ClearPass 6.6.8

Release Notes

Open Source Code

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

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

Contents

ClearPass 6.6.8 is a cumulative patch release that introduces new features and provides fixes to previously outstanding issues. An HTML version of these Release Notes is also available.

These release notes contain the following chapters:

- "What's New in This Release" on page 11—Describes new features and issues introduced in this 6.6.8 release as well as issues fixed in this 6.6.8 release.
- "Change of Behaviors in Previous 6.6.x Releases" on page 19—Provides a summary of behavior and resource changes introduced in earlier 6.6 releases.
- "Enhancements in Previous 6.6.x Releases" on page 23—Describes new features introduced in earlier 6.6 releases.
- "Issues Fixed in Previous 6.6.x Releases" on page 55—Lists issues fixed in earlier 6.6 releases.
- "Known Issues Identified in Previous Releases" on page 87—Lists currently existing issues identified in previous releases.
- "System Requirements for ClearPass 6.6" on page 111—Provides important system requirements information for this release.
- "Upgrade and Update Information " on page 121—Provides considerations and instructions for version upgrades and patch updates.

Related Documents

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

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

Use of Cookies

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

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

not store any permanent cookies on a user's computer. Session cookies are deleted when the user closes his or her Web browser.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-Life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins Email: sirt@arubanetworks.com

This chapter provides a summary of the new features and changes in the ClearPass 6.6.8 release.

This chapter contains the following sections:

Release Overview

ClearPass 6.6.8 is a cumulative patch release that introduces new features and provides fixes for known issues. The 6.6.8 cumulative patch is available in ClearPass Policy Manager under **Administration > Agents and Software Updates > Software Updates**.

Change of Behaviors in the 6.6.8 Release

The following changes to ClearPass behaviors, resources, or support were introduced in the 6.6.8 release. For a list of behavior changes introduced in previous 6.6.x releases, see the Change of Behaviors in Previous 6.6.x Releases chapter.

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

- ClearPass now supports SMBv2 and SMBv3 to use with PEAPv0/EAP-MSCHAPv2 and Microsoft Active Directory Domain Services when SMBv1 is disabled. This includes changes to the way ClearPass automatically handles SMB versions. For details, see #40757.
- If you are using SMBv2 or SMBv3, you must increase the remote procedure call (RPC) port range in your firewalls. The new default start port is 49152 and the new default end port is 65535 for these versions; however, the actual port range to use depends on the Windows server version used in your Active Directory deployment. For details, please refer to #41500.

Customers who use ClearPass OnGuard must upgrade to the OnGuard Plugin version 2.0 (V4 SDK) by the end of April 2018 in order to maintain application signature and virus definition updates. The V3 SDK will no longer be supported by OPSWAT after this date. Since virus definitions are updated at least once a day, and sometimes several times a day, it is important to maintain regular automatic updates.

New Features and Enhancements in the 6.6.8 Release

The following new features were introduced in the ClearPass 6.6.8 release. For a list of features introduced in previous 6.6.x releases, see "Enhancements in Previous 6.6.x Releases" on page 23.

This section includes:

OnGuard

The following new features are introduced in OnGuard in the 6.6.8 release:

- For the OnGuard Plugin version 2.0 (V4 SDK), enhancements and support are added as shown below: (#41005)

  Support was added for the following products:

  - AhnLab V3 Endpoint Security 9.x (Windows)
  - Bitdefender Endpoint Security for Mac 4.0 (macOS)
  - FileVault 10.13.x (macOS)
  - F-Secure SAFE 17.0 (Windows)
  - Mac OS X Built-in Firewall 10.13.x (macOS)
  - Mac OS X Trend Micro Antivirus 7.0.2015 (macOS)
  - McAfee LiveSafe version 16.0 (Windows)
  - Microsoft Security Essentials 4.10.0209.0 (Windows)
  - Norton Security 22.9.3.13 (Windows)
  - Software Update 10.13.x (macOS)
  - Symantec Endpoint Protection Cloud 22.9.3.13 (Windows)

  Support was enhanced for the following products:

  - AhnLab V3 Internet Security (Windows)
  - Avast Endpoint Protection Suite (Windows)
  - Avast Endpoint Protection Suite 8.x (Windows)
  - Avast Mac Security 12.5 (macOS)
  - AVG AntiVirus Free 17.5.3021 (Windows)
  - AVG Internet Security 2016 (Windows)
  - Avira Free Antivirus (Windows)
  - Bitdefender Antivirus Free Edition 1.0.6.12 (Windows)
  - Bitdefender Endpoint Security for Mac (macOS)
  - Bitdefender Endpoint Security Tools (Windows)
  - Bitdefender Total Security (Windows)
  - Comodo Antivirus for Mac (macOS)
  - ESET Cyber Security 6.4 (Windows)
  - ESET Endpoint Security (Windows)
  - F-Secure Internet Security (Windows)
  - HP Drive Encryption v8.6.7.27 (Windows)
  - Hyper-V Manager for Windows Server 2016 (Windows)
  - McAfee LiveSafe – Internet Security (Windows)
  - McAfee VirusScan Enterprise (Windows)
  - McAfee VirusScan Enterprise 8.7 (Windows)

- Microsoft Windows Automatic Update 7.x (Windows)
- Norton Security 22.10.0.85 (Windows)
- Norton Security with Backup (Windows)
- Software Update (macOS)
- Sophos 10.7 (Windows)
- Sophos Cloud Endpoint (Windows)
- Sophos Endpoint 11.5.5 (Windows)
- Symantec Encryption Desktop (Windows)
- Symantec Endpoint Protection (Windows)
- Symantec Hosted Endpoint Protection (Windows)
- System Center Configuration Manager Client (Windows)
- Vba32 for Windows Vista (Windows)
- Trend Micro OfficeScan Client (Windows)
- Trend Micro Worry-Free Business Security Agent (Windows)
- VMware Workstation (Windows)
- VMware Fusion Professional 7.1.3 (macOS)
- Windows Defender (Windows)
- Webroot SecureAnywhere 9.x (macOS)

- For the OnGuard Plugin version 1.0 (V3 SDK), enhancements and support were added as shown below: (#41003)

  Support was added for the following products:

  - Avast Business Security 17.x (Windows)
  - Avast Premier 17.x (Windows)
  - Comodo Antivirus 10.x (Windows)
  - F-Secure SAFE 17.x (Windows)
  - FileVault 10.13.x (macOS)
  - Mac OS X Built-in Firewall 10.13.x (macOS)
  - Symantec Endpoint Protection Cloud 22.x (Windows)

  Support was enhanced for the following products:

  - AVG Internet Security 2016.x (Windows)
  - AVG AntiVirus 17.x (macOS)
  - Kaspersky Internet Security 16.x (Windows)
  - Microsoft Windows Update Agent 6.x (Windows)
  - Symantec Endpoint Protection 14.x (Windows)
  - Symantec Hosted Endpoint Protection 3.x (Windows)
  - Webroot SecureAnywhere 9.x (macOS)

Policy Manager

The following new features are introduced in Policy Manager in the 6.6.8 release:

- ClearPass now supports SMBv2 and SMBv3 to use with PEAPv0/EAP-MSCHAPv2 and Microsoft Active Directory Domain Services when SMBv1 is disabled. (#40757)

  After you install this patch, no further configuration is needed to enable the support. When SMBv1 is disabled, ClearPass will attempt to use the highest Samba dialect available on the domain controller.

  Users should be aware of the following expected behaviors:

  - SMBv3 will be automatically used by default for AD joins and any requests that use PEAPv0/EAP-MSCHAPv2.
  - If SMBv3 is not enabled, ClearPass will then automatically failover to SMBv2. If SMBv2 is also not enabled, ClearPass will then failover to use SMBv1.
  - If higher SMB versions are later enabled on the client, ClearPass will then detect the changes and attempt to use the highest available SMB version automatically.
  - If you are using SMBv2 or SMBv3, you must increase the remote procedure call (RPC) port range in your firewalls. The new default start port is 49152 and the new default end port is 65535 for these versions; however, the actual port range to use depends on the Windows server version used in your Active Directory deployment. For details, please refer to #41500.
- Backup and restore operations during migration are now supported for ClearPass Extensions. (#41556)

Issues Resolved in the 6.6.8 Release

The following issues have been fixed in the ClearPass 6.6.8 release. For a list of issues fixed in previous 6.6.x releases, see "Issues Fixed in Previous 6.6.x Releases" on page 55.

This section includes:

Endpoint Context Servers

Table 1: *Endpoint Context Server Issues Fixed in 6.6.8*

Bug ID	Description
#40573	The endpoint context server removed the following special characters from attribute values: { } / < >
#40643	Aruba access points (APs) with new HPE part numbers were not profiled.
#40929	Group information cached from a previous user session was sent to iBoss.

Guest

Table 2: *Guest Issues Fixed in 6.6.8*

Bug ID	Description
#40908	The PHP version is now updated to 5.6.31. This includes fixes for CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, and CVE-2017-9229.
#42071	After upgrading from ClearPass 6.5, a guest's device details could not be viewed and the database error "invalid input syntax for integer" was displayed if there were duplicate values for Role ID. Data migration now supports scenarios where duplicate Role ID values exist in a system.
#42251	Devices that were created with the REST API did not send a RADIUS RFC-3576 change of authorization (CoA) call to automatically bring them onto the network.

Onboard

Table 3: *Onboard Issues Fixed in 6.6.8*

Bug ID	Description
#41360	The Onboard Certificate API now supports MAC address searches (mdps_mac_address) using a subset of a MAC address.
#41362	Deleting all the certificates for a Certificate Authority that had a large number of certificates caused an out-of-memory error.
#41363	An Onboard Certificate Authority (CA) could not be created using an Elliptic Curve key type.
#41365	During routine database cleanup, the **Revoke certificates for inactive devices setting** in Onboard's **Provisioning Settings** form caused certificates to be revoked even if they showed as currently active in the Insight database.
#41366	Trying to delete an Onboard user displayed the error message "Delete failed, check object is not used" if the certificate was of device type "External" and a MAC address field was also present.
#41367	Onboard could not act as a Registration Authority to a Certificate Authority that used an Elliptic Curve (EC) private key for the CA certificate.
#41429	Corrected a migration issue where, when restoring a backup from a version earlier than 6.6.3, the application log displayed the error message "schema 'londiste' does not exist".

OnGuard

Table 4: *OnGuard Issues Fixed in 6.6.8*

Bug ID	Description
#37297	The ClearPass OnGuard Unified Agent for Windows now supports Norton Security with Backup 22.9.x.
#40303	The ClearPass OnGuard Unified Agent sometimes did not detect running processes.
#40692	The ClearPass OnGuard Unified Agent for Windows now supports AhnLab V3 Endpoint Security 9.x when using the OnGuard plugin version 2.0 (V4 SDK).
#40767	Under certain conditions, the **Next** button on the **Start** page of the customizable user interface for custom remediation scripts did not work, although the remediation script was still correctly executed in the background.

Table 4: *OnGuard Issues Fixed in 6.6.8 (Continued)*

Bug ID	Description
#40989	The ClearPass OnGuard Unified Agent sometimes returned an incorrect encryption state for Symantec Encryption Desktop. This issue was seen with the OnGuard Plugin version 2.0 (V4 SDK).
#41118	The ClearPass OnGuard Unified Agent failed to download the file for Agent Script Enforcement if the download took more than 15 seconds.
#42234	The ClearPass OnGuard Unified Agent now supports FileVault 10.13.x on macOS 10.13 when using the OnGuard plugin version 2.0 (V4 SDK).

Policy Manager

Table 5: *Policy Manager Issues Fixed in 6.6.8*

Bug ID	Description
#40255 #40917 #40922 #40923 #40930	The Access Tracker's **Request Details** window took a long time to load data (15 minutes or more). This occurred only under certain conditions — for example, when accessing a remote subscriber's records from the publisher.
#40528 #40926	The SNMPv3 engineID used for sending traps was different from the engineID discovered through SNMP polling in a cluster. Each node in the cluster now has a unique default engineID based on the MAC address of its eth0 interface. This default engineID is used for sending SNMPv3 traps and for responding to SNMPv3 Get/Walk.
#40704	Onboarding Android 7 devices failed if the System store was selected for installing certificates.
#40931	When adding an Oracle database instance as an authentication source, ClearPass now supports using either the Service Name of the Oracle DB instance or the System Identifier (SID) in the **Database Name** field at **Configuration > Authentication > Sources.**
#41037	The RADIUS server sometimes stopped working if a client presented an empty certificate during EAP-TLS authentication.
#41123	When ClearPass was joined to multiple domains, after the 6.6.7 Hotfix patch was applied the ad auth CLI command for testing user authentication did not work correctly for all the domains, and the domain service had to be restarted before the command could be used.
#41209	At **Configuration > Posture > Posture Policies > Posture Plugins**, the error message "Internal error: Null element" was displayed for a user who had Read-only Administrator privileges for posture policies.
#41268	The RADIUS server sometimes did not automatically restart if it exited abnormally or crashed.
#41290	The Policy Server crashed if it was installing antivirus updates at the same time it was processing isLatestChecks for antivirus products.
#41330	When FIPS mode was enabled, changes to a device's configuration in Onboard's **Provisioning Settings** form could not be saved and the error message "This page is not working" was displayed.
#41368	Services sometimes were not restarted if they stopped abruptly or crashed.
#41430	When trying to send updates to PANW versions earlier than PAN-OS 7.1, retrieval of the PAN-OS version failed with unhandled error code 400, "Illegal value for parameter".
#41445	Active Directory authentication policy simulation did not work after the 6.6.7 hotfix patch was installed.

Table 5: *Policy Manager Issues Fixed in 6.6.8 (Continued)*

Bug ID	Description
#41808	
#41809	Corrected an issue in the post authentication process where sending updates to multiple iBoss servers failed and the error message "Second simultaneous write" was displayed.
#41887 #41915 #41916 #41918 #41919 #41920	This release includes fixes for CVE-2017-9001 and CVE-2017-9002.
#42030 #42031	The Struts2 version is now upgraded to 2.3.34.x. This includes fixes for CVE-2017-9804 and CVE-2017-12611.

New Known Issues in the 6.6.8 Release

The following known issues were identified in the ClearPass 6.6.8 release. For a list of known issues identified in previous releases, see "Known Issues Identified in Previous Releases" on page 87.

This section includes:

OnGuard

Table 6: *OnGuard Known Issues in 6.6.8*

Bug ID	Description
#42081	**Symptom:** The ClearPass OnGuard Agent for Windows reports the status of Symantec Endpoint Protection 14.X Firewall as enabled even though the firewall is actually disabled. **Scenario:** This issue is seen with OnGuard Plugin version 1.0 (V3 SDK). **Work around:** Use OnGuard Plugin version 2.0 (V4 SDK) instead.
#42268	**Symptom/Scenario:** The ClearPass OnGuard Agent for macOS does not support FileVault 10.13.x on macOS 10.13 with OnGuard plugin version 1.0 (V3 SDK). **Workaround:** Use OnGuard Plugin version 2.0 (V4 SDK) instead.

Policy Manager

Table 7: *Policy Manager Known Issues in 6.6.8*

Bug ID	Description
#30277	Users should be aware that editing the ClearPass configuration from two tabs within the same Web browser is not supported. Attempting to do so may have unexpected results such as a policy overwriting another policy.
#37037 #42070	Users should be aware of the following allowed and disallowed special characters for the Active Directory (AD) **Username** and **Password** fields on the **Administration > Server Manager > Server Configuration > System > Join AD Domain** form:

Table 7: *Policy Manager Known Issues in 6.6.8 (Continued)*

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Allowed</th><th>Not Allowed</th></tr>
<tr><td>Username</td><td>~ ! @ # $ % ^ * _ - + = { } , . \ ' " ? /</td><td>` & ( )</td></tr>
<tr><td>Password</td><td>! @ # $ % ^ & * ( ) _ - + = { } < , > . ? /</td><td>~ ` [ ] \ | ; : ' "</td></tr>
</table>
</td></tr>
<tr><td>#42218</td><td>Symptom: Under certain conditions a ClearPass backup fails and the error message “ERROR - Failed to backup extensions: ERROR: Backup extensions: Extensions service is disabled, extensions will not be backed up” is displayed.
Scenario: If you do not use Extensions functionality, this issue will not affect your backup and the error message can be ignored. This issue only occurs if the Extensions service is not running during a backup or make-subscriber operation. In this case, any installed Extensions will not be included, but the rest of the backup will proceed normally. The Extensions service must be running during a backup or make-subscriber operation in order to include Extensions in the backup file.
Workaround: If you have ClearPass Extensions installed and you need to back them up — for example, if you are upgrading to the next major version or if you are migrating to a different 6.6.8 server — ensure that the Extensions service is running during a backup or make-subscriber operation.</td></tr>
</table>

This chapter provides a summary of changes to behaviors, resources, or support that were introduced in previous ClearPass 6.6.x releases. For a list of behavior changes introduced in the ClearPass 6.6.8 release, see the What's New in This Release chapter.

Previous Behavior Changes

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

- The 6.6.0 release introduced the ClearPass Extensions functionality. Extensions makes use of the 172.17.0.0/16 network address space. Customers may experience problems with network connectivity, including the error message "no route to host," if there are network conflicts in their existing network with this address space. Customers whose networks include addresses in the 172.17.0.0/16 range are advised to either disable the ClearPass Extension service or to contact TAC for assistance in re-allocating the Extensions to use a different network address space.
- The ClearPass OnGuard Agents for Windows and macOS now support the OnGuard plugin version 2.0, based on the OESIS V4 SDK. Users are recommended to upgrade from plugin version 1.0 to 2.0 as soon as possible. After upgrading, users should be aware of the following changes in behaviors and options: (#36517)
  - For agent enforcement profiles, a new **SDK Type** attribute is used to specify either the V4 SDK (plugin version 2.0) or the V3 SDK (plugin version 1.0) for the agent.
  - At **Administration > Support > Documentation**, a new **OnGuard Agent Support Charts for Plugin Version 2.0 (V4 SDK)** link has been added. This chart provides information about third-party products supported by plugin version 2.0 and the V4 SDK. The chart for plugin version 1.0 provides information for the V3 SDK.
  - The names of some third-party products have changed. For example, the **AntiVirus** and **AntiSpyware** health classes in plugin version 1.0 are now combined in a single **AntiVirus** health class in plugin version 2.0. Also, in version 1.0 all McAfee products were categorized as VirusScan, whereas McAfee products are now categorized in a few different categories in 2.0. To review the changes, go to **Administration > Support > Documentation** and compare the product lists in the two OnGuard agent support charts.
  - Disabling Real-Time Protection (RTP) checks for antivirus products is not supported, so the **Off** option will not be available in the **Real-time Protection Status Check** field for the **AntiVirus** health class in **Posture Policies**.
  - The **Selected on Server** and **Security** options are not supported for detecting or installing missing patches on Windows, so these options will not be available in the **Install Level Check Type** field for the **Patch Management** health class in **Posture Policies**.
  - The **Display Update URL** option will not be available for the **AntiVirus** health class in **Posture Policies**.
  - Engine version checks are not supported, so the **Engine version check** option will not be available for the **AntiVirus** health class in **Posture Policies**.
- The existing **Guest - Expired** report that combines the user account and device account information in a single report is now renamed to **Guest User and Device - Expired**. (#34942)

- In **Operator Logins**, when the **Logout After** field is set to the default value of zero, ClearPass Guest will now use the same value that is configured in ClearPass Policy Manager for the **Admin Session Idle Timeout** cluster-wide parameter. (#39534)
- The ClearPass OnGuard persistent and native dissolvable agents are not supported on macOS 10.7. (#40666)
- The ClearPass OnGuard Native Dissolvable Agent is now supported on the Microsoft Edge browser. (#32664)
- For deployments that have Palo Alto Networks (PANW) configured as an endpoint, and where the ClearPass Configuration API is used to load endpoint context servers, the XML file should include the following attributes: (#39028)
  - **PA_Panorama_RegisterDevice**
  - **PA_Panorama_SendRoles**
- The ClearPass OnGuard Unified Agent now supports the **Disable USB Mass Storage Device** auto-remediation action on Windows 64-bit operating systems. (#29613)
- The Java-based OnGuard Dissolvable Agent is no longer supported on Windows, MacOS, or Ubuntu systems. Only the Native OnGuard Dissolvable Agent workflow will be used for those platforms in the 6.6.5 release and future releases. (#38141)
- For deployments that have Palo Alto Networks (PANW) configured as an endpoint, ClearPass now sends the user's ClearPass role information to PANW during login. The role is unregistered from PANW when the user logs out. (#37163, #37204)
- ClearPass now supports Windows Server 2012 and Windows Server 2012 R2 in the ClearPass OnGuard Unified Agent. (#37121)
- The ClearPass OnGuard Unified Agent and Native Dissolvable Agent for Windows can now be localized in the French language. (#37506)
- ClearPass now supports Microsoft Hyper-V Server 2016. (#37674)
- ClearPass now supports VMware vSphere Hypervisor (ESXi) 6.5. (#37675)
- ClearPass now supports MAC Notification Traps from HPE ArubaOS-Switches. This automatic notification can be used to discover new devices connected to an HPE ArubaOS-Switch or to perform an OnConnect enforcement. (#37180)
- In network discovery, if custom fingerprints are configured, now the custom rules will always be evaluated before the default rules. (#37545)
- In the ClearPass OnGuard Unified Agent, antivirus detection is now performed every two hours instead of every minute. (#37630)
- If MAC authentication is configured against an external MySQL database, parallelism is now enabled on the MySQL driver, allowing multiple queries to be sent to the MySQL server over multiple connections. (#35854)
- Non-alphanumeric characters are now accepted at the beginning of passwords. (#37160)
- The underscore character (_) is now supported in hostnames. (#37509)
- Access-requests that contain the following attributes will now be dropped only when ClearPass is in CC mode: (#37770)
  - The response attributes Password-Retry, Reply-message, or Error-Cause.
  - Both an EAP-Message and an ARAP-Password, User-Password, or CHAP-Password attribute.

- In network discovery, when endpoints do not have a MAC address, ClearPass will create MAC addresses for them that include the prefix "xa". (#37410)
- After running a subnet scan, discovered endpoints that do not have a MAC address will be displayed with a hyphen in the **MAC Address** column in the **Configuration > Identity > Endpoints** list. (#38125)
- For accounts that are configured to use only an access code instead of a username and password, the **Finished Creating Guest Accounts** results page (create_multi_result.php) now displays the **Access Code** field instead of the **Username** and **Password** fields. (#36656)
- When an iOS device is reconnecting after onboarding, a count-down timer and the message "Completing configuration, please wait <#> seconds..." are now displayed while the change of authorization (CoA) is in process, alerting the user to stay on the page until the CoA is complete. (#36277)
- IPsec Phase2 now uses the same encryption and hash algorithms that are configured for **IKE Phase1 Mode** on the **Administration > Server Manager > Server Configuration > Network tab > Create IPsec Tunnel** form. Users should be aware that if the peer does not support the configured encryption and hash algorithms, the connection will not succeed. (#34624)
- ClearPass will now drop access-request messages that contain the following attributes: (#35712)
  - The response attributes Password-Retry, Reply-message, or Error-Cause.
  - The EAP-Message attributes ARAP-Password, User-Password, or CHAP-Password.
- ClearPass will now drop the access-request packet that contains the invalid message-authenticator, and log the corresponding error message in **Event Viewer**. (#35761)
- In Insight reports, a dynamic search for endpoint IP addresses sometimes took several minutes or failed to complete. The autocomplete function is now removed from report filters and alert filters. Users should enter the full IP address in the search field. (#36641)
- The ClearPass OnGuard Unified Agent for Windows used the same Event ID number for both Healthy status and Unhealthy status in the Windows Event Viewer logs. Two separate Event ID numbers are now used: (#35746)
  - Healthy events ID is now 1029
  - Unhealthy events ID is now 1030
- Users should be aware that IPsec pre-shared keys are now limited to 128 characters. (#35786)
- ClearPass 6.6 is the last release that will support Java for the Windows or Mac OS X ClearPass OnGuard Dissolvable Agent. ClearPass 6.6.3 (cumulative patch 3) will contain the last updates to the Java-based Dissolvable Agent. No further updates will be provided.
- If you plan to download the 6.6.8 cumulative patch from the **Software Updates** portal for use with the **Cluster Update** interface on a ClearPass 6.6.0 appliance, you must first install the **ClearPass 6.6.0 Cluster Update Interface Patch**. This patch is required for ClearPass 6.6.0-based clusters in order to enable the **Cluster Update** user interface to recognize ClearPass patches and hotfixes when they have been downloaded through the **Software Updates** portal. It only needs to be installed on the publisher. This patch is NOT needed if the patches or hotfixes are manually imported into the ClearPass appliance. (#34962)
  - If you accidentally download the 6.6.8 cumulative patch before installing the **ClearPass 6.6.0 Cluster Update Interface Patch**, the **Start Update** link will be missing from the **Cluster Update** interface. To resolve this issue, delete the 6.6.8 cumulative patch, click **Check Status Now** and then download the cumulative patch again.
- Some IPsec connection encryption algorithms are no longer supported. Existing systems that have these algorithms configured will be updated to currently supported algorithms:

- ClearPass no longer supports using the 3DES encryption algorithm for IPsec connections. Existing systems that have 3DES configured will be updated to AES-128.
- ClearPass no longer supports using AES-192 for IPsec connections. Existing systems that have AES-192 configured will be updated to AES-128.
- ClearPass no longer supports using Diffie-Hellman (DH) Group 1 or 2 for IPsec connections. Existing systems that have DH Group 1 or 2 configured will be updated to DH Group 5.
- ClearPass no longer supports using IKEv1 in Aggressive Mode for IPsec connections. Existing systems that have Aggressive Mode configured will be updated to Main Mode.

- The system requirements for the CP-VA-500 virtual appliances have changed. For details, see "Virtual Appliance Requirements" on page 113.
- All VMware ESXi virtual machines now use hardware version 8.
- VMware ESX 4.0 is no longer supported.
- Changes to the TAG mappings tables to improve performance and scalability may impact SQL filters in use by custom authentication sources. The following tables have been removed and a more efficient method has been implemented. If you are currently using these tables, we recommend that you contact Aruba support prior to upgrade:
  - TIPS_AUTH_LOCAL_USER_TAG_MAPPINGS
  - TIPS_GUEST_USER_TAG_MAPPINGS
  - TIPS_NAD_CLIENT_TAG_MAPPINGS
  - TIPS_ENDPOINT_TAG_MAPPINGS
  - TIPS_TAG_VALUES
- The **Configuration > Posture > Posture Servers** page and the **Administration > Dictionaries > Posture** page have been removed.
- ClearPass VMs are now shipped as a single virtual machine installation image per hypervisor type: either VMware ESXi or Microsoft Hyper-V image. During installation, a new menu option lets the administrator select the type of image they want to install — either CP-SW-EVAL, CP-VA-500, CP-VA-5K, or CP-VA-25K. For more information, refer to the *Installing or Upgrading to ClearPass 6.6 on a Virtual Appliance* Tech Note. (#28018)
- ClearPass 6.6.0 introduces a re-designed ClearPass Insight. Not all pre-6.6.0 features are currently available, but will be added in future releases. In the new Insight, several data columns have been replaced which may impact Syslog filters after upgrade. For example, if the **Authentication** columns were used, you need to manually update the Syslog filter to use the new **Endpoint** columns. A notification or error is not displayed during upgrade, but is displayed if you open the Syslog filters and attempt to save again.
- The Aruba Linux Cryptographic Module, which is based upon OpenSSL 1.0.2h as of 6.6.1, no longer supports Diffie-Hellman parameters shorter than 1024 bits. This might impact third-party applications that have not updated their software to protect against the Logjam vulnerability.

Chapter 4
Enhancements in Previous 6.6.x Releases

This chapter provides a brief summary of the features and enhancements introduced in previous ClearPass 6.6.x releases. For a list of enhancements introduced in the ClearPass 6.6.8 release, see the What's New in This Release chapter.

This chapter includes:

APIs

Features Added in 6.6.3

ClearPass now includes the following REST APIs: (#35135, #35206, #35207, #35211, #35212, #35213, #35214, #35577, #35622, #37225)

- AccessControl
- ClusterWideParameter
- Service
- ServerSnmp
- LocalUserPasswordPolicy
- AdminUserPasswordPolicy
- EndpointContextServer
- ServerVersion
- ServerFips
- RandomPassword

CLI

Features Added in 6.6.7

- A new cluster-wide parameter, **Console Session Idle Timeout**, lets administrators configure the idle time allowed during a console session before the session times out. With this parameter configured, the CLI console will be automatically logged out if there is no keystroke in the specified time. To use this feature, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab and configure the **Console Session Idle Timeout** value as needed. The default timeout value is 360 minutes. (#37851)

Since background processes are not counted as part of an active session, setting a low console timeout value may lead to auto-logout during a system upgrade. Admins must provide an adequately high timeout value.

- When an admin user logs in to ClearPass while in Common Criteria (CC) mode through the console or via SSH, the console displays a message with the source and timestamp of the most recent successful login, as well as the number of failed attempts that were made through both SSH and the console since the most recent successful login. Details of the events will also be displayed in Policy Manager's **Event Viewer** if **Ingress logger service** is enabled at **Administration > Server Manager > Server Configuration > Services Control**. (#38903, #40651)
- The **`filename`** argument in the CLI's **`backup, system update, system upgrade, restore`** and **`dump logs`** commands now accepts filenames with alphanumeric characters and the following special characters: hyphen, period, underscore. (#40260)

Features Added in 6.6.3

- The ability to lock out the CLI based upon SSH public key authentication failures is now supported. To use this feature, first go to **Administration > Server Manager > Server Configuration** and select **Enable Ingress Events Processing** on the **System** tab. On the **Services Control** tab, start the **Ingress logger service** and the **Ingress logrepo service**. Then in the CLI, configure: (#35398)
  - **ssh lockout count** — The number of failed password attempts allowed before the account is locked (for example, **`ssh lockout count 5`**).
  - **ssh lockout duration** — The amount of time in minutes that the account will remain locked after the maximum failed SSH login attempts (for example, **`ssh lockout duration 15`**).
  - **ssh lockout mode** — Set this to **advanced**. In this mode, the account will be locked after the maximum failed SSH password or public key login attempts.
- If access to ClearPass via SSH (CLI) is attempted with unsupported protocol versions or with unsupported encryption or cryptographic hash algorithms, an alert is now logged in the **Event Viewer**. This feature requires the **Enable Ingress Events Processing** option and services to be enabled for the server at **Administration > Server Manager > Server Configuration**. (#35402)
- Two new CLI commands, **`show ports`** and **`configure port`**, were added for displaying and filtering incoming or outgoing traffic on the particular port. The **`show ports`** command shows the status of all the ports, and the **`configure port`** command is used to configure the filtering of a given port. (#35801)
- ClearPass will now log **Event Viewer** entries for CLI session (SSH) idle timeout scenarios. This feature requires Ingress Event Engine options and services to be enabled. (#36320)

Features Added in 6.6.1

Support was added for a timed `SSH lockout` feature. This provides the ability to lock the CLI account for a specified duration after a maximum number of consecutive password failures. This feature can only be

configured in the CLI for this release. (#34852)

- Use the `ssh lockout count X` command, where `X` is the number of failed authentication attempts, before a lockout. The default is five attempts.
- Use the `ssh lockout duration X` command, where `X` is the number of minutes from 1-10080, to specify the duration of the lockout after the count has been exceeded. The default is 15 minutes.
- Use the `ssh lockout reset` command to unlock the appadmin account. This can always be done through console.

