ClearPass 6.6.0

Release Notes

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com.

Contents

Chapter 1
About ClearPass 6.6.0

ClearPass 6.6.0 is a major release that introduces new features and provides fixes to previously outstanding issues. These release notes contain the following chapters:

- "System Requirements for ClearPass 6.6" on page 9—Provides important system requirements information for this release.
- "Upgrade and Update Information" on page 19—Provides considerations and instructions for version upgrades and patch updates.
- "What's New in This Release" on page 25—Describes new features and issues introduced in this 6.6.0 release as well as issues fixed in this 6.6.0 release.
- "Known Issues Identified in Previous Releases" on page 53—Lists currently existing issues identified in previous releases.

Related Documents

The following documents are part of the complete documentation set for the 6.6 platform:

- *ClearPass Policy Manager 6.6 User Guide*
- *ClearPass Guest 6.6 User Guide*
- *ClearPass Policy Manager 6.6 Getting Started Guide*
- *ClearPass Deployment Guide*
- *Tech Note: Installing or Upgrading ClearPass 6.6 on a Virtual Machine*
- *Tech Note: Upgrading to ClearPass 6.6*

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, as well as 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 his/her Web browser.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/contact-support/
Software Licensing Site	licensing.arubanetworks.com
End of Support information	arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
Security Incident Response Team (SIRT)	arubanetworks.com/support-services/security-bulletins/

This chapter provides important system requirements information specific to this release. It should be read carefully before upgrading to ClearPass 6.6.

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

This chapter provides the following information:

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 rules allowing access, please be sure to update the IP address information accordingly.

End of Support

Please be aware that the following vendors have officially stopped supporting their respective operating systems on the stated dates.

Arubawill attempt to preserve compatibility with these legacy operating systems; however, recent versions of software agents (such as the ClearPass OnGuard Unified Agent) might not be able to provide the same level of functionality that they provide on newer operating systems.

We will not provide any further bug fixes or feature enhancements related to supporting these operating systems. Our TAC organization will also not be able to service customer support requests related to clients running these operating systems. Customers should consider these operating systems as unsupported with ClearPass:

- Microsoft Corporation:
  - Windows Server 2003 — July 14, 2015
  - Windows XP — April 8, 2014

- Apple, Inc:
  - Mac OS X 10.6 (Snow Leopard) — February 26, 2014

Virtual Appliance Requirements

Please carefully review all virtual appliance (VA) requirements, including functional IOP ratings, and verify that your system meets these requirements. These recommendations supersede earlier requirements that were published for ClearPass Policy Manager 6.x installations.

Virtual appliance recommendations have been adjusted to align with the shipping ClearPass hardware appliance specifications. If you do not have the VA resources to support a full workload, then you should consider ordering the ClearPass Policy Manager hardware appliance.

For VMware ESXi™ system requirements, see "ESXi Requirements " on page 10. For Microsoft Hyper-V™ system requirements, see "Hyper-V Requirements " on page 11. For complete information on installing, configuring, or morphing either ESXi or Hyper-V, see the *Tech Note: Installing or Upgrading ClearPass 6.6 on a Virtual Machine*.

Supported Hypervisors

The following hypervisors are supported. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 5.0, 5.1, 5.5, 6.0, or higher
- Microsoft Hyper-V Server 2012 R2
- Hyper-V on Microsoft Windows Server 2012 R2

ESXi Requirements

CP-SW-EVAL (Evaluation OVF)

- 2 Virtual CPUs
- 4 GB RAM
- 80 GB disk space

CP-VA-500 (500 Virtual Appliance OVF)

- 8 Virtual CPUs
  - Underlying CPU is recommended to have a PassMark® of 3000 or higher
- 8 GB RAM
- Disk space:
  - 500 GB disk space required for existing deployments (upgrading from 6.3.6, 6.4.7, or 6.5.x)
  - 1000 GB disk
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

CP-VA-5K (5K Virtual Appliance OVF)

- 8 Virtual CPUs
  - Underlying CPU is recommended to have a PassMark® of 9600 or higher

- 8 GB RAM
- Disk space:
  - 500 GB disk space required for existing deployments (upgrading from 6.3.6, 6.4.7, or 6.5.x)
  - 1000 GB disk
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

CP-VA-25K (25K Virtual Appliance OVF)

- 24 Virtual CPUs
  - Underlying CPUs are recommended to have a PassMark® of 9900 or higher
- 64 GB RAM
- Disk space:
  - 1000 GB disk space required for existing deployments (upgrading from 6.3.6, 6.4.7, or 6.5.x)
  - 1800 GB disk
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 350

Hyper-V Requirements

CP-SW-EVAL (Evaluation VHDX)

- 2 Virtual CPUs
- 4 GB RAM
- 80 GB disk space

CP-VA-500 (500 Virtual Appliance VHDX)

- 8 Virtual CPUs
  - Underlying CPU is recommended to have a PassMark® of 3000 or higher
- 8 GB RAM
- Disk space:
  - 500 GB disk space required for existing deployments (upgrading from 6.5.x)
  - 1000 GB disk space recommended for new deployments
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

CP-VA-5K (5K Virtual Appliance VHDX)

- 8 Virtual CPUs
  - Underlying is recommended to have a PassMark® of 9600 or higher
- 8 GB RAM
- Disk space:
  - 1000 GB disk

- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

CP-VA-25K (25K Virtual Appliance VHDX)

- 24 Virtual CPUs
  - Underlying CPUs are recommended to have a PassMark® of 9900 or higher
- 64 GB RAM
- Disk space:
  - 1800 GB disk
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 350

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, Windows 8.x, Windows 10, and Mac OS X.
- Google Chrome for Mac OS X and Windows.
- Apple Safari 3.x and later on Mac OS X.
- Mobile Safari 5.x on iOS.
- Microsoft Internet Explorer 10 and later on Windows 7 and Windows 8.x. When accessing ClearPass Insight with Internet Explorer (IE), IE 11 or above is required.
- Microsoft Edge on Windows 10.

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
- 300 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
- Ubuntu: 12.04 LTS and 14.04 LTS

Windows Vista, Windows 7, Windows 8.x Pro, Windows 10, 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 ClearPass 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
ClearPassOnGuardAgentService.exe
C:\Program Files (x86)\Aruba Networks\ClearPassOnGuard
C:\Program Files\Aruba Networks\ClearPassOnGuard

In current laboratory tests for ClearPass 6.6.0, we use the following antivirus software for our validations. Due to the large number of products available, this list may change at any time:

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

Some third-party anti-malware products are not supported by ClearPass OnGuard. For a complete list of supported third-party products, in Policy Manager go to **Administration > Support > Documentation**, and then click the **OnGuard Agent Support Charts** link.

ClearPass OnGuard Dissolvable Agent Requirements

This section provides version information for both the Native Dissolvable Agent and the Java-based Dissolvable Agent. For more information on the Dissolvable Agent, refer to the ClearPass Policy Manager online help.

ClearPass OnGuard Native Dissolvable Agent Version Information

In current laboratory tests for ClearPass 6.6.0, the browser versions shown in Native Dissolvable Agent Latest Supported Browser Versions for This Release 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.

The Native Dissolvable Agent is not currently supported with the Microsoft Edge browser. (#32664)

Table 1: *Native Dissolvable Agent Latest Supported Browser Versions for This Release*

Operating System	Browser
Windows 10 64-bit	Chrome 48.x (#24518, #24986)
	Firefox 44.x
	Internet Explorer 11.x
Windows 10 32-bit	Chrome 48.x (#24518, #24986)
	Firefox 44.x
	Internet Explorer 8.x (#25827)
Windows 8.1 64-bit	Chrome 49.x (#24986)
	Firefox 44.x
	Internet Explorer 11.x
Windows 8.1 32-bit	Chrome 49.x (#24986)
	Firefox 45.x
	Internet Explorer 11.x
Windows 8 64-bit	Chrome 48.x (#24986)
	Firefox 44.x
	Internet Explorer 10.x
Windows 8 32-bit	Chrome 48.x (#24986)
	Firefox 44.x
	Internet Explorer 10.x
Windows 7 64-bit	Chrome 48.x (#24518, #24986)
	Firefox 44.x
	Internet Explorer 11.x (#25827)
Windows 7 32-bit	Chrome 48.x (#24518, #24986)
	Firefox 44.x
	Internet Explorer 11.x
Windows 2008 64-bit	Chrome 48.x (#24986)
	Firefox 44.x
	Internet Explorer 8.x (#24766)

Table 1: *Native Dissolvable Agent Latest Supported Browser Versions for This Release (Continued)*

Operating System	Browser
Windows Vista	Chrome 48.x (#24986)
	Firefox 44.x (#29186)
	Internet Explorer 7.x (#29186)
Mac OS X 10.11	Safari 9.x (#29609)
	Firefox 44.x (#29609)
	Chrome 48.x (#24518, #24986, #29609)
Mac OS X 10.10	Safari 9.x (#29609)
	Firefox 44.x (#29609)
	Chrome 48.x (#24518, #24986, #29609)
Mac OS X 10.9	Safari 7.x (#29609)
	Firefox 44.x (#28398, #29609)
	Chrome 48.x (#24518, #24986, #29609)
Mac OS X 10.8	Safari 6.x (#28398, #29609)
	Firefox 43.x (#29609)
	Chrome 47.x (#24986, #29609)
Mac OS X 10.7.5	Safari 6.x (#29609)
	Firefox 44.x (#29609)
	Chrome 48.x (#24986, #29609)
Ubuntu 14.04 64-bit LTS	Firefox 44.x
Ubuntu 14.04 32-bit LTS	Firefox 38.x (#28398)
Ubuntu 12.04 64-bit LTS	Firefox 34.x
Ubuntu 12.04 32-bit LTS	Firefox 38.x

ClearPass OnGuard Java-Based Agent Version Information

In current laboratory tests for ClearPass 6.6.0, the browser and Java versions shown in Supported Browser and Java Versions for This Release were verified for the ClearPass OnGuard Java-based dissolvable agents. There are considerations to be aware of with some browser versions. For 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 2: *Supported Browser and Java Versions for This Release*

Operating System	Browser	Java Version
Windows 10 64-bit	Firefox 44.x (#7165)	JRE 1.8 Update 73
	Internet Explorer 11.x (#7165)	JRE 1.8 Update 73
Windows 10 32-bit	Firefox 44.x (#7165)	JRE 1.8 Update 73
	Internet Explorer 11.x (#7165)	JRE 1.8 Update 73
Windows 8.1 64-bit	Firefox 40.x	JRE 1.8 Update 73
	Internet Explorer 11.x	JRE 1.8 Update 73
Windows 8.1 32-bit	Firefox 45.x	JRE 1.8 Update 77
	Internet Explorer 11.x	JRE 1.8 Update 77
Windows 8 64-bit	Firefox 44.x (#7165, #33332)	JRE 1.8 Update 73
	Internet Explorer 10.x (#7165)	JRE 1.8 Update 73
Windows 8 32-bit	Firefox 44.x	JRE 1.8 Update 73
	Internet Explorer 10.x	JRE 1.8 Update 73
Windows 7 64-bit	Firefox 44.x (#7165, #33332)	JRE 1.8 Update 73
	Internet Explorer 11.x	JRE 1.8 Update 73
Windows 7 32-bit	Firefox 44.x	JRE 1.8 Update 73
	Internet Explorer 11.x	JRE 1.8 Update 73
Windows 2008 64-bit	Firefox 44.x (#7165)	JRE 1.8 Update 73
	Internet Explorer 7.x (#7165)	JRE 1.8 Update 73
Windows Vista	Firefox 44.x (#7165, #33332)	JRE 1.8 Update 73
	Internet Explorer 9.x (#7165)	JRE 1.8 Update 73
Mac OS X 10.11	Safari 9.x (#20191)	JRE 1.8 Update 73
	Firefox 44.x	JRE 1.8 Update 73
Mac OS X 10.10	Safari 9.x (#20191)	JRE 1.8 Update 73

Table 2: *Supported Browser and Java Versions for This Release (Continued)*

Operating System	Browser	Java Version
	Firefox 44.x	JRE 1.8 Update 73
Mac OS X 10.9.5	Safari 7.x (#20191)	JRE 1.8 Update 73
	Firefox 44.x	JRE 1.8 Update 73
Mac OS X 10.8	Safari 6.x	JRE 1.8 Update 73
	Firefox 44.x (#20191)	JRE 1.8 Update 73
Ubuntu	Firefox 44.x	JRE 1.8 Update 73
CentOS	Firefox 44.x	JRE 1.8 Update 73
RedHat	Firefox 44.x	JRE 1.8 Update 73
SUSE	Firefox 44.x	JRE 1.8 Update 73

ClearPass Onboard Requirements

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

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 6.5.x to 6.6.0. For information on upgrading from a version prior to 6.6, see "Upgrading to ClearPass 6.6 from 6.3.6, 6.4.7, or 6.5.x" on page 19.
  - To upgrade a cluster to 6.6.0, we recommend using the Cluster Upgrade Tool. For more information, see Appendix B, “Cluster Upgrade/Update Tool,” in the *ClearPass Policy Manager User Guide*, and the “Cluster Upgrade and Update” sections in these Release Notes.
- The term “update” refers to applying a patch release within the same major version—for example, from 6.4.3 to 6.4.4, or from 6.5.2 to 6.5.5. For information on updating, see "Updating Within the Same Major Version" on page 22.

