ClearPass 6.7.3

a Hewlett Packard
Enterprise company

Release Notes

Copyright Information

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release, ClearPass 6.7.3

ClearPass 6.7.3 is a 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 12—Describes new features and issues introduced in this 6.7.3 release as well as issues fixed in this 6.7.3 release.

- "Change of Behaviors in Previous 6.7.x Releases" on page 20—Provides a summary of behavior and resource changes introduced in earlier 6.7 releases.

- "Enhancements in Previous 6.7.x Releases" on page 26—Describes new features introduced in earlier 6.7 releases.

- "Issues Fixed in Previous 6.7.x Releases" on page 52—Lists issues fixed in earlier 6.7 releases.

- "Known Issues Identified in Previous Releases" on page 66—Lists currently existing issues identified in previous releases.

- "System Requirements for ClearPass 6.7" on page 90—Provides important system requirements information for this release.

- "Upgrade and Update Information " on page 100—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 6.7 platform:

- *ClearPass Policy Manager 6.7 User Guide*

- *ClearPass Guest 6.7 User Guide*

- *ClearPass Policy Manager 6.7 Getting Started Guide*

- *ClearPass 6.7 Deployment Guide*

- *Tech Note: Installing or Upgrading to 6.7 on a Virtual Appliance*

- *Tech Note: Upgrading to ClearPass 6.7*

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 6.7.3 release.

This chapter contains the following sections:

Release Overview

ClearPass 6.7.3 is a patch release that introduces new features and provides fixes for known issues. The 6.7.3 cumulative patch is available in ClearPass Policy Manager under **Administration > Agents and Software Updates > Software Updates**.

This section includes:

Change of Behaviors in the 6.7.3 Release

This release does not introduce any changes in ClearPass behaviors, resources, or support that would require you to modify existing system configurations after updating to 6.7.3. For a list of behavior changes introduced in previous 6.7.x releases, see the Change of Behaviors in Previous 6.7.x Releases chapter.

6.7 Upgrades on KVM Hypervisors are Deferred

Virtual appliance customers who use KVM hypervisors are advised to not apply the ClearPass 6.7.0 upgrade at this time. Our tests have shown a negative performance impact when 6.7.0 is installed on a KVM virtual appliance. To prevent this happening to our customers, at the time of this release we have not posted the virtual appliance image for KVM with the other 6.7.0 images. We are working to resolve the issue in a future patch release. We will then repost the KVM virtual appliance image and let users know we again recommend upgrading to 6.7.0 on KVM hypervisors. (#42601)

New Features and Enhancements in the 6.7.3 Release

The following new features were introduced in the ClearPass 6.7.3 release.

This section includes:

Endpoint Context Servers

The following new features are introduced in Endpoint Context Servers in the 6.7.3 release.

- Two context-specific AirWatch attributes, LocationGroupID and LocationGroupName, are now added to the endpoints database. If you have Organization Groups defined in AirWatch, these attributes can be used in ClearPass enforcement policies. When a device tries to authenticate, access can be allowed or denied according to the AirWatch group the device or user belongs to. The LocationGroupID attribute is mapped to the **Group ID** endpoint attribute, and the LocationGroupName attribute is mapped to the **Group Name** endpoint attribute. (#40407)

OnGuard

The following new features are introduced in OnGuard in the 6.7.3 release:

- Support was added for the following products: (#44224)
  - AsiaInfo Officescan 12.x (Windows)
  - Avast Free Antivirus 18.x (Windows)
  - AVG 18.2 (macOS)
  - AVG AntiVirus Free 18.1.3044 (Windows)
  - Carbon Black Response 6.x (Windows)
  - F-Secure Client Security for Mac 13.x (macOS)
  - Norton Internet Security 22.12.0.104 (Windows)
  - Norton Security v22.12.0.104 (Windows)
  - Sophos Anti-Virus v9.7.x (macOS)
  - Sophos Cloud Endpoint Antivirus 2.x (Windows)
  - Symantec Endpoint Protection for MAC Version 14.0.1 (macOS)
  - TrendMicro Virus Buster Cloud v12 (Windows)

  Support was enhanced for the following products:
  - BitTorrent 7.x (macOS)
  - FileVault 10.12.6 (macOS)
  - Kaspersky Endpoint Security (Windows)
  - McAfee Endpoint Security 10.5.1 (Windows)
  - McAfee Host Intrusion Prevention Firewall (Windows)
  - McAfee Total Protection 18.0.9019 (Windows)
  - Norton Internet Security (Windows)
  - Sophos Endpoint Security and Control 10.x (Windows)
  - Trend Micro OfficeScan Client (Windows)

- A new feature to enable application authentication in Guest Web login pages allows the OnGuard Native Dissolvable Agent to also identify the username. The default Dissolvable Agent does not perform end-user authentication. The Dissolvable Agent will be supported with VPN interfaces if the same username is used to identify the client in both RADIUS VPN authentication and application authentication, and if **Pre-Auth Check** is configured using one of the following values: (#43715)
  - **App Authentication**

- **Local**
- **RADIUS**
- **Single Sign On**

Policy Manager

The following new features are introduced in Policy Manager in the 6.7.3 release:

- For multi-factor authentication (MFA) workflows that use TACACS+, a new **TACACS+ Authentication Timeout** service parameter lets you specify the TACACS server's timeout interval. The default value for this parameter is 30 seconds. The minimum allowed value is 1 second, and the maximum allowed value is 300 seconds (5 minutes). Previously, the default timeout value was 10 seconds and could not be changed. An extended TACACS+ timeout interval might be needed when MFA workflows such as phone calls or text messages are used, which can take longer for the user to complete. To use this feature, go to the **Administration > Server Manager > Server Configuration** and select the service. On the **Service Parameters** tab, select **Tacacs server** as the service and then configure a value for the **TACACS+ Authentication Timeout** parameter. (#43268)

- A new admin privilege has been added for use exclusively with Aruba Downloadable Role Enforcement. This new privilege allows you to limit an admin account's permissions to just role download operations. Existing user accounts currently used for role downloads will be supported as before, but those accounts will not be updated with the new **Aruba User Role Download** admin privilege. You will need to create new users specifically with the new admin privilege level if you want to restrict them only to this feature. To use this feature, create a new user at **Administration > Users and Privileges > Admin Users > Add** and select **Aruba User Role Download** in the **Privilege Level** drop-down list. (#43958)

- A new service parameter, **Disable CPPM Machine account password expiry in AD**, was added to the list of RADIUS server parameters available on the **Administration > Server Manager > Server Configuration > Service Parameters** tab. When the value for this parameter is set to **TRUE**, it disables the Samba machine password timeout setting so that a machine password change will not be forced. If this parameter is left at the default setting of **FALSE**, the Samba machine password timeout setting will remain in effect. This parameter corrects an issue where MSCHAPv2 authentications against Active Directory sometimes failed with an "AD status: Access denied" error. (#44571)

Issues Resolved in the 6.7.3 Release

The following issues have been fixed in the ClearPass 6.7.3 release.

This section includes:

APIs

Table 2: *API Issues Fixed in 6.7.3*

Bug ID	Description
#44610	The log message "API call 'GET /api/cppm-version' failed due to an exception: Access denied" was sometimes displayed after upgrading from 6.6.x to 6.7.0.

Endpoint Context Servers

Table 3: *Endpoint Context Server Issues Fixed in 6.7.3*

Bug ID	Description
#44368	The endpoint OS version number fetched by the JAMF server was trimmed and did not include the complete number. The Endpoint OS Version attribute now also includes the minor version.

Guest

Table 4: *Guest Issues Fixed in 6.7.3*

Bug ID	Description
#44491	The PHP version is now updated to 7.1.5. This includes fixes for CVE-2018-7584.
#44601 #44667	Corrected multiple issues where emails sent from self-registrations or other areas of ClearPass Guest sometimes were not sent if they used any of the email templates other than the plain text template, and sometimes contained duplicate From addresses. This issue only occurred for some email domains. Compatibility issues with certain SMTP servers are now resolved.
#44608	Depending on the configuration of the operator translation rules, the list of print templates was sometimes empty or incomplete. This was not an issue with the default configuration.
#44805	In Guest deployments using sponsor lookups over LDAP, an LDAP sponsor lookup failed to match an existing account if two or more LDAP servers were configured.

Insight

Table 5: *Insight Issues Fixed in 6.7.3*

Bug ID	Description
#44371	Insight sometimes took a long time (4 - 5 hours) to generate a report. The SQL query is now optimized for CSV report generation.

Onboard

Table 6: *Onboard Issues Fixed in 6.7.3*

Bug ID	Description
#43988	Saving edits at **Guest > Onboard > Deployment and Provisioning > Provisioning Settings** caused the ClearPass user interface to crash.
#44604	In ClearPass 6.7.1, onboarding failed with Windows 10 devices. Onboard now enforces the QuickConnect client to use an HTTPS URL for EST certificate generation even if it is initially accessed over HTTP.

OnGuard

Table 7: *OnGuard Issues Fixed in 6.7.3*

Bug ID	Description
#43583	The ClearPass OnGuard Unified Agent detected the Global Protect VPN interface as Other and performed frequent health checks, resulting in high CPU usage on macOS and Windows.
#44022	The Native Dissolvable Agent for Windows displayed the error message "No active Interface" when health checks were performed for the Cisco AnyConnect VPN interface.
#44115	When the ClearPass OnGuard Unified Agent was run as a service, it sometimes took a long time (> 30 seconds) to perform health checks after the client was started.
#44204	The ClearPass OnGuard Agent for Windows did not detect DAT file deletion for McAfee Endpoint Protection on endpoints.
#44421	The ClearPass OnGuard Agent for Windows sometimes did not read the encryption state of drives that had been encrypted using BitLocker Drive Encryption.
#44440 #44454	The ClearPass OnGuard Agent for macOS did not terminate BitTorrent as part of auto-remediation of the Peer To Peer health class.
#44459	The ClearPass Agent Controller Service took a long time to start (three to six minutes), causing the OnGuard Agent to stay in the "initializing" state.

Policy Manager

Table 8: *Policy Manager Issues Fixed in 6.7.3*

Bug ID	Description
#38122	If a 6.6.x cluster was upgraded to 6.7.0 while an IPSec tunnel was enabled between the publisher and the subscribers, the tunnel could not be established, the subscribers could not connect back to the publisher, and the error message "No proposal chosen" was displayed.
#42982	ClearPass could not be rolled back to the last known good signature if it failed to load a new signature update. Posture signature updates are now automatically reverted to the previous signature if there is a problem that prevents the signature from loading correctly.
#43971	The computed attribute **Connection:Client-Mac-Vendor** did not fetch the vendor information from RM43836 for a newly-added Cisco device. The MAC Vendor list is now reloaded as part of manually importing fingerprints or automatically downloading them, and the details are displayed at **Configuration > Identity > Endpoints > Edit Endpoint**.
#43992	ClearPass deleted a valid user if an AirGroup authorization occurred after 802.1x authentication. This issue only occurred during post-authentication events.
#44178	After upgrading to 6.7.0 on system where the browser language was Japanese, some of the Japanese characters were replaced with question marks (?) in the **Configuration > Services** list, and a new MAC Authentication service could not be saved at **Configuration > Services > Add**. Characters are now displayed correctly and services can be added and edited when the browser language is Japanese or Chinese.
#44215	The DigiCert Global Root Certificate G2 CA is now added to the ClearPass certificate trust list as part of the updated server certificate for the Aruba Active Server.
#44249	The Apache Tomcat version is now upgraded to 7.0.85. This includes fixes for the vulnerabilities described in CVE-2018-1304 and CVE-2018-1305.

Table 8: *Policy Manager Issues Fixed in 6.7.3 (Continued)*

Bug ID	Description
#44257	A service certificate that was configured on one service was also applied to all the services below that service in the order of processing, even if they were configured with a different service certificate. This had caused requests to the lower services to be denied with the error "Unknown CA."
#44271	The patch-rollback command was not available in an Amazon Web Services (AWS) ClearPass instance.
#44297	Public key authentication did not always lock out SSH access when configured in Advanced mode.
#44350	ClearPass failed to apply the standard downloadable user role on an Aruba switch. The class commands no longer include tab characters.
#44359 #44424 #44781	After upgrading to 6.7.0 or 6.7.1, the message "Error in processing request. Please retry" was displayed in the banner, and the log files showed "Battery stopped" errors.
#44403	When setting more than 200 RADIUS services, loading the RADIUS configuration took a long time (two minutes).
#44425	SMS over SMTP failed if the recipient's email address included a plus sign (+) — for example, *+somenumber@sms.domain*.
#44433	After post-authentication enhancements were introduced in 6.7.2, some HTTP operations were no longer supported. When using Post-Auth v2, the PUT, PATCH, and DELETE operations are now supported again for generic HTTP servers.
#44492	This release includes fixes for the vulnerability described in CVE-2018-0489.
#44502	In PSK mode, IPsec VPN connections between ClearPass and some remote devices failed to establish. This issue had affected tunnels to Aruba controllers, but had not affected tunnels between ClearPass systems.
#44535	The validator for the Extensions Network Address service parameter was restricted to values in the range 172.16.0.0/14 instead of the correct RFC1918 value, 172.16.0.0/12.
#44563	If a ClearPass appliance was restarted or rebooted, its time zone was reset to one that was configured in the previously-installed ClearPass version instead of retaining the currently configured time zone.
#44566	The user interface did not indicate that an Identity Provider certificate was required in order to use ClearPass as a service provider. Validation is now added, and the message "Identity Provider (IdP) Certificate is mandatory" is displayed in the banner if an IdP certificate is not selected at **Configuration > Identity > Single Sign-On > SAML SP Configuration**.
#44620	When creating or editing a network access device (NAD) group at **Configuration > Network > Device Groups**, the changes could not be saved. This issue occurred in ClearPass 6.7.0 and higher on Internet Explorer.
#44621	After upgrading to 6.7.2, an snmpwalk of UCD-SNMP-MIB showed "Invalid argument" entries for some ClearPass service status attributes in the SNMP polling results.
#44653	This release includes fixes for the vulnerability described in CVE-2018-7063.
#44684	The port number could not be changed for a MySQL authentication source that was already created with a default port, and the error message "Communication link failure. The last packet sent successfully to the server was 0 milliseconds ago. The driver has not received any packets from the

Table 8: *Policy Manager Issues Fixed in 6.7.3 (Continued)*

Bug ID	Description
	server" was displayed when trying to save the filter configuration on the **Configuration > Authentication > Sources > Attributes** tab.
#44685	After a custom attribute was created in the **Attributes** dictionary with the **Is Mandatory** field set to **Yes**, the new attribute was not available in service rules at **Configuration > Services > Add**.
#44693	A SAML POST request failed if the request was greater than 8 KB, and the response showed the error message "Your browser sent a request that this server could not understand. Size of a request header field exceeds server limit."
#44825	Corrected an issue with the connection pooling service where the service did not restart properly.

New Known Issues in the 6.7.3 Release

The following known issues were identified in the ClearPass 6.7.3 release. For a list of known issues identified in previous releases, see .

This section includes:

-
-
-
-

CLI

Table 9: *CLI Known Issues in 6.7.3*

Bug ID	Description
#44744 #44748	**Symptom:** The "Last Login" notification banner in the CLI shows the two failed login attempts when it should show one. The **Event Viewer** in the user interface also shows two command line login failures instead of the one that occurred, and with slightly different timestamps. **Scenario:** This issue occurs only in the 6.7.3 release. Users should be aware that this is expected behavior. When logging in through SSH, and with SSH lockout enabled, two messages are generated: One message indicating the login failure, and one message keeping count of the failed login attempts. Both messages are in the **Login Failure** event category. To distinguish between the two, refer to the event description in **System Events**: **Failed SSH login attempt 1 using appadmin account** is the login message containing the failed attempt count, and is generated due to the SSH lockout feature. **Failed SSH password login attempt using appadmin account** is the login message that keeps track of the failed login attempts.

Guest

Table 10: *Guest Known Issues in 6.7.3*

Bug ID	Description
#44658	**Symptom/Scenario:** In the **Login Form** area of the **Self-Registration** form, the **Username Authentication** field is not displayed if the **Pre-Auth Check** field is set to **Local - match a local account**.