Cluster Upgrade and Update

Features Added in 6.6.0

The Cluster Upgrade Tool, which automates the process of upgrading a ClearPass cluster, is now natively available within Policy Manager's Administration module, and includes additional enhancements: (#28327, #28454)

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

Endpoint Context Servers

Features Added in 6.6.7

- A **Compliance** attribute for endpoint entities was added to the **Attributes** dictionary, and is used to summarize an endpoint's posture against AirWatch corporate policy. Values for this attribute are **NotAvailable**, **NonCompliant**, or **Compliant**. The AirWatch "ComplianceStatus" attribute maps to the ClearPass **Compliance** endpoint attribute. (#38630)
- For ClearPass deployments that are integrated with Palo Alto Networks firewalls running PANOS 7.1.5+, ClearPass now sends a timeout parameter of zero to these firewalls to ensure that the active user information does not expire. This overrides the firewall's default timeout of 60 minutes in PANOS 7.1.5 + (#39084)

Features Added in 6.6.5

- For deployments that have Palo Alto Networks (PANW) configured as an endpoint, and where sending large amounts of information might cause performance concerns, new UI options and API attributes can be used to send device registration and ClearPass role information to PANW. (#38189, #38507, #39208)
  - To use this feature from the UI, go to **Administration > External Servers > Endpoint Context Servers > Add**. Select either **Palo Alto Networks Firewall** or **Palo Alto Networks Panorama** as the server type, and then configure the following two fields:
    - **ClearPass Profiler** — To enable sending endpoint profiling context to PANW, select this check box. This option is enabled by default.
    - **ClearPass Role** — To enable sending ClearPass role information to PANW, select this check box. This option is disabled by default.
  - If you use the ClearPass Configuration API to load endpoint context servers, you should include the following attributes in the XML file:
    - **PA_Panorama_RegisterDevice**
    - **PA_Panorama_SendRoles**

Features Added in 6.6.4

- For deployments that have Palo Alto Networks (PANW) configured as an endpoint, ClearPass now sends the user's ClearPass role information to PANW during login. The role is unregistered from PANW when the user logs out. (#37163, #37204)

Users should be aware that this change might cause performance issues for deployments that have PANW configured as an endpoint. If this is a concern, we recommend that you not apply the 6.6.4 patch and instead wait for further enhancements in a future patch.

Features Added in 6.6.3

The Aruba Activate Connector has been enhanced to support API calls to download larger numbers of endpoints (for example, 50K) by using pagination. (#35871)

Features Added in 6.6.1

- For AirWatch integrations where polling for full endpoint details is not needed, that secondary poll can now be disabled. To use this feature, go to the **Administration > External Servers > Endpoint Context Servers > Add > Server** tab. In the **Security Details** field, use the **Enable to fetch Endpoint Security Info** option: (#32578)
  - To disable the secondary poll, leave this check box unselected. The MDM connector will only make an API call to list the devices. It will not make a secondary API call for details of each device, so polling time will be reduced. The secondary poll is disabled by default.
  - To enable the secondary poll, select this check box. The MDM connector will make the API call for each device's details, and the polling time will be the same as it was in earlier ClearPass releases.
- Namespace and context attributes are now commonly accessible. This enables the Post-Auth module to receive HTTP-action content either partly filled or fully filled (previously, no values were received if any were missing). The user can now modify HTTP-action content by adding or removing parameters from the user interface without having to depend on Post-Auth changes. To use this feature, go to **Administration > Dictionaries > Context Server Actions**. To create a new custom action you may either click **Add** or make a copy of an existing action and then click its row in the list. On the **Content** tab of the **Endpoint Context**

Server Details form, modify parameters in the **Content** field to create the custom context server action. (#33934)

- In a SOTI MDM environment, ClearPass now marks a device as unmanaged if the SOTI supplicant is removed from the device. (#34107)

Features Added in 6.6.0

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

Guest

Features Added in 6.6.7

In **Operator Logins**, when the **Logout After** field is set to the default value of zero, ClearPass Guest will now use the same value that is configured in ClearPass Policy Manager for the **Admin Session Idle Timeout** cluster-wide parameter. This is the amount of idle time after which an operator's session will be terminated. If a cumulative patch is applied, this field will retain the value that was configured for it before the patch. (#39534)

Features Added in 6.6.3

- Support was added for MS-CHAP authentication with Xirrus controllers. To use this feature, on either the **Configuration > Pages > Guest Self-Registrations** form or the **Configuration > Pages > Web Logins** form, select **Xirrus** in the **Vendor Settings** field and then specify **MS-CHAP with shared secret** in the **Password Encryption** field. (#36615)
- In multi-factor authentication (MFA) workflows, auto-enrolling new users is now an opt-in choice instead of the default for some providers. To use this feature, if you select Facial Network, ImageWare Systems, or Kasada as the provider in **Multi-Factor Authentication** configurations, select the **Enroll** check box to allow auto-enrolling usernames with the provider. (#36657)

- Multi-factor authentication (MFA) workflows no longer require device-level checking at every authentication. Instead, a **Grace Period** field in **Multi-Factor Authentication** configurations lets you specify an interval between MFA checks. To use this feature, enter a number of hours after the secondary authentication before authentication would be required again. As long as the device name and username are still the same, the user can skip the secondary check if they log in again before the interval expires. If you wish to require authentication every time, the **Grace Period** field can be left empty. The default interval is 24 hours. (#36659)
- ClearPass now supports Kasada Authenticator as a multi-factor authentication vendor. (#36660)
- The list of public profile attributes that are retrieved by default for social logins is increased. ClearPass now automatically detects all major attributes for Facebook and LinkedIn social logins. (#37226)

Features Added in 6.6.2

- Support was added for configuring a source address Numbering Plan Indicator (NPI) and for null termination of C-Octet Strings on SMPP SMS servers. To use this feature, go to **ClearPass Guest > Configuration > SMS Services > Gateways > Create new SMS gateway** and select **SMPP v3.4** as the **SMS Gateway**. (#35357)
- In social logins, support was added for login with Clever. Using an OAuth2-based Single Sign-On workflow with access to Student Information Systems (SIS) identity sources, this option offers schools enhanced access control, preserving bandwidth. (#35641)
- The FIAS Micros transaction processor includes several new enhancements: (#36029)
  - Timestamps used in the FIAS protocol are now relative to the ClearPass system's time. If the hotel Property Management System (PMS) and ClearPass are in different time zones, the time zone can be overridden in the **Transaction Processor Configuration** form at **ClearPass Guest > Configuration > Hotspot Manager > Transaction Processors**.
  - FIAS transaction processors can now be configured to send a periodic keepalive command. A keepalive may be needed in scenarios where room updates are infrequent, or if other networking devices such as switches or firewalls can otherwise drop connections. The FIAS transaction processor has two options for keepalive commands: **Link Start** (LS) and **Link Active** (LA). Only the LS command will receive a response from the PMS software. To use this feature, create a new transaction processor with a FIAS gateway and configure the **Keep Alive** field on the **Transaction Processor Configuration** form.
  - The room transaction details shown on the **Occupied Room List** page are now displayed in real time.
  - The **Occupied Room List** page also includes a summary of current information regarding the connection to the PMS software. You can see current connection status, recent commands received, and any pending or queued payment requests.
  - A new transaction processor action is available to overcome out-of-sync room information. If room data appears to be stale, a **Re-Synchronize Rooms** link is available on the **Transaction Processors** page. Users should be aware that choosing this option will cause all current room data and any pending payment requests to be lost.

Features Added in 6.6.1

- When enabling SSO for ClearPass Guest, you can now distinguish between guest Web logins and guest operator logins. The new **GuestOperators** option for operator logins is available at **Policy Manager > Configuration > Identity > Single Sign-On (SSO)**. (#34680)
  - If only the **GuestOperators** option is selected, SSO will be enabled for operator logins only, and Web logins will use normal non-SSO authentication.

- If only the **Guest** option is selected, SSO will be enabled for Web logins only, and operator logins will use normal non-SSO authentication.
- If both the **GuestOperator** and the **Guest** options are selected, then operator logins and Web logins will both use SSO authentication.

- Email notifications for account expiration may now be sent as many as 30 days prior to the expiration date. To use this feature, go to **Configuration > Guest Manager**, enable **Expiration Warning Options**, and enter a number from 1 to 30 in the new **Account Expiry Notification** field. The default value is 1 day, matching the behavior in previous releases. (#34474)
- You can now extend a guest account's expiration window each time the password is changed. This allows an account's lifetime to be automatically renewed in cases where it would otherwise expire before the next required password change. To use this feature, go to **Configuration > Pages > Guest Self-Registrations** and edit a registration page. In the **Self-Service Portal** form, the **Change Password** area includes the new **Extend Expiration** field. (#34477)
- Pages rendered with the stock skin now declare their language in the HTML header. (#34840)

Features Added in 6.6.0

- ClearPass Guest now supports **SMPP v3.4** as an SMS gateway. This option is available at **Configuration > SMS Services > Gateways** in the **SMS Gateway** field. (#9747)
- The **expire_timezone** field is now stored as a persistent guest field. Receipts and edits made after an account is created are now displayed in the account's local time zone. (#26032)
- Hotspot Manager now includes the following enhancements for customizing Payment Management System (PMS) plans based on data about the hotel guest: (#27691, #28539, #28540)
  - Hotel hotspot plans can be created so that guest accounts expire on the expected day of departure. On the hotspot plan configuration form, the **Time Tracking** field includes a new option, **Checkout date - Expiration will be midnight the day of the checkout (Hotel PMS only)**.
  - Hotel hotspot plans can be created so that new devices can use a plan that is already created and paid for. On the hotspot plan configuration form, the **Time Tracking** field includes a new option, **Already paid - Select for other devices to share a paid plan (Hotel PMS only)**.
- A new option in Social Logins configurations, **Friends**, allows retrieval of the guest's friends list when Facebook is selected as the provider. Permission must also be granted by the guest, and only friends who also use your application ID can be retrieved. (#27836)
- A new option in Social Logins configurations, **Google Groups**, allows retrieval of Google Group membership information when Google is selected as the provider. If this option is selected, the **Admin SDK Refresh Token** and **Authorization Code** must also be regenerated. (#27882)
- A new **Terms and Conditions** Web page template has been added to the list of templates at **Configuration > Pages > Web Pages**. This page can be customized and used to present your terms and conditions of use to guests, and is referenced by the **Terms Of Use URL** field on the **Configuration > Guest Manager** form. (#28156)
- ClearPass now provides multi-factor authentication for guest logins. Multi-factor authentication lets you require multiple factors, or proofs of identity, when authenticating a user. To configure multi-factor authentication (MFA) in ClearPass, you first create an account with an MFA provider and create the users for the guest account. You then set up either a captive portal login or an Onboard login. The list of MFA providers currently supported in ClearPass includes Duo Security Two Factor Authentication, Facial Network ZOOM Multi-Factor Authentication, Imageware Systems GoMobile Interactive, and SMS Verification Codes. Multi-factor authentication can be configured in ClearPass Guest at **Configuration > Pages > Web Logins**, and at **Onboard > Deployment & Provisioning > Provisioning Settings > Web Login**. For

more information, see "About Multi-Factor Authentication" in the *ClearPass Guest User Guide*. (#28452, #30199, #30420, #32711)

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

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

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

- Time-based policy: Policy might require MFA on a daily or weekly basis, or if the user has not logged in from the device for a certain number of days, or if the device was unhealthy in the past 30 days.
- Posture-based policy: Policy might require MFA if the device's posture changes to unhealthy, or if the posture of any of the user's other devices changes to unhealthy, or if a company alert or security check is issued.
- Policy based on other conditions: Policy might require MFA if the user has never logged in from the location before, or has failed authentication three times, or if a third-party application or system triggers MFA.

- A new option, **Arbitrary Sort**, is available in the API Framework Plugin configuration. This option lets you override default sort-field settings and specify any field as the sort column through the API. (#29462)
- The page loading time is faster for admin pages with HTML editing areas that include content item drop-down lists. (#31087)
- Social login support was added for Microsoft Azure Active Directory. (#32338)
- Support was added for Norwegian translations in many guest-facing pages. (#33470)

Insight

Features Added in 6.6.7

- Two new reports let you view information specifically about either expired user accounts or expired device accounts. To use these reports, go to **Insight > Reports > Create New Report**. In the **Category** drop-down list select **Guest Authentication**, and then select and configure either the **Guest Devices - Expired** template or the **Guest Users - Expired** template. (#34942)

The existing **Guest - Expired** report that combines the user account and device account information in a single report is now renamed to **Guest User and Device - Expired**.

Features Added in 6.6.3

- A new **Onboard Enrollment** report lets you view information about the onboarded devices. To use this report, go to **Insight > Reports > Create New Report**. In the **Category** drop-down list select **Onboard**, and then select the **Onboard Enrollment** option. (#29300)
- The **Onboard Certificate Report** template now shows a **Revoked Devices** count and a pie chart for **Revoked Onboard Device Distribution**. (#33676)

- The count of unique devices and the total number of devices onboarded per user are now available in the **Onboard Enrollment** report template (#35765)
- The Insight database now includes the Framed-IPv6-Address attribute value (the supplicant IPv6 address) to support filtering and reports based on Framed-IPv6-Address. (#36311)

Features Added in 6.6.2

- A new **Guest - Expired** report lets you view information about expired guest accounts. To use this report, go to **Insight > Reports > Create New Report**. In the **Category** drop-down list select **Guest Authentication**, and then select the **Guest - Expired** option. (#34943)
- Support was added to Insight reports and searches for filtering by endpoint IP address and by username. A new widget is also added to the accounting reports to provide an overview of authentications per domain. (#35381)

Features Added in 6.6.1

- Insight's **OnGuard Posture** reports now include a **Hostname** column. In scenarios where two MAC addresses might be recorded for a single host if the user makes a wired or wireless connection, the machine hostname can uniquely identify the endpoint. (#29075)
- A new **Endpoint Overview** report lets you view information for endpoints that were added to the network but not yet authenticated. To use this report, go to **Insight > Reports > Create New Report**. In the **Category** drop-down list select **Endpoint**, and then select the **Endpoint Overview** option. (#31753)
- Insight alerts for failed authentications can now be filtered by Network Access Device. To use this feature, go to **Insight > Alerts > Configuration > Create New Alert**. Set the **Category** to **Authentication > Failed Authentication**, and then select **NAD IP** in the **Filter** drop-down list. (#33814)
- A new **Social Login** report lets you view information for social media. To use this report, go to **Insight > Reports > Create New Report**. In the **Category** drop-down list select **Guest Authentication**, and then select the **Guest - Social Login** option. (#34135)

Features Added in 6.6.0

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

  The new Insight UI includes:

  - Counts summary — Counts for **Total Auth**, **Failed Auth**, **Unique Endpoints**, **Unique Users**, and **Alerts Created** are displayed at the top of each page.
  - **Dashboard** section — This item in the left navigation opens the **Dashboard** home page, which displays several report widgets. Subheadings in the left navigation let you display pages for any of the following categories: **Authentication**, **Endpoints**, **Guest**, **Network**, **Posture**, **System**, or **System Monitor**. Whether you are on the Dashboard home page or one of its subheadings, controls in each widget let you create a report or alert for it. You can also customize the Dashboard home page by adding or removing widgets. The default look-back window for the data in each widget is 24 hours. An exception to this is the System Monitor widget, which shows data for the previous two hours.
  - **Reports** section — This item in the left navigation opens the **Reports** home page, which displays the "news feed" activity summaries for **Yesterday**, **Today**, and **Tomorrow**, the list of **Created Reports**, and the **Create New Report** button. You can click the name of a report in the list to view it in a new tab, or click the **Configuration** subheading in the left navigation to edit a report. Creating a new report is

simple and easy, with a wizard to walk you through each step. Report categories available in this release are authentication, endpoint, guest authentication, network, OnGuard (Linux, Mac, and Windows), Onboard, RADIUS authentication, system, and TACACS.

- **Alerts** section — This item in the left navigation opens the **Alerts** home page, which displays the list of created alerts and the **Create New Alert** button. You can click the name of an alert in the list to view it in a new tab, or click the **Configuration** subheading in the left navigation to edit an alert. Alert categories available in this release are authentication, system, and TACACS.
- **Administration** section — This item in the left navigation opens the Insight **Administration** home page, where you can work with file transfer settings and database settings.
- **Search** field — Allows searching by username (Username or Auth_username), endpoint (Host, MAC, or Host IP), ClearPass appliance (ClearPass Server IP or name), or network device (NAD IP, NAD Name, or NAD MAC). The **Search** field can auto-complete
- Workflow — The new workflow for creating or editing a report or alert is simple and intuitive.
- Differentiated user access — Insight now supports multi-level administrator access:
  - Each of the Insight modules (Dashboard, Reports, Alerts, Administration) can have three privilege levels or no privilege: read, read/write, or read/write/delete.
  - A login area on each page of the Insight user interface lets the user log in as an administrator or super administrator.
  - In the case of no privilege, the link on the left navigation won't be visible for a user who does not have the appropriate privilege.
  - Users can be assigned Insight privileges from two locations: **Guest > Administration > Operator Logins > Profiles**, and **Policy Manager > Users and Privileges > Admin Privileges**.

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

- The Insight OnGuard reports now include Posture Evaluation Results as part of Raw data. The following health classes indicate which checks failed for these health classes: (#29783)
  - AntiSpyware
  - AntiVirus
  - Disk Encryption
  - File Check
  - Firewall
  - Installed Applications
  - Network Connections
  - P2P
  - Patch Management
  - Processes
  - Registry Keys
  - Services
  - USB Devices
  - Virtual Machines
  - Windows Hotfixes

- Support for Domain Name was added to the inbound legacy API and the OAuth2-based API. (#30469)

Onboard

Features Added in 6.6.7

- When setting up a new Registration Authority, you can now customize the subject used in certificate signing requests generated by the Onboard SCEP server. To use this feature, go to **Onboard > Certificate Authorities > Create new certificate authority**, create a new CA with **Registration Authority** as the mode, and then click **Fetch CA Certificate**. In the **Certificate subject** field, select the **Customize certificate subject** check box and enter the information for the **SCEP Client**, **SCEP Signing**, and **SCEP Encryption** areas. The details you enter are used to create Distinguished Names for the client certificate used for communication with the CA, and for the server certificates used to sign and encrypt SCEP responses. (#40465)

Features Added in 6.6.2

- Support was added for using Onboard as a Registration Authority (RA). When this option is used, instead of issuing certificates, Onboard will proxy a certificate request to another Certificate Authority (CA) via SCEP. The issued certificate is included in the certificate list. To use this feature, go to **ClearPass Guest > Onboard > Certificate Authorities > Create new certificate authority** and select **Registration Authority** in the **Mode** field. After you configure the SCEP-RA certificate, you can specify the CA to use for TLS client certificates independently of the CA used for enrollment: At **Guest > Onboard > Deployment and Provisioning > Provisioning Settings**, the **General** tab now includes a **TLS Certificate Authority** field. Both the **TLS Certificate Authority** and the **Certificate Authority** fields include the **SCEP-RA** option. This functionality has been validated with Microsoft Active Directory Certificate Services (ADCS) and ClearPass Onboard CAs. (#35579)

Features Added in 6.6.0

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

OnConnect Enforcement

Features Added in 6.6.3

During OnConnect Enforcement, the domain name and the machine name are now fetched along with the logged-in username. The domain name can be used as an attribute for the enforcement policy. (#34953)

Features Added in 6.6.2

- OnConnect Enforcement is no longer in feature-preview mode and can now be used in a ClearPass cluster. OnConnect can be enabled on a per-appliance basis and roles can be assigned per zone. In each zone, one primary master and one secondary master must be designated. If the primary master fails for any reason, the secondary master takes over until the designated primary master is back on line. Only the primary master in each zone will trigger OnConnect Enforcement. To use this feature, go to **Administration > Server Manager > Server Configuration** and select a server in the list. In the **OnConnect Setting** field, select the **Enable OnConnect** check box, and then select either **Primary master** or **Secondary master** in the drop-down list. (#34418, #34419)
- Network Access Devices (NADs) can now be assigned to a zone, allowing the SNMP service to poll or query only the NADs that are in its zone. As part of this feature, the **Zone** drop-down list at **Configuration > Network > Devices** is renamed **Policy Manager Zone** and is moved to the **SNMP Read Settings** tab instead of the **OnConnect Enforcement** tab. (#34421, #35767)
- Support was added for querying and selecting port names for the Network Access Device for OnConnect Enforcement. To use this feature, go to **Configuration > Network > Devices** and enable SNMP Read and OnConnect Enforcement for a device. On the **OnConnect Enforcement** tab click **Query Ports**, select the ports to use, and click **Add to Port Names**. Alternatively, port names may be entered as comma-separated values. (#34424)

Features Added in 6.6.1

ClearPass 6.6.1 includes a new feature called ClearPass OnConnect Enforcement. This feature enables ClearPass to detect and apply enforcement to endpoints connected to wired switches without the need to enable AAA methods such as 802.1x or MAC Authentication. Using standards-based SNMP, wired switches can notify ClearPass when a new device has connected. Then using the native profiling capabilities of ClearPass, it can match the learned MAC address against profiled information to apply a policy using SNMP. OnConnect Enforcement can also use information from Windows Management Instrumentation (WMI) to identify the user in the case of a domain-joined computer in order to apply identity-aware enforcement policies. This also allows enforcement in non-AAA environments without the need for an agent, such as OnGuard, on the endpoint. (#34416, #34422)

Prerequisites:

- Configure SNMP v2c or v3 MIB access on the wired switch.
- Configure SNMP traps from the wired switch to the ClearPass appliance.
- Define a Network Access Device with SNMP information and physical ports to be used with OnConnect Enforcement (at **Configuration > Network > Devices**).
- Configure Windows Management Instrumentation details in the Profile settings (at **Configuration > Profile Settings > WMI Configuration**).
- Configure a service using the ClearPass OnConnect Enforcement template (at **Configuration > Services > Add**, select **ClearPass OnConnect Enforcement** in the **Type** drop-down list).

Sample Workflow:

1. Log in to a domain-joined endpoint.
2. Connect the endpoint to the port configured for OnConnect Enforcement.
3. The switch will send an SNMP trap to ClearPass with the endpoint MAC details.
4. ClearPass will learn of the endpoint IP and device details through profiling (for example, DHCP).
5. Using WMI, ClearPass will then initiate a scan against the endpoint to identify the logged-in user.
6. Based upon the user information, the endpoint can be placed into an appropriate VLAN or have its port bounced to apply a different policy.

OnConnect Enforcement is in feature-preview mode for ClearPass 6.6.1. It is made available for use in proof-of-concept environments and only tested with a limited number of Cisco and HPE ArubaOS- Switch platforms with domain-joined clients in this release. Support for additional third-party vendors and workflows will be added in subsequent releases.

OnGuard

- For the OnGuard Plugin version 1.0 (V3 SDK), enhancements and support were added as shown below: (#32719, #33905, #33906, #35597, #35706, #36280, #36362, #37091, #37529, #36281, #38270, #39219, #39256)

  Support was added for the following products:

  - AhnLab V3 Endpoint Security 9.x (Windows)
  - AhnLab V3 Internet Security 9.0 antivirus
  - Avast Free Antivirus 17.x (Windows)
  - Avast Free Antivirus 12.x (Windows)
  - Avast Free Antivirus 11.x (Windows)
  - Avast Pro Antivirus 17.x (Windows)
  - Avast Pro Antivirus 12.x (Windows)
  - Avast Pro Antivirus 11.x (Windows)
  - Avast Internet Security 17.x (Windows)
  - Avast Internet Security 12.x (Windows)
  - AVG AntiVirus 2016.x (Windows)
  - AVG AntiVirus Free 17.x (Windows)
  - AVG AntiVirus Free Edition 16.x (Windows)
  - Avira Free Antivirus 15.x (Windows)
  - Bitdefender Antivirus for Mac 5.x (macOS)
  - Bitdefender Endpoint Security for Mac 4.x (Mac OS X)
  - Bitdefender Internet Security 21.x (Windows)
  - Bitdefender Total Security 21.x (Windows)
  - Check Point Endpoint Security 8.x (Mac OS X)
  - Check Point Endpoint Security [Firewall] 8.x (Mac OS X)

- Check Point Endpoint Security 7.x
- ESET Internet Security 10.x (Windows)
- ESET Smart Security 10.x (Windows)
- F-Secure Anti-Virus for Mac 16.x (macOS)
- HP Drive Encryption 8.x (Windows)
- Hyper-V Manager 10.x (Windows)
- Kaspersky Anti-Virus 16.x (Mac OS X)
- Kaspersky Anti-Virus 16.x (Windows)
- Kaspersky Internet Security 16.x (Mac OS X)
- Kaspersky Internet Security 16.x (Windows)
- Kaspersky Total Security 16.x (Windows)
- MacKeeper 3.X (Mac OS X)
- McAfee Endpoint Security for Linux Threat Prevention 10.x (Linux)
- McAfee Endpoint Security for Mac 10.x (Mac OS X)
- McAfee Endpoint Security Threat Prevention 10.x (Windows)
- McAfee ePolicy Orchestrator Agent 5.0.2
- McAfee Personal Firewall 16.x (Windows)
- McAfee VirusScan 20.x (Windows)
- McAfee VirusScan 19.x (Windows)
- McAfee VirusScan 18.x (Windows)
- Oracle VM VirtualBox 5.x (Windows)
- Quick Heal Internet Security 17.x (Windows)
- SafeGuard 8.x (Windows)
- Security and Patch Manager 10.x (Windows)
- Sophos Anti-Virus 11.x (Windows)
- Symantec Endpoint Protection 14.x
- Symantec Hosted Endpoint Protection 3.x (Windows)
- Symantec Hosted Endpoint Protection 2.x (Windows)
- Trend Micro Internet Security 7.x (macOS)
- Trend Micro Internet Security 6.x (Mac OS X)
- Trend Micro Security for Mac 3.x (macOS)
- Trend Micro Worry Free Business Security Agent 6.x (Windows)
- VMware Workstation 12.x (Windows)

Support was enhanced for the following products:

- Avast Endpoint Protection Suite 8.x (Windows)
- Avast Free Antivirus 12.x (Windows)
- Avast Internet Security 12 (Windows)

- Avast Mac security 12.x (macOS)
- Avira Free Antivirus 15.x (Windows)
- Bitdefender Antivirus Free Edition 1.x (Windows)
- BitLocker Drive Encryption 6.x (Windows)
- Casper Suite 9.x (Mac OS X)
- Check Point Endpoint Security Antivirus 8.x (Windows)
- ESET Cyber Security 6.x (Mac OS X)
- ESET Cyber Security 6.x (Windows)
- ESET Endpoint Antivirus 6.x (Mac OS X)
- ESET Endpoint Antivirus 6.x (Windows)
- ESET Endpoint Antivirus 5.x (Windows)
- ESET Endpoint Security 6.x (Windows)
- ESET Endpoint Security (Windows)
- Kaspersky Anti-Virus on Mac 15.x (Mac OS X)
- Kaspersky Endpoint Security 10.x (Mac OS X)
- Kaspersky Endpoint Security 10.x (Windows)
- Kaspersky Internet Security 16.x (macOS)
- Kaspersky Total Security (Windows)
- McAfee Endpoint Security Firewall 10.x (Windows)
- McAfee Endpoint Security Threat Prevention 10.5 (Windows)
- McAfee Host Intrusion Prevention 8.x (Windows)
- McAfee Virus Enterprise 8.8.06000 (Windows)
- McAfee VirusScan Enterprise 8.x (Windows)
- Malwarebytes Anti-Malware 2.x (Windows)
- Microsoft Windows Firewall 10.x (Windows)
- Norton 360 22.x (Windows)
- Norton AntiVirus 22.x (Windows)
- Norton Internet Security Online 22.x (Windows)
- Norton Security 22.x (Windows)
- Norton Security 7.x (macOS)
- Norton Security with Backup 22.x (Windows)
- PGP Whole Disk Encryption 10.x (MacOS)
- Sophos Anti-Virus 9.x (Mac OS X)
- Symantec Endpoint Protection 14.x (Windows)
- Symantec Endpoint Encryption 11.x (Windows)
- System Center Endpoint Protection 4.x (Mac OS X)
- System Center Endpoint Protection 4.x (Windows)

- Symantec Hosted Endpoint Protection 3.x (Windows)
- System Center Endpoint Protection (Windows)
- Trend Micro Security for Mac 3.x (macOS)
- Webroot AntiVirus 9.x (Windows)

Features Added in 6.6.7

- The ClearPass OnGuard Agents for Windows and macOS now support the OnGuard plugin version 2.0, which provides faster performance, enhanced product detection, and more efficient resource allocation. ClearPass 6.6.7 supports both the 1.0 and 2.0 plugin versions by default, but because plugin version 2.0 includes significant enhancements, we recommend that you upgrade from version 1.0 to 2.0 as soon as possible. (#36176, #36386, #36396, #36517, #40370, #36511)

  The new OnGuard plugin version 2.0 is based on the OESIS V4 SDK, while the earlier plugin version 1.0 is based on the OESIS V3 SDK. After you update your ClearPass version to ClearPass 6.6.7, OnGuard will continue to use plugin version 1.0 and your existing V3 SDK policies until you explicitly upgrade to plugin version 2.0. When you are ready to upgrade to plugin version 2.0, you will first upgrade the OnGuard agents, after which you create a new enforcement profile, posture policy, and Web Auth service, and modify any existing V3 SDK enforcement policy to use the V4 SDK. For complete information about the upgrade process, including a list of important points to be aware of, please refer to the "Upgrading from OnGuard Plugin Version 1.0 to 2.0" section of the *ClearPass Policy Manager User Guide*.

  Some options that are available when using OnGuard plugin version 1.0 are not supported when using 2.0, and some options have changed. For a list of changes in fields and behaviors when using 2.0, see "Change of Behaviors in the 6.6.8 Release" on page 11

OnGuard customers are encouraged to test the OnGuard plugin version 2.0 upgrade in a lab environment prior to moving to production. Policy differences between plugin versions 1.0 and 2.0 should be evaluated individually by administrators to ensure that the desired security policy continues to be enforced after upgrading to 2.0. Some third-party products and posture policy options have been renamed or are no longer available, and policies should be updated to reflect these changes. Until you upgrade to 2.0, existing 1.0 policies will continue to work correctly.

- OnGuard now provides the ability to show end users a custom interface, or wizard, that guides them through the remediation process if their device is quarantined. When this feature is enabled and OnGuard needs to run a custom remediation script, the wizard tells the user why the device was denied network access and describes the tasks that are required to fix the problem. While the script is being executed and new health checks are run, status and progress messages are displayed. The user can close the wizard at any time and the remediation script will continue to execute in the background. This feature is only available for the Windows OS. For complete information about setting up the custom user interface, please refer to the "Creating OnGuard Custom Web Pages" section of the *ClearPass Policy Manager User Guide*. (#38273)

  The pages of the wizard are created using ClearPass Guest's **Web Pages** configuration forms, and can be customized with logo, text, and images. To use this feature:

  - Go to **Administration > Agents and Software Updates > OnGuard Settings** and use the options in the new **Agent Remediation User Interface Customization** area to enable the custom user interface, configure its behavior, and create and design the pages the end user sees.
  - At **Configuration > Enforcement > Profiles**, select or add the **Agent Enforcement** profile and configure the **Show Custom UI for Custom Scripts** attribute for it. Then add the **Agent Script Enforcement** profile and configure the **Success Message**, **Failure Message**, **Progress Message**, and **Description** attributes.

