 32+). |
| 20718 | After upgrading or migrating using an older version backup that includes Session records, TACACS+ session details are now correctly shown in the Access Tracker. |
| 20724 | After restoring an older backup on 6.3, some of the older and previously deleted service templates were also restored. |
| 20742 | Corrected an issue where CPPM, although properly configured, did not always output the appropriate enforcement profile when cached roles and posture were used. |
| 21364<br>18244 | Corrected a RADIUS vulnerability issue where, in tunneled EAP methods, having different valid inner and outer identities could result in incorrect authorization handling. |
| 21573 | Corrected an issue that resulted in execution of native OS commands if they were passed as an argument in certain combination to a few specific CLI commands. |
| | The subscription ID was not retained after upgrading to CPPM 6.0.2. |
| | Upgrading from previous versions to 6.0.1 failed if ClearPass Policy Manager was already joined to the domain. |

## AirGroup

**Table 16** *AirGroup Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 18272 | A new configuration option for the AirGroup controller allows the timeout value to be specified when getting configuration information from the device. This defaults to 15 seconds (up from 5 seconds in previous releases) but might need to be increased further if the controller is a master controller with many APs configured, or if network conditions require additional delay. |

## Dissolvable Agent

**Table 17** *Dissolvable Agent Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 7165 | To have Health data collection work correctly in 64bit Windows 7, please use the JRE version provided by CPPM. It can be downloaded from the following URL:<br>https://<CPPM-IP-Address>/agent/html/help.html |

## Guest

**Table 18** *Guest Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 14687 | The CSS class field available for a custom field set to type "Submit Button" was being ignored when rendering the form. The class will now be included as expected. |

**Table 18** *Guest Issues Fixed in 6.3.0 (Continued)*

| Bug ID | Description |
|---|---|
| 15684 | If the MAC delimiter for the Mac Auth profile was not set to “dash” ( - ) in the controller, CoA was not sent to the active MAC connection. CoA requests are now correctly sent to the controller regardless of the MAC delimiter setting used on the controller. |
| 15736 | Added reporting capabilities for up to 20 custom fields defined in Guest. |
| 15817 | Improved support for uploading very large files using the Content Manager. Files may now be uploaded to the maximum allowed upload size without errors or the need to adjust the PHP memory limit. The maximum allowed upload size is specified as two service parameters -- “Form POST Size” and “File Upload Size”. |
| 16218 | Changed the guest role ID attribute from “[Role ID]” to “Role ID” and removed the ability to configure the attribute name. By using “Role ID”, it will now be possible to add new guest roles to the guest role mapping policy “[Guest Roles]”. |
| 16233 | When a device is created a RADIUS Change of Authorization will be sent if the device is seen on the network. |
| 16375 | Added an error message to indicate that Windows Home versions are not supported by QuickConnect. |
| 16434 | A user waiting for sponsor confirmation that had an end point created could log in prior to the account being approved. |
| 16461 | 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. |
| 16530 | Onboard device provisioning pages were sometimes imported as Web login pages. |
| 16666 | Unexpected entries in the [Guest Roles] role mapping policy sometimes caused paging issues on the List Accounts page. |
| 16747 | 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. |
| 16982 | Multiple, identical copies of the same entry could be shown in the **Active Sessions** list. |
| 17016 | User search and autocomplete in the L**DAP Sponsor Lookup** field would fail with a JavaScript error for certain skins. |
| 17154 | 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. |
| 17420 | Corrected a potential security issue regarding the redirect functionality of the “target” field in ClearPass Guest login page authentication. Redirect behavior is now restricted to internal addresses. |
| 17623 | Added support for print receipts for mobile and tablet devices. Previously printing was disabled on these kinds of devices, but with modern devices including iOS, Android and Surface, printing is well supported. |
| 17884 | Updated the plain text format used when exporting the application log. The text file generated now includes any arguments that were logged, in addition to the existing fields. |
| 18268 | The operator profile AirGroup Operator is replaced by Device Registration. There is no longer an AirGroup Administrator operator profile as this functionality exists in the default administrator profile. If desired, a separate operator profile can be created with limited access to the default device registration forms (mac_create, mac_edit, mac_list) to simulate the previous AirGroup Administrator profile. |
| 18277 | **Create Multiple Guest Accounts** will now attempt to find a username that isn’t in use when it generates an existing username. |
| 18546 | Japanese characters were not being encoded correctly when used as the subject line for an email message. |
| 18788 | Xirrus could not be properly configured as a vendor for a self-registration. |
| 18903 | Corrected an issue with the **Account Expiration Time** field’s calendar button when the browser’s language settings were set to Japanese or Korean. |
| 18498 | The auto_send_sms and auto_send_smtp fields will never be stored with the created guest account. This prevents an account receipt from being sent when the account expires. |

