ClearPass 6.4.2

aruba
NETWORKS

Release Notes

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1
About ClearPass 6.4.2

ClearPass 6.4.2 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 and Update Information" on page 11—Provides considerations and instructions for version upgrades and patch updates.
- Chapter 3, "What's New in This Release" on page 17—Describes new features and issues introduced in this 6.4.2 release as well as issues fixed in this 6.4.2 release.
- Chapter 4, "Enhancements in Previous 6.4.x Releases" on page 21—Describes new features introduced in earlier 6.4 releases.
- Chapter 5, "Issues Fixed in Previous 6.4.x Releases" on page 29—Lists issues fixed in earlier 6.4 releases.
- Chapter 6, "Known Issues Identified in Previous Releases" on page 45—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 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 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.

End of Support

Please note that Microsoft officially stopped supporting the Windows XP operating system as of April, 2014. Aruba Networks will not remove existing ClearPass features or software agents that are compatible with Windows XP, such as OnGuard. We will not, however, be providing any further bug fixes or feature enhancements related to supporting the Windows XP operating system. Our TAC organization will not be able to service customer support requests related to Windows XP-based clients. Customers should consider Windows XP an unsupported operating system on ClearPass. (#21679)

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

If you do not have the VA resources to support a full workload, then you should consider ordering the ClearPass Policy Manager hardware appliance.

Important: Please review the functional IOP rating specified below for your VA version and verify that your system meets this requirement.

VMWare Player is not supported.

CP-VA-500

- 2 Virtual CPUs
- 500 GB disk space
- 4 GB RAM
- 2 Gigabit virtual switched ports
- 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
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

CP-VA-25K

- 24 Virtual CPUs
- 1024 GB disk space
- 64 GB RAM

- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 350

Evaluation Version

- 2 Virtual CPUs
- 80 GB disk space
- 4 GB RAM
- 2 Gigabit virtual switched ports

An evaluation version can be upgraded to a later evaluation version in a manner similar to a production upgrade.

ClearPass OnGuard Unified Agent Requirements

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

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

Windows 7, Windows 8.x Pro, Windows Vista, and Windows Server 2008 are all supported with no Service Pack requirements. OnGuard does not support Windows 8.x RT or Windows 8.x Phone.

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 Versions, OnGuard

For OnGuard to work properly, please whitelist the following executable files and installation folders in your antivirus products:
ClearPassOnGuard.exe
ClearPassAgentController.exe
C:\Program Files (x86)\Aruba Networks\ClearPassOnGuard
C:\Program Files\Aruba Networks\ClearPassOnGuard

In the lab, we use the following antivirus software for our validations. Due to the large number of products available, this list may change at any time:

- Kaspersky: IS-11 and above
- Sophos: 9 and above
- Avast
- COMODO
- McAfee
- Microsoft Security Essentials
- Microsoft Forefront Endpoint Protection-2008
- AVG

- Trend Micro
- Windows Defender Firewall
- Microsoft Windows Firewall


NOTE

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

This section provides version information for both the Java-based Dissolvable Agent and the Native Dissolvable Agent.

For more information on the Dissolvable Agent, refer to the ClearPass Policy Manager online help.

ClearPass OnGuard Java-Based Agent Version Information

In current laboratory tests for ClearPass 6.4.2, the browser and Java versions shown in Table 1 were verified for the ClearPass OnGuard Java-based Dissolvable Agents. There are considerations to be aware of with some browser versions. For more information, click the ID number next to the browser's name.

The latest Java version is required in order to perform client health checks.

Table 1 *Java-Based Agent Latest Supported Browser and Java Versions for This Release*

Operating System	Browser	Java Version
Windows 7 64-bit	Chrome 38.x (#7165)	JRE 1.8 Update 25 32-bit
	Firefox 33.x (#7165)	JRE 1.8 Update 25 32-bit
	IE 8.x	JRE 1.8 Update 25
Windows 7 32-bit	Chrome 38.x	JRE 1.8 Update 25
	Firefox 33.x	JRE 1.8 Update 25
	IE 11.x	JRE 1.8 Update 25
Windows 8 64-bit	Chrome 38.x (#7165)	JRE 1.8 Update 25 32-bit
	Firefox 33.x (#7165)	JRE 1.8 Update 25 32-bit
	IE 10.x 32-bit (#7165)	JRE 1.8 Update 25
Windows 8 32-bit	Chrome 38.x	JRE 1.8 Update 25
	Firefox 33.x	JRE 1.8 Update 25
	IE 10.x	JRE 1.8 Update 25
Windows 8.1 64-bit	Chrome 38.x (#7165)	JRE 1.8 Update 25 32-bit
	Firefox 33.x	JRE 1.8 Update 25 32-bit
	IE 11.x 32-bit	JRE 1.8 Update 25

Table 1 *Java-Based Agent Latest Supported Browser and Java Versions for This Release (Continued)*

Operating System	Browser	Java Version
Windows 2008 64-bit	Chrome 38.x (#7165)	JRE 1.8 Update 25 32-bit
	Firefox 33.x (#7165)	JRE 1.8 Update 25 32-bit
	IE 9.x 32 bit (#7165)	JRE 1.8 Update 25
Windows 2003 32-bit	NOT SUPPORTED	
Windows XP 32-bit	NOT SUPPORTED	
MAC 10.9	Safari 7.x (#20191)	JRE 1.8 Update 25
	Firefox 33.x	JRE 1.8 Update 25
MAC 10.8	Safari 6.x	JRE 1.8 Update 25
	Firefox 33.x (#20191)	JRE 1.8 Update 25
MAC 10.7.5	Safari 6.x (#20191)	JRE 1.8 Update 25
	Firefox 31.x	JRE 1.8 Update 25

ClearPass OnGuard Native Agent Version Information

In current laboratory tests for ClearPass 6.4.2, the browser versions shown in Table 2 were verified for the ClearPass OnGuard Native Dissolvable Agents. There are considerations to be aware of with some browser versions. For more information, click the ID number next to the browser's name.

Table 2 *Native Agent Latest Supported Browser Versions for This Release*

Operating System	Browser
Windows 7 64-bit	Chrome 38.x (#24518, #24986)
	Firefox 33.x
	IE 8.x (#25827)
	IE 8.x 64-bit
Windows 7 32-bit	Chrome 38.x (#24518, #24986)
	Firefox 33.x
	IE 11.x
Windows 8 64-bit	Chrome 38.x (#24986)
	Firefox 33.x
	IE 10.x 32-bit

Table 2 *Native Agent Latest Supported Browser Versions for This Release (Continued)*

Operating System	Browser
Windows 8 32-bit	Chrome 38.x (#24986)
	Firefox 33.x
	IE 10.x
Windows 8.1 64-bit	Chrome 38.x (#24986)
	Firefox 33.x
	IE 11.x 32-bit
Windows 2008 64-bit	Chrome 38.x (#24986)
	Firefox 33.x
	IE 9.x 32 bit (#24766)
Windows 2003 32-bit	NOT SUPPORTED
Windows XP SP3	NOT SUPPORTED
Windows Vista	Chrome 38.x (#24986)
	Firefox 33.x
	IE 7.x 32-bit
MAC 10.9	Safari 7.x
	Firefox 33.x
	Chrome 38.x (#24518, #24986)
MAC 10.8	Safari 6.x
	Firefox 33.x
	Chrome 38.x (#24986)
MAC 10.7.5	Safari 6.x
	Firefox 33.x
	Chrome 38.x (#24986)

ClearPass Onboard Requirements

Onboard does not support Windows 8.x RT or Windows 8.x Phone.

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 3 *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) 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/
Security Incident Response Team (SIRT)	http://www.arubanetworks.com/support-services/security-bulletins/
Support Email Addresses	
Americas, APAC, and EMEA	support@arubanetworks.com
Security Incident Response Team (SIRT)	sirt@arubanetworks.com

Chapter 2
Upgrade and Update Information

This chapter provides considerations and instructions for upgrading or updating your ClearPass application:

- The term “upgrade” refers to moving from one major release version to another—for example, from 6.3.x to 6.4.x. For information on upgrading from a version prior to 6.4, see “Upgrading to ClearPass 6.4 from 6.1, 6.2, or 6.3” on page 11.
- The term “update” refers to applying a patch release within the same major version—for example, from 6.4.1 to 6.4.2. For information on updating to a patch release, see “Updating Within the Same Major Version” on page 14.

Upgrading to ClearPass 6.4 from 6.1, 6.2, or 6.3

An upgrade is the process of moving from one major release version to another—for example, from 6.3.x to 6.4. This section describes accessing upgrade images, considerations to be aware of, and instructions for restoring the log database after the upgrade (optional).

You can upgrade to ClearPass 6.4 from ClearPass 6.1.x, 6.2.x, or 6.3.x. Before you proceed with the upgrade, we recommend that you apply the latest available patch updates to your current release. For information on the patch update procedure, see “Updating Within the Same Major Version” on page 14.

- 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, upgrade to the latest 6.1, 6.2, or 6.3 before upgrading to 6.4. The 6.1, 6.2, and 6.3 upgrade images are available for download on the Support site under **ClearPass > Policy Manager > Archives**.
- Direct upgrades from versions prior to ClearPass 6.1.x are not supported. Customers with versions earlier than 6.1.0 must upgrade to the latest 6.1.x, 6.2.x, 6.2.x VM, or 6.3.x version first before upgrading to 6.4.

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) depending on the size of your configuration database. A large number of audit records (hundreds of thousands) due to MDM integration can significantly increase upgrade times. Refer to the sample times shown in Table 4 in “Sample Times Required for Upgrade” on page 12.
- Review the VMware disk requirements. These are described in “System Requirements” on page 3 of the About ClearPass 6.4.2 chapter.

- 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.

NOTE

Log Database and Access Tracker records are not restored as part of the upgrade. If required, you can manually restore them after the upgrade. For more information, please review "After You Upgrade" on page 13.

- Before initiating the Upgrade process in CPPM, we recommend you set the **Auto Backup Configuration Options** to **Off** (if it was set to other values such as **Config** or **Config|Session**). This reason for disabling this setting is to avoid interference between the Auto Backup process and the Migration process.

  To change this setting:

  Navigate to **Administration** > **Cluster Wide Parameters** > **General** > **Auto Backup Configuration Options** = **Off**.
- If you have a custom authentication source configured to use the session log database, additional steps are required after upgrade. You have such an authentication source configured if you have a source of type **Generic SQL DB** in **ClearPass Policy Manager > Configuration > Sources** with server name **localhost** or **127.0.0.1** and with the database name **tipsLogDb**. In such cases, manually restoring the session log database is required after the upgrade completes (see "After You Upgrade" on page 13). Please contact Customer Support for configuration recommendations to move away from using the session log database as an authentication source.
- **VM only**: 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.

CAUTION

Never remove SCSI 0:0

Sample Times Required for Upgrade

To help you estimate how much time the upgrade might take, Table 1 shows representative numbers for upgrade times under test conditions. Remember that the figures here are only examples. The actual time required for your upgrade depends on several factors:

- Your hardware or virtual appliance model. In the case of VM installations, upgrade times vary significantly based on the IOPS performance of your VM infrastructure.
- The size of the configuration database to be migrated.
- For Insight nodes, the size of the Insight database.
- For subscriber nodes, the bandwidth and latency of the network link between the subscriber and the publisher.