- The ClearPass OnGuard Agent for Windows now logs auto-remediation results for the **Services** health class in the Windows Event Viewer. These items are listed with the **Event ID 1034**. (#38943)
- A new Global Agent Settings parameter, **Use Current OS Language (Windows Only)**, enables the ClearPass OnGuard Unified Agent to use the current user's display language, if supported, overriding the language that was selected during installation. This parameter applies only to Windows clients. To use this feature, go to **Administration > Agents and Software Updates > OnGuard Settings > Global Agent Settings** and add the **Use Current OS Language (Windows Only)** parameter. (#39467)
- A new attribute, **Server Communication Mode**, provides OnGuard support for using the IP, hostname, or fully qualified domain name (FQDN) while communicating with the ClearPass server. As a prerequisite for using the hostname or FQDN as the server communication mode, the ClearPass Server's hostname and FQDN should be resolvable on the client. This feature is only available for the Windows persistent agent. To use this feature, to **Administration > Agents and Software Updates > OnGuard Settings > Global Agent Settings**. Add the attribute **Server Communication Mode** and select either **IP**, **HostName**, or **FQDN** as the value. (#39915)
- A new attribute, **Host:OSNameVersion**, provides OnGuard support for creating posture policies for different versions of Windows 10 based on the OS name or OS build number — for example, "2015 LTSB" or "2016 LTSB." To use this feature, go to **Configuration > Services > Add**. On the **Service** tab, select **Web-based Health Check Only** in the **Type** field, and enter a **Name** that clearly associates the health check with the appropriate Windows version. In the **Service Rule** area, click to add a new rule. Select **Host** as the rule **Type**, select the new attribute **OSNameVersion** as the **Name**, and select **CONTAINS** as the **Operator**. In the **Value** field, create the group name according to the version name — for example, "Windows 10 Enterprise 2016 LTSB". The **Host:OSNameVersion** attribute can also be used in role mapping. (#39941, #39967)

Features Added in 6.6.5

- The ClearPass OnGuard Unified Agent now supports the **Disable USB Mass Storage Device** auto-remediation action on Windows 64-bit operating systems. (#29613)
- The ClearPass OnGuard Native Dissolvable Agent is now supported on the Microsoft Edge browser. (#32664)
- A new Global Agent Settings parameter, **Server Certificate Validation**, enables the ClearPass OnGuard Unified Agent to validate the ClearPass Server Certificate when it sends a WebAuth health request to ClearPass. To use this feature, go to **Administration > Agents and Software Updates > OnGuard Settings > Global Agent Settings** and add the **Server Certificate Validation** parameter. Users should be aware that in the 6.6.5 release, OnGuard uses the ClearPass server IP address for communication, so the server certificate Common Name (CN) should be the server IP address. (#37175)

Features Added in 6.6.4

- ClearPass now supports Windows Server 2012 and Windows Server 2012 R2 in ClearPass OnGuard Agent. (#37121)
- The ClearPass OnGuard Unified Agent and Native Dissolvable Agent for Windows can now be localized in the French language. (#37506)
- A new option, **Product Evaluation Rule**, was added to the **Patch Management** health class. This option allows AND/OR conditions between patch management products, enabling ClearPass to set the health status of the Patch Management health class based on the status of all the configured products. To use this feature, go to **Configuration > Posture > Posture Policies > Posture Plugins > ClearPass Windows Universal System Health Validator**. Enable **Patch Management** checks for the appropriate operating system, and configure rules for product evaluation. (#37540)

- The Windows Hotfixes health class now lets you check a group of hotfixes. To use this feature, go to **Configuration > Posture > Posture Policies > Posture Plugins > ClearPass Windows Universal System Health Validator**. Enable **Windows Hotfixes** checks for the appropriate operating system, and configure rules for Windows hotfixes groups. The following checks are supported: (#37541)
  - All the hotfixes from a group should be present
  - Any hotfixes from the group should be present
  - All the groups should be Healthy
  - Any group should be healthy

Features Added in 6.6.3

- A new attribute, **Host:OSName**, is now available for service rules, and allows you to select a WebAuth Service based on an operating system name — for example, "Host:OSName CONTAINS Windows 8.1". To use this feature, go to **Policy Manager > Configuration > Services > Add**. (#35531)
- Support was added for the LiveUpdate method for McAfee Endpoint Security Threat Prevention 10.x. (#36520)

Features Added in 6.6.2

- A new enforcement profile, **Agent Script Enforcement**, was added. It allows admins to execute external scripts or programs on endpoints by using the ClearPass OnGuard Unified Agent as part of agent enforcement. With this profile, OnGuard can execute external scripts or programs stored in the local endpoint or on an external http/https server. The Agent Script Enforcement profiles you create are available in WEBAUTH (SNMP/Agent/CLI/CoA) type enforcement policies. To use this feature, go to **Configuration > Enforcement > Profiles > Add** and select **Agent Script Enforcement** in the **Template** drop-down list. (#34136, #34532)

  This feature allows Multiple Agent Script Enforcement policies to be defined. These policies can then be mapped against different System Posture Tokens (SPT) or Application Posture Tokens (APT). An APT is another term for a Health Class. Below is an example of multiple Agent Script Enforcement profiles that can be defined in a single policy.

  If **Condition** = **Posture:WindowsUniversal:Services *NOT_EQUALS* HEALTHY**

  Then **Actions** = **agent-script-remediate-services**

  If **Condition** = **Tips:Posture *NOT_EQUALS* HEALTHY (0)**

  Then **Actions** = **agent-script-remediate-client**

  Admin users can configure various attributes for the script to be executed, such as **Path Of The Script**, **Command To Execute**, **Wait Time (Seconds) Before Executing Script**, **SHA256 Checksum**, and more. The **SHA256 Checksum** attribute can take multiple checksums separated by commas.

  Users should be aware of the following limitations:

  - The **Agent Script Enforcement** profile is currently supported only with the OnGuard Unified Agent for Windows.
  - The ClearPass OnGuard Unified Agent supports downloading scripts only from http and unauthenticated https URLs. For https URLs, OnGuard will skip server certificate verification.
- Support was added for AND/OR combinations in the Services health class for Windows in the ClearPass Windows Universal System Health Validator. This allows checking for services that might go by different

names on different systems. To use this feature, go to **Configuration > Posture > Posture Policies > Posture Plugins > ClearPass Windows Universal System Health Validator**. (#34633)

- A new attribute, **Bounce Delay (in seconds)**, was added to the Agent Enforcement profile. If this attribute is configured, the interface will be bounced after the specified delay. To use this feature, go to **Configuration > Enforcement > Profiles > Add**. Select the **Agent Enforcement** template, and on the **Attributes** tab configure the **Bounce Delay (in seconds)** attribute. (#35130)
- The VIA component of the Windows ClearPass OnGuard Unified Agent is now updated to Windows VIA 2.3.3. For information about the features and enhancements available in VIA 2.3.3, refer to the Aruba VIA 2.3.3 Windows Edition Release Notes available on support.arubanetworks.com at **Documentation > Software User & Reference Guides > Aruba VIA > Release Notes > Windows**. (#35418)
- The VIA component of the Linux ClearPass OnGuard Unified Agent is now updated to Linux VIA 3.0.0. For information about the features and enhancements available in VIA 3.0.0, refer to the Aruba VIA 3.0.0 Linux Edition Release Notes available on http://support.arubanetworks.com at **Documentation > Software User & Reference Guides > Aruba VIA > Release Notes > Linux**. (#35839)

Features Added in 6.6.1

In the posture policies configuration for Windows Hotfixes health classes, you can now quickly view information about superseded updates without having to scroll through the list of updates. To use this feature, go to **Configuration > Posture > Posture Policies > Add**. On the **Posture Plugins** tab, select **ClearPass Windows Universal System Health Validator** and click its **Configure** button. Select the appropriate Windows operating system and then select **Windows Hotfixes**. Select the check box to enable checks for the operating system, filter the **Available Hotfixes** list, and highlight an update. In the information for the selected hotfix that is displayed below the list, updates that supersede it and updates that are superseded by it are displayed near the top. (#34402)

Features Added in 6.6.0

- The **Install Level Check Type** option offered in the Patch Management health class allows OnGuard to check Mac OS X client devices for missing updates. When auto-remediation is enabled, OnGuard installs the missing updates automatically. (#23834)
- The ClearPass Native Dissolvable Agent now supports Auto-Upgrade. When a new version becomes available on the ClearPass appliance, the Native Dissolvable Agent will upgrade automatically and run health checks after the upgrade is installed. (#25061)
- Two new fields were added for health classes. Perl regular expressions are supported for both of the following fields: (#25819, #31886)
  - The **Enable Regular Expression** field was added to the **Installed Applications** health class. If this field is enabled, the policy server treats the application name as a regular expression when comparing application names. This option can be used for Windows and Mac OS X.
  - The **Enter Regex pattern for Registry value** field was added to the **Registry Keys** health class. If a Regex pattern is specified, the policy server will use the regular expression for comparing registry key values.
- ClearPass now computes OnGuard licenses based on devices/endpoints instead of MAC addresses. (#27748)
- The ClearPass OnGuard Unified Agent on Windows now supports running in Service mode; it performs health checks even if the user is not logged in. To use this feature, go to **Administration > Agents and Software Updates > OnGuard Settings** and click **Global Agent Settings**. Select the new parameter

Run OnGuard As, and specify the value as either **Agent**, **Service**, or **BothAgentAndService**. For creating different policies for OnGuard mode, two new attributes, **Host::AgentType** and **Host::HealthCheckLevel**, are available in service rules. (#29673)

- On the **Administration > Agents and Software Updates > OnGuard Settings** page, a new **Native Dissolvable Agent Customization** area allows administrators to select which interfaces are to be allowed for the Native Dissolvable Agent. The Native Dissolvable Agent will only perform health checks for interfaces that are specified in the **Native Dissolvable Agent Customization** area. Options include **Wired**, **Wireless**, **VPN**, and **Other**. This ensures that, if both wired and wireless interfaces are connected, the OnGuard Agent will send health requests through the correct interface. (#30333)
- System tray icons for the ClearPass OnGuard Unified Agent running in VIA + OnGuard mode now show the status of both VIA and OnGuard components. OnGuard standalone system tray icons have also been updated. (#31074)
- The OnGuard Agent support charts that used to be accessed through the online help are now directly available in the user interface at **Administration > Support Documentation**. Click the **OnGuard Agent Support Charts** link on that page to open a list of platform-specific links providing complete information regarding supported antivirus, anti-spyware, firewall, disk encryption, peer-to-peer, patch management, and virtual machine software. (#32722)

Policy Manager

Features Added in 6.6.7

- A new parameter, **Authentication:TacacsAuthenService**, is available in rule configurations for TACACS services and policies and can be used for service selection and profile selection. This parameter can accept three values: none, login, or enable. To use this feature, go to either **Configuration > Services** or **Configuration > Enforcement > Policies** and add or select a service or policy of type **TACACS+**. Add a rule where the type is **Authentication** and the name is **TacacsAuthenService**, and make the value equal to either **AUTHEN-SV-NONE**, **AUTHEN-SV-LOGIN**, or **AUTHEN-SV-ENABLE**. (#34760)
- When using the EAP-TLS authentication method, if an OCSP server is not available to perform certificate validation, ClearPass now provides the option to skip the OCSP check and use a certificate revocation list (CRL) for the validation instead. To use this feature, go to **Configuration > Authentication > Methods > Add** and select **EAP-TLS** as the **Type**. In the **Verify Certificate using OCSP** field, select the **Required (CRL fallback)** option. A CRL should be configured before using this option. (#37406, #39156)
- When an admin user logs in to ClearPass in CC mode, a message on the Dashboard or home page in Policy Manager, Guest, Onboard, or Insight now shows when the most recent successful login occurred as well as the number of failed attempts that were made since the last successful login. (#37853, #40652)
- Support was added for configuring Network Time Protocol (NTP) authentication. You can specify SHA or SHA1 as the encryption type, and enter a key ID and key value (shared secret) the client and server will use to authenticate NTP messages. To use this feature, go to **Administration > Server Manager > Server Configuration > Set Date & Time**. Select the **Synchronize time with NTP server** option, and then configure the **Key ID**, **Key Value**, and **Algorithm** fields. In the UI, the **Key Value** field will accept up to 20 printable ASCII characters. To use up to 40 hexadecimal characters for the key value, use the **`-v <key-value>`** parameter in the CLI instead. (#37848, #39229, #39948)

  With this feature enabled, the NTP key details generate the parameters for the "ntpdate" command and update the ClearPass database accordingly. When you configure the NTP authentication fields and click **Save**, several services are restarted. When the ClearPass NTP service (cpass-ntp) restarts it reads the NTP parameters from the ClearPass database, and the Linux NTP configuration files — ntp.conf (/etc/ntp.conf)

and keys (/etc/ntp/keys) — are updated with the key and server mappings. The Linux NTP service is then used to synchronize the ClearPass server's time with the NTP server.

- ClearPass now provides a notification when an OCSP server is unavailable. Messages are triggered in the **Event Viewer** if an OCSP server is not reachable, if there is no response from the OCSP server, if a CRL is expired, or if a CRL download fails. (#38235)
- Support for a new **HPE-CPPM-Role** attribute for use with ArubaOS-Switches (16.04+) was added to the **Aruba Downloadable Role** enforcement profile in **Advanced** mode. (#39112)

Features Added in 6.6.5

- Administrators can now include tag attributes for endpoints in Insight syslog export filters. The endpoint attributes are sent as a JSON string. To use this feature, go to **Administration > External Servers > Syslog Export Filters**. On the **General** tab, select **Insight Logs** as the **Export Template**. On the **Filter and Columns** tab, select **Endpoints** in the **Predefined Field Groups** list, and then select **EndpointTag** in the **Available Columns - Type** drop-down list. (#38032)
- Support was enhanced in the Accounting-Proxy for roaming scenarios. Now when an Accounting-Stop is received, if the value for the "Additional time before session deletion from multi-master cache" Policy Server service parameter is zero, the RADIUS server will delete the multi-master cache entry. Otherwise, if a value is configured for this service parameter, the RADIUS server will wait the configured number of seconds before deleting the entry. When an Account-Start is received, the RADIUS server will update the multi-master cache with the default value of seven days. (#38150)
- You can now perform bulk updates of endpoint attributes, either for a single endpoint or for multiple endpoints simultaneously. To use this feature, go to **Configuration > Identity > Endpoints** and mark the check box for the endpoint or endpoints in the list. Click the **Bulk Update** button and use the **Bulk Update Attributes** window to select a list of attributes and update them. (#38215)

Features Added in 6.6.4

- ClearPass now supports Microsoft Hyper-V Server 2016. (#37674)
- ClearPass now supports VMware vSphere Hypervisor (ESXi) 6.5. (#37675)
- A new cluster-wide parameter, **TACACS Connection Idle Timeout**, lets you control connection idle timeout settings. To use this feature, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab and configure the **TACACS Connection Idle Timeout** value as needed. The default value is 900 seconds (15 minutes). The minimum allowed value is 60 seconds (one minute) and the maximum allowed value is 172800 seconds (two days). (#37682)

Features Added in 6.6.3

- ClearPass now lets you customize username and password prompts for TACACS+ sessions. To use this feature, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab and modify the default text in the **TACACS User Prompt Text** and **TACACS Password Prompt Text** fields. (#33139)
- A new cluster-wide parameter lets you enable or disable TLS v1.1. To use this feature, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters** tab and configure the **Disable TLSv1.1 support** parameter. (#33399)
- The Event Viewer now shows logging for IPsec connection status. Detailed information is now shown whenever an IPSec tunnel is brought up or down. (#35216)

- ClearPass now introduces a Common Criteria (CC) Mode, which limits certain functions in order to adhere to Common Criteria protection profiles. These include: (#35218, #35219, #35711, #35714, #35861, #35905, #36122)
  - Only CA-issued certificates can be used for ClearPass Server Certificates.
  - All X.509 v3 trusted CA certificates must satisfy the basic constraints.
  - No self-signed certificates will be allowed as Trusted Certificates.
  - All HTTPS communication to external services using X.509 v3 certificates must pass basic constraints checks.
  - An EAP-NAK will be sent in the access-challenge if the supplicant sends an EAP-MD5 response in the EAP-Message.
  - EAP-TLS authentication is limited to only use the following ciphers:
    - TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    - TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    - TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
    - TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

  To enable CC mode, you must first enable FIPS mode and then go to **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Mode** and set **Common Criteria Mode** to **True**. This option will be grayed out if FIPS is not first enabled.
- ClearPass can now optionally be enabled to validate that the cRLSign bit has been set when using certification-based authentication with IPsec connections. If **Strict CRL Policy** is enabled at **Administration > Server Manager > Server Configuration > Service Parameters > ClearPass IPsec service**, then the connection will not succeed if the certificate of the CRL response has no cRLSign bit set. (#35220)
- An option to configure the peer's certificate subject DN as "Peer Certificate Subject DN" is now provided for IPsec certificate-based connections. This is not a mandatory value; it can be empty. When a value is provided, only peers presenting certificates with a subject DN that exactly matches the configured subject DN will succeed. (#35322)
- Traffic selector-based rules can now be configured when you create an IPsec tunnel. A new **Traffic Selectors** tab provides configuration options for **Encrypt Rules**, **Bypass Rules**, and **Drop Rules**. These let you specify the packets to encrypt and allow through the tunnel, the packets that can bypass the tunnel in cleartext, and the packets to be dropped. For each type of rule, you can specify the protocol and port. Configuring rules is optional. If no rules are configured, all traffic is encrypted by default. To use this feature, go to **Administration > Server Manager > Server Configuration** and select a server in the list. On the **Network** tab, click **Create IPsec Tunnel**. (#35397)

- If access to ClearPass through the Web UI is attempted with unsupported SSL protocol versions or with unsupported ciphers, an alert is now logged in the **Event Viewer**. This feature requires the **Enable Ingress Events Processing** option and services to be enabled for the server at **Administration > Server Manager > Server Configuration**. (#35403)
- At **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters**, the **Login Banner Text** field now accepts large character counts (greater than 40,000). (#35692)
- ClearPass will now send an Access-Reject containing an EAP-Message attribute encapsulating the EAP-Failure (for example, NAK) when a fatal error occurs. (#35711)

Features Added in 6.6.2

- Support was added for SNMP version 3 Trap Receivers. To use this feature, go to **Administration > External Servers > SNMP Trap Receivers > Add** and select one of the V3 options in the **SNMP Version** drop-down list. Support was also added for SNMPv3 Traps and SNMPv3 Informs. SNMP V3 requires an authentication key and private key to encrypt the Inform and Trap notifications. The protocol for authentication can be MD5 or SHA hashing. The supported encryption algorithms are AES (128 bit) and DES. SNMPv3 requires an SNMP Engine ID, and the default value for this ID has been set to 6620000004030662. This value can be changed in the **Engine ID** field at **Administration > Server Manager > Server Configuration > System Monitoring**. To receive traps, the same value must be configured at the trap receiver side. (#34449, #35815)
- Checks to validate OCSP URI entries are now supported. To use this feature, go to **Administration > Server Manager > Server Configuration > Service Parameters** and select **ClearPass IPsec service**. (#34740)
- SSL ciphersuite versions are now updated. The updated ciphersuites match those in ArubaOS, and are consistent between FIPS and non-FIPS deployments. Currently supported ciphersuites are listed below; all others are disabled. For information about a ciphersuite's definition, refer to its corresponding RFC. (#34843)

  The following ciphersuites are supported:

  - TLS_RSA_WITH_AES_128_CBC_SHA (RFC 3268)
  - TLS_RSA_WITH_AES_256_CBC_SHA (RFC 3268)
  - TLS_RSA_WITH_AES_128_CBC_SHA256 (RFC 5246)
  - TLS_RSA_WITH_AES_256_CBC_SHA256 (RFC 5246)
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA (RFC 3268)
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA (RFC 3268)
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 (RFC 5246)
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 (RFC 5246)
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (RFC 4492)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (RFC 4492)
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (RFC 5289)
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (RFC 5289)
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (RFC 4492)
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (RFC 4492)
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (RFC 5289)

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (RFC 5289)

- The Apache SSLHonorCipherOrder Directive is now enabled. When a cipher is selected during a TLS handshake, the preferred cipher available in ClearPass is used. (#34844)
- Additional log entries are now included for password policy violations and changes for both admin users and local users at **Monitoring > Event Viewer** and **Monitoring > Audit Viewer**. Entries are included for users whose accounts are locked due to account settings validations, and for users whose accounts are enabled again after being locked out. To find these entries in the **Event Viewer**, you can filter for **User Account Settings** in the **Source** column, or for **Admin User Enable** or **Local User Enable** in the **Category** column. (#35399, #35401)
- All attempted upgrade, patch, and hotfix installations are now logged in the **Event Viewer**, including failed attempts. (#35400)
- Diffie-Hellman (DH) Groups 19 (ECP_256) and 20 (ECP_384) are now included in the list of supported Diffie-Hellman algorithms for IPsec connections. (#35485)
- Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are now supported for IPsec connections. (#35623)

Features Added in 6.6.1

- Admin users and local users can now be disabled when they exceed an allowed number of failed login attempts. For example, if the allowed number is five, the user will be disabled after the fifth failed attempt. The number of attempts you can specify can be from 1 to 100. When the configured number of failed login attempts is exceeded for an admin or local user account and the account is disabled, you can reset the failed attempts count to zero and re-enable all the account's users. To use this feature: (#30517, #34538, #30521, #34555)
  - For local users, go to **Configuration > Identity > Local Users > Account Settings > Disable Accounts**. To disable accounts, enter the number of allowed attempts in the **Failed attempts count** field. To reset accounts, click the **Reset** button.
  - For admin users, go to **Administration > Users and Privileges > Account Settings > Disable Accounts**. To disable accounts, enter the number of allowed attempts in the **Failed attempts count** field. To reset accounts, click the **Reset** button.
- Support was added for the `Framed-IPv6-Address` RADIUS attribute (IETF 168). The data type of this attribute is `IPv6Address`. (#31912)
- Support was added for disabling the TACACS password-change option. A new cluster-wide parameter, **Disable Change Password for TACACS**, is available on the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab. (#33424)
- Support was added to validate whether the OCSP extended key usage extension "keyPurpose" is set or not during EAP-TLS authentication. If the value of the parameter is TRUE, EAP-TLS authentication will fail unless the OCSP signing certificate also has OCSP "keyPurpose" set. If the value of the parameter is FALSE, the OCSP signing certificate does not need to include "keyPurpose". The default value is FALSE. To use this feature, go to **Administration > Server Manager > Server Configuration > Service Parameters** tab. (#33637)
- Support was added for configuring IKEv1 and IKEv2 SA lifetimes. To use this feature, go to **Administration > Server Manager > Server Configuration** and click a server in the list. On the **Network** tab select **Create IPsec Tunnel**. The form includes the **IKE Version**, **IKE Lifetime**, and **Lifetime** fields, with default

values populated. The **Lifetime** value (for Phase2 session keys) should always be less than or equal to the **IKE Lifetime** value (for Phase1 session keys). (#34040)

- ClearPass now supports OCSP-based and CRL-based validations for IPsec connections that use certificates for authentication. A Certificate Revocation List (CRL) will automatically be used if one is defined. To configure an OCSP URL, go to **Administration > Server Manager > Server Configuration** and click a server in the list. On the **Service Parameters** tab select **ClearPass IPsec service** and then configure a value for **OCSP URI**. The certificate status is checked against the OCSP URL present in the certificate or the configured OCSP URL. (#34137)
- Post-Auth-Session-Restriction configuration is more flexible and granular. Customers can restrict or blacklist clients based on bandwidth consumed as well as on session duration, whichever is exceeded first. The blacklisting hold-off period can also be configured (replacing the previous 24-hour limit). To use this feature, go to **Configuration > Enforcement > Profiles > Add**. On the **Profile** tab, select the **Session Restrictions Enforcement** template. (#34554)

Features Added in 6.6.0

- The Access Tracker now displays the results of unhealthy endpoints. Go to **Monitoring > Live Monitoring > Access Tracker**, double-click on a request, and then click the **Output** tab. A new section, **Posture Evaluation Result**, indicates which checks failed for the following health classes: (#12089, #29782, #29783, #31887)
  - AntiSpyware
  - AntiVirus
  - Disk Encryption
  - File Check
  - Firewall
  - Installed Applications
  - Network Connections
  - P2P
  - Patch Management
  - Processes
  - Registry Keys
  - Services
  - USB Devices
  - Virtual Machines
  - Windows Hotfixes
- ClearPass 6.6 is now able to extract the auth-session-id from CiscoAVPair VSA to use in Change of Authorization (CoA). The username value is now used as the key when creating or querying a session in a multi-master session cache. This makes it possible to send a CoA when the Calling-Station-ID value includes the IP address format. To use this feature, in Policy Manager go to **Configuration > Enforcement > Profiles**, copy the default [Cisco - Terminate Session] profile, and modify it to include the Cisco-AVPair attribute. For more information on configuration, testing, and troubleshooting, refer to the *Policy Manager 6.6 User Guide*. (#17812)
- Cisco ASA requires the audit Session ID in the RADIUS Change of Authorization (CoA) message. ClearPass extracts the audit-session-id from the VPN RADIUS authentication message. There are new properties to

cache the Cisco-AVPair with the value that contains the audit-session-id. These properties can be used to cache any custom attribute that contains the particular value. (#24403)

- Various new options such as protocol filters and port filters were added to the packet capture diagnostic tool in the admin UI and the CLI. (#26091)
- The Trapeze RADIUS dictionary was updated. (#26478)
- Syslog support was added for Apache and Samba logs. Data in Apache access and error logs and SAMBA windbindd logs can now be streamed to external syslog servers for third-party monitoring. To use this feature, go to **Administration > Server Manager > Log Configuration > System Level** tab and enable the **Apache web server** and **Domain service** log services. (#27123, #28347, #31316)
- Endpoint fingerprints functionality is updated to allow the administrator to either override the fingerprint or add a new rule based on the learned attributes, creating a new entry in the Fingerprint dictionary. This allows unknown endpoints to be categorized as desired with a new custom fingerprint. The device MAC vendor is added by default when a new rule is created. (#27659)
- The new Ingress Event Engine enables ClearPass to process Syslog events from third-party devices to make policy changes in realtime. For example: (#28446, #29415, #30254, #32451)
  - A third-party device could signal to a ClearPass appliance to quarantine or block a user if the contents indicate the presence of malware.
  - Syslog dictionaries from leading vendors such as Palo Alto Networks, Checkpoint, Juniper Networks, and Fortinet are included by default.
  - Administrators may also create custom dictionaries on their own.
  - An **Event Requests** filter is also included in the data filters at **Monitoring > Live Monitoring > Access Tracker > Select Filter**, letting you filter for all event-based records.
  - The **Batch Processing Interval** service parameter is available on the **Service Parameters** tab at **Administration > Server Manager > Server Configuration** when **Async network services** is selected for a server. This parameter lets you control the batch processing interval of Ingress Event processing. The default interval value is 30 seconds. The allowed values are 10-300 seconds. Users should be aware that, in order for changes to this service parameter to take effect, **Async network services** must be restarted.
- Network Discovery is a new feature that facilitates the addition of network devices. It uses a configured "seed network device" (typically a switch/router/controller) to discover endpoints and network devices. The seed device is queried using configured SNMP credentials (see **Configuration > Profile Settings > SNMP Configuration**). Network Discovery scans are initiated from **Monitoring > Network Discovery > Start Network Discovery Scan**. The following information is read from the seed device: (#28448)
  - SNMP information: The system name, vendor, system location, system contact, and system description are captured from accessible network access devices.
  - Connected endpoints: Information about endpoints connected to the network device (typically MAC addresses of endpoints connected to switch ports). These are added as discovered endpoints.
  - ARP table: Provides information about MAC > IP associations for endpoints that were seen by this device recently. These endpoints are probed further in an attempt to profile them using all supported mechanisms.
  - Neighbor network devices: Other network devices connected to the seed device, as determined by neighbor discovery protocols like Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) (if enabled in your network).

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

Network devices discovered through a scan are available for review at **Monitoring > Network Discovery > View Discovered Devices**. Discovered devices can be imported and added to **Network Devices**.

- Support for port bounce was added to Mobility Access Switches as part of their 7.4.0.3 release to facilitate VLAN changes and profiling. To enable this support, the ClearPass RADIUS dictionary is updated to support VSA 40 (Aruba-Port-Bounce-Host). The default `Aruba Terminate Session` attribute now includes this entry. (#28532)
- The structure for endpoint attributes is now simplified to achieve better performance. The **`tips_endpoints`** table has a new column **`attributes::JSONB`**. The attributes column holds information for an endpoint in JSON structure. (#28642)
- ClearPass 6.6 provides a new option to disable log database backups during major upgrades. This reduces the time to upgrade a node, especially with large log database sizes. Enable this option if you do not plan to restore the log database post-upgrade. (#28841)
- The `system morph-vm` command is now supported for non-evaluation VM versions. It has been modified to allow conversions from a lower capacity VM to a higher capacity VM only, using the new single virtual machine installation image, in case the wrong VM is installed. Additional enhancements are described below: (#28862, #30762)
  - The restore step after rebooting was eliminated. This significantly reduces the overall time for the morph operation, and the cluster setup is retained.
  - Node service parameters whose defaults and range are set based on the model number are now automatically reset in the local database when morphing a publisher, and on the remote publisher when morphing a subscriber.
  - During the first boot and morph command, additional warning messages are provided if system requirements are not met.

