ClearPass 6.5.0

aruba NETWORKS

Release Notes

Contents

ClearPass 6.5.0 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 6.5" on page 7—Provides important system requirements information for this release.
- "Upgrade and Update Information" on page 15—Provides considerations and instructions for version upgrades and patch updates.
- "What's New in This Release" on page 21—Describes new features and issues introduced in this 6.5.0 release as well as issues fixed in this 6.5.0 release.
- "Known Issues Identified in Previous Releases" on page 71—Lists currently existing issues identified in previous releases.

Related Documents

The following documents are part of the complete documentation set for the ClearPass 6.5.0 platform:

- *ClearPass Policy Manager 6.5 User Guide*
- *ClearPass Guest 6.5 User Guide*
- *ClearPass Insight 6.5 User Guide*
- *ClearPass Policy Manager 6.5 Getting Started Guide*
- *ClearPass Policy Manager Configuration API Guide*
- *ClearPass Policy Model: An Introduction*
- *Tech Note: Installing or Upgrading ClearPass 6.5 on a Virtual Machine*
- *Tech Note: Upgrading to ClearPass 6.5*
- *Tech Note: Cluster Upgrade Tool, ClearPass 6.5*

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/support-program/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/
Support Email Addresses	
Americas, APAC, and EMEA	support@arubanetworks.com
Security Incident Response Team (SIRT)	sirt@arubanetworks.com

Chapter 2
System Requirements for ClearPass 6.5

This chapter provides important system requirements information specific to this release. It should be read carefully before upgrading to ClearPass 6.5.

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

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 protections 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. Aruba Networks will not remove existing ClearPass features or software agents (such as OnGuard) that are compatible with these operating systems. We will not, however, be providing 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 XP — April 8, 2014
- Apple, Inc:
  - Mac OS X 10.6 (Snow Leopard) — February 26, 2014

Virtual Appliance Requirements

Please carefully review all 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.

Supported Hypervisors

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

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

CP-VA-500

- 2 Virtual CPUs
- 500 GB disk space
- 4 GB RAM
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

CP-VA-5K

- 8 Virtual CPUs
- Disk space:
  - 500 GB disk space required for existing deployments (upgrading from 6.2.6, 6.3.6, or 6.4.x)
  - 1000 GB disk space recommended for new deployments
- 8 GB RAM
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

CP-VA-25K

- 24 Virtual CPUs
- Disk space:
  - 1000 GB disk space required for existing deployments (upgrading from 6.2.6, 6.3.6, or 6.4.x)
  - 1800 GB disk space recommended for new deployments
- 64 GB RAM
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 350

CP-SW-EVAL (Evaluation Version)

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

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

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, 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

ClearPass OnGuard Unified Agent Requirements

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

- 1 GB RAM recommended, 512 MB RAM minimum
- 200 MB Disk Space
- Mac OS X: Version 10.6 or higher (64-bit only)
- Windows XP: Service Pack 3 or higher
- Windows 2003: Service Pack 2 or higher
- Ubuntu: 12.04 LTS and 14.04 LTS

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

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

Supported Antivirus Versions, OnGuard

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

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

- Avast
- AVG
- COMODO
- Kaspersky: IS-11 and above

- MacAfee
- 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 CPPM go to **Administration > Agents and Software Updates > OnGuard Settings**, click the **Help** link, 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 Agent Version Information

In current laboratory tests for ClearPass 6.5.0, the browser versions shown in Table 1 were verified for the ClearPass OnGuard Native Dissolvable Agents. There are considerations to be aware of with some browser versions. For more information, click the ID number next to the browser's name.

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

Operating System	Browser
Windows 7 64-bit	Chrome 38.x (#24518, #24986)
	Firefox 33.x
	IE 9.x (#25827)
Windows 7 32-bit	Chrome 39.x (#24518, #24986)
	Firefox 35.x
	IE 11.x
Windows 8 64-bit	Chrome 38.x (#24986)
	Firefox 33.x
	IE 10.x 32-bit
Windows 8 32-bit	Chrome 39.x (#24986)
	Firefox 34.x
	IE 10.x
Windows 8.1 64-bit	Chrome 39.x (#24986)
	Firefox 34.x

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

Operating System	Browser
	IE 11.x 32-bit
Windows 2008 64-bit	Chrome 38.x (#24986)
	Firefox 33.x
	IE 9.x 32 bit (#24766)
Windows Vista	Chrome 39.x (#24986)
	Firefox 34.x
	IE 7.x 32-bit
Mac OS X 10.9	Safari 7.x
	Firefox 33.x
	Chrome 38.x (#24518, #24986)
Mac OS X 10.8	Safari 6.x
	Firefox 33.x
	Chrome 38.x (#24986)
Mac OS X 10.7.5	Safari 6.x
	Firefox 34.x
	Chrome 39.x (#24986)
Ubuntu 12.04 32-bit LTS	Firefox 34.x
Ubuntu 12.04 64-bit LTS	Firefox 34.x
Ubuntu 14.04 32-bit LTS	Firefox 34.x
Ubuntu 14.04 64-bit LTS	Firefox 34.x

ClearPass OnGuard Java-Based Agent Version Information

In current laboratory tests for ClearPass 6.5.0, the browser and Java versions shown in Table 2 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*

Operating System	Browser	Java Version
Windows 7 64-bit	Chrome 40.x (#7165)	JRE 1.8 Update 31 32-bit
	Firefox 33.x (#7165)	JRE 1.8 Update 31 32-bit
	IE 8.x	JRE 1.8 Update 31
Windows 7 32-bit	Chrome 40.x	JRE 1.8 Update 31
	Firefox 35.x	JRE 1.8 Update 31
	IE 11.x	JRE 1.8 Update 31
Windows 8 64-bit	Chrome 40.x (#7165)	JRE 1.8 Update 31 32-bit
	Firefox 35.x (#7165)	JRE 1.8 Update 31 32-bit
	IE 10.x (#7165)	JRE 1.8 Update 31
Windows 8 32-bit	Chrome 40.x	JRE 1.8 Update 31
	Firefox 35.x	JRE 1.8 Update 31
	IE 10.x	JRE 1.8 Update 31
Windows 8.1 64-bit	Chrome 40.x (#7165)	JRE 1.8 Update 31 32-bit
	Firefox 35.x	JRE 1.8 Update 31 32-bit
	IE 11.x	JRE 1.8 Update 31
Windows 2008 64-bit	Chrome 40.x (#7165)	JRE 1.8 Update 31 32-bit
	Firefox 33.x (#7165)	JRE 1.8 Update 31 32-bit
	IE 9.x (#7165)	JRE 1.8 Update 31
Mac OS X 10.10	Safari 8.x (#20191)	JRE 1.8 Update 31
	Firefox 35.x (#26514)	JRE 1.8 Update 31
	Chrome 40.x	JRE 1.8 Update 31
Mac OS X 10.9	Safari 7.x (#20191)	JRE 1.8 Update 31
	Firefox 34.x	JRE 1.8 Update 31
	Chrome 40.x	JRE 1.8 Update 31

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

Operating System	Browser	Java Version
Mac OS X 10.8	Safari 6.x (#20191)	JRE 1.8 Update 31
	Firefox 33.x	JRE 1.8 Update 31
	Chrome 40.x	JRE 1.8 Update 31
Mac OS X 10.7.5	Safari 6.x (#20191)	JRE 1.8 Update 31
	Firefox 35.x (#23340)	JRE 1.8 Update 31
	Chrome 40.x	JRE 1.8 Update 31

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 6.4.x to 6.5. For information on upgrading from a version prior to 6.5, see "Upgrading to ClearPass 6.5 from 6.2.6, 6.3.6, or 6.4.x" on page 15.
- 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 6.5.0 to 6.5.1. For information on updating from an earlier 6.5.x release to 6.5.0, see "Updating Within the Same Major Version" on page 18.

Upgrading to ClearPass 6.5 from 6.2.6, 6.3.6, or 6.4.x

An upgrade is the process of moving from one major release version to another—for example, from 6.4.x to 6.5. 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 6.5 from ClearPass 6.2.6, 6.3.6, or 6.4.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 18.

- For 6.4.x upgrades through the Software Updates portal in the Policy Manager user interface, or through the Web service, upgrade is supported for any 6.4.x version.
- For 6.4.x upgrades through the CLI, there are two options:
  - If you are on 6.4.2 or later, you can upgrade directly to 6.5 through the CLI.
  - If you are on 6.4.0 or 6.4.1, you must first download and install the 6.4.0 CLI updates patch. At support.arubanetworks.com, go to **Download Software > ClearPass > Policy Manager > Current Release** and select **CPPM-x86_64-20140919-cli-der-support-patch**. After you have installed the patch, update to 6.4.2 or higher. You can then upgrade to 6.5 through the CLI.
- For 6.3.x, upgrade is only supported from the latest cumulative patch. You must update to 6.3.6 before upgrading to 6.5.
- For 6.2.x, upgrade is only supported from the latest cumulative patch. You must update to 6.2.6 before upgrading to 6.5.
- For 6.1.x, direct upgrades are not supported. Customers on 6.1.x must intermediately upgrade to 6.2.6, 6.3.6, or 6.4.x first before upgrading to 6.5.
- For appliance upgrades from 5.2.0, you must upgrade to 6.2.6, 6.3.6, or 6.4.x before upgrading to 6.5.
- Upgrade images are available within ClearPass Policy Manager from the Software Updates portal at **Administration > Agents and Software Updates > Software Updates**.
- Upgrade images are also available for download on the Support site under **ClearPass > Policy Manager > Archives**.

If you are upgrading from 6.4.0, the Software Updates portal incorrectly shows a warning during upgrade asking for two hard drives. This message can be ignored. (#27736)

MySQL is supported in CPPM 6.0.x and greater. Aruba does not ship drivers for MySQL by default. Customers who

require MySQL can contact Aruba support to get the required patch. Users should be aware that this patch does not persist across upgrades, so customers using MySQL should contact support before they upgrade.

Before You Upgrade

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

- Plan downtime accordingly. Upgrades can take longer (several hours) depending on the size of your configuration database. A large number of audit records (hundreds of thousands) due to MDM integration can significantly increase upgrade times. Refer to the sample times shown in Table 3 in "Sample Times Required for Upgrade" on page 16.
- Review the VMware disk requirements. These are described in "Virtual Appliance Requirements" on page 7 of the "System Requirements for ClearPass 6.5" 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 17.

- Before initiating the Upgrade process in CPPM, we recommend you set the **Auto Backup Configuration Options** to **Off** (if it was set to other values such as Config or Config|Session). 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 17). Please contact Customer Support for configuration recommendations to move away from using the session log database as an authentication source.
- VM only: If you have two disks already loaded with previous ClearPass versions—for example, 6.2 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 6.5 disk requirements. For current requirements, see "Virtual Appliance Requirements" on page 7.

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

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

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

Restoring the Log DB Through the User Interface

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

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

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

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

1. Go to **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 6.4.3 to 6.4.4. 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 CPPM server, and then install it through the user interface:

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

This chapter provides a summary of the new features and changes in the ClearPass 6.5.0 release.

This chapter contains the following sections:

Release Overview

ClearPass 6.5.0 is a major release that introduces new features and provides fixes for known issues. The 6.5.0 upgrade is available in ClearPass Policy Manager under **Administration > Agents and Software Updates > Software Updates**.

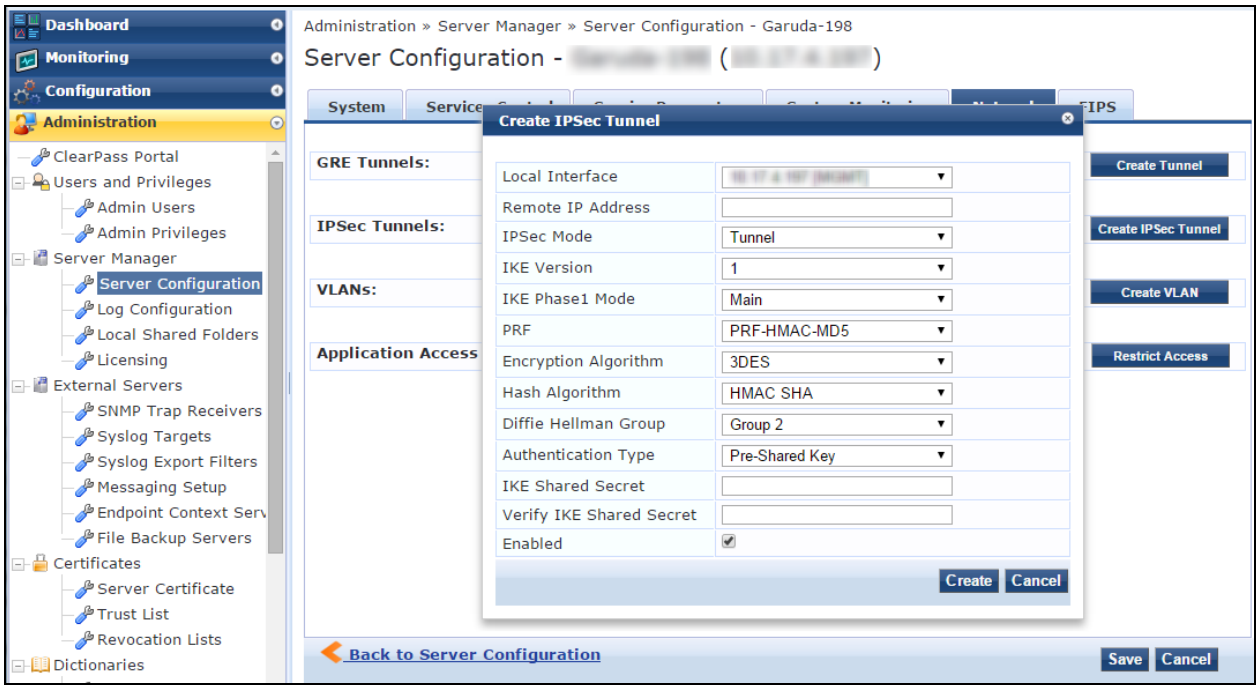
New Features and Enhancements in the 6.5.0 Release

The following new features were introduced in the ClearPass 6.5.0 release.

Policy Manager

- Support was added for terminating IPSec VPN tunnels. To use this feature, go to **Administration > Server Manager > Server Configuration** and click the server in the list. On the **Network** tab, click the **Create IPSec Tunnel** button. Items that can be configured for an IPSec tunnel include: (#8378)
  - Local Interface
  - Remote IP Address
  - IPSec Mode
  - IKE Version
  - IKE Phase1 Mode
  - Encryption Algorithm
  - Hash Algorithm
  - Diffie Hellman Group
  - Authentication Type
  - IKE Shared Secret

Figure 1 *Support for IPSec VPN Tunnels*



- Support was added for broadcasting a RADIUS accounting request to proxy targets configured in the service. A new **Accounting Proxy** option is available when you configure new or modify existing RADIUS services, providing the ability to proxy RADIUS accounting events. (#15002, #25647)

  To use this feature, go to **Configuration > Services** and select or add a RADIUS service. On its configuration form, click the **Service** tab. Complete the fields as needed and, in the **More Options** field, select the **Accounting Proxy** check box. An **Accounting Proxy** tab is added to the form. Fields on this tab let you configure a hierarchical list of proxy targets to which the RADIUS server should be forwarded, and configure attributes to include in the accounting packet. Attribute values can be static or any parameterized value. These options are shown in the figures below.

Figure 2 *RADIUS Accounting Proxy Configuration, Service Tab*

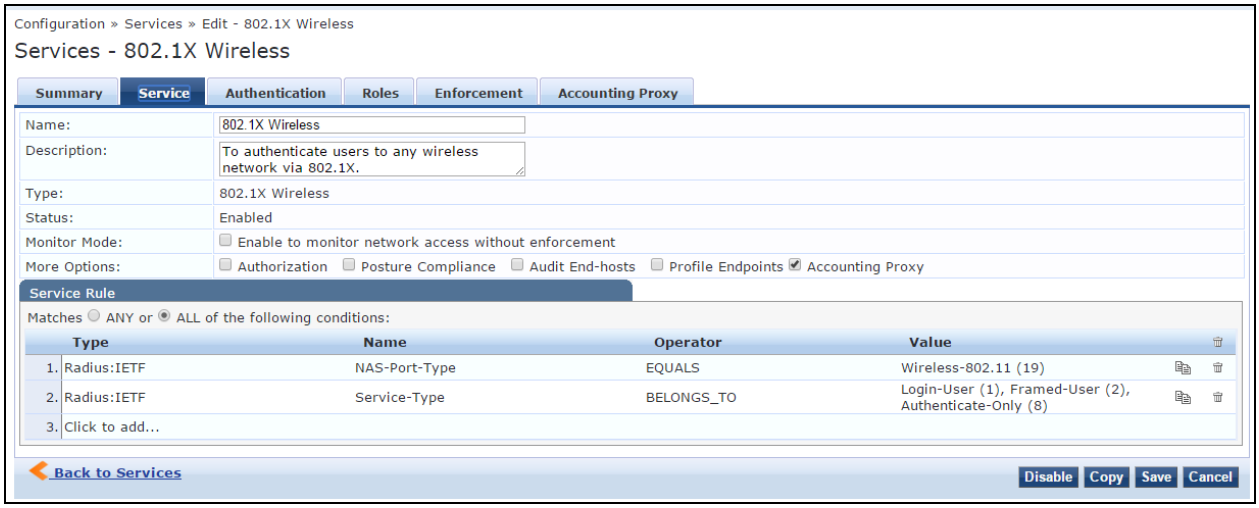
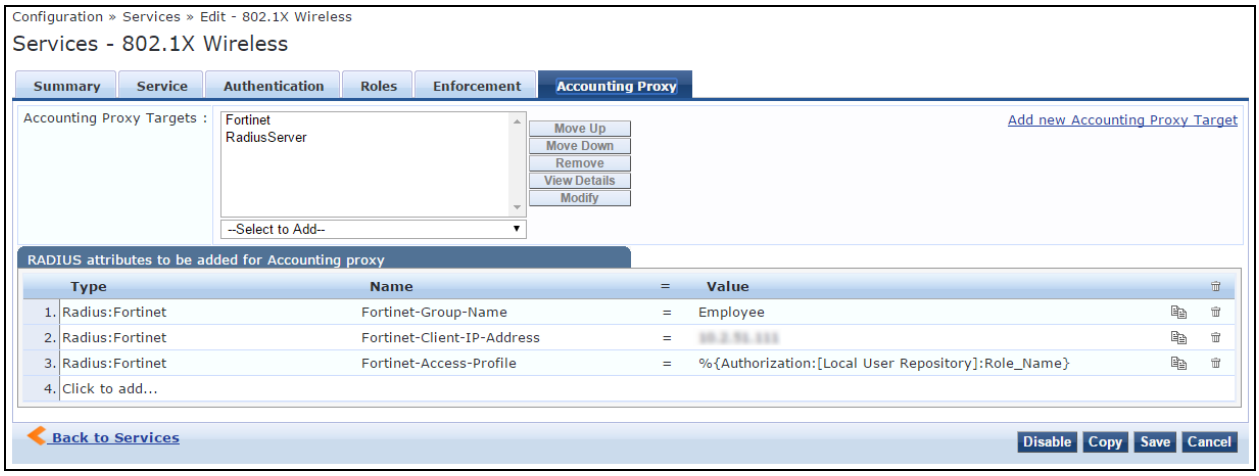
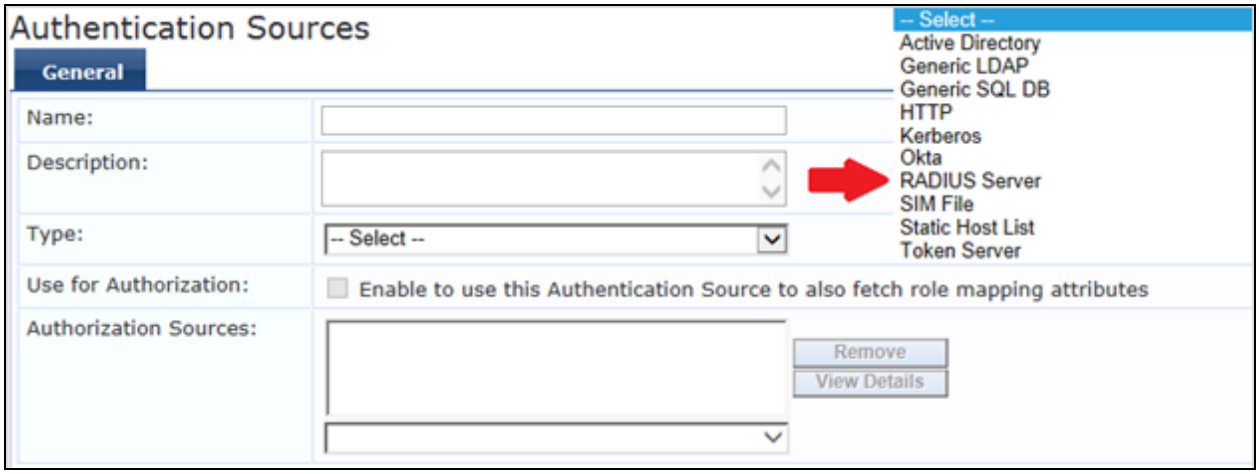


Figure 3 *RADIUS Accounting Proxy Configuration, Accounting Proxy Tab*



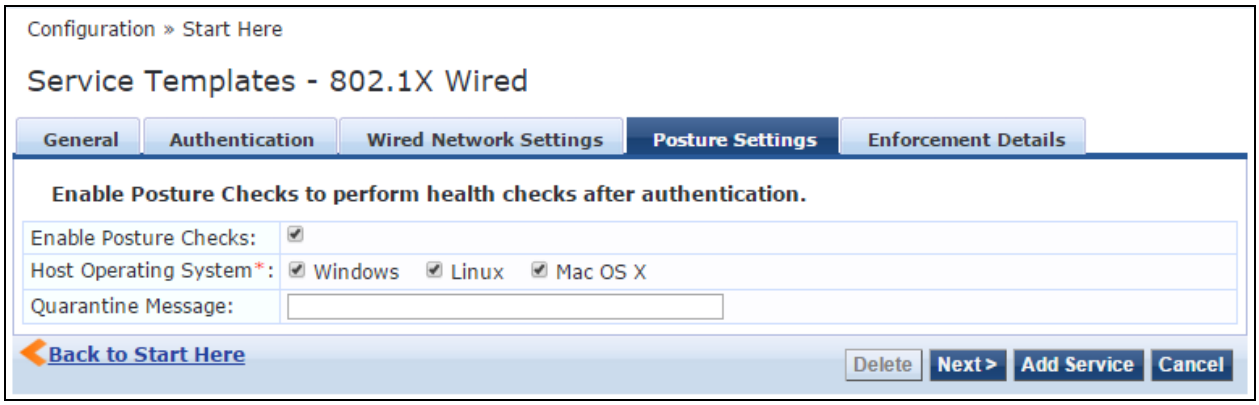
- RADIUS is now supported as an authentication and authorization source, allowing ClearPass to query third-party RADIUS servers. When you add a new authentication source, the new **RADIUS Server** source type is available in the **Type** drop-down list at **Configuration > Authentication > Sources > General tab**. The RADIUS Server source type can be used with any RADIUS-based authentication service. Extra RADIUS attributes can be added before sending the RADIUS request to a RADIUS-based remote server, and the response attributes can be used as role or authorization attributes. (#20550, #25646)

Figure 4 *Authentication Sources, RADIUS Server Option*



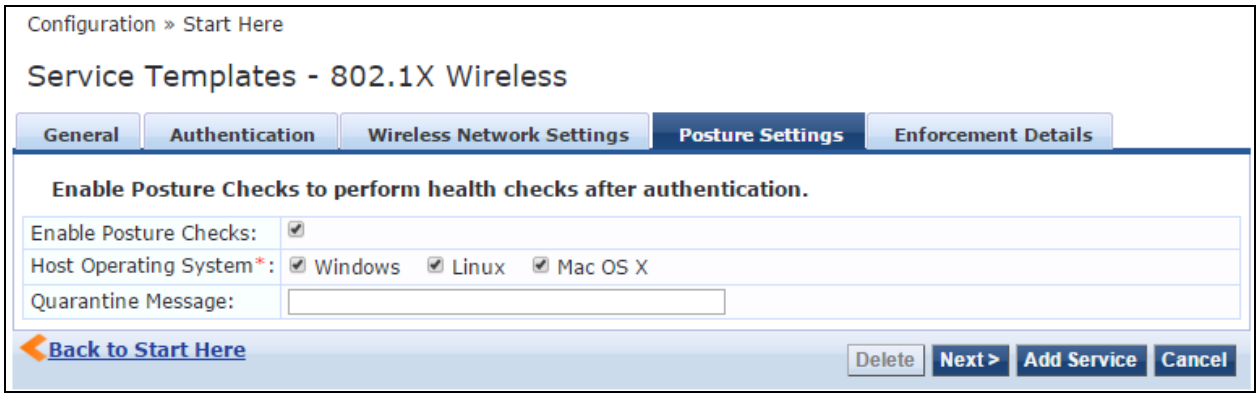
- Four service templates were enhanced to streamline workflows for some common ClearPass configurations. To use these features, go to **Configuration > Start Here** and select the following service template links: (#20659)
  - **802.1X Wired —** A **Posture Settings** tab was added. Options on this tab let you enable or disable posture checks, specify host operating systems (Windows, Linux, or Mac OS X), and provide a quarantine message.