Table 4 *Sample Times Required for Upgrade*

Hardware Model	Config DB Size	Insight DB Size	Publisher Upgrade Time	Subscriber Upgrade Time	Insight Restoration Time in Publisher OR Subscriber
CP-500	100 MB	5 GB	50 minutes	50 minutes	20 minutes
	200 MB	5 GB	60 minutes	60 minutes	20 minutes

Table 4 *Sample Times Required for Upgrade*

Hardware Model	Config DB Size	Insight DB Size	Publisher Upgrade Time	Subscriber Upgrade Time	Insight Restoration Time in Publisher OR Subscriber
CP-5K	100 MB	5 GB	50 minutes	50 minutes	15 minutes
	200 MB	5 GB	60 minutes	60 minutes	15 minutes
CP-25K	200 MB	5 GB	30 minutes	30 minutes	15 minutes
	500 MB	10 GB	40 minutes	40 minutes	20 minutes

After You Upgrade

To reduce downtime, the default upgrade behavior will now back up Log Database and Access Tracker records but will not restore them as part of the upgrade. If required, you can manually restore them after the upgrade through either the application or the CLI. The session log database contains:

- Access Tracker and Accounting records
- Event Viewer
- ClearPass Guest Application Log

The Insight database is not part of the session log database, and will be migrated as part of the upgrade.

Restoring the Log DB Through the User Interface

To restore the Log DB after upgrade through the UI, restore from the auto-generated **upgrade-backup.tar.gz** file (available at **Administration > Server Manager > Local Shared Folders**).

The restoration process could take several hours, depending on the size of your session log database. All services are accessible and will handle requests during the restoration, but there will be a performance impact while the restoration is in progress. We recommend that you perform this operation during a planned change window.

The restoration process will continue in the background even if the UI is closed or the session times out. A “Restore complete” event is logged in the Event Viewer when the restoration is complete.

This process needs to be repeated on each server in the cluster that should retain the session log database.

1. Go to A**dministration > Server Manager > Server Configuration** and click **Restore** for the server.
2. In the **Restore Policy Manager Database** window, select the **File is on server** option, and select the **upgrade-backup.tar.gz** file.
3. Also select the following options:
   - **Restore CPPM session log data (if it exists on the backup)**
   - **Ignore version mismatch and attempt data migration**
   - **Do not back up the existing databases before this operation**
4. De-select the **Restore CPPM configuration data** option.
5. Click **Start**.

Restoring the Log DB Through the CLI

To restore the Log Database after the upgrade process is complete, use the `restore` command. Go to **Administration > Server Manager > Local Shared Folders** and download the **upgrade-backup.tar.gz** file. Host the file at an `scp` or `http` location accessible from the ClearPass server and execute the command `restore <location/upgrade-backup.tar.gz> -l -i -b`.

The restoration process could take several hours depending on the size of your session log database. All services are accessible and handling requests during the restoration, but there will be a performance impact while the restoration is in progress. We recommend that you perform this operation during a planned change window.

The restoration process will abort if the CLI session is closed or times out. We recommend that you initiate the restoration from the User Interface, especially if you have a large number of Access Tracker and Accounting records.

This process needs to be repeated on each server in the cluster that should retain the session log database.

The `restore` command syntax is as follows:

```
Usage:
   restore user@hostname:/<backup-filename> [-l] [-i] [-b] [-c] [-r] [-n|-N] [-s]
   restore http://hostname/<backup-filename>[-l] [-i] [-b] [-c] [-e] [-n|-N] [-s]
   restore <backup-filename> [-l] [-i] [-b] [-c] [-r] [-n|-N] [-s]

   -b -- do not backup current config before restore
   -c -- restore CPPM configuration data
   -l -- restore CPPM session log data as well if it exists in the backup
   -r -- restore Insight data as well if it exists in the backup
   -i -- ignore version mismatch and attempt data migration
   -n -- retain local node config like certificates etc. after restore (default)
   -N -- do not retain local node config after restore
   -s -- restore cluster server/node entries from backup.
         The node entries will be in disabled state on restore
```

Updating Within the Same Major Version

An update is the process of applying a minor patch release within the same major version—for example, from 6.4.1 to 6.4.2. Updates are available from the Software Updates page in ClearPass Policy Manager. This section describes how to install a patch update either through the user interface or as an offline update.

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

During a patch update, the log database is migrated. No extra steps are needed to retain the session log history during a patch update.

If you are installing the 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.

If you are on 6.4.0 or 6.4.1 and want to install a cumulative update patch through the CLI, you must first download and install the 6.4.0 CLI updates patch. At support.arubaneworks.com, go to **Download Software > ClearPass > Policy Manager > Current Release** and select **CPPM-x86_64-20140919-cli-der-support-patch**.

Installation Instructions Through the User Interface

If access is allowed to the Web service, ClearPass servers will show the latest patch update on the Software Updates portal:

1. In ClearPass Policy Manager, go to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware and Patch Updates** area, find the latest patch update and click the **Download** button in its row.
3. After the patch is downloaded, click **Install**.
4. When the installation is complete, if the status on the **Software Updates** page is shown as Needs Restart, click the **Needs Restart** button to restart ClearPass. The status for the patch is then shown as Installed.

Installation Instructions for an Offline Update

If you do not have access to the Web service and you need to do an offline update, you may download the signed patch from the Support site, upload it to the CPPM server, and then install it through the user interface:

1. Download the appropriate patch update from the support site (http://support.arubanetworks.com)
2. Open ClearPass Policy Manager and go to **Administration > Agents and Software Updates > Software Updates**.
3. At the bottom of the **Firmware and Patch Updates** area, click **Import Updates** and browse to the downloaded patch file.
4. Click **Install**. When the installation is complete, if the status on the **Software Updates** page is shown as Needs Restart, click the **Needs Restart** button to restart ClearPass. The status for the patch is then shown as Installed.

Chapter 3
What's New in This Release

This chapter provides a summary of the new features and changes in the ClearPass 6.4.2 release.

This chapter contains the following sections:

Release Overview

ClearPass 6.4.2 is a monthly patch release that introduces new features and provides fixes for known issues. The 6.4.2 cumulative patch update is available in Policy Manager under **Administration > Agents and Software Updates > Software Updates**.

New Features and Enhancements in the 6.4.2 Release

The following new features were introduced in the 6.4.2 release.

The IP address to access the licensing server clearpass.arubanetworks.com changed from 199.127.104.89 to 104.36.248.89 on September 27th, 2014. If you have any firewall protections allowing access, please be sure to update the IP address information accordingly.

Guest

- The performance of captive portal pages was improved. (#26039)
- Support was added for the Media4u SMS gateway (Japan). (#26036)

OnGuard

- Support was added for the following products: (#26015)
  - avast! Free Antivirus 2015.x (Windows)
  - avast! Premier 10.x (Windows)
  - AVG AntiVirus 2015.x (Windows)
  - AVG AntiVirus Free Edition 2015.x (Windows)
  - AVG Internet Security 2015.x (Windows)
  - Bitdefender Internet Security 18.x (Windows)
  - Kaspersky Internet Security 15.x (Windows)

  Support was enhanced for the following products:
  - Avira Mac Security 2.x (Mac)
  - Kaspersky Anti-Virus 13.x (Windows)
  - Kaspersky Anti-Virus 14.x (Windows)

- Kaspersky Internet Security 14.x (Windows)
- McAfee VirusScan Enterprise 8.x (Windows)

Issues Resolved in the 6.4.2 Release

The 6.4.2 release resolved specific vulnerability issues in ClearPass. For details, refer to issues #26059, #26067, and #26075.

The following issues have been fixed in the ClearPass 6.4.2 release.

Policy Manager

Table 5 *Policy Manager Issues Fixed in 6.4.2*

Bug ID	Description
#25731	Corrected an issue where, on the **Monitoring > Live Monitoring > System Monitor page > System Monitor tab**, the Y-axis of the **CPU Usage** graph was labeled "Percentage". The Y-axis is now correctly labeled **Load Average**.
#25735	Corrected an issue where, after ClearPass was upgraded to 6.4.0, some pre-existing guest accounts could not authenticate.
#25937	Corrected an issue where file permissions prevented replication services from starting.
#26021	Corrected an issue where Palo Alto Networks UID updates failed because of WebSocket subscription errors in the PostAuth module.
#26075	The PHP version was upgraded to version 5.4.34. This includes fixes for CVE-2014-3669, CVE-2014-3670, and CVE-2014-3668.
#26081	The periodic database cleanup operation for endpoints was optimized.
#26082	Support was added for the Send Full Username option in Palo Alto Networks UID updates.
#26059	This patch includes fixes for CVE-2014-3566, the POODLE security vulnerability that could allow a man-in-the-middle attacker to decrypt ciphertext using a padding Oracle side-channel attack. POODLE stands for Padding Oracle On Downgraded Legacy Encryption. The POODLE vulnerability affects older encryption standards, specifically SSLv3. It does not affect TLS encryption.
#26067	This patch includes fixes for CVE-2014-8367, an unauthenticated SQL injection vulnerability issue that could allow an attacker to read sensitive information from the ClearPass database. Additional information is available at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8367.
#26188	Corrected an issue where, on 6.4.1, an administrator with Read and Write privileges was not able to list or view endpoints.

Guest

Table 6 *Guest Issues Fixed in 6.4.2*

Bug ID	Description
#26010	Corrected an issue with synchronizing the skin.translation enabled state between the publisher and the subscriber that caused database query errors in the subscriber's Application Log.
#26038	Corrected an issue with importing guest accounts using a CSV file. To import devices, make sure your file contains a `mac` column with the MAC address, and a `mac_auth` column with a value set to `1`.
#26075	The PHP version was upgraded to version 5.4.34. This includes fixes for CVE-2014-3669, CVE-2014-3670, and CVE-2014-3668.

Insight

Table 7 *Insight Issues Fixed in 6.4.2*

Bug ID	Description
#25887	Corrected an issue where an Insight report would fail if an endpoint attribute contained a Unicode character.
#26099 #26166	Corrected an issue where Insight's **Replicate** option failed with the error message "Internal Server Error".

OnGuard

Table 8 *OnGuard Issues Fixed in 6.4.2*

Bug ID	Description
#25727	Corrected an issue where the Dissolvable Agent was not able to detect McAfee 1.9 on CentOS 6.5.
#25905	Corrected an issue where, on Mac OS X, the OnGuard agent did not check for disk encryption with PGP.
#25921	Corrected an issue where auto-upgrade for the ClearPass OnGuard Unified Agent failed because the ClearPassOnGuard.exe file was being used by another application.
#26004	Corrected an issue where, on Mac OS X, the OnGuard Agent would sometimes log out after health checks were completed in Health-Only mode.
#26005	Corrected an issue where, on Mac OS X, the OnGuard Backend Service sometimes would not send a health check when the system started because it failed to load Japanese resources, even if the system did not use Japanese characters.
#26015	The OPSWAT SDK was updated to the latest version at the time of this release.
#26196	Corrected an issue where the disk encryption check failed because of a trailing backslash character (\ ) in the encrypted location.
#26252 #25797	The ClearPass OnGuard Unified Agent now supports Mac OS X 10.10 (Yosemite).