  For information about how to morph a VM more than once, see the "*Installing or Upgrading to 6.6 on a Virtual Appliance*" Tech Note.
- A new service parameter, **Additional time before session deletion from multi-master cache**, was added to the list of policy server parameters available at **Administration > Server Manager > Server Configuration**. When configured, the policy server will wait the additional configured number of seconds before deleting an entry from the multi-master cache. The default value is zero. This feature is useful in wireless roaming situations where a client may roam from one controller to another and ClearPass may receive an Accounting-Stop and Start in rapid succession, which can result in ClearPass mistaking which NAD the client is attached to. (#29015)
- The **`pg_stat_statements`** extension is now added to the ClearPass log collection. This feature tracks the queries executed in the database, and provides daily log with PostgreSQL stats for debugging. It is available under the system-load-monitor directory as part of collect logs. (#29115)
- The Infoblox RADIUS dictionary was added. (#29406)
- REST API support was added for the following ClearPass entities: (#29458)
  - AdminUser
  - AuthMethod
  - AdminPrivilege
  - Endpoint

    - Insight/Endpoint
    - LocalUser
    - NetworkDevice
    - NetworkDeviceGroup
    - ProxyTarget
    - Role
    - StaticHostList
- A new cluster-wide parameter, `cli session idle timeout`, lets clients configure the idle time allowed during a CLI session before a session timeout. Any changes made to the idle time duration will go into effect when a new session is opened. This option is available at **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab. (#29797)
- SNMP support has been enhanced to include the hrProcessorTable. (#29857)
- A new RADIUS service parameter, **Check the validity of intermediary certificates in the chain using OCSP**, was added to enhance certificate security. This feature is disabled by default. Enabling this feature will put greater load on the system and is not intended for all customer use cases. (#30077)
- Support was added for disabling TLS 1.0 in the Web UI and the RADIUS server. A new cluster-wide parameter, **DisableTLSv1.0 support**, is available on the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab. (#30078)
- The SNMP private management information base (MIB) in ClearPass now includes service start, stop, and restart Traps, providing more granular control for handling these service actions. (#30186)
- ClearPass 6.6 adds the ability to profile endpoints based on commands executed over an authenticated SSH or WMI session. Multiple SSH/WMI credentials can be configured per subnet under **Configuration > Profile Settings > SSH/WMI Configuration**. When a new endpoint IP address is detected through one of the endpoint discovery mechanisms (subnet scans, SNMP based ARP table read), the endpoint is probed to determine if SSH (TCP port 22) or WMI (TCP port 135) is open. If a port is open, an attempt is made to establish a session using configured credentials. If a session is established successfully, commands are executed over the session to determine the endpoint's device type. ClearPass 6.6 includes fingerprints to profile endpoints based on device type determined from a SSH/WMI session. (#30260, #30319)
- ClearPass now supports public key-based SSH logins on a per-appliance basis. A new **SSH Public Keys** option is available at **Administration > Server Manager > Server Configuration > Network**. (#30286).
- A timeout option is now available in LDAP bind operations for AD/LDAP authentication sources. The value for the **Server Timeout** option is configured on the **General** tab at **Configuration > Authentication > Sources (LDAP/AD type)**. (#30330)
- You can now provide port information when you specify a server name at **Administration > External Servers > Endpoint Context Servers**. Port information should be provided in the format "hostname:port". (#30407)
- All references to HP are now renamed to HPE or Hewlett Packard Enterprise. (#30435, #30436, #30437, #31830)
- At **Configuration > Services > Reorder Services**, reordering is now easier: Simply click a service to select it, and then click again on the new position you want to move it to. (#30446)
- In previous versions of Policy Manager, users had to add or modify Admin access privileges by importing XML files. ClearPass Policy Manager 6.6 provides a way to modify Admin access privileges in Policy Manager and Insight via the Web UI. (#30449)

- All endpoints discovered on the network as part of profiling/network discovery are now added as Endpoint entries even if Profiler cannot fingerprint the device. (#30466)
- Several enhancements were made in the areas of advanced password policy options for the local user database. To use this feature, go to **Configuration > Identity > Local Users > Password Policy**. The following options are available: (#30514, #30515, #30529, #30530, #30531, #30533)
  - **Disable account if Date exceeds**: Local users are disabled at midnight when the current date exceeds the configured date.
  - **Disable account if Days exceed**: Local users are disabled when the specified number of days has passed since the account was enabled.
  - **Disable user account after n days if password is not changed**: The user's account is disabled if they do not change their password after the specified number of days.
  - **Password must be different from the previous n versions**: The number of previous passwords (including the default password) to compare to the new password the user enters. Values of 1 through 99 may be specified.
  - **Display reminder message after n days**: Number of days after which a reminder to change the password is displayed to the user. Values of 1 through 365 may be specified. This option is only for displaying the reminder; it does not include the new-password prompt. This option is applicable only for TACACS+ authentication.
  - **Check to force change password on next TACACS+ login**: The local user must change their password immediately after their next TACACS login. This option is available when you select an account in the list at **Configuration > Identity > Local Users**.
- Any changes to attributes on the Modify Endpoint Context Server form are now reflected automatically. (#30582)
- ClearPass 6.6 introduces a new feature that adds the ability to profile endpoints on the network based on open TCP ports. The list of TCP ports to be probed during endpoint profiling is controlled by a new cluster-wide parameter called **Profiler Scan Ports**. (#30844)
- All endpoints discovered from **Network Devices** with SNMP read enabled and via network discovery scan are now automatically added as endpoints with **Status=UNKNOWN**. (#30845)
- A new service parameter, **Connection Timeout**, was added under **Async Network Service** to control HTTP connection timeout scenarios when connecting to external servers in Generic HTTP Enforcement. (#30941)
- If location details from Insight are available, they are now displayed at **Configuration > Identity > Endpoints** on the **Endpoint** tab of the **Edit Endpoint** window. Location information includes the NAD and port values for wired devices, and the access point and network SSID for wireless devices. (#30992)
- The `tips_audit` table in the configuration database can now be accessed by the appexternal DB user. This table contains audit records for Policy Manager configuration changes. (#31229)
- The Aruba RADIUS dictionary was updated. (#31436)
- New field groups are added to Insight Logs for Posture. APT (Application posture token) is used as part of posture. Also a few fields have been removed from the Insight Logs authentication table and moved to the endpoints table. New field groups have been created exclusively for Posture-related details. The new field groups added to Insight Logs are as follows: (#31458)
  - Posture Summary
  - Posture Firewall Summary
  - Posture AntiVirus Summary

- Posture Antispyware Summary
- Posture DiskEncryption Summary
- Posture Windows HotFixes Summary

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

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

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

Profiler and Network Discovery

Features Added in 6.6.5

- A new option lets you configure a schedule for recurring subnet scans. You can specify a time of day for the scan to start, and can set the frequency to be hourly, daily, or weekly. If hourly is selected, you can set an interval of 3 to 350 hours between the scans. You can also assign the scan to a specific Policy Manager zone. To use this feature, go to **Configuration > Profile Settings** and click the **Schedule Subnet Scan** link. (#38358, #38637)

Features Added in 6.6.4

- ClearPass now supports MAC Notification Traps from HPE ArubaOS-Switches. This automatic notification can be used to discover new devices connected to an HPE ArubaOS-Switch or to perform an OnConnect enforcement. (#37180)
- A new cluster-wide parameter lets you specify the interval after which endpoints will be reprofiled. To use this feature, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Profiler** tab and configure the **Netflow Reprofile Interval** field. The default value is 24 hours. The minimum value is one hour. (#37281)
- If custom fingerprints are configured, now the custom rules will always be evaluated before the default rules. (#37545)

Features Added in 6.6.3

- Support was added for Profiler rules based on Host:Services (operator contains substring) as identified by Nmap. (#36167)
- ClearPass can now act as a flow collector to identify endpoint open port information for profiling. Supported versions are NetFlow V5, V9 and IP Flow Information Export (IPFIX). (#36285)
- Support has been added to fetch service and process information using Windows Management Instrumentation (WMI) from domain-joined Windows Devices. Active and inactive services and processes can now be viewed in either Policy Manager or Insight. To use this feature: (#36427, #36491, #36492)
  - First, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Profiler** tab, and set the **Parameter Value** to **TRUE** for the new **Enable Endpoint Posture scan using WMI** parameter. This step enables fetching the information about the services

and processes running on the endpoint during a subnet scan, network discovery, or OnConnect Enforcement.

- The fetched information can then be viewed in the user interface. To view it in Policy Manager, go to the **Configuration > Identity > Endpoints > Edit Endpoint > Fingerprints** tab and review the **Active Services**, **Inactive Services**, and **Processes** information. To view it in Insight, enter the MAC address in the search field and then review the **Active Services List**, **Inactive Services List**, and **Processes** information in the **OnGuard** widget.

Features Added in 6.6.2

- Support was added for using Nmap port scans to detect services running on a host. This information is used to determine the device profile. Nmap port scanning is not enabled by default. To use this feature, go to **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters** and, on the **Profiler** tab, set the **Enable Endpoint Port Scans using Nmap** parameter to **TRUE**. To see the services and open ports information returned by the scan, go to **Configuration > Identity > Endpoints**, select an endpoint in the list, and select the **Fingerprints** tab. (#35181, #35875)

Features Added in 6.6.1

- Address Resolution Protocol (ARP) probing can now be enabled for network discovery scans. Network discovery uses Simple Network Management Protocol (SNMP) to read a variety of Management Information Bases (MIB) from a Network Access Device. When this option is enabled, the scan will now also probe all ARP entries available. To use this feature, go to **Monitoring > Profiler and Discovery > Network Discovery > Start Network Discovery Scan** and select the check box in the **Probe ARP entries** field. Users should be aware that when ARP probing is enabled, network discovery scans will take longer. (#34169)

QuickConnect

Features Added in 6.6.0

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

The following issues were fixed in previous 6.6.x releases. For a list of issues resolved in the 6.6.8 release, see "What's New in This Release" on page 11.

This chapter includes:

Fixed in 6.6.7

The following issues were fixed in the 6.6.7 release.

APIs

Table 8: *API Issues Fixed in 6.6.7*

Bug ID	Description
#37435	In the AdminUser Rest API, admin users could not be sorted based on the user_id field.
#37436 #37437	Trying to filter by an usupported field gave an "Internal server" error. Filtering with a field that is not supported now correctly displays a validation error message that describes the problem.
#39963	The API Explorer did not load correctly in Internet Explorer (IE) version 11.

Cluster Upgrade and Update

Table 9: *Cluster Upgrade and Update Issues Fixed in 6.6.7*

Bug ID	Description
#39628	Operations such as collecting logs, leaving the domain, or joining the domain from remote servers within the cluster sometimes failed and the error message "1" was displayed.
#40223	After a patch update was successfully applied to the publisher, database replication failed. This caused the patch update on the subscribers to fail with the error message "Updates are not applied on the publisher node."

Endpoint Context Servers

Table 10: *Endpoint Context Server Issues Fixed in 6.6.7*

Bug ID	Description
#38710	The "Corporate Shared" tag value for the "Ownership" attribute could not be correctly mapped to the "Shared" value.
#39515	The authentication token from MaaS360 was not refreshed while polling the managed devices.

Guest

Table 11: *Guest Issues Fixed in 6.6.7*

Bug ID	Description
#39218	The list of time zones is now updated to reflect time zone changes that have been made in some locations.
#39288	Numeric names for AP groups were not handled correctly for AirGroup shared groups.
#39958	Octet strings were incorrectly null-terminated when using an SMPP gateway to send SMS messages.
#40022	API calls to return the guest or device list returned unexpected results when filtering for the create_ time for an account.

Insight

Table 12: *Insight Issues Fixed in 6.6.7*

Bug ID	Description
#39097	If there was a time change due to daylight savings, Insight did not update some precomputed statistics for the Dashboard and the error message "High I/O wait (10 min avg) was displayed in the Event Viewer.
#39174	Insight logins failed with the error message "No privilege for Insight" if the username or password included certain special characters. The following special characters are now allowed in ClearPass usernames and passwords: ! @ # $ % ^ & * ( ) < > [ ] { } ' : ~ ` / \ | " + , - . ; = ? _
#39358	The default number of Insight NetEvents writers sometimes could not process all the events if the request load was high, resulting in a backlog. The number of Insight NetEvent writers is now automatically configured based on the number of CPU processors in the ClearPass appliances.

Onboard

Table 13: *Onboard Issues Fixed in 6.6.7*

Bug ID	Description
#39954	Users who logged in through the self-service portal were able to view the list of certificates by entering the Certificate Management URL.
#39956	Attempting to migrate a pre-6.6.2 Onboard backup to 6.6.5 failed if it included an imported-mode certificate authority (CA) that had not yet imported a certificate.

Table 13: *Onboard Issues Fixed in 6.6.7 (Continued)*

Bug ID	Description
#40276	Onboard device provisioning pages now load much more quickly.
#40318	Although certificate revocation after a specified period of inactivity was configured in a device's provisioning settings, the certificate was not revoked after the configured time had elapsed.
#40434	When upgrading to ClearPass 6.6.0 from a lower version, migration of Onboard data failed and the error message "Restore failed" was displayed on the UI's home page.
#40464	An Onboard registration authority (RA) failed if the upstream Certificate Authority (CA) required a SCEP password.
#40530	Onboarding failed if a certificate authority was configured with the key created by the Onboard server and its retention policy configured to not store copies of the client certificates.

OnGuard

Table 14: *OnGuard Issues Fixed in 6.6.7*

Bug ID	Description
#36707	The ClearPass OnGuard Unified Agent now supports enabling Real-Time Protection (RTP) status of Avira Free Antivirus 15.x.
#38407	The ClearPass OnGuard Unified Agent showed the health status as **Not Known** if the user clicked the **Retry** button while the **RunOnGuardAs** mode was set to **Service**.
#38961	The ClearPass OnGuard Unified Agent for macOS now supports full-system scans for Kaspersky Internet Security 16.x.
#39075	The ClearPass OnGuard Unified Agent now supports enabling Real-Time Protection (RTP) status of Kaspersky Total Security 17.0 on Windows OS.
#40082	The ClearPass OnGuard Unified Agent for macOS was sometimes not able to read the DAT file time of Trend Micro Security for Mac 3.x.
#40109	The ClearPass OnGuard Unified Agent was sometimes unable to read the encryption state using Symantec Encryption Desktop 10.4, and the client was marked unhealthy.
#40110	The **Logout** button was enabled after a system reboot if the Health Check Interval was configured. Now when the client is in a Health Check Interval after a reboot, the state of the **Logout** button is correctly based on the configuration of the **Enable to hide Logout button** parameter at **Administration > Agents and Software Updates > OnGuard Settings > Global Agent Settings**.
#40351	For the McAfee Endpoint Security Threat Prevention antivirus product, the DAT file time reported by OnGuard and shown in the Access Tracker did not match the DAT file time shown in the antivirus product itself.
#40359	The ClearPass OnGuard Unified Agent took a long time to perform health checks if some ClearPass servers were not reachable.
#40384	On Windows 10, the ClearPass OnGuard Unified Agent could not enable Microsoft Windows Firewall unless the Windows Firewall service was running.

Policy Manager

Table 15: *Policy Manager Issues Fixed in 6.6.7*

Bug ID	Description
#37304	The local node's IPsec configuration files and database were out of synch after a database backup was restored. Existing IPsec local node configurations are now retained, and are not replaced with the ones in the database backup during a restore operation.
#37850	ClearPass 6.6.7 introduces the following changes in default ICMP behavior: • ClearPass will not respond to ICMPv6 traffic sent to an anycast or multicast address. • ClearPass will not transmit to ICMPv6 type-3 messages (Destination Unreachable).
#38247	An SNMP query to the Clearpass server showed the sysObjectID value as Linux instead of ClearPass. SNMP queries now correctly return the Clearpass OID corresponding to .1.3.6.1.4.1.14823.1.6.1.
#38868	Authentication requests failed because Policy Server connection timeouts did not happen if MSSQL was used as the authorization source.
#39152	Firewall rules for IPsec connections were not cleared when IPsec was disabled.
#39307	The “nf_conntrack_max” value was reset to the default value of 65536 after a system reboot.
#39579	External service providers and other external entities were not able to fetch ClearPass Identity Provider (IdP) metadata using the IdP metadata URL.
#39604 #39886	The automatic Change of Authorization (CoA) process intermittently failed to occur because the Multi-Master Cache replicator process had terminated abruptly.
#39650	Recent data shown in the Access Tracker for an endpoint would sometimes revert to values from a previous authentication.
#39657	Trying to import a RADIUS server certificate or an HTTPS certificate failed with the error message “Certificate file is not valid. Either the certificate signature is tampered or the file is corrupted” if the certificate included Bag Attributes in the private key file.
#40031	The Apache Tomcat version is now upgraded to 7.0.77. This version includes fixes for CVE-2017-5647. Users should be aware that although ClearPass was not vulnerable to this CVE issue, this upgrade was made in order to alleviate any concerns our customers might have.
#40049	Corrected an issue where the ClearPass Policy Manager user interface did not load correctly in the Chrome 58.x browser, and only the header and footer of the UI were displayed. If you need to use the Chrome browser to open a ClearPass version earlier than 6.6.7, use the keystrokes **Ctrl +** or **Ctrl -** to resize the text and the content will be displayed.
#40153	The list of ciphers supported by ClearPass is now reordered to give preference to higher-security ciphers first.
#40265	On the **Access Tracker > Request Details > Input** tab for a RADIUS request, the **Authorization Attributes** and **Computed Attributes** areas were empty if the computed attributes included any null values.
#40399	Tthe **Event Viewer** did not include entries for expired certificate status.
#40455	A race condition between the Async DB write service and the RADIUS server caused frequent restarts of the RADIUS server.

Profiler and Network Discovery

Table 16: *Profiler and Network Discovery Issues Fixed in 6.6.7*

Bug ID	Description
#37778	If a double-byte language (Chinese, Japanese, Korean) was selected as the preferred language in the browser's settings, the **Monitoring > Profiler and Discovery > Endpoint Profiler** page categorized all devices as "unmanaged devices."

Fixed in 6.6.5

The following issues were fixed in the 6.6.5 release.

CLI

Table 17: *CLI Issues Fixed in 6.6.5*

Bug ID	Description
#39081	ClearPass ignored the SSH client LANG variable and forced the session to be in en_US.UTF-8. This had caused the ClearPass server IPv4 configuration to not be shown in the CLI, although it was shown in the UI.

Cluster Upgrade and Update

Table 18: *Cluster Upgrade and Update Issues Fixed in 6.6.5*

Bug ID	Description
#36112 #38500	After a patch was installed through the **Cluster Update** interface, the installed status was not shown for the patch file on the **Software Updates** portal.
#36717	Attempting to add a new subscriber or rejoin a subscriber to the cluster while the subscribers were also handling other traffic sometimes failed, depending on the amount of traffic.
#38461	New database tables added in a patch update were not replicated on the subscribers.

Guest

Table 19: *Guest Issues Fixed in 6.6.5*

Bug ID	Description
#38646	Editing and re-saving a guest self-registration page that had been configured with social logins sometimes lost the social-login API secrets, causing all social logins to fail.
#38803	Guest self-registrations that were configured for OnGuard health checks forced a pre-authentication even if the configuration did not include pre-authentication.
#38846	The FIAS-Micros transaction processing gateway did not support room numbers that included letters.
#38941	Corrected a potential cross-site scripting (XSS) issue in Web site content management.

Insight

Table 20: *Insight Issues Fixed in 6.6.5*

Bug ID	Description
#36094	The error message "Insight sync unstable" was displayed in the **Event Viewer** for an Insight-enabled appliance in a cluster if both the management port and the data port were configured. This was a false alert and could be ignored.
#36748	Simultaneous system updates of Endpoints and RadiusAcct netevents caused a deadlock, preventing those records from being updated in the database.
#37005 #38258	After upgrading to 6.6.x, netevents files generated during backlog processing were not processed and Insight(Sync) error messages such as "Netevent backlog:<###> detected" were displayed in the Event Viewer.

Onboard

Table 21: *Onboard Issues Fixed in 6.6.5*

Bug ID	Description
#36772 #38430	The Onboard license usage count at **Onboard > Management and Control > Usage** was displayed as a rolling average. Onboard license usage is now correctly shown as the total number of onboarded devices with currently valid certificates. This is the count as of the time of the query; it is not an average. When this number is exceeded, no further certificates can be issued. A device can only be listed as enrolled if it has a valid certificate.
#38430	Corrected an issue where the **License Usage** count was not updated at **Onboard > Management and Control > Usage**.
#38801	On the **Onboard > Configuration > Network Settings > Trust** tab, a custom Android trust certificate could not be saved.
#38918	A failed migration of the 6.6.2, 6.6.3 or 6.6.4 patch sometimes caused Onboard enrollment failure.
#39405	Corrected an issue where, in a cluster with a large number of Onboard certificates, an update from 6.6.0 to 6.6.4 did not complete. The migration speed is now improved for pre-6.6.3 backups that include a large number of Onboard certificates.

OnGuard

Table 22: *OnGuard Issues Fixed in 6.6.5*

Bug ID	Description
#38720	The ClearPass OnGuard Unified Agent did not perform health checks after the configured grace period expired for patch management products.
#38954	The ClearPass OnGuard Unified Agent performed health checks every hour if more than one patch management application was configured to "Pass Any One" rule at **Configuration > Posture > Posture Policies > Posture Plugins**.

Policy Manager

Table 23: *Policy Manager Issues Fixed in 6.6.5*

Bug ID	Description
#38362	The “poweroff user” option for shutting down a ClearPass instance from the console was still available after the initial bootstrapping process. This option is no longer available when the system bootstrap is complete. Administrators must log in to the CLI and use the “system shutdown” command instead.
#36404 #38697	Multi-master cache synchronization in large cluster deployments (10 or more) would sometimes hang if polling took a long time, and the error message “Battery sync unstable” was displayed.
#37049	A RADIUS CoA (Change of Authorization) failed during an NMAP audit scan and displayed the error message “mandatory fields missing”.
#37438	The Network Time Protocol (NTP) version is now upgraded to ntp-4.2.6p5-10. This includes fixes for CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311, and CVE-2016-9312.
#38047	User-created roles could not be deleted if a policy simulation was configured with no role association.
#38560	If attributes were updated through an entity update enforcement profile for a guest device account, the last attribute was not updated in the database.
#38689	Corrected an issue where a memory leak in post-authentication led to high system memory usage and impacted overall system performance.
#38811	An incorrect time zone offset was shown for Europe/Istanbul. The correct GMT + 3 offset is now shown for the Turkey time zone.
#38897	Trying to add SAML Service Provider (SP) metadata in an SSO configuration failed and the error message “Exception occurred during processing request: Method "execute" failed for object ...” was displayed. This occurred because a third-party .jar file was missing.
#38969 #38972	The Apache Struts version is now upgraded to 2.3.32. This includes fixes for CVE-2017-5638.
#38988	When attempting to change the ClearPass portal’s logo by uploading a new image file at **Administration > ClearPass Portal**, the file upload never completed and the logo could not be replaced.

Profiler and Network Discovery

Table 24: *Profiler and Network Discovery Issues Fixed in 6.6.5*

Bug ID	Description
#37768	Endpoints that could not be classified were categorized as “Unknown”. Now if classification is not possible from an endpoint’s current set of attributes, it is assigned either a Generic, MAC Vendor, or Unclassified Device profile. Devices are then further classified as far as possible in the hierarchy under each profile.
#38212	At **Configuration > Identity > Endpoints**, the **Switch Port** field did not clearly identify whether the location information shown for a device was from the access port or the trunk port. Now if a device is seen on the trunk port, the port name will have “(Trunk)” displayed after it.
#38953	The Event Viewer did not show the “Scan completed” message for an on-demand subnet scan.

Fixed in 6.6.4

The following issues were fixed in the 6.6.4 release.

APIs

Table 25: *API Issues Fixed in 6.6.4*

Bug ID	Description
#37762	Corrected an issue in Insight endpoint API responses where, for role values, a line break would occur in the string at the characters N, U, or L, resulting in incorrect output. Array parsing is now improved.

CLI

Table 26: *CLI Issues Fixed in 6.6.4*

Bug ID	Description
#37672	When working in the CLI, using the **Ctrl + Alt + Delete** keystroke combination caused the system to reboot.

Endpoint Context Servers

Table 27: *Endpoint Context Server Issues Fixed in 6.6.4*

Bug ID	Description
#36746	Aruba access points that were shipped with new HPE-Aruba part numbers were not categorized as APs by ClearPass and could not be profiled.
#37193	When a Google Admin console was used as the endpoint context server, after the first poll the refresh token was cleared from the database and subsequent polls failed.
#37712	ClearPass did not update the Palo Alto Networks endpoint context server “UserID Posturl” during a system patch update. Updating the ClearPass version now correctly changes the PANW Firewall or Panorama UserID Post URL from “`https://{server_ip}/api/?type=user-id&action=set&key={key}&cmd={cmd}`” to “`https://{server_ip}/api/?type=user-id&action=set&key={key}`”.

Guest

Table 28: *Guest Issues Fixed in 6.6.4*

Bug ID	Description
#37892	Corrected an issue where 802.1x with multi-factor authentication did not work with Duo.
#38192	The PHP version is now updated to 5.6.30. This includes fixes for CVE-2016-9935.

Onboard

Table 29: *Onboard Issues Fixed in 6.6.4*

Bug ID	Description
#37782	Trying to import an intermediate CA displayed the error message "Call to undefined function NwaCheckSignature()" if the certificate had already been imported. Now if the user attempts to import a CA certificate twice, Onboard displays an appropriate error message advising that "A CA using this certificate already exists."
#37783	Web-based enrollments were not counted toward the Onboard device limit.
#37859	A migration failure during the 6.6.2 or 6.6.3 patch sometimes caused Onboard enrollment failure.
#38246	Invalid encoding of the signature algorithm field for a Certificate Revocation List (CRL) caused the entire CRL to be invalid.

OnGuard

Table 30: *OnGuard Issues Fixed in 6.6.4*

Bug ID	Description
#36248	The ClearPass Server reachability test passed even if the OnGuard application was denied at **Administration > Server Manager > Server Configuration > Network > Application Access Control**. This fix also corrects an issue where, in some cases, the ClearPass OnGuard Unified Agent only checked the first two Server IP addresses in the Authentication Server list.
#36515	OnGuard incorrectly categorized the network connection type of an F5 VPN client as "Other". The F5 VPN interface is now correctly detected as "VPN".
#37009	The agent.conf file was sometimes corrupted or empty, causing the ClearPass OnGuard Unified Agent to hang at the initializing stage.
#37333	On devices using Mac OS X 10.11 or macOS 10.12, the **Network** tab of the VIA dialog displayed incorrect remote server hostnames for VIA connection profiles if multiple connection profiles were configured. Configuration information is now correctly retrieved from the controller selected for the connection.
#37423	On an Ubuntu operating system, the ClearPass OnGuard Unified Agent incorrectly detected the status of the "chef-client" service as stopped when it was running.
#37630	The ClearPass OnGuard Unified Agent caused spikes in CPU consumption at one-minute intervals while detecting installed antivirus products. The antivirus detection will now be performed every two hours instead of every minute.
#38382	The ClearPass OnGuard Unified Agent for the Mac OS did not send the VPN username in the WebAuth request if the OnGuard mode was set to "Check Health - no authentication".

Policy Manager

Table 31: *Policy Manager Issues Fixed in 6.6.4*

Bug ID	Description
#30958	ClearPass integration with a Palo Alto Networks (PANW) Panorama server failed due to a missing Content-Length header. Content-Length is now added by the library while posting.
#35854	When MAC authentication was configured against an external MySQL database, some MAC authentication requests were rejected and the error message "No free connections available" was displayed. Parallelism is now enabled on the MySQL driver, allowing multiple queries to be sent to the MySQL server over multiple connections.
#36106 #36667 #37733	The RADIUS service crashed, causing authentications to fail, if unprintable characters were present in the State attribute from third-party RADIUS targets.
#36147	When a proxy server was configured, ClearPass license activation over the proxy server failed. Now after the connection is established between ClearPass and the proxy server, all packets will go through the proxy server.
#36848	After a cumulative update patch was installed and the system restarted, the incorrect username "clusteradmin" was shown in the **Event Viewer**. The **System Event Details** now correctly shows the user as "appadmin".
#36872 #37059	High CPU usage occurred during the cleanup interval. Bulk Guest user operations such as deletion, insertion, and updates are now optimized to avoid interference with request processing.
#36879	Corrected a TACACS+ issue where the `ENABLE` authentication failed if the `authen_type` field contained an invalid type. ClearPass now uses ASCII for the `authen_type` when this field has an invalid value.
#36880	In a cluster setup, ClearPass sent multiple reverse DNS queries to DNS servers.
#37160	ClearPass did not accept a password change if the new password began with special characters. Non-alphanumeric characters are now accepted at the beginning of passwords.
#37173	Some events were missing from a Syslog export if the value for accounting input or output octets was greater than the Integer data type's range.
#37457	On a cluster with an accounting proxy configured, Active Directory authentications failed and the error message "Winbind reply failed" was displayed when an excessive number of file handlers caused high CPU consumption.
#37509	SSH-related failure events and rekey events were not shown in the **Event Viewer** if the hostname contained an underscore character (_). The underscore character is now supported in hostnames.
#37520	A Certificate Revocation List (CRL) update failed and the error message "CRL updater encountered an internal error" was displayed if the CRL file size was large (greater than 1MB).
#37709	The username was not always updated in the **Access Tracker** after authentication when an EAP-TLS session was restarted.
#37770	Dropping access-request messages that contain certain attributes caused problems in some scenarios. Now access-requests that contain the following will be dropped *only* when ClearPass is in CC mode: • The response attributes Password-Retry, Reply-message, or Error-Cause. • Both an EAP-Message and an ARAP-Password, User-Password, or CHAP-Password attribute.
#38121	Configuration Database replication between the cluster nodes would hang if both the `username` and

Table 31: *Policy Manager Issues Fixed in 6.6.4 (Continued)*

Bug ID	Description
	`certificate_id` values were null in a row in the `cpg_onboard_user` table and this row was replicated in the subscriber.
#38237	Configuring the **Disable TLSv1.0 support** or **Disable TLSv1.1 support** cluster-wide parameters was not applied to subscribers in a cluster, although it was applied to the publisher.

Profiler and Network Discovery

Table 32: *Profiler and Network Discovery Issues Fixed in 6.6.4*

Bug ID	Description
#37410	Discovered endpoints that did not have a MAC address were ignored. Now for endpoints that do not have a MAC address, ClearPass will create MAC addresses for them that include the prefix “xa”.
#38125	Users should be aware that after running a subnet scan, discovered endpoints that do not have a MAC address will be displayed with a hyphen in the **MAC Address** column in the **Configuration > Identity > Endpoints** list.

Fixed in 6.6.3

The following issues were fixed in the 6.6.3 release.

Guest

Table 33: *Guest Issues Fixed in 6.6.3*

Bug ID	Description
#36503	Hotel hotspot registration did not work if the hotel guest’s name included an apostrophe character (‘).
#36614	After updating to 6.6.2, SOAP API calls failed and the error “failed to load external entity” was shown in the Application Log.
#36616	Hotspot invoice number sequences for online transactions were not retained during ClearPass upgrades.
#36621	For social logins configurations, the Clever API account did not have privileges to access the full profile. Now for social logins that use Clever, the account type is correctly set in the social_vip attribute.
#37062	The PHP version is now updated to 5.6.28.
#37224	The special value “_admin” was not recognized as a valid email address for sending guest account expiration warnings.
#37228	AirPlay authorization did not work for some devices if they were added through a bulk upload using comma-separated values (CSV).
#37154	Guest account expiration warning messages were not sent unless the **ClearPass Guest Services** plugin configuration had been updated.
#37156	If an SMS message included special characters and an email address, some of the special characters and the “@” character in the email address were removed from the received message. Support is now added for configuring the character set used to communicate with an SMPP server. To use this feature,

Table 33: *Guest Issues Fixed in 6.6.3 (Continued)*

Bug ID	Description
	go to **Guest > Configuration > SMS Services > Gateways > Create new SMS gateway**. In the **SMS Gateway** field select **SMPP v3.4**, and then use the **Message Encoding** field to specify the message encoding to use when sending messages to the SMPP provider.
#37335	Social logins failed with the error "Your username could not be determined" for the following vendors: Bitbucket, Disqus, Fitbit, Tumblr, VK, and Xing.
#37337	Self-registrations that allow a timezone to be selected were setting the wrong value if the expire_time date picker was used.