Figure 5 *802.1X Wired Service Template Configuration, Posture Settings Tab*



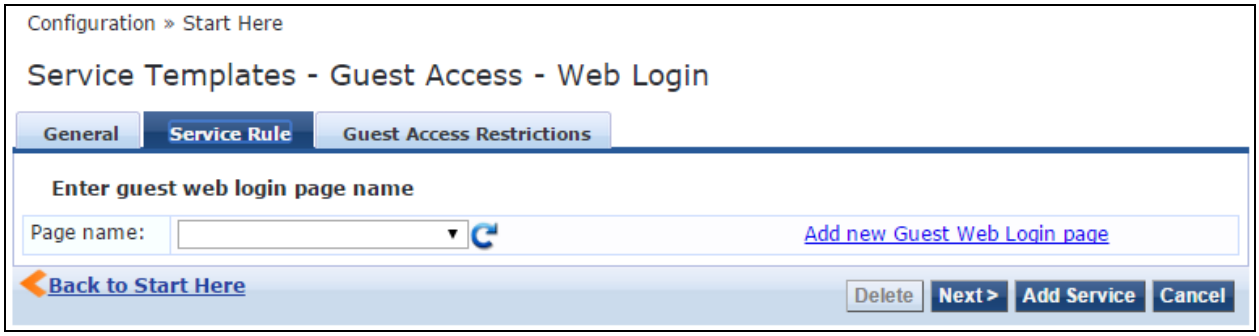
- **802.1X Wireless —** A **Posture Settings** tab was added. Options on this tab let you enable or disable posture checks, specify host operating systems (Windows, Linux, or Mac OS X), and provide a quarantine message.

Figure 6 *802.1X Wireless Service Template, Posture Settings Tab*



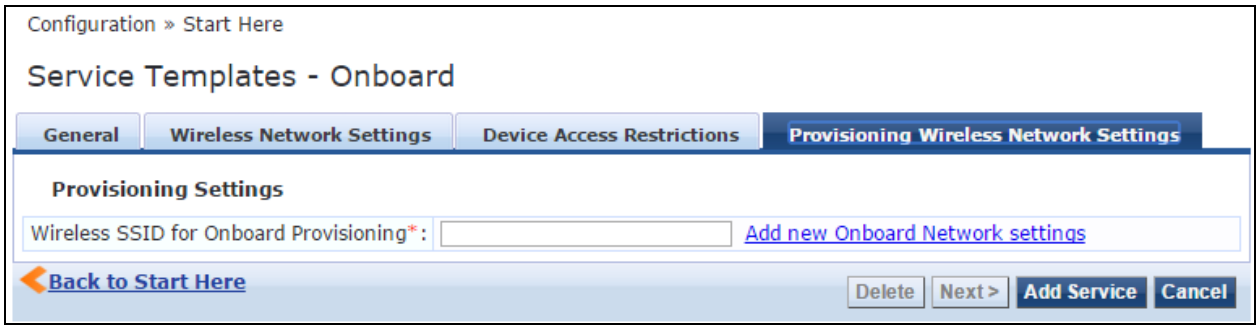
- **Guest Access - Web Login —** The **Service Rule** tab now includes a link to open the **ClearPass Guest > Configuration > Web Logins** page, where you can create a new guest Web login page.

Figure 7 *Guest Access - Web Login Service Template, Link to Guest Web Logins Config*

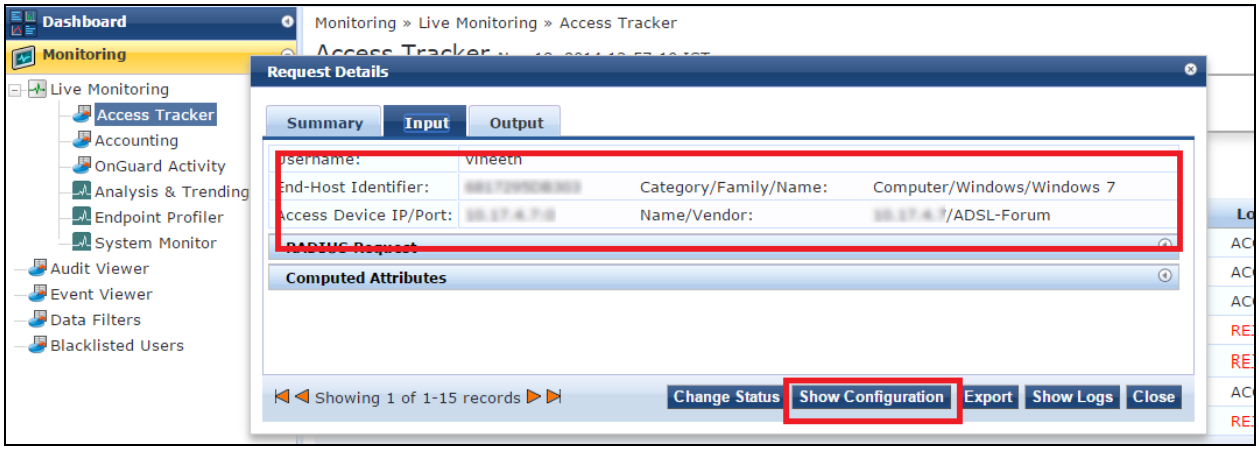


- **Onboard —** The **Provisioning Wireless Network Settings** tab now includes a link to open the **Onboard > Configuration > Network Settings** page, where you can add new Onboard network settings.

Figure 8 *Onboard Service Template, Link to Onboard Network Settings*

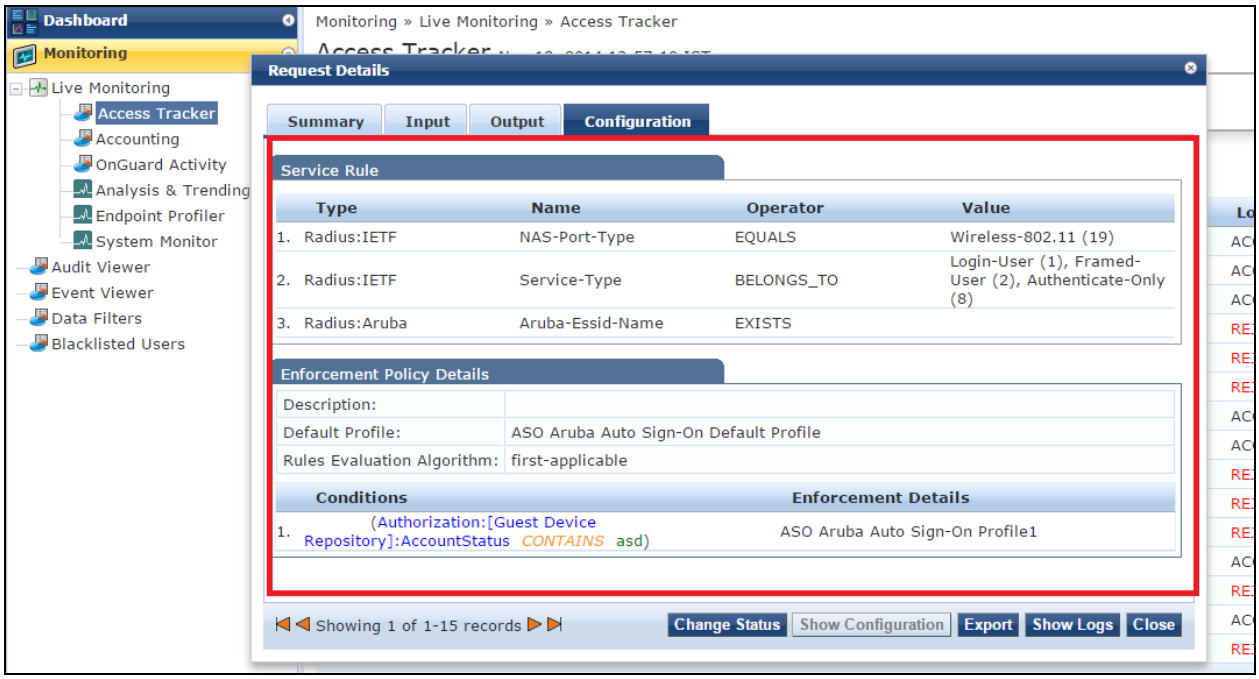


- Enhancements to the Access Tracker provide additional information. To see this feature, go to **Monitoring > Live Monitoring > Access Tracker** and click a server in the list. The **Request Details** form opens. Changes to this form include: (#20660, #26127)
  - The **Input** tab now shows the category, family, and OS of the device, and the name of the vendor. This tab also includes a new **Show Configuration** button, which adds a tab to the Request Details form.



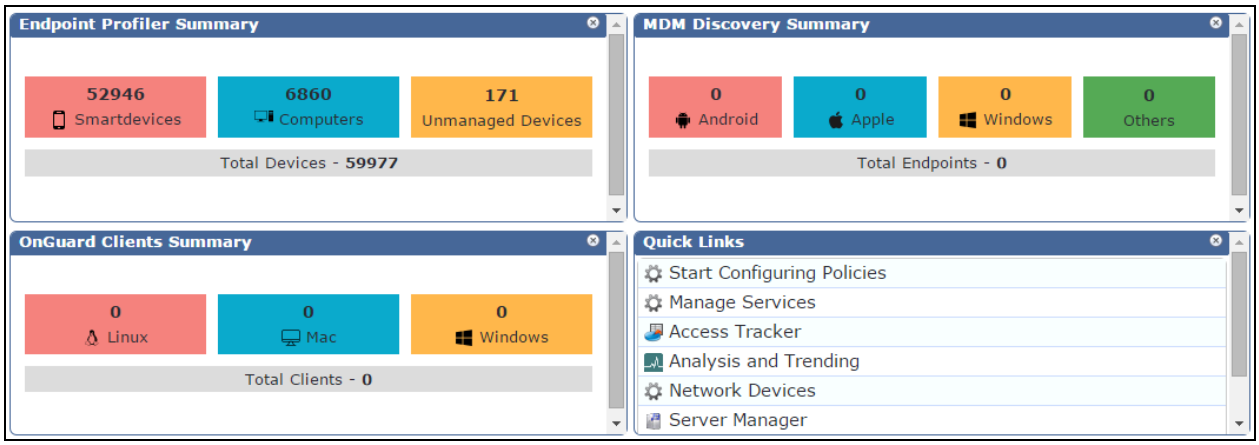
  - When you click the **Show Configuration** button on the **Input** tab, the **Configuration** tab is added to the **Request Details** form. This tab provides **Service Rule**, **Role Mapping Policy Details**, and **Enforcement Policy Details** information.

Figure 9 *Configuration Tab on Access Tracker > Request Details*



- Three new widgets were added to the Dashboard: (#20664)
  - Endpoint Profiler Summary
  - MDM Discovery Summary
  - OnGuard Client Summary

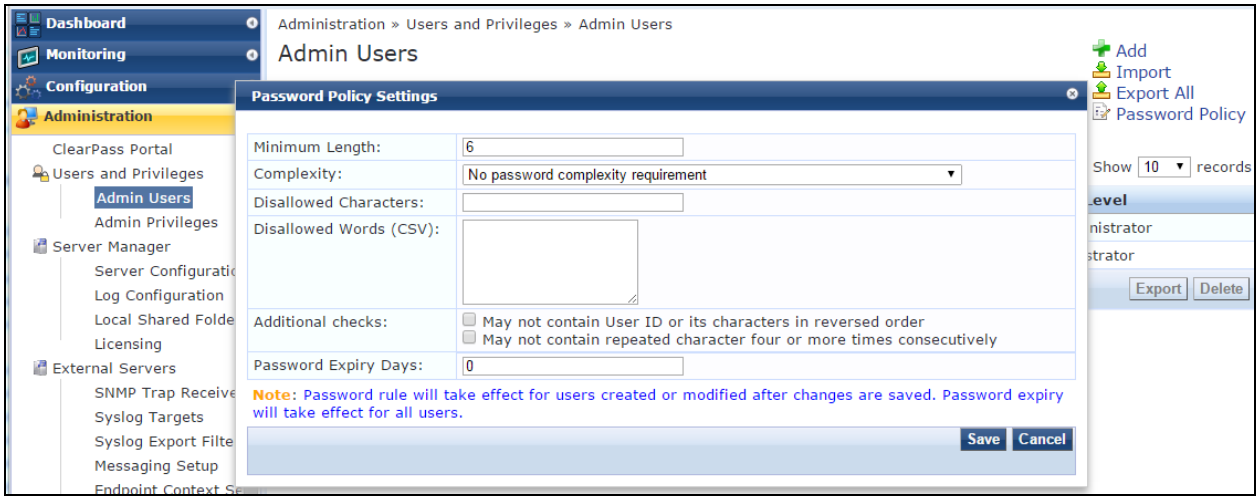
Figure 10 *Policy Manager Dashboard: Three New Widgets*



- Several enhancements were made related to Common Criteria Protection Profile and FIPS 140. Changes were made in the areas of password complexity policies, idle session timeout configuration, admin passwords, and performance monitor rendering. As part of this feature: (#20667, #23819, #24191, #26272, #26273, #26274, #27208, #27475)
  - Password security was strengthened.
  - A new **Password Policy Settings** form was added for both local users and admin users. To use this feature, go to either **Administration > Users and Privileges > Admin Users > Password Policy** or **Configuration > Identity > Local Users > Password Policy**. Options that can be configured for the

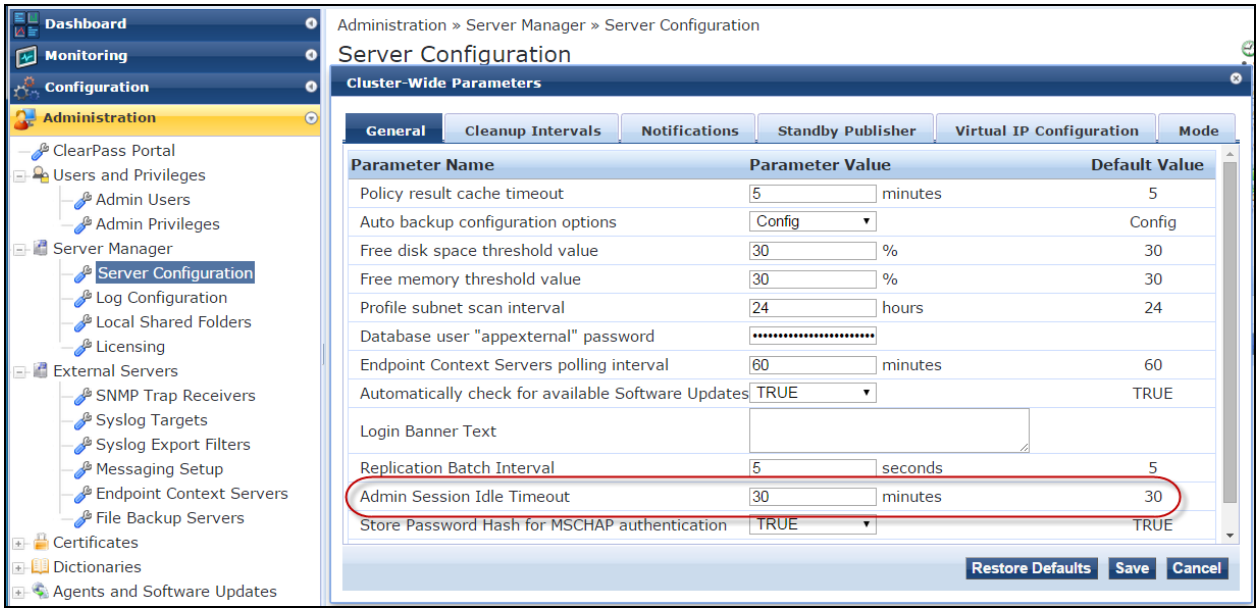
password include length, complexity, disallowed characters, disallowed words, disallowed user ID or repeated characters, and the number of days to expiration.

Figure 11 *Password Policy Settings*



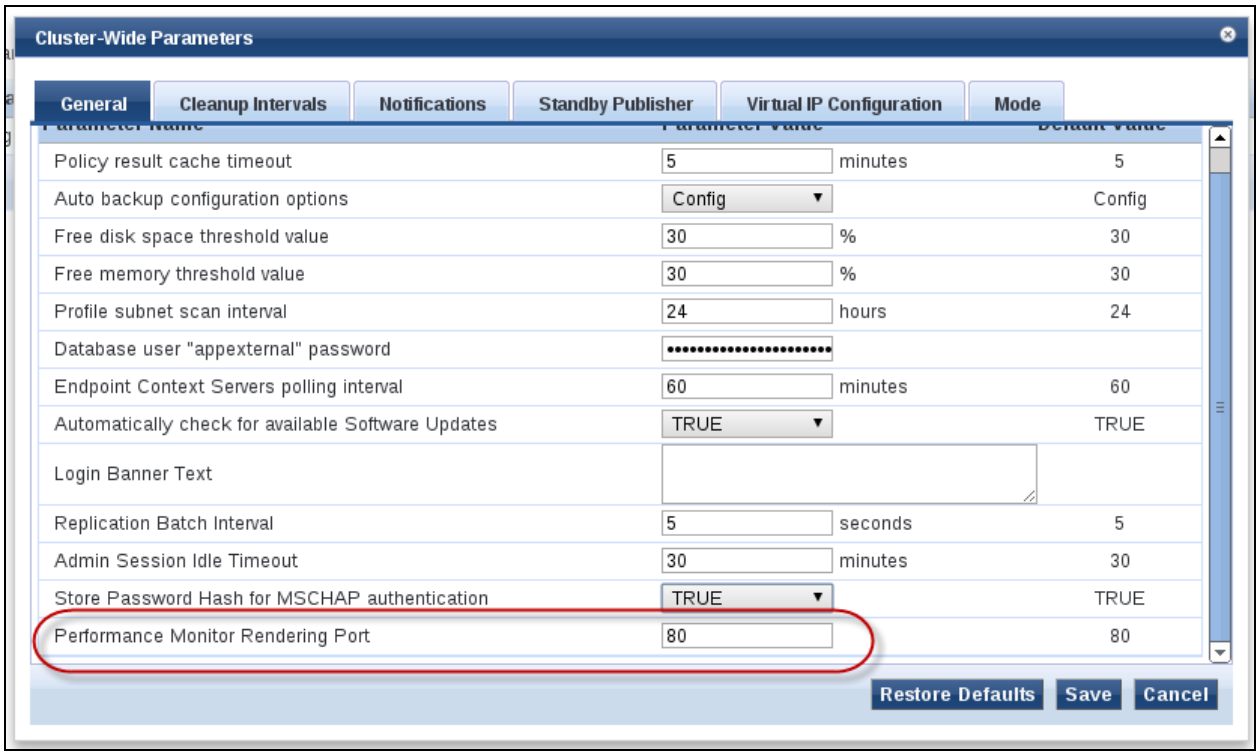
- A new cluster-wide parameter, **Admin Session Idle Timeout**, allows administrators to configure the maximum idle time permitted for a session before it times out. To use this feature, go to **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General tab**. Scroll to the **Admin Session Idle Timeout** row and enter the number of minutes to allow before timeout. The default value is 30 minutes.

Figure 12 *Cluster-Wide Parameters, Admin Session Idle Timeout Parameter*



- A new cluster-wide parameter, **Performance Monitor Rendering Port**, controls performance metrics rendering among the nodes in the cluster. The port can be altered depending on the firewall requirements in deployments.

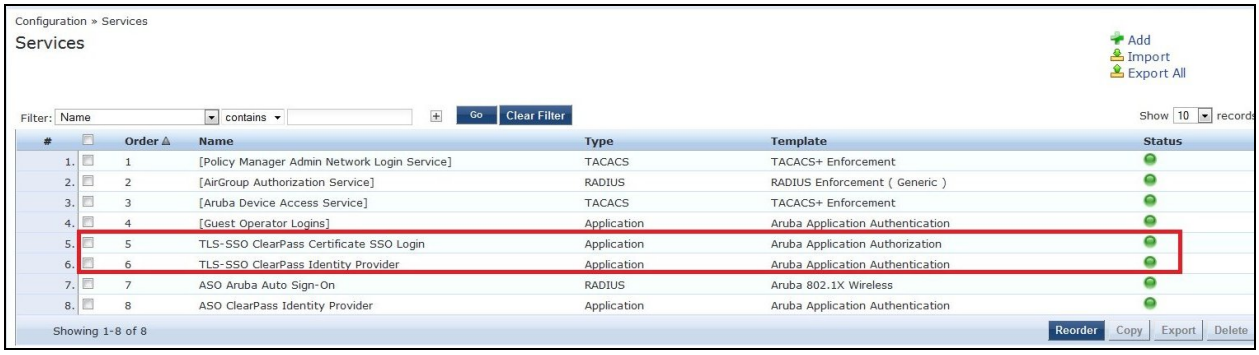
Figure 13 *Cluster-Wide Parameters, Performance Monitor Rendering Port*



- Default values have changed for two items in the Administration module: (#25998)
  - The default value of **Old Audit records cleanup interval** is changed from 30 days to 7 days under the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Cleanup Intervals** tab.
  - The default value of the **Limit each log file size** parameter under **Administration > Log Configuration > System Level** is changed from 25 MB to 50 MB.
- ClearPass now provides the ability to add a number of devices that have contiguous IP addresses. To use this feature, go to **Configuration > Network > Devices > Add Device**. In the **IP Address or Subnet** field, use a hyphen to indicate the range of device IP addresses, following the format **a.b.c.d-e** (for example, 192.168.1.1-20). (#20841, #26134)
- A new option lets you clear the machine authentication cache on all the nodes. This option is available at **Administration > Server Manager > Server Configuration > Clear Machine Authentication Cache**. (#20959)
- Information retrieved by API queries to the Endpoints table now includes endpoint profile information. (#21004)
- A new RADIUS service parameter, **Enable signing for OCSP Request**, was added for specifying whether ClearPass should sign an OCSP request with a RADIUS server certificate. To use this feature, go to **Administration > Server Manager > Server Configuration** and click the server in the list. On the **Service Parameters** tab, select **RADIUS server** in the **Select Service** drop-down list. Scroll to the **Enable signing for OCSP Request** row and set the value to either TRUE or FALSE. The default value is FALSE to disable the signing process. (#21677)
- Administrators and guest operators can now log in to ClearPass using smart cards and TLS certificates. To use this feature: (#23050)

1. In **ClearPass Policy Manager**, go to **Configuration > Start Here**, click **Certificate/Two-factor Authentication for ClearPass Application Login**, and configure the service template and add it. It will then be available in the list at **Configuration > Services**.