Table 8 *OnGuard Issues Fixed in 6.4.2 (Continued)*

Bug ID	Description
#26264	Corrected an issue where, on Mac OS X 10.10, the OnGuard user interface did not automatically start when when the system was restarted, and had to be manually started from the finder.

New Known Issues in the 6.4.2 Release

The following known issues were identified in the ClearPass 6.4.2 release.

Policy Manager

Table 9 *Policy Manager Known Issues in 6.4.2*

Bug ID	Description
#28318	**Symptom:** When upgrading from 6.3.x to 6.4.0, if non-default or custom Role IDs were configured for guest accounts, they are not migrated after the upgrade and cannot be manually restored from the backup data. **Scenario:** This issue only occurs when upgrading from 6.3.x to 6.4.0. It is not an issue when upgrading from 6.3.6 to 6.5.0. **Workaround:** After upgrading from 6.3.x to 6.4.0, apply the patch update to 6.4.2 or higher. You can then manually restore the backup data. If you need assistance, contact Support at support.arubanetworks.com

OnGuard

Table 10 *OnGuard Known Issues in 6.4.2*

Bug ID	Description
#26224	**Symptom/Scenario:** Some combined products that include both antivirus and antispyware (for example, McAfee VirusScan Enterprise + AntiSpyware Enterprise) are not shown in the AntiSpyware Posture configuration. **Workaround:** Add products like this only in Antivirus. Both the AntiVirus and AntiSpyware values are the same.
#26232	**Symptom:** When installing or running the Native Dissolvable Agent on Mac OS 10.10, the message "'ClearPass OnGuard WebAgent' can't be opened because the identity of the developer cannot be confirmed" is displayed. **Workaround:** When opening the OnGuard WebAgent application for the first time after installing, the user must open it manually. Right-click and select the **Open** option. The Web browser will then be able to launch the OnGuard WebAgent.
#26275	**Symptom/Scenario:** On Mac OS X 10.10, after changing mode on the CPPM server the ClearPass OnGuard Unified Agent does not relaunch, either automatically or when the user clicks the **Retry** option.
#26276	**Symptom/Scenario:** On Mac OS X 10.10, the ClearPass OnGuard Unified Agent 's VIA component fails to download the connection profile when the tunnel is established, and the log window shows the error "Configuration download... failed".

This chapter provides a brief summary of the features and enhancements introduced in previous ClearPass 6.4.x releases.

Features and Enhancements in Previous 6.4.x Releases

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

Policy Manager

- IPv6 support was added at the platform level. The following IPv6 options are supported: (#8199)
  - Management and data port addresses:
    - DNS addresses
    - NTP server addresses
    - Access Control List Configuration
    - Profile module now tracks IPv6 elements in the network
  - Insight stores IPv6 data for endpoints
- The **Administration > Server Manager > Server Configuration > System** tab includes options for specifying the IPv6 addresses for configuring Management port, Data (external) port, and DNS addresses. For more information on the newly introduced CLI commands and updates, see the *ClearPass Policy Manager 6.4.0 User Guide*. (#12398)
- **Syslog Export Filters** now support export of Insight Report attributes. These can be used to export information such as: (#18245)
  - RADIUS Accounting
  - RADIUS Authentications
  - TACACS Authentications
  - WebAuth Authentications
  - Endpoints details
  - Guest details
- SMS and SMTP services are now integrated in the ClearPass platform for notifications. SMS and SMTP services no longer need to be configured individually in the Policy Manager, Guest, and Insight modules. The **Administration > Server Manager > Messaging Setup** page in ClearPass Policy Manager is enhanced to provide the interface for configuring the SMTP server for email and SMS notifications. The **Configuration > SMS Services > Gateways** page in ClearPass Guest is used by ClearPass Policy Manager, Guest, and Insight to send SMS notifications. This provides a single point of configuration that helps to ease the administration tasks and reduce configuration errors. (#25035, #23034, #23036, and #20662)
- Support was added to link context server actions to context servers of type **Generic Http**. This helps to show or filter appropriate actions for Generic Http servers in the **Trigger Server Action** page and **Server Action** in the **Access Tracker** page. (#20663)
- An **Uninstall** button for uninstalling skins or plugins through the ClearPass Policy Manager GUI was added to the popup that shows installation logs. (#20828)

- The **Standby Publisher** was enhanced to reach subscribers in a cluster through HTTPS - TCP port 443 protocol. In many customer deployments, the firewall does not allow the Internet Control Message Protocol (ICMP), and gateways are configured not to respond to ICMP communication. (#21295)
- The ClearPass Policy Manager server lets you define a virtual IP address without necessarily adding a secondary server. (#21527)
- ClearPass now supports encrypted communication to MS SQL databases. (#21540)
- Support was added to send the AD domain in the UID updates to Palo Alto firewall and Panorama devices. To use this option, the user must be authenticated against the AD, and the **Prefix NETBIOS name in UID updates** option must be selected in the Palo Alto firewall and Panorama device configuration in ClearPass Policy Manager. (#21710)
- The **High Capacity Guest** (HCG) mode was added to address the high volume licensing requirements in the Public Facing Enterprises (PFE) environment, where a large volume of unique endpoints need wireless access. A **Mode** tab was added to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters** page, and lets you enable or disable the High Capacity Guest mode. Because the intention of this mode is to handle a high volume of guest users in a PFE environment, only guest licenses can be added to the High Capacity Guest mode. After enabling the High Capacity Guest mode, you cannot add enterprise licenses. In High Capacity Guest mode, a maximum of 2x licenses are allowed. For example, if you use the CP-HW-5K platform that supports 5k licenses, a maximum of 10k licenses are allowed in High Capacity Guest mode. For more information, see the *ClearPass Policy Manager 6.4.0 User Guide*. (#21786)
- The User-Name attribute in the Enforcement Profile is now always included in Radius Access-Accept messages. (#23407)
- The **PAP** authentication method with external authentication sources (LDAP and Generic SQL DB) now supports the following encryption schemes: (#21842)
  - Clear
  - Crypt
  - MD5
  - SHA1
  - SHA256
  - NT Hash
  - LM Hash
  - Aruba-SSO
- The Service Template UI was enhanced to let you view, edit, or delete the pre-configured services through service templates. This can be done by selecting the prefix in each template. Now you can use the UI to select any authentication source from the list of all available authentication sources in ClearPass Policy Manager and add a new active directory. (#23037, #23039, and #23040)
- The EAP-PEAP-Public authentication method was introduced for authenticating and providing secured wireless guest access to the endpoints. To provide secured wireless guest access, Wi-Fi Protected Access (WPA) is provided for a publicly-known username and password. This ensures that every device gets a unique wireless session key that is used to encrypt the traffic and provide secured wireless access, yet without intruding on the privacy of others even when the same username and password is shared by all devices. (#23300)
- Support was added to SAP Afaria MDM integration with ClearPass Policy Manager to enable collection of endpoint profile information from different types of devices. These servers provision mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. (#23310)

- Syslog Export Filters now support Insight Report attributes. This eliminates the need for individual nodes to send duplicate syslog data. (#23504)
- The **Network Address Translation (NAT) Pool Configuration** page was added to the **Aruba Downloadable Role Enforcement** profile in ClearPass Policy Manager. This is used to configure the start and end of the source NAT range and associate them with session ACLs. (#23529)
- A new **Reinstall Patch** link allows the ClearPass Policy Manager Administrator to reinstall a patch in the event that the previous attempt to install fails. You can only install the last installed patch, which is indicated by a "!" symbol next to it in the **Firmware & Patch** Updates table on the **Administration** > **Agents and Software Updates** > **Software Updates** page. (#23645)
- A new Service parameter, **Re-attempt AD login with different Username formats**, lets you control re-tries with different username formats to the Active Directory in MS CHAP v2 authentication. (#23701)
- Active Directory authentication source configuration supports a new option, **Always Use NETBIOS Name**. If this option is enabled, when authenticating users, CPPM will always use the NETBIOS name configured in the authentication source instead of the domain information received in RADIUS request username. (#23796)
- Information for **FIPS** and **High Capacity Guest** mode is now exposed through SNMP MIB. (#23841)
- The language-selection flags on the Guest login page were removed. The language is automatically detected based on the client's browser settings. To display the flags on the login page, go to **Guest > Administration > Operator Logins > Login Configuration** and enter the following in the **Login Footer** field: (#23847)

```
<pre>
{assign var=query_target value=$target|urlencode} {capture
name=auth_login}auth_login.php{if $query_target}?target={$query_target}{/if}{/
capture} {nwa_translations href=$smarty.capture.auth_login} </pre>
```

- PAP authentication performance against Active Directory and LDAP authentication sources was optimized by using a connection pool. (#24132)
- RADIUS authentication performance against a Kerberos authentication source is improved. (#24168)
- Support was added for SQL authentication sources with five-digit port numbers. (#24345)
- Support was added for the Insight Replication feature to use the IP addresses of Insight-enabled nodes for replication instead of using the DNS resolvable Hostname. (#24386)
- A new **OAuth2 API User Access** service template was added to authenticate API clients by username and OAuth2 grant type password. (#24421)

CLI

- To support the **Reinstall Patch** feature in the CLI, the **system update** command has a new **-f** option. This reinstalls the last installed patch in the event that the previous attempt to install fails (`system update -f`). (#23643)
- The `configure mtu <mgmt|data> <mtu-value>` command was added to set the Maximum Transmission Unit (MTU) for the management and data port interfaces. (#23737)

Guest

- Individual LDAP translation rules for the Policy Manager operator profiles are now consolidated into a single rule, matching by name. If you are restoring an old configuration, your existing rules are retained. (#10067)

- A new notification was added to inform users when their guest account is about to expire. The notification is sent 24 hours prior to the account expiration. Configuration options for this feature are available in the **Expiration Warning Options** area of the form at **Configuration > Guest Manager**. (#12623)
- Support for users to log in with their social network credentials was added. Configuration options for this feature and the list of social network providers are available on **Configuration > Pages > Web Logins** form and the **Configuration > Pages > Guest Self-Registrations > Login Message** form. (#12624)
- A new action link, **Show Details**, was added to the **Guest > Manage Accounts** list view. The form displays all the properties of the guest account, including endpoint details. A user must have the Show Details privilege in their operator profile in order to use this feature. (#13573, #23971)
- A new option for SMS delivery of guest registration receipts was added, and is available on the **Configuration > Pages > Guest Self-Registrations** form. (#19506)
- In the XML-RPC API, fields that have a default value will now pick up the default value automatically, and no longer need to have the value specified in the XML-RPC API call. (#20817)
- A new vendor option, **Single Sign-On —Authorize Only**, was added to **Configuration > Pages > Web Logins**. This option lets you configure the server as an IdP, but without displaying a login form. If the AppAuth request to validate the SAML SP request is successful, the user is logged in through the usual SAML IdP flow. If the AppAuth request fails, a SAML Failure response is returned to the service provider. This feature is useful for configuring Aruba Auto Sign-On (ASO) with third-party identity providers such as Ping Federate. (#22815)
- To help you easily identify and translate page content, a new option, **Text IDs**, was added to the **Configuration > Translations > Translation Assistant** form. When this option is selected, the text ID numbers are displayed on all headings and field names in the ClearPass Guest user interface, and an **Override all translations generated for this page** link is displayed at the bottom of each page. (#22252)
- The Advertising Services forms now include a tag feature for specifying labels in promotions and materials. Similar to the tag feature in AirGroup forms, tags in the Labels field let you create new labels and provide autocomplete suggestions for selecting existing labels. (#22725)
- A **Single Sign-On — Authorize Only** vendor option was added to **Configuration > Pages > Web Logins**. This enables the server to be configured as an IdP, but a login form is never displayed. If the AppAuth request to validate the SAML SP request is successful, then the user is logged in as per the normal SAML IdP flow; otherwise a SAML Failure response is returned to the service provider. This is useful when configuring Aruba Auto Sign-On (ASO) with third-party identity providers. (#22815
- Support was added for storing SAML enforcement profile attributes in the user's session variable, `$smarty.session.userauth_user`. (#22923)
- Several areas of the ClearPass Guest user interface are reorganized or renamed to make navigation easier and more logical: (#23111)

  Guest—

  - Edit Accounts is renamed **Manage Multiple Accounts.**
  - List Accounts is renamed **Manage Accounts**.
  - List Devices is renamed **Manage Devices**.