**Table 18** *Guest Issues Fixed in 6.3.0 (Continued)*

| Bug ID | Description |
|---|---|
| 19033 | Connecting to an LDAP server from Guest failed with an error such as 'certificate verify failed (unable to get local issuer certificate)'. SSL connections to LDAP servers from Guest will now use the CPPM Trust List to verify the identity of the LDAP server. Note 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. |
| 19085 | A performance issue caused user list search to be slow if multiple different fields were enabled for searching. |
| 19089 | Guests could not log in to a Motorola WiNG4 controller. |
| 20727 | MAC devices could not be created or edited using the XML-RPC API. |
| 20732 | Auto-sending did not work for self-registration emails and SMS. |

## Insight

**Table 19** *Insight Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 11696 | Insight's generated report did not display missing hotfixes as expected. |
| 12315 | **Edit Report** did not retain the previously configured **Report Analytics** section. |
| 12414 | Insight HTML reports did not show images when configured in the report. |
| 14420 | Corrected an issue where Insight was disabled by default. |
| | The previous configuration for the Report Analytics selection was not retained when a report was edited. |

## Onboard

**Table 20** *Onboard Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 14208 | Onboard supports different types of authentication under **Provisioning Settings > Web Login**. This includes single sign-on, access code logins, and anonymous logins. |
| 15922 | Onboard now supports Aruba Application Authentication. |
| 16612 | The error message is now more descriptive if the profile signing certificate trust chain is incomplete. |
| 16675 | Corrected an issue that prevented migrating Onboard backups that contained multiple copies of the same certificate. |
| 16879 | Corrected an issue that prevented signing previously-created certificate signing requests (CSRs). |
| 17655 | Corrected an error in retrieving certificates generated by ADCS during enrollment. |
| 18612 | Onboard now correctly detects Windows RT devices as unsupported. |
| 18628 | Added support for onboarding devices running Mac OS X 10.9 Mavericks. |
| 18766 | Onboard was not recording multiple MAC addresses in the tls-client certificate. |
| 19021 | Added support for SHA224 digest algorithm in Onboard. |

## OnGuard

**Table 21** *OnGuard Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 7144 | Access Tracker did not show an unhealthy WebAuth request when the health status changed and auto-remediation was on. |
| 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. |
| 15176 | Enabling Real-Time Protection of AVG Free AntiVirus (2013) is now supported by ClearPass OnGuard. |
| 15360 | The ClearPass OnGuard Unified Agent for Mac OS X always reported 7.x Peer To Peer Application as running even after terminating/closing 7.x. |
| 16032 | Corrected an issue related to Symantec Endpoint Encryption 8.2.1 (Full Disk) disk encryption software. |
| 16329 | The **Monitoring > Live Monitoring > OnGuard Activity** page now shows the current health status. Added fields include Last Seen Health Status, Unhealthy Health Classes, Status, and Added By. |
| 18849 | Corrected an issue on Mac OS where the ClearPass OnGuard installer package displayed a warning message about “unidentified developer”. |
| 18924 | The ClearPass OnGuard Unified Agent did not print remediation messages of antivirus if the .dat file’s has to be update interval was configured on Mac Os. |
| 20591 | The Cancel and Send buttons and subject line are now properly localized for Japanese on the Mac OS in the ClearPass OnGuard Unified Agent’s Send Logs. |
| 20743 | The ClearPass OnGuard Unified Agent would crash while decoding a health state information file. This occurred on Windows machines while rebooting a client directly connected to a broadband network. |

## QuickConnect

**Table 22** *QuickConnect Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 16375 | Added an error message to indicate that Windows Home versions are not supported by QuickConnect. |
| 18670 | Android versions 4.3 or newer now support the installation of multiple trusted certificates. |