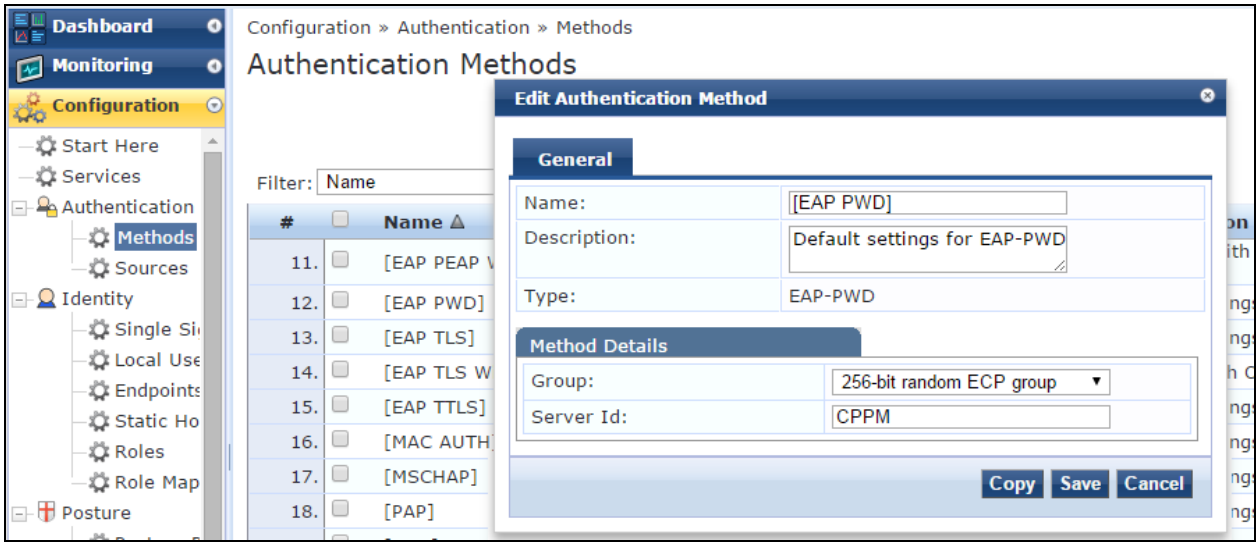
Figure 14 *Services List, TLS-SSO Authentication*



2. In **ClearPass Guest**, go to **Configuration > Pages > Web Logins** to create a Web login page. In the **Vendor Settings** drop-down list, select **Single Sign-On - SAML Identity Provider**. In the **Login Form** area, select the appropriate values in the **Client Certificate** and **Authentication** fields to allow admins and guests to log in via smart cards and TLS certificates.

- The following additional OIDs are now exposed for reporting CPU load averages for one minute, five minutes, and fifteen minutes: (#24057)
  - .1.3.6.1.4.1.2021.10.1.3.1
  - .1.3.6.1.4.1.2021.10.1.3.2
  - .1.3.6.1.4.1.2021.10.1.3.3
- A new attribute, **Mac-Address-Upper-Hyphen**, was added to the Connection namespace. This attribute contains the client's MAC address in uppercase with a hyphen delimiter. (#24074)
- Support was added for the EAP-PWD authentication method. To use this feature, go to **Configuration > Authentication > Methods** and scroll to the **[EAP PWD]** method in the list. The EAP-pwd protocol method uses a shared password for authentication. For more information, see http://www.rfc-base.org/rfc-5931.html. (#24149)

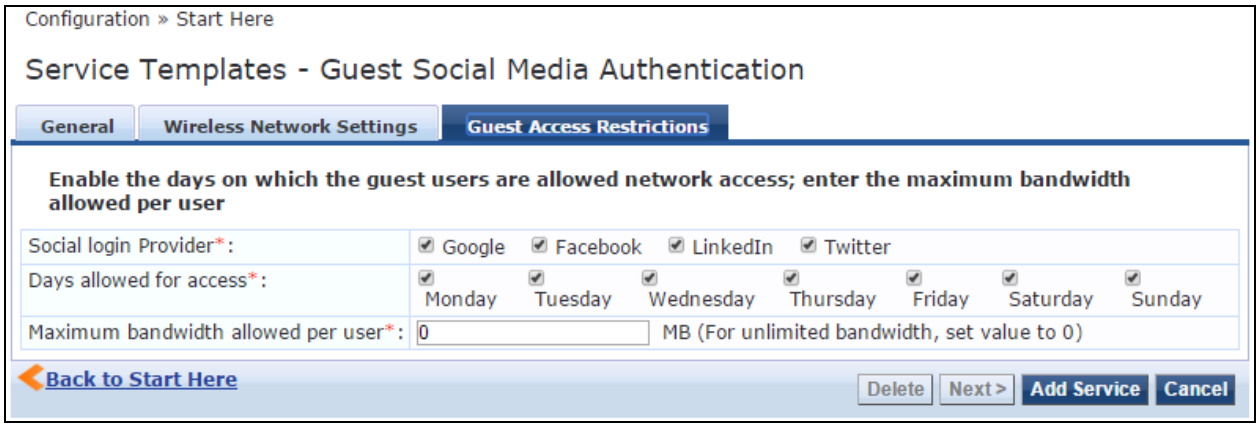
Figure 15 *Support for the EAP-PWD Authentication Method*



- The Cisco Adaptive Security Appliance (ASA) RADIUS dictionary was added. When you upgrade or restore from a previous version, the Cisco ASA dictionary automatically replaces the Cisco VPN3000 RADIUS dictionary. If you require the Cisco VPN3000 dictionary, you may import it. (#24337)
- A new service parameter, **Include Nonce in OCSP request**, was added for specifying whether an OCSP request should contain a nonce or not. A nonce is a unique identifier for an OCSP request. To use this feature, go to **Administration > Server Manager > Server Configuration** and click the server in the list. On the **Service Parameters** tab, select **RADIUS server** in the **Select Service** drop-down list. Scroll to the **Include Nonce in OCSP request** row and set the value to either TRUE or FALSE. The default value is TRUE. If the OCSP server does not support nonce, set the value of this parameter to FALSE to avoid an EAP-TLS authentication failure. (#24443)
- ClearPass now provides the ability to authenticate users belonging to trusted domains when the Global Catalog server is configured as an authentication source and the username does not contain the domain name. (#24731)
- ClearPass now displays information from the SNMP Management Information Base (MIB). On an SNMP query, the information is exposed beginning one minute after changes are made to the configuration. Details include: (#24850)
  - System information
  - Authentication counters
  - Authorization counters
  - Network traffic counters
  - Traps for various system and application events

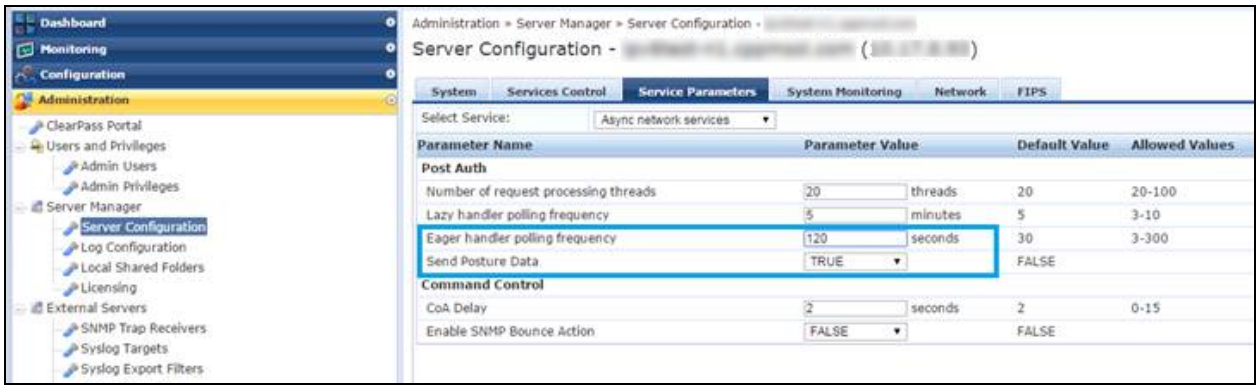
  For more information, see http://support.arubanetworks.com/DownloadSoftware/tabid/75/DMXModule/510/Default.aspx?EntryId=16480.
- A new service template was added for to provide authentication sources for social logins. To see this feature, go to **Configuration > Start Here** and select **Guest Social Media Authentication**. (#25183)

Figure 16 *Guest Social Media Authentication Service Template*



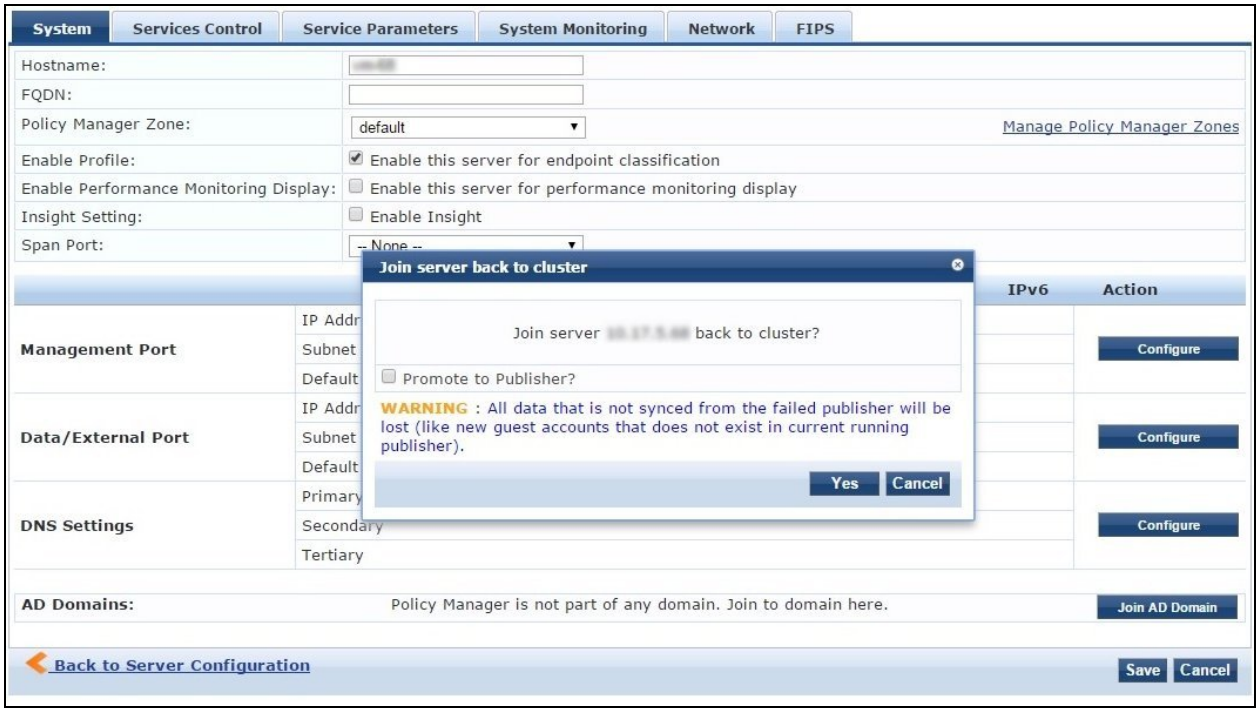
- Data about the various posture classes and their status for endpoints, as derived by the OnGuard agent, can now be sent to Palo Alto Networks devices. To use this feature, when configuring a Palo Alto firewall or panorama device as an external context server, go to **Administration > Server Manager > Server Configuration**, open the server's configuration form, and click the **Service Parameters** tab. Set the **Send Posture Data** option to **TRUE**, and enter a value higher than two minutes for the **Eager handler polling interval** option. Because this feature can be resource-intensive, the eager handler-polling interval must be two minutes or more. (#25217)

Figure 17 *Enable GlobalProtect for a Palo Alto Firewall*



- A new option, **Join Server Back to Cluster**, was added to the **Server Configuration** page for nodes whose replication status is DISABLED. This option is only available to users with the Admin role. The Join Server Back to Cluster option lets administrators join a failed node back to the cluster. The node can also be promoted to publisher. This option can only be triggered from a node that is currently active in the cluster. To use this option, go to **Administration > Server Manager > Server Configuration** and click the node whose replication status is DISABLED. (#25304)

Figure 18 *Server Configuration, Join Server Back to Cluster Dialog*

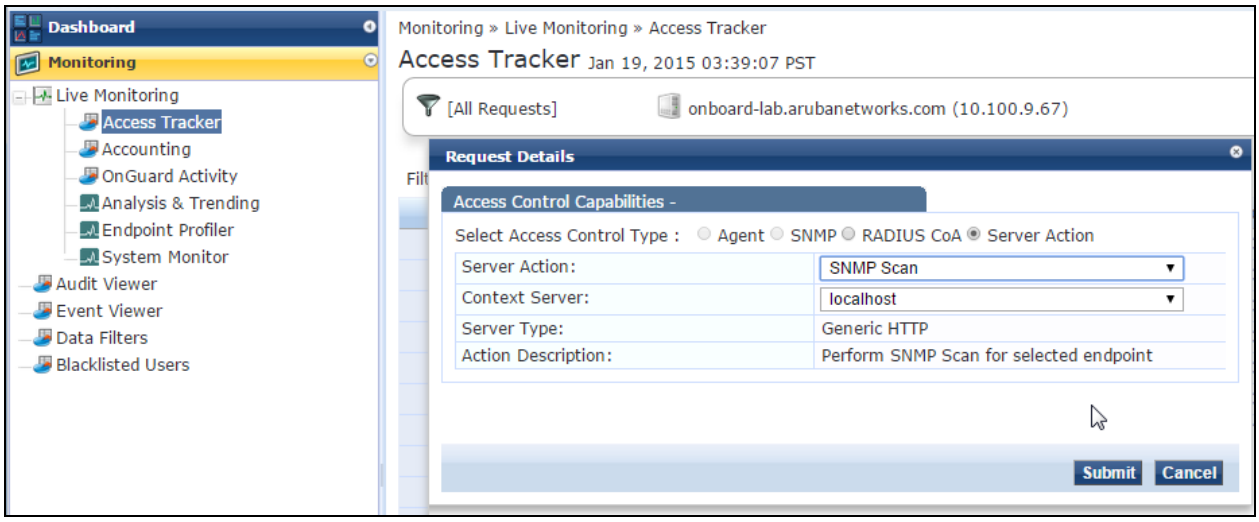


- The **Certificate Trust List** at **Administration > Certificates > Trust List** now includes DoD (Department of Defense) certificates. These are disabled by default, and can be enabled as needed. A DoD certificate allows a browser to trust Web sites whose secure communications are authenticated by a Department of Defense agency. (#25329)
- For wired network profiling, MAC OUI (Organizationally Unique Identifier) information is now populated for all endpoints even when no other profiling information is available for an endpoint. This feature is available at **Configuration > Identity > Endpoints > Edit Endpoint**. (#25377)

Figure 19 *Edit Endpoint, MAC OUI Information*

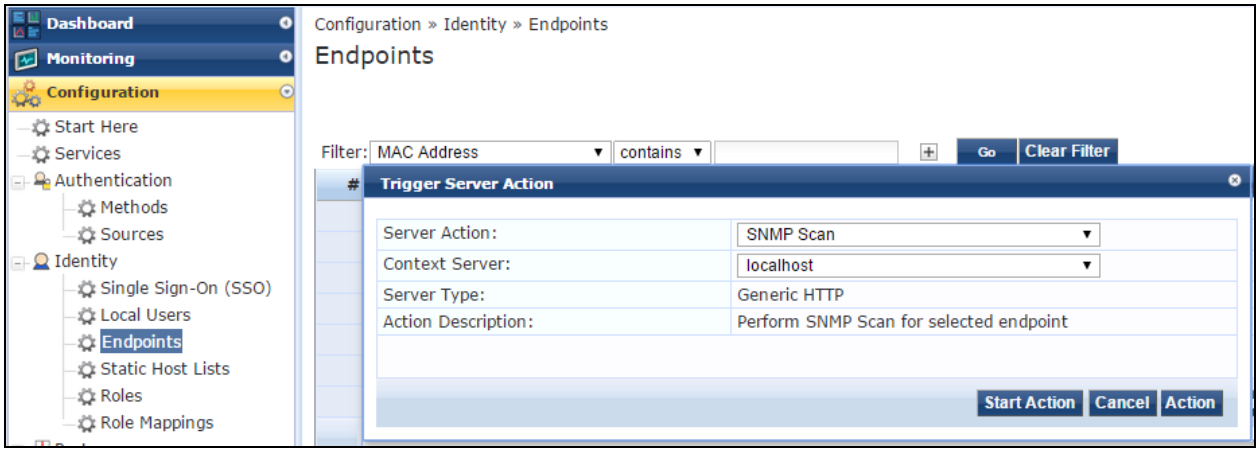
- For wired network profiling, a list of multiple SNMP community strings can now be configured and used to query static IP devices discovered by the Profiler. If a static IP device does not respond to queries from the default public community string, the SNMP service can use the credentials from this custom list to query the device. This feature is available at **Configuration > Profile Settings > SNMP Configuration**. (#25417, #25837)
- For wired network profiling, a one-time scan can now be triggered to discover and profile devices in specified network IP subnets. To use this feature, go to **Configuration > Profile Settings > Subnet Scans** and click the **On-Demand Subnet Scan** link. Enter the subnets to scan and click **Submit**. (#25418)
- Insight now records the last connected location for an endpoint when such information is available. This information is determined from RADIUS authentication and accounting information, and from SNMP queries of network devices that have been set up for SNMP read and trap notification. Insight reports based on the Endpoints template can report on the following columns related to device location: (#25421)
  - NadIp (switch or controller IP)
  - NadPort (port information for wired devices)
  - Access Point (AP for wireless devices)
  - Ssid (SSID for wireless devices)
- For wired network profiling, an SNMP scan of an endpoint can now be triggered from its **Access Tracker** authentication record or **Endpoints** configuration in order to profile the endpoint. The option for the SNMP scan of the endpoint is only available if the client IP address is available. Only one endpoint can be scanned at a time. (#25456, #25420)
  - To use this feature from **Monitoring > Live Monitoring > Access Tracker**, click the server in the list to open the **Request Details** form. On the **Summary** tab, click **Change Status**. On the **Access Control Capabilities** tab, select the **Server Action** radio button. Select **SNMP Scan** in the **Server Action** drop-down list, and then click **Submit**.

Figure 20 *Access Tracker, Trigger SNMP Scan of Endpoint Option*



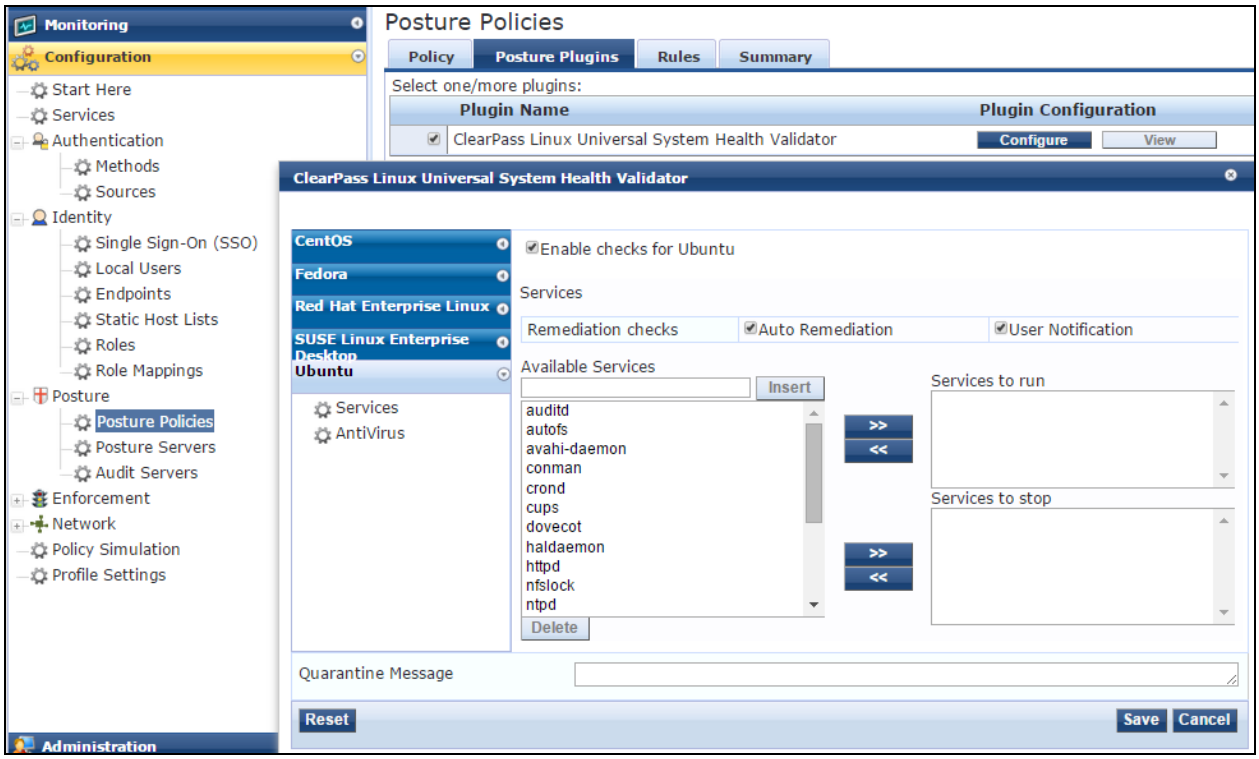
- To use this feature from **Configuration > Identity > Endpoints**, mark the check box for the endpoint in the list and click **Trigger Server Action**. In the **Server Action** drop-down list select **SNMP Scan**, and then click **Submit**.