Upgrading to ClearPass 6.6 from 6.3.6, 6.4.7, or 6.5.x

An upgrade is the process of moving from one major release version to another—for example, from 6.5.x to 6.6.0. 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 6.6.0 from ClearPass 6.3.6, 6.4.7, or 6.5.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 22.

- For 6.5.x upgrades, versions 6.5.0 (FIPS/Non-FIPS) and 6.5.1 (FIPS only) require applying the ClearPass 6.6.0 Upgrade Preparation Patch before upgrading to 6.6.0 if the upgrade image needs to be manually imported into the UI or installed through the CLI. This patch is available through the Aruba Support site or through the Software Updates portal. Version 6.5.2 and later do not require the preparation patch.
- For 6.4.x upgrades, you must update to 6.4.7 followed by applying the ClearPass 6.6.0 Upgrade Preparation Patch before upgrading to 6.6.0 if the upgrade image needs to be manually imported into the UI or installed through the CLI. This patch is available through the Aruba Support site or through the Software Updates portal.
- For 6.3.x upgrades, you must update to 6.3.6 followed by applying the ClearPass 6.6.0 Upgrade Preparation Patch before upgrading to 6.6.0 if the upgrade image needs to be manually imported into the UI or installed through the CLI. This patch is available through the Aruba Support site or through the Software Updates portal.
- For 6.1.x and 6.2.x, direct upgrades are not supported. Customers on 6.1.x or 6.2.x must intermediately upgrade to 6.3.6, 6.4.7, or 6.5.x first before upgrading to 6.6.0.
- For appliance upgrades from 5.2.0, you must upgrade to 6.3.6, 6.4.7, or 6.5.x before upgrading to 6.6.0.
- Upgrade images are available within ClearPass Policy Manager from the Software Updates portal at **Administration > Agents and Software Updates > Software Updates**.
- Upgrade images and preparation patches are also available for download on the Support site under **ClearPass > Policy Manager**.

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 Mobile Device Management (MDM) integration can significantly increase upgrade times. Refer to the sample times shown in Sample Times Required for Upgrade in "Sample Times Required for Upgrade" on page 20.
- Review the ESXi and Hyper-V disk requirements. These are described in "Virtual Appliance Requirements" on page 10 of the "System Requirements for ClearPass 6.6" 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.

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 21.

- Before initiating the Upgrade process in ClearPass, we recommend you set the **Auto Backup Configuration Options** to **Off** (if it was set to other values such as Config or Config|Session). The 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 21). Please contact Customer Support for configuration recommendations to move away from using the session log database as an authentication source.
- MySQL is supported in ClearPass 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.
- VM only: If you have two disks already loaded with previous ClearPass versions—for example, 6.2 on SCSI 0:1 and 6.3 on SCSI 0:2—then drop the inactive disk before upgrading. You must then add a newer disk based on the 6.6 disk requirements. Earlier releases used separate disks to store the current and previous ClearPass release; newer releases use just a single drive to store both installations. For current requirements, see "Virtual Appliance Requirements" on page 10.

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 3: *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
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 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 **Administration > 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. Uncheck 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 6.5.4 to 6.5.5. 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 retained. No extra steps are needed to retain the session log history during a patch update.

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 ClearPass 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**.

This chapter provides a summary of the new features and changes in the ClearPass 6.6.0 release.

This chapter contains the following sections:

Release Overview

ClearPass 6.6.0 is a major release that introduces new features and provides fixes for known issues. The 6.6.0 upgrade is available in ClearPass Policy Manager under **Administration > Agents and Software Updates > Software Updates**.

Important Changes

Users should be aware of the following important changes in ClearPass behaviors and resources:

- The system requirements for the CP-VA-500 virtual appliances have changed. For details, see "Virtual Appliance Requirements" on page 10.
- All VMware ESXi virtual machines now use hardware version 8.
- VMWare ESX 4.0 is no longer supported.
- Changes to the TAG mappings tables to improve performance and scalability may impact SQL filters in use by custom authentication sources. The following tables have been removed and a more efficient method has been implemented. If you are currently using these tables, we recommend that you contact Aruba support prior to upgrade:
  - TIPS_AUTH_LOCAL_USER_TAG_MAPPINGS
  - TIPS_GUEST_USER_TAG_MAPPINGS
  - TIPS_NAD_CLIENT_TAG_MAPPINGS
  - TIPS_ENDPOINT_TAG_MAPPINGS
  - TIPS_TAG_VALUES
- ClearPass 6.6.0 is the last release that will support Java for the Windows or Mac OS X ClearPass OnGuard Dissolvable Agent.
- The **Configuration > Posture > Posture Servers** page and the **Administration > Dictionaries > Posture** page have been removed.
- ClearPass VMs are now shipped as a single virtual machine installation image per hypervisor type: either VMWare ESXi or Microsoft Hyper-V image. During installation, a new menu option lets the administrator select the type of image they want to install — either CP-SW-EVAL, CP-VA-500, CP-VA-5K, or CP-VA-25K. For more information, refer to the *Installing ClearPass 6.6 on a Virtual Machine* Tech Note. (#28018)

- ClearPass 6.6.0 introduces a re-designed ClearPass Insight. Several data columns have been replaced which may impact Syslog filters after upgrade. For example, if the **Authentication** columns were used, you need to manually update the Syslog filter to use the new **Endpoint** columns. A notification or error is not displayed during upgrade, but is displayed if you open the Syslog filters and attempt to save again.
- The Aruba Linux Cryptographic Module, which is based upon OpenSSL 1.0.2f, no longer supports Diffie-Hellman parameters shorter than 1024 bit. This might impact third-party applications that have not updated their software to protect against the Logjam vulnerability.

New Features and Enhancements in the 6.6.0 Release

The following new features were introduced in the ClearPass 6.6.0 release.

This section includes the following:

Cluster Upgrade and Update

The following new features are introduced for cluster upgrades and updates in the 6.6.0 release.

- The Cluster Upgrade Tool, which automates the process of upgrading a ClearPass cluster, is now natively available within Policy Manager's Administration module, and includes additional enhancements: (#28327, #28454)
  - In addition to the interface for upgrading a cluster, the Cluster Upgrade Tool now also provides an interface for cluster updates. The administrator can use it to update subscribers with cumulative patch updates within a release train (for example, from 6.6.0 to 6.6.1), or apply other available software updates. The process for updates is similar to the process for upgrades.
  - The administrator can install software upgrades or updates to all subscribers in a cluster or specify only certain subscribers.
  - On the **Administration > Agents & Software Updates > Software Updates page**, two new links in the upper-right corner, **Cluster Upgrade** and **Cluster Update**, let you open the appropriate page. These links become available when the publisher is upgraded to ClearPass 6.6.
  - On the publisher, after updates are downloaded on the **Software Updates** portal, they are available for selection in a drop-down list on the **Cluster Update** page. You can use either the **Cluster Update** link or the **Install** button for a patch to open the **Cluster Update** page.
  - Starting with the 6.6.0 release, the Cluster Upgrade Tool documentation is no longer separate. Cluster Upgrade Tool issues are now included in the ClearPass Release Notes. The information that was provided in the Cluster Upgrade Tool Tech Note in earlier versions is now included in Appendix B, "Cluster Upgrade/Update Tool," in the *ClearPass Policy Manager User Guide*, and can be accessed from the online help link on the **Cluster Upgrade** page or the **Cluster Update** page.

Endpoint Context Servers

The following new features are introduced in Endpoint Context Servers in the 6.6.0 release.

- The following Context Server Actions are now supported to improve joint functionality with MobileIron: (#28144)
  - Delete only corporate information stored and remove device from MobileIron EMM management – Retire/Enterprise Wipe (UUID or Device MAC Address)
  - Send wake-up to device, request check-in – Wake-up Device (UUID or Device Mac Address)
  - Remove label and corresponding policies
  - Apply label to identify when devices have attached to corporate WiFi and apply corresponding policies
  - Send SMS message to cellular devices (UUID)
  - Send Push Notification (UUID)
- The Check Point® login and logout actions have been enhanced with new URLs and updated content and attributes. The Check Point login action has also been separated into **Check Point Login – AD User** for active directory users and **Check Point Login – Guest User** for guests. To view or configure the updated Check Point login and logout actions, go to **Administration > Dictionaries > Context Server Actions**. (#28145)
- ClearPass supports Juniper Networks SRX servers as endpoint context servers. This allows a ClearPass server to enable communication between the ClearPass server and the Juniper SRX server. (#28455)
- Clearpass natively supports Endpoint Context Server Action for Infoblox, enhancing its IP address management service by providing username context. (#29559)

Guest

The following new features are introduced in ClearPassGuest in the 6.6.0 release.

- ClearPass Guest now supports **SMPPv3.4** as an SMS gateway. This option is available at **Configuration > SMS Services > Gateways** in the **SMS Gateway** field. (#9747)
- The **expire_timezone** field is now stored as a persistent guest field. Receipts and edits made after an account is created are now displayed in the account's local time zone. (#26032)
- Hotspot Manager now includes the following enhancements for customizing Payment Management System (PMS) plans based on data about the hotel guest: (#27691, #28539, #28540)
  - Hotel hotspot plans can be created so that guest accounts expire on the expected day of departure. On the hotspot plan configuration form, the **Time Tracking** field includes a new option, **Checkout date - Expiration will be midnight the day of the checkout (Hotel PMS only)**.
  - Hotel hotspot plans can be created so that new devices can use a plan that is already created and paid for. On the hotspot plan configuration form, the **Time Tracking** field includes a new option, **Already paid - Select for other devices to share a paid plan (Hotel PMS only)**.
- A new option in Social Logins configurations, **Friends**, allows retrieval of the guest's friends list when Facebook is selected as the provider. Permission must also be granted by the guest, and only friends who also use your application ID can be retrieved. (#27836)
- A new option in Social Logins configurations, **Google Groups**, allows retrieval of Google Group membership information when Google is selected as the provider. If this option is selected, the **Admin SDK Refresh Token** and **Authorization Code** must also be regenerated. (#27882)
- A new **Terms and Conditions** Web page template has been added to the list of templates at **Configuration > Pages > Web Pages**. This page can be customized and used to present your terms and

conditions of use to guests, and is referenced by the **Terms Of Use URL** field on the **Configuration > Guest Manager** form. (#28156)

- ClearPass now provides multi-factor authentication for guest logins. Multi-factor authentication lets you require multiple factors, or proofs of identity, when authenticating a user. To configure multi-factor authentication (MFA) in ClearPass, you first create an account with an MFA provider and create the users for the guest account. You then set up either a captive portal login or an Onboard login. The list of MFA providers currently supported in ClearPass includes Duo Security Two Factor Authentication, Facial Network ZOOM Multi-Factor Authentication, Imageware Systems GoMobile Interactive, and SMS Verification Codes. Multi-factor authentication can be configured in ClearPass Guest at **Configuration > Pages > Web Logins**, and at **Onboard > Deployment & Provisioning > Provisioning Settings > Web Login**. For more information, see "About Multi-Factor Authentication" in the *ClearPass Guest User Guide*. (#28452, #30199, #30420, #32711)

  When you configure the multiple factors, or proofs of identity, for authenticating a user, usually at least two of the following categories are required:

  - Knowledge: A secret the user knows, such as their password or PIN.
  - Possession: Something the user has, such as a security token generator or a certificate. This requirement can also be met by having the user answer a registered phone number or email address to retrieve a temporary code.
  - Inherence: A physical characteristic of the user, such as their voice, face, or fingerprint.