## WorkSpace

**Table 23** *WorkSpace Issues Fixed in 6.3.0*

| Bug ID | Description |
|---|---|
| 17137 | References to www.amigopod.com have been changed to clearpass.arubanetworks.com. Any firewall policies that currently reference www.amigopod.com should be updated. Note that these hostnames resolve to the same IP address and continue to be treated identically. |

# 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 6.3.1 release, see the What's New in This Release chapter.

## Policy Manager

**Table 24** *Known Issues in Policy Manager*

| Bug ID | Description |
|---|---|
| 10881 | Entity updates with PostAuth enforcement fail if publisher is down. |
| 11744 | **Symptom:** Upgrading from 5.2 to 6.x fails if CPPM is joined to the domain.<br>**Scenario:** The issue will not be seen if the latest cumulative patch is installed before performing the upgrade. |
| 11906 | The Aruba dictionary becomes disabled by default after upgrading from Policy Manager 4.x to 6.0.1.<br>**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 | **Symptom/Scenario:** In the 6.1 release, the default unit for the CRL update interval was changed to "hours" from an earlier default unit of "days". Restoring a 5.x backup on CPPM 6.x causes the update interval to be "hours". For example, "2 days" in 5.2.0 becomes "2 hours" in 6.1.0.<br>**Workaround:** Manually change the value in days to the value in hours. In the above example, that would be 48 hours. |
| 13999<br>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 | **Symptom:** Post auth doesn't work properly for UNKNOWN endpoints in a MAC Authentication Bypass (MAB) flow.<br>**Scenario:** This has been observed if the user tries to connect using an endpoint that is unknown to CPPM. |
| 14190 | **Symptom:** Blacklisted MAC Authentication Bypass (MAB) users cannot be blocked using the Blacklist User Repository.<br>**Workaround:** In order for post auth to work in a MAB flow, a new blacklist repository must be added with a custom filter. |
| 17232 | **Symptom/Scenario:** The error and warning messages returned by the Web service are displayed in English instead of the localized language. |
| 17876 | **Symptom/Scenario:** CPPM does not include a service template for Single Sign-On (SSO) using network login information.<br>**Workaround:** In the Auto Sign On feature, the administrator needs to add the Aruba SSO Token in the RADIUS enforcement profile.<br>Example: Aruba-Network-SSO-Token = %{Authentication:Network-SSO-Token} |

**Table 24** *Known Issues in Policy Manager (Continued)*

| Bug ID | Description |
|---|---|
| 18064 | **Symptom:** AirWatch custom HTTP actions needs content even though it's not required.<br>**Scenario:** For AirWatch MDM, custom-defined HTTP actions such as Lock Device or Clear Passcode fail with error messages. This is due to a bug in AirWatch.<br>**Workaround:** Do either of the following:<br>• Add a header **Content-Length:0** in the **Context Server Action**.<br>• Add a dummy JSON data {"a":"b"}. |
| 18701 | **Symptom/Scenario:** Performing an AddNote operation using AirWatch as the MDM connector fails in CPPM. This is due to a bug in AirWatch. |
| 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.<br>**Workaround:** Refresh ClearPass or log out and log in again. |
| 19087 | **Symptom:** The Server Configuration page processes indefinitely while changing the NTP server.<br>**Scenario:** Occasionally when modifying the NTP settings in CPPM at **Administration > Server Manager > Server Configuration**, it might not show the progress updates.<br>**Workaround:** Manually refresh the page. |
| 19125 | **Symptom/Scenario:** The CPPM user interface does not include a link to download IDP metadata, although the ability to configure the data is provided.<br>**Workaround:** Use the following link to download the CPPM IDP metadata, then replace "{cppm-host-name}" and "{amigopod-saml-page-name}" with appropriate values:<br>http://{cppm-host-name}/networkservices/saml2/idp/cppm-metadata.xml?page={amigopod-saml-page-name} |
| 19176 | CPPM does not currently support posting of Palo Alto Networks (PANW) user ID information when the PAN OS uses Vsys. |
| 19826 | Palo Alto Networks (PANW) devices will only accept the backslash character ( \ ) as a separator between the domain name and the username. |
| 20139 | Currently, if the remote SSH (Remote Assist feature) browser window is kept open without any activity for more than half an hour, the window becomes unresponsive and there is no indication that it has timed out. This is the page seen by Support Engineers; not the customer's UI. |
| 20293 | **Symptom:** The subscriber join to cluster fails.<br>**Scenario:** In rare cases DB migration results in some bad data being carried over from an earlier version to 6.3.<br>**Workaround:** Share the backup with Customer Advocacy team, who will analyze and provide steps to manually clean up bad data. |
| 20383 | The system posture status may still be maintained after Post Auth agent disconnect action. This is likely to happen when Posture result cache timeout service parameter is higher than the Lazy handler polling frequency. |
| 20416 | **Symptom:** The Palo Alto Networks (PANW) operating system firewall rejects user ID updates from CPPM when the user ID limit is reached on the firewall. When this happens, user ID updates are rejected with errors.<br>**Scenario:** This occurs when the PANW firewall exceeds its supported limit advertised for user ID registration.<br>**Workaround:** There is no workaround at this time. |
| 20453 | If profiling is not turned on, CPPM is not able post the HIP report with complete data to Palo Alto devices. |
| 20455 | When doing an SSO & ASO flow in Safari browsers, the certificate needs to be added in the trust list of the browser. Please follow these steps:<br>1. Open the Safari browser and enter the SP URL.<br>2. After you enter the SSO application in the browser, the Show Certificate option is provided in a popup window.<br>3. Click **Show Certificate** and select the "**Always trust** "**FQDN of SP machine**" **when connecting to IPaddress"** check box, and then click the **Continue** button. |