Figure 21 *Endpoints, Trigger SNMP Scan of Endpoint Option*



- A new cluster-wide service parameter, **Replication Batch Interval**, was added. This parameter can be used to change the number of seconds for the minimum replication time. This parameter should only be modified as instructed by Support. (#25461)
- The Policy Server now logs an alert message if an authentication source filter takes a long time (more than 6 to 10 seconds) or times out. The alert message can be viewed in the logs at **Monitoring > Live Monitoring > Access Tracker**. (#25508)
- Ubuntu was added to the list of Linux Posture configuration settings at **Configuration > Posture > Posture Policies > Posture Plugins**. (#25676)

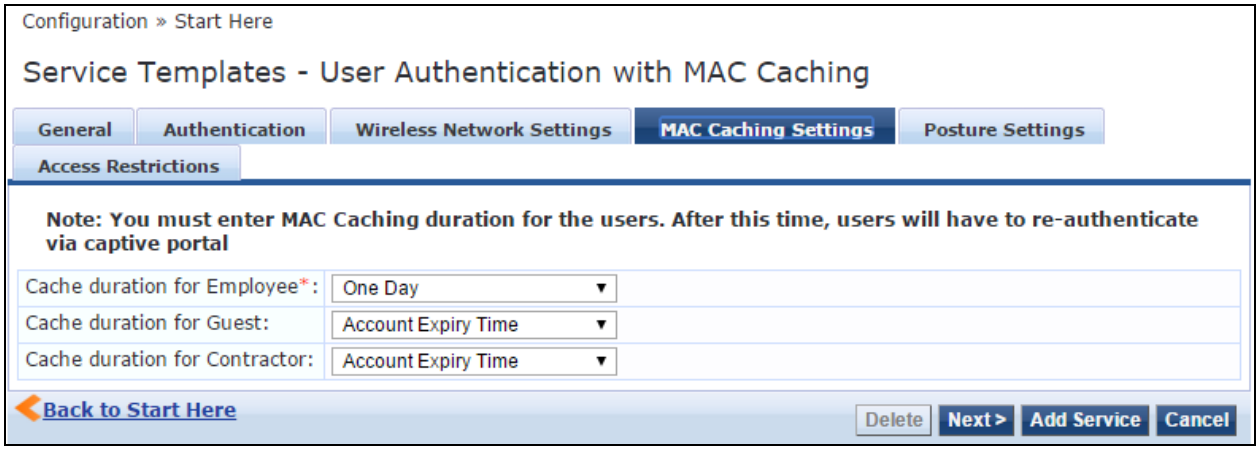
Figure 22 *Posture Policies, Ubuntu in Linux Posture Configuration*



- ClearPass now supports two new event type formats, CEF (Common Event Format) and LEEF (Log Event Extended Format). On the **Administration > External Servers > Syslog Export Filters** configuration form, the **Export Event Format Type** field includes the **LEEF** and **CEF** options in addition to the **Standard** option. (#25764)
- The **Certificate Trust List** at **Administration > Certificates > Trust List** now includes Alcatel root certificates. These are disabled by default, and can be enabled as needed. An Alcatel root certificate allows Alcatel Lucent IP phones to authenticate via EAP-TLS. (#25782)
- The Linux Posture plugin was modified to simplify AV health class configuration under each Linux distribution. (#25792)
- The following Graphite counters were added to the RADIUS server: (#25862)
  - Kerberos Authentication Time
  - Number of RADIUS Accounting Packets Processed
  - Number of Timed Out Requests
  - RADIUS Accounting Packets Processed
  - RADIUS Duplicate Packets Received
  - RADIUS Policy Evaluation Time
  - RADIUS Service Evaluation Time
  - Time Taken for a RADIUS Request Process
  - Time Taken to Verify the Certificate Against OCSP Server
- A new MAC Caching service template was added. Instead of using Insight as the authorization source, this service uses an endpoint attribute containing the MAC cache expiry date, and checks this attribute against the authentication date. If the authentication date is earlier than the expiry date, access is granted. To see

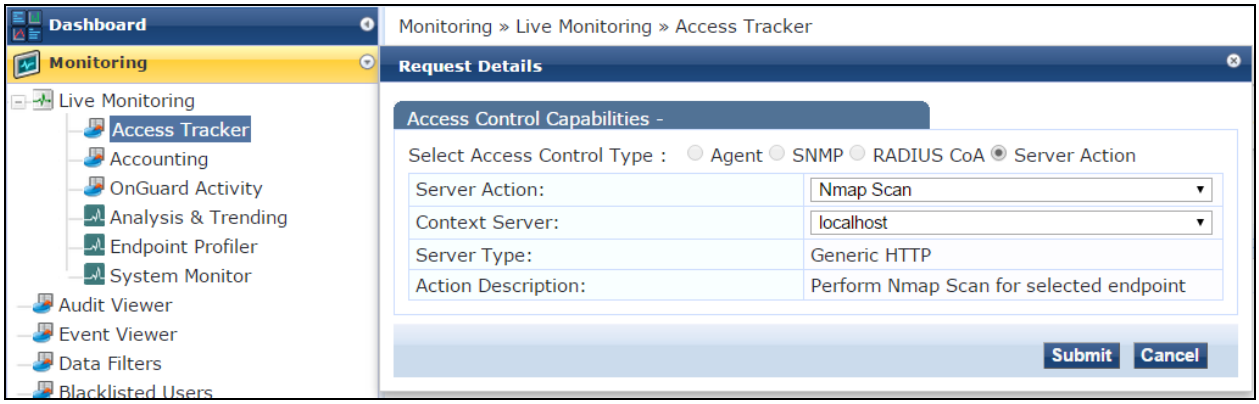
this feature, go to **Configuration > Start Here** and select the **User Authentication with MAC Caching** template. (#25900)

Figure 23 *User Authentication with MAC Caching Service Template*



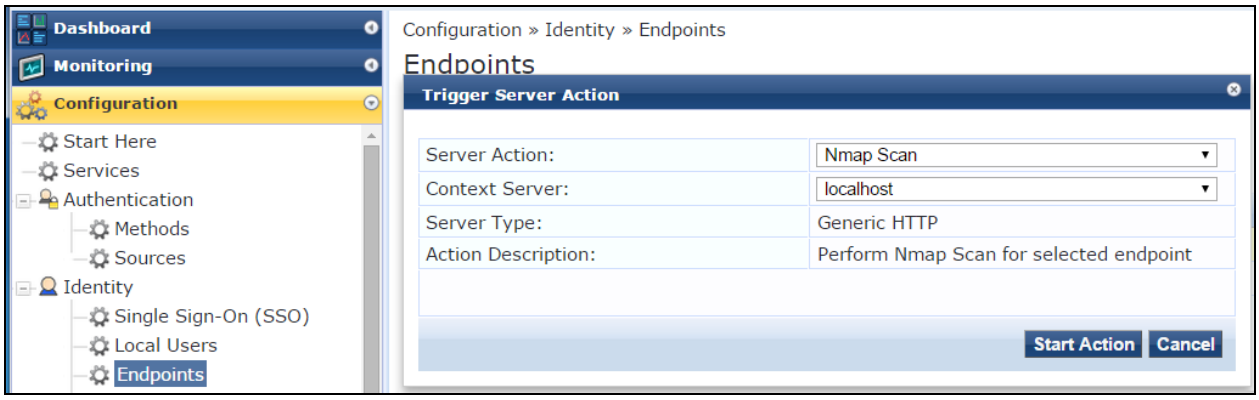
- An Nmap scan of an endpoint can now be triggered from its **Access Tracker** authentication record or **Endpoints** configuration in order to profile the endpoint. The option for the Nmap scan is only available if the endpoint's IP address is available. Only one endpoint can be scanned at a time. (#25943)
  - To use this feature from **Monitoring > Live Monitoring > Access Tracker**, click the server in the list to open the **Request Details** form. On the **Summary** tab, click **Change Status**. On the **Access Control Capabilities** tab, select the **Server Action** radio button. Select **Nmap Scan** in the **Select Action** drop-down list, and then click **Submit**.

Figure 24 *Access Tracker, Trigger Nmap Scan of Endpoint Option*



  - To use this feature from **Configuration > Identity > Endpoints**, mark the check box for the endpoint in the list and click **Trigger Server Action**. In the **Server Action** drop-down list select **Nmap Scan**, and then click **Submit**.

Figure 25 *Endpoints, Trigger Nmap Scan of Endpoint Option*



- An alert is now shown in the Access Tracker if an enforcement action fails with an error code returned from the external context server. Alerts indicate the details of the HTTP request, and are shown on the **Alerts** tab of the **Request Details** form when you select a server in the list at **Monitoring > Live Monitoring > Access Tracker**. (An example of an enforcement action would be an HTTP enforcement invoking a GET/POST/PUT to an external context server such as a generic HTTP server or an MDM context server) (#25972)
- ClearPass Profile can now determine device type using TCP OS Fingerprinting. It also uses ARP (Address Resolution Protocol) packets to get the MAC:IP binding. To support TCP fingerprinting, the **Administration > Server Manager > Server Configuration > System tab > Span Port field** now includes an **Enable TCP fingerprinting** check box. This option is disabled by default. When the check box is selected to enable TCP fingerprinting, a warning message is displayed that advises the user of the potential impact on system performance. TCP session-based fingerprinting is a CPU-intensive operation, and the server should not be used for request processing while this option is enabled. (#25984, #26168)
- A new service template, Device MAC Authentication, was added. This service template can be used for plain device accounts that do not have a user directly associated with them. (#26033)
- Support was added for notifications to registered subscribers when a device profile changes. (#26106)
- New UI options and CLI commands let users perform on-demand cleanup operations. In addition, the system checks disk utilization every hour and purges data if the configured disk threshold is met: (#26121, #24005)
  - To use this feature in the UI, go to **Administration > Server Manager > Server Configuration**, select the radio button in the rows of the servers you wish to clean up, and click the **Cleanup** button. A pop-up window lets you specify, in days, the age of the files to remove. File types that are removed include:
    - System and application log files
    - Past authentication records
    - Audit records
    - Expired guest accounts
    - Past auto and manual backups
    - Stored reports
  - To use this feature in the CLI, the new **system cleanup** command performs on-demand cleanup. The new **system sysinfo** command provides information on disk and memory utilization.
- New endpoint attributes capture information about endpoints that have generated threat events. Administrators can create policies based on a threat's category, risk, or severity level, or a combination thereof. A device's threat resolution status can also be captured for logging purposes. The attributes are

shown in Table 4, and are available in the Attributes dictionary (**Administration > Dictionaries > Attributes**) (#26222)

Table 4: *New Endpoint Attributes for Threat Information*

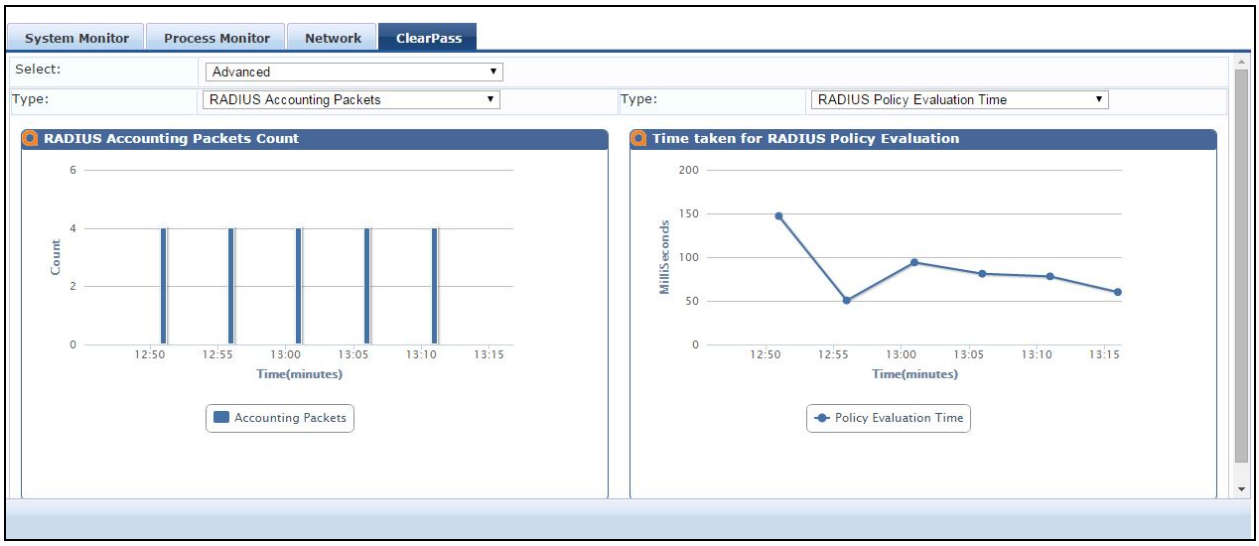
Endpoint Attribute	Data Type
[Threat Category]	String
[Threat Detection Device IP]	IPv4Address
[Threat Detection Device Name]	String
[Threat Name]	String
[Threat Risk]	Integer32
[Threat Severity]	List
[Threat Status]	List
[Threat Timestamp]	Date-Time

- User passwords are now stored as password hashes instead of the reversible AES-256 encrypted form. This feature also supports MSCHAPv2 authentication. As part of this feature: (#26288, #26310, #26324, #26325, #26346)
  - Support was added for password hash-based user authentication for SQL authentication sources.
  - Async netd modifications were made to support hashed admin user passwords.
  - PostAuth modifications were made to support hashed user passwords.
  - API modifications were made to support exporting password hash fields.
  - An option is provided to store password hashes in a format compatible with MSCHAP authentication. This can be controlled from a cluster-wide parameter.

If you disable this feature, RADIUS MSCHAP authentications against the Local User and Admin User repositories are not possible because NTLM hashes are reset for all local and admin users. To re-enable RADIUS MSCHAP authentication against the user repositories, you must reset all the affected passwords in addition to enabling this feature.

- The RADIUS server was modified to integrate with Vasco IdentiKey Authentication Server. The changes also ensure that the State attribute does not contain any non-printable (non-ASCII) characters. (#26320, #27103)
- New System Monitoring graphs are available. To view these graphs, go to **Monitoring > Live Monitoring > System Monitor** and click the **ClearPass** tab. Select the new **Advanced** option, and then select the **Type**. The following graph types were added: (#26362)
  - RADIUS Accounting Packets processed
  - RADIUS Duplicate Packets received
  - Time taken to verify the certificate against OCSP server
  - RADIUS Policy Evaluation Time
  - RADIUS Service Evaluation Time
  - Number of RADIUS timed out requests

Figure 26 *System Monitoring, Advanced Graphs*



- The following RADIUS counters are now logged at the INFO level instead of the DEBUG level: (#26419)
  - Service Categorization Time
  - User Lookup time in rlm_ldap and rlm_sql modules
  - User authentication time in rlm_mschap module
  - Policy Evaluation time
  - End-to-End request processing time
- A new Service Template, **Guest Social Media Authentication**, was added to provide a step-wise wizard for easy setup of CPPM policies that allow social logins for Guest access.(#26434)
- The RADIUS dictionary was updated with the latest information for all CheckPoint platforms. (#26616)
- For users who connect to a Microsoft SQL server using Integrated Authentication, the login username in the authentication source now allows the backslash (\ ) and at-sign (@) characters in addition to the hyphen and underscore characters. Only the DOMAIN\\Username format is supported for Integrated Authentication (UPN format is not supported). To use this feature, go to **Configuration > Authentication > Sources > Add** and create a new source of type **Generic SQL DB**. On the **Primary** tab, enter the username in the format DOMAIN\\Username in the **Login Username** field, and select **MSSQL** in the **ODBC Driver** field. (#26670)
- A new **Endpoint Details API** can be used to query the endpoint attributes for a given IP address or MAC address. The admin should always use this API on nodes where Insight is enabled, and make sure that RADIUS accounting is enabled. The following endpoint attributes can be retrieved using this API: (#26778)
  - `mac`
  - `ip`
  - `user`
  - `device_category`
  - `device_family`
  - `device_name`
  - `is_online`
  - `updated_at`

- To improve the efficiency of error handling, ClearPass now excludes the following errors from the Active Directory errors that are used for recovery actions: (#26946)
  - 0xC000006D - STATUS_LOGON_FAILURE
  - 0xC000006E - STATUS_ACCOUNT_RESTRICTION
  - 0xC000006F - STATUS_INVALID_LOGON_HOURS
  - 0xC0000071 - STATUS_PASSWORD_EXPIRED
  - 0xC0000072 - STATUS_ACCOUNT_DISABLED
  - 0xC0000064 - STATUS_NO_SUCH_USER
  - 0xC000006C - STATUS_PASSWORD_RESTRICTION
  - 0xC000006A - STATUS_WRONG_PASSWORD
  - 0xC0000193 - STATUS_ACCOUNT_EXPIRED
  - 0xC0000234 - STATUS_ACCOUNT_LOCKED_OUT
  - 0xC0000224 - STATUS_PASSWORD_MUST_CHANGE

Dissolvable Agent

- The `OnGuard Mac Health Checker.dmg` file for the Mac OS X Native Dissolvable Agent now uses the Native Agent Installer instead of the Native Agent App. This allows users to easily uninstall the agent. (#25063)
- The Native Dissolvable Agent is now supported for the Ubuntu operating system with the Firefox browser (it is not supported for the Chrome browser). The following Ubuntu OS versions are supported:
  - 12.04 32-bit LTS
  - 12.04 64-bit LTS
  - 14.04 32-bit LTS
  - 14.04 64-bit LTS

  For more information, see #20656 under "OnGuard" on page 53. (#25271)
- To uninstall the Native Agent from Mac OS X, you can now run the following command: (#27163)

  ```
  open ~/Library/Application\ Support/ClearPassWebAgent/Uninstaller.app/
  ```

Endpoint Context Servers

- ClearPass now provides the ability to turn off HTTP Basic authentication for context server actions, and to specify user credentials as Action Attributes. To see this feature, go to **Administration > Dictionaries > Context Server Actions** and either click a server type in the list or click **Add** to add a new server. The **Endpoint Context Server Details** window opens. (#18919)
  - To use the HTTP Basic authentication option, on the **Action** tab, use the check box in the **Skip HTTP Auth** field to enable or disable HTTP Basic authentication.
  - To use the Action Attributes option, on the **Attributes** tab, add the attributes in the following formats:

Table 5: *Options for HTTP Basic Authentication and User Credentials as Action Attributes*

Attribute Name	Attribute Value
Server Name	%{Server.Name}
User Name	%{Server.UserName}
Password	%{Server.Password}

- The Event Viewer at **Administration > External Servers > Endpoint Context Servers** now includes a **Poll Status** tab for MDM polling information. This tab is available when editing the context server if MDM is enabled for polling and if at least one poll has been completed. (#24225)

  Information shown on the Poll Status tab for a successful poll includes:

  - Last poll status
  - Last successful poll time
  - Total elapsed time for polling MDM and posting endpoints to ClearPass
  - Number of endpoints (fetched from MDM)
  - Number of invalid endpoints (invalid MAC addresses or duplicates)
  - Number of endpoints updated to ClearPass
  - Number of incomplete device profiles (missing category or family information, or device model not present in dictionary)
  - Number of device profiles updated in ClearPass

  Information shown on the Poll Status tab if the poll fails includes:

  - Last poll status
  - Last successful poll time
  - URL that MDM was trying to access
  - HTTP status code
  - Reason for failure

- ClearPass now supports the Google Administration Console as an MDM External Context Server. To use this feature, a project must first be created in the Google Developer Console, and then the Google Admin Console can be added as a context server in ClearPass Policy Manager. The procedures are described below. (#24499)

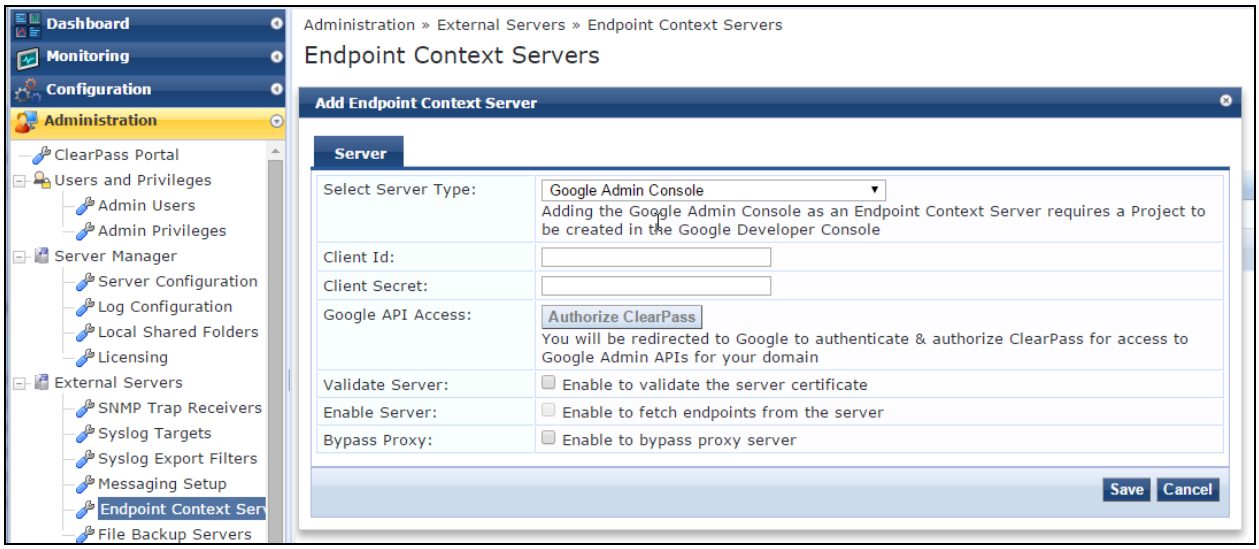
  Steps in the Google Developer Console:

  1. Make sure to enable **Admin SDK API**.
  2. Create a new **Client ID** and **Client Secret** (select **Web Application** as the **Application Type**).
  3. Create a **Consent Screen** with the desired logo and text (This screen is seen by the ClearPass administrator when authorizing ClearPass Policy Manager - more below).
  4. Add **Redirect URIs**. This is of the format **https://<clearpass-server>/async_netd/mdm/oauth/google**, where "clearpass-server" should be a fully qualified domain name (FQDN) and not an IP address. This server should be reachable by that FQDN by the device the administrator is using to access the ClearPass Admin UI over a Web browser.
  5. Configure the domain's security setting to allow API access.

Steps in ClearPass Policy Manager:

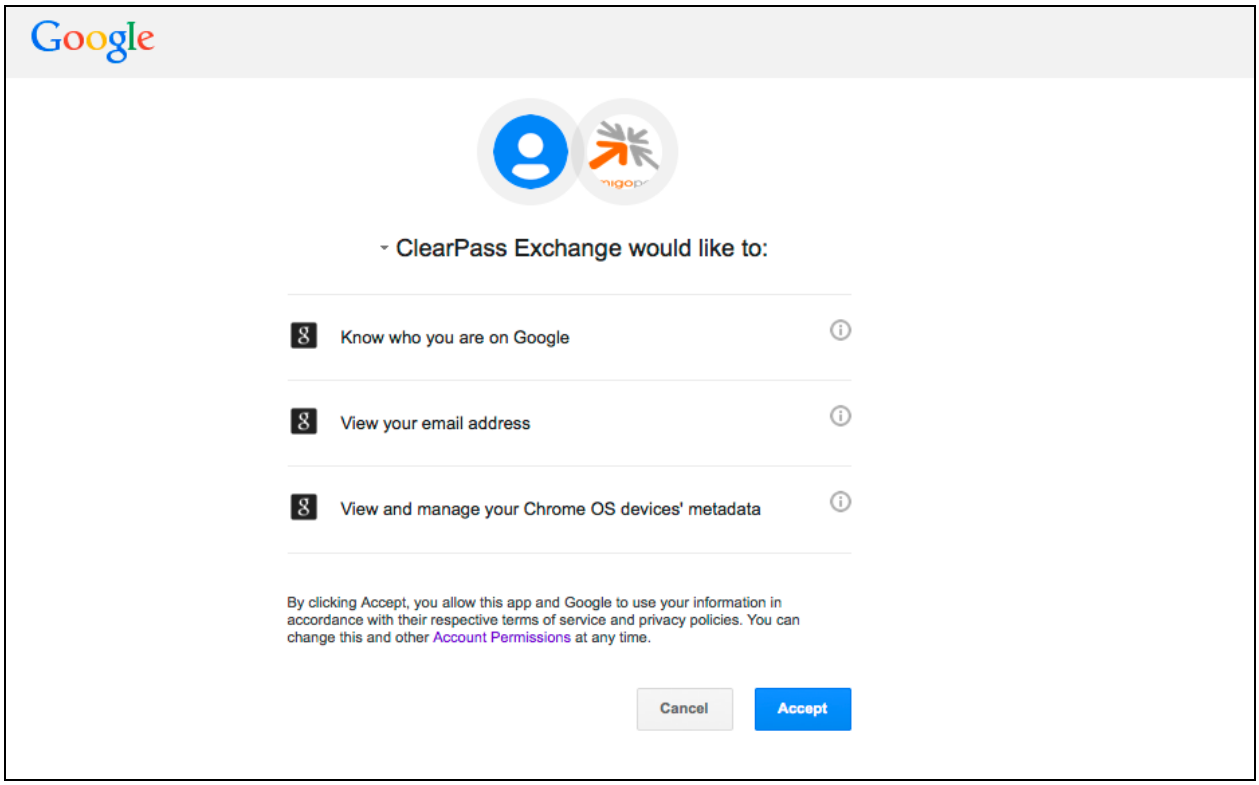
1. Go to **Administration > External Servers > Endpoint Context Servers > Add**. On the **Server** tab, select **Google Admin Console** in the **Select Server Type** drop-down list.