  Policy configurations can define how often multi-factor authentication will be required, or conditions that will trigger it:

  - Time-based policy: Policy might require MFA on a daily or weekly basis, or if the user has not logged in from the device for a certain number of days, or if the device was unhealthy in the past 30 days.
  - Posture-based policy: Policy might require MFA if the device's posture changes to unhealthy, or if the posture of any of the user's other devices changes to unhealthy, or if a company alert or security check is issued.
  - Policy based on other conditions: Policy might require MFA if the user has never logged in from the location before, or has failed authentication three times, or if a third-party application or system triggers MFA.
- A new option, **Arbitrary Sort**, is available in the API Framework Plugin configuration. This option lets you override default sort-field settings and specify any field as the sort column through the API. (#29462)
- The page loading time is faster for admin pages with HTML editing areas that include content item drop-down lists. (#31087)
- Social login support was added for Microsoft Azure Active Directory. (#32338)
- Support was added for Norwegian translations in many guest-facing pages. (#33470)

Insight

The following new features are introduced in Insight in the 6.6.0 release.

- ClearPass Insight has a new user-friendly interface. In addition to a new look and feel and added Dashboard elements, the new Insight UI provides improved, easy-to-use reporting and alerts features. Search and performance are enhanced, data and analytics are more powerful, and pre-configured reports and alerts are available. (#28449, #29238, #29270, #29339, #29420, #31409, #31410, #31411)

  The new Insight UI includes:

  - Counts summary — Counts for **Total Auth**, **Failed Auth**, **Unique Endpoints**, **Unique Users**, and **Alerts Created** are displayed at the top of each page.
  - **Dashboard** section — This item in the left navigation opens the **Dashboard** home page, which displays several report widgets. Subheadings in the left navigation let you display pages for any of the following categories: **Authentication**, **Endpoints**, **Guest**, **Network**, **Posture**, **System**, or **System Monitor**. Whether you are on the Dashboard home page or one of its subheadings, controls in each widget let you create a report or alert for it. You can also customize the Dashboard home page by adding or removing widgets. The default look-back window for the data in each widget is 24 hours. An exception to this is the System Monitor widget, which shows data for the previous two hours.
  - **Reports** section — This item in the left navigation opens the **Reports** home page, which displays the "news feed" activity summaries for **Yesterday**, **Today**, and **Tomorrow**, the list of **Created Reports**, and the **Create New Report** button. You can click the name of a report in the list to view it in a new tab, or click the **Configuration** subheading in the left navigation to edit a report. Creating a new report is simple and easy, with a wizard to walk you through each step. Report categories available in this release are authentication, endpoint, guest authentication, network, OnGuard (Linux, Mac, and Windows), Onboard, RADIUS authentication, system, and TACACS.
  - **Alerts** section — This item in the left navigation opens the **Alerts** home page, which displays the list of created alerts and the **Create New Alert** button. You can click the name of an alert in the list to view it in a new tab, or click the **Configuration** subheading in the left navigation to edit an alert. Alert categories available in this release are authentication, system, and TACACS.
  - **Administration** section — This item in the left navigation opens the Insight **Administration** home page, where you can work with file transfer settings and database settings.
  - **Search** field — Allows searching by username (Username or Auth_username), endpoint (Host, MAC, or Host IP), ClearPass server (ClearPass Server IP or name), or network device (NAD IP, NAD Name, or NAD MAC). The **Search** field can auto-complete
  - Workflow — The new workflow for creating or editing a report or alert is simple and intuitive.
  - Differentiated user access — Insight now supports multi-level administrator access:
    - Each of the Insight modules (Dashboard, Reports, Alerts, Administration) can have three privilege levels or no privilege: read, read/write, or read/write/delete.
    - A login area on each page of the Insight user interface lets the user log in as an administrator or super administrator.
    - In the case of no privilege, the link on the left navigation won't be visible for a user who does not have the appropriate privilege.
    - Users can be assigned Insight privileges from two locations: **Guest > Administration > Operator Logins > Profiles**, and **Policy Manager > Users and Privileges > Admin Privileges**.

  Insight is not enabled by default. To enable Insight, go to the server configuration page at **https://<Your-ClearPass-IP>/**. On the **System** tab, select the appropriate option in the **Insight Setting** field.

- The Insight OnGuard reports now include Posture Evaluation Results as part of Raw data. The following health classes indicate which checks failed for these health classes: (#29783)
  - AntiSpyware
  - AntiVirus
  - Disk Encryption
  - File Check
  - Firewall
  - Installed Applications
  - Network Connections
  - P2P
  - Patch Management
  - Processes
  - Registry Keys
  - Services
  - USB Devices
  - Virtual Machines
  - Windows Hotfixes
- Support for Domain Name was added to the inbound legacy API and hte OAuth2-based API. (#30469)

Onboard

The following new features are introduced in Onboard in the 6.6.0 release.

- Onboard certificate signing requests now track the time the request was received. On the **Onboard > Management and Control > View by Certificate** list view, this information is included in the details provided by the **View request** link, and can also be displayed by configuring the view's columns to include **Request Received At**. (#27053)
- The logic Onboard uses to send required RADIUS certificates is updated. To avoid the need to reprovision when the RADIUS certificate expires, only the chain will be sent instead of the certificate itself. (#28715)
- Support was added for the EAP-SIM authentication protocol for both iOS and Android devices. This can be configured at **Onboard > Configuration > Network Settings** on the **Protocols** tab. (#30134)
- Support was added for properly filling the "Configure Certificate Selection" option available in Windows 8 and higher. This enables usage of the correct client certificate for EAP-TLS even when multiple 802.1X-eligible certificates are present in the client. (#32554)
- A new option in Onboard allows QuickConnect to install certificates in the system store for Android. The **Onboard > Network Settings > Authentication** tab now includes an **Android Authentication** area with a **Certificate Store** field. The options available for this field, **Private** or **System**, specify the certificate store where the client certificate will be provisioned when configuring an Android device. When certificates are installed in the system store, they will be available for use by other applications. Additional security prompts might be required during provisioning.(#32700)
- Support was added for renewal of SCEP certificates in Onboard. (#33234)

OnGuard

The following new features are introduced in OnGuard in the 6.6.0 release.

- Support was added for the following products: (#32719)
  - Avast Free Antivirus 11.x (Windows)
  - Avast Pro Antivirus 11.x (Windows)
  - AVG AntiVirus 2016.x (Windows)
  - AVG AntiVirus Free Edition 16.x (Windows)
  - Avira Free Antivirus 15.x (Windows)
  - Check Point Endpoint Security 8.x (Mac OS X)
  - Check Point Endpoint Security [Firewall] 8.x (Mac OS X)
  - McAfee Endpoint Security for Mac 10.x (Mac OS X)
  - Oracle VM VirtualBox 5.x (Windows)
  - Symantec Hosted Endpoint Protection 2.x (Windows)

  Support was enhanced for the following products:
  - Casper Suite 9.x (Mac OS X)
  - ESET Cyber Security 6.x (Mac OS X)
  - ESET Endpoint Antivirus 6.x (Mac OS X)
  - ESET Endpoint Antivirus 6.x (Windows)
  - ESET Endpoint Security 6.x (Windows)
  - Kaspersky Anti-Virus on Mac 15.x (Mac OS X)
  - Kaspersky Endpoint Security 10.x (Windows)
  - McAfee Host Intrusion Prevention 8.x (Windows)
  - McAfee Virus Enterprise 8.8.06000 (Windows)
  - Malwarebytes Anti-Malware 2.x (Windows)
  - Microsoft Windows Firewall 10.x (Windows)
  - Sophos Anti-Virus 9.x (Mac OS X)
  - Symantec Endpoint Encryption 11.x (Windows)
- The **Install Level Check Type** option offered in the Patch Management health class allows OnGuard to check Mac OS X client devices for missing updates. When auto-remediation is enabled, OnGuard installs the missing updates automatically. (#23834)
- The ClearPass Native Dissolvable Agent now supports Auto-Upgrade. When a new version becomes available on the ClearPass server, the Native Dissolvable Agent will upgrade automatically and run health checks after the upgrade is installed. (#25061)
- Two new fields were added for health classes. Perl regular expressions are supported for both of the following fields: (#25819, #31886)
  - The **Enable Regular Expression** field was added to the **Installed Applications** health class. If this field is enabled, the policy server treats the application name as a regular expression when comparing application names. This option can be used for Windows and Mac OS X.

    - The **Enter Regex pattern for Registry value** field was added to the **Registry Keys** health class. If a Regex pattern is specified, the policy server will use the regular expression for comparing registry key values.
- ClearPass now computes OnGuard licenses based on devices/endpoints instead of MAC addresses. (#27748)
- The ClearPass OnGuard Unified Agent on Windows now supports running in Service mode; it performs health checks even if the user is not logged in. To use this feature, go to **Administration > Agents and Software Updates > OnGuard Settings** and click **Global Agent Settings**. Select the new parameter **Run OnGuard As**, and specify the value as either **Agent**, **Service**, or **BothAgentAndService**. For creating different policies for OnGuard mode, two new attributes, **Host::AgentType** and **Host::HealthCheckLevel**, are available in service rules. (#29673)
- On the **Administration > Agents and Software Updates > OnGuard Settings** page, a new **Native Dissolvable Agent Customization** area allows administrators to select which interfaces are to be allowed for the Native Dissolvable Agent. The Native Dissolvable Agent will only perform health checks for interfaces that are specified in the **Native Dissolvable Agent Customization** area. Options include **Wired**, **Wireless**, **VPN**, and **Other**. This ensures that, if both wired and wireless interfaces are connected, the OnGuard Agent will send health requests through the correct interface. (#30333)
- System tray icons for the ClearPass OnGuard Unified Agent running in VIA + OnGuard mode now show the status of both VIA and OnGuard components. OnGuard standalone system tray icons have also been updated. (#31074)
- The OnGuard Agent support charts that used to be accessed through the online help are now directly available in the user interface at **Administration > Support Documentation**. Click the **OnGuard Agent Support Charts** link on that page to open a list of platform-specific links providing complete information regarding supported antivirus, antispyware, firewall, disk encryption, peer-to-peer, patch management, and virtual machine software. (#32722)

Policy Manager

The following new features are introduced in Policy Manager in the 6.6.0 release.

- The Access Tracker now displays the results of unhealthy endpoints. Go to **Monitoring > Live Monitoring > Access Tracker**, double-click on a request, and then click the **Output** tab. A new section, **Posture Evaluation Result**, indicates which checks failed for the following health classes: (#12089, #29782, #29783, #31887)
    - AntiSpyware
    - AntiVirus
    - Disk Encryption
    - File Check
    - Firewall
    - Installed Applications
    - Network Connections
    - P2P
    - Patch Management
    - Processes
    - Registry Keys
    - Services

- USB Devices
- Virtual Machines
- Windows Hotfixes

- ClearPass 6.6 is now able to extract the auth-session-id from CiscoAVPair VSA to use in Change of Authorization (CoA). The username value is now used as the key when creating or querying a session in a multi-master session cache. This makes it possible to send a CoA when the Calling-Station-ID value includes the IP address format. To use this feature, in Policy Manager go to **Configuration > Enforcement > Profiles**, copy the default [Cisco - Terminate Session] profile, and modify it to include the Cisco-AVPair attribute. For more information on configuration, testing, and troubleshooting, refer to the *Policy Manager 6.6 User Guide*. (#17812)
- Cisco ASA requires the audit Session ID in the RADIUS Change of Authorization (CoA) message. ClearPass extracts the audit-session-id from the VPN RADIUS authentication message. There are new properties to cache the Cisco-AVPair with the value that contains the audit-session-id. These properties can be used to cache any custom attribute that contains the particular value. (#24403)
- Various new options such as protocol filters and port filters were added to the packet capture diagnostic tool in the admin UI and the CLI. (#26091)
- The Trapeze RADIUS dictionary was updated. (#26478)
- Syslog support was added for Apache and Samba logs. Data in Apache access and error logs and SAMBA windbindd logs can now be streamed to external syslog servers for third-party monitoring. To use this feature, go to **Administration > Server Manager > Log Configuration > System Level** tab and enable the **Apache web server** and **Domain service** log services. (#27123, #28347, #31316)
- Endpoint fingerprints functionality is updated to allow the administrator to either override the fingerprint or add a new rule based on the learned attributes, creating a new entry in the Fingerprint dictionary. This allows unknown endpoints to be categorized as desired with a new custom fingerprint. The device MAC vendor is added by default when a new rule is created. (#27659)
- The `system morph-vm` command is now supported for non-evaluation VM versions. It has been modified to allow conversions from a lower capacity VM to a higher capacity VM only, using the new single virtual machine installation image, in case the wrong VM is installed. Additional enhancements are described below: (#28862, #30762)
  - The restore step after rebooting was eliminated. This significantly reduces the overall time for the morph operation, and the cluster setup is retained.
  - Node service parameters whose defaults and range are set based on the model number are now automatically reset in the local database when morphing a publisher, and on the remote publisher when morphing a subscriber.
  - During the first boot and morph command, additional warning messages are provided if system requirements are not met.