**Table 24** *Known Issues in Policy Manager (Continued)*

| Bug ID | Description |
|---|---|
| 20456 | **Symptom:** SNMP bounce fails.<br>**Scenario:** When only the SNMP bounce in the SNMP Enforcement profile of a Web auth service is configured, SNMP bounce functionality does not work.<br>**Workaround:** Also configure a VLAN ID along with the SNMP bounce in the SNMP enforcement profile. |
| 20484 | **Symptom:** Dropping the Subscriber and then adding it back to the cluster may fail at times.<br>**Scenario:** CPPM system time might not have been synchronized with an NTP source.<br>**Workaround:** Configure an NTP server. CPPM will synchronize its time with the NTP source. Attempt the cluster operation. |
| 20489 | **Symptom/Scenario:** CPPM 6.3 does not allow a server certificate with a Key Length of 512 bits as seen in the Self-Signed Certificate and Certificate Signing Request UIs. Earlier CPPM versions did not have this restriction, hence their server certificate may use one with a 512 bit Public Key. After upgrade, these servers will not work properly.<br>**Workaround:** The admin must manually fix the server certificate to allow a minimum of 1024 bits long Public Key prior to upgrade. |
| 20522 | An XML response in AirWatch version 6.5.1.2 produces endpoint discovery issues, causing CPPM to discover only one endpoint. The issue is specific to the 6.5.1.2 version of AirWatch. |

## Dissolvable Agent

**Table 25** *Known Issues in the Dissolvable Agent*

| Bug ID | Description |
|---|---|
| 18031 | **Symptom:** The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 installed.<br>**Scenario:** This occurs when Java 7 is installed. Java 7 is released as 64-bit binaries; the Java plugin will not work in Chrome, which currently has a 32-bit version.<br>**Workaround:** The Web agent works fine with Firefox-23.x or later versions. Use the Firefox browser for the Web agent until Chrome resolves 64-bit support for Mac OS X. |
| 18035 | **Symptom:** The OnGuard Web agent applet fails to launch on Mac OS X 10.9.<br>**Scenario:** New security restrictions in Mac OS X 10.9 and Safari 7 prevent the launch of the OnGuard Web agent.<br>**Workaround:** Go to **Safari menu > Preferences > Security > Allow**. **Allow plugins** should already be selected. Click **Manage Website Settings**, look for your portal Web site IP/name, and select **Run in Unsafe Mode**. |
| 18230 | **Symptom/Scenario:** The ClearPass OnGuard dissolvable agent might not work properly if the client machine runs on two different Java versions—for example, Java 6 and Java 7.<br>**Workaround:** Uninstall the old Java component if it exists and keep the latest Java version. |
| 20191 | The OnGuard applet needs to run in Safari's “Unsafe mode” to perform health checks. This can be enabled in **Safari > Preferences > Security > Manage Website Settings > Java > [Select IP/ hostname of ClearPass server] >** select **“Run in Unsafe Mode”** in the drop-down list. |
| 20226 | OnGuard activity does not show the status of clients connecting using dissolvable agents. |
| 20514 | Client health checks might not work if the client is not running the latest Java version. |