Figure 27 *Google as MDM External Context Server, Configuration*



2. Enter the valid **Client ID** and **Client Secret** that were configured in the Google Developer Console.
3. Click **Save** to save the Client ID and Client Secret. This also enables the Authorize ClearPass button.
4. Click **Authorize ClearPass**. The Google page for entering the username and password for the Google domain (account) opens in a new tab or window.
5. Enter the credentials. A consent screen (the one that was set up in the Google Console steps) is displayed, where you will be given the choice to authorize ClearPass to communicate with the Google Admin Console to fetch the MDM data for the Google Chrome Devices registered with the domain.

Figure 28 *Google Consent Screen*



6. After the approval, the status of the operation is displayed — either that a "Refresh Token has been fetched and saved", or an error message.
7. You can return to the main ClearPass Admin UI window and make additional selections (such as enabling ClearPass to poll for MDM data) before you click Save to save the settings.

When all configuration is complete in the Google Developers Console and in CPPM, subsequent MDM polling cycles will fetch the MDM data for the Google Chrome Devices and add that to the endpoints, profiling data to use with functionality of ClearPass Policy Manager, such as in creating and configuring policies and services. The details of the devices fetched can be seen from several places in the UI. The figures below show details of a Google Chrome Device whose MDM data was fetched by ClearPass from the Google Admin Console. This information is displayed when an endpoint row is clicked at **Configuration > Identity > Endpoints**. The list of devices (rows) on can be filtered by using the filter attribute **Source > contains > Google Admin Console**.

Figure 29 *Google as Endpoint Context Server, Edit Endpoint*

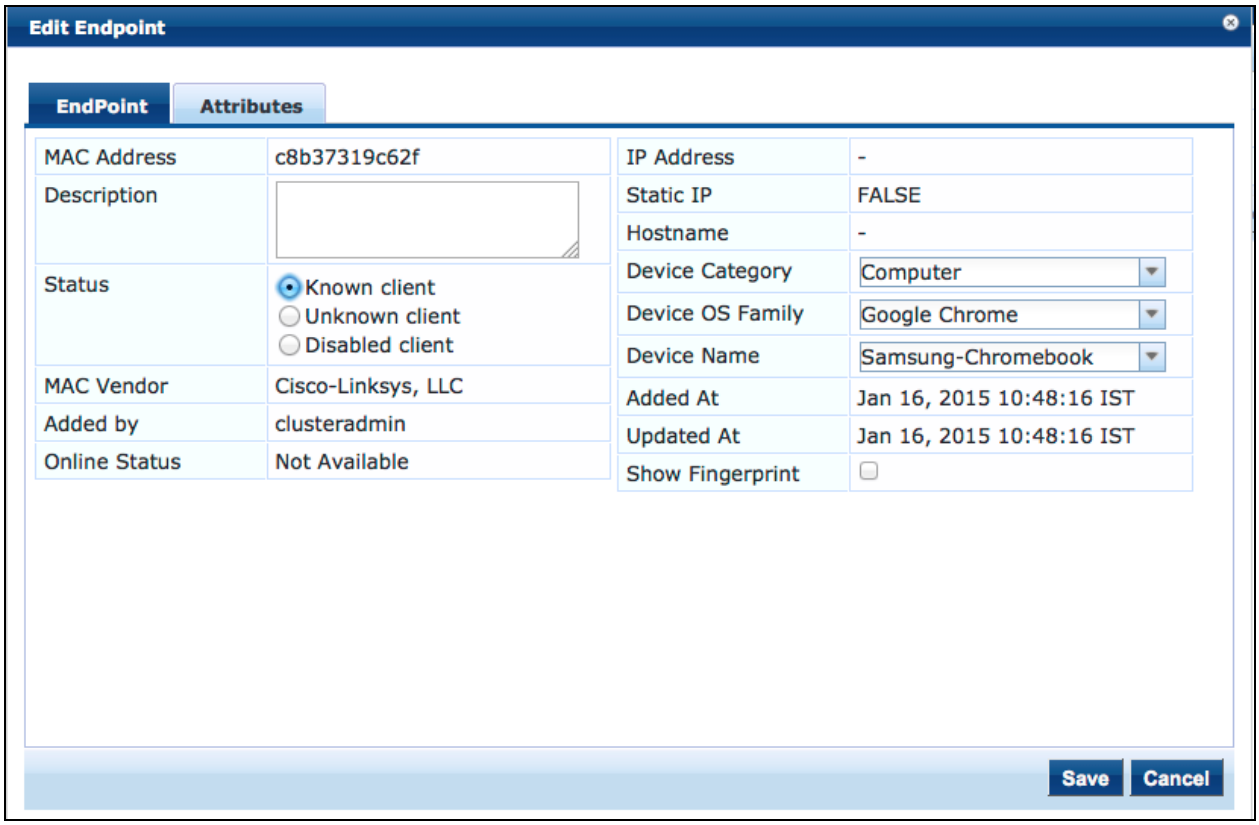
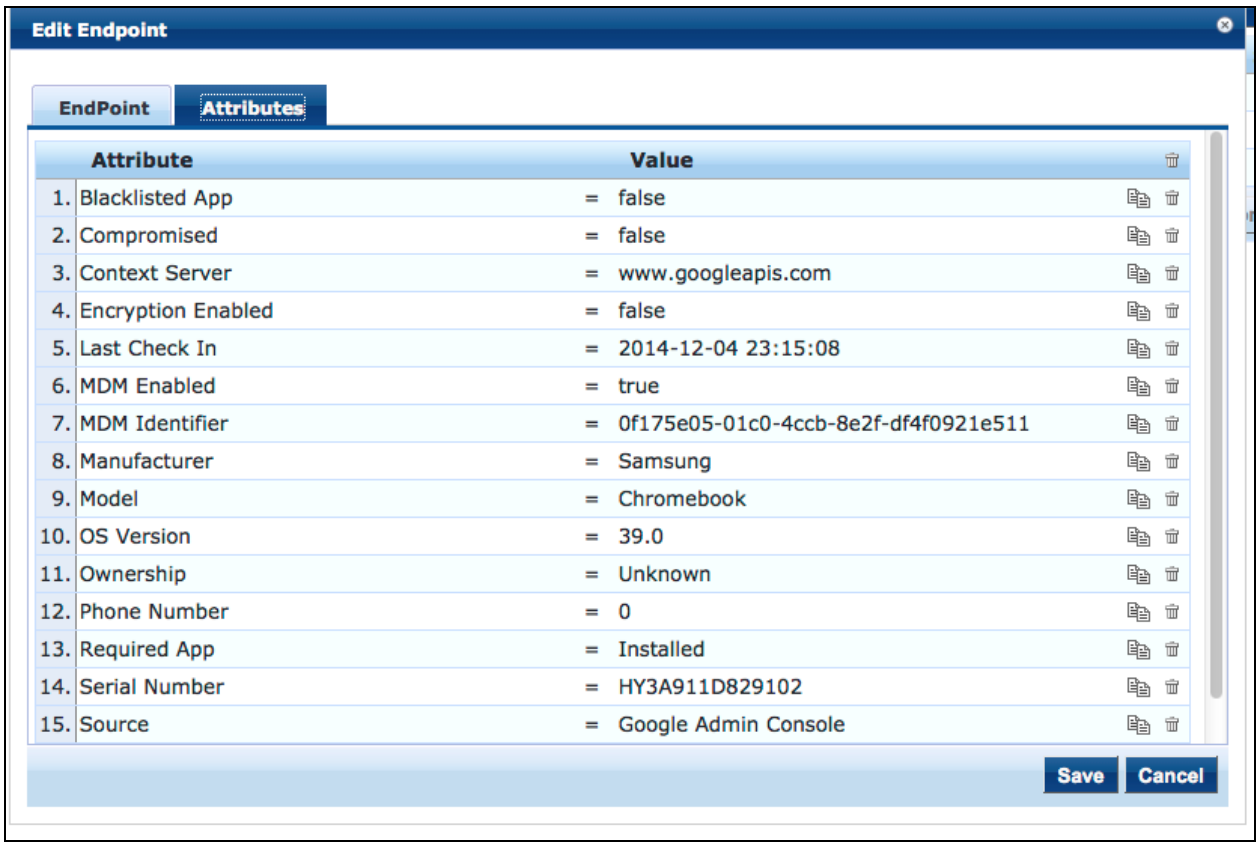


Figure 30 *Google as Endpoint Context Server, Edit Attributes*



- A new enforcement profile, **Session Notification Enforcement**, is introduced in 6.5.0. Notification of a change in IP address can now be sent to any external context server (such as a firewall) by configuring that server as a generic HTTP server and adding the appropriate generic HTTP context server actions. The content of the payload to be posted by CPPM to the external server is based on the REST API defined by the external server for communication. (#24508, #24509)

  Prior to 6.5, session restrictions enforcement allowed a Palo Alto Firewall device to be added as a value for an attribute of type "Session-Check" and name "IP-Change-Notify". When used as part of a policy and service, that profile let CPPM notify the firewall when users logged in or out of the network. In the 6.5.0 release, the new enforcement profile type, **Session Notification Enforcement**, provides the same functionality not only for Palo Alto firewalls but also for firewalls for other vendors. It replaces the IP-Change-Notify attribute, which will no longer be supported. Any pre-6.5.0 configuration will be migrated to the new enforcement type during upgrade to 6.5. Three different configuration options are described in the tables below.

Table 6: *Session Notification Enforcement Configuration: PANW Integration*

Field	Configuration
Session-Notify Server Type	Palo Alto Networks Firewall
Session-Notify Server IP	<IP ADDRESS>

Table 7: *Session Notification Enforcement Configuration: PANW Integration Extended to Guest MAC Caching*

Field	Configuration
Session-Notify Server Type	Palo Alto Networks Firewall
Session-Notify Server IP	<IP ADDRESS>
Session-Check Username	%{Endpoint:Username}

Table 8: *Session Notification Enforcement Configuration: Generic HTTP Servers (Check Point)*

Field	Configuration
Session-Notify Server Type	Generic HTTP
Session-Notify Server IP	<IP ADDRESS>
Session-Notify Login Action	Check Point Login
Session-Notify Logout Action	Check Point Logout

To use this new enforcement profile type, go to **Configuration > Enforcement > Profiles > Add**. On the **Profile** tab, select **Session Notification Enforcement** in the **Template** drop-down list. On the **Attributes** tab, select the **Session-Notify** type.

Figure 31 *The New Enforcement Profile, Session Notification Enforcement*

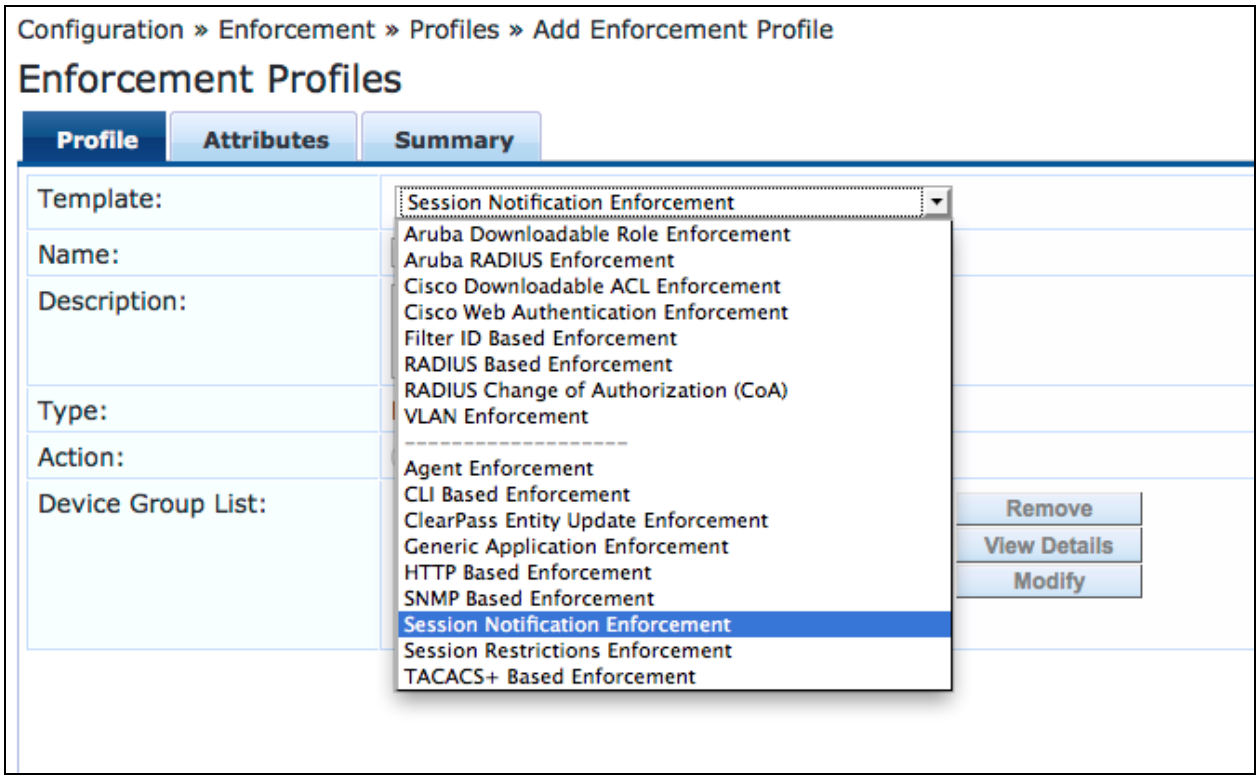
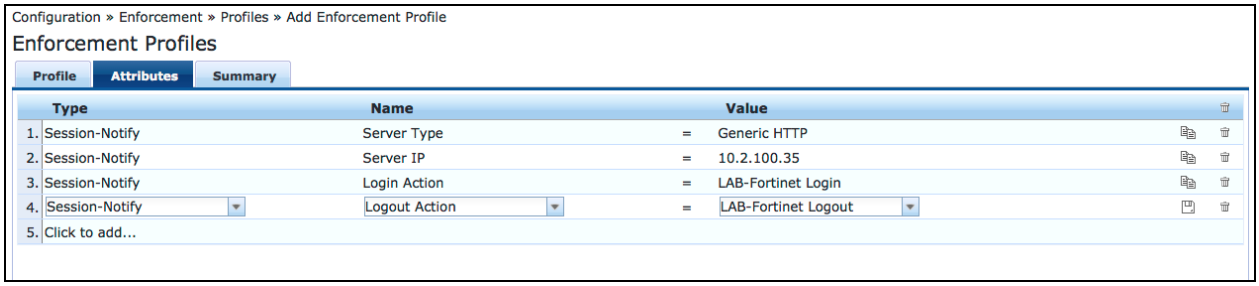


Figure 32 *The Session-Notify Attribute*

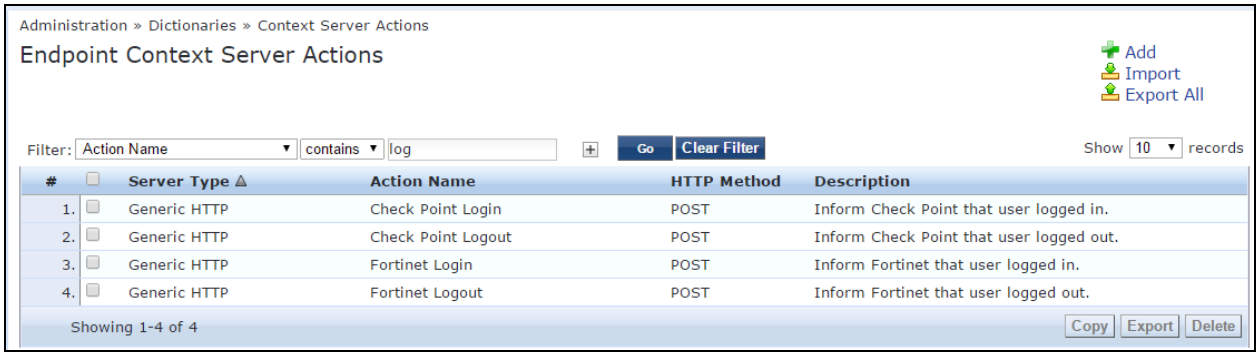


- MobileIron MDM integration was updated to the 5.5 VSP release API specification, improving the device discovery logic for large deployments (tens of thousands of managed devices). Device discovery is now much faster and timeout issues are eliminated. (#24690)
- The server configuration form at **Administration > External Servers > Endpoint Context Servers** now includes a **Bypass Proxy** option. An administrator can select this option to specify that the endpoint context server should not use the configured proxy settings (if a proxy is used). ClearPass would then bypass the proxy for functions such MDM API, Endpoint Context Server Actions, or Generic HTTP outbound enforcement. (#25686)
- ClearPass now lets you configure multiple endpoint context servers of the same server type. To use this feature, go to **Administration > External Servers > Endpoint Context Server > Add** and select the **Server Type**. A new attribute to identify the server from which the endpoints are fetched was added to the dictionary at **Administration > Dictionaries > Attributes**. This attribute, **Context Server**, is populated with the Server Name value of the endpoint context server the endpoint is fetched from.(#25826)
- New generic HTTP context server actions are available. They can be used in conjunction with CheckPoint and Fortinet firewalls that are configured as external context servers in order to communicate end user logins and logouts in the form of session notification enforcement. To use this feature, go to

Administration > Dictionaries > Context Server Actions. In the **Filter** drop-down lists, select **Action Name > contains > Log** and click **Go**. The following server actions were added: (#26682)

- Check Point Login
- Check Point Logout
- Fortinet Login
- Fortinet Logout

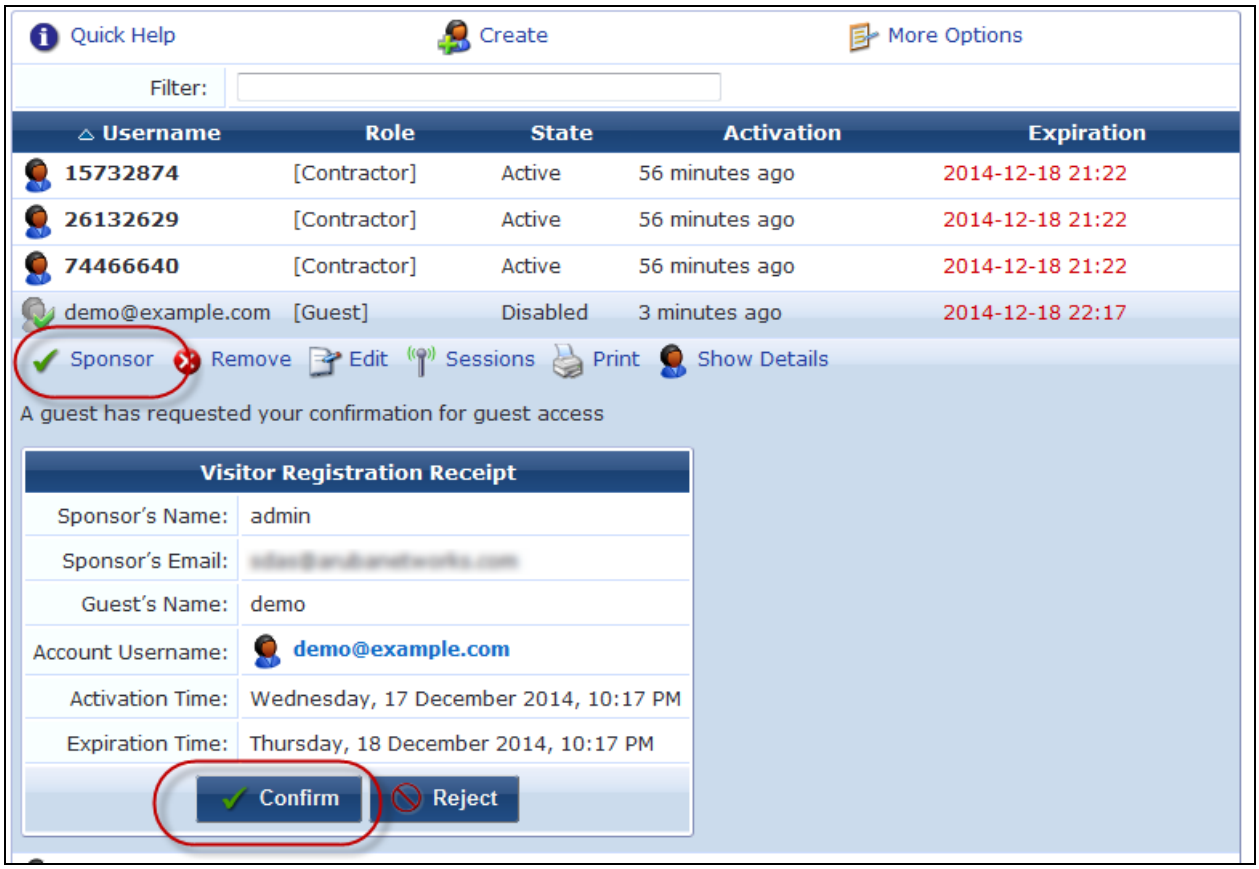
Figure 33 *Context Server Actions*



Guest

- Support was added to Transaction Services for the following Property Management Systems (PMS): (#19271, #23108, #25239)
  - Agilysys hotel PMS
  - Protel PMS
- A new Web Analytics plugin was added. This plugin can be used to inject a Web analytics tracking code into guest-facing application pages. This functionality does *not* collect any user information. (#20552)
- The sponsor can now confirm or reject a guest account or device account directly from the **Guest > Manage Accounts** or **Guest > Manage Devices** page, respectively, instead of by email. To configure this option, go to **Configuration > Pages > Guest Self-Registrations** and click the **Edit** link for a Guest Self-Registration (GSR). In the diagram, click the **Sponsor Confirmation** link. Select the **Enabled** check box for sponsorship confirmation and save your changes. Register the guest account. On the **Guest > Manage Accounts** list, the account's row will include the **Sponsor** link. (#20633)

Figure 34 *Sponsor Confirmation for Guest Access*



- The PHP opcode cache was updated to OPcache 7. (#21188)
- **Web Pages** was added to **Configuration > Pages**. You can manage your list of custom Web pages and create simple new custom pages. The Web Pages list also provides four page templates: **Browser Unsupported**, **Jailbroken Device**, **Posture Check**, and **Service Unavailable**. (#24439)

NOTE

If you have configured Bulk SMS as your SMS provider, the outgoing port has changed from TCP port 5567 to TCP port 80. Please review any firewall settings you may have configured. An override is available in the **Configuration > SMS Services > Gateways** configuration form to override the default port. (#24453)