OnGuard

Table 11: *OnGuard Known Issues in 6.7.3*

Bug ID	Description
#44915	**Symptom/Scenario:** The ClearPass OnGuard Agent does not work if support for TLS 1.0 or TLS 1.1 is disabled in cluster-wide parameters for the ClearPass server.

Policy Manager

Table 12: *Policy Manager Known Issues in 6.7.3*

Bug ID	Description
#44654	**Symptom:** The **Event Viewer** shows an unexpected number of license errors when the license usage is exceeded. **Scenario:** While the license usage limit is exceeded, ClearPass detects the license violation each time the **Refresh Count** link is clicked. Users should be aware of the following behaviors: ● When any ClearPass Application License's limit is exceeded, alerts are logged in **Event Viewer** messages, SNMP traps are sent, and the alert is shown in the banner. ● The frequency of these alerts is every 15 minutes, and each time the **Refresh Count** link is clicked at **Administration > Server > Licensing**.
#44818	**Symptom/Scenario:** Traffic is not sent through an IPsec VPN tunnel in Transport mode between ClearPass and an Aruba Controller running ArubaOS 8.x, even though the tunnel is successfully established.
#44904	Corrected an issue where the BIOS firmware included as part of patch updates sometimes caused the patch installation to fail. The BIOS update for HPE-based C2000 appliance models (purchased under SKU JX921A or JZ509A) that was published in previous patches is now removed from the cumulative update patch.

This chapter provides a summary of changes to behaviors, resources, or support that were introduced in previous ClearPass 6.7.x releases. For a list of behavior changes introduced in the ClearPass 6.7.3 release, see the What's New in This Release chapter.

This chapter includes:

Licensing Enhancements

The 6.7.0 release introduced major enhancements in the ClearPass licensing platform. The licensing structure is improved to be easily scalable for networks of any size, whether small or large. Almost all license management is available within the Policy Manager user interface, and up-to-the-minute usage statistics can be viewed at a granular level. As part of these changes: (#39222, #39705, #39711, #39716, #41079, #43007,)

- Two new license types are included: the ClearPass Platform Activation Key and the Access License. The ClearPass Platform Activation Key enables ClearPass on the server, and replaces the Policy Manager License. The Access License handles authentications on the system.

- The ClearPass Guest Application License has been deprecated. The Web-Based User Registration and Authentication capability previously enabled with the ClearPass Guest License is now enabled with the new Access Application License. The Onboard Application licenses are now counted per-user rather than per-device.

- Licenses can be purchased in smaller minimum quantities, and additional blocks of licenses can be added in increments as small as 100 or as large as 10K.

- One Virtual Appliance SKU which can be used for the C1000V, C2000V, and C3000V virtual appliance types.

- When a subscription license or an evaluation license expires, ClearPass will continue to work normally but Administrators will not be able to make services configuration changes, and updates and upgrades will not work.

- Now that Guest Application licensing is bundled into the Access Application license and is based upon concurrency, High Capacity Guest mode is no longer required or available. It has been removed from the cluster-wide parameters configuration.

- ClearPass 6.7.0 eliminates the use of the Subscription ID to validate support entitlement for access to the **Software Updates** portal (for example, posture and profile data updates, firmware and patch updates, and skins). The HPE Passport account credentials that are associated with customers' ClearPass licenses are now used to validate entitlement — this serves to simplify and reduce the frequency of issues previously seen by customers if they updated their support contract but it was not recognized by the Subscription ID. On the **Software Updates** page, enter your HPE Passport username and password in the **HPE Passport Credentials** area. We recommend that customers use a "generic" HPE Passport account (for example, clearpass@customerX.com or CustomerXClearPass) to avoid any future issues in the event that an individual employee leaves the business and the HPE Passport account is closed or the password is forgotten. Legacy ClearPass licenses and their associated Subscription ID(s) should be moved to this generic account for validation purposes.

- All license installation is now performed through the Policy Manager user interface. Licenses cannot be installed through the CLI.

ClearPass Platform Activation Key

The ClearPass Activation Key enables ClearPass on the appliance, and replaces the Policy Manager License.

- If you are upgrading to ClearPass 6.7.0 from an earlier version, your existing Policy Manager License Key will be automatically converted to a Platform Activation Key (PAK). You will not need to do anything to make the conversion happen, and the PAK is pre-activated.

- If you are a new customer doing a fresh installation of ClearPass 6.7.0, then in the HPE My Networking Portal you will receive a Platform Activation Key (PAK) for each ClearPass appliance and redeem your licenses. When you first log in to ClearPass, you will be prompted to enter the Platform Activation Key in the license key field of the End-User License Agreement, and then prompted to activate the product. This associates the ClearPass Platform License with the appliance. Remember to activate your Platform Activation Key as soon as it is installed. If it is not activated within 90 days, access to the ClearPass user interface will be locked and must be reopened by TAC.

The ClearPass Platform License is the base-level license and enables ClearPass on the appliance, including the Policy Manager and Guest user interface. You must have a ClearPass Platform license for every appliance. You can activate the license offline by submitting a case through the My Networking portal.

Each hardware and virtual appliance receives a permanent Platform License that never expires.

Application Licenses

ClearPass supports three Application License types: Access, OnGuard, and Onboard. Application licenses can be added for Onboard and OnGuard. To add an application license, go to **Administration > Server Manager > Licensing** and click **Add License**. To update or activate an Application License, go to the **Administration > Server Manager > Licensing > Applications** tab. To activate the license offline, submit a case through My Networking portal.

- **Access —** The Access license accounts for authentications on the system, and is now based on actual current usage — that is, each user or device consumes an Access License during an active session. The Access License is also no longer associated with an appliance, and Guest functionality is now included in this license. It is available as either a perpetual license, or as a one year, three year, or five year subscription license. The minimum number of Access licenses is 100.

- **Onboard —** Each Onboard Application License is now computed based on the number of users with Onboard-generated device certificates rather than on the user's number of enrolled devices. It is available as either a perpetual license, or as a one year, three year, or five year subscription license. The minimum number of Onboard licenses is 100.

- **OnGuard —** The OnGuard Application License is computed for all endpoints using OnGuard in any mode of operation. It is consumed by device rather than by MAC address or username, and for a period of 24 hours. It is available as either a perpetual license, or as a one year or three year subscription license. The minimum number of OnGuard licenses is 100.

License Tracking

License usage counts are now computed every 15 minutes, and the count on the **Administration > Server Manager > Licensing** page is updated accordingly.

License Management in the User Interface

- The **Administration > Server Manager > Licensing** page lets you access and manage your licenses:

  - The **Add License** link lets you add licenses that have been purchased and redeemed in My Networking Portal (MNP), and a new **Refresh Count** link lets you update the license usage counts to the current moment.

  - The **License Summary** tab now shows the total count and used count for each of the new license types (Access, Onboard, and OnGuard).

  - The **Servers** tab now lets you see information for the ClearPass Platform license on the server (instead of the Enterprise license), and activate or update the Platform license.

  - The **Applications** tab lets you see information for the product Application licenses on the server and activate or update the licenses.

- In Insight, you can go to **Dashboard > Licensing** to open the **Licensing Dashboard** page. Three graphs on this page let you view license information for the Access, Onboard, and OnGuard license types:

  - **Current License Usage (15 minutes interval)** — For each type, this graph shows the **Total**, **Exceeds limit**, and **Used** counts over the past 15 minutes.

  - **License Usage In Last 24 Hours** — For each type, this graph shows the **Used Count** and **Available Count** for each hour over the past 24 hours.

  - **Maximum License Usage** — For each type, this graph shows the **Max used count** for a given time frame. This graph can be set for a look-back window of the last 24 hours, one week, or one month.

- In the Policy Manager **Dashboard**, the pie chart in the **License Usage** widget shows the **Available Count** and **Used Count** for Access, Onboard, and OnGuard Application Licenses.

Licenses in Cluster Scenarios

- All license management operations for a cluster must be performed on the publisher.

- When you add an appliance to a cluster, it loses all of its licenses except for the Platform Activation Key. Any Application Licenses it had before it became a subscriber must then be added to the publisher.

- When you drop an appliance from a cluster, it loses all of its licenses except for the Platform Activation Key.

- When an appliance is *manually* promoted to publisher, all of its Application Licenses must be reactivated.

- When an appliance is *automatically* promoted to publisher, there is no change in the status of any of its licenses.

- Licenses are shared by a cluster. For example, if there are five ClearPass appliances in the cluster and a 10K Access license is applied, that capacity is distributed across the cluster as needed.

Insight Reports for Licensing

- Two new licensing reports, **Licensing Dashboard** and **Licensing Report**, are added in 6.7.0. These replace the previous **System Dashboard** and **System License Usage** reports, which are now deprecated.

- Since Guest functionality is included in the Access License, the **Guest License Usage Trend** graph is now deprecated.

Upgrade Process Overview

During a ClearPass upgrade the following activities will occur:

- The Policy Manager license (500, 5K, and 25K) will be used as the PAK for ClearPass hardware and virtual appliances. It will also be automatically activated irrespective of Internet access.

- 1000 Access, 100 Onboard, and 100 OnGuard evaluation licenses will be auto-installed in the system with an expiration period of six months.

- The Subscription ID will be replaced by the HPE Passport credentials.

We recommend that you capture the in-use Subscription ID before you upgrade.

The inclusion of the above evaluation licenses for Access, Onboard, and OnGuard licenses ensures that customers can continue operating after the upgrade if there are any issues issuing or converting the license keys to ClearPass 6.7.

Previous Behavior Changes

Users should be aware of the following important changes in ClearPass behaviors, resources, or support that might require changes in existing system configurations after updating or upgrading. For more information, refer to the ticket descriptions in these Release Notes, and to the *Policy Manager User Guide* and *Guest User Guide*. For a list of behavior changes introduced in the 6.7.3 release, see the What's New in This Release chapter.

The following behavior changes were introduced in previous 6.7.x releases:

- For TACACS+ authentications, the license usage accounting methodology has changed. On a ClearPass system with a valid Access license, TACACS+ sessions will not be counted towards Access license consumption.

- The character limits for AirGroup shared location, shared user name, shared user group, and shared role fields are now updated to match the value limits in the controller. AirGroup users should review the new character limits. (#20748)

- Context server actions that were defined prior to ClearPass 6.7.0 cannot be imported to a 6.7.x version by using the Endpoint Context Servers list's Import or Export options, nor by any other import action that includes context server actions. (#32365, #32366)

- Social Logins fields in ClearPass Guest are now renamed to Cloud Identity, reflecting the expanding variety of cloud-based external login platforms. (#32943)

- Insight configurations from Insight versions earlier than ClearPass 6.6 are not retained during migration or upgrade, and will need to be manually recreated after upgrading to ClearPass 6.7.0. (#33667)

- The names of the ClearPass virtual appliance (VA) and hardware appliance types have changed: (#39899)

  - CP-SW-EVAL is now CLABV

  - CP-VA-500 is now C1000V

  - CP-VA-5K is now C2000V

  - CP-VA-25K is now C3000V

  - CP-HW-500 is now C1000

  - CP-HW-5K is now C2000

  - CP-HW-25K is now C3000

- ClearPass 6.7 replaces MySQL support with MariaDB and now includes the SQL driver by default. A separate patch is no longer required in order to create and use MySQL or MariaDB authentication sources. MariaDB is the open-source fork of Oracle MySQL. The ClearPass 6.7 MariaDB driver is compatible with either MySQL or MariaDB. (#40212)

- OnGuard Plugin Version 1.0 (V3 SDK) is now deprecated. To help administrators migrate from OnGuard Plugin 1.0 to OnGuard Plugin 2.0, ClearPass now automatically converts existing Plugin 1.0 posture policies

to Plugin 2.0 posture policies. For more information, please refer to the descriptions in the "New Features and Enhancements" section. (#40372, #40397, #41098, #41100)

- The name of the ClearPass Virtual IP service is now changed from **cpass-vip-service** to **cpass-vip**. (#40954)

- Users should be aware that for both CLI and UI logins, "eTIPS123" can no longer be used as the new password during installation. The password you set during installation will be used for both the CLI and the UI. (#42242)

- In OnGuard's **Global Agent Settings**, the attributes **Allowed Subnets for Wired access** and **Allowed Subnets for Wireless access** are now deprecated and should not be used. (#42305)

- In the **Software Updates** portal, the **AntiVirus and AntiSpyware Updates** patch is now renamed to **Posture Signature Updates**. (#42449)

- Customers who use OnGuard or who use endpoint profiling must explicitly enable two new cluster-wide parameters in order to continue receiving automatic updates, even if they received automatic OnGuard or profiling updates prior to the 6.7.0 release. (#42605)

- Refer to the *6.6.7 Hotfix Patch with SMBv2 and v3 Support Release Notes*. With this change, when joining an AD domain and doing PEAPv0+MSCHAPv2 authentication, ClearPass will negotiate and use the highest SMB protocol version supported by the server. ClearPass will support SMB v1, SMB v2, and SMB v3. This adds additional TCP dynamic port requirements. There are no user visible changes for CLI, UI, processes, or behaviors.

- Connection settings for SMS Global are updated. If you use SMS Global, you should manually test sending with ClearPass Guest. (#44003)

- Before performing a patch rollback operation from any 6.7.x patch version, please read the new section in the Upgrade and Update Information chapter, "After You Update: Performing a Patch Rollback" on page 109.

- Certain OIDs have been temporarily removed from ClearPass, potentially affecting some existing SNMP configurations. (#43734)

This chapter provides a brief summary of the features and enhancements introduced in previous ClearPass 6.7.x releases. For a list of enhancements introduced in the ClearPass 6.7.3 release, see the What's New in This Release chapter.

> For ClearPass 6.7 licensing information, see "Licensing Enhancements " on page 20.

This chapter includes:

APIs

Features Added in 6.7.0

- The **ActiveSession** API includes additional sorting options. The following fields are now sortable: (#34175)
  - **nasipaddress**
  - **calledstationid**
  - **nasportid**
  - **nasporttype**
  - **nas_name**
  - **acctsessiontime**
  - **acctinputoctets**
  - **acctoutputoctets**
  - **total_traffic**
  - **sponsor_name**
  - **sponsor_email**
  - **sponsor_profile_name**

CLI

Features Added in 6.7.1

- After a cumulative patch is applied, the new CLI command **system patch-rollback** allows administrators to revert to the last installed version. For example, if a system is at 6.7.1 and cumulative update 6.7.x is applied, it can be reverted to 6.7.1 through the **system patch-rollback** command. This command can be used if a problem is found after the patch update, such as an issue identified in production that was not identified during testing, resulting in a degradation of capabilities. (#22924)

  Before using this command to revert from 6.7.1 to 6.7.0, you must first download the **ClearPass 6.7.0 Rollback RPM Package** from the **Software Updates** page and install it.

  As part of this feature, users should be aware of the following:

  - As best practice, users should always take a data backup before an update.

  - This command cannot be used after an upgrade to revert to an earlier major version (for example, 6.6.x).

  - Although you can only roll back to the last version that was installed, if multiple hotfix patches are included within the cumulative patch version you are rolling back from, then you can roll back multiple hotfix patches, one at a time, to a specific hotfix within the current version. To roll back to the previously installed version, you must first roll back each intervening hotfix patch.

  - When this command is used in a cluster, it must be done to all the appliances in the cluster. The publisher must be rolled back first, followed by each subscriber individually. The rollback must be completed on all appliances in the cluster within 24 hours after the publisher rollback is initiated in order to maintain the cluster status.

  - Any custom skins that are installed in the current version are retained after the rollback to the earlier version.

  - System rollback events are logged in the Event Viewer.