  Onboard—

  - WorkSpace and MDM features were removed and the module is renamed **Onboard**. Other navigation items (for example, push certificates, distribution certificates, asset database, WorkSpace configuration) were removed to reflect this, and Onboard/MDM Configuration within the Onboard module is now renamed **Configuration**.

- **Certificate Authorities** is now a top-level category in the left navigation and the Initial Setup category was removed.
- The configuration units that used to be in the left navigation under Onboard/MDM Configuration are reorganized. All iOS-specific configuration units are now accessed through **Onboard > Configuration > iOS Settings > Add New**. Network settings configuration is accessed separately at **Onboard > Configuration > Network Settings**. A new category, **Onboard > Configuration > Windows Applications** provides access to App Sets management.

Configuration—

- A new top-level **Pages** category was added to the left navigation. This includes **Fields**, **Forms & Views**, **Guest Self-Registrations**, and **Web Logins**.
- A new top-level **Receipts** category was added to the left navigation. This includes **Digital Pass Templates**, **Email Receipts**, **SMS Receipts**, and print **Templates**.
- **SMS Services** was moved into the Configuration module as a top-level category.
- IP Phones was removed.

Administration—

- A new top-level **API Services** category was added to the left navigation. This includes the new **API Clients** feature as well as **SOAP Web Services**. The **XML-RPC API** features are also included in the API Clients feature.
- **SMS Services** was moved from the Administration module to the **Configuration** module.

- (#22935) Sponsorship confirmation would default-enable guests when a role override or expiration extension was configured. The enabled state on creation is now configurable.
- Support was added for specifying the character set used by the Micros Fidelio FIAS transaction processor. This configuration option is available at **Configuration > Hotspot Manager > Transaction Processors** when you create or edit a transaction processor with Micros Fidelio as the gateway. (#23808)
- A new variable, **{$simultaneous_use}**, was added to use within Web login pages. The value of this variable is taken from the **Active Sessions** field on the **Configuration > Guest Manager** form. (#24003)
- Support for the OnGuard native dissolvable agent was added to the Guest portal. The **Configuration > Pages > Web Logins** form includes related options in the **Login Method** and **Authentication** fields. (#24062)
- Two new options were added to the **Configuration > Pages > Web Logins** form as part of the OnGuard dissolvable agent support. The **Authentication: Auto** option can be used when no authentication or prompting is necessary. This option is similar to the Anonymous User option, but the page is automatically submitted. A pre-existing account is required. This option should be selected if you are using OnGuard health checks. The **Login Method: Policy Initiated** option should be selected if a Policy Manager policy that includes a “bounce client” will be run as part of the page's actions. This option should be selected if you are using OnGuard health checks. (#24241)
- A new API services feature was added at **Administration > API Services**. All API-related privileges are included in API Services: new privileges are defined for it, and the XML-RPC API and SOAP API privileges are moved into it. (#24336, #10119)

  API Services includes:

  - **API Clients**— For API management, the list view under this heading shows all API clients you have defined, and includes a link to the Create API Client form.
  - **SOAP Web Services**—All forms that used to be under **Administration > Web Services** are now here.

Customers who have been using the XML-RPC API or the SOAP API should review the operator profiles used for API access to ensure that the appropriate privileges are set up. Any existing operator profiles with the Administrator privilege set to Full Access should be updated to specifically include the appropriate new privilege in order for XML-RPC clients to work. In the Operator Profile Editor, set the **API Services** privilege to **Custom**, grant **Allow API Access**, and then specify the access levels for each API, SOAP, and XML-RPC privilege.

These API changes are backwards-compatible. The SOAP API and XMLRPC API are now considered legacy and will not be extended.

- A new authentication provider, Ping SSO, was added and is available on the **Configuration > Pages > Web Logins** form for social logins configuration. (#23972)

Insight

- The Insight **Posture Report** template now shows just the last health status for an endpoint. (#19665)
- The Insight Report templates are categorized into different groups based on functionality. For example, authentication related templates are grouped under the **Authentication** group. A new **Select Template Group** field is added in the **Add Reports - Configuration** tab. (#20542)
- Support was added for off-line download or upload of Insight reports to a remote location using **Session Control Protocol** (SCP) or **SSH File Transfer Protocol** (SFTP) protocols. You can configure the SFTP/SCP settings in the **Administration** tab in Insight. (#22423)
- Insight's **Posture Report** template is enhanced to support the following health classes: (#20951)
  - HotFixes
  - Running Services
  - Running Processes
  - Registry keys
  - Disk Encryption
  - Installed Applications
  - Network Connections
  - Virtual Machines
  - USB Devices

Native Dissolvable Agent

- ClearPass Guest's Health Check portal now supports native dissolvable agents for Windows and Mac OS. Native dissolvable agents are each native to a specific platform and do not require Java, so having these options available eliminates the need to have Java installed on client machines. OnGuard Dissolvable Agents communicate with the Guest portal to send information about endpoints such as status, health status, and remediation messages. Health checks can be configured with the following client agent options: (#20657)
  - Native agents only
  - Native agents with Java fallback
  - Java Only

  The Dissolvable Agent flow requires the latest Java version if the Web login mode is set to **Java Only**.

  This configuration option is available when the OnGuard Health Check is enabled in ClearPass Guest on the **Configuration > Pages > Web Login** or **Configuration > Pages > Guest Self-Registrations > Login Message** form. For more information, see the *ClearPass Policy Manager 6.4.0 User Guide* and the *ClearPass Guest 6.4.0 User Guide*.

Onboard

- Support was added for Chromebook. New configuration options are included in the **General** tab of the **Onboard > Deployment and Provisioning > Provisioning Settings** form, and a new **Chromebook** tab was added. This feature requires Chrome 37 or later. (#12123)
- Support was added for EST, the Enrollment over Secure Transport protocol (RFC 7030). Configuration options are available in the **SCEP & EST Server** area of the form when you edit a CA in the **Onboard > Certificate Authorities** list. (#20924, #14017)
- id-kp-eapOverLAN extended key usage is now added when creating trusted certificates. (#16460)
- Support was added for using the SHA-2 family of digest algorithms for client certificates issued by the Onboard certificate authority. This configuration option is available in the **Self-Signed Certificate** area of the form at **Onboard > Certificate Authorities > Create a new certificate authority**. (#20696)
- In the **Onboard > Management and Control > View by Device** list view, when you click the **Certificates** link for a device the **Manage Certificates** form now shows the certificates currently issued to the device in addition to the options for revoking or deleting certificates. (#21453)
- A new status, **Enrolled**, was added to the **Onboard > Management and Control > View by Device** list view. Status (All, Enrolled, Allowed, Denied) was also added as a filter for the list. A device is considered to be enrolled if it is using a license. (#21819)
- Support was added for devices running the Ubuntu operating system. An **Ubuntu** tab is now included in the **Onboard > Deployment and Provisioning > Provisioning Settings** form, and Ubuntu options are included in the **Onboard > Configuration > Network Settings** form. (#22007)
- All Onboard configuration settings that apply only to iOS are now consolidated into a single iOS Settings list at **Onboard > Configuration > iOS Settings**. The **Add New** link in the list view includes options for creating and configuring new iOS settings configuration units. (#23876)
- The default EAP type in ClearPass Onboard is now EAP-TLS for all platforms that support this method (iOS, Android, OS X, Windows, and Ubuntu). (#24459)

OnGuard

- Support was added for the following products: (#25295, #25719, #22464)
  - avast! Free Antivirus 9.x (Mac)
  - AVG AntiVirus 14.x (Mac)
  - Bitdefender Antivirus Plus 18.x (Windows)
  - Kaspersky Antivirus 15.x (Windows)
  - Kaspersky Internet Security 15.x (Windows)
  - Malwarebytes Anti-Malware 2.x
  - Malwarebytes Anti-Malware Premium 2.x
  - Trend Micro Endpoint Encryption (FullDiskEncryption) 5.x (Windows)
  - VMware Player 6.x (Windows)
  - ZoneAlarm Internet Security Suite 13.x

  Support was enhanced for the following products:
  - avast! Free Antivirus 8.x
  - Avira Antivirus Pro 14.x
  - Avira Free Antivirus 14.x
  - Avira Free Antivirus 14.x (Windows)

  - Avira Mac Security 2.x
  - Bitdefender Antivirus for Mac 3.x
  - BitTorrent 7.x (Windows)
  - Endpoint Security 9.x (Windows)
  - Kaspersky Antivirus 14.x (Mac)
  - Microsoft Security Essential 4.x (Windows)
  - Symantec Endpoint Protection (Firewall) 12.1.5 (Windows)
  - Symantec Endpoint Protection 12.x (Mac)
  - System Center Endpoint Protection 4.x (Windows)
  - VirtualBox 4.x (Mac)
  - Window Defender 4.x
  - VMware Player 6.x (Windows)
- Support was added for enabling RTP for System Center Endpoint Protection 4.x AntiVirus. (#25293)
- Support was added for enabling RTP for Microsoft Security Essentials 4.x/MIcrosoft Forefront Endpoint Protection 4.x (#25294)
- The ClearPass OnGuard Unified Agent is updated to include the latest code from standalone Aruba VIA. (#25673)
- The ClearPass OnGuard Unified Agent for Mac OS X can now automatically upgrade when a newer version of the OnGuard Unified Agent is available on the ClearPass Policy Manager server. To configure automatic upgrades, go to the **OnGuard Settings** page and select the **Download and Install** option in the **Agent action when an update is available** field. This feature will not work with Mac OS X OnGuard Agent versions prior to ClearPass 6.4.0. (#17900)
- An **Enable to hide Quit option** parameter was added to the **Agent Enforcement** profile to hide the **Quit** option in the ClearPass OnGuard Unified Agent. This is supported on both Windows and Mac OS X. (#19320)
- The ClearPass OnGuard Unified Agent's connectivity tests for Windows now include the test to check connectivity with the ClearPass Agent Controller Service and Port 6658 on the ClearPass Policy Manager server. (#22943)

The following issues were fixed in previous 6.4.x releases. For a list of issues resolved in the 6.4.2 release, see the What's New in This Release chapter.