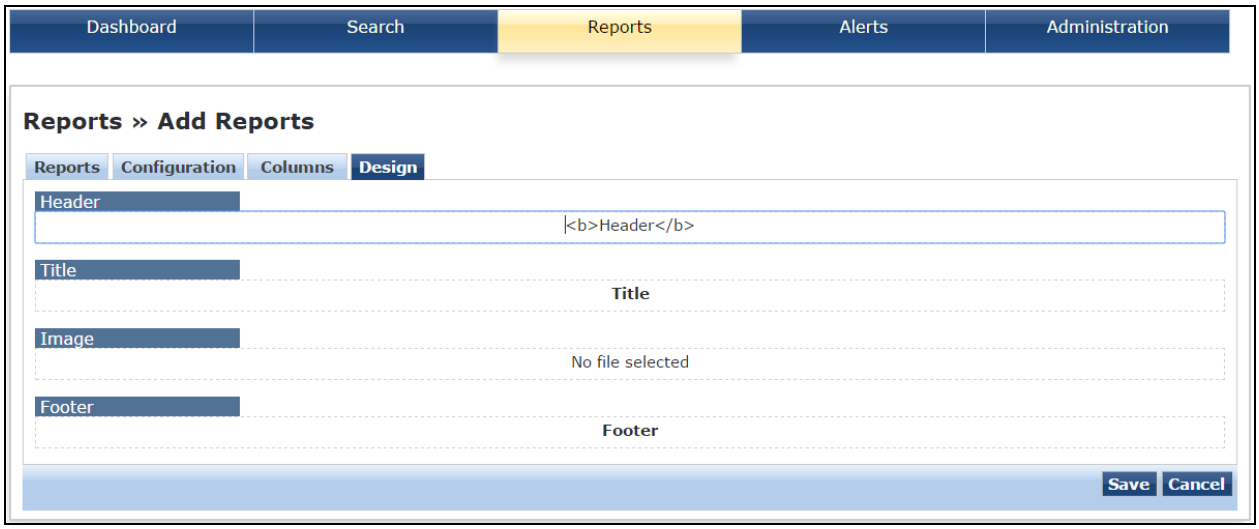
- The **Self-Service Portal** summary page now displays the NAT IP if it is available in the authentication session of the user. (#25165)
- Transaction processors using the FIAS protocol will now adhere to the No Post NP flag and deny access. Previously guests were still able to attempt a charge or otherwise be granted access. (#25240)
- Support was added for the Media4u SMS gateway (Japan). (#25551)
- The **Administration > API Services > API Clients** page includes a new link, **API Explorer**, that provides access to the various APIs used for configurations in Guest and Onboard. (#25556)
- The **Guest > Active Sessions > Show Details** window now includes the ClearPass Policy Manager service and the session ID of the user's connection. The **Service Type** and **SSID** fields can be added to the **Guest > Active Sessions** list as a custom view. To add these columns, click the **More Options** link above the table, click **Choose Columns**, click the field name you want to add, and then click **Enable Field**. (#25633)
- Two new skins have been added to the list of available skins at **Administration > Plugin Manager**. The **Galleria Skin** and **Galleria Skin 2** provide a customizable and dynamic full-screen user experience for guests. (#25672)

- In Transaction Processor configuration, for matching names against Property Management Systems (PMS) you can now configure how many characters of the name require matching. To use this feature, go to **Configuration > Hotspot Manager > Transaction Processors** and open the configuration form for a new or existing processor. In the **Processing Gateway** drop-down list, select one of the PMS providers. In the **Name Match** field, you can specify either an exact name match or matching just the first 3, 4, 5, 6, or 7 letters of the last name. (#25783)
- The performance of captive portal pages was improved. (#25965)
- When you configure a guest self-registration to use a Facebook Wi-Fi social login, a new option lets you enable a RADIUS Change of Authorization (CoA) when the guest's session expiration time is reached. To use this feature, go to **Configuration > Pages > Guest Self-Registrations > Advanced Editor link**. In the **Customize Guest Registration** page, scroll to the **Social Logins** area and select the check box in the **Social Login** row, and then select the Advanced check box. The new **Disconnect Action** drop-down list specifies the action to take when a disconnect is requested by Facebook. If a CoA Enforcement Profile is selected, it must be compatible with the NAD the guests are connecting to. (#26001)
- When **Single Sign-On _ SAML Identity Provider** is selected in the **Vendor Settings** field at **Configuration > Pages > Web Logins**, a new configuration option, **Client Certificate**, lets you request a client certificate from the user to be used for authentication. (#26046)
- Access control lists in Guest and Onboard now support IPv6 addresses in addition to IPv4. These access control lists include any "allow access", "deny access", or "enable access" fields , found on forms such as **Web Logins**, **Guest Self Registration**, **Provisioning Settings**, or the SCEP server settings in **Certificate Authority Settings**. (#26079)
- Significant performance enhancements were made to guest-facing pages such as Web Logins and Guest Self-Registration pages, improving performance by 32% to 166% more requests per second. (#26119)
- Support was added for specifying security options for Cross-Origin Resource Sharing (CORS). This applies to API requests made from Web applications. The default is to not permit any cross-origin requests. To configure this behavior, you can specify a list of hostnames, optionally including wildcards, at **Administration > Plugin Manager > API Framework > Configuration > Allowed Origins**. (#26179)

Insight

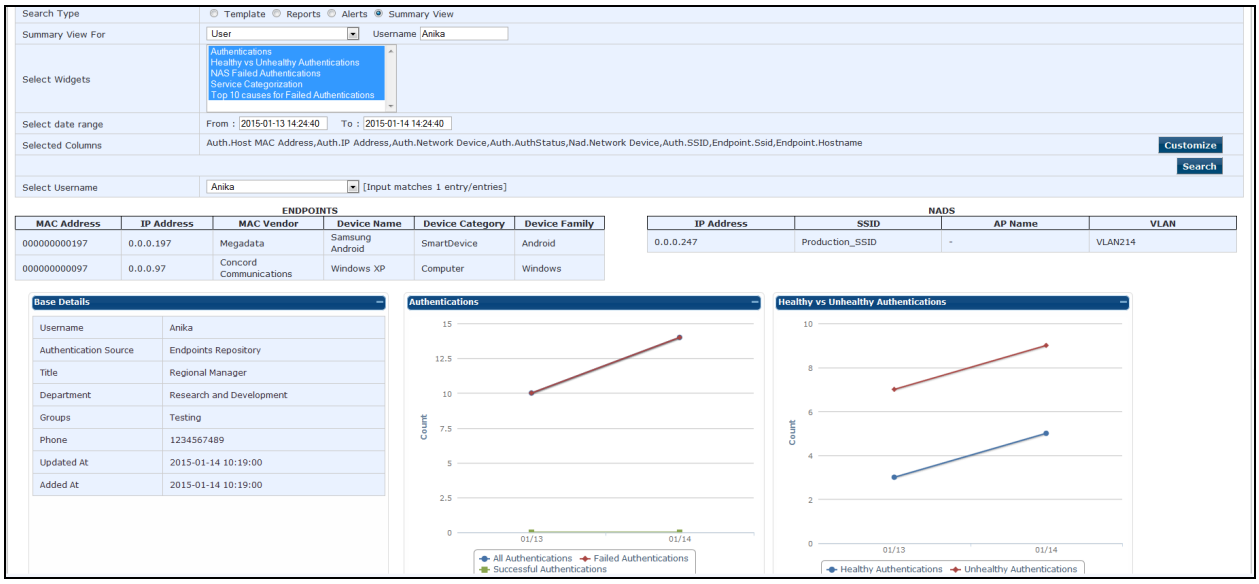
- Support was added for WYSIWYG graphical report design in Insight. This feature includes the following changes: (#20541)
  - On the Insight **Dashboard**, a **Report** button was added. You can click this button to open the **Add Reports** form and generate a report of the currently-displayed Dashboard widgets.
  - On the **Add Reports** form, you can add a Dashboard report by selecting the new **Dashboard** template. The report uses the current Dashboard widgets in the configuration. To change the widgets in the report, first change them in the Dashboard and then return to the report configuration.
  - The **Add Reports** form also includes a new **Design** tab. You can click the **Header**, **Title**, or **Footer** row to edit the HTML, or the **Image** row to add a file.

Figure 35 *Insight Reports, Design Tab*



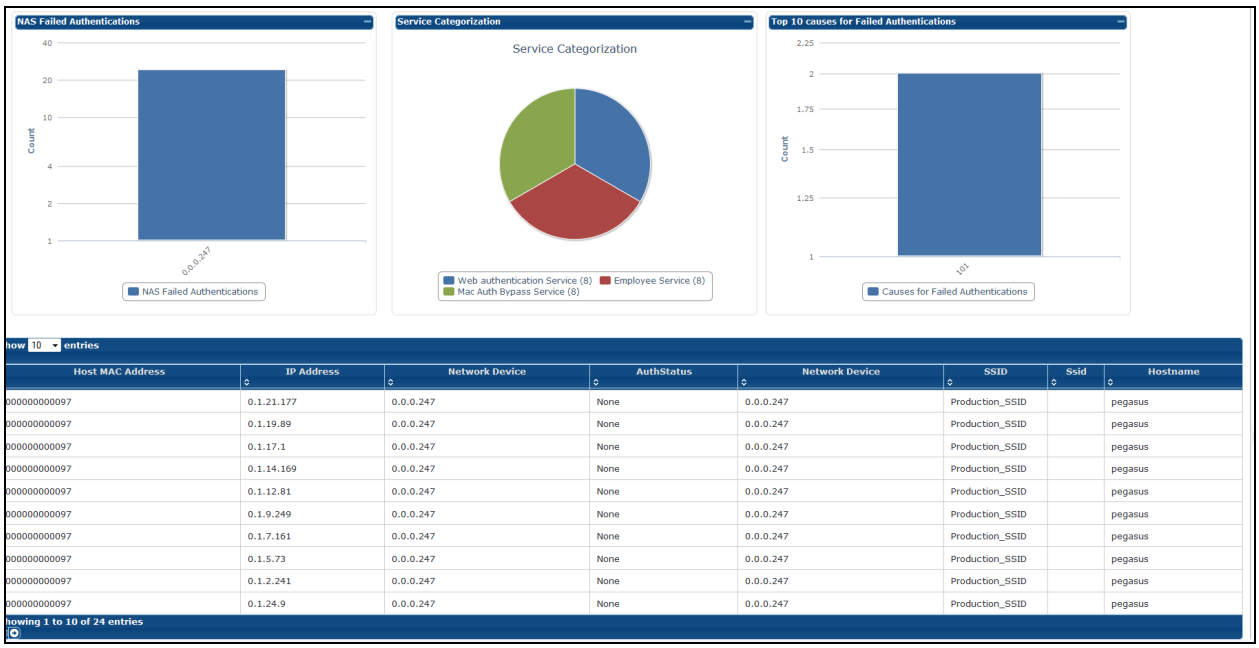
- Insight reports now support OnGuard Agent **Type** and **Version** fields in WebAuth reports. (#22689)
- A new template, **Endpoint Latest**, was added to Insight report configuration to allow reporting on location attributes. (#23219, #24079)
- A new template, **MAB**, is now supported in Insight report configuration for MACAUTH BYPASS reports. (#23421)
- A new widget, **Insight Disk Usage**, was added to the Insight Dashboard. It displays Insight resource consumption statistics such as disk usage of the Insight DB and the Reports Directory. (#23620)
- A sample report can now be viewed for each of the template types within a template group. In the **Select Template** field on Insight's **Reports > Configuration** tab, the **Sample Report** link downloads an example of the selected report in PDF format. (#25123)
- Support was added for including endpoint connection information such as Switch Port/Controller and Access Point in Insight reports. (#25422)
- Insight report configuration now displays uploaded images in the Design Tab. Support was also added for uppercase image file extensions for JPEG and PNG. GIF images are not supported. (#25514)
- Insight reports now include the following new **Posture** fields for the File Check Health class: (#25575)
  - Files Missing
  - Files Not Allowed
  - Invalid MD5 Sum Files
- Enhancements to Insight's **Search** tab provide additional information. Changes to this form include: (#26125, #26126, #20660)
  - A **Summary View** button was added to the **Search Type** options. You can configure the Summary View for and endpoint, a network device, or a user and specify the widgets to include. When you select columns and click **Save**, the details are correlated across cluster nodes in the displayed information.

Figure 36 *Summary View for a User*



- The **List View** shows details in report format and correlates details across users, endpoints, and devices.

Figure 37 *List View*



Onboard

- The guest self-registration page can now be configured to initiate Onboard device enrollment as an alternative to NAS login, allowing the guest to log in and proceed to Onboard enrollment in one step. To use this feature, go to **Configuration > Pages > Guest Self-Registrations** and click the link to either create or edit a page. In the diagram, you can either: (#9859, #25652)
  - Click **Advanced Editor**, scroll to **Login > Enabled**, and select the **Enable Onboard device enrollment** option.
  - Under **Receipt Page > Submit**, click either **Title**, **Login Message**, **Login Delay**, or **NAS Vendor Settings**. In the **Enabled** field at the top of the form, select the **Enable Onboard device enrollment** option.

- Onboard now provides the ability to require a sponsor to approve a new device that is being provisioned for the network. A field for the sponsor's email address will be added to the guest's login form below the username and password fields. When the user logs in to register their device, an email is sent to the sponsor requesting approval, and a message is displayed on the user's screen advising them that it is in process. To set up the email to the sponsor, first go to **Onboard > Deployment and Provisioning > Provisioning Settings > Web Login tab**, click in the **Custom Fields** text box, and select **Sponsor's Email: (sponsor_email)** from the drop-down list. Next, click the new **Sponsorship Confirmation tab** and then click the **Enabled** check box. Options on this tab let you specify provisioning settings related to sponsorship confirmation and UI overrides. (#11912)

Figure 38 *Message Displayed to User*

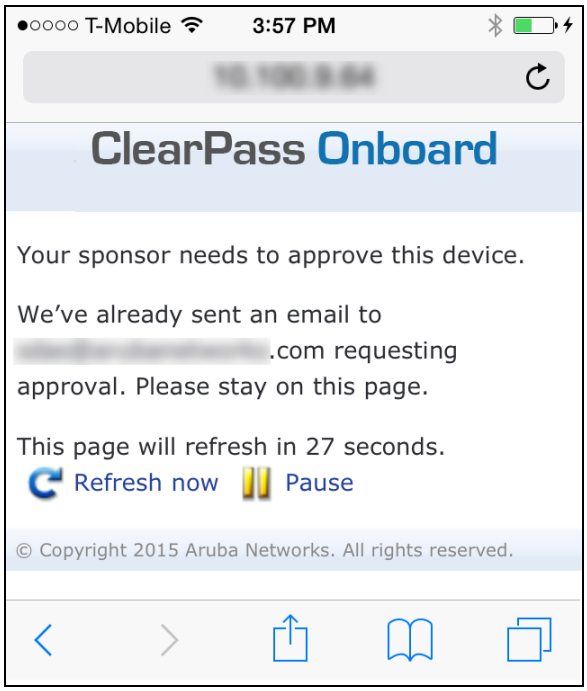
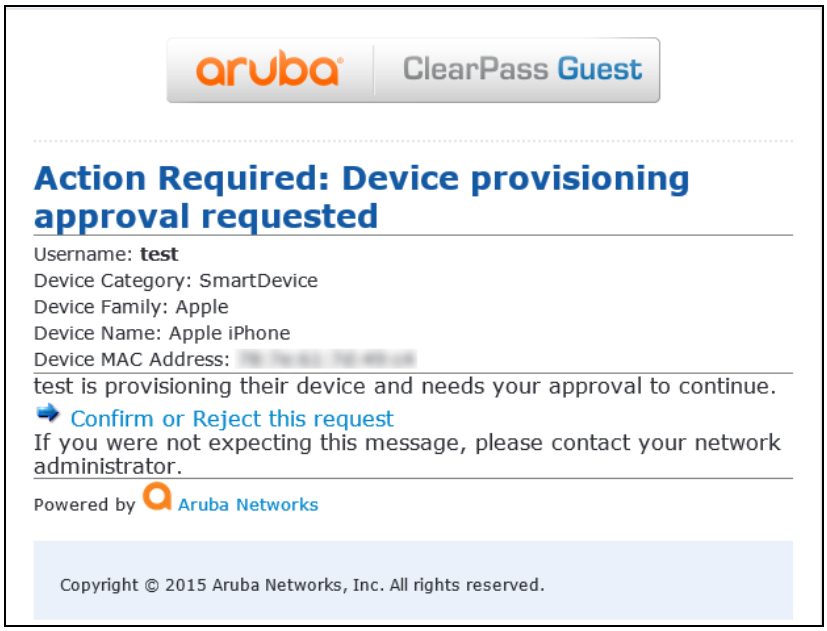


Figure 39 *Email Sent to the Sponsor*



- The list of available settings you can configure for an iOS device at **Onboard > Configuration > iOS Settings** now includes **Device Restrictions Settings**. (#12402)
- Automatic cleanup options were added for Onboard certificates. In the **Actions** area of the **Onboard > Deployment and Provisioning > Provisioning Settings** form, options let you: (#14424)
  - Revoke certificates for inactive devices, specifying the period of inactivity
  - Delete duplicate certificates, specifying the number of days to wait after re-enrollment before deletion
- The default algorithm to use for the certificate authority in Onboard is now changed to SHA-512 from SHA-1 because SHA-1 digest algorithm is no longer considered fully trustworthy by many browsers. Additionally, attempting to create a certificate authority with SHA-1 results in the following warning message in the UI: (#25671)

  The SHA-1 digest algorithm is no longer considered fully trustworthy by many browsers and, if used, may result in security warnings being displayed.
- When a device is disabled or deleted through the Onboard BYOD self-service portal, active sessions for the device are now terminated. (#15599)

The {php} Smarty tag is now deprecated. Please be aware that PHP is no longer allowed in editable templates. A warning message will be displayed if you attempt to save a template that contains the {php} tag. Existing templates that include this tag will not work. (#16900)

- An error message is now displayed if a user tries to onboard an Android or iOS device with a browser that is not supported for that operating system (for example, iOS with Chrome, Dolphin, or Opera Mini). The **Onboard > Deployment and Provisioning > Provisioning Settings > Supported Devices tab** includes options to enable the browser check for Android and for iOS. For new installations, these options are enabled by default. For existing installations, these options are disabled by default. (#17164)
- In the 6.5 release, a switchip is no longer necessary in order to reconnect a device after onboarding. The device's MAC address is all that is required. (#18599)
- Onboard now provides the ability to specify different instructions for iOS and OS X provisioning. (#21007)
- Onboard now provides the ability to customize the iOS and OS X enrollment wizard's post-login instructions. (#21008)
- You can now filter devices by MDM enrollment status. A **Managed By** column was added to the **Onboard > Management and Control > View by Device** list, and the **Show Details** link for the device displays all endpoint attributes, MDM and otherwise. (#23877)
  - Windows 8
  - Windows Phone 8
  - Windows Phone 8 RT
- Onboard now provides the ability to create certificates suitable for use as HTTPS server certificates. At **Onboard > Management and Control > View by Certificate**, the **HTTPS** option is available as a certificate type when importing or creating a code-signing certificate and can be used to filter the certificate list. (#25301)
- Onboard can now use the same code-signing certificate for signing Windows applications and iOS and OS X profiles. Profile-signing certificates are no longer needed and have been removed. (#25648)
- Certificates that are currently valid can now be deleted. This has the same effect as revoking them or disabling the device. The **Delete Certificate** option is available in the certificate's row at **Onboard > Management and Control > View by Certificate**. (#25741)

- Onboard certificates can now be provisioned in a browser for manual installation on devices that do not have an Onboard client. To use this feature, go to **Onboard > Deployment and Provisioning > Provisioning Settings**. The **Supported Devices** tab now includes a **Web-Based Provisioning** section, and the **Instructions & Messages** tab includes a **Web-Based Instructions** section. (#25752)
- Onboard now provides the ability to onboard devices via social login. To use this feature, go to **Onboard > Deployment and Provisioning > Provisioning Settings > Web Login** and scroll to the **Social Logins** section. (#25754)
- The trusted servers configuration at **Onboard > Configuration > Network Settings** now defaults to the automatic setting of only trusting the common names of servers in the ClearPass cluster. (#25767)
- Onboard now provides the ability to manually override device detection for scenarios where the device cannot be accurately detected from the browser user agent. To use this feature, go to **Onboard > Deployment and Provisioning > Provisioning Settings**. Both the **Supported Devices** tab and the **Instructions & Messages** tab now include an **Override Device Type Detection** field. (#25815)
- A new page, **Usage**, was added under **Onboard > Management and Control**. This page displays usage statistics for Onboard. Information shown here includes: (#25869)
  - **License Usage**: Count representing a 30-day rolling average of the number of devices with valid certificates
  - **Devices**: For each device type, the number enrolled, not enrolled, and denied
  - **Certificates**: For each CA, the number valid, expired, and revoked
- Support was added for the Chromebook System TPM Token certificate store. To use this feature, go to **Onboard > Deployment and Provisioning > Provisioning Settings > Supported Devices tab** and scroll to **Chromebook Provisioning > Chromebook Token**. (#26570)

OnGuard

- Support was added for the following products (#26283, #26515):
  - Avast Security 2015 on Mac OS X

  Support was enhanced for the following products:
  - FileVault 10.7.x (Mac)
  - Symantec Hosted Endpoint Protection 2.x (Windows)
- A new health class, File Check, was added for both Mac OS X and Windows OS to check for the presence or absence of files. Auto-Remediation is not supported for the File Check health class. (#14032, #14034)
- The ClearPass OnGuard Unified Agent is now supported on Ubuntu OS. The ClearPass OnGuard Unified Agent Installer for the Ubuntu OS can be downloaded from **Administration > Agents and Software Updates > OnGuard Settings**. As part of support for the Ubuntu OS, the ClearPass OnGuard Unified Agent user interface now has an **OnGuard** tab and a **Common** tab, and the **Diagnostics** tab now includes **Health Logs**. Currently, only two health classes are supported for Ubuntu: Services and AntiVirus. Support for the Persistent Agent for Ubuntu was added in the Beta 1 release. In the Beta 2 release, support was added for the Dissolvable Agent, with Firefox supported on the Native Agent and Chrome supported on the Java-based Agent. (#20656, #25267, #26493)

  The system requirements, procedures, and rpm dependencies for OnGuard installation on Ubuntu are shown below:

  Supported Operating Systems

  All Ubuntu flavors based on version 12.04 or above are supported.

  Installing the ClearPass OnGuard Persistent Agent

(1) Ensure the system is up to date. Run the **`sudo apt-get update and then sudo apt-get upgrade`** command.

(2) Make sure all rpm dependencies are installed (gksudo, gdebi library dependency) prior to OnGuard installation.

(3) Download the Ubuntu **ClearPassOnGuardInstall.tar.gz** file and extract it.

(4) Select the binary installer provided for the target platform. For Ubuntu, use **clearpass-onguard-installer-< versionnumber>-ubuntu-i386** for 32 bit machines. Use **clearpass-onguard-installer-<version number>-ubuntu-x86_64** for 64 bit machines.

(5) Run the selected binary installer either by mouse click or from the terminal.

(6) When the installer starts, it asks for permissions for system changes with a password prompt. Accept the End-user license agreement (EULA) and continue. The native installation mechanism (debi) begins the actual installation.

(7) When the installation is complete, the installer closes and the ClearPass OnGuard Agent starts automatically. If the installation fails, the installer displays installation logs for troubleshooting.

Uninstalling the ClearPass OnGuard Persistent Agent

To uninstall the application, run the **`sudo apt-get purge clearpass-onguard`** command from the terminal.

Dependencies

The binary Installer and the application require the following packages:

- libc6 (>= 2.15)
- libdbus-1-3 (>= 1.0.2)
- libdbus-glib-1-2 (>= 0.78)
- libgcc1 (>= 1:4.1.1)
- libglib2.0-0 (>= 2.14.0)
- libgnome-keyring0 (>= 2.22.2)
- libnm-glib-vpn1 (>= 0.7.999)
- libnm-glib4 (>= 0.7.999)
- libnm-util2 (>= 0.7.0)
- libproxy1 (>= 0.4.7),
- libqtcore4 (>= 4:4.7.0~beta1)
- libqtgui4 (>= 4:4.6.1)
- libstdc++6 (>= 4.6)
- libtdb1 (>= 1.2.7+git20101214)
- libxml2 (>= 2.7.4)
- zlib1g (>= 1:1.2.0)
- gdebi
- gksu

- Two new fields were added in Patch Management configuration for Windows OS. The **Grace Period** field lets you specify a time interval during which the client will be treated as Healthy even if some patches are missing. The **Scan Interval** field lets you specify the time interval after which the OnGuard Agent should check for missing patches. (#24125)

- Authentication server IP addresses used by OnGuard persistent agents can now be manually configured. At **Administration > Agents and Software Updates > OnGuard Settings > Policy Manager Zones**, the user can configure an ordered list of authentication server IPs per zone. (#25836)

Issues Resolved in the 6.5.0 Release

NOTE

The 6.5.0 release resolved specific vulnerability issues. For details, refer to issues #24141, #24783, #25196, #25197, #25343, #25368, #26048, #26073, #26393, #26850, #26941, #26988, #27050, #27298, #27300, #27478, and #27532.