Features Added in 6.7.0

- A ClearPass hardware appliance can now be reset to factory default settings if needed, and a new, fresh software image can be installed. In the case of a software issue such as a problem with an operating system or a concern about a system compromise, this feature makes it possible to easily recover the system instead of having to return it for replacement. If an appliance does need to be returned for hardware issues, this feature can also be used to remove sensitive data first. Also, if an appliance that needs to be returned is part of a cluster running on an earlier version of ClearPass, but a replacement would be shipped as a later version, this feature allows the new appliance to be easily re-imaged to the earlier version without requiring Support to do it. (#21416, #41021)

  As part of this feature, two new CLI system commands are introduced, and are available only for the appadmin login:

  - The **system factory-reset** command resets the user's current partition of a hardware appliance to factory defaults. This command resets policy settings and system settings such as network settings and FIPS mode, and resets ClearPass Guest, ClearPass Onboard, and ClearPass Extensions. It resets or clears configuration files such as SSH, IPsec, and NTP, and clears licensing information and log files. It does not change the ClearPass version of the current partition. This command does not affect the second partition. After execution, the system is rebooted and must be bootstrapped at login.

  - The **system install-image** command installs a fresh image of version 6.7.0 or later on the second partition of the hardware appliance. None of the data from the current partition is migrated, and any data already present on the second partition is lost. No licensing information is carried forward to the

new partition where the image is installed. The system is rebooted to the second partition, and must be bootstrapped at login. The second partition is marked as the active partition after this command is executed. If the system is connected to the Internet, the image is installed from a Web service. If the system is not connected to the Internet, then the image must be imported into ClearPass by uploading and installing a file.

For each of these commands, the user should be aware of the effects of the command and first perform all necessary data backups. A warning message alerts the user to this need, and the command is not executed until they confirm it. If the appliance is a publisher, running either of these commands drops it from the cluster, and the stand-by publisher then becomes the publisher. If the appliance is a subscriber, it is dropped from the cluster and becomes a stand-alone appliance. For more information, see the "System Commands" section of the *ClearPass Policy Manager 6.7 User Guide*.

> ⚠️ **CAUTION**
>
> Users must take a backup first, and must store it outside of the system. Any backup that is stored inside the system will be deleted.

- The command **network ip list** is now enhanced to show route information from the **main**, **static**, **management**, **data**, and **ipsec** tables. (#30093)
- The **show ntp** command is now enhanced to display the NTP authentication key details corresponding to the configured NTP server. (#39781)

Endpoint Context Servers

Features Added in 6.7.0

- A ClearPass hardware appliance can now be reset to factory default settings if needed, and a new, fresh software image can be installed. In the case of a software issue such as a problem with an operating system or a concern about a system compromise, this feature makes it possible to easily recover the system instead of having to return it for replacement. If an appliance does need to be returned for hardware issues, this feature can also be used to remove sensitive data first. Also, if an appliance that needs to be returned is part of a cluster running on an earlier version of ClearPass, but a replacement would be shipped as a later version, this feature allows the new appliance to be easily re-imaged to the earlier version without requiring Support to do it. (#21416, #41021)

  As part of this feature, two new CLI system commands are introduced, and are available only for the appadmin login:

  - The **system factory-reset** command resets the user's current partition of a hardware appliance to factory defaults. This command resets policy settings and system settings such as network settings and FIPS mode, and resets ClearPass Guest, ClearPass Onboard, and ClearPass Extensions. It resets or clears configuration files such as SSH, IPsec, and NTP, and clears licensing information and log files. It does not change the ClearPass version of the current partition. This command does not affect the second partition. After execution, the system is rebooted and must be bootstrapped at login.

  - The **system install-image** command installs a fresh image of version 6.7.0 or later on the second partition of the hardware appliance. None of the data from the current partition is migrated, and any data already present on the second partition is lost. No licensing information is carried forward to the new partition where the image is installed. The system is rebooted to the second partition, and must be bootstrapped at login. The second partition is marked as the active partition after this command is executed. If the system is connected to the Internet, the image is installed from a Web service. If the system is not connected to the Internet, then the image must be imported into ClearPass by uploading and installing a file.

For each of these commands, the user should be aware of the effects of the command and first perform all necessary data backups. A warning message alerts the user to this need, and the command is not executed until they confirm it. If the appliance is a publisher, running either of these commands drops it from the cluster, and the stand-by publisher then becomes the publisher. If the appliance is a subscriber, it is dropped from the cluster and becomes a stand-alone appliance. For more information, see the "System Commands" section of the *ClearPass Policy Manager 6.7 User Guide*.

> **CAUTION**
>
> Users must take a backup first, and must store it outside of the system. Any backup that is stored inside the system will be deleted.

- The command **network ip list** is now enhanced to show route information from the **main**, **static**, **management**, **data**, and **ipsec** tables. (#30093)

- Context Server Action content can now be customized for Palo Alto Networks Firewall (PANW) endpoint context servers. You can notify PANW of additional attributes by adding a new action or modifying an existing action. You can also create or import new attributes for PANW at **Administration > Dictionaries > Context Server Actions**. (#31343, #38979, #40754)

  As part of this feature, some new default actions have been added and some have been removed:

  - The Context Server Actions dictionary now includes the following new actions for a total of 18 actions — Register Device, Register Posture, Register Role, Send HIP Report (Global Protect), Send Login Info, Send Logout Info, Unregister Device, Unregisture Posture, and Unregister Role.

  - The following four options in the Endpoint Context Server have been removed — ClearPass Profiler, ClearPass Role, GlobalProduct, and UserID Post URL.

  - On the **Administration > Server Manager > Server Configuration > Service Parameters** tab, the **Send Posture Data** option is removed from **Async Network Services**. This is now controlled by associating or dissociating Send posture in the default actions.

- Support was added for OAuth2 authentication in endpoint context servers. When OAuth2 authentication is selected, ClearPass can post the context server action to third-party firewall vendors that require OAuth2 authentication. You can configure an endpoint context server to use either OAuth2 authentication, basic authentication, or both. After this option is configured for the endpoint context server, you can also update each server action to use one of the authentication options. OAuth2 authentication in endpoint context servers only supports the **client_credential** grant type. (#32365, #32366)

  - To use this feature to specify OAuth2 for an endpoint context server, go to **Administration > External Servers > Endpoint Context Servers**. In the **Authentication Method** drop-down list for a new or existing server, select either **Basic**, **OAuth2**, or **Both**. For the OAuth2 options, the **OAuth2 Client ID**, **OAuth2 Client Secret**, and **OAuth2 Resource URL** must also be provided.

  - To use this feature to update individual actions for the context server type, go to **Administration > Dictionaries > Context Server Actions**, and select an **Action Name** for the server type. In the **Authentication Method** drop-down list for the action, select either **None**, **Basic**, or **OAuth2**.

> **NOTE**
>
> Users should be aware that context server actions that were defined prior to ClearPass 6.7.0 cannot be imported to a 6.7.x version by using the **Endpoint Context Servers** list's **Import** or **Export** options, nor by any other import action that includes context server actions (for example, from **Services** with context server actions included).

- The PATCH method is now supported in endpoint context server actions for sending information to the HTTP server. This method can be used to append content to existing endpoints or values. (#34519)

- A new **Compliance** attribute is added to the Endpoints dictionary. This attribute is used to summarize an endpoint's posture against Airwatch corporate policy. The **Compliance** attribute can have one of three

values: NotAvailable, NonCompliant, or Compliant. The AirWatch **ComplianceStatus** attribute can be mapped to the **Compliance** attribute and used to make enforcement policy decisions. (#39266)

- The **show ntp** command is now enhanced to display the NTP authentication key details corresponding to the configured NTP server. (#39781)

Guest

Features Added in 6.7.2

- As part of an API services update by SMS Global, connection settings for SMS Global are now updated to use a new subdomain. If you use SMS Global as an SMS gateway, you should manually test sending with ClearPass Guest. If you have firewall rules configured, they should be updated to allow the new required domain **api.smsglobal.com** instead of smsglobal.com.au. (#44003)

Features Added in 6.7.0

- Phone number fields now use visual country selectors and have country-specific validation. When you enter data in a phone number field (visitor_phone or sponsor_phone), you must first use the drop-down list in the field to select the country. The drop-down lists are visually identified by country flags. After selecting the country, you then enter the local number in full international format. Phone numbers must pass validation. If the number is not in international format, it may cause a random country to be detected. The phone field can be reverted to a simple text field by customizing the field. If you had accounts with false numbers, they may not be able to be re-saved. (#8949)

- In the **Network Access Server** portion of a **Self-Registration** configuration, the **Login Form** area now includes some new **Pre-Auth Check** options. In addition to the existing option to match the username and password against a local account before doing the NAS check, the following options are also provided: (#11759)

  - **None — no extra checks will be made**

  - **App Authentication — check using Aruba Application Authentication**

  - **RADIUS — check using a RADIUS request**

- When editing a date/time picker field in the custom field editor, a new option now lets you specify a time of day. When a value is entered for this option, the date/time picker becomes only a date picker, and the time is always set to the specified value. To use this feature, go to **Guest > Configuration > Pages > Fields**, edit a field that includes a date or time component, and in the **User Interface** field select **Date/time picker**. The form expands to include the Time of Day option. (#10024)

- A new field validator, **IsValidEmailList**, can validate more than one email address. Each email address is validated and the check will only pass if all of the email addresses are valid. (#13281)

- The ability to apply translations to the user interface has been enhanced. A new **Translations** option is now available in most list views in **ClearPass Guest > Configuration**, allowing administrators to apply a language pack directly to a selected item in a list, and to customize translations for individual fields, labels, and descriptions of customized forms, views, or print templates. The **Translations** link is available in **Self-Registrations**, **Web Logins**, **Fields**, **Forms**, **List Views**, **Web Pages**, and **Receipts > Templates**. The **Translations** option replaces the previous **Override Translations** option. (#15276)

- The **IsValidEmail** email validator is now enhanced to also support **allow** and **deny** rules for specific email addresses as well as for domains. (#25382)

- LDAP sponsored lookups can now complete a registration when multiple values are returned. When doing a sponsored lookup, if an attribute is returned as an array the first value will be taken. (#25590)

- For a user account in ClearPass Guest, the **create_time** field is now set only once, so it retains the time when the account was first created and the actual account lifetime can be determined. If the same username is registered again, the **create_time** field will not be overwritten. (#26305)

- The role to map to an operator profile no longer needs to be created manually. When an administrator creates a new operator profile in ClearPass Guest, the corresponding role will now be automatically created and available in Policy Manager. The new role will be created with the same name as the operator profile. If an administrator later wants to rename the role, the role is not replaced — instead, the first role is kept unchanged and another role is created with the new name. (#26355)

- Social Logins fields are now renamed to Cloud Identity, reflecting the expanding variety of cloud-based external login platforms. (#32943)

- The Guest and Onboard applications log can now be sent to a remote syslog server. To use this feature, go to the **Policy Manager > Administration > Server Manager > Log Configuration > System Level** tab and enter the remote server's address in the **Syslog Server** field. In the **Guest/Onboard** service's row, mark the **Enable Syslog** check box and then select the log level in the **Syslog Filter Level** drop-down list. Syslog data is generated in RFC 5424 format. (#34011)

- OAuth permission scopes can now be customized for cloud identity authentication providers (previously social logins). To use this feature, go to either Onboard's **Provisioning Settings > Web Login** form, the **Configuration > Pages > Web Logins** form, or the **Pages > Self-Registrations** form. Open the advanced authentication provider options in the **Cloud Identity** area and enter any overrides in the **Scope** field. Syntax information is available in the individual authentication providers' documentation. (#35303)

- For customers who use ClearPass Extensions, a new page lets you manage your installed Extensions, and search for new Extensions in the Extensions Store and install them. To use this feature, go to **Guest > Administration > Extensions**. All currently installed Extensions are displayed in the list, and the **Install Extension** link lets you search for an Extension by keyword or Extension ID and install it. (#35345, #40191, #40468)

- Support was added for Basque Euskara, Russian, Swedish, Italian, and Polish translations in many guest-facing pages. (#36188, #37687, #37688, #42379, #42380, #42381)

- Slack is now available in the list of cloud identity (previously social logins) authentication providers. (#38888)

- A new page lets you customize list views in ClearPass Guest. You can modify various properties, such as change the title; add, edit, or reorder columns; show usage; and download or modify translations. To use this feature, go to **Guest > Configuration > Pages > List Views**. (#39284)

Insight

Features Added in 6.7.0

- The **Onboard** category of Insight reports allows you to schedule a report that shows the number of certificates due to expire within a selected time frame. (#25255)

- When Insight reports are sent via email to notification recipients, the recipients receive an email with a link to an HTML version of the report, and a zip file containing the report in CSV and PDF formats. If the zip file is larger than 2MB, the CSV file is not be included in the zip file, but the email includes a link for downloading the CSV file. (#26237)

- Insight includes a new guest authentication report template; **Guest - Hotspot**. This template displays information about hotspot user logins recorded over the selected time frame, such as hotspot plan

distribution (for example, free vs. hourly paid access) and hotspot purchase amount. This report is available in the **Guest Authentication** category of reports. (#26879)

- The file names for Insight report PDFs downloaded from the Insight user interface now include the report name and the date and time the report was generated, in the format **<ReportName>-<Report_Run_Date>-<Report_Run_Time>.pdf**; where the <Report_Run_Time> is in UTC. (#29518)

- The list of created reports on the Insight **Reports** page and the list of configured reports on the **Reports > Configuration** page display a colored indicator dot by each report name to indicate the status of that report. A red dot by the report name indicates that the report failed to generate. Starting with ClearPass 6.7.0, you can hover your mouse over a red indicator dot on these pages to display a tooltip with additional information on why the report failed to generate. (#31180)

- The predefined **Insight Repository** authentication source in ClearPassPolicy Manager supports the following new filter queries to fetch authentication and authorization attributes: active sessions, online status, daily duration, weekly duration, and monthly duration. (#31281)

- When you hover your mouse over the header statistics on the Insight **Dashboard** pages, a tooltip confirms that the reported data was collected over the previous 24 hours. (#32290)

- Insight includes a new report template, **Unique Failed Authentication**. This report allows you to view detailed statistics based on unique authentication failures. (#32613)

- Insight includes two new authentication alert templates, **RADIUS Failed Authentication** and **WebAuth Failed Authentication**. You can select multiple filter options within these templates to customize these alert conditions. (#34630)

- Report configurations can be exported and imported between ClearPass servers. To export a report definition, select the report on the **Reports > Configuration** page, and then click the export (∧) icon to the right of the report name. To import a report, navigate to the **Reports > Configuration** page and click **Import Report**. (#35234)

- The Insight **Reports > Configuration** page allows you to select multiple reports to bulk export several report definitions at once in a single export file. If you import a report definition file that contains multiple report definitions, Insight will update to include all definitions within that file and will display a status message showing which report definitions were added or updated. (#40591, #40592)

- Starting with ClearPass 6.7.0, you can upload a custom report template using the **Import** option at **Reports > Custom Reports**. To create a new report based on a custom report template, navigate to **Reports > Configuration** and select the **Custom** option in the **Category** drop-down list. Log files for custom template events appear on the **Administration > Custom Reports** page of the Insight user interface. (#35253, #40595)

- If you upload a report definition that uses an existing custom report template with the same name, Insight displays an alert to warn you that the template name already exists, and that uploading a new report will overwrite the previous uploaded custom report configuration. (#35253, #40596)

- Most Insight reports allow you to use the **Service** filter to filter the report contents by service type. This feature is available in all reports *except* the following: (#37620)

  - System > Events
  - Guest Authentication > Guest Devices - Expired
  - Guest Authentication > Guest – User and Device Expired
  - Guest Authentication > Guest – Users Expired
  - Licensing > License Usage
  - Onboard > Onboard Certificate

- Onboard > Onboard Enrollment
- The following Insight reports now include information about authentication methods in the report output in CSV format. (#37771)

Table 13: *Reports with Authentication Source Information*

Report Category	Report Name
Authentication	Auth Overview Auth Trend Auth by AuthSrc Auth by ClearPass Failed Auth
Guest Authentication	Guest - Auth Overview Guest - Auth Trend Guest - Auth by ClearPass Guest - Hotspot Guest - Social Login
RADIUS Authentication	RADIUS - Auth Overview RADIUS - Auth Trend RADIUS - Auth by AuthSrc RADIUS - Auth by ClearPass RADIUS - Failed Auth
Network	Auth by NAD Guest - Auth by NAD RADIUS - Auth by NAD
TACACS	TACACS- Authentication

- ClearPass 6.7.0 introduces an **Inventory** page that lists all authenticated endpoints on the network. View inventory information for all endpoints by navigating directly to **Insight > Inventory**, or click a graph widget on the **Endpoints**, **Posture** or **Authentication** Insight dashboards and drill down to display inventory data related to that graph. Click any column heading in the **Inventory** table to re-sort the table by that column data type, or click the filter (▽) icon and select one or more filter options to display only selected endpoint types. You can also select any MAC address in the **Inventory** table to display an **Endpoint Details** page with detailed information about that specific device. (#38627)

- The **Endpoint Details** page appears when you select any MAC address in the **Inventory** table, or when you enter and search for a search string in the Insight search bar. This page is enhanced in ClearPass 6.7 to display additional authentication details such as endpoint role and policy enforcement information, and the current endpoint authentication status. If the endpoint is a switch, this page lists all the devices connected to that switch, as well as the port information for those connected devices. (#38628)

- To regenerate an updated version of an existing report definition, click the run (▶) icon beside any report definition on the **Reports** or **Reports > Configured Reports** pages. (#38629)

- The Insight Dashboard includes a new **Dashboard > Licensing page** that displays the current Access, OnGuard, and Onboard license usage over the previous 15 minutes and previous 24 hours, and the maximum usage for these license types in the previous day, week, or month. This dashboard replaces the **System** dashboard available in previous releases. The **Top 10 Restarted Services** graph is now moved to the **System Monitor** dashboard. **The System > License Usage** reports are deprecated, and are replaced with a new **Licensing > License Usage** report. This report includes the following licensing information: (#39222, #39766, #41405)

- License statistics, including the total number of licenses, and the number of licenses used for each license type.