  For information about how to morph a VM more than once, see the "*Installing or Upgrading ClearPass 6.6 on a Virtual Machine*" Tech Note.
- The SNMP private management information base (MIB) in ClearPass now includes service start, stop, and restart Traps, providing more granular control for handling these service actions. (#30186)
- The new Ingress Event Engine enables ClearPass to process Syslog events from third-party devices to make policy changes in realtime. For example: (#28446, #29415, #30254, #32451)
  - A third-party device could signal to a ClearPass server to quarantine or block a user if the contents indicate the presence of malware.

- Syslog dictionaries from leading vendors such as Palo Alto Networks, Checkpoint, Juniper Networks, and Fortinet are included by default.
- Administrators may also create custom dictionaries on their own.
- An **Event Requests** filter is also included in the data filters at **Monitoring > Live Monitoring > Access Tracker > Select Filter**, letting you filter for all event-based records.
- The **Batch Processing Interval** service parameter is available on the **Service Parameters** tab at **Administration > Server Manager > Server Configuration** when **Async network services** is selected for a server. This parameter lets you control the batch processing interval of Ingress Event processing. The default interval value is 30 seconds. The allowed values are 10-300 seconds. Users should be aware that, in order for changes to this service parameter to take effect, **Async network services** must be restarted.

- Network Discovery is a new feature that facilitates the addition of network devices. It uses a configured "seed network device" (typically a switch/router/controller) to discover endpoints and network devices. The seed device is queried using configured SNMP credentials (see **Configuration > Profile Settings > SNMP Configuration**). Network Discovery scans are initiated from **Monitoring > Network Discovery > Start Network Discovery Scan**. The following information is read from the seed device: (#28448)
  - SNMP information: The system name, vendor, system location, system contact, and system description are captured from accessible network access devices.
  - Connected endpoints: Information about endpoints connected to the network device (typically MAC addresses of endpoints connected to switch ports). These are added as discovered endpoints.
  - ARP table: Provides information about MAC > IP associations for endpoints that were seen by this device recently. These endpoints are probed further in an attempt to profile them using all supported mechanisms.
  - Neighbor network devices: Other network devices connected to the seed device, as determined by neighbor discovery protocols like Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) (if enabled in your network).

  Each of the discovered neighbor network devices is further queried as a seed device; this is repeated for multiple levels in your network up to a specified scan depth parameter (maximum 3 levels).

  Network devices discovered through a scan are available for review at **Monitoring > Network Discovery > View Discovered Devices**. Discovered devices can be imported and added to **Network Devices**.
- Support for port bounce was added to Mobility Access Switches as part of their 7.4.0.3 release to facilitate VLAN changes and profiling. To enable this support, the ClearPass RADIUS dictionary is updated to support VSA 40 (Aruba-Port-Bounce-Host). The default Aruba Terminate Session attribute now includes this entry. (#28532)
- The structure for endpoint attributes is now simplified to achieve better performance. The **`tips_endpoints`** table has a new column **`attributes::JSONB`**. The attributes column holds information for an endpoint in JSON structure. (#28642)
- ClearPass 6.6 provides a new option to disable log database backups during major upgrades. This reduces the time to upgrade a node, especially with large log database sizes. Enable this option if you do not plan to restore the log database post-upgrade. (#28841)
- A new service parameter, **Additional time before session deletion from multi-master cache**, was added to the list of policy server parameters available at **Administration > Server Manager > Server Configuration**. When configured, the policy server will wait the additional configured number of seconds before deleting an entry from the multi-master cache. The default value is zero. This feature is useful in wireless roaming situations where a client may roam from one controller to another and ClearPass may

receive an Accounting-Stop and Start in rapid succession, which can result in ClearPass mistaking which NAD the client is attached to. (#29015)

- The **`pg_stat_statements`** extension is now added to the ClearPass log collection. This feature tracks the queries excecuted in the database, and provides daily log with PostgreSQL stats for debugging. It is available under the system-load-monitor directory as part of collect logs. (#29115)
- The Infoblox RADIUS dictionary was added. (#29406)
- REST API support was added for the following ClearPass entities: (#29458)
  - AdminUser
  - AuthMethod
  - AdminPrivilege
  - Endpoint
  - Insight/Endpoint
  - LocalUser
  - NetworkDevice
  - NetworkDeviceGroup
  - ProxyTarget
  - Role
  - StaticHostList
- A new cluster-wide parameter, `cli session idle timeout`, lets clients configure the idle time allowed during a CLI session before a session timeout. Any changes made to the idle time duration will go into effect when a new session is opened. This option is available at **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab. (#29797)
- SNMP support has been enhanced to include the hrProcessorTable. (#29857)
- A new RADIUS service parameter, **Check the validity of intermediary certificates in the chain using OCSP**, was added to enhance certificate security. This feature is disabled by default. Enabling this feature will put greater load on the system and is not intended for all customer use cases. (#30077)
- Support was added for disabling TLS 1.0 in the WebUI and the RADIUS server. A new cluster-wide parameter, **DisableTLSv1.0 support**, is available on the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab. (#30078)
- ClearPass 6.6 adds the ability to profile endpoints based on commands executed over an authenticated SSH or WMI session. Multiple SSH/WMI credentials can be configured per subnet under **Configuration > Profile Settings > SSH/WMI Configuration**. When a new endpoint IP address is detected through one of the endpoint discovery mechanisms (subnet scans, SNMP based ARP table read), the endpoint is probed to determine if SSH (TCP port 22) or WMI (TCP port 135) is open. If a port is open, an attempt is made to establish a session using configured credentials. If a session is established successfully, commands are executed over the session to determine the endpoint's device type. ClearPass 6.6 includes fingerprints to profile endpoints based on device type determined from a SSH/WMI session. (#30260, #30319)
- ClearPass now supports public key-based SSH logins on a per-appliance basis. A new **SSH Public Keys** option is available at **Administration > Server Manager > Server Configuration > Network**. (#30286).

- You can now provide port information when you specify a server name at **Administration > External Servers > Endpoint Context Servers**. Port information should be provided in the format "hostname:port". (#30407)
- All references to HP are now renamed to HPE or Hewlett Packard Enterprise. (#30435, #30436, #30437, #31830)
- At **Configuration > Services > Reorder Services**, reordering is now easier: Simply click a service to select it, and then click again on the new position you want to move it to. (#30446)
- In previous versions of Policy Manager, users had to add or modify Admin access privileges by importing XML files. ClearPass Policy Manager 6.6 provides a way to modify Admin access privileges in Policy Manager and Insight via the WebUI. (#30449)
- All endpoints discovered on the network as part of profiling/network discovery are now added as Endpoint entries even if Profiler cannot fingerprint the device. (#30466)
- Several enhancements were made in the areas of advanced password policy options for the local user database. To use this feature, go to **Configuration > Identity > Local Users > Password Policy**. The following options are available: (#30514, #30515, #30529, #30530, #30531, #30533)
  - **Disable account if Date exceeds**: Local users are disabled at midnight when the current date exceeds the configured date.
  - **Disable account if Days exceed**: Local users are disabled when the specified number of days has passed since the account was enabled.
  - **Disable user account after n days if password is not changed**: The user's account is disabled if they do not change their password after the specified number of days.
  - **Password must be different from the previous n versions**: The number of previous passwords (including the default password) to compare to the new password the user enters. Values of 1 through 99 may be specified.
  - **Display reminder message after n days**: Number of days after which a reminder to change the password is displayed to the user. Values of 1 through 365 may be specified. This option is only for displaying the reminder; it does not include the new-password prompt. This option is applicable only for TACACS+ authentication.
  - **Check to force change password on next TACACS+ login**: The local user must change their password immediately after their next TACACS login. This option is available when you select an account in the list at **Configuration > Identity > Local Users**.
- Any changes to attributes on the Modify Endpoint Context Server form are now reflected automatically. (#30582)
- ClearPass 6.6 introduces a new feature that adds the ability to profile endpoints on the network based on open TCP ports. The list of TCP ports to be probed during endpoint profiling is controlled by a new cluster-wide parameter called **Profiler Scan Ports**. (#30844)
- All endpoints discovered from **Network Devices** with SNMP read enabled and via network discovery scan are now automatically added as endpoints with **Status=UNKNOWN**. (#30845)
- A new service parameter, **Connection Timeout**, was added under **Async Network Service** to control HTTP connection timeout scenarios when connecting to external servers in Generic HTTP Enforcement. (#30941)
- If location details from Insight are available, they are now displayed at **Configuration > Identity > Endpoints** on the **Endpoint** tab of the **Edit Endpoint** window. Location information includes the NAD and port values for wired devices, and the access point and network SSID for wireless devices. (#30992)

- The `tips_audit` table in the configuration database can now be accessed by the appexternal DB user. This table contains audit records for Policy Manager configuration changes. (#31229)
- The Aruba RADIUS dictionary was updated. (#31436)
- New field groups are added to Insight Logs for Posture. APT (Application posture token) is used as part of posture. Also a few fields have been removed from the Insight Logs authentication table and moved to the endpoints table. New field groups have been created exclusively for Posture-related details. The new field groups added to Insight Logs are as follows: (#31458)
  - Posture Summary
  - Posture Firewall Summary
  - Posture AntiVirus Summary
  - Posture Antispyware Summary
  - Posture DiskEncryption Summary
  - Posture Windows HotFixes Summary

  Migration is not supported from versions of ClearPass prior to 6.6 if the Posture-related fields are configured in Insight logs that were available in the authentication table.

Syslog filters with the old authentication columns configured from Insight logs are being disabled. Customers need to manually update the syslog filters to use the new endpoint column. Notifications to this effect are displayed in migration screens. Notifications are not displayed during the upgrade.

- Device name, device category, and device OS family profiling information can now be used with endpoint context servers. (#31596, #31608)

QuickConnect

The following new features are introduced in QuickConnect in the 6.6.0 release.

- The Windows QuickConnect client can now be configured to bypass the proxy server configured on the client during the Onboard enrollment process. The **Bypass Proxy** option is available at **Onboard > Deployment and Provisioning > Provisioning Settings > Onboard Client**. (#28015)

Issues Resolved in the 6.6.0 Release

The following issues have been fixed in the ClearPass 6.6.0 release.

This section includes the following:

CLI

Table 4: *CLI Issues Fixed in 6.6.0*

Bug ID	Description
#29929	Users should be aware that ClearPass no longer supports the following CLI commands: • service activate • service deactivate

Dissolvable Agent

Table 5: *Dissolvable Agent Issues Fixed in 6.6.0*

Bug ID	Description
#29513	The native dissolvable agent did not work properly on Chrome 42.x or higher, and the guest page failed to detect whether the ClearPass OnGuard Unified Agent was installed. The ClearPass OnGuard native dissolvable agent (WebAgent) is now supported on Chrome Browser 42 and higher versions.

Endpoint Context Servers

Table 6: *Endpoint Context Server Issues Fixed in 6.6.0*

Bug ID	Description
#27704	Endpoint attributes were not deleted if a device was reset in Aruba Activate. Endpoint attributes are now deleted from the ClearPass server when the corresponding attributes are deleted in the MDM context server.
#31242	Endpoints from MobileIron were not discovered if any of the attribute values were empty.