The following issues have been fixed in the ClearPass 6.5.0 release.

Policy Manager

Table 9: *Policy Manager Issues Fixed in 6.5.0*

Bug ID	Description
#20280	CPPM license usage counters in Graphite were not available on ClearPass 6.3.x.
#20639	The "**Guest Access - Web Login PreAuth**" and "**Onboard Authorization - RADIUS**" service templates were removed. These two templates were replaced by the **Onboard** template.
#20788	Corrected a RADIUS server issue where `rlm_device_sensor` crashed if a burst of accounting requests was sent that included device sensor information.
#21874	The **Event Viewer** page displayed an incorrect authentication count when the node authentication capacity exceeded the licensing limit. The error was in the authentication count which was same as the license capacity instead of the actual authentication count.
#22057	A device could not be disconnected after an AirGroup authorization request was received from the client.
#22910	The Access Tracker on the publisher would hang if one of the subscribers was down. An error message is now shown to let the user know if the nodes selected in the Access Tracker are unreachable, so the user can remove the node and execute it again.
#23851	The Active Sessions data filter query that is used to get authentication details is now optimized to retrieve information more quickly.
#24141	CentOS was updated to version 6.6. This provides fixes for the kernel vulnerability CVE-2014-2523.
#24397	Using certificate namespace attributes in authentication source filters caused AD lookups to fail.
#24423	Mobile devices could not be polled from JAMF. The JAMF connector configuration is now reset after each poll.
#24484	ClearPass could not be accessed through the CLI because logs used too much disk space. To fix this issue: • The new 'system cleanup' command performs on-demand cleanup. • The 'system sysinfo' command provides information on the disk and memory utilization. • The system checks the disk utilization every hour and purges data if the configured disk threshold is met.
#24674	Incorrect error messages were shown after OCSP responses without nonce were rejected. The appropriate messages are logged now when OCSP checks fail.
#24783	The CURL library was updated to 7.19.7-37.3. This includes fixes for CVE-2013-4545.
#25112	ClearPass 6.5.0 now supports extended network traffic counters for database traffic (port 5432) and HTTP and HTTPS web traffic (ports 80 and 443) between the nodes in the cluster. These counters also increment during cluster operations that add or drop a subscriber, or promote a subscriber to a publisher.

Table 9: *Policy Manager Issues Fixed in 6.5.0 (Continued)*

Bug ID	Description
#25191	The event viewer failed to show an accurate SMTP delivery status for an email sent using the **Send Test Email** action on the **Administration > External Servers > Messaging Setup** page.
#25197	This release includes fixes for a vulnerability issue where the CPPM version was displayed during the launch of an SSH session in CPPM before authentication completed.
#25202	A space after a comma in a comma-separated whitelist host header configuration sometimes caused the HTTPD service to stop.
#25305	Users were not able to filter the endpoint repository using an attribute name with '_' .
#25714	Users were not assigned the correct user role after a subscriber in a multi-node cluster was promoted to a publisher.
#25732	Endpoint cache entries did not update correctly when endpoints were manually deleted in bulk.
#25733	Some of the guest accounts did not authenticate after CPPM was upgraded to the latest version.
#25737	The event viewer now logs start and end events for subnet scans for static IP device discovery, providing enhanced visibility into the subnet scan process.
#25744	Corrected an issue where the error message “Can’t contact LDAP server” was shown intermittently. CPPM will now reconnect once to the LDAP/AD server if the bind fails with the error code LDAP_SERVER_ DOWN during authentication.
#25860	The Policy Server service parameter "Authentication Cache Timeout" is removed in this release, because Policy Manager does not use this parameter anymore.
#25878	Corrected an intermittent issue where users could not update the management/data port gateway IP address.
#25916	In the CPU Load screen, the Y-axis was labeled incorrectly. The CPU Load Y-axis now displays "Load Average" instead of "Percentage."
#25983	The “Use Full Username” option is now supported for Palo Alto Networks UID updates.
#26048 #25196	OpenSSL was upgraded to the latest version available. This includes fixes for CVE-2014-3511, CVE-2014-3566, CVE-2014-3567, and CVE-2014-3568.
#26057	A warning message was not displayed when the RADIUS certificate expiration would occur within 30 days. The warning is now correctly displayed when the RADIUS certificate is about to expire.
#26112	The Dashboard’s **Quick Links** widget pointed to an incorrect link if **Configuration > Network > Devices** or **Administration > Server Manager > Server Configuration** was selected.
#26178	The administrator was unable to insert a service in the OnGuard **Posture Plugin** configuration if the service name included special characters.
#26182	The **Analysis & Trending** page showed an incorrect correlation of authentication count and time. This occurred only if the user changed the time duration scale.
#26279	Authentications sometimes failed against an AD/LDAP server if the length of the user DN exceeded 255 characters.
#26370	Mobile devices were not updated from JAMF. The JAMF MDM connector configuration is now reset after

Table 9: *Policy Manager Issues Fixed in 6.5.0 (Continued)*

Bug ID	Description
	each poll.
#26377	Reject requests were not shown in red in the Access Tracker.
#26412	Corrected an issue where CLI based enforcement failed on extreme switches.
#26499	Any changes made to the cluster password caused the syslog queries to the database to fail.
#26519	If a disabled node was part of a VIP configuration and it is in Enabled status during a "join back to cluster" operation, then VIP service will be started automatically after the node joins back to the cluster. The VIP service will be started after the node is made a subscriber and before it is promoted to publisher (if that is selected).
#26660	Corrected a spacing issue between the application name and text in the Clearpass UI.
#26717	Corrected an issue where, when configuring an SMTP mail server for email notifications with SSL enabled, server certificates were not validated. Server certificate validation is now added for SMTP configuration with Connection Security set to SSL. To fetch Server Certificates, use the following configuration: 1. Go to **Administration > External Servers > Endpoint Context Servers > Add**. 2. On the **Server** tab, use the following values: ▪ **Select Server Type** = Generic HTTP ▪ **Server Name** = smtp.gmail.com ▪ **Server Base URL** = https://smtp.gmail.com:465 ▪ **Validate Server** = Mark the **Enable** check box to validate the server certificate. This fetches the server certificate, and a **Certificates** tab is added to the form, where you can see the certificate listed. 3. Click **Save**.
#26723	Downloading skins from the **Administration > Agents and Software Updates > Software Updates** page failed with a **Download Stuck** error.
#26745	The error message that was displayed at **Monitoring > Event Viewer** did not provide enough information when a RADIUS server failed to start due to an expired server certificate.
#26850	This release includes fixes for CVE-2015-1389, a cross-site scripting vulnerability that could permit an unauthenticated user to inject script code that could be executed by a ClearPass administrator while inside an administrative session.
#26891	Corrected an issue with server certificate validation by retrieving the Certificate Extension Values like **Subject Key Identifier** and **Authority Key Identifier** while the Certificate Chain for Radius Server Certificate and Https Server Certificate were being built.
#26933	Users should be aware that, during upgrade to 6.5, the AntiVirus check in the Linux Posture Policy will not be restored by default. The administrator must manually reconfigure AntiVirus checks for Linux systems if they are required. A message is now displayed in the UI advising the user of this.
#26946	Performance is improved for Active Directory error handling. Now the Domain Service is not restarted when authentication fails with the following error codes: • 0xC000006D - STATUS_LOGON_FAILURE • 0xC000006E - STATUS_ACCOUNT_RESTRICTION • 0xC000006F - STATUS_INVALID_LOGON_HOURS • 0xC0000071 - STATUS_PASSWORD_EXPIRED • 0xC0000072 - STATUS_ACCOUNT_DISABLED • 0xC0000064 STATUS_NO_SUCH_USER

Table 9: *Policy Manager Issues Fixed in 6.5.0 (Continued)*

Bug ID	Description
	• 0xC000006E STATUS_ACCOUNT_RESTRICTION • 0xC000006C STATUS_PASSWORD_RESTRICTION • 0xC000006A STATUS_WRONG_PASSWORD • 0xC0000193 STATUS_ACCOUNT_EXPIRED • 0xC000006F STATUS_INVALID_LOGON_HOURS • 0xC0000234 STATUS_ACCOUNT_LOCKED_OUT • 0xC0000224 STATUS_PASSWORD_MUST_CHANGE
#27103	Attempting to integrate a Vasco Identikey Authentication server with Clearpass 6.5.0 using Vasco as a Radius Authentication source failed. The RADIUS server is now modified to integrate with the Vasco IdentiKey Authentication Server.
#27171 #27112	CPPM updates to PANW did not update the NETBIOS name for users.
#27298	This release includes fixes for multiple cross-site scripting vulnerabilities that existed within ClearPass and that could be used by one authenticated administrative user to inject script code into the session of another administrative user.
#27336	The IPSec tunnel was not reestablished when configuration parameters such as the IKE version or hash algorithm were modified.
#27342	Usage of port 4231 in the External Netevent Target URL is removed in 6.5. To specify an external Insight server, use **http://<CPPM-IP-Address>/netwatch/netevents** in the Target URL.
#27497	Corrected an issue where, if the default “admin” or “apiadmin” account’s name or user ID was changed, it reverted to the default after upgrade. ClearPass now gives a validation error in such cases. Users should be aware that ClearPass 6.5.0 does not support any changes to the name or ID of the default admin user (admin, apiadmin). If these values were changed in previous versions of ClearPass, they will be reset to their original default values upon upgrading to ClearPass 6.5.0. (The password will be carried forward as in the previous version.)
#27532	The glibc package was updated. This includes fixes for CVE-2015-0235.
#27857	Users should be aware that, to enable upgrade from 6.2 or 6.3 now that the 6.5 upgrade image is DER-signed, the **CPPM-x86_64-20140919-cli-der-support** patch update is now required before upgrading from ClearPass 6.2.6 or 6.3.6 to 6.5.0. The patch is available in the Software Updates portal and the support site.

AirGroup

Table 10: *AirGroup Issues Fixed in 6.5.0*

Bug ID	Description
#26361	Corrected an issue where a dot (".") character was not permitted in an AP-Name used for AirGroup sharing rules.

CLI

Table 11: *CLI Issues Fixed in 6.5.0*

Bug ID	Description
#25669	Users should be aware that the 'network app' command is now deprecated in the CLI as it is no longer needed.

Dissolvable Agent

Table 12: *Dissolvable Agent Issues Fixed in 6.5.0*

Bug ID	Description
#25871	Users should be aware that the Java-based Onguard Dissolvable Agent does not display remediation results unless the latest version of Java is installed on the client. This is the expected behavior, and reflects ever-changing Java security policies. The latest Java version is always required in order to perform client health checks.
#27239	The Native Dissolvable Agent for Mac OS X displayed the warning " **Identity of the developer cannot be confirmed**" during launch.

Endpoint Context Servers

Table 13: *Endpoint Context Server Issues Fixed in 6.5.0*

Bug ID	Description
#24170	CPPM was unable to fetch Endpoints from Maas360. This issue was observed only for endpoints that had wired interfaces.
#25470	Improvements to the requests library resolved an issue where the Clearpass server was unable to retrieve information from an MDM simulated server when proxy was configured on the CPPM Server.
#25498	All endpoint types were downloaded from Aruba Activate, even though a filter for Aruba Active MDM was configured in **Administration > External Servers > Endpoint Context Servers** that limited the download to remote and instant APs.
#26996	Corrected an issue that occurred while configuring **Administration > External Servers > Endpoint Context Servers**.The **ClearPass Cloudy Proxy** option listed in the **Server Type** drop-down list is now disabled.
#27005	An issue with multiple occurrences of TCP connections while polling MDM Servers from MDM Connector was resolved by upgrading the library.
27640	Additional ContextServers could not be added if the same ServerName was used for both and the base URL was different. The ServerName can now be configured as the proper HostName or IP address for MDM ContextServers.

Guest

Table 14: *Guest Issues Fixed in 6.5.0*

Bug ID	Description
#14368	Page action links were not displayed correctly if a custom skin was used as the non-default skin.
#19568	Database errors occurred when RADIUS accounting data was sent to a server that did not process the RADIUS authorization (access-request). This issue was triggered when a session had RADIUS accounting data but did not match any authentication records.
#22011	Corrected an issue where Firefox could not save or auto-complete passwords. This prevented the username and password of the operator be auto-filled in various configuration forms, such as the Edit Account form.
#25135	Guest sponsorship approval could be incorrectly configured to allow role override when operator authentication was disabled.
#25327	Unwanted JavaScript appeared in emails when certain skins were used.
#25339	Messages sent using the SMS Global SMS gateway were not encoded according to the gateway's requirements.
#25343	This release includes fixes for CVE-2014-6628, a vulnerability issue that permitted an authenticated administrative user to execute arbitrary uploaded code on the underlying operating system with the privilege level of the Web server. As part of this fix, the ability to run PHP within Guest's custom pages has been removed. If you previously ran PHP from Content Manager or within a login or registration page, you should contact Aruba Support for assistance.
	The ability to run PHP within the custom pages for ClearPass Guest has been removed.
#25639	The contents of folders under **CPGuest > Config > Content Manager > Public** could not be deleted.
#26103	The initial state of the account was incorrect if a role override for sponsored registrations was set to [Prompt].
#26258	The value for the **`IdP-Cookie-Timeout-Mins`** attribute was applied as seconds instead of minutes.
#26327	To improve performance of Web login pages, Advertising Services can now be selectively enabled or disabled from either **Configuration > Pages > Web Logins** or **Configuration > Pages > Guest Self-Registrations > Master Enable**.
#26371	Operating as a SAML Identity Provider (IdP) failed due to browser redirection issues.
#26400	Changing a guest account role on the **Guest > Manage Accounts > Edit Account** form did not trigger an appropriate CoA request for active sessions. To configure CoA requests to handle changes in guest roles, the admin must create CoA profiles in the correct format: 1. At **Policy Manager > Configuration > Enforcement > Profiles > Add**, on the **Profile** tab, select **RADIUS Change of Authorization (CoA)** in the **Template** drop-down list. 2. In the **Name** field, the name entered for the profile must include the exact role name in square brackets. For example, for the role "[Guest]", the profile name might be "My Company [Guest] CoA". 3. On the **Attributes** tab, select **Aruba - Change-User-Role** in the **Select RADIUS CoA Template** drop-down list. 4. Click a row and add an attribute with the **Type** as **Radius:IETF**, and for the **Value** enter the role name, but without the square brackets this time.
#26401	On **Guest > Manage Devices**, disabling or deleting an account did not disconnect an active session for the device. Disabling or deleting a device account now triggers a session disconnect for all active sessions associated with the account.

Table 14: *Guest Issues Fixed in 6.5.0 (Continued)*

Bug ID	Description
#26444	Enabling a Web login security hash did not work for Apple devices. Devices are now verified and authenticated successfully when the same hash is present in the Web login and the controller.
#26489	A RADIUS CoA from Active Sessions did not work due to proxy settings being used incorrectly by internal communications.
#26889	On the **Active Sessions** list, if the **Role** column was added, it was not populated with the authenticated devices. The **Role** column now shows the device's role for authenticated devices. If there is a CoA, however, this column is not updated.
#26941	This release includes fixes for CVE-2015-1551, a vulnerability that permitted an authenticated administrative user to read information which he or she may not be authorized to read by uploading content which exploits a bug that fails to enforce proper file path restrictions.
#27273	Device accounts that are paired with guest accounts that require sponsorship are now updated when sponsorship confirmation is received.
#25368 #26073 #26393 #27050 #27478	The PHP version was updated to 5.5.21. This includes fixes for CVE-2014-2497, CVE-2014-3538, CVE-2014-3587, CVE-2014-3597, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710, CVE-2014-4698, CVE-2014-4670, CVE-2014-5120, CVE-2014-8142, CVE-2014-9427, CVE-2015-0231, and CVE-2015-0232.
#27506	The active session was not disconnected for the user if the expiration time was set to "now". For an active session, a role-change CoA attempt will be made if there is an applicable profile, and no CoA will be sent if the user expiration time is extended.
#27595	The bypass CNA configuration sometimes failed on the subscriber.
#27606 #27607	If a proxy was configured, ClearPass Guest used it incorrectly when contacting the publisher. ClearPass requires direct access to all other servers in the cluster.
#27628	The random password generator allowed some inappropriate words.

Insight

Table 15: *Insight Issues Fixed in 6.5.0*

Bug ID	Description
#20096	Authentication records could not be updated in the auth table of the Insight DB. To fix this issue, the 20-character limit for the field has been removed and the data type of the "ip" column is changed to Text.
#25306	Headers on a PDF report were not displayed correctly. Column headers are now displayed only at the beginning of the table.
#25476	Uploaded Images were not correctly displayed in Insight reports in PDF and HTML formats.

Table 15: *Insight Issues Fixed in 6.5.0 (Continued)*

Bug ID	Description
#26157	Corrected an issue where including special characters (such as the '=') in a cluster password caused upgrades to fail.
#26988	This release includes fixes for CVE-2015-1550, a vulnerability that permitted an authenticated administrative user to execute arbitrary uploaded code on the underlying operating system with the privilege level of the Web server. As part of this fix, report names now cannot contain characters such as a slash (/) or two sequential periods (..).
#27300	This release includes fixes for CVE-2015-1392, multiple SQL injection vulnerabilities that existed within ClearPass. An administrative user with a lower privilege level could have leveraged these vulnerabilities to read information that should only be available at a higher privilege level.

Onboard

Table 16: *Onboard Issues Fixed in 6.5.0*

Bug ID	Description
#21010	Auto-reconnect is not supported for Mac OS X, and the Provisioning Settings forms are updated to reflect this.
#24553	When you connect to ADCS to issue an Onboard certificate, the server certificate is verified against the CPPM Trust list.
#24879	The ClearPass Endpoint profile now correctly displays the device family for Ubuntu and Chromebook devices.
#25132	The **iOS Settings > Settings Type > Create** and **Cancel** buttons both initiated the Create function. The **Cancel** button now works correctly.
#25291	To address an issue where Mac OS X systems with no airport card failed onboarding with a “Profile installation failed” error, the console application now displays the error message "mdmclient: No wireless interface was found." Users should be aware that configuring wired networks with Mac OS X is only supported when the Mac has a Wi-Fi adapter (AirPort card or similar), otherwise the profile installation will fail with the message "Profile installation failed. The 'Wi-Fi Network' payload could not be installed. The Wi-Fi network either could not be found, or could not be connected. You may need to try to reconnect at a later time." This is due to system limitations of Apple’s device provisioning process.
#25364	Corrected an issue that prevented the generation of EC keys in Onboard.
#25484	The requirement to have a network configured to enroll Chromebook devices in Onboard has been removed, since there is no network configuration done on Chromebook.
#25667	An incorrect signature algorithm was used with certificates using the SHA-2 family of signature algorithms.
#25671	The default configuration for a newly installed or created Onboard Certificate Authority (CA) is updated to use the SHA-512 digest algorithm. The SHA-1 cryptographic hash algorithm is not recommended for SSL or code-signing certificates. Its use is being deprecated by major providers, and it will soon be untrusted for code-signing certificates. More informationis available at sites such as http://googleonlinesecurity.blogspot.com/2014/09/gradually-sunsetting-sha-1.html and http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx.

Table 16: *Onboard Issues Fixed in 6.5.0 (Continued)*

Bug ID	Description
#25812	The Onboard device incorrectly displayed the marketing model names of iOS devices instead of the internal product numbers of the device.
#25909	A Windows client failed to sign the Aruba QuickConnect application in FIPS mode.
#26350	Options to control reconnect behavior are no longer included in the **Provisioning Settings** form. For iOS, reconnect behavior is now automatic when Insight is enabled and the same SSID provisioning is used, and is disabled otherwise.
#26558	The UI navigation to **Onboard > Deployment and Provisioning > Provisioning Settings** did not work correctly when the Aruba ClearPass skin was used.
#26601	Onboard incorrectly displayed a warning message about RADIUS server certificates missing the id-kp-eapOverLAN key usage even when the server certificate specified “Any Extended Key Usage”.
#27349	Onboard enrollment failed against the latest version of ADCS on Windows 2008.
#27365	For non-Apple devices, the device type was displayed as “None” if ADCS was used for issuing client certificates. When signing a client certificate with ADCS, Onboard now records the device information against the certificate, even when the certificate itself does not embed this information.
#27369	Duplicate device entries sometimes caused re-enrollment to fail.
#27455	When SSO was configured for Onboard, the “Unsupported Device” informational text was not displayed correctly. Error messages are now correctly displayed when SSO is configured.
#27746	QuickConnect.exe could not be downloaded successfully on legacy versions of Internet Explorer.

OnGuard

Table 17: *OnGuard Issues Fixed in 6.5.0*

Bug ID	Description
#6012	The ClearPass OnGuard Unified Agent for Windows now categorizes virtual Interfaces such as VMware Network Adapter VMnet8 as **Other** instead of **Wired**.
#20279	On Mac OS X, the ClearPass OnGuard Unified Agent’s **Quit** and **Force Quit** options sometimes did not work and the machine would not restart.
#25081	The Access Tracker showed a status of Service even after the Service was removed from the Posture Policy configuration.
#25843	A disk encryption check failed due to a trailing backslash character (\) in the location path.
#25848	Network administrators were unable to uninstall OnGuard silently (without startup confirmation or uninstall status messages) using an MSI package.
#25906	The ClearPass OnGuard Unified Agent failed Disk Encryption Checks for PGP on Mac OS X.
#26275	On Mac OS X 10.10, after changing the mode on the CPPM server the ClearPass OnGuard Unified Agent would not relaunch.
#26300	The ClearPass OnGuard Agent now performs health checks every time system wakes up from

Table 17: *OnGuard Issues Fixed in 6.5.0 (Continued)*

Bug ID	Description
	hibernation/sleep mode.
#26369	The ClearPass OnGuard Unified Agent caused delays in loading the desktop after rebooting the Windows OS.
#26513	The Native Dissolvable Agent for Windows did not send health for Windows Security Health Validator.
#26613	The following method has been added for mass deployment environments that need MSI based solution to uninstall. **`(msiexec /i ClearPassOnGuardInstall.msi CLEANUP=1 /q)`**
#26669	The ClearPass OnGuard Unified Agent was unable to detect Casper Suite Patch Agent.
#26808	The ClearPass OnGuard Unified Agent was unable to detect Korean applications for the Installed Applications Health Class in the Korean Windows OS.
#26844	The ClearPass OnGuard Unified Agent in the **OnGuard Activity > Bounce Agent** option displayed an incorrect message in the Korean language.
#27011	The ClearPass OnGuard Unified Agent displayed an incorrect disk encryption state while using FileVault.
#27183	The ClearPass OnGuard Unified Agent for Mac OS X was not able to launch processes while performing auto-remediation of the **Processes** health class on Mac OS X 10.10.
#27207	A user could not log in to ClearPass using a client certificate with a chain length of more than one. The depth of the client certificate chain validation has now been increased.
#27374	During installation of the ClearPass OnGuard Unified Agent, the message "Windows cannot verify the publisher of this software" was displayed.