Fixed in 6.4.1

The 6.4.1 release resolved specific vulnerability issues in Policy Manager. For details, refer to issues #25203, #25428, #25317, #25402, #25424, #25425, #25431, #25434, #25436, #25439, #25442, #25537, #25830, and #25857.

The following issues were fixed in the 6.4.1 release.

Policy Manager

Table 11 *Policy Manager Issues Fixed in 6.4.1*

Bug ID	Description
#23559	Duplicate routes were added to the system if the GRE tunnel was reconfigured.
#25140	In a comma-separated whitelist host header configuration, a space after a comma could cause the HTTPD service to stop.
#25203	This patch includes fixes for CVE-2014-3511, an OpenSSL SSL/TLS server code issue that could allow a man-in-the-middle attack to force a downgrade to TLS 1.0.
#25215	The Event Viewer message now shows the correct authentication count when the system exceeds the licensing limit.
#25317	This patch includes fixes for CVE-2014-5342, a vulnerability issue where a user could execute arbitrary Linux commands through user interface input fields.
#25365	The Software Updates portal was not updated automatically, and the **Check Status Now** link had to be clicked to update it.
#25413	Profiled device counts on the **Monitoring > Live Monitoring > Endpoint Profiler** page showed discrepancies.
#25434	This patch includes fixes for CVE-2014-6620, a Cross-Site Scripting (XSS) issue where an XSS attack could be carried out through unescaped parameters in JSP pages.
#25436	This patch includes fixes for CVE-2014-6626, a vulnerability issue where certain administrative actions could be executed without authentication.
#25439	This patch includes fixes for CVE-2014-6625, a vulnerability issue where a user could execute certain operations even though the privileges for them were not included in the user's operator profile.
#25516	Publisher failover was incorrectly triggered if both the management and data ports were on the nodes and the standby publisher lost connectivity through the management port.

Table 11 *Policy Manager Issues Fixed in 6.4.1 (Continued)*

Bug ID	Description
#25537	This patch includes fixes for CVE-2014-0475 and CVE-2014-5119, a glibc package vulnerability that could allow an attacker to execute arbitrary code. The glibc packages contain the standard C and math libraries and are required for a Linux system to function properly.
#25642	Corrected integration issues in fetching endpoint details from MobileIron. Endpoint attributes are now encoded as UTF- 8 instead of ASCII, and iOS information is updated in the device dictionary.
#25776 #25777	The SMIME format for signed patches was not supported in 6.4.0. The Software Updates portal and the CLI now support both the DER and SMIME formats.
#25785	With a VPN authentication configured against the Active Directory, the VPN connection sometimes failed. CPPM will reconnect one time to the LDAP/AD server if the bind fails with the error code LDAP_SERVER_DOWN during authentication.
#25830 #25857	This patch includes fixes for CVE-2014-6271 and CVE-2014-7169, a Bash code injection vulnerability issue that could allow for arbitrary code execution through environment variables.
#25910	The database replication service on the publisher in a cluster periodically stopped, causing the subscriber status to be out of synch. This was a file permission issue that prevented the DB replication service from starting.

CLI

Table 12 *CLI Issues Fixed in 6.4.1*

Bug ID	Description
#25308	The data port could be configured without the gateway information during bootstrapping.
#25333	The CLI now displays an error message if the requested MTU value cannot be set.

Endpoint Context Servers

Table 13 *Endpoint Context Server Issues Fixed in 6.4.1*

Bug ID	Description
#24699	The device discovery logic for MobileIron MDM integration was updated to the 5.5 VSP release API specification, allowing faster discovery and avoiding timeouts when there is a large number of devices.
#25033	On the **Configuration > Identity > Endpoints > Edit Endpoint** form, Mobility Access Switches imported from Activate were not correctly recognized as **Switches** in the **Device Category** field or as **Aruba** in the **Device OS** field. The dictionary has been updated to correct this.

Guest

Table 14 *Guest Issues Fixed in 6.4.1*

Bug ID	Description
#25402 #25424	This patch includes fixes for CVE-2014-6621 and CVE-2014-6622, vulnerability issues that could allow unauthenticated information disclosure.
#25404	Messages sent using the SMS Global SMS gateway were not encoded according to the gateway's requirements. This could cause certain characters (for example, the plus sign) to not be sent in the body of the SMS message.
#25407	Unwanted JavaScript could appear in an email if certain skins were used.
#25425	This patch includes fixes for CVE-2014-6627, a vulnerability issue that could allow privilege escalation.
#25428	PHP was upgraded to 5.4.32. This includes fixes for CVE-2014-2497, CVE-2014-3538, CVE-2014-3587, CVE-2014-3597, CVE-2014-4670, CVE-2014-4698, and CVE-2014-5120.
#25697	Guest sponsorship approval could be incorrectly configured to allow role override when operator authentication was disabled.
#25699	Corrected an issue that prevented deletion of the contents of folders in content manager.
#25706	Corrected an issue where page action icon links were not displayed in the correct positions if a custom skin was used as a non-default skin.

Insight

Table 15 *Insight Issues Fixed in 6.4.1*

Bug ID	Description
#25395 #13980	Non-ASCII values were missing in reports. Chinese, Japanese, and other Unicode characters are now supported in Insight PDF report generation.
#25431	This patch includes fixes for CVE-2014-6624, a vulnerability issue that could allow privilege escalation.
#25442	This patch includes fixes for CVE-2014-6623, a vulnerabilty issue with Cross-Site Request Forgery (CSRF).
#25455	For the MAC caching flow, the system used MAC Auth Time instead of Captive Portal Login time to enforce the MAC auth policy.

Onboard

Table 16 *Onboard Issues Fixed in 6.4.1*

Bug ID	Description
#25426	Microsoft Internet Explorer 8 failed to download the QuickConnect application when Onboard was using HTTPS. The error displayed by IE8 was similar to “Unable to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.”

Table 16 *Onboard Issues Fixed in 6.4.1 (Continued)*

Bug ID	Description
#25429	Corrected an issue that prevented the generation of EC keys in Onboard.
#25700	ClearPass no longer requires that a network be configured in order to enroll Chromebook devices in Onboard.
#25703	The **Cancel** button on the **Onboard > Configuration > iOS Settings > Add New** form had the same effect as the **Create** button.
#25705	The device family is now shown correctly for Ubuntu and Chromebook devices in the ClearPass endpoint profile.
#25712	Corrected an issue with signing of certificates using the SHA-2 family of signature algorithms.
#25768	The Onboard network configuration "Trusted Server Names" did not set "Connect To These Servers" on the Windows client.

OnGuard

Table 17 *OnGuard Issues Fixed in 6.4.1*

Bug ID	Description
#25200	The Access Tracker showed the "Service" status even after the service was removed from the Posture Policy configuration.
#25355	The ClearPass OnGuard Installer EXE failed Sign Verification on some clients and showed an error message that indicated the publisher was unknown.
#25468	The "Is Latest" and "Last N Updates" checks failed for McAfee VirusScan AntiVirus.
#25519	Disk encryption health class checks did not work with the Java-based Dissolvable Agent on Windows.
#25580	On Mac 10.10, OnGuard crashed during download of the VIA connection profile.
#25717	The ClearPass OnGuard Unified Agent now caches the encryption state of drives across reboots. If reading the encryption state takes more than 30 seconds, it uses the cached value.
#25726	The OnGuard Persistent Agent was not able to detect BitTorrent 7.x.

QuickConnect

Table 18 *QuickConnect Issues Fixed in 6.4.1*

Bug ID	Description
#25427	QuickConnect provisioning failed on non-English Windows systems where virtual interfaces were present.
#25738 #25766	Corrected an issue where the "Connect to these servers" option in the client's wireless profile did not include the trusted server names that had been configured in **Onboard > Configuration > Network Settings > Trust**.

Fixed in 6.4.0

Policy Manager

Table 19 *Policy Manager Issues Fixed in 6.4.0*

Bug ID	Description
#10067	Individual Translation Rules for the Policy Manager profiles have been consolidated into a single rule matching by name. If you are restoring an old configuration, your existing rules will remain.
#18947	During a patch installation through the user interface, CPPM would occasionally hang for a long time when the installation was almost complete, and the **need to restart** message was not displayed. The page now correctly shows the updated progress.
#19125	The CPPM user interface did not include a link to download IDP metadata, although the ability to configure the data was provided.
#20186	MDM context definitions can now be disabled. New options are available to enable or disable polling of Endpoint Context Servers of type PaloAlto_Panorama, PaloAlto_Firewall, HTTP, AirWave, and CPPM_CLOUD_PROXY.
#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. The SNMP settings now show the correct value.
#20293	Corrected an issue where the subscriber join to cluster failed. In rare cases, database migration had resulted in some bad data being carried over from an earlier version to ClearPass Policy Manager 6.4.0.
#20435	**id-kp-eapOverLAN extended key usage** is now added when creating a Certificate Signing Request (CSR) in ClearPass Policy Manager.
#20522	An XML response in AirWatch version 6.5.1.2 had produced endpoint discovery issues, causing CPPM to discover only one endpoint. The issue was specific to the 6.5.1.2 version of AirWatch.
#20838	Profile now exposes additional classification output to derive potential conflicts.
#20995	The **`system update`** and **`upgrade`** commands now support secure file downloads using https.
#21015	SNMP v3 read with non-privileged security levels (NOAUTHNOPRIV and AUTHNOPRIV) was allowed even if the AUTHPRIV security level was selected.
#21874	The authentication count display is now shown correctly in the Event Viewer when the node authentication capacity exceeds the licensing limit.
#22034	The client certificate checks and captive portal configuration elements are now removed from the **OnGuard Agent Settings** page.
#22036	After the Aruba Support SSH session established by a TAC engineer was terminated, the TAC engineer had to manually exit the SSH tunnel session established between the TAC engineer's host and the Remote Assistance Server.
#22468	Corrected an issue that caused CLI login failure through the serial console.
#22607	Endpoint updates removed any additional attributes when MDM updates were enabled.
#22667	The **Config|SessionInfo** option in the **Administration** > **Server Configuration** > **Cluster-Wide Parameters** > **Auto backup configuration options** field now also backs up the Insight database.