Guest

Table 7: *Guest Issues Fixed in 6.6.0*

Bug ID	Description
#18700	An out-of-date message could be displayed in the **List Accounts** view.
#27847	Corrected a potential Cross-Site Scripting (XSS) issue when using the `nwa_mdps_config` smarty function.
#28480	The SMS provider selection could not be overridden in a self-registration.
#28877	Corrected some issues with performance when there is a large number of accounts. Tag lookup performance is now greatly improved in guest management queries.
#28974	Corrected some issues with syntax checking for template scripts.
#29027	The application would hang if an overly restrictive password configuration was chosen.
#30154	Date pickers were not rendered correctly when using the Galleria skin.
#30304	Deleting a guest account sometimes took as long as five minutes. This was observed on a CP-HW-5K system after upgrading to 6.5, following an upgrade path of 6.1.4 > 6.2.6 > 6.5.2.

Table 7: *Guest Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#30840	The "Permit login on validation error - validation errors will be logged" option is now removed from **Security Hash** drop-down list on the **Configuration > Pages > Web Logins** form or the **Guest Self-Registrations > Advanced editor** form. If you had this option set, please re-save the configuration with a valid option.
#30842	Corrected some visual issues with the color picker controls that could occur with certain skins.
#31335	For Web logins configured to require a Universal Access Method (UAM) challenge, the challenge was not sent.
#31386	Forcing a default destination in a Cisco Wi-Fi environment did not redirect to the specified address.
#31450	The MAC address was not normalized during import. MAC devices imported into Guest now format the MAC to the system standard.
#31664	Emails were generated incorrectly of the No Skin option was configured. Users should be aware that emails sent with one of the No Skin options might not display correctly in all email clients.
#31745	With a Ruckus controller configured, Clearpass did not send the proper POST URL information to the client for captive portal authentication. Login configuration parameters for Ruckus Wireless have been adjusted.
#31934	Partial configuration backups could fail if not all selections were made in the list of items to back up.
#32292	Users should be aware that the default privileges for the **Help Desk** operator profile have been changed in this release. The **Manage Customization** and **Manage Print Templates** privileges are now set to **Read Only** instead of **Full**. System administrators should review their **Help Desk** operator profile and update the privileges accordingly.
#32735	The `_browser=1` URL parameter was not compatible with some social login providers. If you have configured social logins, please review any URL access control lists within the application configuration. URLs prior to ClearPass 6.6 required the `?_browser=1` parameter to be appended. That argument must now be removed.
#33071	HTTP User Agent profiling was not collected for Guest Web pages other than Web login pages. Guest Web pages now correctly populate attributes and record client profile information.
#33329	The PHP version is now updated to 5.6.19. This includes fixes for CVE-2015-3152, CVE-2015-2325, CVE-2015-2326, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2015-1351, and CVE-2015-1352.
#33650	When using XML-RPC, API responses were in the ISO-8859-1 character set instead of UTF-8. All XML-RPC responses are now encoded in UTF-8.

Insight

Table 8: *Insight Issues Fixed in 6.6.0*

Bug ID	Description
#30384	If there was a session timeout while logging in to Insight, the login failed and the message "Bad Request - The browser (or proxy) sent a request that this server could not understand" was displayed. Session timeouts now redirect the user to the login page to reauthenticate.
#31227	The disk usage displayed in Policy Manager at **Monitoring > System Monitor > Disk Usage** did not match the disk usage displayed in Insight at **System Monitor > Disk Usage**.
#32345	If an alert was configured with the time interval in hours, the alerts were not generated.
#32494	In OnGuard CSV reports that include Unicode characters, some characters might not be retained. Users should be aware that, in order to view all characters correctly, the CSV report must first be imported into Excel.
#32945	An Endpoints report failed and displayed error messages such as "Errors: 'ascii' codec can't decode byte 0xe2 in position 0: ordinal not in range(128).

Onboard

Table 9: *Onboard Issues Fixed in 6.6.0*

Bug ID	Description
#27590	A superfluous reconnect message was displayed when enrolling a Chromebook.
#28114	Filtering by username on the **View by Username** list view did not return any results. The filter is now modified to match any part of the username.
#28242	EC certificates did not work on Windows 7. The keyUsage Onboard generates for TLS Client certificates is now modified to improve compatibility, in particular for Windows 7 clients using EC key types.
#30907	Onboard logic is now altered to deal with Android 6 devices not providing their MAC address. Users should be aware that the MAC address is not provided by Android 6 and later devices. Instead, it must be provided in the captive portal redirect. When an Aruba controller is used, we strongly recommend that you enable the URL hash to prevent tampering.
#31041	The list of iOS trusted certificates in Onboard is updated.
#31387	Onboard was unable to re-connect iOS clients after provisioning on a subscriber node.

OnGuard

Table 10: *OnGuard Issues Fixed in 6.6.0*

Bug ID	Description
#31114	The ClearPass OnGuard Unified Agent stalled in "connecting" mode when the user was switched during a health check.
#31201	For Windows 8 clients, the ClearPass OnGuard Unified Agent was not able to read last scanned time for Symantec Hosted Endpoint Protection.
#31581	OnGuard WebAuth requests were not evenly distributed among cluster nodes if **OnGuard Load**

Table 10: *OnGuard Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
	Balancing was enabled in the **OnGuard Global Agent Settings**. Load balancing is now improved to more efficiently distribute OnGuard WebAuth Requests across the cluster.
#31619	On Mac OS X, the ClearPass OnGuard Unified Agent could not read the RTP status of ESET Cybersecurity 6.1.12.0.
#31993	The ClearPass OnGuard Unified Agent reported an incorrect status for the McAfee Host Intrusion Prevention Firewall.
#32024	The ClearPass OnGuard Unified Agent did not perform health checks if there were new-line characters in the **Override Server IPs** field.
#33388	The ClearPass OnGuard Unified Agent sometimes categorized the **Aruba Virtual Adapter #2** network adapter as **OTHER** instead of **VPN**.

Policy Manager

Table 11: *Policy Manager Issues Fixed in 6.6.0*

Bug ID	Description
#21593	Corrected an issue where a customer's ClearPass server was using port 4949 and port 8443. All access to TCP ports 4949 and 8443 is now blocked.
#23923	Bulk deletion of endpoints from the user interface might have resulted in inconsistencies between endpoint-related tables. Now when 50 or more endpoint profiles are deleted at one time, the profile attributes for these endpoints are retained in the Profile table. Retention of these profile attributes does not interfere with authentication.
#27363	If the default role-mapping policy [Guest Roles] was renamed, the guest roles in ClearPass Guest were not populated. Now a name change is not allowed in the **> Policy Name** field on the **Policy** tab at **Policy Manager > Configuration > Identity > Role Mappings > [Guest Roles]**.
#27737	Session Restriction Enforcement was not converted to Session Notification if Session check User name was configured.
#27800	The value for the endpoint status was not displayed in Insight reports if the status was changed using POST Auth enforcement. Endpoint status change operations through Post Authentication enforcement are now propagated to Insight.
#27885	The **Administration > Server Manager > Licensing** page continued to display a message that the Onboard license count had been exceeded even after the actual license count was reduced to within limits.
#27908	When upgrading from 6.4.0 or 6.4.1 through the CLI, you had to first download and install a 6.4.0 CLI updates patch and then update to 6.4.2 or later before upgrading to 6.6.
#27922	In some upgrade cases, the services did not come up properly on subscriber nodes, resulting in Webauth/TACACS Authentication failures, and the **Access Tracker > Session Details** form showed the internal error message "Failed to authenticate user".
#28049	The RADIUS server's authentication and accounting ports could not be changed. The ClearPass RADIUS server's authentication port and accounting port can now be set to custom values. To use this option, go to **Administration > Server Manager > Server Configuration**, click the **Service Parameters** tab, and select the **RADIUS Server** service.

Table 11: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#28457	OCSP checks are now supported when using smartcard certificates for 802.1X authentication.
#28693	When zones were created with certain special characters, the CPU Usage and CPU Load graphs were not displayed on the **Monitoring > Live Monitoring > System Monitor** page. Users should be aware that only the following special characters are allowed in zone names: - . { } [ ] ( ) and spaces. Do not use the following unsupported characters in zone names: ` ~ ! @ # $ % ^ & * + = \ | " ' < > , ? /
#28743	An excessive number of account lockouts occurred for users authenticating against Active Directory after changing their password. ClearPass now always uses the **Name** field value from the EAP MSCHAPv2 packet to calculate the challenge. The RADIUS service parameter **Re-attempt AD login with different Username formats** has also been removed.
#28787	No information was displayed for VPN clients on the **Accounting Record Details** form at **Monitoring > Live Monitoring > Accounting**.
#28991	Endpoint context server updates failed after Palo Alto Networks firewall was upgraded to PAN-OS 7.0.
#29038	The “Subject-serialNumber” attribute could not be used in the LDAP filter for authorization. The “Subject-serialNumber” attribute is now incorporated into the certificate namespace.
#29169	A RADIUS service failure occurred when using the ClearPass Upgrade Tool. During the domain join operation or domain service start-up after the upgrade process, if the Alt Name or Domain SID is null, ClearPass will ignore them and proceed with the domain join and service start.
#29196	RADIUS CoA could not be done if the machine and user authentication were configured in HP switches.
#29464	Changing the appadmin password in Post Auth Enforcement Profile checks caused disconnect failures via RADIUS Change of Authorization (CoA).
#29662	The OpenSSL version is now upgraded to 1.0.1p. This includes fixes for CVE-2015-1793.
#29876	The Curl version is now upgraded to 7.19.7-46.1. This includes Curl bug fixes and enhancements, and fixes for CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, and CVE-2015-3148.
#29914	Corrected an issue where performing Guest application authentication against the Active Directory failed.
#30075	On the **Monitoring > Live Monitoring > OnGuard Activity** page, the online/offline **Status** sort option did not work.
#30221	Installing a patch update might fail if the boot partition did not meet the free space requirements required by the update.
#30280	When using the DHCP SPAN port, ClearPass Profiler was unable to profile devices if the spn packets had an 802.1q header.
#30293	Role mapping failed after updating from 6.5.0 to 6.5.2 for devices enrolled in JAMF, making clients unable to connect. This was caused by endpoint update issues from JAMF if one of the endpoints had an empty attribute value.
#30318	A RADIUS server authentication source failed with Aruba Application service types. A validation error is now displayed if a RADIUS Server authentication source is part of a non-RADIUS-based service.
#30444	Under **Administration > Dictionaries > Attributes**, attributes of different entity types but using the

Table 11: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
	same name could not be imported.
#30510	ClearPass user interface displayed the error message "No licenses configured", and the "`system refresh-license`" command had to be entered in the CLI to correct it.
#30556	At **Administration > Server Manager > Server Configuration**, DNS information was not saved after editing.
#30564	CoA and Profiling API access is now restricted to Administrator and API Administrator accounts.
#30595	Adding new devices to in the **Configuration > Network > Device Groups** list caused existing devices to be deleted.
#30641	ClearPass now supports migration of multi-value non-string attributes.
#30731	The Endpoint Profiler table and pie chart did not update with the correct values if the user selected the **Choose View** option.
#30984	Guest account attributes could have been overwritten when using the **expired_notify_status** field.
#30995	Updating information in Insight failed if a cluster password was configured with 20 or more characters.
#31111	It was sometimes necessary to clear the router ARP entry in order for VIP to work correctly after a network flap.
#31126	The ClearPass server failed to fetch endpoint attributes for random user authentications.
#31202	The publisher database was left in an inconsistent state after a subscriber attempted a promote operation. This occurred when the switch to publisher API call as part of a promote publisher operation failed.
#31247	The JQuery version is now upgraded to 1.11.1.
#31277	Corrected an issue where the ClearPass RADIUS server stopped responding. Information-level logs are now included that print the number of requests in the processing tree in order to determine configuration reloading time.
#31291	On the **Administration > Server Manager > Server Configuration > Service Parameters** tab, the default values did not match the parameter values. The values are now set to the same as the default values for each hardware platform.
#31534	Access was not restricted to some pages of the admin UI. Support is now added to control API URLs. This includes: • A new resource, "ClearPass API," was added at **Server Configuration > node > Network > Application Access Control**. • By default, access to /api* urls is allowed for all IP addresses. • Users can modify the setting to allow or deny additional IP addresses.
#31661	NAD clients were sometimes removed from the NAD group.
#31673	Corrected an issue where a SQL Injection attack could occur on callback URL for a Google MDM Connector.
#31953	When the subscribers were not reachable, parallel execution of the cron job to check whether the standby had failed over caused an out-of-memory condition on the publisher.