QuickConnect

Table 18: *QuickConnect Issues Fixed in 6.5.0*

Bug ID	Description
#21736	The ClearPass QuickConnect application on an Android device no longer displays errors when a user manually launches the application and selects a configured network.
#25216	Corrected an issue where Onboarding failed for Mac OS X 10.6.8.
#25249	Corrected an issue where, on Windows 7 running 6.3.2, when the maximum number of devices was reached, a 404 error page was shown. A message is now displayed on the device that explains, "This device is not authorized to use this service. You have already provisioned the maximum number of devices:1".
#25323	Onboarding failed on a Korean Windows system when virtual interfaces were present.

New Known Issues in the 6.5.0 Release

The following known issues were identified in the ClearPass 6.5.0 release.

Policy Manager

Table 19: *Policy Manager Known Issues in 6.5.0*

Bug ID	Description
#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.
#22963	**Symptom:** A cluster split-brain occurrs during recovery of a failed publisher. **Scenario:** A configured standby publisher is promoted automatically when a publisher outage occurs. If the publisher comes back online after this event, it will start servicing requests and act as a standalone publisher. This might lead to problems since there are two active "publishers" in the network at this point. **Workaround:** When a standby failover event is triggered, the failed publisher node should be reset and joined back to the cluster explicitly as part of recovery.
#24646 #24919 #26698 #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. **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.
#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:** SHA1 RSA is not recommended for security reasons. You must update your certificates to use stronger keys, such as RSA with > 1024 bits length.
#26939	**Symptom:** The error message “Guest application has exceeded recommended capacity...” is displayed in the Event Viewer. **Scenario:** When the ClearPass Enterprise license is valid and Guest license capacity is exceeded, the system logs an alert indicating that the Guest application has exceeded the limit. This warning can be ignored; the backend continues to use ClearPass Enterprise license pool.
#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**.
#27379	The **Save** operation gets stuck when you try to save the server configuration changes using the IE browser.
#27428	In the **Service Rule** area on the **Configuration > Services > Edit** page, the mouse cursor changes to a pointer and none of the options are clickable. This does not affect the functionality.
#27586	**Symptom/Scenario:** When a network administrator changes the value of the cluster-wide parameter "Store Password Hash for MSCHAP" to "false," ClearPass does not display a warning that the NTLM hashes for local and admin users will be permanently removed. If this parameter is returned to its previous "true" state, all passwords for local and admin users

Table 19: *Policy Manager Known Issues in 6.5.0(Continued)*

Bug ID	Description
	must be redefined.
#27592	**Symptom:** SAML-SSO using TLS certificate does not work in the Firefox or Safari browser. **Workaround:** Use alternate browsers such as Google Chrome or IE.
#27615	**Symptom:** Importing and exporting Google MDM type endpoint context servers does not work. **Scenario:** At **Administration > External Servers > Endpoint Context Servers**, the **Import** and **Export All** options cannot be used for Google MDM context servers. **Workaround:** For the Google MDM type, use the **Add Endpoint Context Server** form to add the configuration manually instead of using Import or Export.
#27621	**Symptom:** The number of authentications per second for non-MSCHAPv2 methods is reduced when 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.
#27630	**Symptom/Scenario:** The FQDN field details in the **Server Configuration** page are not retained after a restore operation in 6.5.0.
#27661	**Symptom/Scenario:** JRE installers linked to in the Java Dissolvable Agent help page (/agent/html/help.html) are not available post-upgrade. **Workaround:** Install the 6.5.0 patch **JRE installers for Dissolvable Agent help** to make the installers available in agent help. They are available through the upgrade portal or manual download at http://support.arubanetworks.com/DownloadSoftware.
#27737	**Symptom/Scenario:** Session Restriction Enforcement is not converted to Session Notification if Session check User name is configured. **Workaround:** Configure a new Session Notification Enforcement as shown below and associate it with the service: • **Session-Notify Server Type = Palo Alto Networks Firewall** • **Session-Notify Server IP = <IP ADDRESS>** • **Session-Check Username = %{Endpoint:Username}**
#27745	**Symptom:** Some CPPM Dashboard widgets do not work properly. **Scenario:** On the CPPM 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	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 local users and admin users.

Table 19: *Policy Manager Known Issues in 6.5.0(Continued)*

Bug ID	Description
#27903	**Symptom/Scenario:** Trying to upgrade from 6.2.6 to 6.5.0 using the **Import Updates** option on the **Software Updates** portal does not work, and the error message "Uploaded file is invalid..." is displayed. **Workaround:** Use either the CLI or Web server option instead to perform the upgrade.
#27908	If you will be upgrading through the CLI and are upgrading from 6.4.0 or 6.4.1, you must update to 6.4.2 or later before upgrading to 6.5. This is due to the changes in the signing mechanism of the updates and upgrade images. Prior to updating to 6.4.2, you must first download and install the 6.4.0 CLI updates patch. At support.arubanetworks.com, go to **Download Software > ClearPass > Policy Manager > Current Release** and select **CPPM-x86_64-20140919-cli-der-support-patch**. If you are upgrading through the Software Updates portal in the Policy Manager user interface, or through the Web service, upgrade is supported for any 6.4.x version.
#27922	**Symptom:** TACACS/WebAuth authentication fails and shows an internal error. **Scenario:** In some upgrade cases the services might not come up properly on subscriber nodes, resulting in Webauth/TACACS Authentication Failures. The **Access Tracker > Session Details** form shows the internal error message "Failed to authenticate user", **Workaround:** Manually restart the corresponding services that cause the failures.

Dissolvable Agent

Table 20: *Dissolvable Agent Known Issues in 6.5.0*

Bug ID	Description
#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/`

Endpoint Context Servers

Table 21: *Endpoint Context Server Known Issues in 6.5.0*

Bug ID	Description
#27666	**Symptom/Scenario:** Users cannot create more than one Google Admin Console type context server.
#27815	**Symptom/Scenario:** Endpoint attribute information is not deleted when a device is reset in Aruba Activate.

Guest

Table 22: *Guest Known Issues in 6.5.0*

Bug ID	Description
#27363	**Symptom/Scenario:** If the default role-mapping policy [Guest Roles] is renamed, the guest roles in ClearPass Guest are not populated.

Insight

Table 23: *Insight Known Issues in 6.5.0*

Bug ID	Description
#26899	**Symptom:** Use of System Events and Audit Events via the Insight template is not recommended. **Workaround:** Use the default **System Events and Audit Events** template from syslog filters instead.
#27245	**Symptom/Scenario:** CPPM supports SSO login across all applications; however, when a CPPM session is active, idle session timeout for Insight does not take effect.
27445	**Symptom/Scenario:** The **Service** column from the **Monitoring** > **Live Monitoring** > **Access Tracker** page truncates the text if the **Service** name contains more than 20 characters. **Workaround:** You can view the full name when you click or mouse over the service name.
#27529	Insight report generation for the **Endpoint Latest** template might take a long time or might not complete if the number of endpoints is greater than 1,00,000.
#27597	The Insight search utility does not correctly display an error message if a user searches for a device by username when no username data exists.

Onboard

Table 24: *Onboard Known Issues in 6.5.0*

Bug ID	Description
#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.
#27783	**Symptom:** The user cannot complete onboarding when the pre-auth type is configured as **Application Authentication**. **Scenario:** When the pre-auth type is configured as **Application Authentication** in Onboard, if authenticating with a username that starts with the letter “u” in the format NETBIOS\uxxxx, the application authentication request is not seen and the user cannot complete onboarding.

OnGuard

Table 25: *OnGuard Known Issues in 6.5.0*

Bug ID	Description
#21152	**Symptom:** The ClearPass OnGuard Unified Agent fails to establish a control channel on Windows or Mac OS X if more than one instance of the OnGuard Agent is running. **Scenario:** This occurs if multiple instances of OnGuard are running due to multiple users having logged in using Switch User.
#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. **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.
#27668	**Symptom:** OnGuard does not select the correct patch management application. **Scenario:** On a system where two patch management applications are installed, when one of them is uninstalled, OnGuard does not check for the second application. **Workaround:** For a scenario where there are two patch management applications: 1. Create two posture policies that have the same configuration for all the health classes (AV, AS, FW) except Patch Management. 2. The first posture policy should be configured only for the patch management application that is wanted. 3. The second posture policy should be configured only for the uninstalled patch management application. 4. Add both the posture policies in the service (at **Configuration > Services**). It is important to add the policy that is configured for the existing application first, and add the policy that is configured for the uninstalled application second.
#27876	**Symptom/Scenario** RADIUS CoA over VPN is not supported on Ubuntu.

QuickConnect

Table 26: *QuickConnect Known Issues in 6.5.0*

Bug ID	Description
#27694	**Symptom** An Ubuntu device cannot be onboarded by a new user if it has already been onboarded by another user. **Workaround:** Manually delete the directory **/tmp/quickconnect** before onboarding.

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

Policy Manager

Table 27: *Known Issues in Policy Manager*

Bug ID	Description
#10881	Entity updates with PostAuth enforcement fail if the publisher is down.
#11744	**Symptom:** Upgrading from 5.2 to 6.x fails if CPPM is joined to the domain. **Scenario:** The issue will not be seen if the latest cumulative patch is installed before performing the upgrade.
#11906	**Symptom:** The Aruba dictionary becomes disabled by default after upgrading from Policy Manager 4.x to 6.0.1. **Workaround:** Customers who run into this issue must enable the Aruba dictionary manually from the **Administration > Dictionaries** page.
#12316	Syslog Filters and Data Filters configuration will be removed after an upgrade. Policy Manager does not carry forward Syslog Filters and Data Filters configuration. Only default data is migrated.
#13645	Authorization attributes are not cached for the Okta authentication source.
#13781	**Symptom/Scenario:** In the 6.1 release, the default unit for the CRL update interval was changed to "hours" from an earlier default unit of "days". Restoring a 5.x backup on CPPM 6.x causes the update interval to be "hours". For example, "2 days" in 5.2.0 becomes "2 hours" in 6.1.0. **Workaround:** Manually change the value in days to the value in hours. In the above example, that would be 48 hours.
#13999 #13975	In order to add or update a PostAuth profile configuration, the admin must first delete old profiles from CPPM, and then add the new/updated profiles.
#14186	**Symptom:** Post auth doesn't work properly for UNKNOWN endpoints in a MAC Authentication Bypass (MAB) flow. **Scenario:** This has been observed if the user tries to connect using an endpoint that is unknown to CPPM.
#14190	**Symptom:** Blacklisted MAC Authentication Bypass (MAB) users cannot be blocked using the Blacklist User Repository. **Workaround:** In order for post auth to work in a MAB flow, a new blacklist repository must be added with a custom filter.
#17232	**Symptom/Scenario:** The error and warning messages returned by the Web service are displayed in English instead of the localized language.
#18064	**Symptom:** AirWatch custom HTTP actions needs content even though it's not required. **Scenario:** For AirWatch MDM, custom-defined HTTP actions such as Lock Device or Clear Passcode fail with error messages. This is due to a bug in AirWatch. **Workaround:** Do either of the following: • Add a header **Content-Length:0** in the **Context Server Action**.

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

Bug ID	Description
	• Add a dummy JSON data {"a":"b"}.
#18701	**Symptom/Scenario:** Performing an AddNote operation using AirWatch as the MDM connector fails in CPPM. This is due to a bug in AirWatch.
#19176	CPPM does not currently support posting of Palo Alto Networks (PANW) user ID information when the PAN OS uses Vsys.
#19826	Palo Alto Networks (PANW) devices will only accept the backslash character (\ ) as a separator between the domain name and the username.
#20383	The system posture status may still be maintained after Post Auth agent disconnect action. This is likely to happen when Posture result cache timeout service parameter is higher than the Lazy handler polling frequency.
#20416	**Symptom:** The Palo Alto Networks (PANW) operating system firewall rejects user ID updates from CPPM when the user ID limit is reached on the firewall. When this happens, user ID updates are rejected with errors. **Scenario:** This occurs when the PANW firewall exceeds its supported limit advertised for user ID registration. **Workaround:** There is no workaround at this time.
#20453	In order for CPPM to have complete data to post to Palo Alto Networks devices in HIP reports, profiling must be turned on. This is the expected behavior.
#20455	**Symptom/Scenario:** When doing an SSO & ASO flow in Safari browsers, the certificate needs to be added in the trust list of the browser. **Workaround:** Please follow these steps: 1. Open the Safari browser and enter the SP URL. 2. After you enter the SSO application in the browser, the Show Certificate option is provided in a popup window. 3. Click **Show Certificate** and select the **"Always trust 'FQDN of SP machine' when connecting to IPaddress"** check box, and then click the **Continue** button.
#20456	**Symptom:** SNMP bounce fails. **Scenario:** When only the SNMP bounce in the SNMP Enforcement profile of a Web auth service is configured, SNMP bounce functionality does not work. **Workaround:** Also configure a VLAN ID along with the SNMP bounce in the SNMP enforcement profile.
#20484	**Symptom:** Dropping the Subscriber and then adding it back to the cluster may fail at times. **Scenario:** CPPM system time might not have been synchronized with an NTP source. **Workaround:** Configure an NTP server. CPPM will synchronize its time with the NTP source. Attempt the cluster operation.
#20489	**Symptom/Scenario:** CPPM 6.3 does not allow a server certificate with a Key Length of 512 bits as seen in the Self-Signed Certificate and Certificate Signing Request UIs. Earlier CPPM versions did not have this restriction, hence their server certificate may use one with a 512 bit Public Key. After upgrade, these servers will not work properly. **Workaround:** The admin must manually fix the server certificate to allow a minimum of 1024 bits long Public Key prior to upgrade.
#20943	**Symptom/Scenario:** After upgrading from 6.2.0 to 6.3.0, the WorkSpace Attributes under Service Rules, Role Mapping, and Enforcement Policy Rules are not updated. In 6.2, under **Enforcement Policy > Rules**, the WorkSpace Dictionary Items are used with Application:WorkSpace:<Attribute>. In 6.3 this is changed to Application:ClearPass:<Attributes>.

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

Bug ID	Description
#21334	**Symptom:** CPPM does not launch. **Scenario:** The ClearPass user interface will not launch from Firefox or from older versions of Internet Explorer (IE) browsers if an EC-based HTTPS server certificate is used. On Firefox, the error message "Secure Connection Failed. An error occurred during a connection to <*server*>. Certificate type not approved for application" is displayed. On older versions of IE, the error message "Internet Explorer cannot display the Web page" is displayed. **Workaround:** Use the latest version of IE, or the Chrome browser instead.
#22023	**Symptom/Scenario:** Launching the customer's ClearPass user interface through a proxy does not work on the Internet Explorer or Safari browsers. **Workaround:** Use the Chrome or Firefox browser instead.
#23581	**Symptom:** A database connection error occurs in the Access Tracker UI when it is updated to 6.3.2 with MD2 server certificates. **Scenario:** This is a database connection problem because of the MD2 certificate available for PostgreSQL. MD2 is not supported. **Workaround:** After updating to 6.3.2 (patch installation from 6.3.0), if Access Tracker or Analysis & Trending show errors relating to database query errors, it can be due to an invalid Server Certificate. 1. Go to Server Certificate and select the certificate for the server and RADIUS service. 2. Click View Details for each certificate in the chain. 3. Look for the Signature Algorithm and check to see if it uses MD2. 4. Download the certificate that is MD5 or SHA1-based algorithm to replace the MD2 algorithm from the corresponding Certificate Authority site. 5. From the Support shell, restart the cpass-postgresql service.
#23625	**Symptom:** Restoring the log DB in 6.3.2 overwrites existing event viewer entries. **Scenario:** In 6.3.2, restoring the log database alone (without configuration database restoration) from a backup results in the Event Viewer entries being overwritten with the ones from the backup. This has occurred in cases where the log database is restored manually after the upgrade. **Workaround:** There is no workaround at this time.
#23848	**Symptom:** The ClearPass server's time setting might sometimes be off by as much as eight hours. **Scenario:** This is due to a known issue with VMware tools, which periodically checks and synchronizes time between the host and the guest operating systems. This issue is documented by VMware at http://pubs.vmware.com/vSphere-50/index.jsp?topic=%2Fcom.vmware.vmtools.install.doc%2FGUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html. **Workaround:** There is no workaround at this time.
#24781	Palo Alto Networks (PANW) devices accept only the backslash (\ ) character as a separator between the domain name and the username. If the update uses an "at" sign (@) between the domain name and the username, the HIP report will not be shown in PANW.
#25211	**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.

Dissolvable Agent

Table 28: *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 CPPM. It can be downloaded from the following URL: https://<CPPM-IP-Address>/agent/html/help.html
#18031	**Symptom:** The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 installed. **Scenario:** This occurs when Java 7 is installed. Java 7 is released as 64-bit binaries; the Java plugin will not work in Chrome, which currently has a 32-bit version. **Workaround:** The Web Agent works fine with Firefox-23.x or later versions. Use the Firefox browser for the Web agent until Chrome resolves 64-bit support for Mac OS X.
#18035	**Symptom:** The OnGuard Web Agent applet fails to launch on Mac OS X 10.9. **Scenario:** New security restrictions in Mac OS X 10.9 and Safari 7 prevent the launch of the OnGuard Web Agent. **Workaround:** Go to **Safari menu > Preferences > Security > Allow**. **Allow plugins** should already be selected. Click **Manage Website Settings**, look for your portal Web site IP/name, and select **Run in Unsafe Mode**.
#18230	**Symptom/Scenario:** The ClearPass OnGuard Dissolvable Agent might not work properly if the client machine runs 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..." **Workaround:** Click **Allow** to let the health checks proceed.
#23340	**Symptom:** The OnGuard Agent does not display remediation messages. **Scenario:** This happens on Mac OS X using Firefox 27 and JRE 1.7 update 55. It is not an issue on later versions of Firefox. **Workaround:** Reload the page and log in again.
#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.

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

Bug ID	Description
#24768	**Symptom:** The Native Dissolvable Agent does not work well in Internet Explorer on Windows XP. **Scenario:** The agent works after downloading it and allowing pop-ups, but no remediation results are displayed and, after clicking **Launch ClearPass Application**, a series of messages is displayed in a loop. **Workaround:** Windows XP is an unsupported operating system. Use a later Windows version or the Chrome or Firefox browser instead.
#24792	**Symptom/Scenario:** 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.
#26514	**Symptom:** AVG 2014 and Avast Security 2015 are not detected on Mac OS X. **Scenario:** This happens only with the Java Dissolvable Agent. The OnGuard Persistent Agent and the Native Dissolvable Agent successfully detect these products.

Guest

Table 29: *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 30: *Known Issues in Insight*

Bug ID	Description
#11827	**Symptom/Scenario:** Insight is not supported in Internet Explorer 8 (IE8).
#12096	**Symptom/Scenario:** Editing a report to select some columns for analytics overwrites/replaces the chosen columns for the corresponding report.
#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.
#19507	**Symptom/Scenario:** PDF and HTML Data Tables are not created if the CSV file size is larger than 1MB,

Table 30: *Known Issues in Insight (Continued)*

Bug ID	Description
	although the generated PDF and HTML reports include analytics if configured in the report.
#20601	Insight custom templates used in report configurations of 6.3.x versions are not supported in 6.4.x. Customers must contact Aruba TAC by providing logs from **Insight > Administration > Collect logs** and a new set of custom templates for the 6.4.x version will be provided. Custom templates in 6.4.x work fine with 6.5.x and are carried forward.

Onboard

Table 31: *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. **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.
#25711	iOS always displays SHA-1 for the signing algorithm regardless of the actual algorithm used. This is an issue with iOS, not Onboard.

OnGuard

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

Table 32: *Known Issues in OnGuard*

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.
#13379	Uninstalling OnGuard is not supported from the UI. Users must currently run the following script from the CLI to remove OnGuard from the system completely: `/usr/local/bin/clearpassonguarduninstaller.sh`
#13929	At times, OnGuard may fail to detect peer-to-peer applications, such as /uTorrent, on Windows 2008 R2.
#13935	OnGuard does not support enabling/disabling the Windows Update Agent Patch Management Application.
#13970	After anti-virus software is installed, the system must be rebooted before using ClearPass OnGuard.
#14196	ClearPass OnGuard will not be able get the correct status of 'Software Update' PM application on Mac OS X, if "Check for updates" and "Download updates automatically" are not toggled at least once.
#14673	The 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 CPPM server from a wired interface if the VPN is connected from a trusted network.
#14842	Installing the ClearPass OnGuard Unified Agent removes an existing VIA installation. To continue to use VPN functionality, go to **Administration > Agents and Software Updates > OnGuard Settings** and select **Install and enable Aruba VPN component** from the drop-down list.
#14996	If McAfee VE is running on Windows XP, the ClearPass OnGuard Unified Agent VPN will not work.
#15072	VIA connection profile details are not carried forward after 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.

Table 32: *Known Issues in OnGuard (Continued)*

Bug ID	Description
#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 X. This causes the client to be treated as healthy even if none of the disk is encrypted. **Workaround:** There is no workaround at this time.
#18259	**Symptom/Scenario:** The ClearPass OnGuard Unified Agent does not support Stop or Pause remediation actions for Oracle VM Box Guest virtual machines on Mac OS X.
#18281	The ClearPass OnGuard configured health quiet period is supported in Health only mode. It doesn’t work in Auth+Health mode.
#18341	**Symptom/Scenario:** OnGuard cannot start a process on Mac OS 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.
#19685	**Symptom:** After upgrading OnGuard to 6.3, the backend service fails to start and is unable to collect logs. **Scenario:** This rarely occurs. It has been observed on the Mac OS X 10.6, 10.8, or 10.9 OS after upgrading OnGuard from 6.2.4 or 6.3 to 6.3. **Workaround:** If the backend service fails to communicate with the plugin, reboot the system after the OnGuard upgrade is complete.
#20316	OnGuard’s Health Check Quiet Period is applicable per network interface. If a machine has more than one network interface, then each interface will have its own Health Check Quiet Period duration.
#23470	**Symptom/Scenario:** On a Japanese OS, when upgrading from VIA 2.1.1.3 to the ClearPass OnGuard

Table 32: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	Unified Agent, a known issue with uninstalling VIA displays a message asking the user to select the VIA driver. This does not occur on an English OS.
#23636	**Symptom:** The value of the Posture:Applied Policy attribute is not correctly displayed in the Access Tracker for posture policies carried over from releases earlier than 6.3.0. **Scenario:** This has been observed when upgrading from 6.2.6 to 6.3.2. **Workaround:** This can be corrected by manually saving the affected posture policy once after upgrade.
#23861	**Symptom/Scenario:** On Mac OS X, the ClearPass OnGuard Unified Agent sometimes fails to download a VIA connection profile after the application mode is changed. **Workaround:** None.
#24986	**Symptom:** The Native Dissolvable Agent is not automatically launched after downloading and running the agent the first time on the Chrome browser. **Scenario:** This occurs on Windows and on Mac OS X. **Workaround:** The first time you launch the Dissolvable Agent, click **Launch ClearPass OnGuard Agent**.
#25827	**Symptom/Scenario:** On Internet Explorer 8, when the security warning message 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.
#26232	**Symptom:** When installing or running the Native Dissolvable Agent on Mac OS X 10.10, the message "'ClearPass OnGuard WebAgent' can't be opened because the identity of the developer cannot be confirmed" is displayed. **Workaround:** When opening the OnGuard WebAgent application for the first time after installing, the user must open it manually. Right-click and select the **Open** option. The Web browser will then be able to launch the OnGuard WebAgent.
#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".

QuickConnect

Table 33: *Known Issues in QuickConnect*

Bug ID	Description
#20867	**Symptom/Scenario:** Android 4.3 and above fails to install a self-signed certificate for the CA certificate. **Workaround:** For onboarding Android version 4.3 and above, CPPM must have a RADIUS server certificate issued by a proper Certificate Authority and not a self-signed certificate. This is a requirement of Android's API for Wi-Fi management. In **Onboard > 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.