Insight

Table 34: *Insight Issues Fixed in 6.6.3*

Bug ID	Description
#35738	Corrected an issue where the System Monitor widget on the Insight Dashboard did not display any data.
#36641	In Insight reports, a dynamic search for endpoint IP addresses sometimes took several minutes or failed to complete. The autocomplete function is now removed from report filters and alert filters. Users should enter the full IP address in the search field.

Onboard

Table 35: *Onboard Issues Fixed in 6.6.3*

Bug ID	Description
#36530	At **Onboard > Certificate Authorities > Create new certificate authority**, the error message "NwaMdpsCertificate with id %2 not found" was displayed if either of the Elliptic Curve Digital Signature Algorithm (ECDSA) options was selected in the **Key Type** field (either **X9.62/SECG curve over a 256 bit prime field** or **NIST/SECG curve over a 384 bit prime field**).
#36594	If an Onboard Certificate Authority (CA) was successfully created as a Registration Authority type (RA) that used an intermediate certificate, attempting to edit it after creation changed its status to "Chain Incomplete" and it could not be used.
#36689 #36922	Corrected an issue where the Onboard license usage count was not updated for devices whose certificate key was created by the server, so the number of records shown in **Onboard > Management and Control > View by Certificate**, **Onboard Usage**, and **Policy Manager > Administration > Server Manager > Licensing > License Summary > Used Count** was incorrect.
#36701	When enrollments created by the standalone SCEP server were migrated to 6.6, serial numbers for external device records were not correctly migrated. This resulted in a number of records in the **Onboard > Management and Control > View by Device** list having no **Device Name** displayed.
#36853	In ClearPass 6.6.2, the SCEP server was unable to handle long input (1024 characters). This caused Airwatch SCEP integration with ClearPass to fail, and the error message "Cannot parse SCEP message: E1: scep.c:792: error while reading msg" was shown in the **Application Log** at **ClearPass Guest > Administration > Support**.
#36871	Attempting to import an intermediate Certificate Authority (CA) failed and the error message "Fatal Application Error: Cannot pass parameter 1 by reference" was displayed.

Table 35: *Onboard Issues Fixed in 6.6.3 (Continued)*

Bug ID	Description
#36958	Onboard certificate migration failed if some fields contained embedded null characters.
#37153	The Onboard Registration Authority CA did not accept responses from an upstream SCEP server if the server returned multiple CA certificates.

OnGuard

Table 36: *OnGuard Issues Fixed in 6.6.3*

Bug ID	Description
#35530	ClearPass was not able to select the correct WebAuth service based on the Host:OSType attribute. This applied to the Persistent and Native agents only; this attribute is not applicable to the Java-based Dissolvable Agent.
#35745	Trying to uninstall the ClearPass OnGuard Unified Agent failed if the Windows **Event Viewer** was open.
#35950	When a quarantine message was configured in the HTML with an anchor tag, the ClearPass OnGuard Unified Agent for Mac OS X did not display the message as a hyperlink, and displayed the tag instead. Anchor tags are now supported for quarantine messages.
#36023	The VIA component of the ClearPass OnGuard Unified Agent for Mac is now updated to Mac VIA 3.0.1. For information about the features and enhancements available in Mac VIA 3.0.1, refer to the *Aruba VIA 3.0.1 Mac Edition Release Notes* available on the **Support** site (support.arubanetworks.com) at **Documentation > Software User & Reference Guides > Aruba VIA > Release Notes > macOS**.
#36514	Auto-update of the ClearPass OnGuard Unified Agent for Windows sometimes failed for non-administrator users.

Policy Manager

Table 37: *Policy Manager Issues Fixed in 6.6.3*

Bug ID	Description
#35190 #35192	Duplicate updates were sent to Palo Alto Networks if client authentication occurred on two different appliances within a one-hour interval.
#35573	ClearPass sometimes dropped packets and displayed the error message “nf_conntrack: table full, dropping packet.” The size of the connection tracking table is now increased from the previous default value of 65,563 to the following values: • CP-VA-500 = 262,144 (256 K) • CP-VA-5K = 262,144 (256 K) • CP-VA-25K = 524,288 (512 K) • CP-HW-500 = 262,144 (256 K) • CP-HW-25K = 524,288 (512 K) • CP-HW-5K = 262,144 (256 K)
#35732	The Policy Manager **Dashboard** did not display graphs in the **System CPU Utilization** widget or the **Request Processing Time** widget due to a time zone issue. ClearPass is now updated to use the latest time zone information.
#35733	Users should be aware that, for used disk space calculations, the displayed values shown in the user interface at **Monitoring > Live Monitoring > System Monitor** do not match the free disk space values shown in the CLI or through the snmpwalk application.

Table 37: *Policy Manager Issues Fixed in 6.6.3 (Continued)*

Bug ID	Description
	Disk usage can be monitored three different ways: • Through the **System Monitor** page. The value displayed on this page shows used space. • Through the CLI **`show sysinfo`** command. The value displayed this way shows the free space. • Through snmpwalk. The value displayed this way also shows the free space. When the used space displayed in the **System Monitor** is subtracted from the total disk size, it does not equal the free space indicated by the CLI and SNMP methods. This is because the used space value does not take into consideration the blocks of disk space that are reserved for the root user, but the free space value does include this.
#35737	Admin users were not able to copy a network device from the table summary at **Policy Manager > Configuration > Network > Devices**.
#35743	RADIUS authentications failed if the service name was more than 63 characters long. At **Policy Manager > Configuration > Services > Add**, the length of the entry in the **Name** field for a **RADIUS Proxy** type is now limited to 63 characters.
#35787	Updating a password for a PSK-based IPsec tunnel caused the tunnel connection to fail.
#35862	TACACS authentications failed and the error message "(error=28) Timeout was reached" was displayed. This was due to an out-of-memory condition that occurred if the TCP protocol was configured and messages could not be delivered.
#35867	A successfully established IPsec tunnel was incorrectly described as failed on the **Monitoring > Event Viewer > System Event Details** form. ClearPass now correctly displays the status details for an IPsec tunnel connection.
#35930 #36301	ClearPass periodically stopped sending updates to Palo Alto Networks (PANW) firewall. Data is now sent as a payload instead of URL-encoded. This change allows a larger Host Intrusion Prevention (HIP) update to be posted to PANW and the register update to be skipped in case device profile information is missing. If the Palo Alto Networks integration was already configured prior to upgrading to ClearPass 6.6.3, a minor modification needs to be made to the **UserID Post URL**. Go to **Administration > External Servers > Endpoint Context Servers** and select any applicable Palo Alto Networks firewalls. Remove the **&cmd={cmd}** from the UserID Post URL so that it only shows the following: **`https://{server_ip}/api/?type=user-id&action=set&key={key}`**
#35982	For an IPsec tunnel established with ClearPass, the Windows 2008 server might time out and abruptly terminate the connection if there is no traffic over the tunnel for more than five minutes. Users should be aware that this is the expected behavior with Windows 2008. To avoid it, under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSec use the registry setting SAIdleTime to define the allowed idle-time duration.
#36051 #36323	After updating to 6.6.1 or 6.6.2, the serial console was not accessible on hardware versions of ClearPass.
#36059	After the zone was changed for a Network Access Device (NAD) the **Monitoring > Audit Viewer** form correctly showed the modification but it also incorrectly showed the community string as having been changed.
#36062	A deleted CRL was cached and still showed in the revocation list. Users should be aware, however, that deleting a CRL will restart the IPsec service.
#36141	Fingerprints were not updated during a cumulative patch update, and a status check had to be performed after the update in order to get the most recent fingerprint versions. The latest fingerprints are now included in the patch update process.

Table 37: *Policy Manager Issues Fixed in 6.6.3 (Continued)*

Bug ID	Description
#36150	The RADIUS server was not able to process requests for some time (as much as an hour) after a configuration change and displayed the error message "Client couldn't complete EAP transaction."
#36194	Corrected a cluster join issue where trying to add a new node to an existing cluster failed and displayed the error message "Setting up subscriber failed". This was caused by manual deletion of the default zone in the cluster. As part of the fix, manual deletion of the default zone in a cluster is now blocked. This is because the newly added nodes in the cluster are assigned to the default zone, so the default zone must be retained.
#36197	ClearPass was able to accept weak ciphers in an IPsec connection. Now the peers must support all the configured algorithms in order for an IPsec connection to succeed.
#36237	MSCHAPv2 authentications against Active Directory sometimes failed with an "AD status: Access denied" error.
#36294	In EAP authentication, the RADIUS service frequently crashed and restarted if the inner identity had a null value.
#36398	Trying to parse a samba configuration file failed if any line in the file was long (greater than 1024 characters). The maximum read line length is now increased to 4096.
#36401	The **Access Tracker** took a long time to show individual records the first time it was accessed after login.
#36487	ClearPass added extra Message-Authenticators in the RADIUS packet if an external RADIUS server was used as the authentication source.
#36535	Timestamps on Ingress Events engine requests were logged in the database in Universal Time Code (UTC) instead of the local system's time zone.
#36557	After updating to 6.6.2, a modification to an enforcement policy or profile displayed an error message if migration of the agent profile was not successful.
#36626	The cpass-radius-service crashed and restarted if a username was not present in the Access-Request and both the Inner-Identity and Outer-Identity were different.
#36775	Offline license activation failed in ClearPass 6.6.x versions.
#36843	Corrected an issue where the IPsec tunnel frequently disconnected.
#36859	ClearPass is now updated with the latest Universal Time Code (UTC) time zone information for all countries.
#37089	Events were not displayed in the **Event Viewer** if SSH connections to ClearPass appliances were attempted using unsupported keyed-hash message authentication code (HMAC).
#37543	If the Palo Alto Networks Panorama server had multiple firewalls listed under it, ClearPass tried to send the update to multiple targets in single post.

Fixed in 6.6.2

The following issues were fixed in the 6.6.2 release.

CLI

Table 38: *CLI Issues Fixed in 6.6.2*

Bug ID	Description
#35166	CLI logs sometimes grew too large, causing a CP-HW-500 server to crash. Pre-checks are now added to prevent this scenario.

Cluster Upgrade and Update

Table 39: *Cluster Upgrade and Update Issues Fixed in 6.6.2*

Bug ID	Description
#34962	ClearPass patches downloaded from the **Software Updates** portal were shown on the **Administration > Agents and Software Updates > Software Updates > Cluster Update** interface but could not be installed.
#35318	Cluster-wide patch or skin installations were not removed from the log files.

Guest

Table 40: *Guest Issues Fixed in 6.6.2*

Bug ID	Description
#35327	In custom fields, the allowed generators for Initial Value were missing GeneratorFromSession.
#35580	Corrected an issue where, when trying to filter for a guest account, an invalid Role ID data could cause database query errors in ClearPass Guest.
#35639	Expired accounts were not caught if the Pre-Authentication was set to Local.
#35863	The PHP version is now updated to 5.6.25.
#36002	After upgrading to 6.6, exporting guest accounts in Comma-Separated Value (CSV) format failed with database errors due to issues with the way the guest account `Create Time` attribute was stored.
#36005	If multi-factor authentication was configured with a device-first workflow, first-time authentications asked for the account password at two different times.
#36006	Certain configuration forms could not be viewed by read-only operators even though they had permission to view them, and the users were logged out.
#36008	The “Created” time was incorrectly displayed as “1969-12-31 16:00” when importing a Guest user accounts list from a Comma-Separated Value (CSV) file. Data imported in CSV files now supports field formats similar to those in the GUI forms, and no longer needs to be uploaded in its native format.

Onboard

Table 41: *Onboard Issues Fixed in 6.6.2*

Bug ID	Description
#35451	Devices running Windows 8 or higher could not connect to the secure SSID after onboarding if the TLS client certificate private key was configured to be generated by Onboard.
#36001	Corrected an issue where the Onboard license count was not being updated.

OnGuard

Table 42: *OnGuard Issues Fixed in 6.6.2*

Bug ID	Description
#34400	The ClearPass OnGuard Unified Agent for Windows failed to read the Windows Hotfix list and displayed the error "WBEM_E_SHUTTING_DOWN (0x80041033 or -2147217357)".
#34594	The spelling of "ClearPass Agent Controller Service" is now corrected in the Windows OnGuard Unified Agent logs.
#35145	The ClearPass OnGuard Unified Agent checked for Windows Updates every hour even if Windows Security Health Validator was not configured.
#35147	The ClearPass OnGuard Unified Agent sometimes took a long time to collect health information on a Windows 8 Operating System.
#35188	The Windows OnGuard Unified Agent did not prompt for a password if a wrong password was entered or if authentication failed.
#35595	The ClearPass OnGuard Unified Agent failed to read the DAT file time and DAT file version of Norton Security with Backup 22.7.0.76 AntiVirus.
#35620	A RADIUS disconnect or Change of Authorization (CoA) was not triggered after quitting or exiting the ClearPass OnGuard Unified Agent. Now, if a post-authentication enforcement profile is configured to disconnect OnGuard when the OnGuard session ends, ClearPass sends a CoA and disconnects the client when OnGuard is down for more than five minutes.

Policy Manager

Table 43: *Policy Manager Issues Fixed in 6.6.2*

Bug ID	Description
#28534	Corrected an issue where IPsec did not work unless ClearPass was restarted.
#30937	On the **Software Updates** portal, an **Uninstall** button was available for cumulative and point patch updates. The **Uninstall** button is now available only for skin files.
#33359	In some situations (for example, VIA authentication), the controller set the value of the Calling-Station-Id attribute to 000000000000 and ClearPass treated it as a valid MAC address, which caused VIA + Health check to not work. Now if the client's MAC address is all zeros, it is considered an invalid address, and the RADIUS server does not add any computed attributes for the MAC address. The authentication should succeed. Instead of the MAC address, the username must be treated as a session entry in the Multi-Master Cache.
#34134	In the **Fingerprints** dictionary, a forward slash (/) was not an allowed character when adding or

Table 43: *Policy Manager Issues Fixed in 6.6.2 (Continued)*

Bug ID	Description
	updating values for a device Category, Family, or Name, and the error message "Category contains special characters other than -, _, {}, [], (), period and space" was displayed. The forward slash is now one of the allowed special characters.
#34338	After upgrading to ClearPass 6.6.0, some custom admin privileges did not work and ClearPass screens were blank for users with custom admin privileges that included the **Monitoring > Live Monitoring > Endpoint Profiler** attribute.
#34409	The TipsAPI for the GuestUser entity missed <EntityMaxRecordCount> in the response. Two other attributes, "sendEmail" and "sendSms", are now added to the <GuestUser> element in 6.6.0. Users should be aware that ClearPass 6.6 is the last release that will support certain TipsAPI (XML), Guest SOAP APIs, and Guest XML-RPC APIs. ClearPass 6.6 now includes a variety of RESTful APIs to replace these legacy APIs. We recommend that you migrate to the appropriate RESTful API as soon as possible. For more information, see"ClearPass 6.6 Deprecation Notice" on page 111.
#34823 #34946	After upgrading to 6.6, the **Event Viewer** showed error messages such as "Battery put failed err:Post", "Profiler ip<address> unstable", or "High iowait(25)". The **Event Viewer** now only generates these warnings if an operation fails three times in a row within 15 minutes.
#34845	ClearPass was unable to complete an Active Directory (AD) connection using TLS 1.2. The TLS 1.2 protocol is now supported for AD-over-SSL connections.
#34853	Multiple values were not allowed for the List data type in the 6.6.0 release. The **Allow Multiple** field is now restored to the **Add Attribute** and **Edit Attribute** forms for List attributes.
#34890	If an attribute name was edited at **Administration > Dictionaries > Attributes**, the name was not updated in **Enforcement Profiles**.
#34925	The Apache Struts version is now upgraded to 2.3.29 GA.
#35031	When trying to authenticate with an HTTP authorization source configured for a service, authentication failed and the alert "RADIUS: Service Categorization failed\nCannot send request to Policy server" was displayed. Unsupported JSON objects are now handled correctly.
#35062	Authentication failures occurred if the RADIUS server or policy server processes reached the maximum allowed number of open files, especially if a large number of authentication or authorization sources were configured (65+). The "max open file handlers limit" (`ulimit -n`) is now increased to 100,000 for RADIUS server and policy server processes.
#35075	The Apache Tomcat version is now upgraded to 7.0.70.
#35109	Support for DES and IDEA cipher suites is now removed.
#35113	Corrected an issue where a Network Administrator could create a local user with Super Administrator privileges. Administrators can only create new admin users with privileges that are the same as or lower than their own. Administrators can only create new admin privileges that are the same as or lower than their own. The default Network Administrator privilege has read-only access to certain configuration pages, such as: • Local Users • Service configuration • Start-Here • Role-mapping • Enforcement Policy • Enforcement Profile

Table 43: *Policy Manager Issues Fixed in 6.6.2 (Continued)*

Bug ID	Description
#35193	In rare cases, local users were disabled even though the correct username and password were used. A local user's failed login attempts are now counted only for the PASSWORD_MISMATCH, PASSWORD_ NOT_AVAILABLE, and USER_AUTHENTICATION_FAILED error codes.
#35202	Exceeding the default threshold values for CPU load averages caused the monitoring server to trigger "System Error" SNMP alerts. The default settings for the CPU load-average service parameters are now dynamic based on the number of CPU cores. This ensures that alerts are based on appropriate thresholds for each system's CPU usage limits.
#35216	The **Event Viewer** did not show audit logs for IPsec connections. Detailed information is now shown whenever an IPsec tunnel is brought up or down.
#35222 #34694	After upgrading to 6.6.0, the **Event Viewer** showed a "High iowait" error. The CPU and memory statistics were collected every 15 minutes and the value of memory and iowait at that instant was compared to the configured threshold. ClearPass now collects CPU and memory statistics every five seconds and computes the average for iowait and free memory over a ten minute period. The average value is compared to the threshold to generate alerts.
#35236	A RADIUS server or HTTPS server certificate could be installed even though the signature byte of the certificate hash had been modified.
#35238	An IPsec tunnel was established even if OCSP or Certificate Revocation List (CRL) validation failed. Strict CRL policy can now be enabled or disabled. To use this feature, go to **Administration > Server Manager > Server Configuration > Service Parameters** and select **ClearPass IPsec service**. In the **Strict CRL Policy** field, select **yes** (the default value is **no**). When this option is enabled, a fresh CRL must be available in order for a peer connection to succeed. Whenever the **Strict CRL Policy** value is modified, existing IPsec tunnels that use Public Key Authentication will be brought down and then brought up again.
#35254 #35458	Corrected an issue where Checkpoint integration failed. All Checkpoint action attributes are now correctly substituted.
#35259	JQuery libraries are now updated to 1.11.1 for Policy Manager and 2.1.4 for Insight.
#35291	An IPsec connection could not be established between ClearPass and a Windows 2008 server using PSK and IKEv1.
#35459 #35460 #35461 #35524	Users should be aware of the following support changes for IPsec connections. These encryption algorithm changes apply to both FIPS mode and non-FIPS mode: • ClearPass no longer supports using the 3DES encryption algorithm for IPsec connections. Existing systems that have 3DES configured will be updated to AES-128. • ClearPass no longer supports using AES-192 for IPsec connections. Existing systems that have AES-192 configured will be updated to AES-128. • ClearPass no longer supports using Diffie-Hellman (DH) Group 1 or 2 for IPsec connections. Existing systems that have DH Group 1 or 2 configured will be updated to DH Group 5. • ClearPass no longer supports using IKEv1 in Aggressive Mode for IPsec connections. Existing systems that have Aggressive Mode configured will be updated to Main Mode.
#35495	In ClearPass 6.6.0 and 6.6.1, the configuration database used date and time in the UTC (GMT) time zone instead of using the system's configured time zone, and the date and time were also displayed in UTC in the [Time Source] authentication source and external SQL queries. ClearPass 6.6.2 now behaves like ClearPass 6.5 and earlier versions, where the configuration database and [Time Source] use the system's configured time zone.
#35500	During ClearPass license activation, some workflows did not perform certificate validation for the Activation Server Certificate.

Table 43: *Policy Manager Issues Fixed in 6.6.2 (Continued)*

Bug ID	Description
#35532	The Ingress Events service did not run as expected after a system update.
#35715	The accounting records calculation for input and output octet bytes was incorrect if the Acct-Output-Gigawords attribute was also present.
#35747	Corrected an issue where `acct_start` and `interim_update` accounting information was not updated. The accounting event's timestamp now records the time filed in milliseconds.
#35758	After installing a patch update on the **Software Updates** portal, the **Reboot** button did not initiate a system restart.
#35812	The **Install Update** window on the **Software Updates** portal did not include an **Uninstall** button for Guest skins that were installed before ClearPass 6.6.1.

Fixed in 6.6.1

The following issues were fixed in the 6.6.1 release.

Guest

Table 44: *Guest Issues Fixed in 6.6.1*

Bug ID	Description
#33620	For self-registrations configured to interact with a FIAS-based hotel Property Management System (PMS), a room page was not created when the transaction processor was changed from non-PMS to PMS.
#34174 #34642 #34968	The PHP version is now updated to 5.6.23. This includes fixes for CVE-2013-7456, CVE-2016-3074, CVE-2016-5093, CVE-2016-5094, and CVE-2016-5096.
#34464	Corrected an issue with guest self-registration pages where, when a new account was successfully created, the application logs showed the error " relation "tips_guest_user_tag_mappings" does not exist".
#34468 #34475	Extension installations did not honor the configured list of trusted certificates. In certain circumstances this could have led to the extension installation failing with an "unknown issuer certificate" error.
#34479	Corrected an issue with **Guest Self-Registrations** configuration where, after enabling sponsorship confirmation, editing and saving **Login Delay** or **NAS Vendor Settings** disabled the sponsorship confirmation.
#34483	In **Configuration > Receipts > Digital Pass Templates**, uploading a certificate along with a passphrase failed with the error message "Unable to handle request at this time".
#34735	ClearPass Guest could not send emails over TLS to servers with custom certificates.
#34794	The shortcut to include guest pages and content URLs was missing from some HTML configuration areas.
#34810	Deleting a Web page or a pass template displayed the error message "Row query failed: ERROR: column o.object_id does not exist".
#34818	When a device's locale settings used a comma separator in currency, there were problems posting charges to the guest's account and some room charge communications had formatting errors.

Insight

Table 45: *Insight Issues Fixed in 6.6.1*

Bug ID	Description
#33255	In the **Auth Trend** report, the guest authentication counts shown for certain days in the **1 month** section did not match the authentication counts shown for the same days in the **1 week** section. The weekly graph widget is now removed.
#33585	While creating a report with the **Notify by Email** or **Notify by SMS** fields selected but where the email or phone number for the notification were not provided, the report could be saved and no error message was displayed about the missing information.
#34097 #34533	A user with the Super Administrator role could not log in to Insight with their Active Directory (AD) credentials if the **Full Access** option was configured in the operator profile.

Onboard

Table 46: *Onboard Issues Fixed in 6.6.1*

Bug ID	Description
#33822 #34465	If a device limit was set, Onboard enrollment failed with the error “Fatal Application Error: Call to undefined method....”
#34466	On the **View by Username** and **View by Device** pages, devices could not be deleted and the message “Error: 500” was displayed.
#34467	After upgrading to ClearPass 6.6.0, selecting **Onboard > Management and Control > View by Username** displayed the error message “Row query failed: ERROR: column "object_id" does not exist”.
#34469	Corrected an issue where device expiration notifications were not sent.
#34471	When upgrading to ClearPass 6.6.0, Onboard configurations that used an ECDSA CA certificate could not be migrated and caused the upgrade to fail.
#34473	When upgrading from ClearPass 6.5.5 to 6.6.0, Onboard migration failed.
#34476	At **Onboard > Management and Control > Usage**, the **License Usage** description incorrectly stated that a rolling average was used. It is now correctly described as a count.
#34478	If a custom trusted certificate was specified during Onboard enrollment, the error message “Onboard server returned HTTP Status code - 500” was displayed and onboarding failed.
#34480	After saving settings migrated from earlier versions, a user logging in to Onboard was redirected to securelogin.arubanetworks.com instead of to the Onboard workflow.
#34481	In the **Self-Service Portal**, devices were correctly displayed in the list but the options row was not visible, so users could not delete a device or perform other actions even if they had full-access permissions.

OnGuard

Table 47: *OnGuard Issues Fixed in 6.6.1*

Bug ID	Description
#26085	Editing the ClearPass Linux Universal System Health Validator plugin cleared the default services configuration data.
#26276	On Mac OS X 10.10, the ClearPass OnGuard Unified Agent 's VIA component failed to download the connection profile when the tunnel was established, and the log window showed the error "Configuration download... failed".
#27602	The ClearPass OnGuard Unified Agent failed to return health-check data over a VPN tunnel if the agent was installed on a client running MAC OS X 10.10 and used Kaspersky AntiVirus software.
#30573	The ClearPass OnGuard Unified Agent now supports Encrypted Locations checks for FileVault 10.11 on Mac OS X 10.11.
#33862	The ClearPass OnGuard Unified Agent categorized Check Point VPN Adapter as WIRED or OTHER.
#33865	The ClearPass OnGuard Unified Agent did not use the value of LogoutBounceDelay if the OnGuard Agent was closed or killed.
#34144	On Mac OS X, if a VPN was connected when the ClearPass OnGuard Unified Agent was uninstalled, the VPN interface was not removed and the client remained connected to the VPN interface.

Policy Manager

Table 48: *Policy Manager Issues Fixed in 6.6.1*

Bug ID	Description
#28399	In OnGuard Settings, it was not clear which IP address was applied to the ClearPass OnGuard Unified Agent. At **Administration > Agents and Software Updates > OnGuard Settings > Policy Manager Zones**, the **Default ClearPass Server IPs** field for a Policy Manager zone now shows the correct IPs when both the data and management ports are configured.
#32088	Network discovery sometimes did not add some devices to the endpoints table if they did not return a MAC address.
#32759	During a bulk import of Network Access Devices (1000+), a backend process sometimes took a long time to complete even though the user interface indicated the import had completed.
#33312	If authentication latency to Active Directory was greater than 30 ms, a specific process thread used by the TACACS service to internally communicate with the authentication service might have been overwhelmed using the default static value. A new option, **TACACS+ HTTP Thread Pool Size**, lets you adjust the maximum number of simultaneous requests as needed within a range of 5 to 200. This option is available at **Administration > Server Manager > Server Configuration > <server name> > Service Parameters > Tacacs server**.
#33353	The postauth do_expire action blacklisted users based on exceeded session counts and agent connection checks. Users monitored under session restriction are now blacklisted only if the bandwidth usage or session duration exceeds the configured limit, if any, and not in any other case.
#33472	The libssh2 version is now upgraded to libssh2-1.4.2-2.el6_7.1.x86_64. This includes fixes for CVE-2016-0787.
#33551	The RADIUS service stopped if a 24th authentication source was added to a service using a static host list. The warning message "No. of Authentication Sources cannot exceed 23" is now displayed if the user

Table 48: *Policy Manager Issues Fixed in 6.6.1 (Continued)*

Bug ID	Description
	attempts to add more than 23 authentication sources.
#33635	After morphing a virtual machine (VM), the total disk space shown in the **Monitoring > Live Monitoring > System Monitor** dashboard in Policy Manager was incorrect. This value is now consistent in the CLI and the System Monitor dashboard in both Policy Manager and Insight.
#33725	Corrected an issue where low disk alerts and low memory alerts were not logged.
#33736	After morphing a virtual machine (VM), the total memory shown in the **System Monitor** dashboard in both Policy Manager and Insight was incorrect. The value is now consistent in the CLI and System Monitor dashboard in both Policy Manager and Insight.
#33741	After adding additional memory in a virtual machine (VM) image, the total memory shown in the **Monitoring > Live Monitoring > System Monitor** dashboard in Policy Manager was incorrect.
#33843	Corrected an issue where a memory leak was triggered when a RADIUS server configuration was reloaded.
#33926	The PostgreSQL version is now upgraded to 9.4.8. This includes fixes for CVE-2016-0773.
#33928 #33958 #33959 #34021 #34243	This release includes fixes for CVE-2016-2118, CVE-2016-2034, and CVE-2016-2107.
#33956	Sending Syslog messages to multiple TCP-enabled Syslog servers did not work. ClearPass now allows sending Syslog messages to any number of TCP or UDP-enabled Syslog servers.
#33964	Session Log syslog filters (if configured) caused high consumption of CPU and System resources. Query generation is now optimized to fix this issue. Users should be aware that some attributes or rows might be missed if tables are not updated.
#34014	The **Access Tracker** did not show the TACACS Authentication request details if its corresponding Authorization requests did not contain any details.
#34057	On ClearPass ESXi 6.0 (and later) virtual machines, an operating system process repeatedly tried to respawn a process for ttyS but failed because serial ports were not present.
#34129	Corrected an issue where a high volume of authentication requests and EMM/MDM updates resulted in periodic authentication failures.
#34130	Updating usernames through a policy did not update them properly in the Multi-Master Cache, which caused Change of Authorization (CoA) to fail with HPE ArubaOS-Switches running 16.02. The Policy Server now posts the updated username to the Multi-Master Cache, and the value is properly sent in the CoA request.
#34153	When creating a new 802.1X service using a template, the service configuration failed and displayed the error message “Error in processing request. Please retry”.
#34223	TACACS authentications failed if there were null parameter values, and displayed the message “Internal error in performing authentication”.
#34447	A new root certificate for the Activate server could not be validated. The **CN=GeoTrust Primary Certification Authority – G3** root certificate is now added to the default trust list.

Table 48: *Policy Manager Issues Fixed in 6.6.1 (Continued)*

Bug ID	Description
#34615	Corrected an issue where the NETBIOS name was not appended in the user ID updates sent to Palo Alto Networks (PANW) if `UserPrincipleName` was used to authenticate the user and modified using the RADIUS username enforcement profile.
#34639 #34824	When the endpoint profile fingerprint file was updated, the error message "Failed to update fingerprints from ClearPass Portal (Online)" was displayed in Insight Alerts.
#34662	Configuring ClearPass as a TACACS authentication server created a loop and caused high CPU utilization (99%) on the Network Access Device if the device continuously sent an empty password.
#34728	With simultaneous-limit checking enabled, ClearPass disconnected a user as having exceeded the configured number of simultaneous sessions even though the user had fewer active sessions than the limit.

Fixed in 6.6.0

The following issues were fixed in the 6.6.0 release.