Table 11: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#31968	Under certain traffic loads, the internal communications between various processes used with TACACS+ authentication could get overwhelmed, which would cause sporadic authentication failures. This issue was not seen in bursts of requests, only in long, sustained requests.
#32002	The output/input bytes calculation was incorrect if the number of output/input bytes was more than 2^32-1. The Acct-Output-Gigawords/Acct-Input-Gigawords attribute value is now included in the input/outputs bytes calculation in the Dashboard utilization tab and insight.
#32007	If guest usernames were created using both uppercase and lowercase characters, the guest's expiration time was not updated via Post Auth.
#32028	SNMP alerts were issued from all the nodes if a change was made on any one node of the cluster. System monitoring configuration updates are now specific to the local node.
#32130	Users should be aware that the following two pages are deprecated from the user interface: **Configuration > Posture > Posture Servers** and **Administration > Dictionaries > Posture**.
#32201	The Apache Commons Collections .jar file is now updated to version 3.2.2.
#32599	Corrected an issue where Insight NetEvents without accounting session IDs created an unnecessary load on an appliance.
#32617	Some subscribers in a cluster displayed the error message "Certificate verifications against this CA will fail till the CRL is updated or removed" before the scheduled update time. The calculation for the check to download the new CRL file is updated to the current time plus 16 minutes, allowing the script to run and download new files every 15 minutes without encountering a CRL expiry error.
#32621	Multiple instances of the AppsUpdater script could run simultaneously, generating a high CPU load.
#32656	When using TACACS, the "change password" prompt was displayed even though the username field was empty.
#32604	Cluster operations were blocked by certificate revocation list (CRL) updates running in the background.
#32678	Users should be aware that, on the Internet Explorer 11 browser, graphs and charts are best viewed in the Edge document mode.
#32787	On the Chrome 48.x browser, adding an enforcement profile at **Configuration > Enforcement > Policies** also added a null enforcement profile.
#33003	Corrected an issue where the RADIUS server could crash when processing badly formatted usernames.
#33025	One of the nodes of a cluster failed to upgrade from 6.3.4 to 6.5.0. During system upgrade, under rare circumstances `route-eth*` was empty, causing the upgrade process to fail. Fixed the system upgrade issue to any empty `route-eth*` and `rule-eth*` files for IPv4 and IPv6 in the current partition.
#33031	If the domain Fully-Qualified Domain Name (FQDN) was provided instead of the DC FQDN, the attempt to join the domain failed with the error message, "<name> failed to join the domain <DOMAIN NAME> with domain controller as <domain name>". The ad netjoin command is now enhanced to include a detailed description for the domain controller FQDN input field.
#33042	Users were denied ClearPass admin access due to a space between the IP address and subnet mask, which resulted in an invalid host name. Validations have been added for IP address and subnet mask entries on the Application Access Control screen to check for spaces in the host name, which can

Table 11: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
	prevent users from gaining ClearPass admin access.
#33084	glibc is now updated to the latest version. This includes fixes for CVE-2015-7547 in relation to the glibc stack-based buffer overflow in getaddrinfo().
#33098	After upgrading to 6.5.5, the error message “Error in processing request. Please retry” was displayed because of an incompatible certificate.
#33138	The RADIUS Change of Authorization (CoA) could not be sent if the IP range was given in the Network Device.
#33145	An authentication error occurred if an IP address value at **Configuration > Network > Devices** was configured in IP/32 format (for example, 192.168.1.1/32).
#33190	The **OnGuard Clients Summary** widget on the Policy Manager **Dashboard** displayed incorrect data when endpoint attributes were updated manually.
#33748	Users should be aware that ESX 4.x is not supported.

New Known Issues in the 6.6.0 Release

The following known issues were identified in the ClearPass 6.6.0 release.

This section includes the following:

Cluster Upgrade and Update

Table 12: *Cluster Upgrade and Update Known Issues in 6.6.0*

Bug ID	Description
#29710	**Symptom:** Upgrading with the Cluster Upgrade Tool fails if the cluster password includes special characters such as the "at" symbol (@), colon (:), or slash (/). **Scenario:** This occurs on all versions of the Cluster Upgrade Tool. **Workaround:** Before installing the upgrade patch, if the cluster password contains special characters, please change it temporarily to only use alpha-numeric characters (letters and numbers). The cluster password can be changed back to the old password after the cluster upgrade completes.
#33668	Users should be aware that, when performing upgrades with the Upgrade Tool, there are some limitations regarding identification of cluster node status. • If a cluster node goes out of sync or is dropped during upgrade, migration, or a cluster join operation, the Cluster Upgrade Tool cannot detect the status of that node. After the cause of the failure is identified, the failed node must be manually rejoined to the cluster. • If any nodes in the cluster are out of sync or force-dropped before the upgrade is started, the Cluster Upgrade Tool cannot detect the status of those nodes. Before starting the upgrade, confirm that all nodes are in proper sync. • During a cluster add or rejoin operation, failure alerts might be displayed if the Cluster Upgrade Tool installs dependent patches before the cluster operation is complete. The upgrades can be initiated through the Cluster Upgrade Tool when the nodes are back in proper sync.
#33669	Users should be aware that there are some Cluster Update Tool scenarios where view, logs, or status update information is not shown. These do not affect functionality. • If a patch update (either a point patch or a cumulative patch) requires an admin-server or async-netd service restart, the INFO logs information on the **Update** tab might be incomplete. • If a patch is updated through the Software Updates portal instead of through the Cluster Updates interface, no status or installation log information is displayed for it in the Cluster Update interface. The **Start Update** option is also still shown for that node, unless there is a manual admin-server restart, or unless there is a cluster operation that triggers a status check of installed patches. • If a node is dropped from the cluster or rejoined to the cluster, the Update Status, View Logs, and Last Step information is cleared for that node.
#33670	Users should be aware that, in cluster setups, skin updates cannot be done in batches. Skin updates must either be done for all the cluster nodes at once, or be manually done on each node.

Dissolvable Agent

Table 13: *Dissolvable Agent Known Issues in 6.6.0*

Bug ID	Description
#29609	**Symptom/Scenario:** The ClearPass OnGuard Native Dissolvable Agent for Mac OS X does not support status checks for the "Software Updates" patch management application.
#32664	**Symptom:** The Native Dissolvable Agent is not supported on the Microsoft Edge browser. **Scenario:** The Microsoft Edge browser is not able to detect whether the Native Dissolvable Agent is installed or not, and displays a message to download the agent even if the agent is already installed. **Workaround:** Use the Firefox, Chrome, or Internet Explorer browsers instead.

Endpoint Context Servers

Table 14: *Endpoint Context Server Known Issues in 6.6.0*

Bug ID	Description
#33779	**Symptom/Scenario:** If the **Enable to validate the server certificate** option is enabled for an MDM device and then ClearPass is upgraded to 6.6.0, MDM discovery fails. **Workaround:** Re-enter the password, or enable/disable the certificate in the trust list.

Guest

Table 15: *Guest Known Issues in 6.6.0*

Bug ID	Description
#33620	**Symptom:** A room page was not created when the transaction processor was changed from non-PMS to PMS. **Scenario:** Self-registrations configured to interact with FIAS-based hotel PMS systems might show a blank white page when launched. **Workaround:** Re-save the self-registration to resolve the problem.

Insight

Table 16: *Insight Known Issues in 6.6.0*

Bug ID	Description
#31048	**Symptom/Scenario:** When the Internet Explorer browser is refreshed, icons on the Insight Dashboard are displayed as text. **Workaround:** Navigate to any other other page in Insight and then come back to the Dashboard page.
#32276	**Symptom/Scenario:** The secure flag is not set for Insight sessions.
#32316	**Symptom/Scenario:** Users should be aware that posture data in the Insight database from Insight versions earlier than 6.6 cannot be migrated due to database changes.
#32317	**Symptom/Scenario:** Users should be aware that report configurations from Insight versions earlier than 6.6 are not carried forward after migration or upgrade.
#32318	**Symptom/Scenario:** Users should be aware that alerts configurations from Insight versions earlier than 6.6 are not carried forward after migration or upgrade.
#32430	**Symptom:** There is a discrepancy between the data shown in some of the Insight Dashboard's widgets and the data displayed in reports and other widgets. **Scenario:** If the time zone is changed, Insight graphs in hourly widgets might show discrepancies for data from the past 24 hours. For example, the **Authentication Trend** widget might show only six entries while the **Access Tracker** correctly shows seven entries for the same date and the **Auth Overview** report shows the proper data and trend.
#32455	**Symptom/Scenario:** Graphs in the PDF report do not expand over the entire width of the PDF.
#32624	If the report period is more than one month, the PDF report does not show the X,Y data table below the graphs.

Table 16: *Insight Known Issues in 6.6.0 (Continued)*

Bug ID	Description
#32786	Users should be aware that, in order to generate reports and alerts, one of the Insight nodes must be enabled as the Insight master. This is configured in Policy Manager at **Administration > Server Manager > Server Configuration** on the **System** tab.
#32901	Users should be aware that the RADIUS Accounting ID must be unique in Insight.
#33178 #33183	Users should be aware that, in Insight reports, filter entities such as Auth Service and Auth Source are fetched from tipsDB, and only the latest name in the database will be fetched in the prepopulated field for the selection. This means that if a service name or source name has been changed, only the latest name will be fetched, so reports can only be configured with those latest changes. All previously stored names will be discarded.
#33208	**Symptom/Scenario:** In a setup with a loaded insightDb, Search does not give an autocompletion-based search. **Workaround:** The user must provide a full phrase to search and then select the appropriate category from the drop-down list.
#33227	Users should be aware that, if SFTP is configured in Insight and the SFTP server is a Windows server, the remote directory must be provided with the relative path and not the absolute path. If the SFTP/SCP server is on Linux, however, the absolute path must be provided.
#33243	**Symptom/Scenario:** SCP for reports does not work when configured for an SCP server in Windows; however, SFTP does work for Windows.
#33244	**Symptom/Scenario:** Generated reports displayed in the Calendar widget are not available to view or download if the Insight Master is switched.
#33245	**Symptom:** Reports, alerts and admin settings can only be configured using the Insight master. **Scenario:** In a cluster of nodes with multiple nodes enabled with Insight, the Insight master is the only node allowed to configure reports, alerts, and admin settings. On the Insight slave nodes, only the Dashboard page is available to view.
#33255	**Symptom/Scenario:** In the **Auth Trend** report, the guest authentication counts shown for certain days in the **1 month** section do not match the authentication counts shown for the same days in the **1 week** section. Users should be aware that the report widgets' x-axis range is for the report date range that was configured, but some of the widgets will not contain data for the entire date range.
#33265	Users should be aware that Insight only supports the English language.
#33448	**Symptom/Scenario:** An Insight report might be aborted due to timeout if all the available columns are selected for CSV export when the Insight database has millions of records.
#33582	**Symptom:** Deselecting **Notify by Email** or **Notify by SMS** check box is not saved. **Scenario:** On reports and alerts, if a **Notify by Email** or **Notify by SMS** check box is deselected, saving appears to work but the check boxes are still selected when the report is reopened. **Workaround:** To remove the notification settings, first deselect the check box, and then clear the associated notification text field. Save the report or alert.
#33608	**Symptom/Scenario:** In the Insight Dashboard, hovering the mouse pointer over a MAC address in a widget visibly changes the pointer to a click pointer, but no action occurs if the pointer is clicked.
#33657	**Symptom/Scenario:** The Insight Dashboard display becomes blank after it had been displaying items correctly (0 total auth, no authentication trend, failed auth, endpoints etc). This occurs even though it is receiving RADIUS and guest traffic.