## Guest

**Table 26** *Known Issues in Guest*

| Bug ID | Description |
|---|---|
| 9967 | Unicode SMS messages (UTF-16 encoded) 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.<br>**Workaround**: If you plan to use Unicode SMS messages, check your SMS receipt carefully to ensure it is not over 70 characters in length. |

## Insight

**Table 27** *Known Issues in Insight*

| ID | Description |
|---|---|
| 11827 | Insight is not supported in Internet Explorer 8 (IE8). |
| 12096 | Editing a report to select some columns for analytics overwrites/replaces the chosen columns for the corresponding report. |
| 12159 | Insight reports do not show license changes immediately. The changes might take up to 24 hours, depending on when the changes are made. |
| 13980 | Columns with non-ASCII values are missing in PDF reports. |

## Onboard

**Table 28** *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. |
| 7627 | PSK networks cannot be configured for iOS or Android devices in this release. |
| 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. |

**Table 28** *Known Issues in Onboard (Continued)*

| Bug ID | Description |
|---|---|
| 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.<br>The process to provision an OS X system with a system profile is:<br>• The administrator should log in to the OS X system and connect to the provisioning SSID. Do not select "Remember this network."<br>• Use Onboard to provision the device with an EAP-TLS profile, ignoring the username/password prompt.<br>• Connect to the provisioned network, selecting EAP-TLS as the mode and selecting the provisioned certificate, but ignoring the username field.<br>• When the system connects and authorizes to the network, use Network Preferences to place the EAP-TLS network first in the priority list.<br>• After the administrator logs out, users logging in are connected by EAP-TLS and cannot modify those settings. |
| 20983 | **Symptom:** HTC Android asks the user to enter a certificate name to be installed when onboarding.<br>**Scenario:** HTC Androids running Android version less than Android 4.3 and greater than Android 2.3 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.<br>**Workaround:** None. This issue is due to a limitation in the Android phone's firmware. |

# 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 29** *Known Issues in OnGuard*

| ID | Description |
|---|---|
| 6541 | **Symptom:** Sometimes after an abrupt shutdown, OnGuard Agent does not work. After restart, the agent.conf file is blank.<br>**Scenario:** This may happen if there is a power failure or similar situation.<br>**Workaround:**- Re-install OnGuard. |
| 10165 | **Symptom:** ClearPass OnGuard cannot restrict the clients based on Windows service packs.<br>**Scenario:** If any of the Windows System Health Validator check fails, the health status of the client is set to unhealthy but no SoHR is sent to OnGuard. OnGuard cannot display a specific remediation message; however, the red shield icon is displayed to indicate the client is unhealthy.<br>**Workaround:** There is no workaround at this time. |
| 11806 | ClearPass OnGuard 6.1 does not support Sophos 10.0.4 on Windows XP SP3. |
| 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.<br>**Scenario:** This might occur during the installation of the ClearPass OnGuard Unified Agent on WinXP and Windows 2003 SP2.<br>**Workaround:** Users should click **"**Continue Anyway**"** to proceed. |

**Table 29** *Known Issues in OnGuard (Continued)*

| ID | Description |
|---|---|
| 13363 | **Symptom:** On the 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.<br>**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 to remove OnGuard from the system completely:<br>`/usr/local/bin/clearpassonguarduninstaller.sh` |
| 13556 | On a Mac running OS X 10.8, OnGuard fails to read the last scan time for the MacKeeper or Kaspersky antivirus packages. |
| 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 /uTorrent, 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. |
| 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. |
| 15351 | **Symptom:** The state of the Real_Time Scanning button in the Trend Micro Titanium Internet Security for Mac user interface is not updated.<br>**Scenario:** This is observed when the ClearPass Unified OnGuard Agent has Real Time Protection (RTP).<br>**Workaround:** Close the UI using **Command +Q** and restart. |
| 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.<br>**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”. |