CLI

Table 49: *CLI Issues Fixed in 6.6.0*

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

Dissolvable Agent

Table 50: *Dissolvable Agent Issues Fixed in 6.6.0*

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

Endpoint Context Servers

Table 51: *Endpoint Context Server Issues Fixed in 6.6.0*

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

Guest

Table 52: *Guest Issues Fixed in 6.6.0*

Bug ID	Description
#18700	An out-of-date message could be displayed in the **List Accounts** view.
#27847	Corrected a potential Cross-Site Scripting (XSS) issue when using the `nwa_mdps_config` smarty function.
#28480	The SMS provider selection could not be overridden in a self-registration.
#28877	Corrected some issues with performance when there is a large number of accounts. Tag lookup performance is now greatly improved in guest management queries.
#28974	Corrected some issues with syntax checking for template scripts.
#29027	The application would hang if an overly restrictive password configuration was chosen.
#30154	Date pickers were not rendered correctly when using the Galleria skin.
#30304	Deleting a guest account sometimes took as long as five minutes. This was observed on a CP-HW-5K system after upgrading to 6.5, following an upgrade path of 6.1.4 > 6.2.6 > 6.5.2.
#30840	The "Permit login on validation error - validation errors will be logged" option is now removed from **Security Hash** drop-down list on the **Configuration > Pages > Web Logins** form or the **Guest Self-Registrations > Advanced editor** form. If you had this option set, please re-save the configuration with a valid option.
#30842	Corrected some visual issues with the color picker controls that could occur with certain skins.
#31335	For Web logins configured to require a Universal Access Method (UAM) challenge, the challenge was not sent.
#31386	Forcing a default destination in a Cisco Wi-Fi environment did not redirect to the specified address.
#31450	The MAC address was not normalized during import. MAC devices imported into Guest now format the MAC to the system standard.
#31664	Emails were generated incorrectly of the No Skin option was configured. Users should be aware that emails sent with one of the No Skin options might not display correctly in all email clients.
#31745	With a Ruckus controller configured, ClearPass did not send the proper POST URL information to the client for captive portal authentication. Login configuration parameters for Ruckus Wireless have been adjusted.
#31934	Partial configuration backups could fail if not all selections were made in the list of items to back up.
#32292	Users should be aware that the default privileges for the **Help Desk** operator profile have been changed in this release. The **Manage Customization** and **Manage Print Templates** privileges are now set to **Read Only** instead of **Full**. System administrators should review their **Help Desk** operator profile and update the privileges accordingly.
#32735	The `_browser=1` URL parameter was not compatible with some social login providers. If you have configured social logins, please review any URL access control lists within the application configuration. URLs prior to ClearPass 6.6 required the `?_browser=1` parameter to be appended. That argument must now be removed.

Table 52: *Guest Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#33071	HTTP User Agent profiling was not collected for Guest Web pages other than Web login pages. Guest Web pages now correctly populate attributes and record client profile information.
#33329	The PHP version is now updated to 5.6.19. This includes fixes for CVE-2015-3152, CVE-2015-2325, CVE-2015-2326, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2015-1351, and CVE-2015-1352.
#33650	When using XML-RPC, API responses were in the ISO-8859-1 character set instead of UTF-8. All XML-RPC responses are now encoded in UTF-8.

Insight

Table 53: *Insight Issues Fixed in 6.6.0*

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

Onboard

Table 54: *Onboard Issues Fixed in 6.6.0*

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

OnGuard

Table 55: *OnGuard Issues Fixed in 6.6.0*

Bug ID	Description
#31114	The ClearPass OnGuard Unified Agent stalled in “connecting” mode when the user was switched during a health check.
#31201	For Windows 8 clients, the ClearPass OnGuard Unified Agent was not able to read last scanned time for Symantec Hosted Endpoint Protection.
#31581	OnGuard WebAuth requests were not evenly distributed among cluster nodes if **OnGuard Load Balancing** was enabled in the **OnGuard Global Agent Settings**. Load balancing is now improved to more efficiently distribute OnGuard WebAuth Requests across the cluster.
#31619	On Mac OS X, the ClearPass OnGuard Unified Agent could not read the RTP status of ESET Cyber Security 6.1.12.0.
#31993	The ClearPass OnGuard Unified Agent reported an incorrect status for the McAfee Host Intrusion Prevention Firewall.
#32024	The ClearPass OnGuard Unified Agent did not perform health checks if there were new-line characters in the **Override Server IPs** field.
#33388	The ClearPass OnGuard Unified Agent sometimes categorized the **Aruba Virtual Adapter #2** network adapter as **OTHER** instead of **VPN**.

Policy Manager

Table 56: *Policy Manager Issues Fixed in 6.6.0*

Bug ID	Description
#21593	Corrected an issue where a customer’s ClearPass appliance was using port 4949 and port 8443. All access to TCP ports 4949 and 8443 is now blocked.
#23923	Bulk deletion of endpoints from the user interface might have resulted in inconsistencies between endpoint-related tables. Now when 50 or more endpoint profiles are deleted at one time, the profile attributes for these endpoints are retained in the Profile table. Retention of these profile attributes does not interfere with authentication.
#27363	If the default role-mapping policy [Guest Roles] was renamed, the guest roles in ClearPass Guest were not populated. Now a name change is not allowed in the **> Policy Name** field on the **Policy** tab at **Policy Manager > Configuration > Identity > Role Mappings > [Guest Roles]**.
#27737	Session Restriction Enforcement was not converted to Session Notification if Session check User name was configured.
#27800	The value for the endpoint status was not displayed in Insight reports if the status was changed using POST Auth enforcement. Endpoint status change operations through Post Authentication enforcement are now propagated to Insight.
#27885	The **Administration > Server Manager > Licensing** page continued to display a message that the Onboard license count had been exceeded even after the actual license count was reduced to within limits.
#27908	When upgrading from 6.4.0 or 6.4.1 through the CLI, you had to first download and install a 6.4.0 CLI updates patch and then update to 6.4.2 or later before upgrading to 6.6.

Table 56: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#27922	In some upgrade cases, the services did not come up properly on subscribers, resulting in Webauth/TACACS authentication failures, and the **Access Tracker > Session Details** form showed the internal error message "Failed to authenticate user".
#28049	The RADIUS server's authentication and accounting ports could not be changed. The ClearPass RADIUS server's authentication port and accounting port can now be set to custom values. To use this option, go to **Administration > Server Manager > Server Configuration**, click the **Service Parameters** tab, and select the **RADIUS Server** service.
#28457	OCSP checks are now supported when using smart card certificates for 802.1X authentication.
#28693	When zones were created with certain special characters, the CPU Usage and CPU Load graphs were not displayed on the **Monitoring > Live Monitoring > System Monitor** page. Users should be aware that only the following special characters are allowed in zone names: - . { } [ ] ( ) and spaces. Do not use the following unsupported characters in zone names: ` ~ ! @ # $ % ^ & * + = \ | " ' < > , ? /
#28743	An excessive number of account lockouts occurred for users authenticating against Active Directory after changing their password. ClearPass now always uses the **Name** field value from the EAP MS-CHAPv2 packet to calculate the challenge. The RADIUS service parameter **Re-attempt AD login with different Username formats** has also been removed.
#28787	No information was displayed for VPN clients on the **Accounting Record Details** form at **Monitoring > Live Monitoring > Accounting**.
#28991	Endpoint context server updates failed after Palo Alto Networks firewall was upgraded to PAN-OS 7.0.
#29038	The "Subject-serialNumber" attribute could not be used in the LDAP filter for authorization. The "Subject-serialNumber" attribute is now incorporated into the certificate namespace.
#29169	A RADIUS service failure occurred when using the ClearPass Upgrade Tool. During the domain join operation or domain service start-up after the upgrade process, if the Alt Name or Domain SID is null, ClearPass will ignore them and proceed with the domain join and service start.
#29196	RADIUS CoA could not be done if the machine and user authentication were configured in HP switches.
#29464	Changing the appadmin password in Post Auth Enforcement Profile checks caused disconnect failures via RADIUS Change of Authorization (CoA).
#29662	The OpenSSL version is now upgraded to 1.0.1p. This includes fixes for CVE-2015-1793.
#29876	The Curl version is now upgraded to 7.19.7-46.1. This includes Curl bug fixes and enhancements, and fixes for CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, and CVE-2015-3148.
#29914	Corrected an issue where performing Guest application authentication against the Active Directory failed.
#30075	On the **Monitoring > Live Monitoring > OnGuard Activity** page, the online/offline **Status** sort option did not work.
#30221	Installing a patch update might fail if the boot partition did not meet the free space requirements required by the update.
#30280	When using the DHCP SPAN port, ClearPass Profiler was unable to profile devices if the spn packets had an 802.1q header.

Table 56: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#30293	Role mapping failed after updating from 6.5.0 to 6.5.2 for devices enrolled in JAMF, making clients unable to connect. This was caused by endpoint update issues from JAMF if one of the endpoints had an empty attribute value.
#30318	A RADIUS server authentication source failed with Aruba Application service types. A validation error is now displayed if a RADIUS Server authentication source is part of a non-RADIUS-based service.
#30444	Under **Administration > Dictionaries > Attributes**, attributes of different entity types but using the same name could not be imported.
#30510	ClearPass user interface displayed the error message "No licenses configured", and the "`system refresh-license`" command had to be entered in the CLI to correct it.
#30556	At **Administration > Server Manager > Server Configuration**, DNS information was not saved after editing.
#30564	CoA and Profiling API access is now restricted to Administrator and API Administrator accounts.
#30595	Adding new devices to in the **Configuration > Network > Device Groups** list caused existing devices to be deleted.
#30641	ClearPass now supports migration of multivalue non-string attributes.
#30731	The Endpoint Profiler table and pie chart did not update with the correct values if the user selected the **Choose View** option.
#30984	Guest account attributes could have been overwritten when using the **expired_notify_status** field.
#30995	Updating information in Insight failed if a cluster password was configured with 20 or more characters.
#31111	It was sometimes necessary to clear the router ARP entry in order for VIP to work correctly after a network flap.
#31126	The ClearPass appliance failed to fetch endpoint attributes for random user authentications.
#31202	The publisher database was left in an inconsistent state after a subscriber attempted a promote operation. This occurred when the switch to publisher API call as part of a promote publisher operation failed.
#31247	The jQuery version is now upgraded to 1.11.1.
#31277	Corrected an issue where the ClearPass RADIUS server stopped responding. Information-level logs are now included that print the number of requests in the processing tree in order to determine configuration reloading time.
#31291	On the **Administration > Server Manager > Server Configuration > Service Parameters** tab, the default values did not match the parameter values. The values are now set to the same as the default values for each hardware platform.
#31534	Access was not restricted to some pages of the admin UI. Support is now added to control API URLs. This includes: • A new resource, "ClearPass API," was added at **Server Configuration > node > Network > Application Access Control**. • By default, access to **/api* urls** is allowed for all IP addresses. • Users can modify the setting to allow or deny additional IP addresses.

Table 56: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#31661	NAD clients were sometimes removed from the NAD group.
#31673	Corrected an issue where a SQL Injection attack could occur on callback URL for a Google MDM Connector.
#31953	When the subscribers were not reachable, parallel execution of the cron job to check whether the standby had failed over caused an out-of-memory condition on the publisher.
#31968	Under certain traffic loads, the internal communications between various processes used with TACACS+ authentication could get overwhelmed, which would cause sporadic authentication failures. This issue was not seen in bursts of requests, only in long, sustained requests.
#32002	The output/input bytes calculation was incorrect if the number of output/input bytes was more than 2^32-1. The Acct-Output-Gigawords/Acct-Input-Gigawords attribute value is now included in the input/outputs bytes calculation in the Dashboard utilization tab and insight.
#32007	If guest usernames were created using both uppercase and lowercase characters, the guest's expiration time was not updated via Post Auth.
#32028	SNMP alerts were issued from all the nodes if a change was made on any one node of the cluster. System monitoring configuration updates are now specific to the local node.
#32130	Users should be aware that the following two pages are deprecated from the user interface: **Configuration > Posture > Posture Servers** and **Administration > Dictionaries > Posture**.
#32201	The Apache Commons Collections .jar file is now updated to version 3.2.2.
#32599	Corrected an issue where Insight NetEvents without accounting session IDs created an unnecessary load on an appliance.
#32617	Some subscribers in a cluster displayed the error message "Certificate verifications against this CA will fail till the CRL is updated or removed" before the scheduled update time. The calculation for the check to download the new CRL file is updated to the current time plus 16 minutes, allowing the script to run and download new files every 15 minutes without encountering a CRL expiry error.
#32621	Multiple instances of the AppsUpdater script could run simultaneously, generating a high CPU load.
#32656	When using TACACS, the "change password" prompt was displayed even though the username field was empty.
#32604	Cluster operations were blocked by certificate revocation list (CRL) updates running in the background.
#32678	Users should be aware that, on the Internet Explorer 11 browser, graphs and charts are best viewed in the Edge document mode.
#32787	On the Chrome 48.x browser, adding an enforcement profile at **Configuration > Enforcement > Policies** also added a null enforcement profile.
#33003	Corrected an issue where the RADIUS server could crash when processing badly formatted usernames.
#33025	One of the nodes of a cluster failed to upgrade from 6.3.4 to 6.5.0. During system upgrade, under rare circumstances `route-eth*` was empty, causing the upgrade process to fail. Fixed the system upgrade issue to any empty `route-eth*` and `rule-eth*` files for IPv4 and IPv6 in the current partition.

Table 56: *Policy Manager Issues Fixed in 6.6.0 (Continued)*

Bug ID	Description
#33031	If the domain Fully-Qualified Domain Name (FQDN) was provided instead of the DC FQDN, the attempt to join the domain failed with the error message, "<name> failed to join the domain <DOMAIN NAME> with domain controller as <domain name>". The `ad net join` command is now enhanced to include a detailed description for the domain controller FQDN input field.
#33042	Users were denied ClearPass admin access due to a space between the IP address and subnet mask, which resulted in an invalid host name. Validations have been added for IP address and subnet mask entries on the Application Access Control screen to check for spaces in the host name, which can prevent users from gaining ClearPass admin access.
#33084	glibc is now updated to the latest version. This includes fixes for CVE-2015-7547 in relation to the glibc stack-based buffer overflow in getaddrinfo().
#33098	After upgrading to 6.5.5, the error message "Error in processing request. Please retry" was displayed because of an incompatible certificate.
#33138	The RADIUS Change of Authorization (CoA) could not be sent if the IP range was given in the Network Device.
#33145	An authentication error occurred if an IP address value at **Configuration > Network > Devices** was configured in IP/32 format (for example, 192.168.1.1/32).
#33190	The **OnGuard Clients Summary** widget on the Policy Manager **Dashboard** displayed incorrect data when endpoint attributes were updated manually.
#33748	Users should be aware that ESX 4.x is not supported.

The following known issues for this release were identified in previous releases. Workarounds are included when possible. For a list of known issues identified in the ClearPass 6.6.8 release, see the What's New in This Release chapter.

This chapter includes:

CLI

Table 57: *Known Issues in CLI*

Bug ID	Description
#35750	**Symptom/Scenario:**On a CP-HW-25K / JW772A or CP-HWDL360-25K / JX920A, the total system memory is shown as 65.9 GB instead of 64 GB.

Cluster Upgrade and Update

Table 58: *Known Issues in Cluster Upgrade and Update*

Bug ID	Description
#29710	**Symptom:** Upgrading with the Cluster Upgrade Tool fails if the cluster password includes special characters such as the "at" symbol (@), colon (:), or slash (/). **Scenario:** This occurs on all versions of the Cluster Upgrade Tool. **Workaround:** Before installing the upgrade patch, if the cluster password contains special characters, please change it temporarily to only use alpha-numeric characters (letters and numbers). The cluster password can be changed back to the old password after the cluster upgrade completes.
#33668	Users should be aware that, when performing upgrades with the Upgrade Tool, there are some limitations regarding identification of cluster node status.

Bug ID	Description
	• If a cluster node goes out of sync or is dropped during upgrade, migration, or a cluster join operation, the Cluster Upgrade Tool cannot detect the status of that node. After the cause of the failure is identified, the failed node must be manually rejoined to the cluster. • If any nodes in the cluster are out of sync or force-dropped before the upgrade is started, the Cluster Upgrade Tool cannot detect the status of those nodes. Before starting the upgrade, confirm that all nodes are in proper sync. • During a cluster add or rejoin operation, failure alerts might be displayed if the Cluster Upgrade Tool installs dependent patches before the cluster operation is complete. The upgrades can be initiated through the Cluster Upgrade Tool when the nodes are back in proper sync.
#33669	Users should be aware that there are some Cluster Update Tool scenarios where view, logs, or status update information is not shown. These do not affect functionality. • If a patch update (either a point patch or a cumulative patch) requires an admin-server or async-netd service restart, the INFO logs information on the **Update** tab might be incomplete. • If a patch is updated through the Software Updates portal instead of through the Cluster Updates interface, no status or installation log information is displayed for it in the Cluster Update interface. The **Start Update** option is also still shown for that node, unless there is a manual admin-server restart, or unless there is a cluster operation that triggers a status check of installed patches. • If a node is dropped from the cluster or rejoined to the cluster, the Update Status, View Logs, and Last Step information is cleared for that node.
#33670	Users should be aware that, in cluster setups, skin updates cannot be done in batches. Skin updates must either be done for all the cluster nodes at once, or be manually done on each node.
#35734	Users should be aware that, after a patch update is installed through the **Administration > Agents and Software Updates > Software Updates > Cluster Update** portal, the "Installed" status is not displayed on the **Software Updates** portal. To check the status of a patch that was installed through the **Cluster Update** portal, you must select and view the patch in the **Cluster Update** portal.
#36089	**Symptom:** Patches that have been downloaded but not installed will disappear from the **Software Updates** portal after upgrading to ClearPass 6.6.2 using the **Cluster Update** interface. These downloaded patches, however, will be visible from the **Cluster Update** interface. **Scenario:** This can occur after updating to the 6.6.2 cumulative patch. **Workaround:** If they are still not installed, these patches will be removed during the periodic cleanup that occurs every seven days.
#36114	**Symptom:** If the **Check Status Now** link is clicked in the **Software Updates** portal while a cluster update to 6.6.2 is in progress, the 6.6.2 patch is not shown in the **Update Info > Update Image Name** list in the **Cluster Update** interface, even though the patch updates correctly. This occurs if the appliance was upgraded in this order: 6.6.0 > 6.6.1 > 6.6.2. **Workaround:** We recommend that you do not click the **Check Status Now** link in the **Software Updates** portal while performing the 6.6.2 update.
#37192	**Symptom:** The list of patches available in the **Cluster Updates** page is not the same as the list of patches in the **Software Updates** page. **Scenario:** The **Software Updates** page displays patches that have been both downloaded and installed. On the **Cluster Updates** page, the **Update Image Name** drop-down list incorrectly includes all the patches that have been downloaded, whether they have been installed or not. **Workaround:** The seven-day cleanup interval will remove the non-relevant patches.

Dissolvable Agent

Table 59: *Known Issues in the Dissolvable Agent*

Bug ID	Description
#7165	To have health data collection work correctly in 64-bit Windows 7, please use the JRE version provided by ClearPass. It can be downloaded from the following URL: https://<CPPM-IP-Address>/agent/html/help.html
#18031	**Symptom:** The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 or 8 installed. **Workaround:** The Java plugin is now deprecated in Chrome 42.x and above. This is an issue with Chrome, not with ClearPass. Use the Firefox, Internet Explorer, or Safari browser instead.
#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.
#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 Internet Explorer on Windows 2008 or Windows XP if the "Do not save encrypted pages to disk" check box is enabled. **Workaround:** Go to **Internet Options > Advanced**. Uncheck (disable) the check box for the "*Do not save encrypted pages to disk*" option.
#24768	**Symptom:** The Native Dissolvable Agent does not work well in Internet Explorer on Windows XP. **Scenario:** The agent works after downloading it and allowing pop-ups, but no remediation results are displayed and, after clicking **Launch ClearPass Application**, a series of messages is displayed in a loop. **Workaround:** Windows XP is an unsupported operating system. Use a later Windows version or the Chrome or Firefox browser instead.
#24792	**Symptom/Scenario:** The Native Dissolvable Agent flow will not work properly on IE if ActiveX Filtering is

Table 59: *Known Issues in the Dissolvable Agent (Continued)*

Bug ID	Description
	enabled on IE settings. **Workaround:** For Native Dissolvable Agent to work properly on Internet Explorer, ActiveX Filter should be disabled.
#24862	**Symptom/Scenario:** The Native Dissolvable Agent uses ActiveX on IE on Windows OS. Based on IE Security Settings, the browser may ask the user to run or allow "ClearPass OnGuard Web Agent Control". **Workaround:** For the Native Dissolvable Agent to work properly on Internet Explorer, the user should allow "ClearPass OnGuard Web Agent Control" ActiveX Control to run.
#27117	**Symptom:** On Mac OS X, the Native Dissolvable Agent might not work properly on Google Chrome or Firefox if Avast Mac Security 2015 Antivirus is installed.
#27756	**Symptom/Scenario:** The Native Dissolvable Agent can not be installed on Mac OS X 10.6. **Workaround:** On Mac OS X 10.6, admin/root permission is required to install the Native Dissolvable Agent. After installation, the admin user should execute the following command: `sudo chmod –R 777 ~/Library/Application\ Support/ClearPassOnGuardWebAgent/`
#27871	**Symptom:** The Java dissolvable agent does not detect AVG 2014. **Scenario:** This occurs on Mac OS 10.10 with the Java dissolvable agent. The native dissolvable agent is able to detect it.
#28398	**Symptom:** The native dissolvable agent does not automatically relaunch the applet. **Scenario:** This can occur on Mac OS or on Ubuntu after upgrading from 6.5.0 to 6.5.1. This is not seen on a clean upgrade; however, in scenarios where there is a machine shut-down and reboot or switch, this might be seen until a proper network connection is restored. **Workaround:** If this occurs, launch manually if auto-launch does not help.
#29127	**Symptom:** The OnGuard Java-based Dissolvable Agent is not supported on the Chrome 42.x or higher browser. **Scenario:** The Java plugin is now deprecated in Chrome. This is an issue with Chrome, not with ClearPass. **Workaround:** Use the Firefox, Internet Explorer, or Safari browser.
#29186	**Symptom/Scenario:** The Native Dissolvable Agent sometimes does not run on Windows Vista, Windows 2008 R2, or Windows 8. **Workaround:** Right-click the OnGuard application to open **Properties**, and then unblock the .exe file.
#29609	**Symptom/Scenario:** The ClearPass OnGuard Native Dissolvable Agent for Mac OS X does not support status checks for the "Software Updates" patch management application.
#37967	Users should be aware that the ClearPass OnGuard Dissolvable Agent flow might not work in the Firefox browser on the following operating systems, because Mozilla no longer supports Firefox on these platforms: Mac OS X 10.6, 10.7, and 10.8.
#40690	Users should be aware that the Java-based OnGuard dissolvable agent is not supported on Firefox 52.x and later on the CentOS, RedHat, SUSE, or Fedora browsers.

Guest

Table 60: *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.
#40714	**Symptom:** In the **Extension > InstanceLog** API, clicking the **Try it out!** button to view the logs causes the system to hang and the error message "Warning: Unresponsive script" is displayed. **Scenario:** This can occur if a value of "all" is configured for the **tail** parameter and the size of the log file is very large (20,000 entries or more). **Workaround:** It is best practice to avoid using "all" as the value for the tail parameter. Instead, limit the output to a manageable size by always specifying a finite, reasonable value less than 10,000. Go to **Guest > Administration > API Services > Start Here > API Explorer > Extension > InstanceLog**, click **InstanceLog**, and then click to expand the **Get** method. In the **tail** field, enter a number less than 10,000.

Insight

Table 61: *Known Issues in Insight*

Bug ID	Description
#12159	**Symptom/Scenario:** Insight reports do not show license changes immediately. The changes might take up to 24 hours, depending on when the changes are made.
#31048	**Symptom/Scenario:** When the Internet Explorer browser is refreshed, icons on the Insight Dashboard are displayed as text. **Workaround:** Navigate to any other page in Insight and then come back to the Dashboard page.
#32276	**Symptom/Scenario:** The secure flag is not set for Insight sessions.
#32316	**Symptom/Scenario:** Users should be aware that posture data in the Insight database from Insight versions earlier than 6.6 cannot be migrated due to database changes.
#32317	**Symptom/Scenario:** Users should be aware that report configurations from Insight versions earlier than 6.6 are not carried forward after migration or upgrade.
#32318	**Symptom/Scenario:** Users should be aware that alerts configurations from Insight versions earlier than 6.6 are not carried forward after migration or upgrade.
#32430	**Symptom:** There is a discrepancy between the data shown in some of the Insight Dashboard's widgets and the data displayed in reports and other widgets. **Scenario:** If the time zone is changed, Insight graphs in hourly widgets might show discrepancies for data from the past 24 hours. For example, the **Authentication Trend** widget might show only six entries while the **Access Tracker** correctly shows seven entries for the same date and the **Auth Overview** report shows the proper data and trend.
#32455	**Symptom/Scenario:** Graphs in the PDF report do not expand over the entire width of the PDF.
#32624	If the report period is more than one month, the PDF report does not show the X,Y data table below the

Table 61: *Known Issues in Insight (Continued)*

Bug ID	Description
	graphs.
#32786	Users should be aware that, in order to generate reports and alerts, one of the Insight nodes must be enabled as the Insight master. This is configured in Policy Manager at **Administration > Server Manager > Server Configuration** on the **System** tab.
#32901	Users should be aware that the RADIUS Accounting ID must be unique in Insight.
#33178 #33183	Users should be aware that, in Insight reports, filter entities such as Auth Service and Auth Source are fetched from tipsDB, and only the latest name in the database will be fetched in the prepopulated field for the selection. This means that if a service name or source name has been changed, only the latest name will be fetched, so reports can only be configured with those latest changes. All previously stored names will be discarded.
#33208	**Symptom/Scenario:** In a setup with a loaded insightDb, Search does not give an autocompletion-based search. **Workaround:** The user must provide a full phrase to search and then select the appropriate category from the drop-down list.
#33227	Users should be aware that, if SFTP is configured in Insight and the SFTP server is a Windows server, the remote directory must be provided with the relative path and not the absolute path. If the SFTP/SCP server is on Linux, however, the absolute path must be provided.
#33243	**Symptom/Scenario:** SCP for reports does not work when configured for an SCP server in Windows; however, SFTP does work for Windows.
#33244	**Symptom/Scenario:** Generated reports displayed in the Calendar widget are not available to view or download if the Insight Master is switched.
#33245	**Symptom:** Reports, alerts and admin settings can only be configured using the Insight master. **Scenario:** In a cluster of nodes with multiple nodes enabled with Insight, the Insight master is the only node allowed to configure reports, alerts, and admin settings. On the Insight slave nodes, only the Dashboard page is available to view.
#33265	Users should be aware that Insight only supports the English language.
#33448	**Symptom/Scenario:** An Insight report might be aborted due to timeout if all the available columns are selected for CSV export when the Insight database has millions of records.
#33582	**Symptom:** Deselecting **Notify by Email** or **Notify by SMS** check box is not saved. **Scenario:** On reports and alerts, if a **Notify by Email** or **Notify by SMS** check box is deselected, saving appears to work but the check boxes are still selected when the report is reopened. **Workaround:** To remove the notification settings, first deselect the check box, and then clear the associated notification text field. Save the report or alert.
#33608	**Symptom/Scenario:** In the Insight Dashboard, hovering the mouse pointer over a MAC address in a widget visibly changes the pointer to a click pointer, but no action occurs if the pointer is clicked.
#33770	**Symptom/Scenario:** Endpoint reports will be empty if they are generated soon after upgrading or migrating from versions lower than 6.6. This report is generated properly only after the corresponding endpoints are authenticated in the 6.6.0 version.
#33771	**Symptom/Scenario:** Insight reports that use custom templates and their corresponding generated reports are not carried forward from versions lower than 6.6.0.
#33776	**Symptom/Scenario:** A delay in the WAN or a slow network might cause problems with the way the

Table 61: *Known Issues in Insight (Continued)*

Bug ID	Description
	Insight page layout is displayed.
#33825	**Symptom/Scenario:** Guest MAC/Device Authentication is not reflected on the **Guest Authentication Trend** graph. **Workaround:** The information is available in the **Authentication Trend Graph**.
#35947	**Symptom:** Disabled reports are enabled after they are edited and saved. **Scenario:** For a disabled report with no repeat configured, editing the report triggers running the report with the updated configuration. For a disabled report with scheduling configured, the report is enabled and a run is scheduled for the report with the updated configuration. Both scenarios result in the report being enabled when it is saved after editing. **Workaround:** None. This is expected behavior, since a report is usually edited in order to use it.
#40480	**Symptom:** In Insight's **Top 20** charts, data for some nodes is not shown. **Scenario:** Users should be aware that, because data is rounded off in the report widgets on Insight's **Dashboard**, some items might not be listed in the **Top 20** charts. For example, if node one has 2.5 K items and node two has 0.004 K items, the data for node two will not be shown because it is rounded off to the second decimal place.

Onboard

Table 62: *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.

Table 62: *Known Issues in Onboard (Continued)*

Bug ID	Description
#23287	**Symptom:** Embedding Admin credentials for onboarding does not work in Windows 8 and above. The system hangs and there is no error message. **Scenario:** When onboarding Windows systems with Windows 8 and above, if operations requiring admin privileges are configured, then the end user doing the onboarding needs to have admin privileges on the system. These operations include installing applications, configuring wired networks, installing certificates in the machine certificate store, and so on. Embedding admin credentials along with the QuickConnect wizard for this purpose does not work for Windows 8 and above. **Workaround:** There is no workaround. This is a Windows system limitation.
#23699	**Symptom:** Mac OS X disconnects before it completes a certificate renewal. **Scenario:** On Mac OS X, automatic certificate renewal through the "Update" option on Apple's interface does not work. This occurs on provisioned (wireless) networks. **Workaround:** This is an issue with OS X limitations, and is not an Onboard issue. Users should be aware that when their certificate is about to expire, they should renew the certificate through Onboard instead of using Apple's automatic certificate renewal.
#25711	iOS always displays SHA-1 for the signing algorithm regardless of the actual algorithm used. This is an issue with iOS, not Onboard.
#36485	**Symptom:** The QuickConnect app crashes during onboarding and displays the error message "Could not check connection to wireless network: Error querying autoconfig info - code: 5023, msg The group or resource is not in the correct state to perform the requested operation." **Scenario:** This has been observed on ClearPass 6.6.2 when trying to onboard Windows 8.1 Surface Pro devices if multiple MAC addresses are associated with a single device. **Workaround:** Search for devices with multiple MAC addresses (for example, 00:00:00:BA:60:3C:31). Delete those devices, and then onboard them again wirelessly. Do not use an external adapter such as an ethernet connector or dongle to onboard multiple devices.