- Number of unique endpoints on the network over the selected time period.

- Number of ClearPass Access licenses used over the selected time period.

- Number of ClearPass Guest licenses used over the selected time period.

- ClearPass licenses distribution (available vs used.)

- ClearPass license usage per host.

Onboard

Features Added in 6.7.0

- In the ClearPass Onboard EST server, support was added for username-and-password HTTP authentication and proof of possession (tls-unique). When this option is selected, the username and password must match a guest account. To use this feature, go to **Onboard > Certificate Authorities**, view a CA in the list, and select the check box in the **EST Server** field to display the EST options. In the **EST Auth Method** drop-down list, select **HTTP Basic or Digest Authentication**. (#25753)

- Onboard can now be configured to merge devices that have overlapping MAC addresses. This option is set to "on" by default. To use this feature, go to **Guest > Administration > Plugin Manager**, click the **Configuration** link for the **ClearPass Onboard** plugin, and then select the check box in the **Merge Devices** field. (#27784)

- For Apple device endpoints that are created through Onboard, the **Attributes** tab at **Policy Manager > Configuration > Identity > Endpoints** now includes an **Expanded Device Type** attribute. The value shows the marketed model name that can be more easily recognized by most users, similar to that in the **Device Type** field on Onboard's **View by Device** form — for example, "iPhone 6S Plus" or "iPad Air". (#31432)

- The validity period for a certificate can now be set when you create it or import it through the Onboard user interface. To use this feature, go to **Onboard > Management and Control > View by Certificate**, and choose either **Generate a new certificate signing request** or **Upload a certificate signing request**. Complete the configuration and then select the **Approval** check box in the **Issue Certificate** area. The form expands to include the **Expiration** field, where you can enter the number of days before the certificate will expire. (#38102)

- When creating a new provisioning setting at **Onboard > Deployment and Provisioning > Provisioning Settings**, the default key type is now 2048 bits. (#40624)

OnGuard

- Support was added for the following products: (#36574, #43215)

  - Avast Free Antivirus 17.6 (Windows)

  - Avast Mac Security 13.x (macOS)

  - AVG AntiVirus Business Edition 16.x (Windows)

  - BullGuard Internet Security 17.1.x (Windows)

  - Comodo Disk Encryption 1.2.114847.152 (Windows)

  - ESET Internet Security 11.x (Windows)

- F-Secure Anti-Virus 17.x (Windows)

- F-Secure Client Security 13.x (Windows)

- F-Secure Computer Protection 17.1 (macOS)

- F-Secure Internet Security 17.x (Windows)

- G DATA Security Client (macOS)

- Kaspersky Anti-Virus 18.x (Windows)

- Kaspersky Endpoint Security 10.2.x (Windows)

- Kaspersky Internet Security 18 (Windows)

- Malwarebytes Anti-Malware Enterprise 1.80.2.1012 (macOS)

- Malwarebytes Anti-Malware Premium 3.x (Windows)

- McAfee Endpoint Security 10.5.3 (Windows)

- McAfee LiveSafe 16.x (Windows)

- McAfee Total Protection 16.0.3 (Windows)

- McAfee VirusScan 20.3.169 (Windows)

- Sophos Anti-Virus 11.x (Windows)

- Symantec Endpoint Protection Cloud 22.11.2.7 (Windows)

- Trend Micro Maximum Security 12.x (Windows)

- Trend Micro Titanium 12.x (Windows)

- Webroot SecureAnywhere 9.0.17.28 (Windows)

Support was enhanced for the following products:

- AVG AntiVirus Business Edition 14.x (Windows)

- AVG AntiVirus Free Edition 17.9.3040 (Windows)

- AVG internet Security 17.x (Windows)

- Bitdefender Antivirus Free Edition 1.0.5.12 (Windows)

- Bitdefender Internet Security 2018 (Windows)

- BullGuard Internet Security 18.x (Windows)

- Cisco Advanced Malware Protection for Endpoints (Windows)

- ESET Endpoint Antivirus 6.5 (Windows)

- F-PROT Antivirus for Windows 6.0.96 (Windows)

- F-Secure Computer Protection (Windows)

- FileVault 10.13.x (macOS)

- GFI LanGuard 12.x (Windows)

- Kaspersky Internet Security 17.x (Windows)

- McAfee Endpoint Security (Windows)

- McAfee Total Protection 18.0.9019 (Windows)

- Mac OS X Built-in Firewall 10.13 (macOS)

- Microsoft Security Essentials (Windows)

- Norton AntiVirus 22.x (Windows)

- Norton Internet Security 22.x (Windows)

- Norton Security 22.11.0.41 (Windows)

- Norton Security Scan 4.x (Windows)

- Norton Security Suite 22.x (Windows)

- Software Update 10.13.x (macOS)

- Sophos Endpoint Security and Control 10.7.2 (Windows)

- Symantec Encryption Desktop 10.3.2 (Windows)

- Symantec Endpoint Protection 14.x (macOS)

- Symantec Endpoint Protection 14.x (Windows)

- Symantec Endpoint Protection Cloud (Windows)

- Trend Micro Full Disk Encryption (Windows)

- Trend Micro Internet Security 12 (Windows)

- Trend Micro OfficeScan Client (Windows)

- Trend Micro OfficeScan Client 11.0.x (Windows)

- Trend Micro Security 3.x (Windows)

- Trend Micro Titanium Maximum Security (Windows)

- Trend Micro Worry-Free Business Security Agent 19.0.2166 (Windows)

- Support was added for the following operating systems: (#35938, #38603)

  - Windows Server 2016

  - Ubuntu 16.04 LTS

Features Added in 6.7.2

- Users can now configure a maximum timeout value for OnGuard remediation scripts to run. A new attribute, **Script Execution Timeout (Seconds)**, is added to the **Agent Script Enforcement** profile. When a time is configured for this attribute, the ClearPass OnGuard Unified Agent waits the specified number of seconds for a custom script to finish execution. If the custom script's execution is not completed within that time, the OnGuard Agent returns a failure for the script. If this attribute is not configured, OnGuard uses the default value of 20 minutes if the Custom Remediation user interface is enabled, or one minute if the Custom Remediation user interface is not enabled. To use this feature, go to **Policy Manager > Configuration > Enforcement > Profiles > Add** and select **Agent Script Enforcement** as the template. On the **Attributes** tab, add the **Script Execution Timeout (Seconds)** attribute and enter a number of seconds for the value. The minimum allowed value for this attribute is 60 seconds (one minute), and the maximum allowed value is 3600 seconds (60 minutes). (#42172)

- A new attribute in OnGuard Global Agent Settings lets you specify a VPN adapter (device) name and categorize the network interface as a VPN on macOS. To use this feature, go to **Administration > Agents and Software Updates > OnGuard Settings > Global Agent Settings**, add the **VPN Device Names (macOS)** parameter, and enter a device name as the value. As part of this feature, the name of the similar attribute for windows is now changed from "VPN Device Names (Windows only)" to "VPN Device Names (Windows)". (#43494)

- ClearPass now supports standalone installations of VIA 3.x and of the OnGuard Agent. This allows administrators to use VIA 3.x functionality that is not yet available in the Unified Agent in conjunction with

the OnGuard Agent. This feature is supported by OnGuard 6.7.2 and higher and by VIA 3.2.2 and higher. This feature is available only for the Windows OS. To use this feature: (#43537)

- OnGuard must be installed by passing the AllowBothVIAAndOnGuard flag to the installer in the following format:

  ClearPassOnGuardInstall.exe /AllowBothVIAAndOnGuard=1
  msiexec /i ClearPassOnGuardInstall.msi ALLOWBOTHVIAANDONGUARD=1

  Both OnGuard and VIA must be installed with this flag in order for them to co-exist on the same system. If either of them is installed without this flag, the other cannot be installed.

- In addition, VIA must be installed with the ALLOWBOTHVIAANDONGUARD flag in the following format:

  msiexec /i Aruba-VIA-3.2.0.0.XXXXX-64(86).msi ALLOWBOTHVIAANDONGUARD=1

Users should be aware that if the ClearPass OnGuard Unified Agent is installed with **AllowBothVIAAndOnGuard=1**, then it will not enable the VPN component even if it is enabled in the ClearPass user interface. In other words, the ClearPass OnGuard Unified agent will run in OnGuard-only mode even if the **Administration > Agents and Software Updates > OnGuard Settings > Installer Mode** option is set to **Install and enable Aruba VIA component**.

Features Added in 6.7.1

- The ClearPass OnGuard Persistent Agents and Native Dissolvable Agents for macOS and Ubuntu now support automatic updates for the OnGuard Agent Library Updates. (#41955, #42301)

The OnGuard Agent and services will be restarted approximately 30 seconds after installing an OnGuard Agent Library Update.

Features Added in 6.7.0

- The ClearPass OnGuard Unified Agent for macOS and for Ubuntu now supports running OnGuard as a service in order to run system health checks. To use this feature, go to **Administration > Agents and Software Updates > OnGuard Settings > Global Agent Settings**. Add the **Run OnGuard As** parameter, and then set the value to **Service**. (#19599)

- Health status log entries in the Windows Event Viewer are enhanced to include additional network information. The ClearPass OnGuard Agent for Windows now adds entries for network interface details such as the wireless SSID, device driver information, and more. In these logs, the following Event IDs are used for the different OnGuard modules: (#33839)

  - Agent Controller Service = **1035**
  - OnGuard Plugin = **1036**
  - OnGuard Agent Service = **1037**

The ClearPass OnGuard Agent for Windows now also sends two new attributes in WebAuth requests. These attributes are also available in service rules for service categorization and role mapping:

- **Host:SSID** — This attribute contains the name of the wireless SSID, and is applicable only for wireless interfaces.

- **Host:InterfaceDriver** — This attribute contains the device driver details of the network interface in the following format: **<Driver Provider>, <Driver Version>, <Driver Date>**

The ClearPass OnGuard Agent for Windows also sends the device driver details of each active network connection to the Network Connections health class.

- A **Broadcast Notification** link is now added to the **OnGuard Activity** page. This option allows administrators to send bounce or restart session notifications to every connected OnGuard Agent. A custom message can be included with the notifications. To use this feature, go to **Monitoring > Live Monitoring > OnGuard Activity** and click the **Broadcast Notification** link. In the **Action** area of the **Broadcast Notification to Agents** window, to have the OnGuard Agent bounce the network interface, select **Bounce**. To have the OnGuard Agent restart the session in order to perform authentication and health checks again, select **Restart Session**. Complete the other fields as needed, and then click **Send Notification**. As part of this feature, the **Bounce** button on the **OnGuard Activity** list is now renamed to **Send Notification**, and lets you apply the same notification options to one or more endpoints you select in the list. (#34051, #40742)

- A new attribute in OnGuard Global Agent Settings lets you specify a VPN adapter (device) name and categorize the network interface as a VPN. To use this feature, go to **Administration > Agents and Software Updates > OnGuard Settings > Global Agent Settings**. Add the **VPN Device Names (Windows Only)** parameter and enter a device name as the value. This feature is only available for Windows. (#34082)

- The ClearPass OnGuard Agent now sends the **Host:MachineType** attribute in WebAuth requests. This attribute can be used to differentiate between laptops and desktops. Possible values are: **Desktop**, **Laptop**, **VirtualMachine**, **Server**, **Other**, and **Unknown**. This attribute is also available in service rules for service categorization and role mapping, and is supported on both Windows and macOS. (#37651)

- OnGuard modules, including detection libraries for client programs (V4 SDK), can now be upgraded without having to upgrade your ClearPass or OnGuard installations. To support this feature, "OnGuard Agent Library" update patches with new versions of the detection library/SDK will be released periodically. When they are released, the OnGuard Agent Library update patches will be available on the **Software Updates** page under **Firmware & Patch Updates**. When a new version of an OnGuard Agent Library patch is installed, it is immediately available in **OnGuard Settings**. OnGuard Agents can be configured to install the update automatically, or administrators may install them manually instead. The OnGuard Agent Library update patches are also available on the Support site for offline updates through the CLI. (#39448)

  OnGuard Agent Library update patch versions are independent of ClearPass and OnGuard versions, so newer versions of OnGuard Agent Library update patches can be installed on older versions of ClearPass. This feature is available for both the persistent and dissolvable agents, and for Windows, macOS, and Ubuntu operating systems.

  To enable auto-update of the OnGuard Agent Library, go to **Configuration > Enforcement > Profiles** and configure an **Agent Enforcement** profile with the new attribute **Enable to auto update OnGuard Agent Library** set to **true**.

  As OnGuard Agent Library update files become available, the files for the various operating systems are listed on the new **OnGuard Settings > Installers** tab. Administrators can download these files for manual installation or to push via Patch Management applications such as SCCM.

- Users should be aware that the OnGuard Plugin Version 1.0 (V3 SDK) is now deprecated. In ClearPass 6.7.0, only Plugin Version 2.0 (V4 SDK) is used by the OnGuard Agents to collect health. Plugin Version 2.0 is now supported on Windows, macOS, and Ubuntu, and in posture policies for Linux. After you upgrade to ClearPass 6.7.0, OnGuard will use the V4 SDK by default for all new policies. (#40372, #40397, #41098)

  As part of this change, any existing policies that were configured for the V3 SDK must be reconfigured to use the V4 SDK. To help administrators migrate from OnGuard Plugin 1.0 to OnGuard Plugin 2.0, ClearPass now automatically converts existing Plugin 1.0 posture policies to Plugin 2.0 posture policies. If a product that was configured in Plugin 1.0 has a different name in Plugin 2.0, then the new policy will use the new name from Plugin 2.0. The name of the new posture policy itself will be the name of the earlier policy but

with "_PluginVersion2.0" appended to it. This migration of existing posture policies to the new Plugin 2.0 posture policies is done while restoring the backup from the earlier ClearPass version (6.6.8 and below) and upgrading to 6.7.0.

Some options that were available when using OnGuard Plugin Version 1.0 are not supported in 2.0, and some options have changed. The **Administration > Support > Documentation** page includes support information charts for both versions that you can review and compare. For more information, refer to the *Policy Manager User Guide*.

- The information on the **Administration > Agents and Software Settings > OnGuard Settings** page is now organized on two tabs. The **Settings** tab provides all the OnGuard Agent mode and customization configuration options. The **Installers** tab provides all available installer files for OnGuard and for library updates. (#42191)

Policy Manager

Features Added in 6.7.2

- The policy server will now time out if the AD/LDAP source fails to send a response to an authorization query after ten seconds. To specify a different duration for the timeout, go to **Policy Manager > Configuration > Authentication > Sources > Add**, select either **Active Directory** or **Generic LDAP** as the **Type**, and enter a value in the **Server Timeout** field. (#35646)

- ClearPass 6.7.2 includes support for a new Post-Auth v2 function to improve performance and scaling for post-authentication events when inter-operating with third-party systems. To enable this feature: (#38977)

  1. First configure the new **Post-Auth v2** cluster-wide parameter. The default setting for this parameter is disabled. Go to **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters**. On the **General** tab, scroll down to the **Post-Auth v2** parameter and change the value to **Enable**, and then click **Save**.