Table 19 *Policy Manager Issues Fixed in 6.4.0 (Continued)*

Bug ID	Description
#22684	Adding a node as a subscriber now shows a confirmation message that the node can reach the publisher's database before proceeding with the subscriber setup operation.
#23058	Post Authentication intermittently failed to initiate Change of Authorization (CoA).
#23348	Corrected an issue with cache replication when shell special characters such as **$** or **!** were used.
#23405	Corrected an issue where tag values with single quotes did not persist during a Post Authentications entity update operation.
#23418	When a CoA was sent for a device that was removed from the endpoint repository, the **Access Tracker** page showed errors that were hard to understand. The error message “Device not present in Endpoint Repository” is now shown instead.
#23503	While restoring a backup from an older version to 6.4.0, existing custom report templates in the older version won’t be loaded. Customers who have custom templates in their older version of Policy Manager should contact TAC, who can provide them with updated custom templates after moving to 6.4.0.
#23535	The Policy server crashed intermittently if it was configured to retrieve authorization attributes from an Oracle database.
#23593	The Device Registration Role was not updated in enforcement profiles after upgrading from 6.1 and 6.2 to 6.3.2.
#23662	ClearPass Policy Manager was not able to communicate with the AirWatch MDM server if ClearPass Policy Manager used a proxy server.
#23667 #24721	The virtual IP (VIP) subnet mask did not change for the data interface.
#23735	In **Administration > External Servers > Syslog Export Filters**, when RADIUS.Acct fields were combined with common attributes, duplicate syslog records were generated.
#23742	The promote publisher operation did not clean up the temporary database changes, which caused failures in subsequent promote publisher operations.
#23743	IP addresses that ended with “.255” could not be added.
#23790	Corrected an issue with tag values so that now no SQL errors are seen after upgrading to Policy Manager 6.4.
#23796	The **Active Directory** authentication source configuration supports a new **Always Use NETBIOS Name** option. If this option is enabled, ClearPass Policy Manager will always use the **NETBIOS** name configured in the authentication source instead of the domain information received in RADIUS request username when authenticating users.
#23801	The ClearPass portal redirected to the welcome.action page instead of a specified self-registered portal.
#23831	Descriptions of RTP Status Check values were added to the online help.
#23889	Migration failed due to the same usernames but in different case (uppercase and lowercase) being present in the list of blacklisted users.
#23979	Apache Tomcat is upgraded to the latest version, Tomcat 7.0.54.X.

Table 19 *Policy Manager Issues Fixed in 6.4.0 (Continued)*

Bug ID	Description
#24001	Corrected an issue related to Insight authentication source fallback order. The following behaviors are now used: • When an Insight-enabled node is dropped from a cluster, the corresponding node entry in the Insight repository is removed. • When an Insight-enabled node in a cluster is down or is out of sync for more than 30 minutes, it becomes the last Insight node in the fallback list.
#24010	Corrected an issue where the Performance Monitoring data was not displayed.
#24063	A **Java Exception** message was displayed during patch installation using the **Software Update** page.
#24117	The following Admin Security Vulnerability issues were corrected: CVE-2014-4013, SQL Injection vulnerability in ClearPass Policy Manager; and CVE-2014-4031, Credential Disclosure vulnerability in ClearPass Policy Manager.
#24127	An invalid TACACS accounting response packet that was missing shell cmd fields was sent to edge devices.
#24212	The ClearPass OnGuard Unified Agent was not displaying non-English Agent Enforcement Profile messages correctly.
#24272	Corrected an issue with restarting the Domain Service when it exited due to errors in authenticating users against Active Directory.
#24395	The supplicant sent EAP data as NULL for the ACK Response.
#24291	Corrected kernel vulnerability CVE-2014-2523.
#24414	Corrected an issue that resulted in empty default gateway and missing routes when the systems were upgraded to 6.3.2. After the upgrade is complete, the system must be rebooted.
#24131	A section on best practices when using the ClearPass API was added to the Policy Manager User Guide.
#24477	The **Collect Logs** option in ClearPass Policy Manager now has an option to check or uncheck logs from Performance metrics.
#24688	Corrected an issue where product upgrades turned off console (VGA) logging during the system boot.
#24839	Read-Only Administrators could export other Admin accounts and use their credentials.
#24854	Corrected an issue where modifying an existing VIP configuration could cause unpredictable behavior in VIP ownership.
#24872	The **Open in AirWave** link in the **Access Tracker** page now points to /user_proxy. This connects to the **user_diagnostic** page if the user is connected and to the **client_details** page if the user is disconnected.
#24909	The **Onboard** service template is changed to check the [Guest Users Repository] in the **Onboard Authorization** service created by the template. Earlier, this was checking the [Guest Devices Repository]. Administrators using this service can update the Enforcement Profile for the **Onboard Authorization** service or re-run the Onboard service template to get the new policy rules.
#24922	The **OnboardDeviceName** attribute is now included in the **Certificate** namespace.
#24575	Role Mapping for some accounts was not correct on Publisher.

Table 19 *Policy Manager Issues Fixed in 6.4.0 (Continued)*

Bug ID	Description
#24618	Each node in a cluster now displays graphs relevant to the local node. To view graphs specific to other nodes in the cluster, Performance Monitoring must be enabled on one of the nodes in the cluster.
#24782	An error message was displayed only on the **System Monitor** page instead of ClearPass Policy Manager Dashboard when Performance Monitoring was disabled in a cluster.
#24868	Certificate migration failed during upgrade to 6.3.X if Private Key Type was not in the PKCS8 format and private key password contained special characters.
#24977	New service parameters are available to enable a Host header check, which allows Web access to valid CPPM entities (IP Address, HostNames, Virtual IPs). Custom host names can be added to the default whitelisted names.
#25085	Triggering an upgrade now locks the configuration database until the upgrade is complete and the node is booted into the new version.
#25136	Progress messages during a **Restore** operation now display information about the size and restore time for large database restore operations.
#25147	You can set the value of the cluster-wide parameter **Auto Backup Configuration Options** to **Off**, **Config**, and **Config|SessionInfo**. • If you select the **Config** option, the config DB will be backed up automatically. • If you select the **Config|SessionInfo** option, ClearPass will back up the config DB, Log DB, and the Insight DB.

CLI

Table 20 *CLI Issues Fixed in 6.4.0*

Bug ID	Description
#23763	Checks were added to return an error if the **network nslookup** command is executed with incorrect commands.
#24244	The command **network reset mgmt** was added for resetting CPPM's management port's IPv6 address.

Dissolvable Agent

Table 21 *Dissolvable Agent Issues Fixed in 6.4.0*

Bug ID	Description
#24062	The OnGuard Native Dissolvable Agent is supported in the Guest Portal.
#24518	An "External protocol request" popup appears during the first time there is a run/scan again operation on the Native Dissolvable Agent flow on the Chrome browser.
#24762	MAC OSX will display the following popup message: "You are opening application ClearPass Webagent first time" while launching the Native Dissolvable Agent.
#24768	Native Dissolvable Agent flow is not supported on Windows XP.

Guest

Table 22 *Guest Issues Fixed in 6.4.0*

Bug ID	Description
#13573	A new action link, **Show Details**, is available on the List Guest Accounts page. This requires the **Show Details** privilege within the Operator profile.
#19172	Support was added for Dutch translations.
#19260	Support was added for languages that display right-to-left, such as Arabic and Hebrew.
#19287	Custom fields created with capital letters in their names were exported as blank to the CSV and TSV formats.
#19506	An SMS delivery option is now available for the sponsor confirmation workflow.
#20126	Not all disallowed characters were validated for manually entered passwords. The validator for the custom password field is now set to IsValidPassword.
#20209	Support was added for Arabic translations.
#20245	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 expiration time is now displayed in this case.
#20454	Certain user account filter expressions specified in the operator profile sometimes resulted in a database query error.
#20495	The {nwa_radius_query} function returned incorrect results for a valid MAC address.
#20530	Contents of a Zip file containing a directory did not show up in Content Manager after extraction.
#20571	Support was added for the Twilio SMS Gateway.
#20727	In 6.3.0, devices could not be created or edited over XML-RPC.
#20732	Auto-sending emails and SMS from a self-registration did not work in 6.3.0.
#20817	XML-RPC calls now have all initial values defaulted so the sender does not need to set these values.
#20877	The amigopod.guest.list call returned both guests and devices. It now only returns guests. To retrieve devices, use amigopod.mac.list.
#20947	Support was added for German translations.
#20560	The complete RADIUS server certificate trust chain is now installed in the provisioned profile by default.
#21362	Corrected an issue with database query errors when migrating data from ClearPass Guest 6.2 to 6.3.
#21442	WebAuth requests were improperly being sent upon guest creation if the MAC field was set.
#21668	Ampersand (&) characters in a password were not correctly escaped for server-initiated web login (Web-Auth) requests.
#21731	If you are using ClearPass Guest to export devices, make sure mac_auth is in the list of fields to export.

Table 22 *Guest Issues Fixed in 6.4.0 (Continued)*

Bug ID	Description
#21844	The `amigopod.guest.list` and `amigopod.mac.list` XML-RPC calls now support a "`sort`" parameter.
#22024	PHP is now upgraded to version 5.4.26. This includes fixes for CVE-2013-6712, CVE-2014-1943, and CVE-2014-2270.
#22128	The correct trust list certificate settings were not used in all cases when performing LDAP directory search (for example, for sponsor lookup use cases).
#22252	Added the **Override all translations generated for this page** link which enables the text IDs used for a given page to be identified and translated easily. To see this link, first enable the Translation Assistant.
#22597	Corrected an issue where an unsupported browser warning message would be incorrectly displayed for Microsoft Internet Explorer 11.
#22672	When health checking applet has been started but no progress information is available, the link to the Java applet usage-related Help page is displayed, even if the Java browser plug in is detected.
#22815	Added the "Single Sign-On — Authorize Only" vendor option to Configuration > Pages > Web Logins. This enables the server to be configured as an IdP, but a login form is never displayed. If the AppAuth request to validate the SAML SP request is successful, then the user is logged in as per the normal SAML IdP flow; otherwise a SAML Failure response is returned to the service provider. This is useful when configuring Aruba Auto Sign-On (ASO) with third-party identity providers.
#22923	Added support for SAML enforcement profile attributes to be stored in the user's session variable ($smarty.session.userauth_user).
#22926	Resolved issue in which post-authentication redirect URL was incorrect on subscriber or showed error. New logic makes the fields sent to a NAS 100% opt-in.
#22937	Corrected an issue where certain special characters (such as ampersand, &) could not be sent using Twilio as the SMS gateway.
#22941	When configuring sponsorship confirmation, you can choose to have the From address get sent to the guest. If the sponsor has their out of office set the guest will receive the alert. Note that the ability to set arbitrary From addresses is dependent on your SMTP server.
#23202	Corrected an issue where the characters shown below would not appear in SMS messages that were sent through Bulk SMS or the default ClearPass SMS Service handler: `^_[]\{}|`
#23209	Fixed issue where expired Apple certificate prevented Onboarding iOS devices.
#23236	Corrected an issue where incorrect HTTP proxy server settings could be used, if different HTTP proxy server settings were configured on different nodes in the cluster.
#23239	Resolved a problem in which the expiration date picker would not display correctly when using German translation pack.
#23517	Corrected an issue where logging a database error sometimes failed during an aborted transaction.
#23808	Added support for specifying the character set used by the Micros Fidelio FIAS transaction processor.
#23822	Corrected an issue with SOAP Web Services where WSDL data describing the Web service was cached across system restarts. It was possible for this to lead to problems if the system's hostname was changed.