OnConnect Enforcement

Table 63: *Known Issues in OnConnect Enforcement*

Bug ID	Description
#34964	**Symptom:** When a domain user attempts to log in on a wired interface, OnConnect Enforcement places the endpoint in the wrong VLAN. **Scenario:** This happens if a user attempts to log in to a domain account several seconds after the device is connected to a wired OnConnect Enforcement-enabled port. In this scenario, OnConnect Enforcement is triggered prior to login and uses only the MAC address, leaving the username empty. **Workaround:** After the domain user login, unplug the Ethernet cable. Wait for a few seconds and then connect the Ethernet cable again. OnConnect Enforcement will be triggered again and the appropriate connection restored.
#34999	**Symptom:** An empty username is returned for an OnConnect Enforcement request and the alert "WebAuthService Username is empty in the request" is displayed. **Scenario:** This occurs in the following scenarios: • The host is not a Windows device and a Windows Management Instrumentation-based (WMI) logged-in user query fails as expected. • The IP address for the MAC address of a connected endpoint cannot be determined. The IP address is typically updated based on DHCP traffic received by the Device Profiler. In this scenario, possible workarounds are to configure a short session timeout (> 3 minutes) to force a re-authentication, or for the user to manually disconnect and reconnect the endpoint to the network. These will resolve transient errors due to timeouts or due to delays in resolving the MAC-to-IP association. • A WMI-based query to the host fails on a Windows device. This typically occurs if a firewall blocks

Table 63: *Known Issues in OnConnect Enforcement (Continued)*

Bug ID	Description
	access to WMI ports on the device, or if a WMI login to the device fails using credentials configured in Profile Settings.
#36119	**Symptom/Scenario:** After a port configuration is changed, ClearPass does not detect the updated switchport configuration when a new SNMP Trap is received. **Workaround:** To have ClearPass detect the recent port configuration, do one of the following: • Wait for the periodic device polling interval to elapse after the port configuration changes are made. To verify the length of this interval, go to the **Administration > Server Manager > Server Configuration > Service Parameters** tab and select **ClearPass network services**. The interval is displayed in the **Device Info Poll Interval** field. • Alternatively, at **Configuration > Network > Devices > Edit Device Details**, make any minor change and then click **Save** to refresh the Network Access Device (NAD).
#36230	**Symptom/Scenario:** On the **Administration > Server Manager > Server Configuration > System Monitoring** tab, if the default value for the **Engine Id** field is replaced with an empty value, SNMP v3 Informs and Traps do not work.

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 64: *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 Windows XP and Windows 2003 SP2. **Workaround:** Users should click **Continue Anyway** to proceed.
#13363	**Symptom:** On Mac OS X, the current version of the ClearPass OnGuard Unified Agent VPN component does not show some VPN-related information—for example, tunnel IP assigned by the controller, packet count, or diagnostic details. **Scenario:** This occurs on Mac OS X. It does not occur on Windows OS.
#13929	At times, OnGuard may fail to detect peer-to-peer applications, such as /uTorrent, on Windows 2008 R2.
#13935	OnGuard does not support enabling or 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).

Table 64: *Known Issues in OnGuard (Continued)*

Bug ID	Description
#14760	In some cases, OnGuard fails to connect to the ClearPass appliance from a wired interface if the VPN is connected from a trusted network.
#14842	Installing the ClearPass OnGuard Unified Agent removes an existing VIA installation. To continue to use VPN functionality, go to **Administration > Agents and Software Updates > OnGuard Settings** and select **Install and enable Aruba VPN component** from the drop-down list.
#14996	If McAfee VE is running on Windows XP, the ClearPass OnGuard Unified Agent VPN will not work.
#15072	VIA connection profile details are not carried forward after upgrading from VIA 2.0 to ClearPass OnGuard Unified Agent 6.1.1.
#15097	The ClearPass OnGuard Unified Agent does not support installation of a VPN component on Mac OS X 10.6.
#15156	VPN configuration is not retained after upgrading to the ClearPass OnGuard Unified Agent using MSI Installer on a 64-bit Windows system.
#15233	On Win 7 (64 Bit), upgrading an existing VIA 2.1.1.X to the ClearPass OnGuard Unified Agent can lead to an inconsistent state. Users should first uninstall VIA and then proceed with the ClearPass OnGuard Unified Agent installation.
#15351	**Symptom:** The state of the **Real_Time Scanning** button in the Trend Micro Titanium Internet Security for Mac OS X is not updated. **Scenario:** This is observed when the ClearPass Unified OnGuard Agent has Real Time Protection (RTP). **Workaround:** Close the UI using **Command +Q** and restart.
#15586	**Symptom:** The ClearPass OnGuard 6.2 dissolvable agent does not support the following new health classes on Mac OS X: Processes, Patch Management, Peer-To-Peer, Services, USB Devices, and Disk Encryption. The dissolvable agent (DA) does not display these health classes as remediation messages in the user interface because java binary sdk support is not included. **Scenario:** The client will be unhealthy if any of the health classes listed above are configured and performing a health scan via the DA.
#15986	ClearPass OnGuard returns the product name of “Microsoft Forefront Endpoint protection” AntiVirus as “Microsoft Security Essential”.
#16181	**Symptom:** The command level process can be detected using the path “none” but the application level process can't be detected by setting the path to ”none”. **Scenario:** This applies to Mac OS X. **Workaround:** The application-level process health should be configured with the path set to **Applications > Firefox.app**.
#16550	**Symptom/Scenario:** The ClearPass OnGuard Unified Agent does not support checking of disk encryption state using the MacKeeper (ZeoBIT LLC) Disk Encryption Product on Mac OS X. This causes the client to be treated as healthy even if none of the disk is encrypted. **Workaround:** There is no workaround at this time.
#18281	The ClearPass OnGuard configured health quiet period is supported in Health only mode. It doesn’t work in Auth+Health mode.
#18341	**Symptom/Scenario:** OnGuard cannot start a process on Mac OS X for non-administrative users. **Workaround:** The user must have root privileges to start process-level health checks by OnGuard on Mac OS X.

Table 64: *Known Issues in OnGuard (Continued)*

Bug ID	Description
#19019	The network interface will be bounced twice (once immediately, and once after the configured interval) when the log-out/bounce delay parameter is configured. This is expected behavior; the first bounce is required to end the existing session.
#20316	OnGuard's Health Check Quiet Period is applicable per network interface. If a machine has more than one network interface, then each interface will have its own Health Check Quiet Period duration.
#23470	**Symptom/Scenario:** On a Japanese OS, when upgrading from VIA 2.1.1.3 to the ClearPass OnGuard Unified Agent, a known issue with uninstalling VIA displays a message asking the user to select the VIA driver. This does not occur on an English OS.
#23636	**Symptom:** The value of the Posture:Applied Policy attribute is not correctly displayed in the Access Tracker for posture policies carried over from releases earlier than 6.3.0. **Scenario:** This has been observed when upgrading from 6.2.6 to 6.3.2. **Workaround:** This can be corrected by manually saving the affected posture policy once after upgrade.
#24986	**Symptom:** The Native Dissolvable Agent is not automatically launched after downloading and running the agent the first time on the Chrome browser. **Scenario:** This occurs on Windows and on Mac OS X. **Workaround:** The first time you launch the Dissolvable Agent, click **Launch ClearPass OnGuard Agent**.
#25827	**Symptom/Scenario:** On Internet Explorer 8, when the security warning message asks whether you want to view only the content delivered through a secure HTTPS connection, the behavior is not as expected. **Workaround:** For the Native Agent flow to work correctly, click **No** in the pop-up dialog.
#26224	**Symptom/Scenario:** Some combined products that include both antivirus and anti-spyware (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.
#27134	**Symptom:** OnGuard does not support dynamic switching between logged-in users on an Ubuntu client.
#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.
#27876	Users should be aware that RADIUS CoA over VPN is not supported on Ubuntu.
#29243	**Symptom:** The Unified Agent fails to disable other types of network connections when "Allow Only One Network Connection" is selected. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent for Windows does not support disabling USB data card/modem type network interfaces.
#29598	**Symptom:** OnGuard does not stop or pause VM Player 7.x virtual machines. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent does not support auto-remediation for Guest VMs running on VMware Player.
#30106	**Symptom:** On Mac OS X, the native and Java dissolvable agents do not get the RTP status of ESET Cyber Security Antivirus 6.x. **Scenario:** Users should be aware that the ClearPass OnGuard Native Dissolvable Agent for Mac OS X does not support the RTP Status check for ESET Cyber Security and ESET NOD32 Antivirus.
#30243 #30212	**Symptom:** The ClearPass OnGuard Unified Agent fails to load on Windows Server 2003, and does not support VPN, Auto Upgrade, or SSO on Windows XP or Windows Server 2003.

Table 64: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	Scenario: Users should be aware that Microsoft stopped supporting Windows Server 2003 on July 14, 2015, and stopped supporting Windows XP on April 8, 2014. Aruba will not provide further ClearPass support for these operating systems. **Workaround:** Windows 2003 server and XP machines are required to update the Microsoft root CA certificate or missing trust certificates in order to load the OnGuard user interface properly. The following Microsoft knowledge base article provides information, as well as a link to the hotfix download that needs to be installed in order to enable certificate support with the SHA-256 algorithm: https://support.microsoft.com/en-us/kb/968730.
#30381	**Symptom:** The ClearPass OnGuard Unified Agent might not be able to detect the installation of certain Windows updates that are not visible in **Control Panel > Programs and Features > View installed updates**. **Scenario:** These are updates that might not use an installer or cannot be removed. Some examples include the Windows Malicious Software Removal Tool, certain Windows Defender updates (but these are validated through AntiVirus health class), and foreign language input method editor (IME) files. **Workaround:** There is no workaround at this time.
#30618	**Symptom:** The ClearPass user interface may become unavailable after installing ClearPass OnGuard hotfix patches due to a service restart. **Workaround:** Log in to the ClearPass CLI using the appadmin account, and restart cpass-admin-server using the 'service restart cpass-admin-server' command. This will only affect the GUI and not the availability of ClearPass services (for example, RADIUS).
#31734	**Symptom/Scenario:** When both the wired and wireless interfaces are connected, the ClearPass OnGuard Dissolvable Agent sometimes picks the wrong interface to perform health checks.
#31893	**Symptom/Scenario:** Although Windows 10 does not support the Network Access Protection (NAP) platform, Windows 10 is still listed in the **Windows System Health Validator** and **Windows Security Health Validator** plugins for OnGuard at **Configuration > Posture > Posture Policies > Posture Plugins** tab.

#32590	**Symptom/Scenario:** The ClearPass OnGuard Unified Agent stops performing health checks on clients where AVG Anti-Virus Free Edition 2016.x is installed.
	Workaround: Perform the following steps to resolve the issue.
	1. Disable AVG self protection : Open the AVG user interface, go to **Options > Advanced settings > AVG Self Protection**, and deselect the **Enable AVG self protection** check box.
	2. Stop the avgwd service. Type the following commands at the elevated command line :
	`rename "c:\Program Files\AVG\Av\avgwdsvcx.exe" avgwdsvcx.exe.org`
	`taskkill /F /IM avgwdsvcx.exe`
	3. Rename stats db. Type the following commands at the elevated command line :
	`rename c:\ProgramData\Avg\AV\DB\stats.db stats1.db`
	4. Start the avgwdsvc service. Type the following commands at the elevated command line :
	`rename "c:\Program Files\AVG\Av\avgwdsvcx.exe.org" avgwdsvcx.exe`
	`sc start avgwd`

#33332	**Symptom:** The Java Dissolvable Agent guest portal page hangs. **Scenario:** This occurs when the user clicks **Continue** on the **Security Warning** dialog after installing or upgrading to JRE 8u73. This is not an issue with current Java versions. **Workaround:** Upgrade to the latest JRE version.
#33458	**Symptom/Scenario:** If there are more than two auto-connect SSIDs configured, a Windows OS will sometimes keep connecting to these SSIDs after the OnGuard Agent disconnects the wireless interface.
#33532	**Symptom/Scenario:** When the ClearPass OnGuard Agent for Windows is running in **Service** mode, the

Table 64: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	Retry button is sometimes disabled and an incorrect system tray icon is shown. **Workaround:** Quit OnGuard and relaunch it.
#34571	**Symptom/Scenario:** The Java-based Dissolvable Agent sometimes does not show health check results on Windows in the Firefox browser. **Workaround:** Rebooting the system or clearing the browser cache might fix the problem.
#34744	Users should be aware that the Dissolvable Agent flow might not work with the latest Google Chrome versions (49.x and later) on the following operating systems because Google no longer supports Chrome on these platforms: Windows XP, Windows Vista, and Mac OS X 10.6, 10.7, and 10.8.
#34829	**Symptom:** The ClearPass OnGuard Unified Agent's **Retry** and **Login** buttons sometimes become inactive if the network interface is disabled or disconnected. **Scenario:** This occurs on Windows operating systems, and is only seen in Service mode. **Workaround:** Quit and relaunch the OnGuard Agent.
#34987	**Symptom/Scenario:** If the VPN component is enabled on the ClearPass OnGuard Unified Agent, multi-user (switch user) use cases are not supported.
#36208	**Symptom:** Double backslash characters (\\ ) are shown in the Access Tracker for the Path and Command attributes of the Agent Script Enforcement profile, but users should only enter a single backslash character (\ ). **Scenario:** On the **Monitoring > Live Monitoring > Access Tracker > Output** tab for an Agent Script enforcement profile, the **Application Response** area shows double backslash characters instead of single backslash characters in Path and Command attribute values. This is normal display behavior for this form and is not an issue. Users should be aware that, when creating an attribute, only single backslash characters may be entered in attribute values. Although a double backslash is displayed in these attribute values on the **Output** tab, the value sent to OnGuard uses the single backslash.
#36334	**Symptom:** The Native Dissolvable Agent does not launch automatically after it is installed, and if the user clicks “Launch ClearPass OnGuard Agent” it again prompts the user to download the Native Agent. **Scenario:** This issue has been observed mostly on Firefox versions 48.x and 49.x. **Workaround:** In the Firefox menu, click the **Add-ons** link and then select **Plugins** in the left menu. The Native Dissolvable Agent will then launch automatically.
#36354	**Symptom:** The Native Dissolvable Agent does not launch automatically after it is downloaded and run for the first time on the Firefox browser. **Scenario:** This occurs on the Firefox browser for both Windows and Mac OS X. **Workaround:** When the agent is launched for the first time , click “Launch ClearPass OnGuard Agent” to launch it manually.
#36630	**Symptom:** Windows Defender is detected as AntiVirus instead of AntiSpyware on Windows 7. **Scenario:** Users should be aware that, by design, the AntiVirus and AntiSpyware categories in the OnGuard plugin version 1.0 are merged into a single AntiVirus category in plugin version 2.0. Products that were previously identified as AntiSpyware will be identified as AntiVirus when using plugin version 2.0.
#36654	**Symptom:** Web authentication requests fail after migrating a WebAuth service from the OnGuard plugin version 1.0 (V3 SDK) to plugin version 2.0 (V4 SDK). **Scenario:** Users should be aware that, by design, after updating to ClearPass 6.6.7 and to the OnGuard plugin version 2.0, OnGuard agents will continue to use plugin version 1.0 (V3 SDK) by default until an Agent Enforcement Profile configured with **SDK Type = V4** is applied to them.
#36764	**Symptom:** OnGuard fails to set Real-Time Protection for F-Secure Anti-Virus.

Table 64: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	Scenario: This issue is seen on F-Secure AntiVirus for Windows. Users should be aware that the ClearPass OnGuard Unified Agent for Windows does not support enabling Real-Time Protection (RTP) of F-Secure Internet Security 16.3.
#36822	**Symptom:** OnGuard's automatic "pause" and "stop" remediation actions do not work for VMware Workstation 12. **Scenario:** Users should be aware that, when using the OnGuard plugin version 2.0 (V4 SDK), the ClearPass OnGuard Unified Agent does not support automatic "stop" or "pause" remediation actions for VMware Workstation 12 Player version 12.5. **Workaround:** Manually pause or stop the VM instead.
#36837	**Symptom:** OnGuard fails to detect the last scan time for WebRoot SecureAnywhere AntiVirus. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent does not support Last Scan Time checks for Webroot SecureAnywhere AntiVirus 9.x when using the OnGuard plugin version 2.0 (V4 SDK).
#36925	**Symptom:** Malwarebytes Antivirus product RTP checks and system scans fail on the Windows 7 and Windows 8 operating systems. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent does not support EnableRTP, UpdateDefinitions, or Scan methods for Malwarebytes Anti-Malware Premium 2.x.
#37354	**Symptom:** The Java Dissolvable Agent does not work with the Safari browser on macOS 10.12. **Scenario:** When trying to perform health checks using the Java Dissolvable Agent, after the applet opens OnGuard stops and does not perform the health checks. This is due to recent changes in the Safari browser, and is not an issue with ClearPass. **Workaround:** None.
#37393	**Symptom/Scenario:** After the RTP status of AhnLab V3 Endpoint Security AntiVirus is enabled on Korean Windows 7 as part of auto-remediation, the ClearPass OnGuard Unified Agent takes a few seconds to detect the RTP status as Enabled.
#37531	**Symptom:**The ClearPass OnGuard Unified Agent fails to enable the Real-Time Protection (RTP) method of Symantec Endpoint Protection 14.x (SEP14). **Workaround:** In Symantec Endpoint Protection, go to **Change Settings > Client Management > Tamper Protection** and un-mark the **Protect Symantec security software from being tampered with or shut down** check box.
#37539	**Symptom:** The ClearPass OnGuard Unified Agent cannot install missing patches using the Microsoft Windows Update Agent if the patch has an empty value in the **KBARTICLEID** field. **Scenario:** This issue is seen on Windows 10 LSTB 14393 Build 2016.
#37939	**Symptom:** The Native Dissolvable Agent does not work in the Firefox browser. **Scenario:** The Native Dissolvable Agent for Windows does not support the 64-bit version of the Firefox browser. **Workaround:** Use the 32-bit version of Firefox browser instead.
#38141	Users should be aware that the Java-based OnGuard Dissolvable Agent is no longer supported on Windows, MacOS, or Ubuntu systems. Only the Native OnGuard Dissolvable Agent workflow will be used for those platforms in the 6.6.5 release and future releases.
#38208	**Symptom:** After the ClearPass OnGuard Unified Agent is installed it does not automatically display the VIA profile download dialog. **Scenario:** When a non-administrator user is logged in and tries to install the agent, they are prompted to provide administrator credentials. When they do, the agent installs, but the VIA profile download dialog does not open.

Table 64: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	Workaround: To download the VIA profile, go to the **Details** tab. In the **Change Detail Type** drop-down list, select **Connection Details**, and then click the **Download** button. Enter the server details and credentials in the **Login** window.
#38303	**Symptom/Scenario:** The ClearPass OnGuard Unified Agent does not support updating Symantec Endpoint Protection 14.x as part of auto-remediation.
#38403	**Symptom:** The Native Dissolvable Agent does not work in the Firefox browser on macOS. **Scenario:** After installing OnGuard through the Firefox browser, the "Install OnGuard" dialog does not open and the plugin cannot be found. This has been observed in the Firefox browser on Mac OS X 10.10 and macOS 10.12. **Workaround:** Use the Safari or Chrome browser instead.
#38976	**Symptom:** The ClearPass OnGuard Native Dissolvable Agent is not supported on Firefox versions 52.x and later. This is because of recent changes in the Firefox browser itself. **Scenario:** This has been observed on MacOS, Windows, and Linux operating systems. **Workaround:** Use the Google Chrome, Internet Explorer (IE), or Safari browsers instead.
#39148	**Symptom:** Attempting to update from 6.6.4 to 6.6.5 using the **Cluster Update** page fails and displays the error message "certificate common name ... doesn't match requested host name." **Scenario:** If you are upgrading a cluster from 6.6.4 to 6.6.5, the **Cluster Upgrade** page only works if the publisher's certificate includes the publisher's IP Address in the Common Name (CN). This only occurs when updating from 6.6.4 to 6.6.5. It is not an issue when updating from other versions. **Workaround:** If the publisher's certificate does not include the publisher's own IP address, manually update the cluster instead of using the **Cluster Update** page.
#40417	**Symptom:** OnGuard fails to start a full-system scan for McAfee Internet Security 14.x and displays a message asking the user to start the scan manually. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent does not support full-system scan auto-remediation actions for McAfee Internet Security 14.x when using the OnGuard plugin version 2.0 (V4 SDK).
#40445	**Symptom:** OnGuard fails to enable real-time protection (RTP) for Webroot SecureAnywhere AntiVirus on macOS. **Scenario:** Users should be aware that the ClearPass OnGuard Unified Agent does not support enabling real-time protection for Webroot SecureAnywhere AntiVirus 9.x when using the OnGuard plugin version 2.0 (V4 SDK). **Workaround:** Manually enable real-time protection of Webroot SecureAnywhere AntiVirus 9.x.
#40666	**Symptom:** In macOS 10.7, the OnGuard Agent does not perform health checks and displays the error message "Auth Server is not available." **Scenario:** Users should be aware that the OnGuard persistent and native dissolvable agents are not supported on macOS 10.7.
#40784	**Symptom:** In the custom user interface's remediation wizard, the error message "OnGuard Start page is missing" is displayed even though the Start page is configured. **Scenario:** This issue occurs if **Bounce Client** is enabled in the **Agent Enforcement** profile.

Policy Manager

Customers whose networks include addresses in the 172.17.0.0/16 network are advised to either disable the ClearPass Extension service or to contact TAC for assistance in re-allocating the Extensions to use a different network address space. For more information, see #34161.

Table 65: *Known Issues in Policy Manager*

Bug ID	Description
#10881	Entity updates with PostAuth enforcement fail if the publisher is down.
#12316	Syslog Filters and Data Filters configuration will be removed after an upgrade. Policy Manager does not carry forward Syslog Filters and Data Filters configuration. Only default data is migrated.
#13645	Authorization attributes are not cached for the Okta authentication source.
#13999 #13975	In order to add or update a PostAuth profile configuration, the admin must first delete old profiles from ClearPass, and then add the new or updated profiles.
#14186	**Symptom:** Post auth doesn't work properly for UNKNOWN endpoints in a MAC Authentication Bypass (MAB) flow. **Scenario:** This has been observed if the user tries to connect using an endpoint that is unknown to ClearPass.
#14190	**Symptom:** Blacklisted MAC Authentication Bypass (MAB) users cannot be blocked using the Blacklist User Repository. **Workaround:** In order for post auth to work in a MAB flow, a new blacklist repository must be added with a custom filter.
#17232	**Symptom/Scenario:** The error and warning messages returned by the user interface are displayed in English instead of the localized language.
#18064	**Symptom:** AirWatch custom HTTP actions needs content even though it's not required. **Scenario:** For AirWatch MDM, custom-defined HTTP actions such as Lock Device or Clear Passcode fail with error messages. This is due to a bug in AirWatch. **Workaround:** Do either of the following: • Add a header **Content-Length:0** in the **Context Server Action**. • Add a dummy JSON data {"a":"b"}.
#18701	**Symptom/Scenario:** Performing an AddNote operation using AirWatch as the MDM connector fails in ClearPass. This is due to a bug in AirWatch.
#19176	ClearPass does not currently support posting of Palo Alto Networks (PANW) user ID information when the PAN OS uses Vsys.
#19826	Palo Alto Networks (PANW) devices will only accept the backslash character (\ ) as a separator between the domain name and the username.
#20292	**Symptom/Scenario:** On the **Monitoring > Live Monitoring > System Monitor** page, the **Last updated at** field displays time based on the time zone of the ClearPass node where the user is viewing the page.
#20383	The system posture status may still be maintained after Post Auth agent disconnect action. This is likely to happen when Posture result cache timeout service parameter is higher than the Lazy handler polling frequency.
#20416	**Symptom:** The Palo Alto Networks (PANW) operating system firewall rejects user ID updates from ClearPass when the user ID limit is reached on the firewall. When this happens, user ID updates are rejected with errors. **Scenario:** This occurs when the PANW firewall exceeds its supported limit advertised for user ID registration. **Workaround:** There is no workaround at this time.
#20453	In order for ClearPass to have complete data to post to Palo Alto Networks devices in HIP reports, profiling must be turned on. This is the expected behavior.

Table 65: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#20455	**Symptom/Scenario:** When doing an SSO & ASO flow in Safari browsers, the certificate needs to be added in the trust list of the browser. **Workaround:** Please follow these steps: 1. Open the Safari browser and enter the SP URL. 2. After you enter the SSO application in the browser, the Show Certificate option is provided in a popup window. 3. Click **Show Certificate** and select the **"Always trust 'FQDN of SP machine' when connecting to IPaddress"** check box, and then click the **Continue** button.
#20456	**Symptom:** SNMP bounce fails. **Scenario:** When only the SNMP bounce in the SNMP Enforcement profile of a Web auth service is configured, SNMP bounce functionality does not work. **Workaround:** Also configure a VLAN ID along with the SNMP bounce in the SNMP enforcement profile.
#20484	**Symptom:** Dropping the Subscriber and then adding it back to the cluster may fail at times. **Scenario:** ClearPass system time might not have been synchronized with an NTP source. **Workaround:** Configure an NTP server. ClearPass will synchronize its time with the NTP source. Attempt the cluster operation.
#20489	**Symptom/Scenario:** ClearPass 6.3 does not allow a server certificate with a Key Length of 512 bits as seen in the Self-Signed Certificate and Certificate Signing Request UIs. Earlier ClearPass versions did not have this restriction, hence their server certificate may use one with a 512 bit Public Key. After upgrade, these servers will not work properly. **Workaround:** The admin must manually fix the server certificate to allow a minimum of 1024 bits long Public Key prior to upgrade.
#21334	**Symptom:** ClearPass does not launch. **Scenario:** The ClearPass user interface will not launch from Firefox or from older versions of Internet Explorer (IE) browsers if an EC-based HTTPS server certificate is used. On Firefox, the error message "Secure Connection Failed. An error occurred during a connection to <*server*>. Certificate type not approved for application" is displayed. On older versions of IE, the error message "Internet Explorer cannot display the Web page" is displayed. **Workaround:** Use the latest version of IE, or the Chrome browser instead.
#22023	**Symptom/Scenario:** Launching the customer's ClearPass user interface through a proxy does not 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 SHA-1-based algorithm to replace the MD2 algorithm from the corresponding Certificate Authority site. 5. From the Support shell, restart the cpass-postgresql service.
#23848	**Symptom:** The ClearPass appliance'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.

Table 65: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	Workaround: There is no workaround at this time.
#24584	**Symptom:** The Event Viewer sometimes shows two SMS entries. **Scenario:** This might occur when "Alert Notification - SMS Address" is saved, or if sending an SMS fails.
#24646 #24919 #26698 #27379 #27568	**Symptom/Scenario:** There are some issues on Internet Explorer 9 (IE 9), including: • The login banner is not centered and the footer is not placed at the bottom of the page. • The IE browser fails to display an error message if connectivity is lost with the ClearPass Policy Manager server. • The scroll function does not work in the pop-up that opens from the **Monitoring > Audit Viewer** page. • ClearPass Policy Manager and Insight do not work properly on IE 9. • The **Save** operation gets stuck when you try to save the server configuration changes using the IE browser. **Workaround:** Use IE 10 or IE 11 or the Firefox or Chrome browsers instead. Users should be aware that ClearPass supports IE 10 and later on Windows 7 and Windows 8.x.
#24781	Palo Alto Networks (PANW) devices accept only the backslash (\ ) character as a separator between the domain name and the username. If the update uses an "at" sign (@) between the domain name and the username, the HIP report will not be shown in PANW.
#25720	**Symptom/Scenario:** The Dashboard shows the server as being down if an HTTPS server certificate is signed by the Onboard CA using SHA-256. **Workaround:** Be aware that SHA-1 RSA is not recommended for security reasons. You must update your certificates to use stronger keys, such as RSA with > 1024 bits length.
#27306	Whenever IPsec configuration is changed on either end of the tunnel (Wireless Controller or ClearPass), after the changes, the ClearPass IPsec service should be restarted in ClearPass from Services Control to establish the IPsec tunnels reliably. After restart, verify the status of the IPsec tunnel from the **Network** tab at **Administration > Server Manager > Server Configuration**.
#27592	**Symptom:** SAML SSO using TLS certificate does not work in Firefox or Safari browser. **Workaround:** Use alternate browsers such as Google Chrome or IE.
#27621	**Symptom:** The number of authentications per second for non-MS-CHAPv2 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.
#27895	Users should be aware that, because of schema changes now that ClearPass supports storing irreversible passwords, any import of old authentication sources using XML files will break the required SQL filters. Avoid any import of old authentication source configuration as this causes authentication failures for guest users and admin users.
#28417	**Symptom:** After DNS settings are changed, services that are dependent on DNS are not restarted and the ClearPass application hangs. **Scenario:** When the DNS is updated, all services are restarted, so the session is lost. **Workaround:** Refresh the ClearPass application and log in again.
#30486	**Symptom:** Custom filters in an Auth Source do not work after upgrading to ClearPass 6.6. **Scenario:** As part of enhancements to tag mappings, the schema for storing the tag values has changed, and all default filters were migrated to the new schema. It is not possible, however, to

Table 65: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	automate the migration of custom filters. **Workaround:** If you have custom filters, contact Support to have the custom filters migrated to the new schema.
#30569	**Symptom/Scenario:** The Guest Portal name in the ClearPass portal is unchanged after updating the name in the ClearPass Guest application. **Workaround:** When you change Guest Portal names in the ClearPass Guest application, the admin must manually update the ClearPass Portal settings if the guest portal is used in that configuration.
#30968	Users should be aware that VMware ESX hosts are not profiled by SNMP CDP based profiling. The Profiler needs a host MAC or IP address in order to identify the device. ESX servers might not report the management IP address and MAC address in the CDP announcements, causing the Profiler to ignore neighbor CDP information for the host.
#31208	**Symptom:** Multiple entries for the same device can be seen in the endpoints page. **Scenario:** Users should be aware that, during the network discovery scan, if devices have multiple endpoints those endpoints will be listed separately in the endpoints page.
#31769	**Symptom/Scenario:** Endpoints with multiple IP addresses for the same MAC address might not be profiled appropriately.
#31810 #30785	Users should be aware that, when upgrading to ClearPass 6.6, any custom authentication source filters must be migrated manually. During an upgrade, the console now displays a warning message when custom filters are defined using tag values for Local and SQL authentication sources.
#31916	**Symptom:** Network discovery adds multiple ports to the display after discovering the same device. **Scenario:** During network discovery, if the same device is connected to two different ports of a switch, the one discovered later will be displayed in the neighbors.
#31942	**Symptom:** Restore operations fail and the error message “Network Device <#>: No dictionary found for vendor ‘HP’” is displayed at **Configuration > Network > Devices > Import**. **Scenario:** This occurs when a network device is imported with the vendorName as “HP”. **Workaround:** Network devices that had the vendorName "HP" must now use the vendorName "Hewlett-Packard-Enterprise".
#32145	**Symptom:** Devices are discovered with incorrect MAC addresses. **Scenario:** Network discovery reads the ARP cache (ipNetToMediaTable) to process all the MAC-IP cache pairs and add them to the endpoints. The Aruba switch returns the same MAC address for all the IPs, resulting in only one endpoint.
#32980	Users should be aware that, on devices using PAP, notifications sent by ClearPass about a required password change or advising of an upcoming password expiration might not work. Although TACACS `authen_type=ASCII` implementations handle these correctly, devices that use `authen_type=PAP` might only accept a status of `SUCCESS/FAILURE` and not accept any other status.
#33103	**Symptom:** After restoring a backup, the SSO page IDP URL still shows the old hostname of the restored backup instead of the hostname/FQDN if the current ClearPass appliance. **Scenario:** This error is only seen when a backup is attempted from one appliance to another appliance. This is very rare in real time. **Workaround:** Manually change the hostname in the IDP URL to the current ClearPass appliance's hostname\FQDN.
#33371	**Symptom/Scenario:** Network Discovery through SNMP v1 does not work for Aruba switches. **Workaround:** Use SNMPv2 or v3 for discovering Aruba switches.
#33425	If you have a custom authentication source configured to use the session log database, additional