Table 16: *Insight Known Issues in 6.6.0 (Continued)*

Bug ID	Description
#33770	**Symptom/Scenario:** Endpoint reports will be empty if they are generated soon after upgrading or migrating from versions lower than 6.6. This report is generated properly only after the corresponding endpoints are authenticated in the 6.6.0 version.
#33771	**Symptom/Scenario:** Insight reports that use custom templates and and their corresponding generated reports are not carried forward from versions lower than 6.6.0.
#33776	**Symptom/Scenario:** A delay in the WAN or network latency might cause problems with the way the Insight page layout is displayed.
#33825	**Symptom/Scenario:** Guest MAC/Device Authentication is not reflected on the **Guest Authentication Trend** graph. **Workaround:** The information is available in the **Authentication Trend Graph**.
#34097	**Symptom:** Users with the Super Administrator privilege cannot log in directly to Insight with their AD credentials. **Scenario:** When configuring Insight access for a Super Administrator profile at **ClearPass Guest > Administration > Operator Logins > Profiles > Edit Operator Profile**, the profile is not updated with the proper privilege level if the **Full Access** option is selected. **Workaround:** Select the **Custom** option in the **Access > Insight** section and provide the privilege levels manually.

Onboard

Table 17: *Onboard Known Issues in 6.6.0*

Bug ID	Description
#33822	**Symptom:** Onboard enrollment fails if a device limit is set. **Scenario:** Attempting to enroll a device when a device limit is configured in Provisioning Settings fails with the error "Fatal Application Error: Call to undefined method...." **Workaround:** If you use this functionality, postpone upgrading to 6.6.0 until the next patch is available.

OnGuard

Table 18: *OnGuard Known Issues in 6.6.0*

Bug ID	Description
#29613	**Symptom:** The **Disable USB Mass Storage Device** auto-remediation action is not supported on Windows 64-bit operating systems. **Scenario:** If **Disable USB Mass Storage devices** is selected as the auto-remediation action in the **USB Devices** health class, the ClearPass OnGuard Unified Agent does not disable USB mass storage devices on Windows 64-bit operating systems. The message "Failed to disconnect following USB mass storage devices.... Please remove manually" is displayed to end users on those 64-bit systems. **Workaround:** None.
#31893	**Symptom/Scenario:** Although Windows 10 does not support the Network Access Protection (NAP) platform, Windows 10 is still listed in the **Windows System Health Validator** and **Windows Security Health Validator** plugins for OnGuard at **Configuration > Posture > Posture Policies > Posture Plugins** tab.
#33332	**Symptom:** The Java Dissolvable Agent guest portal page hangs.

Table 18: *OnGuard Known Issues in 6.6.0 (Continued)*

Bug ID	Description
	Scenario: This occurs when the user clicks **Continue** on the **Security Warning** dialog after installing or upgrading to JRE 8u73. This is not an issue with current Java versions. **Workaround:** Upgrade to the latest JRE version.
#33532	**Symptom/Scenario:** When the ClearPass OnGuard Agent for Windows is running in **Service** mode, the **Retry** button is sometimes disabled and an incorrect system tray icon is shown. **Workaround:** Quit OnGuard and relaunch it.

Policy Manager

Table 19: *Policy Manager Known Issues in 6.6.0*

Bug ID	Description
#24584	**Symptom:** The Event Viewer sometimes shows two SMS entries. **Scenario:** This might occur when “Alert Notification - SMS Address” is saved, or if sending an SMS fails.
#28417	**Symptom:** After DNS settings are changed, services that are dependent on DNS are not restarted and the ClearPass application hangs. **Scenario:** When the DNS is updated, all services are restarted, so the session is lost. **Workaround:** Refresh the ClearPass application and log in again.
#30486	**Symptom:** Custom filters in an Auth Source do not work after upgrading to ClearPass 6.6. **Scenario:** As part of enhancements to tag mappings, the schema for storing the tag values has changed, and all default filters were migrated to the new schema. It is not possible, however, to automate the migration of custom filters. **Workaround:** If you have custom filters, contact Support to have the custom filters migrated to the new schema.
#30569	**Symptom/Scenario:** The Guest Portal name in the ClearPass portal is unchanged after updating the name in the ClearPass Guest application. **Workaround:** When you change Guest Portal names in the ClearPass Guest application, the admin must manually update the ClearPass Portal settings if the guest portal is used in that configuration.
#30968	Users should be aware that VMWare ESX hosts are not profiled by SNMP CDP based profiling. The Profiler needs a host MAC or IP address in order to identify the device. ESX servers might not report the management IP address and MAC address in the CDP announcements, causing the Profiler to ignore neighbor CDP information for the host.
#31208	**Symptom:** Multiple entries for the same device can be seen in the endpoints page. **Scenario:** Users should be aware that, during the network discovery scan, if devices have multiple endpoints those endpoints will be listed separately in the endpoints page.
#31810 #30785	Users should be aware that, when upgrading to ClearPass 6.6, any custom authentication source filters must be migrated manually. During an upgrade, the console now displays a warning message when custom filters are defined using tag values for Local and SQL authentication sources.
#31942	**Symptom:** Restore operations fail and the error message “Network Device <#>: No dictionary found for vendor ‘HP’” is displayed at **Configuration > Network > Devices > Import**. **Scenario:** This occurs when a network device is imported with the vendorName as “HP”. **Workaround:** Network devices that had the vendorName "HP" must now use the vendorName "Hewlett-Packard-Enterprise".
#32088	**Symptom:** Seed devices are not updated in the tips_endpoints table. **Scenario:** Network discovery sometimes does not add some devices to the endpoints table if they do not return a MAC address. The Aruba switch does not implement ipAddrTable, so it cannot determine the

Table 19: *Policy Manager Known Issues in 6.6.0 (Continued)*

Bug ID	Description
	MAC address.
#32145	**Symptom:** Devices are discovered with incorrect MAC addresses. **Scenario:** Network discovery reads the ARP cache (ipNetToMediaTable) to process all the MAC-IP cache pairs and add them to the endpoints. The Aruba switch returns the same MAC address for all the IPs, resulting in only one endpoint.
#32759	**Symptom/Scenario:** A bulk import of Network Access Devices (1000+) can take a long time for a backend process to complete despite the user interface indicating it has completed. This may impact authentication of these new Network Access Devices. **Workaround:** Contact Aruba Support for assistance with this scenario.
#32777	**Symptom:** The OpenVAS tool incorrectly reports high-severity vulnerabilities. **Scenario:** During testing on a ClearPass 6.5.5 system, the OpenVAS tool reports two high-severity vulnerabilities regarding the Format string URI. These are false positives and can be ignored. Functionality is not affected and all ClearPass URLs are correctly handled.
#32916	**Symptom:** Network discovery adds multiple ports to the display after discovering the same device. **Scenario:** During network discovery, if the same device is connected to two different ports of a switch, the one discovered later will be displayed in the neighbors.
#32980	Users should be aware that, on devices using PAP, notifications sent by ClearPass about a required password change or advising of an upcoming password expiration might not work. Although TACACS `authen_type=ASCII` implementations handle these correctly, devices that use `authen_type=PAP` might only accept a status of `SUCCESS/FAILURE` and not accept any other status.
#33103	**Symptom:** After restoring a backup, the SSO page IDP URL still shows the old hostname of the restored backup instead of the hostname/FQDN if the current ClearPass server. **Scenario:** This error is only seen when a backup is attempted from one server to another server. This is very rare in real time. **Workaround:** Manually change the hostname in the IDP URL to the current ClearPass server's hostname\FQDN.
#33312	**Symptom/Scenario:** If authentication latency to Active Directory is greater than 30 ms, a specific process thread used by the TACACS service to internally communicate with the authentication service might get overwhelmed using the default static value. **Workaround:** Contact Aruba Support who can resolve this issue for you by increasing the value as needed.
#33371	**Symptom/Scenario:** Network Discovery through SNMP v1 does not work for Aruba switches. **Workaround:** Use SNMPv2 or v3 for discovering Aruba switches.
#33535	**Symptom:** Importing patches might fail with the error "Content-type 'application/x-macbase64' is not supported". **Scenario:** This occurs on some versions of the Firefox browser. **Workaround:** Use the Chrome or Internet Explorer browser instead.
#33551	**Symptom/Scenario:** The RADIUS service stops if a 24th authentication source is added to a service using a static host list.
#33795	**Symptom/Scenario:** Importing a pre-existing authentication source with custom filter queries is not reflected or updated if the existing authentication source in 6.6.0 already includes some filters with same name.
#33811	**Symptom:** During an upgrade through the user interface, the **Reboot** button might not trigger a machine restart after the image is installed.

Table 19: *Policy Manager Known Issues in 6.6.0 (Continued)*

Bug ID	Description
	Scenario: This occurs when the upgrade image is downloaded from the Web server or installed through the user interface. If the default or configured idle session timeout of the server is exceeded, the system should display the error message "Session is timed out. Please log in again" when the **Install** or the **Reboot** button is clicked, but it does not. Instead, the installation completes and the "Reboot initiated" message is displayed, but the reboot is not actually triggered. **Workaround:** Refresh the page to log in again, and then click **Reboot**.
#33928 #33958 #34021 #34243	There are vulnerability issues in the 6.6.0 release regarding CVE-2016-2118, CVE-2016-2034, and CVE-2016-2107. For full details and patch availability, please refer to the advisory at http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2016-009.txt.
#34086	**Symptom:** If a system is upgraded from ClearPass 6.5.5 or below with a configuration that is affected by issue #33036, the configuration will not be auto-corrected during the upgrade. **Scenario:** This can occur if an authentication source with type RADIUS server is used in a service created through a service template in 6.5.5 or below.
#34338	**Symptom:** After upgrading to ClearPass 6.6.0, some custom admin privileges do not work and ClearPass screens are blank for users with the custom admin privileges. **Scenario:** Custom admin privileges that include the **Monitoring > Live Monitoring > Endpoint Profiler** attribute (mon.li.ep) will not work after upgrading to ClearPass 6.6.0. The **Endpoint Profiler** attribute is now under **Monitoring > Profiler and Discovery**. Until all custom privileges that use the mon.li.ep attribute are updated, admins using other privilege levels will also be affected. **Workaround:** 1. Go to **Administration > Users and Privileges > Admin Privileges** and click the row of the administrator role to edit. The **Edit Admin Privileges** window opens. 2. On the **Policy Manager** tab, expand each of the custom admin privileges and assign them as needed. 3. When the assignments are complete, click **Save** to update the privileges. 4. Confirm the updates by logging in as each of the administrator roles.
#34981	**Symptom/Scenario:** The configuration database uses date and time in the UTC (GMT) time zone instead of using the system's configured time zone, and the date and time are also displayed in UTC in the **Time Source** authentication source and external SQL queries. In ClearPass 6.5 and earlier versions, the date and time reflected the system's configured time zone. **Workaround:** If you wish to display the local time zone, you must manually configure it. Use the "set time zone" parameter explicitly in SQL queries wherever UTC (GMT) time is shown, especially in external SQL queries or additional SQL queries on authentication sources.

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 ClearPass 6.6.0 release, see the What's New in This Release chapter.

This chapter includes:

Dissolvable Agent

Table 20: *Known Issues in the Dissolvable Agent*

Bug ID	Description
#7165	To have health data collection work correctly in 64-bit Windows 7, please use the JRE version provided by ClearPass. 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 or 8 installed. **Workaround:** The Java plugin is now deprecated in Chrome 42.x and above. This is an issue with Chrome, not with ClearPass. Use the Firefox, Internet Explorer, or Safari browser.
#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 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. To enable this, go to **Safari > Preferences > Security > Manage Website Settings > Java > [Select IP/hostname of ClearPass server]**, and 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..."

Table 20: *Known Issues in the Dissolvable Agent (Continued)*

Bug ID	Description
	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 Mac OS X, 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.
#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:** The 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:** The Native Dissolvable Agent uses ActiveX on IE on Windows OS. Based on IE Security Settings, the browser may ask the user to run or allow "ClearPass OnGuard Web Agent Control". **Workaround:** For the Native Dissolvable Agent to work properly on Internet Explorer, the user should allow "ClearPass OnGuard Web Agent Control" ActiveX Control to run.
#27117	**Symptom:** On Mac OS X, the Native Dissolvable Agent might not work properly on Google Chrome or Firefox if Avast Mac Security 2015 Antivirus is installed.
#27756	**Symptom/Scenario:** The Native Dissolvable Agent can not be installed on Mac OS X 10.6. **Workaround:** On Mac OS X 10.6, admin/root permission is required to install the Native Dissolvable Agent. After installation, the admin user should execute the following command: `sudo chmod –R 777 ~/Library/Application\ Support/ClearPassOnGuardWebAgent/`
#28398	**Symptom:** The native dissolvable agent does not automatically relaunch the applet. **Scenario:** This can occur on Mac OS or on Ubuntu after upgrading from 6.5.0 to 6.5.1.
#29127	**Symptom:** The OnGuard Java-based Dissolvable Agent is not supported on the Chrome 42.x or higher browser. **Scenario:** The Java plugin is now deprecated in Chrome. This is an issue with Chrome, not with ClearPass. **Workaround:** Use the Firefox, Internet Explorer, or Safari browser.
#29186	**Symptom/Scenario:** The Native Dissolvable Agent sometimes does not run on Windows Vista, Windows 2008r2, or Windows 8. **Workaround:** Right-click the OnGuard application to open **Properties**, and then unblock the .exe file.