**Table 29** *Known Issues in OnGuard (Continued)*

| ID | Description |
|---|---|
| 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".<br>**Scenario:** This applies to MAC OS.<br>**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.<br>**Workaround:** There is no workaround at this time. |
| 18259 | The ClearPass OnGuard Unified Agent does not support pause and stop remediation for Oracle VM Box Guest Virtual Machines on Mac OS X. |
| 18281 | The ClearPass OnGuard configured health quiet period is supported in Health only mode. It doesn't work in Auth+Health mode. |
| 18341 | **Symptom/Scenario:** OnGuard cannot start a process on Mac OS for non-administrative users.<br>**Workaround:** The user must have root privileges to start process-level health checks by OnGuard on Mac OS. |
| 18574 | The ClearPass OnGuard Unified Agent Japanese version characters are not compatible on English Windows XP if the Asian language support pack is not available on the client. |
| 19019 | The network interface will be bounced twice (once immediately, and once after the configured interval) when the log-out/bounce delay parameter is configured. This is expected behavior; the first bounce is required to end the existing session. |
| 19584 | In a rare case of an installation binary being corrupted, the installer's behavior will be unpredictable. In such cases the installer can correct itself and error out.<br>One known exception to this behavior is if the installation file is corrupted towards the end (most unlikely), the installer can install the VPN-only version of the application. If this occurs, download a new binary and upgrade the existing installation. |
| 19685 | **Symptom:** After upgrading OnGuard to 6.3, the backend service fails to start and is unable to collect logs.<br>**Scenario:** This rarely occurs. It has been observed on the Mac 10.6, 10.8, or 10.9 OS after upgrading OnGuard from 6.2.4 or 6.3 to 6.3.<br>**Workaround:** If the backend service fails to communicate with the plugin, reboot the system after the OnGuard upgrade is complete. |
| 19790 | The ClearPass OnGuard Unified Agent VPN functionality is not supported on Japanese Mac OS. |
| 20279 | The OnGuard Agent Quit/Force options sometimes do not work on the Mac OS if the machine is restarted while health checks are in progress. |
| 20316 | OnGuard's Health Check Quiet Period is applicable per network interface. If a machine has more than one network interface, then each interface will have its own Health Check Quiet Period duration. |

# QuickConnect

**Table 30** *Known Issues in QuickConnect*

| Bug ID | Description |
|---|---|
| 20867 | **Symptom/Scenario:** Android 4.3 and above fails to install a self signed certificate for the CA certificate.<br>**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's 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. |

# WorkSpace

**Table 31** *Known Issues in WorkSpace*

| Bug ID | Description |
|---|---|
| 11152 | **Symptom/Scenario:** The WorkSpace app uses the native iOS email app for sending debug logs.<br>**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.<br>**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.<br>**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.<br>**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 or 6.3. |
| 12726 | **Symptom/Scenario:** A user search for a location on a map might appear to give the wrong coordinates. In fact, for geo-fencing coordinates, when multiple results are returned for a search string, the first result returned is used. |
| 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.<br>**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.<br>**Scenario:** This situation can occur with policy-enabled apps. It does not occur with personal apps.<br>**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.<br>**Scenario:** If sharing is not disabled, files can be sent to any outside users from the registered email account.<br>**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.<br>**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.<br>**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.<br>**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.<br>**Workaround:** The user should manually check for updates to third-party applications. |
| 16123 | **Symptom:** Devices and users cannot be deleted from WorkSpace.<br>**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.<br>**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.<br>**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**.<br>**Workaround:** Delete and reinstall WorkSpace to update the user device ID. |

**Table 31** *Known Issues in WorkSpace (Continued)*

| Bug ID | Description |
|---|---|
| 17160 | ADCS is currently not supported for MDM and WorkSpace. |
| 20537 | **Symptom/Scenario:** After migration from 6.2 to 6.3, the Aruba browser might not work correctly.<br>**Workaround:** Update the WorkSpace App Catalogue and push the Default iOS App Policy Template. |