  2. Next, whenever you either enable or disable **Post-Auth v2**, you must also manually restart the **Async network services** service. Go to **Administration > Server Manager > Server Configuration** and double-click the appropriate ClearPass appliance. On the **Services Control** tab, click **Stop** and then click **Start** in the **Async network services** row, and then click **Save**.

  Users should be aware that in this initial release of the Post-Auth v2 feature, there are some restrictions:

  - ClearPass Proxy is not supported.

  - IPv6 is not supported.

  - When defining a Context-Server-Action, only the following HTTP methods are supported: POST, GET, and PUT.

> **NOTE:** This initial release of Post-Auth v2 only includes support for Palo Alto integrations. Future software releases will add support for Generic HTTP Context-Servers.

- A new cluster-wide parameter, **Content Security Policy (CSP)**, is added to the **Administration > Server Manager > Server Configuration > Cluster wide parameters > General** tab. When this parameter is enabled, it helps reduce cross-site scripting (XSS) risks in browsers by declaring which dynamic resources can be loaded via an HTTP Header. The default setting for this parameter is Disable. Users should be aware that when this parameter is enabled, it can negatively affect any customized HTML they might have for skins, captive portals, self-registration workflows, and so on in ClearPass Guest. If your configurations include customized HTML for items such as these that reference images, media, scripts, or other resources on

servers outside ClearPass, you should either not enable the CSP parameter or use a different approach for accessing these resources. (#42528)

- ClearPass now supports the following secured cipher suites using Active Directory as an authentication source: (#43264)

  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384

  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384

  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384

  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256

  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256

  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA256

  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA

  - TLS_RSA_WITH_AES_256_CBC_SHA256

  - TLS_RSA_WITH_AES_256_CBC_SHA

- Prompt notifications are now displayed in the user interface if license usage is exceeded: (#43545)

  - As license usage is calculated every 15 minutes, the information banner on the **Dashboard** page is immediately updated with a message if the license limit for the appliance has been exceeded. The message is removed when the usage falls within the license limit again. No banner messages are posted for CLABV systems or for systems running in evaluation mode or with evaluation licenses.

  - Messages are also posted in the **Event Viewer** every 15 minutes for each ClearPass application that exceeds its license limit. **Event Viewer** messages state the number of licenses purchased and the current usage by application. When the appliance falls within the license limit again, the **Event Viewer** includes a message to this effect. For CLABV systems or for applications running under an evaluation license, **Event Viewer** messages are not posted at 15-minute intervals but are instead posted once each night at 11:55 PM.

Features Added in 6.7.1

- A new cluster-wide parameter, **Allow Concurrent Admin Login**, is added to the **Administration > Server Manager > Server Configuration > Cluster wide parameters > General** tab. (#42158)

  - When this parameter is set to **FALSE**, if a user logs in to a new session but earlier sessions for the same credentials are still active on other appliances, all earlier sessions will automatically be logged out. In the new session, the message "You have been logged out of previous active session(s)" is displayed.

  - When this parameter is set to **TRUE**, a user will be able to log in to concurrent sessions on different appliances. The default value for the **Allow Concurrent Admin Login** parameter is **TRUE**.

- As part of IPv6 support for SNMP targets, IPv6 addresses are now supported in trap receivers. To use this feature, go to **Administration > External Servers > SNMP Receivers > Add** and enter an IPv6 address in the **Host Address** field. This field now accepts IPv6 and IPv4 addresses. (#43401, #42693)

Features Added in 6.7.0

- ClearPass admins now have the option to configure an external TACACS server to use as an authentication source when they log in to the ClearPass UI. The remote TACACS server's IP address and shared secret must be supplied, and some information must also be configured on the remote TACACS server. (#16107)

  As part of this feature, two new cluster-wide parameters were added: **Admin UI Remote TACACS Server Shared Secret** and **Admin UI Remote TACACS Server Shared Secret**. To use this feature:

  - On the local ClearPass server, configure the external TACACS server in the new cluster-wide parameters. Go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > TACACS** tab. Enter the values for the remote server's IP address and shared secret in the parameters (the shared secret will be encrypted).

  - On the remote TACACS ClearPass server, add the local server as a Network Access Device, configure the users with the appropriate roles, configure an enforcement profile and policy, and then create the server and associate the policy with it. The enforcement profile should have a privilege level of **15 (Privileged)**, and include a service attribute of type **cpass:HTTP** and the name **AdminPrivilege**.

- ClearPass now supports nested attributes in a JSON response from an HTTP authorization source. (#25460, #35387)

- A new cluster-wide parameter lets administrators configure the syslog batch-messaging interval as needed to values from 30 seconds up to 120 seconds. The interval is applied to all appliances in a cluster, and to all the syslog export filters that are enabled. To use this feature, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab and enter a value between 30 and 120 for the **Syslog Export Interval** parameter. (#26265)

- The Alcatel-Lucent Enterprise RADIUS dictionary is now updated with five new attributes: (#27504)

  - Alcatel-End-User-Profile

  - Alcatel-Nms-Group

  - Alcatel-Nms-First-Name

  - Alcatel-Nms-Last-Name

  - Alcatel-Nms-Description

- ClearPass now supports valid JSON types such as Integer, boolean, array, and object in HTTP authorization sources. (#28127)

- SPAN ports can now be enabled for all hardware and virtual appliances that have more than two network interface cards (NICs). The SPAN port will be available in the **Administration > Server Manager > Server Configuration > System** tab's **SPAN Port** drop-down list. (#28232)

- The IPv6 protocol is now supported for IPsec connections between ClearPass and external authorization or authentication sources such as Active Directory (AD), Generic HTTP, MSSQL, MariaDB, OpenLDAP, Oracle, and PostgreSQL, and RADIUS IPv6. As part of this feature: (#28861, #38614, #39305, #39546, #39548, #39564, #39565, #39566, #40239, #41257)

  - IPv6 address formats are supported for Virtual IPs, for IPsec tunnels, in the hostname property in authentication sources, in event sources, in NTP and DNS server configurations, and in endpoint context servers' server name and URL fields. IPv6 addresses are formatted as eight groups of four hexadecimal digits, each representing 16 bits, and separated by colons — for example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

  - When configuring a Virtual IP for ClearPass High Availability, the **Administration > Server Manager > Server Configuration > Virtual IP Settings** window now includes a **Select IP version** field, where you can specify either IPv4 or IPv6 for the VIP used for automatic failover. When IPv6 is selected, the

Primary Node and **Secondary Node** drop-down lists are populated with the corresponding IPv6 addresses for selection. To add an IPv6 address as a Virtual IP, it must be in the same subnet as the primary and secondary nodes.

- When creating an IPsec tunnel on the **Administration > Server Manager > Server Configuration > Network** tab's **Create IPsec Tunnel** form, IPv6 addresses are now available in the **Local Interface** drop-down list, and can be specified as the remote IP. (The local interface and remote IP must either both be IPv4, or both be IPv6.)

- In post-authentications, when a client acquires an IPv6 address, ClearPass will notify the endpoint context server of the new value.

- TACACS authentications are supported for IPv6-based databases as authentication sources.

- ClearPass can post data to the IPv6 interface of an endpoint context server.

- When configuring an HTTP proxy server on the **Administration > Server Manager > Server Configuration > Service Parameters** tab, IPv6 HTTP-proxy addresses are now supported for sending data to third-party context servers.

- ClearPass can receive and process syslog messages from event sources with IPv6 addresses.

● This release introduces several enhancements for certificate management: (#28911, #30496, #38227, #39482, #40724, #41755)

- ClearPass now supports multiple RADIUS server certificates, and allows you to map a different RADIUS server certificate to each ClearPass RADIUS service. The **Create Self-Signed Certificate** form and the **Import Certificate** form let you configure a new certificate as either a **Server Certificate** or a **Service Certificate** . For service certificates, only RADIUS certificates are allowed.

- At **Administration > Certificates**, the **Server Certificates** page is renamed **Certificate Store**, reflecting its purpose as one location to manage both server certificates and service certificates. Information on the **Certificate Store** page is organized in a **Server Certificates** tab and a **Service Certificates** tab.

- New options are available when importing a server certificate, and support is added for importing certificate files in PKCS#12 format. Certificate export behavior is also changed. Now during the import, instead of being required to download and store the private key along with the certificate file, users can choose one of three upload methods. These options are available for both RADIUS and HTTPS server certificate types. As part of this feature, certificate exports now use only the PKCS#12 format. When you click the **Export** button, an **Export to file** dialog opens where you can provide the secret key. To use this feature, at **Administration > Certificates > Certificate Store > Import Certificate**, choose one of the following options:

  - **Upload Certificate and Use Saved Private Key**: This option allows the user to upload only the certificate, and it is matched against the private key saved on their system.

  - **Upload PKCS#12 Certificate (.pfx or .p12 only)**: With this option, the user uploads the PKCS#12 file and provides a passphrase.

  - **Upload Certificate and Private Key Files**: This is the same method that used to be required, but it is now optional. The user can still choose to upload the private key file and password along with the certificate file.

- At **Configuration > Services**, the **Authentication** tab for a service has a new **Service Certificate** drop-down list that includes all available service certificates. The certificate details can be viewed. If no selection is made in this field, the default RADIUS server certificate will be used.

- User actions such as adding, modifying, deleting, importing, or exporting certificates, or assigning service certificates, are now logged.

- A Xirrus RADIUS dictionary is now added, and includes the vendor-specific attribute **Xirrus-Admin-Role**. (#28928)

- The **System Monitor** page now includes CPU and memory-usage data for the IPsec service. To use this feature, go to the **Monitoring > Live Monitoring > System Monitor > Process Monitor** tab and select **ClearPass IPsec service** as the process. (#31113)

- Users can now include a description for each IP address entry in a static host list. To use this feature, go to **Configuration > Identity > Static Host Lists** and open a list to edit. In the **Host Entries** area, use the **Description** field below the **Address** field when you add or edit a host. (#31369)

- The maximum number of characters allowed for URLs in the Context Server Actions dictionary is now increased from 255 to 4000 characters. To use this feature, go to the **URL** field on the **Administration > Dictionaries > Context Server Actions > Action** tab. (#33068)

- Four new OIDs are added to the cppmServerInfoGroup of the cppmSystemTable of the Clearpass Management Information Base (CPPM-MIB). These OIDs allow users to monitor the fan, power, and disk status of HP 5K (C2000) and 25K (C3000) hardware appliances using SNMP get/walk. This feature enables sending hardware traps in the event of a fan, power, or disk failure in a hardware appliance. This feature supports SNMP v1, v2, and v3 queries. This feature is not available for the 500 hardware appliance (c1000), and is not available for virtual appliances. The OIDs are described in the table below: (#33403, #42859)

Table 14: *Hardware Monitoring OIDs*

Name	OID	Description
cppmHardwareFanStatus	.1.3.6.1.4.1.14823.1.6.1.1.1.1.1.19	**Fan Status**
cppmHardwarePowerStatus	.1.3.6.1.4.1.14823.1.6.1.1.1.1.1.20	**Power Status**
cppmHardwarePowerStatusDetails	.1.3.6.1.4.1.14823.1.6.1.1.1.1.1.21	**Power Status Details**
cppmHardwareDiskStatus	.1.3.6.1.4.1.14823.1.6.1.1.1.1.1.22	**Disk Status**

> ⚠️ **CAUTION**
>
> Users should be aware that ClearPass obtains the underlying hardware configuration from the dmidecode system manufacturer property. If the vendor details are not correctly set under system-manufacturer, ClearPass will assume that the underlying configuration is not the corresponding HP hardware box, which would lead to incorrect installation and setup of this feature. For a C1000 hardware appliance or a virtual appliance, these OIDs would return N/A as the value.

- The **Failover Wait Time** cluster-wide parameter now accepts values from 3 minutes to 60 minutes. To use this feature, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Standby Publisher** tab and enter a value in the **Failover Wait Time** field. The default value is ten minutes. (#33563)

- As part of security enhancements, the Policy Manager Admin Network Login Service, used to process network-based authentications for ClearPass apps, is now disabled by default. (#34374)

- A network device's name can now be used instead of its subnet/IP address for adding the device to a device group in list format. To use this feature, go to **Configuration > Network > Device Groups** and add or edit a group. In the **Format** area select **List**, and then enter or filter for the device by either its name or its subnet address. (#34690)

- Policy Manager self-signed server certificates are now signed by the SHA-2 signature algorithm. (#34854)

- Three new SNMP OIDs in the policyServerTable of the ClearPass Management Information Base (CPPM-MIB) show the total number of authentications on the ClearPass server for the previous day.

Authentication counts are calculated over a duration of one 24-hour calendar day — in other words, from 00:00:00 through 23:59:59 each day. If polls are done several times a day, by subtracting a previous poll's count from the latest poll's count the number of authentications within a polling interval can be calculated. The OIDs are described in the following table: (#35014)

Table 15: *Authentication Count OIDs*

Name	OID	Description
dailySuccessAuthCount	.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.17	Daily total number of successful authentications
dailyFailedAuthCount	.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.18	Daily total number of failed authentications
dailyTotalAuthCount	.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.19	Daily total number of authentications

- When importing a Network Access Device (NAD) at **Configuration > Network > Devices > Import**, an existing device can now be updated based on its IP address even if the device name has changed. (#35660)

- For Technical Assistance Center (TAC) engineers, remote access connections now use only @hpe.com email addresses instead of @arubanetworks.com email addresses. The TAC engineer must enter only the user ID part of the address in the **HPE Support Contact** field, and the @hpe.com part of the address is auto-completed. (#35960)

- For RADIUS authentications, ClearPass now supports XXXX-XXXX-XXXX as a valid MAC address format in the Calling-Station-ID. (#36242)

- A new CLI command is introduced in 6.7.0 for performing a cluster diagnostics operation. The **cluster diagnostics** command helps users understand the throughput, ping latency, DB connectivity, and configured interface Maximum Transmission Units (MTU), and check whether there is a minimum path MTU (1400) between the nodes being tested. (#36918)

- ClearPass now supports DNS caching. To use this feature, go to **Administration > Server Manager > Server Configuration** and select a server in the list. In the **DNS Settings** area of the **System** tab, click **Configure**. Select the **Enable DNS Caching** check box, and then click **Update**. DNS caching is disabled by default. (#37077, #40236)

- A new default attribute, **Device Role ID**, is available for the [Guest Device Repository] authentication source. This attribute gets the assigned role information from a ClearPass device registration, making it available to use for authorization in 802.1X and MAC authentication workflows. (#37302)

- To provide information about the most recent posture information ClearPass processed for an endpoint, a **Posture Info** tab is now added to the **Agent and Endpoint Details** window. To use this feature, go to **Monitoring > Live Monitoring > OnGuard Activity** and select an endpoint's row in the list to open the details window. On the **Posture Info** tab, review the information in the **Posture Request**, **Posture Response**, **Posture Evaluation Results**, and **Application Response** areas. (#37786)

- Six Google Trust Services certificates have been added to the ClearPass certificate trust list at **Administration > Certificates > Trust List**. These certificates are disabled by default: (#38253)

  - GTS Root 1

  - GTS Root 2

  - GTS Root 3

  - GTS Root 4

  - GlobalSign Root CA - R2

- GlobalSign ECC Root CA - R4

- ClearPass can now be deployed on the Amazon Web Services (AWS) cloud-hosting service, or Virtual Private Cloud (VPC). This feature frees customers from having to maintain any physical or virtual server infrastructure, but still allows them to use their VPN to maintain network connectivity and security as though the system were local. For more information, see the *Tech Note: Installing ClearPass 6.7 on Amazon Web Services*. (#38279, #40379)

  When ClearPass is hosted on AWS, users should be aware of the following differences:

  - In server configuration, editing is disabled for the management port IP address, subnet mask, default gateway, data port IP address, subnet mask, and default gateway.