Guest

Table 21: *Known Issues in Guest*

Bug ID	Description
#9967	**Symptom/Scenario:** 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.
#25137	Please review your operator privileges for new features that may need to be enabled.

Insight

Table 22: *Known Issues in Insight*

Bug ID	Description
#12159	**Symptom/Scenario:** Insight reports do not show license changes immediately. The changes might take up to 24 hours, depending on when the changes are made.

Onboard

Table 23: *Known Issues in Onboard*

Bug ID	Description
#9897	**Symptom:** ClearPass Onboard does not update the Policy Manager endpoints table with an endpoint record when provisioning an iOS 5 device. **Scenario:** This is because the iOS 5 device does not report its MAC address to ClearPass Onboard during device provisioning.
#10667	**Symptom/Scenario:** 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. **Workaround:** The process to provision an OS X system with a system profile is: 1. The administrator should log in to the OS X system and connect to the provisioning SSID. Do not select the “Remember this network” option. 2. Use Onboard to provision the device with an EAP-TLS profile, ignoring the username/password prompt. 3. Connect to the provisioned network, selecting EAP-TLS as the mode and selecting the provisioned certificate, but ignoring the username field. 4. When the system connects and authorizes to the network, use Network Preferences to place the EAP-TLS network first in the priority list. 5. 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.

Table 23: *Known Issues in Onboard (Continued)*

Bug ID	Description
	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.
#23699	**Symptom:** Mac OS X disconnects before it completes a certificate renewal. **Scenario:** On Mac OS X, automatic certificate renewal through the "Update" option on Apple's interface does not work. This occurs on provisioned (wireless) networks. **Workaround:** This is an issue with OS X limitations, and is not an Onboard issue. Users should be aware that when their certificate is about to expire, they should renew the certificate through Onboard instead of using Apple's automatic certificate renewal.
#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 24: *Known Issues in OnGuard*

Bug ID	Description
#12342	The OnGuard agent fails to collect health on Windows 8 if VMware Server 2.0.2.X is installed.
#13164	**Symptom:** The hardware installation pop-up dialog appears to stop installing the ClearPass OnGuard Unified Agent for VIA+OnGuard mode. A warning message similar to "The software you are installing... has not passed Windows Logo testing" might be displayed during installation. **Scenario:** This might occur during the installation of the ClearPass OnGuard Unified Agent on WinXP and Windows 2003 SP2. **Workaround:** Users should click **Continue Anyway** to proceed.
#13363	**Symptom:** On Mac OS X, 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 X. It does not occur on Windows OS.
#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.

Table 24: *Known Issues in OnGuard (Continued)*

Bug ID	Description
#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 OnGuard Agent for Mac OS X 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 ClearPass server from a wired interface if the VPN is connected from a trusted network.
#14842	Installing the ClearPass OnGuard Unified Agent removes an existing VIA installation. To continue to use VPN functionality, go to **Administration > Agents and Software Updates > OnGuard Settings** and select **Install and enable Aruba VPN component** from the drop-down list.
#14996	If McAfee VE is running on Windows XP, the ClearPass OnGuard Unified Agent VPN will not work.
#15072	VIA connection profile details are not carried forward after upgrading 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 OS X 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 X. **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

Table 24: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	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.
#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 X for non-administrative users. **Workaround:** The user must have root privileges to start process-level health checks by OnGuard on Mac OS X.
#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.
#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.
#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 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.
#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.
#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".
#27134	**Symptom:** OnGuard does not support dynamic switching between logged-in users on an Ubuntu client.
#27572	**Symptom:** If the ClearPass OnGuard Unified Agent uses a VIA connection and is installed on a Mac OS X client, and if the user is idle for five minutes, OnGuard automatically disconnects the VIA tunnel.

Table 24: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	Workaround: If VIA is disconnected, connect again manually.
#27599	**Symptom:** The OnGuard logo is not shown on the desktop on Ubuntu. **Scenario:** On the Ubuntu OS, the OnGuard logo is not visible on the desktop at first. The logo will be updated automatically after the desktop is refreshed.
#27602	**Symptom**: The OnGuard Unified Agent fails to return health-check data over a VPN tunnel when the agent is installed on a client running MAC OSX 10.10 and using the Kaspersky AntiVirus software. **Workaround:** OnGuard services should be whitelisted on Kaspersky AntiVirus in order to work over VPN.
#27876	Users should be aware that RADIUS CoA over VPN is not supported on Ubuntu.
#29243	**Symptom:** The Unified Agent fails to disable other types of network connections when "Allow Only One Network Connection" is selected. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent for Windows does not support disabling USB data card/modem type network interfaces.
#29598	**Symptom:** OnGuard does not stop or pause VM Player 7.x virtual machines. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent does not support auto-remediation for Guest VMs running on VMware Player.
#30106	**Symptom:** On Mac OS X, the native and Java dissolvable agents do not get the RTP status of ESET Cyber Security Antivirus 6.x. **Scenario:** Users should be aware that the ClearPass OnGuard Native Dissolvable Agent for Mac OS X does not support the RTP Status check for ESET CyberSecurity and ESET NOD32 Antivirus.
#30243 #30212	**Symptom:** The ClearPass OnGuard Unified Agent fails to load on Windows Server 2003, and does not support VPN, Auto Upgrade, or SSO on Windows XP or Windows Server 2003. **Scenario:** Users should be aware that Microsoft stopped supporting Windows Server 2003 on July 14, 2015, and stopped supporting Windows XP on April 8, 2014. Aruba will not provide further ClearPass support for these operating systems. **Workaround:** Windows 2003 server and XP machines are required to update the Microsoft root CA certificate or missing trust certificates in order to load the OnGuard user interface properly. The following Microsoft knowledgebase article provides information, as well as a link to the hotfix download that needs to be installed in order to enable certificate support with SHA256 algorithm: https://support.microsoft.com/en-us/kb/968730.
#30381	**Symptom:** The ClearPass OnGuard Unified Agent might not be able to detect the installation of certain Windows updates that are not visible in **Control Panel > Programs and Features > View installed updates**. **Scenario:** These are updates that might not use an installer or cannot be removed. Some examples include the Windows Malicious Software Removal Tool, certain Windows Defender updates (but these are validated through AntiVirus health class), and foreign language input method editor (IME) files. **Workaround:** There is no workaround at this time.

Table 24: *Known Issues in OnGuard (Continued)*

Bug ID	Description
#30618	**Symptom:** The ClearPass user interface may become unavailable after installing ClearPass OnGuard hotfix patches due to a service restart. **Workaround:** Log in to the ClearPass CLI using the appadmin account, and restart cpass-admin-server using the 'service restart cpass-admin-server' command. This will only affect the GUI and not the availability of ClearPass services (for example, RADIUS).
#31734	**Symptom/Scenario:** When both the wired and wireless interfaces are connected, the ClearPass OnGuard Dissolvable Agent sometimes picks the wrong interface to perform health checks.
#33458	**Symptom/Scenario:** If there are more than two auto-connect SSIDs configured, a Windows OS will sometimes keep connecting to these SSIDs after the OnGuard Agent disconnects the wireless interface.

Policy Manager

Table 25: *Known Issues in Policy Manager*

Bug ID	Description
#10881	Entity updates with PostAuth enforcement fail if the publisher is down.
#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.
#13999 #13975	In order to add or update a PostAuth profile configuration, the admin must first delete old profiles from ClearPass, 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 ClearPass.
#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 ClearPass. This is due to a bug in AirWatch.
#19176	ClearPass does not currently support posting of Palo Alto Networks (PANW) user ID information when the PAN OS uses Vsys.

Table 25: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#19826	Palo Alto Networks (PANW) devices will only accept the backslash character (\ ) as a separator between the domain name and the username.
#20292	**Symptom/Scenario:** On the **Monitoring > Live Monitoring > System Monitor** page, the **Last updated at** field displays time based on the time zone of the ClearPass node where the user is viewing the page.
#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 ClearPass 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 ClearPass 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:** ClearPass system time might not have been synchronized with an NTP source. **Workaround:** Configure an NTP server. ClearPass will synchronize its time with the NTP source. Attempt the cluster operation.
#20489	**Symptom/Scenario:** ClearPass 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 ClearPass 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.
#21334	**Symptom:** ClearPass 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.
#22023	**Symptom/Scenario:** Launching the customer's ClearPass user interface through a proxy does not

Table 25: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	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.
#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.
#24646 #24919 #26698 #27379 #27568	**Symptom/Scenario:** There are some issues on Internet Explorer 9 (IE 9), including: • The login banner is not centered and the footer is not placed at the bottom of the page. • The IE browser fails to display an error message if connectivity is lost with the ClearPass Policy Manager server. • The scroll function does not work in the pop-up that opens from the **Monitoring > Audit Viewer** page. • ClearPass Policy Manager and Insight do not work properly on IE 9. • The **Save** operation gets stuck when you try to save the server configuration changes using the IE browser. **Workaround:** Use IE 10 or IE 11 or the Firefox or Chrome browsers instead. Users should be aware that ClearPass supports IE 10 and later on Windows 7 and Windows 8.x.
#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	**Symptom/Scenario:** When messages are sent using the Send Message option, messages are not received on the end points enrolled with SAP Afaria MDM Server.
#25720	**Symptom/Scenario:** The Dashboard shows the server as being down if an HTTPS server certificate is signed by OnBoard CA using SHA-256. **WorkAround:** Be aware that SHA1 RSA is not recommended for security reasons. You must update your certificates to use stronger keys, such as RSA with > 1024 bits length.
#27306	Whenever IPSec configuration is changed on either end of the tunnel (Wireless Controller or ClearPass), after the changes, the ClearPass IPSec service should be restarted in ClearPass from Services Control to establish the IPsec tunnels reliably. After restart, verify the status of the IPsec tunnel from the **Network** tab at **Administration > Server Manager > Server Configuration**.
#27592	**Symptom:** SAML-SSO using TLS certificate does not work in Firefox or Safari browser. **Workaround:** Use alternate browsers such as Google Chrome or IE.
#27621	**Symptom:** The number of authentications per second for non-MSCHAPv2 methods is reduced when

Table 25: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	the Local User or Admin User authentication sources are used. **Scenario:** Local and admin user passwords are now stored as non-reversible PBKDF2 based hashes. A side-effect of this change is reduced performance in password-based authentications (for example, PAP, GTC, WebAuth, or TACACS+) against the Local User and Admin User authentication sources. Refer to product documentation for the latest performance numbers. Authentications against external authentication sources such as AD or external SQL are not affected by this change.
#27745	**Symptom:** Some ClearPass Dashboard widgets do not work properly. **Scenario:** On the ClearPass Dashboard, some widgets (for example, All Requests) do not display information correctly when dragged onto the Dashboard windows. This happens with the Internet Explorer 9 browser. **Workaround:** Use the Firefox or Chrome browser instead.
#27895	Users should be aware that, because of schema changes now that ClearPass supports storing irreversible passwords, any import of old authentication sources using XML files will break the required SQL filters. Avoid any import of old authentication source configuration as this causes authentication failures for guest users and admin users.
#28417	**Symptom:** Updating the DNS settings through the UI causes the application to hang and the error message “Error processing request. Please retry” is displayed. **Scenario:** If the DNS settings are updated at **Administration > Server Manager > Server Configuration**, all services are restarted and the UI session is lost. **Workaround:** Wait a moment to let the Admin server restart, and then refresh the UI and log in again.
#33425	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 21). Please contact Customer Support for configuration recommendations to move away from using the session log database as an authentication source.

QuickConnect

Table 26: *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, ClearPass 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 > Configuration > 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.