Table 65: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	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 123). Please contact Customer Support for configuration recommendations to move away from using the session log database as an authentication source.
#33535	**Symptom:** Importing patches might fail with the error "Content-type 'application/x-macbase64' is not supported". **Scenario:** This occurs on some versions of the Firefox browser. **Workaround:** Use the Chrome or Internet Explorer browser instead.
#33795	**Symptom/Scenario:** Importing a pre-existing authentication source with custom filter queries is not reflected or updated if the existing authentication source in 6.6.0 already includes some filters with same name.
#33811	**Symptom:** During an upgrade through the user interface, the **Reboot** button might not trigger a machine restart after the image is installed. **Scenario:** This occurs when the upgrade image is downloaded from the Web server or installed through the user interface. If the default or configured idle session timeout of the server is exceeded, the system should display the error message "Session is timed out. Please log in again" when the **Install** or the **Reboot** button is clicked, but it does not. Instead, the installation completes and the "Reboot initiated" message is displayed, but the reboot is not actually triggered. **Workaround:** Refresh the page to log in again, and then click **Reboot**.
#34086	**Symptom:** If a system is upgraded from ClearPass 6.5.5 or below with a configuration that is affected by issue #33036, the configuration will not be auto-corrected during the upgrade. **Scenario:** This can occur if an authentication source with type RADIUS server is used in a service created through a service template in 6.5.5 or below.
#34161	**Symptom:** After upgrading from 6.5.x to 6.6.0, the error message "Unknown error: no route to host" is displayed on the **Administration > Agents and Software Updates > Software Updates** page. **Scenario:** This may occur for customers whose networks include addresses in the 172.17.0.0/16 range. **Workaround:** Customers with networks that include addresses in the 172.17.0.0/16 network are advised to either disable the Extension service, or to contact TAC for assistance in re-allocating the Extensions to use a different network address space.
#34491	**Symptom:** A ClearPass Admin UI login will fail against the local user repository if the "force change password " option is enabled. **Scenario:** Users should be aware that the Local User setting to force a password change at the user's next login applies only to network device administration logins using TACACS+.
#34951	**Symptom/Scenario:** The new cluster-wide parameter **Disable Change Password for TACACS** has no effect on TACACS authentications using PAP. Users should be aware that password change is not supported with the TACACS authentication method.
#35030	**Symptom/Scenario:** If blacklisted users are deleted as a result of daily cleanup, or as a result of manual cleanup through the UI, then when those users come back after the defined blacklist period is over they might be disconnected immediately instead of being allowed a fresh bandwidth or session limit. **Workaround:** The user will have to wait for another cycle of the blacklist period to pass before the allowed bandwidth limit or session limit will be applied.
#35158	**Symptom:** Deleting a Certificate Revocation List (CRL) has no effect on the IPsec connection. **Scenario:** Users should be aware that if a CRL in **Administration > Certificates > Revocation Lists** is deleted, the administrator must restart the **ClearPass IPsec service** on the **Administration >**

Table 65: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	Server Manager > Server Configuration > Services Control tab.
#35167 #35735	**Symptom:** On HPE-25K and HPE-5K servers, the total memory shown is slightly higher than the total memory specifications for the VA type. This is consistent in the Dashboard, the CLI, and in Insight. **Scenario:** The HPE-5K and HPE-25K servers slightly overestimate the "pages" used to calculate the total RAM. In testing with a single 8 GB RAM module, it was found that every module overestimated a little bit. **Workaround:** The "dmidecode" command will give the correct number of modules and total RAM installed, and can be used to calculate the RAM; however, this command does not work for some virtual appliances. Be aware that other commands such as "free -m" significantly underestimate the RAM size.
#35946	**Symptom/Scenario:** Trying to import an agent enforcement profile or Web authentication service from 6.5.7 or 6.6.1 to 6.6.2 fails and the error message "File contains invalid XML tags. Try export to see the valid XML tags" is displayed. **Workaround:** There are two possible workarounds: • An Admin user can re-configure the Web authentication service or or agent enforcement profile. • Alternatively, before importing, make the following changes in the enforcement profile XML file: ▪ Replace **<GenericEnfProfiles> </GenericEnfProfiles>** with **<AgentEnfProfiles> </AgentEnfProfiles>**. ▪ Replace **<GenericEnfProfile> </GenericEnfProfile>** with **<AgentEnfProfile> </AgentEnfProfile>**. ▪ The **type="Agent"** attribute must be mapped to **agentEnfType="Agent"**. ▪ The **action="<VALUE>"** attribute should be removed from the XML. The **action** attribute is not applicable in 6.6.2. (for example, action="Accept")
#35965	**Symptom:** SNMPv3 Traps are not sent with the correct user credentials unless the async-netd service is restarted. **Scenario:** In ClearPass, this occurs if the EngineID or the v3 trap receiver configuration is changed and the cpass-async-netd service is not restarted. **Workaround:** After modifications are made in either of the following ways, restart the async-netd service once in order to reflect the changes: • When the **Engine ID** field is modified on the **Administration > Server Manager > Server Configuration > System Monitoring** tab. • When changes are made to any of the fields associated with an existing SNMPv3 user at **Administration > External Servers > SNMP Trap Receivers**. These SNMPv3 Trap Receiver fields include the authentication protocol using MD5 or or SHA, and the **Type**, **Authentication Key**, **Privacy Key**, and **Privacy Protocol** fields.
#36032	**Symptom:** License activation over the proxy server fails. **Workaround:** Do one of the following: • Use offline license activation instead. On the **Administration > Server Manager > Licensing > Servers** tab, click the **Activate** link in the server's row to open the **Activate License** form. Follow the instructions in the **Offline Activation** area to download a request token and contact Support. • If you can reach the activation server, remove the proxy. On the **Administration > Server Manager > Server Configuration > Service Parameters** tab, select **ClearPass system services**. In the **HTTP Proxy** area, clear all values.
#36902	**Symptom:** A ClearPass virtual appliance cannot be installed with a default disk type of "virt-manager". **Scenario:** When installing a ClearPass virtual appliance on a KVM hypervisor through the virt-manager user interface, the provided image file cannot be read and the installation fails if the bus type is left as the default option. **Workaround:** If you are using the virt-manager user interface to install the virtual machine on a KVM hypervisor, follow the steps below. For installation details, please refer to the *Installing or Upgrading to ClearPass 6.6 on a Virtual Appliance Tech Note*. 1. In the virt-manager user interface, import the raw image and add the hard disk as usual.

Table 65: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	2. In the "Power On and Configure the KVM Appliance" part of the installation process, click **Disk 1** in the left menu. The **Virtual Disk** window opens. 3. Click **Advanced Options**. 4. Change the **Disk bus** setting to **SCSI**, and then click **Apply** to save.
#38978	**Symptom:** Trying to deploy a ClearPass 6.6.0 VMware image in a vSphere 6.5+ server through the vCenter Web client fails, and the error message "Issues detected with selected template. Details: -109:5:VALUE_ILLEGAL: Duplicate key 'cpuHotAddEnabled'" is displayed. **Scenario:** This is caused by a duplicate line in the OVF file. This issue only occurs when trying to upload the ClearPass OVF through the vSphere 6.5+ user interface. **Workaround:** To correctly deploy the ClearPass VMware image in a vSphere 6.5+ environment, do one of the following: • Use an earlier version of the vSphere client instead. • Remove the duplicate line in the OVF file, as follows: 1. Open the **CPPM-VM-x86_64-6.6.0.81015-ESX-CP-VA.ovf** file in Notepad or a similar text editor. 2. Search for the following line: **<vmw:Config ovf:required="false" vmw:key="cpuHotAddEnabled" vmw:value="false"/>** 3. Look at the lines above and below that line. You will see the same line twice, a few rows apart. 4. Remove the first occurrence of the line, and then save the file. 5. Deploy the ClearPass image.
#39723	Users should be aware that ClearPass does not support importing an HTTPS Server Certificate chain or RADIUS Server Certificate chain in p7b Base64 format.
#40302	**Symptom/Scenario:** The ClearPass logo image sometimes does not display correctly in the Internet Explorer 11 browser. **Workaround:** Use a different version of the IE browser, or use the Chrome, Firefox, or Safari browser instead.
#41500	**Symptom:** After applying the ClearPass 6.6.7 hotfix patch for SMBv2 and SMBv3 support for PEAPv0/EAP-MSCHAPv2 and Microsoft Active Directory Domain services, users are not able to log in and the domain controller does not respond. **Scenario:** SMBv2 sometimes uses high-numbered ports (TCP 49152 - 65534) that are blocked by most firewalls. This issue is due to changes in Microsoft's dynamic port range; it is not a ClearPass issue. Users should be aware that for Windows Server 2008 and later, the dynamic port range for connections has been increased. The new default start port is 49152 and the new default end port is 65535 for these versions. More information is available on Microsoft's site at the following links: • Service overview and network port requirements for Windows • Active Directory and Active Directory Domain Services Port Requirements **Workaround:** If you are using SMBv2 or SMBv3, you must increase the remote procedure call (RPC) port range in your firewalls: • If your Active Directory deployment uses only Windows Server 2008 or later, you must enable connectivity over the high port range of 49152 through 65535. • If you have a mixed-domain environment that not only includes any of the above versions but also includes Windows Server versions earlier than Windows Server 2008, you must allow traffic over both the low port range of 1025 through 5000 and over the high port range of 49152 through 65535. • If your Active Directory deployment uses only versions of Windows Server earlier than Windows Server 2008, you must enable connectivity over the low port range of 1025 through 5000.

Profiler and Network Discovery

Table 66: *Known Issues in Profiler and Network Discovery*

Bug ID	Description
#34952	**Symptom/Scenario:** At **Configuration > Network > Devices**, port configuration for OnConnect Enforcement might be confusing if the device is configured as a subnet. **Workaround:** If a network device is configured as a subnet and OnConnect is enabled, we recommend that OnConnect Enforcement be enabled on all ports (uplink and trunk ports will be skipped).

QuickConnect

Table 67: *Known Issues in QuickConnect*

Bug ID	Description
#20867	**Symptom/Scenario:** Android 4.3 and above fails to install a self-signed certificate for the CA certificate. **Workaround:** For onboarding Android version 4.3 and above, ClearPass must have a RADIUS server certificate issued by a proper Certificate Authority and not a self-signed certificate. This is a requirement of Android's API for Wi-Fi management. In **Onboard > Configuration > Network Settings**, the CA certificate that issued the server's certificate has to be selected as the trusted root certificate to be installed on Android.
#25521	**Symptom/Scenario:** Embedding admin credentials is not supported on Windows 8+. **Workaround:** Provide the admin credentials manually during Onboard provisioning.

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

This chapter provides the following information:

The IP address to access the licensing server clearpass.arubanetworks.com is 104.36.248.89. If you have any firewall rules allowing access, please be sure to allow access for this IP address.

End of Support

This section describes ClearPass and third-party systems, software, and features that are no longer supported or that are approaching their end-of-support date.

ClearPass 6.6 Milestones

- Release Date: April 6th 2016
- End of Development: April 6th 2018
- End of Support: April 6th 2019

For more details on the Aruba End of Life policy, please refer to http://www.arubanetworks.com/support-services/end-of-life/end-of-life-policy/.

ClearPass 6.6 Deprecated Features

The following features are no longer supported in ClearPass 6.6:

- VMware ESX 4.0.
- OnGuard External Posture Servers: The **Configuration > Posture > Posture Servers** page and the **Administration > Dictionaries > Posture** page have been removed.

ClearPass 6.6 Deprecation Notice

The following features will not be supported after ClearPass 6.6:

- ClearPass 6.6 is the last release that will support Java for the Windows or Mac OS X ClearPass OnGuard Dissolvable Agent. ClearPass 6.6.5 (cumulative patch 5) will contain the last updates to the Java-based Dissolvable Agent. No further updates will be provided.
- ClearPass 6.6 significantly builds on the unified REST API framework introduced in ClearPass 6.5. All future R&D will focus on this framework. Accordingly, this is the last release that will support the TipsAPI (XML), Guest SOAP APIs, and Guest XML-RPC APIs listed below. ClearPass 6.6 now includes a variety of RESTful

APIs to replace these legacy APIs, and we will build on these to enable a wider variety of use cases. Customers are encouraged to migrate any planned or existing applications to interface with the new API framework. We will not provide any further bug fixes or feature enhancements related to supporting the following legacy APIs, and future versions of ClearPass may remove these APIs completely, so we recommend that you migrate to the appropriate RESTful API as soon as possible:

- **GuestUser TipsAPI** is replaced by **GuestManager** RESTful APIs
- **OnboardDevice** TipsAPI is replaced by **Onboard** RESTful API
- **Guest SOAP** APIs are replaced by the **GuestManager**, **Onboard**, **OperatorLogins**, and **SmsServices** RESTful APIs
- **Guest XML-RPC** APIs are replaced by the **GuestManager**, **Onboard**, **OperatorLogins**, and **SmsServices** RESTful APIs

For more details on the RESTful interface, please go to **https://<ClearPass-Server-IP-or-FQDN>/api-docs** (requires login) on any ClearPass appliance.

- ClearPass 6.6 is the last major release that will support the following products, as they are no longer supported by their vendors:
  - VMware ESX 5.1 and earlier.
  - Mac OS X 10.7 (Lion) — October 2014
  - Mac OS X 10.8 (Mountain Lion) — September 2015
  - Mac OS X 10.9 (Mavericks) — September 2016

Customers who use ClearPass OnGuard must upgrade to the OnGuard Plugin version 2.0 (V4 SDK) by the end of April 2018 in order to maintain application signature and virus definition updates. The V3 SDK will no longer be supported by OPSWAT after this date. Since virus definitions are updated at least once a day, and sometimes several times a day, it is important to maintain regular automatic updates.

Third-Party Vendor Operating System End-of-Support

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

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

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

- Microsoft Corporation:
  - Windows Server 2003 — July 14, 2015
  - Windows XP — April 8, 2014
- Apple, Inc:
  - Mac OS X 10.6 (Snow Leopard) — February 26, 2014

Virtual Appliance Requirements

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

Virtual appliance requirements are 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 a ClearPass hardware appliance.

This section includes the following:

For complete information on installing, configuring, or morphing an ESXi™, Hyper-V®, or KVM hypervisor, see the *Tech Note: Installing or Upgrading to 6.6 on a Virtual Appliance*.

Supported Hypervisors

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

- VMware vSphere Hypervisor (ESXi) 5.5. 6.0, or 6.5
- Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016, Windows Server 2012 R2 with Hyper-V, or Windows Server 2016 with Hyper-V
- KVM on CentOS 6.6, 6.7, or 6.8.

VMware vSphere Hypervisor (ESXi) Requirements

CP-SW-EVAL (Evaluation OVF)

- 2 reserved virtual CPUs
- 4 GB RAM
- 80 GB disk space

CP-VA-500 (500 Virtual Appliance OVF)

- 8 reserved virtual CPUs
  - Underlying CPU is recommended to have a PassMark® of 3000 or higher
- 8 GB RAM
- 1000 GB disk space required
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

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

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

- 8 GB RAM
- 1000 GB disk space required
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

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

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

Hyper-V Requirements

CP-SW-EVAL (Evaluation VHDX)

- 2 reserved virtual CPUs
- 4 GB RAM
- 80 GB disk space

CP-VA-500 (500 Virtual Appliance VHDX)

- 8 reserved virtual CPUs
  - Underlying CPU is recommended to have a PassMark® of 3000 or higher
- 8 GB RAM
- 1000 GB disk space required
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

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

- 8 reserved virtual CPUs
  - Underlying CPU is recommended to have a PassMark® of 9600 or higher
- 8 GB RAM
- 1000 GB disk space required
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

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

- 24 reserved virtual CPUs
  - Underlying CPUs are recommended to have a PassMark® of 9900 or higher
- 64 GB RAM
- 1800 GB disk space required

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

KVM Requirements

CP-SW-EVAL (Evaluation RAW Disk Image)

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

CP-VA-500 (500 Virtual Appliance RAW Disk Image)

- 8 reserved virtual CPUs
  - Underlying CPU is recommended to have a PassMark® of 3000 or higher
- 8 GB RAM
- 1000 GB disk space required
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75

CP-VA-5K (5K Virtual Appliance RAW Disk Image)

- 8 reserved virtual CPUs
  - Underlying is recommended to have a PassMark® of 9600 or higher
- 8 GB RAM
- 1000 GB disk space required
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

CP-VA-25K (25K Virtual Appliance RAW Disk Image)

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

Supported Browsers

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

- Mozilla Firefox on Windows Vista, Windows 7, Windows 8.x, Windows 10, and Mac OS X.
- Google Chrome for Mac OS X and Windows.

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

Users should be aware that the ClearPass OnGuard Dissolvable Agent flow might not work on the Mac OS X 10.6, 10.7, or 10.8 operating systems because Mozilla no longer supports Firefox on these platforms.

The Google Chrome browser no longer supports the Windows XP, Windows Vista, or Mac OS X 10.6, 10.7, or 10.8 operating systems. Chrome will still work on these platforms but will not receive updates or security fixes after April 2016.

ClearPass OnGuard Unified Agent Requirements

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

- 1 GB RAM recommended, 512 MB RAM minimum
- 300 MB Disk Space
- Mac OS X 10.7 - 10.11, MacOS 10.12
- Ubuntu: 12.04 LTS and 14.04 LTS

Windows Vista, Windows 7, Windows 8.x Pro, Windows 10, Windows Server 2008, and Windows Server 2012 are all supported with no service pack requirements. OnGuard does not support Windows 8.x RT or Windows 8.x Phone.

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

Customers who use ClearPass OnGuard must upgrade to the OnGuard Plugin version 2.0 (V4 SDK) by the end of April 2018 in order to maintain application signature and virus definition updates. The V3 SDK will no longer be supported by OPSWAT after this date. Since virus definitions are updated at least once a day, and sometimes several times a day, it is important to maintain regular automatic updates.

OnGuard Supported Third-Party Products

For OnGuard to work properly, please whitelist the following executable files and installation folders in your antivirus products:

ClearPassAgent64BitProxy.exe
ClearPassAgentController.exe
ClearPassAgentHelper.exe
ClearPassOnGuard.exe
ClearPassOnGuardAgentService.exe

ClearPassUSHARemediate.exe
C:\Program Files (x86)\Aruba Networks\ClearPassOnGuard
C:\Program Files\Aruba Networks\ClearPassOnGuard

In current laboratory tests for ClearPass 6.6.8, we use the following third-party software for our validations. Due to the large number of products available, this list may change at any time:

Table 68: *Third-Party Software Summary*

Product Type	Product Name
Antivirus	Avast Pro Antivirus (Windows)
	Avira Mac Security (MacOS)
	ESET Cyber Security Pro (MacOS)
	F-Secure Anti-Virus for Mac (MacOS)
	Kaspersky Internet Security (MacOS)
	Kaspersky Total Security (Windows)
	McAfee Endpoint Security Threat Prevention (Windows)
	Sophos Anti-Virus (Windows)
	Symantec Endpoint Protection (Windows)
	Windows Defender (Windows)
Antispyware	McAfee Host Intrusion Prevention (Windows)
	McAfee VirusScan Enterprise (Windows)
Firewall	Mac OS X Built-In Firewall (MacOS)
	McAfee Endpoint Protection for Mac (MacOS)
	Microsoft Windows Firewall (Windows)
Disk Encryption	BitLocker Drive Encryption (Windows)
	FileVault (MacOS)
Patch Management	McAfee ePolicy Orchestrator Agent (Windows)
	Microsoft Windows Update Agent (Windows)
	Software Update (MacOS)
	System Center Configuration Manager (SCCM) (Windows)
Virtual Machine	Oracle VM VirtualBox (Windows)
	VirtualBox (MacOS)
	VMware Fusion (MacOS)

Some third-party anti-malware products are not supported by ClearPass OnGuard. For complete lists of third-party products supported by OnGuard, go to **Policy Manager > Administration > Support > Documentation**. For products supported by the OESIS V4 SDK, click the **OnGuard Agent Support Charts for Plugin Version 2.0** link. For products supported by the OESIS V3 SDK, click the **OnGuard Agent Support Charts for Plugin Version 1.0** link. Next, click the link for the appropriate product type and operating system.

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.

Users should be aware that the Dissolvable Agent flow might not work on the macOS X 10.6, 10.7, or 10.8 operating systems because Mozilla no longer supports Firefox on these platforms. (#37967)

The Google Chrome browser stopped supporting updates on the Windows XP, Windows Vista, and macOS X 10.6, 10.7, or 10.8 operating systems. Chrome will still work on these platforms but will not receive updates or security fixes after April 2016. The ClearPass OnGuard Dissolvable Agent on these platforms using Chrome is only supported through Chrome version 48.x. (#34744)

This section includes the following:

OnGuard Native Dissolvable Agent Version Information

In current laboratory tests for ClearPass 6.6.8, the browser versions shown in Table 69 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 issue ID number next to the browser's name.

The Native Dissolvable Agent is not currently supported with the Firefox browser. (#38976)

Table 69: *Native Dissolvable Agent Latest Supported Browser Versions for This Release*

Operating System	Browser
macOS 10.12	Safari 10.x
	Chrome 60.x (#24518, #24986)
Mac OS X 10.11	Safari 9.x
	Chrome 60.x (#24518, #24986)
Mac OS X 10.10	Safari 9.x
	Chrome 59.x (#24518, #24986)

Table 69: *Native Dissolvable Agent Latest Supported Browser Versions for This Release (Continued)*

Operating System	Browser
Mac OS X 10.9	Safari 9.x
	Chrome 59.x (#24518, #24986)
Mac OS X 10.8	Safari 5.x (#28398)
	Chrome 49.x (#24986)
Windows 10 64-bit	Chrome 59.x (#24518, #24986)
	Internet Explorer 11.x
	Microsoft Edge 38.x
Windows 10 32-bit	Chrome 59.x (#24518, #24986)
	Internet Explorer 11.x (#25827)
	Microsoft Edge 38.x
Windows 8.1 64-bit	Chrome 59.x (#24986)
	Internet Explorer 11.x
Windows 8.1 32-bit	Chrome 59.x (#24986)
	Internet Explorer 11.x
Windows 8 64-bit	Chrome 59.x (#24986)
	Internet Explorer 10.x
Windows 8 32-bit	Chrome 59.x (#24986)
	Internet Explorer 10.x
Windows 7 64-bit	Chrome 59.x (#24518, #24986)
	Internet Explorer 11.x (#25827)
Windows 7 32-bit	Chrome 59.x (#24518, #24986)
	Internet Explorer 11.x
Windows 2008 64-bit	Chrome 59.x (#24986)
	Internet Explorer 8.x (#24766)
Windows Server 2012 R2 64-bit	Chrome 59.x (#24986)
	Internet Explorer 11.x
Windows Server 2012 64-bit	Chrome 59.x (#24986)

Table 69: *Native Dissolvable Agent Latest Supported Browser Versions for This Release (Continued)*

Operating System	Browser
	Internet Explorer 10.x
Windows Vista	Chrome 49.x (#24986)
	Internet Explorer 9.x (#29186)

OnGuard Java-Based Agent Version Information

In current laboratory tests for ClearPass 6.6.8, the browser and Java versions shown in Table 70 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 issue ID number next to the browser's name.

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

The Java-based OnGuard dissolvable agent is no longer supported on Windows, Mac OS, or Ubuntu systems. Only the Native OnGuard Dissolvable Agent workflow will be used for those platforms in this and future releases. (#38141)

The Java-based OnGuard dissolvable agent is not supported on Firefox 52.x and later on the CentOS, RedHat, SUSE, or Fedora browsers. (#40690)

Table 70: *Supported Browser and Java Versions for This Release*

Operating System	Browser	Java Version
Linux - RedHat	Firefox 17.0.10	JRE 1.8 Update 131
Linux - SUSE	Firefox 31.1.0	JRE 1.8 Update 131

ClearPass Onboard Requirements

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

This chapter provides instructions for upgrading or updating your ClearPass appliance:.

- The term “upgrade” refers to moving from one major release version to another—for example, from 6.5.x to 6.6.0.
  - To upgrade a cluster to 6.6.0, we recommend using the **Cluster Upgrade** interface. For more information, see the Cluster Upgrade and Cluster Update Tools section in the *ClearPass Policy Manager User Guide*. For information about known issues with cluster upgrades, please refer to the “Cluster Upgrade and Update” sections in these Release Notes.
- The term “update” refers to applying a patch release within the same major version—for example, from 6.6.5 to 6.6.7.
  - To update a cluster to 6.6.8, we recommend using the **Cluster Update** interface. For more information, see the Cluster Upgrade and Cluster Update Tools section in the *ClearPass Policy Manager User Guide*. For information about known issues with cluster updates, please refer to the “Cluster Upgrade and Update” sections in these Release Notes.

This chapter includes the following sections:

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

An upgrade is the process of moving from one major release version to another—for example, from 6.5.x to 6.6.0. This section describes accessing upgrade images, considerations to be aware of, and instructions for restoring the log database after the upgrade (optional).

You can upgrade to ClearPass 6.6.0 from ClearPass 6.3.6, 6.4.7, or 6.5.x. Before you proceed with the upgrade, we recommend that you apply the latest available patch updates to your current release. For information on the patch update procedure, see "Updating Within the Same Major Version" on page 125.

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

- Upgrade images are available within ClearPass Policy Manager from the **Software Updates** portal at **Administration > Agents and Software Updates > Software Updates**.
- Upgrade images and preparation patches are also available for download on the Support site under **ClearPass > Policy Manager**.

Before You Upgrade

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

- Plan downtime accordingly. Upgrades can take longer (several hours) depending on the size of your configuration database. A large number of audit records (hundreds of thousands) due to Mobile Device Management (MDM) integration can significantly increase upgrade times. Refer to the sample times shown in Sample Times Required for Upgrade in "Sample Times Required for Upgrade" on page 123.
- Review the hypervisor disk requirements. These are described in "Virtual Appliance Requirements" on page 113 of the "System Requirements for ClearPass 6.6" chapter.
- Any log settings that were modified prior to the upgrade are not retained, and are reset to the default. The administrator should configure any custom log settings again after the upgrade.

Log Database and Access Tracker records are not restored as part of the upgrade. If required, you can manually restore them after the upgrade. For more information, please review "After You Upgrade " on page 123.

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

  To change this setting:

  Navigate to **Administration > Cluster Wide Parameters > General > Auto Backup Configuration Options = Off**.
- If you have a custom authentication source configured to use the session log database, additional steps are required after upgrade. You have such an authentication source configured if you have a source of type **Generic SQL DB** in **ClearPass Policy Manager > Configuration > Sources** with server name **localhost** or **127.0.0.1** and with the database name **tipsLogDb**. In such cases, manually restoring the session log database is required after the upgrade completes (see "After You Upgrade " on page 123). Please contact Customer Support for configuration recommendations to move away from using the session log database as an authentication source.
- MySQL is supported in ClearPass 6.x and greater. Aruba does not ship drivers for MySQL by default. Customers who require MySQL can download it from the Support site (http://support.arubanetworks.com). Users should be aware that this patch does not persist across upgrades.
- The 6.6.0 release introduced the Aruba ClearPass Extensions functionality. Extensions are operated as micro-services within the ClearPass system. These micro-services make use of the 172.17.0.0/16 network address space. Customers may experience problems with network connectivity, including the error message "no route to host," if there are network conflicts in their existing network with this address space. Customers whose networks include addresses in the 172.17.0.0/16 network are advised to either disable the ClearPass Extension service or to contact TAC for assistance in re-allocating the Extensions to use a different network address space. A future release will expose the ability to re-assign the micro-service network address space to customers.

- VM only: If you have two disks already loaded with previous ClearPass versions—for example, 6.2 on SCSI 0:1 and 6.3 on SCSI 0:2—then drop the inactive disk before upgrading. You must then add a newer disk based on the 6.6.0 disk requirements. Earlier releases used separate disks to store the current and previous ClearPass release; newer releases use just a single drive to store both installations. For current requirements, see "Virtual Appliance Requirements" on page 113.

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 71: *Sample Times Required for Upgrade*

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

After You Upgrade

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

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

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

Restoring the Log DB Through the User Interface

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

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

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

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

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

Restoring the Log DB Through the CLI

To restore the Log Database after the upgrade process is complete, use the `restore` command. Go to **Administration > Server Manager > Local Shared Folders** and download the **upgrade-backup.tar.gz** file. Host the file at an `scp` or `http` location accessible from the ClearPass appliance 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 6.6.5 to 6.6.7. Updates are available from the **Software Updates** portal in ClearPass Policy Manager. This section describes how to install a patch update either through the **Software Updates** portal, as an offline update, or through the **Cluster Update** interface.

During an update, the log database is retained. No extra steps are needed to retain the session log history during an update.

This section includes the following:

Installation Instructions Through the Software Updates Portal

This method may still be used to manually update appliances in a cluster, beginning with the publisher and then each subscriber; however, we recommend using the **Cluster Update** interface going forward to automate the process.

If access is allowed to clearpass.arubanetworks.com, ClearPass appliances will show the latest patches 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 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** portal is shown as **Needs Restart**, click the **Reboot** button to restart ClearPass. After the restart, the status for the patch is shown as **Installed**.

Installation Instructions for an Offline Update

If you do not have access to clearpass.arubanetworks.com and you need to do an offline update, you may download the signed patch from the Support site, upload it to the ClearPass appliance, 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**.
4. Browse to the downloaded patch file and then click **Import**.
5. When the import is complete, click **Install**.

6. When the installation is complete, if the status on the **Software Updates** portal is shown as **Needs Restart**, click the **Reboot** button to restart ClearPass. After the restart, the status for the patch is shown as **Installed**.

Installation Instructions Through the Cluster Update Interface

The **Cluster Update** interface automates the process of updating a cluster. The publisher is automatically updated first before any selected subscribers. In large cluster deployments (greater than 6) we recommend updating the subscribers in batches of no more than five at a time.

Before you begin, if you plan to download the 6.6.8 cumulative patch from the **Software Updates** portal for use with the **Cluster Update** interface on a ClearPass 6.6.0 appliance, you must first install the **ClearPass 6.6.0 Cluster Update Interface Patch**. This patch is required for ClearPass 6.6.0-based clusters in order to enable the **Cluster Update** user interface to recognize ClearPass patches and hotfixes when they have been downloaded through the **Software Updates** portal. It only needs to be installed on the publisher. This patch is NOT needed if the patches or hotfixes are manually imported into the ClearPass appliance.

If you accidentally download the 6.6.8 cumulative patch before installing the **ClearPass 6.6.0 Cluster Update Interface Patch**, the **Start Update** link will be missing from the **Cluster Update** interface. To resolve this issue, delete the 6.6.8 cumulative patch, click **Check Status Now** and then download it again.

To update the cluster:

1. In ClearPass Policy Manager, go to **Administration > Support > Agents and Software Updates**.
2. Download or import the patch you wish to deploy, and then click the **Cluster Update** link.
3. In the **Update Info** area, select the desired patch from the **Update Image Name** drop-down list.
4. Click the **Start Update** link. The **Start Cluster Update** window opens.
5. Select the cluster subscribers to be updated, and then click **Update**.

For more information about the **Cluster Update** interface, see the Cluster Upgrade and Cluster Update Tools section in the *ClearPass Policy Manager User Guide*. For information about known issues with cluster updates, please refer to the "Cluster Upgrade and Update" sections in these Release Notes, or contact TAC for technical assistance.