  - Virtual IP settings and SPAN port settings are hidden.

  - In service parameters, HTTP proxy settings are hidden.

  - FIPS mode cannot be enabled.

  - In the footer of the Policy Manager user interface, the indicator "[Cloud]" is included after the version number.

- A **RADIUS CoA Templates** dictionary is now added, allowing users to add or update custom Change of Authorization (CoA) and Disconnect Message (DM) dictionaries for specific vendor IDs. (#38483)

- The **Event Viewer** now includes entries for all export and import operations. Any configuration items that can be imported or exported, such as services, enforcement profiles, endpoints, devices, and so on are logged. The user, role, and event description are also included in the event details. (#38505)

- In **Configuration > Enforcement > Profiles**, the **Aruba Downloadable Role Enforcement** profile now lets you specify whether the product is the ArubaOS-Switch, Mobility Access Switch (MAS), or Mobility Controller. As part of this feature: (#39571, #40802, #40803, #41237)

  - In **Standard** mode, the **Role Configuration** tab includes only the options that are appropriate for the selected product.

  - Support was also added for class configuration for the ArubaOS-Switch, and the **Role Configuration** tab includes a **Manage Classes** link and an **Add Policy** link when this product is selected. Traffic classes can be created and configured and the policy can be mapped to them.

  - Enforcement profiles can be imported or exported.

  - Events are logged in the **Audit Viewer** for create, update, and delete operations in the captive portal, policy, and class configurations. Events are also logged for generated user roles and import/export operations in enforcement profiles.

- ClearPass now supports SNMP enforcement profiles for event-based enforcement. This feature allows administrators to enforce SNMP actions on the ClearPass Ingress Event Engine. (#39585)

- The strength of the encryption technique used by the Technical Assistance Center (TAC) to generate support and recovery keys is greatly increased, and the CLI commands "system gen-support-key" and "system gen-recovery-key" are enhanced to make privileged access more secure. The commands use the TAC Support engineer's email ID and output a token, which can then be used by the engineer to generate a password for privileged access. (#39643)

- You can now use the **Application Access Control** option in the ClearPass user interface to restrict access to the CLI, eliminating the need to configure an internal firewall to restrict CLI access. To use this feature, go to **Administration > Server Manager > Server Configuration** and select the server. On the **Network** tab, click the **Restrict Access** button in the **Application Access Control** field, and then select **CLI** in the **Resource name** drop-down list. (#39667)

- Starting with the 6.7.0 release, the names of the ClearPass virtual appliance types and hardware appliance types have changed, as shown in the following table: (#39899)

Table 16: *New ClearPass Appliance Names*

New Name	Previous Name	Description
CLABV	CP-SW-EVAL	Evaluation version
C1000V	CP-VA-500	500 virtual appliance
C2000V	CP-VA-5K	5K virtual appliance
C3000V	CP-VA-25K	25K virtual appliance
C1000	CP-HW-500	500 hardware appliance
C2000	CP-HW-5K	5K hardware appliance
C3000	CP-HW-25K	25K hardware appliance

- ClearPass now natively supports mariadb-connector-odbc to be compatible with MySQL. MariaDB can be selected as an ODBC Driver when configuring an authentication source. (#40212)

- A new vendor-specific attribute, **HPE-CPPM-Secondary-Role (28)**, was added for the ArubaOS-Switch in Aruba downloadable role enforcement profiles. This attribute adds support for a downloadable secondary role that can be used with Per User Tunneled Node (PUTN). When the attribute is added to the profile, ClearPass can send the controller role for the ArubaOS-Switch. To use this feature, go to **Configuration > Enforcement > Profiles > Add**. Select **Aruba Downloadable Role Enforcement** as the template and **ArubaOS-Switch** as the product, and then select **Advanced** for the role configuration mode. On the **Attributes** tab, add an attribute of type **Radius:Hewlett-Packard-Enterprise**, and then select the new attribute named **HPE-CPPM-Secondary-Role (28)**. (#40350, #40799)

- Controller static roles and controller downloadable roles for the ArubaOS-Switch can now be configured as secondary roles in enforcement profiles in standard mode. To use this feature, go to **Configuration > Enforcement > Profiles > Add** and select **Aruba Downloadable Role Enforcement** in the **Template** field. Next, in the **Role Configuration Mode** field select **Standard**, and then select **ArubaOS-Switch** in the **Product** field. Then on the **Role Configuration** tab: (#40842)

  - To configure a static role, select **Static** in the **Secondary Role Type** field. The **Controller Static Role** field is displayed.

  - To configure a downloadable role, select **Dynamic** in the **Secondary Role Type** field. The **Controller Downloadable Role** field is displayed. Select any profile name for the product **Mobility Controller**.

- An **Ingress Events** dictionary is now added, supporting syslog integration with ClearPass IntroSpect. (#40948)

- The default RADIUS change of authorization (CoA) customizable templates and their related enforcement profiles now have new names to match the new product names. The enforcement profiles' descriptions are also enhanced to be more clearly descriptive. The names and descriptions are shown in the tables below. Three new CoA profiles and templates have also been added to support H3C's bounce host port, disable host port, and terminate session commands for H3C [ComWare] devices. To use this feature: (#41555, #37552)

  - To add a RADIUS CoA default enforcement profile to a policy, go to **Configuration > Enforcement > Policies > Add**, select **RADIUS** as the **Enforcement Type**, and then select one of the RADIUS CoA profiles from the **Default Profile** drop-down list.

- To add a TACACS default enforcement profile to a policy, go to **Configuration > Enforcement > Policies > Add**, select **TACACS** as the **Enforcement Type**, and then select one of the TACACS profiles from the **Default Profile** drop-down list.
- To view or import RADIUS CoA templates, go to **Administration > Dictionaries > RADIUS CoA Templates**.

Table 17: *Default Enforcement Profile Names and Descriptions*

Previous Name	New Enforcement Profile Name	New Enforcement Profile Description
Aruba Bounce Host-Port	**ArubaOS Wireless - Bounce Switch Port**	System-defined profile to bounce the switch port on ArubaOS Mobility Controllers, Multi-Port APs & Mobility Access Switches.
Aruba TACACS read-only Access	**ArubaOS Wireless - TACACS Read-Only Access**	System-defined profile for TACACS read-only access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.
Aruba TACACS root Access	**ArubaOS Wireless - TACACS Root Access**	System-defined profile for TACACS root access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.
Aruba Terminate Session	**ArubaOS Wireless - Terminate Session**	System-defined profile to disconnect the user on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.
HPE Bounce Host-Port	**ArubaOS Switching - Bounce Switch Port**	System-defined profile to bounce the switch port on ArubaOS Switching products.
HPE - Terminate Session	**ArubaOS Switching - Terminate Session**	System-defined profile to disconnect the user on ArubaOS Switching, HP ProCurve and HP UWW products.
H3C - Terminate Session	**H3C - Terminate Session**	System-defined profile to disconnect the user on H3C products (including HPE FlexNetwork / Comware).
H3C - Bounce Host-Port	**H3C - Bounce Switch Port**	System-defined profile to bounce the switch port on H3C products (including HPE FlexNetwork / Comware).
H3C - Disable Host-Port	**H3C - Disable Switch Port**	System-defined profile to disable the switch port on H3C products (including HPE FlexNetwork / Comware).

Table 18: *RADIUS CoA Template Names*

Previous Template Name	New Template Name
Aruba - Change-User-Role	**ArubaOS Wireless - Change User Role**
Aruba - Change-VPN-User-Role	**ArubaOS Wireless - Change VPN User Role**
Aruba - Terminate Session	**ArubaOS Wireless - Terminate Session**
Aruba - Port-Bounce-Host-Aruba	**ArubaOS Wireless - Bounce Switch Port**
Hewlett-Packard-Enterprise - Change-VLAN	**ArubaOS Switching - Change VLAN**
Hewlett-Packard-Enterprise - Change-Generic-CoA	**ArubaOS Switching - Generic Change of Authorization**

Previous Template Name	New Template Name
Hewlett-Packard-Enterprise - Port-Bounce-Host-HPE	**ArubaOS Switching - Bounce Switch Port**
Hewlett-Packard-Enterprise - Terminate-Session-HPE	**ArubaOS Switching - Terminate Session**
Hewlett-Packard-Enterprise - Change-User-Role-HPE	**ArubaOS Switching - Change User Role**
H3C - Terminate Session	**H3C - Terminate Session**
H3C - Bounce Host-Port	**H3C - Bounce Switch-Port**
H3C - Disable Host-Port	**H3C - Disable Switch-Port**

- The root certificate authority (CA) used for factory certificates on Aruba network hardware is now added to the ClearPass trust list to allow for EAP-TLS authentication of Aruba access points. (#42066)

- Two new cluster-wide parameters are added: **Automatically download Posture Signature & Windows Hotfixes Updates** and **Automatically download Endpoint Profile Fingerprints**. These parameters are disabled by default, so that ClearPass customers who do not use OnGuard or endpoint profiling will not receive automatic updates for this functionality. Customers who do use OnGuard or endpoint profiling must explicitly enable these parameters in order to receive updates, even if they received automatic OnGuard or profiling updates prior to the 6.7.0 release. To use this feature, after the publisher is upgraded to 6.7.0, go to the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General** tab and scroll to the parameters in the list. To receive automatic downloads of antivirus and hotfix signature updates, set the **Automatically download Posture Signature & Windows Hotfixes Updates** parameter value to **TRUE**. To receive automatic downloads of endpoint profile fingerprint signature updates, set the **Automatically download Endpoint Profile Fingerprints** parameter value to **TRUE**. (#42605)

Profiler and Network Discovery

Features Added in 6.7.0

- SPAN ports are now enabled to capture HTTP User Agent traffic. (#38568)

- ClearPass now supports sFlow for device profiling. As part of this feature, the name of the **Netflow Reprofile Interval** parameter on the **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Profiler** tab is now changed to **Netflow/sFlow Reprofile Interval**. (#38877, #38878)

> **NOTE**
>
> The sFlow collector listens on UDP port 6343. Firewall rules must be updated to open this port.

- ClearPass 6.7.0 introduces enhanced performance and scaling features that allow the processing load for subnet scanning and onConnect requests to be shared among other nodes in the cluster. (#39562)

  - Master Server for a Zone — A new **MasterServer in Zone** setting is added to the **Administration > Server Manager > Server Configuration > System** tab, allowing you to select a primary master and secondary master server for that zone. The master server for each zone distributes loads for various services among the Policy Manager nodes in the zone, and plays an important role in endpoint classification, OnConnect, subnet scan, and network discovery.

- Endpoint Classification — The primary master for a zone does the Endpoint classification. If the primary master is down, then the secondary master assumes the role of primary master. The **Enable Profile** checkbox available in previous releases of Policy Manager is removed from the **Administration > Server Manager > Server Configuration > System** tab.

- Subnet scan and Network Discovery — All subnet and network discovery scans should be configured for a specific zone. The primary master decides which Policy Manager node in the zone will perform the scan, the workload of which may be distributed among other available nodes in the Policy Manager zone. If the primary master is down, then the secondary master assumes the role of primary master.

- OnConnect — The **OnConnect Setting** parameter on the **Administration > Server Manager > Server Configuration > System** tab is deprecated, and is replaced by the **MasterServer in Zone** parameter on that tab.

  SNMP traps from switches (such as LinkUp and MacNotifications) should be sent to the primary and secondary master servers of the zone selected in the **Configuration > Network > Devices** page. The primary master server processes these traps and distributes requests to other nodes, which help process WMI and WebAuth information. If the primary master server is down, secondary master assumes the role of primary master.

- Default Master Server for a Zone — If no primary master is configured, the node with the lowest UUID in that zone will be marked as the primary master. A default secondary master will not be selected automatically, but if the primary master is dropped from the cluster or the zone is changed, a new default primary master is selected, based on its UUID.

- The user interface for network discovery scans and subnet scans is now reorganized so that you can access them both in the same place. To use this feature, go to **Configuration > Profile and Network Scan > Network Scan** and click the **Scan** link. The **Schedule Scan** window opens, where you can specify and configure either a **Network Scan** or a **Subnet Scan**. The scan can be either recurring or on demand. To view the progress of a current scan or results of a past scan, go to **Monitoring > Profile and Network Scan > Network Scan** (only the last 10 scans are available). As part of this feature: (#39574, #39945)

  - A daily, weekly, or hourly schedule can be configured.

  - Multiple schedules can be configured per zone.

  - A scan schedule can be enabled or disabled, effective with the next scheduled instance.

  - Scans can no longer be stopped or restarted.

- The **Read ARP table on this device check box** on the **Configuration** > **Network** > **Devices> Add Device > SNMP Read Settings** allows you to use the ARP table on a layer-3 device to discover endpoints on the network. Starting with ClearPass 6.7, information about MAC-IP pairs read from the ARP table of a switch is used to discover devices only during a periodic NAD update. SNMP, WMI, Nmap, and SSH scans are not triggered by the discovery of new MAC-IP pairs from the ARP table, which reduces the scanning load on the ClearPass server. (#40732)

- A new cluster-wide parameter enables support for NTLMV1 authentication during a WMI scan. By default, WMI scans use NTLMV2 authentication. To use this feature to enable NTLMV1, go to **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Profiler**, and in the **Enable NTLMV1 for WMI scans** drop-down list change the default **False** setting to **True**.

QuickConnect

Features Added in 6.7.2

- Onboard QuickConnect packages for Windows provisioning are now signed by Aruba. A customer-specific code signing certificate is no longer required but can still be used if necessary. The logo, title, and company name can still be customized as needed. (#41379)

The following issues were fixed in previous 6.7.x releases. For a list of issues resolved in the 6.7.3 release, see .

This chapter includes:

Fixed in 6.7.2

The following issues were fixed in the 6.7.2 release.

APIs

Table 19: *API Issues Fixed in 6.7.2*

Bug ID	Description
#44014	Corrected a filtering issue in the Endpoint API where a GET operation failed if the request included an attribute.

Endpoint Context Servers

Table 20: *Endpoint Context Server Issues Fixed in 6.7.2*

Bug ID	Description
#43632	ClearPass failed to fetch endpoints from the Google Admin Console. The access token is now refreshed if it expires during the poll.

Guest

Table 21: *Guest Issues Fixed in 6.7.2*

Bug ID	Description
#44009	In iOS 10.x, trying to install a digital pass generated for Apple Passbook failed with error messages such as "Download failed" or "Sorry, your Pass cannot be installed to Passbook at this time." The Apple Worldwide Developer Relations Certification Authority certificate is now updated and digital pass installations work correctly.
#44166	After upgrading a cluster to 6.7.1, the subscribers failed to send emails for sponsor approvals when a guest registered for an account. Subscribers now correctly send mail receipts for self-registrations.
#44208	Translation customizations that were made to a self-registration were lost if the self-registration configuration page itself was re-saved.
#44214	Corrected an issue where extensions could lose outbound network access in certain circumstances.

Table 21: *Guest Issues Fixed in 6.7.2 (Continued)*

Bug ID	Description
#44230	Certain email clients did not show the default email receipts correctly.
#44236	Using the wildcard (*****) in the **Attribute Name** field at **Guest > Administration > Operator Logins > Translation Rules > Edit** failed to validate the form and the error message "Please enter a valid attribute name" was displayed.

OnGuard

Table 22: *OnGuard Issues Fixed in 6.7.2*

Bug ID	Description
#43867	On macOS, after manually installing an OnGuard Agent Library Update patch, the Agent did not automatically quit and perform health checks or update the AgentLibraryVersion until the user clicked the **Retry** button.
#43897	The ClearPass OnGuard Unified Agent for macOS sometimes failed to detect the encryption state of drives that were encrypted using Check Point Endpoint Security 8.6.710.
#43977	On Windows OS, the ClearPass OnGuard Unified Agent sometimes could not connect to a VPN if a proxy was enabled on the browser.
#43983	ClearPass did not assign the correct Policy Manager zones to OnGuard clients. Policy Manager zones are now evaluated in ascending order of zone names.