Table 22 *Guest Issues Fixed in 6.4.0 (Continued)*

Bug ID	Description
#23892	Resolved an issue in which if an operator was using a non-Latin-based language pack, such as Chinese, form fields could be changed without notice, changing the behavior of the application.
#24080	Corrected an issue where the Reset Password page seen by the guest incorrectly showed two Username fields if a Username field was included but disabled on the guest self-registration form.
#24081	Corrected an issue where the Reset Password page seen by the guest incorrectly performed a case-sensitive search for a matching username. Now the username search is not case-sensitive.
#24133	Fixed a scenario where Guest Expire Post Login was not functioning as desired when the guests were created without the expiration time.
#24164	The PHP version was upgraded to 5.4.29. This includes fixes for CVE-2013-7345, CVE-2014-0185, CVE-2014-0237, and CVE-2014-0238.
#24263	Fixed an issue in which if a self-registration had pre-authentication disabled, and server-initiated logins enabled, it was possible for a typed password to become visible in the username field if the credentials failed the server-initiated WebAuth check.
#24270	The default length of the guest's password is now six digits instead of eight.
#24296	Corrected an issue where policies based on MAC caching sometimes failed unexpectedly if a device was authenticated to the network using multiple different usernames.
#24314 #24315	Corrected potential cross-site scripting (XSS) issues affecting the guest_custom_view (Forms & Views), guest_custom_form_field, and guest_custom_field (Fields), and hotspot_processors (Transaction Processors) pages.
#24311	Resolved reported XSS (Cross Site Scripting) issues.
#24438	The PHP version was upgraded to 5.4.30. This includes fixes for CVE-2014-3981, CVE-2014-0207, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-4049, and CVE-2014-3515.
#24677	Corrected an issue where SMTP messages sent by ClearPass Guest did not include the **Date:** header, which is required by RFC 2822.
#24744	Removed all the logic to look for the SMS mail server in CPPM and set CPPM to look for the eMail mail server.
#24848	Corrected an issue where sending SMS messages on a subscriber could result in the error "Call to a member function GetSubscriptionKey() on a non-object."
#24988	Existing OnGuard deployments will continue to be Java only. We recommend you change this to 'Native agents only' within your login or self-registration setup.

Insight

Table 23 *Insight Issues Fixed in 6.4.0*

Bug ID	Description
#20951	Insight **Posture Report** template is enhanced to support the following health classes: • HotFixes • Running Services • Running Processes • Registry keys • Disk Encryption • Installed Applications • Network Connections • Virtual Machines • USB Devices
#23503	When you restore the backup from previous versions to ClearPass Policy Manager 6.4.0, the existing custom report templates in previous versions will not be loaded. If you already have custom templates in previous versions, contact TAC team to get the updated custom templates after upgrading to ClearPass Policy Manager 6.4.0.
#24312	Corrected an issue where an Insight report on the publisher was not replicated on the subscriber if CPPM hostnames were not resolved using DNS.
#24386	Added support for Insight Replication feature to use IP addresses of the Insight enabled nodes for replication instead of DNS resolvable hostname.

Onboard

Table 24 *Onboard Issues Fixed in 6.4.0*

Bug ID	Description
#16460	When creating “Trusted” certificates in Onboard, id-kp-eapOverLAN extended key usage has been added.
#20696	Added the ability to use the SHA-2 family of digest algorithms for client certificates issued by an Onboard certificate authority.
#20924	Added support for the EST protocol (RFC7030) to Onboard.
#20991	Corrected an issue where the Windows version of QuickConnect was not able to correctly provision wireless networks that were marked as “Hidden SSID.”
#21121	In Windows, check if the SSID to connect is available before showing connect button.
#21453	Added the ability to show the current certificate(s) issued to a device in the “View By Device” Onboard management view.
#21545	Fixed issue that prevented some debug level Onboard messages from appearing in the Application logs.
#21650	Corrected an issue where multiple device entries were sometimes created for devices with multiple MAC addresses.
#21819	Added the ability to display and filter by currently enrolled devices in the Onboard device management view.

Table 24 *Onboard Issues Fixed in 6.4.0 (Continued)*

Bug ID	Description
#21981	Fixed issue where the page displayed after Onboard login had no title.
#22007	Added Onboard support for devices running Ubuntu.
#22629	WorkSpace functionality has been removed in this release.
#23228	Corrected a performance issue where the list of certificates sometimes took a long time to load if there was a large number of certificates (tens of thousands).
#23242	List view columns are now remembered between sessions.
#23289	Onboard Help now indicates that Windows 8 and above does not support embedding administrator credentials for onboarding. UI change on the 'Windows' tab of the Onboard Network Settings editor. Additional help text has been added to the *Admin Username* field.
#23468	Corrected an issue where "Onboard:" computed attributes were not present during authorization.
#23557	Corrected an issue where certificates issued by the Onboard SCEP server did not correctly consume Onboard licenses.
#23876	Consolidated Onboard configuration settings that apply only to iOS into a single iOS Settings list.
#23893	Onboard certificates now record the device name for OS X. On the Certificate Signing Request form, a *Device Name* field is now included if **TLS Client Certificate** is selected as the **Certificate Type**.
#24199	MDM functionality has been removed in this release.
#24311	Corrected some issues with Cross Site Scripting (XSS).
#24376	The message that is displayed when a device certificate expires is updated. Because this message is also shown when a device profile is removed, the message text is more clear about the two scenarios.
#24441	Changed the default wording for the "Certificate Expiry" template to clarify the meaning of the message. The wording now says: "Your network access is about to expire."
#24459	Default EAP type in Onboard has been changed to EAP-TLS, for all platforms that support this authentication method.
#24718	Corrected an issue where deleting an Onboard device did not delete all associated certificates.
#24750	Corrected an issue where Microsoft Internet Explorer 8 failed to download the QuickConnect application if Onboard used HTTPS, and displayed the error message "Unable to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later."
#24830	Fixed Onboard licensing computation from devices with multiple Network Interface Cards (NIC).

OnGuard

Table 25 *OnGuard Issues Fixed in 6.4.0*

Bug ID	Description
#21485	Fixed an issue where the unified agent application is crashing on the system that runs Windows 7 OS during the installation of Onguard.

Table 25 *OnGuard Issues Fixed in 6.4.0 (Continued)*

Bug ID	Description
#21596	OnGuard Agent on Mac OS X is now launched in minimized mode as a system tray icon. This is not available as a dock item and on main window. Main window can be opened from system tray menu **Show ClearPass OnGuard**. Closing the main window removes the dock item and does not quit OnGuard Agent. You can quit from OnGuard Agent using the system tray menu **Quit**.
#22464	From ClearPass Policy Manager 6.4.2, support is added or following new products: • ZoneAlarm Internet Security Suite 13.x • Malwarebytes Anti-Malware 2.x • Malwarebytes Anti-Malware Premium 2.x Support is enhanced for following products: • Avira Antivirus Pro 14.x • Avira Free Antivirus 14.x • Bitdefender Antivirus for Mac 3.x • Avira Mac Security 2.x • avast! Free Antivirus 8.x • VirtualBox 4.x (Mac) • Symantec Endpoint Protection 12.x (Mac) • Window Defender 4.x
#23021	Fixed an issue where adding a new service to **Available Services** in the ClearPass Linux Universal System Health Validator cleared the default services.
#23275	Fixed an issue where the ClearPass OnGuard Unified Agent failed to collect health data after starting a full system scan for Microsoft Security Essential 4.x/Microsoft Forefront Endpoint Protection 4.x.
#23635	From ClearPass Policy Manager 6.3, the Posture policy that is selected for a session is displayed as the value of Posture:Applied-Policy in the Access Tracker. Posture policies created in 6.3.0 use the human-readable name for the value of Posture:Applied-Policy. Posture policies created before 6.3.0 stored an automatically generated string for this value. Posture policies created before 6.3.0 must be manually saved once after upgrading to 6.3.X so that the human-readable name is used for Posture:Applied-Policy value.
#23702	Corrected an issue where, on Japanese and English Windows operating systems, upgrading Onguard from VIA-2.1.1.3 to 6.3.x OnGuard Unified Agent launched a pop-up window for selecting the arubanetflt file.
#23771	Corrected an issue where, after configuring global agent settings email support with UTF-8 characters, the OnGuard page at https://<IP_address>/agent/settings did not load correctly.
#23800	Corrected an issue where Windows defender AV-4.x RTP status was unable to start by Onguard auto-remediation.
#23802	Corrected an issue where, on Mac OS X, the OnGuard Unified Agent's send logs functionality was missing the file attachment.
#24137	Corrected an issue where the ClearPass OnGuard Unified Agent for Windows took too long to detect the encryption state of drives encrypted with Symantec Encryption Desktop.
#24607	Fixed an issue where VIA connected automatically when OnGuard was enabled.

QuickConnect

Table 26 *QuickConnect Issues Fixed in 6.4.0*

Bug ID	Description
#21122	If an Android application is opened without context, the browser will now be launched and redirected to the landing page.
#23730	Corrected an issue where QuickConnect failed to download if a code-signing certificate was used.

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

Policy Manager

Table 27 *Known Issues in Policy Manager*

Bug ID	Description
#10881	Entity updates with PostAuth enforcement fail if the publisher is down.
#11744	**Symptom:** Upgrading from 5.2 to 6.x fails if CPPM is joined to the domain. **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. **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. **Workaround:** Manually change the value in days to the value in hours. In the above example, that would be 48 hours.
#13999 #13975	In order to add or update a PostAuth profile configuration, the admin must first delete old profiles from CPPM, and then add the new/updated profiles.
#14186	**Symptom:** Post auth doesn't work properly for UNKNOWN endpoints in a MAC Authentication Bypass (MAB) flow. **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. **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.
#18064	**Symptom:** AirWatch custom HTTP actions needs content even though it's not required. **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. **Workaround:** Do either of the following: • Add a header **Content-Length:0** in the **Context Server Action**. • 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.

Table 27 *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#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.
#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. **Scenario:** This occurs when the PANW firewall exceeds its supported limit advertised for user ID registration. **Workaround:** There is no workaround at this time.
#20453	In order for CPPM to have complete data to post to Palo Alto Networks devices in HIP reports, profiling must be turned on. This is the expected behavior.
#20455	**Symptom/Scenario:** When doing an SSO & ASO flow in Safari browsers, the certificate needs to be added in the trust list of the browser. **Workaround:** Please follow these steps: 1. Open the Safari browser and enter the SP URL. 2. After you enter the SSO application in the browser, the Show Certificate option is provided in a popup window. 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.
#20456	**Symptom:** SNMP bounce fails. **Scenario:** When only the SNMP bounce in the SNMP Enforcement profile of a Web auth service is configured, SNMP bounce functionality does not work. **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. **Scenario:** CPPM system time might not have been synchronized with an NTP source. **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. **Workaround:** The admin must manually fix the server certificate to allow a minimum of 1024 bits long Public Key prior to upgrade.
#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>.
#21334	**Symptom:** CPPM does not launch. **Scenario:** The ClearPass user interface will not launch from Firefox or from older versions of Internet Explorer (IE) browsers if an EC-based HTTPS server certificate is used. On Firefox, the error message "Secure Connection Failed. An error occurred during a connection to <*server*>. Certificate type not approved for application" is displayed. On older versions of IE, the error message "Internet Explorer cannot display the Web page" is displayed. **Workaround:** Use the latest version of IE, or the Chrome browser instead.