Policy Manager

Table 23: *Policy Manager Issues Fixed in 6.7.2*

Bug ID	Description
#32951	The OpenSSH version is now updated to 7.4. This includes fixes for CVE-2015-5600, CVE-2016-6563, CVE-2016-6564, CVE-2016-8858, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, and CVE-2016-10012.
#39696	The order of the updates sent to Palo Alto Firewall was incorrect, and in some cases caused Palo Alto Firewall to not receive user IDs from ClearPass.
#41165	Old upgrade and patch update files were not removed by the manual cleanup option at **Administration > Server Manager > Server Configuration > Cleanup**. Users should be aware that the **Server Configuration > Cleanup** option does not affect upgrade or update files. Instead, when upgrade and patch update files (with extensions such as .bin, .tar, or .zip) are seven days old or older, they will be deleted by the daily cron job.
#43454	Pagination did not work properly when filtering the **Configuration > Identity > Endpoints** list and caused ordering to be erratic or some items to be duplicated in the list.
#43679	Updating from 6.7.0 to 6.7.1 while FIPS mode was enabled caused the configured user interface password to be reset to the default password (eTIPS123).
#43786	The semicolon special character (;) could not be used in pre-proxy attributes when RADIUS was used as an authentication source.
#43789	No warning was given if an enforcement profile that was still used was deleted. An error message is now displayed if the user tries to delete an enforcement profile while it is still used in an enforcement

Table 23: *Policy Manager Issues Fixed in 6.7.2 (Continued)*

Bug ID	Description
	policy or service.
#43801	Edits that were made to role names were not correctly reflected in posture policies, and added a second role name instead of updating the renamed role.
#43812	Automatic backup files could not be sent to the backup server and the error message "SCP File Transfer" was displayed if FIPS mode was enabled in ClearPass. Users should be aware that when FIPS mode is enabled in ClearPass, transferring automatic file backups to an external Windows server requires that the SFTP server be FIPS compliant. This is not an issue for file transfers done using a Linux server.
#43857	If the **system patch-rollback** command was executed over a remote SSH connection to the appadmin shell, the rollback operation sometimes failed if network connectivity issues caused the SSH session to disconnect.
#43878	The Apache Hypertext Transfer Protocol Server (HTTPd) version is now updated to 2.4.29. This includes fixes for CVE-2017-3167.
#43955	The StrongSwan version is now updated 5.6.0. This includes fixes for CVE-2017-1185.
#44058	An IPsec tunnel connection sometimes failed during reauthentication. IPsec now supports make-before-break reauthentication with remote devices. This change allows greater IPsec tunnel stability for devices that support this behavior.
#44278	This release includes fixes for a potential vulnerability described in CVE-2018-0489.
#44329	Corrected an issue with sending user IDs to Palo Alto Networks (PANW) where ClearPass did not include the domain prefix when it sent user-refresh information. ClearPass now correctly includes the domain prefix each time it sends to PANW.

Fixed in 6.7.1

The following issues were fixed in the 6.7.1 release.

APIs

Table 24: *API Issues Fixed in 6.7.1*

Bug ID	Description
#43785	Corrected an issue where trying to filter the /session API by the **update_at** field failed.

CLI

Table 25: *CLI Issues Fixed in 6.7.1*

Bug ID	Description
#31082	The CLI did not show the default gateway for IPv6, although it was displayed in the user interface. Users should be aware that in order to be reflected in the CLI, the default gateway address must be in the same subnet as the IPv6 address.

Endpoint Context Servers

Table 26: *Endpoint Context Server Issues Fixed in 6.7.1*

Bug ID	Description
#42813	ClearPass did not profile some classes of Aruba devices that were fetched through Activate. Profiling is now supported for the Aruba Switch, Aruba Controller, and Aruba Location Sensor (ALS).

Guest

Table 27: *Guest Issues Fixed in 6.7.1*

Bug ID	Description
#43240	Slow guest queries caused performance issues. Queries for guests are now optimized by MAC address, improving performance significantly for customers who have heavy traffic from a large number of guest devices.
#43406	The **Guest > Active Sessions** list showed multiple active session entries for the same session. The **Active Sessions** list now displays a single master session entry for each session instead of multiple entries for each multi-session ID. The individual multi-session IDs are displayed in the main session record. This is also updated now in the ActiveSession API.
#43410	Disabled fields such as sponsor_name or sponsor_email were not visible when editing the guest self-registration page (guest_register).
#43582	The PHP version is now updated to 7.1.13.
#43704	Email receipts could not be sent in certain ClearPass Guest workflows (for example, while importing guest accounts). The size of the background queue is now increased to accommodate larger requests.
#43770	The Extensions UI did not permit extension-related actions on a subscriber, even though those operations are permissible.
#43781	Corrected some issues with screen reader accessibility for password fields.
#43783	The Galleria skin did not display the phone number field correctly in self-registrations.
#43784	Sponsorship confirmation emails could not be sent to browsers that were set to a non-English language.
#43797	Corrected some issues with keyboard accessibility in the configuration forms at **Guest > Manage Devices** and **Guest > Manage Accounts**.
#43842	Encoded slash characters were not recognized in the ID component of the ActiveSession API URL.

Insight

Table 28: *Insight Issues Fixed in 6.7.1*

Bug ID	Description
#43246 #43573	Appliances in a ClearPass cluster went out of synchronization with the Insight servers until the **Async network services** service was restarted. This was caused by the ivconnector getting into an infinite wait mode.
#43248	The Insight endpoints table did not show the latest posture status for endpoints because an incorrectly

Bug ID	Description
	formatted MAC address in a NetEvents batch caused the entire batch to be discarded from the Insight database.

Onboard

Table 29: *Onboard Issues Fixed in 6.7.1*

Bug ID	Description
#43413	The **Onboard > Management and Control > Usage > License Usage** field still showed a daily average count of enrolled devices. It now correctly shows the count of current users with Onboard-generated certificates, updated every 15 minutes and matching the count at **Policy Manager > Administration > Server Manager > Licensing**.

OnGuard

Table 30: *OnGuard Issues Fixed in 6.7.1*

Bug ID	Description
#43129	If the **Process Location** was set to **None** in the **Processes** health class, the endpoint was sometimes marked as Unhealthy even if the process was actually running on the endpoint.
#43131	The ClearPass OnGuard Agent for Windows sometimes did not read the Last Scan Time of an antivirus product.
#43193	The ClearPass OnGuard Unified Agent sent attributes of McAfee Endpoint Security AntiVirus even after it was uninstalled.
#43195	The ClearPass OnGuard Agent for macOS was sometimes unable to detect the status of a running process.
#43197	If the first server in the list of ClearPass servers in a cluster returned an HTTP Error code 503 in response to an OnGuard WebAuth request, OnGuard did not fail over to the next ClearPass server in the list, and therefore could not perform health checks until the publisher recovered.
#43199	The ClearPass OnGuard Agent for Windows sometimes prompted for credentials even if the **Enable to use Windows Single-Sign On** option was enabled on the ClearPass appliance. This issue was seen when the user account was configured for automatic login.
#43223	On macOS, the client became unhealthy after the ClearPass OnGuard Agent automatically installed a new version of the OnGuard Agent Library Update. This issue was seen on macOS, and only if automatic updates were enabled in the Agent Enforcement Profile and a new version of the OnGuard Agent Library was available on the server.
#43242	The ClearPass OnGuard Agent for macOS did not read the correct DAT file time and version for Trend Micro Security antivirus software. The OnGuard Agent now correctly reads the DAT File time and version of "Smart Scan" for Trend Micro Security.
#43350	An OnGuard custom user interface that had been enabled in 6.6.5 or 6.6.7 was disabled after updating to ClearPass 6.6.8. The Custom User Interface setting in the OnGuard Settings page is now retained during the update from 6.7.0 to 6.7.1.
#43421	When users connected through a VPN device, the ClearPass OnGuard Agent for Windows performed frequent health checks.

Table 30: *OnGuard Issues Fixed in 6.7.1 (Continued)*

Bug ID	Description
#43434	On macOS 10.13.x, the ClearPass OnGuard Agent for macOS was sometimes unable to read the encryption state of drives that had been encrypted using FileVault 10.13.2.
#43471	Posture evaluation for Sophos Anti-Virus failed when the ClearPass OnGuard Unified Agent was unable to read the DAT file version or DAT file time of Sophos Endpoint Security and Control 10.7.2.

Policy Manager

Table 31: *Policy Manager Issues Fixed in 6.7.1*

Bug ID	Description
#42156	Corrected an issue where a local adversary could steal passwords from the autocomplete feature of a browser. Users should be aware that any passwords saved in a browser must be deleted after ClearPass is updated.
#42495	Corrected a cluster time synchronization issue where the time in ClearPass was several minutes behind the Network Time Protocol (NTP) clock because a subscriber was referring directly to the NTP server. ClearPass subscribers now synchronize only with the publisher. The publisher is the only ClearPass server to contact the NTP server, and acts as the NTP server for all the subscribers.
#42975	The ClearPass Server's hard disk was getting filled with the Apache Tomcat and HTTPD service logs because of too many SSL requests from OnGuard Agents in a switch-user or multiple-user use case.
#43086	A new **EST-Label** attribute is added to the Applications dictionary for ClearPass (Application:ClearPass), and a new **EST** attribute value is added to the list of options for the application namespace (Application:Name). This attribute and value support HTTP authentication on an EST server, and are available in the Applications dictionary and in service rules.
#43103 #43144 #43297	Corrected some issues with the **system factory-reset** command and the **system install-image command** where: • After the **system factory-reset** command was executed, the previous Platform Activation Key (PAK) was not deleted and the user was taken directly to the login page. Now when the **system factory-reset** command is executed, the previous PAK is correctly deleted along with the rest of the previous license information, and the user is prompted to enter their new PAK. • After either the **system factory-reset** command or the **system install-image command** was executed, evaluation licenses were added for Access, OnGuard, and Onboard when the system rebooted. Now when the **system factory-reset** command or the **system install-image command** is executed, no evaluation licenses are added.
#43243 #43249	The configured authentication source timeout setting was not applied when connecting to a backup Active Directory/LDAP server, resulting in frequent RADIUS server restarts.
#43252	The policy server intermittently crashed, causing authentications to fail. An exception check is now added to the Fast Common Gateway Interface (FCGI) module to handle invalid FCGI packets.
#43253	Certificate Revocation List (CRL) updates could not be downloaded from the federal CRL server.
#43355	The BIOS firmware for the HPE ProLiant DL20 Gen9 servers used in C2000 (CP-HW-5K) appliances is now updated to address a vulnerability found in the Intel Xeon processor. This includes fixes for CVE-2017-5705, CVE-2017-5706, CVE-2017-5707, CVE-2017-5708, CVE-2017-5709, CVE-2017-5710, CVE-2017-5711, and CVE-2017-5712.
#43475	The PostgreSQL version is now upgraded to 9.6.6. This includes fixes for CVE-2017-15098, CVE-2017-15099, and CVE-2017-12172. Although ClearPass was not vulnerable to these CVE issues, the upgrade was done in order to reduce any false positives that might occur during vulnerability checks.

Table 31: *Policy Manager Issues Fixed in 6.7.1 (Continued)*

Bug ID	Description
#43535 #43570 #43598	Endpoints were deleted or disabled even if the **Known endpoints cleanup interval** or **Unknown endpoints cleanup interval** cluster-wide parameter was disabled (set to 0).
#43554	After updating a cluster password, the Access Tracker showed blank values in all fields and the error message "Database query error; please try again" was displayed.
#43565 #43600	Antivirus updates sometimes failed and the **Event Viewer** displayed the error message "Failed to update AV/AS from ClearPass Portal (Online). Error - [Errno 2] No such file or directory: '/tmp/ext_apps_updates/cppm_antivirus_updates.zip'".
#43593	A read-only user could execute a bulk-update operation on an endpoint.
#43616	For TACACS+ authentications, license usage accounting has changed. On a ClearPass system with a valid Access license, TACACS+ sessions will not be counted towards Access license consumption.

Fixed in 6.7.0

The following issues were fixed in the 6.7.0 release.

AirGroup

Table 32: *AirGroup Issues Fixed in 6.7.0*

Bug ID	Description
#20748	The character limits for AirGroup shared location, shared user name, shared user group, and shared role fields are now updated to match the value limits in the controller, as shown below: ● AP-Name = 63 characters ● AP-FQLN = 247 characters ● AP-Group = 63 characters ● User name = 247 characters ● User groups = 63 characters ● User roles = 63 characters

CLI

Table 33: *CLI Issues Fixed in 6.7.0*

Bug ID	Description
#40954	ClearPass appadmin users should be aware that in the CLI, the name of the VIP service is now changed from **cpass-vip-service** to **cpass-vip**.

Cluster Upgrade and Update

Table 34: *Cluster Upgrade and Update Issues Fixed in 6.7.0*

Bug ID	Description
#40365	During a patch update through the **Software Updates** portal on a cluster that had publisher failover enabled, after updating the publisher and rebooting, a subscriber update failed with the error message "Cluster nodes are not in sync." This occurred because publisher failover was triggered after an interval and the standby publisher became the publisher.
	Users should be aware that the standby publisher value should be set to false before starting a cluster update. A message will now be displayed on the **Software Updates** portal of a publisher if a standby publisher is enabled and the patch requires a reboot. If the update is done through the **Cluster Update** portal, the enable and re-enable actions are handled automatically.

Endpoint Context Servers

Table 35: *Endpoint Context Server Issues Fixed in 6.7.0*

Bug ID	Description
#37807	Google admin console authorization used the hostname instead of the fully-qualified domain name (FQDN) when FQDN was configured.
#41064 #41208 #41263 #41522	Corrected an issue where endpoints could not be fetched from a MaaS360.

Guest

Table 36: *Guest Issues Fixed in 6.7.0*

Bug ID	Description
#30988	After customizing the **Create Multiple Accounts** form with additional fields, the new fields were not included in the comma-separated value (CSV) file of the results. The CSV file now includes all of the fields that are part of the Guest receipt.
#34524	Users should be aware that the **Template Scripting** field has been removed from the **Kernel Plugin** configuration form.
#36373	Corrected a UI workflow that was missing cross-site request forgery (CSRF) protection when enabling a skin plugin.
#36955	In some cases, a valid phone number was not accepted by either the visitor's **Guest Registration** form or the **Send SMS** form. In phone number fields, we recommend the following **visitor_phone** settings: ● Conversion: NwaNormalizePhoneNumber ● Validator: NwaSmsIsValidPhoneNumber ● Validator Param: None
#39424	Corrected a potential reflected cross-site scripting (XSS) issue affecting fields of type static_raw.
#42103	Corrected a potential reflected cross-site scripting (XSS) issue affecting directory names in Content Manager.
#42105	Corrected a potential reflected cross-site scripting (XSS) issue affecting the SMS guest receipt page.

Table 36: *Guest Issues Fixed in 6.7.0 (Continued)*

Bug ID	Description
#42578	The connection to a FIAS (Micros Opera, Protel, Silverbyte) transaction processor could be dropped unexpectedly.
#42821	The PHP version is now updated to 7.1.11. This includes fixes for CVE-2013-7456, CVE-2016-1283, CVE-2016-3074, CVE-2016-3078, CVE-2016-5093, CVE-2016-9933, CVE-2016-9934, CVE-2016-9935, CVE-2016-9936, CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, and CVE-2017-9229.