Table 27 *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#21444	**Symptom:** The CPPM Administrator UI is not accessible after upgrading to 6.3.0. **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. **Workaround:** Follow these steps: 1. Before upgrading to 6.3.0, export the Server Certificate and save it. 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. 3. Proceed with the upgrade. 4. After the upgrade, log in to the Admin UI and import the Server Certificate that was saved in step 1. 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. **Workaround:** Use the Chrome or Firefox browser instead.
#23581	**Symptom:** A database connection error occurs in the Access Tracker UI when it is updated to 6.3.2 with MD2 server certificates. **Scenario:** This is a database connection problem because of the MD2 certificate available for PostgreSQL. MD2 is not supported. **Workaround:** After updating to 6.3.2 (patch installation from 6.3.0), if Access Tracker or Analysis & Trending show errors relating to database query errors, it can be due to an invalid Server Certificate. 1. Go to **Server Certificate** and select the certificate for the server and RADIUS service. 2. Click **View Details** for each certificate in the chain. 3. Look for the **Signature Algorithm** and check to see if it uses MD2. 4. Download the certificate that is MD5 or SHA1-based algorithm to replace the MD2 algorithm from the corresponding Certificate Authority site. 5. From the Support shell, restart the cpass-postgresql service.
#23625	**Symptom:** Restoring the log DB in 6.3.2 overwrites existing event viewer entries. **Scenario:** In 6.3.2, restoring the log database alone (without configuration database restoration) from a backup results in the Event Viewer entries being overwritten with the ones from the backup. This has occurred in cases where the log database is restored manually after the upgrade. **Workaround:** There is no workaround at this time.
#23848	**Symptom:** The ClearPass server's time setting might sometimes be off by as much as eight hours. **Scenario:** This is due to a known issue with VMware tools, which periodically checks and synchronizes time between the host and the guest operating systems. This issue is documented by VMware at http://pubs.vmware.com/vSphere-50/index.jsp?topic=%2Fcom.vmware.vmtools.install.doc%2FGUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html. **Workaround:** There is no workaround at this time.
#24781	Palo Alto Networks (PANW) devices accept only the backslash (\ ) character as a separator between the domain name and the username. If the update uses an "at" sign (@) between the domain name and the username, the HIP report will not be shown in PANW.
#25211	When messages are sent using the Send Message option, messages are not received on the end points enrolled with SAP Afaria MDM Server.

Dissolvable Agent

Table 28 *Known Issues in the Dissolvable Agent*

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: https://<CPPM-IP-Address>/agent/html/help.html
#18031	**Symptom:** The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 installed. **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. **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. **Scenario:** New security restrictions in Mac OS X 10.9 and Safari 7 prevent the launch of the OnGuard Web agent. **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. **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.
#20514	Client health checks might not work if the client is not running the latest Java version.
#23253	**Symptom/Scenario:** Launching the Web Agent applet using some Java versions (7u55 and above) displays the security warning "This web site is requesting access and control of the Java application shown above. Allow access only if you trust the web site..." **Workaround:** Click **Allow** to let the health checks proceed.
#24518	**Symptom:** The first time a run or scan operation is initiated in the Native Dissolvable Agent flow, an "External protocol request" message is displayed, and if the user clicks the "Do Nothing" option, the message stays on the screen. **Scenario:** This occurs on the Chrome browser on both Windows and Mac OS X. **Workaround:** This message is produced by the Chrome browser and can be ignored. Click Launch Application in the External protocol request message.
#24762	**Symptom:** When launching the OnGuard dissolvable agent, Mac OS X displays the message "You are opening the application 'ClearPass OnGuard WebAgent' for the first time. Are you sure you want to open this application?" **Scenario:** This is the normal, default behavior of the Macintosh operating system, and is not an issue in OnGuard.
#24766	**Symptom/Scenario:** The Native Dissolvable Agent fails to download from IE on Windows 2008/XP if the "Do not save encrypted pages to disk" check box is enabled. **Workaround:** Go to **Internet Options** > **Advanced**. Uncheck (disable) the check box for the **"***Do not save encrypted pages to disk"* option.

Table 28 *Known Issues in the Dissolvable Agent (Continued)*

Bug ID	Description
#24768	**Symptom:** The native dissolvable agent does not work well in Internet Explorer on Windows XP. **Scenario:** The agent works after downloading it and allowing pop-ups, but no remediation results are displayed and, after clicking Launch ClearPass application, a series of messages is displayed in a loop. **Workaround:** Windows XP is an unsupported operating system. Use a later Windows version or the Chrome or Firefox browser instead.
#24792	**Symptom/Scenario:** Native Dissolvable Agent flow will not work properly on IE if ActiveX Filtering is enabled on IE settings. **Workaround:** For Native Dissolvable Agent to work properly on Internet Explorer, ActiveX Filter should be disabled.
#24862	**Symptom/Scenario:** Native Dissolvable Agent uses ActiveX on IE on Windows OS. Based on IE Security Settings, the browser may ask the user to run/allow 'ClearPass OnGuard Web Agent Control'. **Workaround:** For Native Dissolvable Agent to work properly on Internet Explorer, the user should allow 'ClearPass OnGuard Web Agent Control' ActiveX Control to run.

Guest

Table 29 *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. **Workaround**: If you plan to use Unicode SMS messages, check your SMS receipt carefully to ensure it is not over 70 characters in length.
#24751	**Symptom:** Disabled Translation packs are enabled after applying a patch update. **Scenario:** This was observed when upgrading from 6.3.0 to 6.3.4.
#25137	Please review your operator privileges for new features that may need enabled.

Insight

Table 30 *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.
#19507	PDF & HTML Data Tables are not created if the CSV file size is larger than 1MB, although the generated PDF and HTML reports include analytics if configured on the report.

Onboard

Table 31 *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.
#10667	When using Onboard to provision a OS X system with a system profile, an administrator user must select the appropriate certificate when connecting to the provisioned network for the first time. The administrator should also ensure that the system's network settings are configured to automatically prefer connecting to the provisioned network, if the intent is for non-administrator users to always use that network. The process to provision an OS X system with a system profile is: • The administrator should log in to the OS X system and connect to the provisioning SSID. Do not select “Remember this network.” • Use Onboard to provision the device with an EAP-TLS profile, ignoring the username/password prompt. • Connect to the provisioned network, selecting EAP-TLS as the mode and selecting the provisioned certificate, but ignoring the username field. • When the system connects and authorizes to the network, use Network Preferences to place the EAP-TLS network first in the priority list. • After the administrator logs out, users logging in are connected by EAP-TLS and cannot modify those settings.
#20983	**Symptom:** HTC Android asks the user to enter a certificate name to be installed when onboarding. **Scenario:** HTC Androids running Android version less than Android 4.3 and greater than Android 2.3 ask the user to enter a name for the certificate to be installed while onboarding. Authentication will fail if the user does not enter the exact certificate name as QuickConnect application instructs in a message prior to the certificate installation dialog. **Workaround:** None. This issue is due to a limitation in the Android phone’s firmware.
#23287	**Symptom:** Embedding Admin credentials for onboarding does not work in Windows 8 and above. The system hangs and there is no error message. **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 networks, 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. **Workaround:** There is no workaround. This is a Windows system limitation.
#25216	Onboarding fails for Mac OSX 10.6.8.
#25702 #25291	**Symptom/Scenario:** On Mac OS X 10.9.2 with no AirPort card installed, the error message **“**Profile installation failed. The wifi network payload could not be installed. Either the wifi network is not found or could not be connected” is displayed. **Workaround:** This is an issue with Apple’s configuration, and is not an Onboard issue. Users should be aware that configuring wired networks with Mac OS X is only supported when the Mac has a Wi-Fi adapter (an AirPort card or similar). This is due to system limitations of Apple’s device provisioning process. The note on the **Network Settings > Network Access** form now mentions this limitation, and specifies that wired-only networks are not supported for Android, iOS, and OS X 10.7+ clients.

Table 31 *Known Issues in Onboard (Continued)*

Bug ID	Description
#25711	iOS always displays SHA-1 for the signing algorithm regardless of the actual algorithm used. This is an issue with iOS, not Onboard.

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 32 *Known Issues in OnGuard*

ID	Description
#10165	**Symptom:** ClearPass OnGuard cannot restrict the clients based on Windows service packs. **Scenario:** If any of the Windows System Health Validator check fails, the health status of 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. **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. **Scenario:** This might occur during the installation of the ClearPass OnGuard Unified Agent on WinXP and Windows 2003 SP2. **Workaround:** Users should click **“**Continue Anyway**”** to proceed.
#13363	**Symptom:** On 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. **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: `/usr/local/bin/clearpassonguarduninstaller.sh`
#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.

Table 32 *Known Issues in OnGuard (Continued)*

ID	Description
#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. **Scenario:** This is observed when the ClearPass Unified OnGuard Agent has Real Time Protection (RTP). **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. **Scenario:** The client will be unhealthy if any of the health classes listed above are configured and performing a health scan via the DA.
#15986	ClearPass OnGuard returns the product name of Microsoft Forefront Endpoint protection AntiVirus as “Microsoft Security Essential”.
#16181	**Symptom:** The command level process can be detected using the path **“**none**”**, but the application level process can't be detected by setting the path to “none”. **Scenario:** This applies to MAC OS. **Workaround:** The application-level process health should be configured with the path set to **Applications > Firefox.app**.
#16550	**Symptom/Scenario:** The ClearPass OnGuard Unified Agent does not support checking of disk encryption state using the MacKeeper (ZeoBIT LLC) Disk Encryption Product on MAC OS X. This causes the client to be treated as healthy even if none of the disk is encrypted. **Workaround:** There is no workaround at this time.
#18259	**Symptom/Scenario:** The ClearPass OnGuard Unified Agent does not support Stop or Pause remediation actions 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. **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. 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.

Table 32 *Known Issues in OnGuard (Continued)*

ID	Description
#19685	**Symptom:** After upgrading OnGuard to 6.3, the backend service fails to start and is unable to collect logs. **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. **Workaround:** If the backend service fails to communicate with the plugin, reboot the system after the OnGuard upgrade is complete.
#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.
#23470	**Symptom/Scenario:** On a Japanese OS, when upgrading from VIA 2.1.1.3 to the ClearPass OnGuard Unified Agent, a known issue with uninstalling VIA displays a message asking the user to select the VIA driver. This does not occur on an English OS.
#23636	**Symptom:** The value of the Posture:Applied Policy attribute is not correctly displayed in the Access Tracker for posture policies carried over from releases earlier than 6.3.0. **Scenario:** This has been observed when upgrading from 6.2.6 to 6.3.2. **Workaround:** This can be corrected by manually saving the affected posture policy once after upgrade.
#23861	**Symptom/Scenario:** On MAC OS X, the ClearPass OnGuard Unified Agent sometimes fails to download a VIA connection profile after the application mode is changed. **Workaround:** None.
#24986	**Symptom:** The Native Dissolvable Agent is not automatically launched after downloading and running the agent the first time on the Chrome browser. **Scenario:** This occurs on Windows and on Mac OS X. **Workaround:** The first time you launch the Dissolvable Agent, click Launch ClearPass OnGuard Agent.
#25827	**Symptom/Scenario:** On Internet Explorer 8, when the security warning message is displayed that asks whether you want to view only the content delivered through a secure HTTPS connection, the behavior is not as expected. **Workaround:** For the Native Agent flow to work correctly, click **No** in the pop-up dialog.

QuickConnect

Table 33 *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. **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.
#25521	**Symptom/Scenario:** Embedding admin credentials is not supported on Windows 8+. **Workaround:** Provide the admin credentials manually during onboard provisioning.