Insight

Table 37: *Insight Issues Fixed in 6.7.0*

Bug ID	Description
#33598	Insight authentication reports did not generate correctly after a CSV export and failed with a timeout error if the Insight database had a very large number of records (> 50 million).
#35548	Report information was sometimes lost after upgrading from an earlier version of ClearPass. Guest authentication reports now support filtering based on sponsor fields such as **Sponsor Name**, **Sponsor Email** and **Sponsor Profile Name**.
#41007	Configuring an Insight report on a publisher caused some processes to hang and a subsequent "make subscriber" action could not be completed.
#41161 #41721	The **System License Usage** report did not generate a valid report. Users should be aware that, as part of the licensing changes introduced in ClearPass 6.7, the **System Dashboard** and **System License Usage** reports are deprecated. They are replaced by the new **Licensing > License Usage** report. This page displays the current Access, OnGuard, and Onboard license usage over the previous 15 minutes or previous 24 hour interval, and the maximum usage for these license types in the previous day, week, or month. The **Top 10 Restarted Services** graph has been moved to the **System Monitor** dashboard. If you have an existing **System > License Usage** report configured, after you upgrade to 6.7.0 it will become the new **Licensing > License Usage** report with the default configuration. The new report includes the following licensing information: • License statistics, including the total number of licenses, and the number of licenses used for each license type • Number of unique endpoints on the network over the selected time period • Number of ClearPass Access licenses used over the selected time period • Number of ClearPass Guest licenses used over the selected time period • ClearPass licenses distribution (available vs. used) • ClearPass license usage per host

Onboard

Table 38: *Onboard Issues Fixed in 6.7.0*

Bug ID	Description
#35499	Onboard sometimes re-used a certificate even after the requested key algorithm was changed in **Provisioning Settings**.
#40021	Generating RSA keys smaller than 2048 bits failed in FIPS mode. The RSA 1024 key type is not available now in FIPS mode.
#42888	If the mdpsUserName OID was not present in the CSR, a unique user was generated in Onboard. This

Table 38: *Onboard Issues Fixed in 6.7.0 (Continued)*

Bug ID	Description
	meant a user with multiple devices enrolled via EST or SCEP was counted as multiple users and consumed multiple Onboard licenses. Onboard now considers the username in certificates created via EST and SCEP when calculating license usage.

OnGuard

Table 39: *OnGuard Issues Fixed in 6.7.0*

Bug ID	Description
#27599	On Ubuntu systems, the OnGuard logo was not shown on the desktop until the UI was refreshed.
#27876	ClearPass now supports RADIUS change of authorization (CoA) over VPN on Ubuntu.
#37427	On a 64-bit Windows OS system, a file check failed when the ClearPass OnGuard Unified Agent was not able to find files that were present in the system32 folder.
#39863	On a system with OnGuard installed, the wireless network interface was sometimes disabled when it came out of sleep mode or if the system was roaming. OnGuard can now bounce the network interface after waking up from sleep mode, using the value of the new **DisableBounceAfterWakeup** registry key in HKLM\Software\Aruba Networks\ClearPassOnGuard. Users should be aware that this registry key is not automatically added to OnGuard during installation; administrators must add it manually: ● If the value of **DisableBounceAfterWakeup = 0**, or if the key is not present, then OnGuard will bounce the network interface after waking up from sleep mode (current behavior). ● If the value of **DisableBounceAfterWakeup = 1**, then OnGuard will not bounce the network interface after waking up from sleep mode. The type for DisableBounceAfterWakeup should be REG_DWORD.
#41431	Users should be aware that, because the V3 SDK is deprecated in ClearPass 6.7, the **V3** option is now removed from the **SDK Type** attribute in the Agent Enforcement profile.
#41580	On OnGuard with VIA, the device driver installation failed and prevented VPN connections and the adapter had to be installed manually. OnGuard now automatically installs the driver if it is needed.
#42245	OnGuard sometimes caused high bandwidth usage in a multiple-user or switch-user scenario.
#42305	In OnGuard's **Global Agent Settings**, the attributes **Allowed Subnets for Wired access** and **Allowed Subnets for Wireless access** are now deprecated and should not be used. These attributes will be removed in a future release.

Policy Manager

Table 40: *Policy Manager Issues Fixed in 6.7.0*

Bug ID	Description
#20292	Information seen in the **Monitoring > Live Monitoring > System Monitor** graph was not created in the time zone of the appliance the user was viewing, but instead was created in the time zone of the appliance on which system performance monitoring was enabled, if those were different.
#30359	Adding an external Nessus audit server failed with the error message "Primary Server: Unable to connect to Nessus Server". This issue is corrected ClearPass; however, some changes are required on the Nessus server side. In the Nessus server configuration, please set "disable_ntp" to "no" and restart the nessus process on

Table 40: *Policy Manager Issues Fixed in 6.7.0 (Continued)*

Bug ID	Description
	the Nessus server:
	1. Set the value for **disable_ntp** to **no**.
	For example, on a CENTOS/RHEL server running Nessus:
	centos# /opt/nessus/sbin/nessuscli fix --set disable_ntp=no
	2. Restart the nessus service.
	For example:
	centos# service nessusd restart
	3. If the Nessus server has TLS enabled, then add the Nessus CA Certificate to the ClearPass **Certificate Trust List**.
	The Nessus CA certificate can be downloaded from https://<nessus-server>:8834/getcert.
#34161	After upgrading from 6.5.x to 6.6.0, the error message "Unknown error: no route to host" was displayed on the **Software Updates** page, and customers whose networks included addresses in the 172.17.0.0/16 range were advised to either disable the Extension service or contact TAC for assistance in re-allocating the Extensions to use a different network address space. On the **Administration > Server Manager > Server Configuration > Service Parameters** tab, for **ClearPass system services** users can now use the **Extensions Network Address** parameter to configure the adapter interface and change the subnet used for the Extension.
#34496	Services were abruptly stopped and restarted, and some DNS settings were changed. Now when a DNS configuration is changed from either the UI or the CLI, messages are logged in the **Event Viewer** and include the IP address of the newly-configured DNS server.
#34557 #36442	Changing the date and time on a subscriber changed it for the entire cluster. When in a cluster, at **Administration > Server Manager > Server Configuration** the **Set Date and Time** option is only available on the publisher. A **Set Time Zone** option is available on a subscriber when a server is selected in the **Server Configuration** list.
#34086	If a system was upgraded from ClearPass 6.5.5 or below with a configuration that was affected by issue #33036, the configuration was not auto-corrected during the upgrade.
#34806	When initiating a network scan, some accidental key strokes in the **Seed Devices (csv)** field caused the scan to hang at "Scheduled" and the scan could not be canceled. Validation is now added for some characters that could possibly be entered accidentally, such the space key or the Enter key.
#34814	The **Restore Defaults** option at **Administration > Server Manager > Log Configuration** did not work. The **Restore Defaults** option now correctly resets the log levels for all modules to the default of WARN.
#35160	A user was locked out of the Policy Manager user interface if they exceeded their Policy Manager license usage four times in an eight-month period, even though the limitation had been stated as a six-month period. With the new licensing platform introduced in ClearPass 6.7.0, users will not be locked out of the UI if their Access, Onboard, or OnGuard license usage exceeds the total count allowed.
#35312	In a load-balanced cluster configured with a login delay, replication to all subscribers sometimes took too long and the login failed with a "user not found" error. The default minimum value configured for the replication lag is now changed from 3 seconds to 1 second. **Note:** Only use this lower interval for a replication lag if your network has good latency and throughput.
#35427	When using the Cluster Upgrade Tool to upgrade to ClearPass 6.6.0 from an earlier 6.x version, an upgrade image metadata file from an older version caused the upgrade process to hang and the upgrade did not complete.
#35551	An SNMPv3 poll did not work if a double-quote character (") was used in the authentication key or

Table 40: *Policy Manager Issues Fixed in 6.7.0 (Continued)*

Bug ID	Description
	privacy key. Users should be aware that the double-quote character is not allowed. Validation is now added for these fields, and if any invalid characters are entered, an error message is displayed that includes a list of the invalid characters. The following characters are not allowed in authentication or privacy keys: **& = . ? | ; : "**
#36302	The **Total Swap Memory** reported for a CP-VA-25K did not match what was reported for the CP-HW-25K on the **Monitoring > Live Monitoring > System Monitor > Swap Memory Usage** graph. Starting with the ClearPass 6.7.0 release, the swap disk space value is now increased from 3 GB to 6 GB on new 25K virtual appliance (C3000V) installations, which matches the 25K hardware appliance (C3000). However, the swap value will not change on existing (pre-6.7.0) 25K virtual appliances that are upgraded to 6.7.0.
#36978 #40319	A join to a ClearPass domain was invalid and the domain server service could not be started. The NETBIOS name is now converted to all uppercase to create the domain server service name.
#37493	At **Administration > Agents and Software Updates > OnGuard Settings > Policy Manager Zones**, trying to add a list of subnets in the **Client Subnets** field failed and the error message "Error in processing request. Please retry" was displayed. The character-limit issue has been fixed.
#38465	Users should be aware that some clients might be unable to authenticate if certificates that use a wildcard as the common name (for example, *.arubanetworks.com) or if Extended Validation certificates (EV, or "Green Bar") are used. When a user is uploading a RADIUS/EAP server certificate on the **Import Server Certificate** window, a warning message is now displayed advising that uploading certain types of certificates is not recommended. This is not an issue with HTTPS certificates.
#38489	An incorrect value for an endpoint's status was retrieved from the Insight database during an API call, and at **Monitoring > Access Tracker > Request Details** the value in the **Online Status** field was **Unavailable**.
#38693	A SAML POST failed with the error message "413: Request entity too large." The maximum size of an HTTP request and response header in Apache is now increased to 5 MB.
#38769	A Change of Authorization (CoA) was not triggered when a guest account expired if the account name included uppercase characters.
#39023	The Multi-Master Cache did not reconnect by itself if the process was abruptly stopped. The monitoring process now detects when the Multi-Master Cache process is down and will try to restart the service within ten seconds.
#39135	After setting the cluster-wide parameter to store a local user's password in reversible encryption and then changing a user's role, an authenticated user was correctly able to log in; however, after the user's role was changed authentication failed.
#39201	At **Configuration > Identity > Endpoints**, the **Connection Type** was shown as **Wired** for a wireless endpoint.
#39644	The Cluster-Wide parameter **Maximum inactive time for an endpoint** is no longer used and has been removed.
#39751	When CC mode was enabled, an administrator could not log in to the ClearPass Administration UI, but was able to log in as appadmin through the CLI. If an admin user is locked out in CC mode, use the **system admin-passwd-reset** command in the CLI to reset the password.

Table 40: *Policy Manager Issues Fixed in 6.7.0 (Continued)*

Bug ID	Description
#39777	When configuring an NTP server, no error was displayed if an encryption type was not entered for the authentication key. Now if the authentication key information is incomplete, the message "Error: Invalid syntax" is displayed on the form and included in the usage log.
#40032	IPsec firewall rules were not removed when FIPS mode was turned on, although the rest of the IPsec configuration was correctly cleared.
#40043	EAP-TLS authentications failed in FIPS mode and displayed the error message "fatal alert by server - decrypt_error." ClearPass in FIPS mode now accepts client certificates that use the RSASSA-PSS signature algorithm.
#40085	Multiple instances of checkfirmwareupdates script were running on the ClearPass server and causing high CPU usage.
#40087	When trying to do a only a packet capture at **Administration > Server Manager > Server Configuration > Collect Logs** with the **Advanced Options for Packet Capture** option selected, the packet capture failed if only the **Destination Port** was specified.
#40090	Only a limited set of ClearPass fields were mapped to the Common Event Format (CEF) dictionary, and CEF-format syslog messages added the prefix "ArubaClearPass" to some attributes. In Syslog Targets, CEF-format field mappings in all templates are now updated to support most features of Arcsight.
#40453	Subscribers in a cluster frequently went out of synchronization and various database instability errors were displayed. Endpoint cleanup now reduces database lock conflicts by purging entries in batches instead of simultaneously in bulk.
#40561	Large batches of events could not be sent to an Insight-enabled appliance, and PANW user information was not updated for some users.
#40935	The **Save** and **Cancel** buttons for adding an available Windows Hotfix were hidden on the **ClearPass Windows Universal System Health Validator** form at **Configuration > Posture > Posture Policies**.
#41018	The Access Tracker showed an F5 Load Balancer IP as a Remote IP instead of a Client IP address. ClearPass now looks at the X-Forwarded-For variable to determine the real Client IP Address if the request is sent from an external load balancer.
#41204	While a scan was running an end time was shown, the endpoints were incorrectly shown as 0, and the endpoints count was not updated when the scan was complete. With the reorganization of the network and discovery scan interface, the **Monitoring > Profile and Network Scan > Network Scan** list view now shows details of all completed discovery scans and subnet scans, and lists their seed devices/IP subnets. For each subnet scan in the list, you can click the scan's row to open the **Subnet scan results** window, which lists the scan results for that subnet. Information includes the zone, start and end times, active and failed hosts, and the status of the scan. It also provides lists of the IP subnet ranges and their active hosts, failed hosts, and any scan errors.
#41353	The RADIUS service abruptly stopped and restarted after an enforcement profile was updated that included vendor-specific RADIUS attributes. Users should be aware that RADIUS vendor-specific attributes are not allowed in RADIUS enforcement profiles. Validation is now added for this, and an error message will be displayed if an enforcement profile includes a vendor-specific attribute.
#41394	In a cluster, Insight synchronization errors were seen on the servers that had Insight enabled and the logs showed the error message "violates check constraint". The Apache Cipher Suite configuration is now modified to address the issue.
#41414	The Ingress Events dictionary could not be exported and the error message "Type EventsDictionary

Table 40: *Policy Manager Issues Fixed in 6.7.0 (Continued)*

Bug ID	Description
	not present in TipsAdminEntityType" was displayed.
#41507	On iOS 11 and macOS 10.13, EAP-FAST with TLS sometimes failed. ClearPass now supports TLS 1.2 in EAP-FAST.
#42059	The **Virtual Host ID** field and related messages were incorrectly labeled "Virtual Router ID" instead on the **Administration > Server Manager > Server Configuration > Virtual IP Settings** form. The field is now correctly labeled **Virtual Host ID** (consistent with the CARP protocol that is used).
#42114	A race condition in the Administration UI's data structure caused very high CPU usage.
#42168	The publisher ran out of disk space and was unresponsive after the standby publisher took over.
#42240	Using the REST API to create or update an endpoint attribute with the **Allow Multiple** attributes property set did not produce expected results.
#42272	Corrected an issue with downloadable roles where standard mode configurations did not work for Aruba PUTN configurations. The generated command will now be the AAA authorization User Role name "cppmrole_89a94c230c554d4". A unique random string of length 15 is added to cppmrole for "Aruba OS-switch" to create the unique role name.
#42300	For ClearPass deployments integrated with Palo Alto Networks firewalls running PAN-OS 7.1.10 up to 7.2.0, the timeout value of zero was not sent.
#42438	Corrected an issue with downloadable roles where QOS, VOIP, and Policer Profile configurations were allowed for the Mobility Controller. They are now correctly restricted to Mobility Access Switches only.
#42449	In the **Software Updates** portal, to reflect the application signatures and virus definitions available in the OnGuard plugin 2.0 (V4 SDK), the **AntiVirus and AntiSpyware Updates** patch is now renamed to **Posture Signature Updates**.
#42584	Corrected an issue with downloadable roles where some configuration fields were missing from the **Class Configuration** form. The **Source Port**, **Source Port Value**, **Destination Port**, and **Destination Port Value** fields are now added to the **Rule Configuration** tab of the **Class Configuration** form.
#42615	The RADIUS service abruptly stopped and had to be manually restarted if an NTHash password type was used in an LDAP Authentication source.
#42630	Error messages of the 4xx type — for example, "404: Page not found" or "403: Forbidden" — are now simpler and less verbose.

Profiler and Network Discovery

Table 41: *Profiler and Network Discovery Issues Fixed in 6.7.0*

Bug ID	Description
#39376	Although log files showed that endpoints were correctly profiled and updated, the information was not correctly reflected in the database. If duplicate DHCP discover/request messages are received from the same MAC address within a five-minute window, ClearPass will now ignore them.

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

This chapter includes:

CLI

Table 42: *Known Issues in CLI*

Bug ID	Description
#33374 #35750	**Symptom**: On a CP-HW-25K running on DELL R630, the total memory is shown as 65.9 GB, which is greater than the total memory specifications for the VA type. **Scenario**: The Dell R630 server overestimates 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.
#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 43: *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. ● 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 network services** 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 #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.

Table 43: *Known Issues in Cluster Upgrade and Update*

Bug ID	Description
#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.
#41575	**Symptom:** After using the **Cluster Upgrade** page to upgrade to 6.7.0, the ClearPass user interface is not automatically refreshed. **Scenario:** When a system is upgraded to 6.7.0 through the **Cluster Upgrade** page, after it successfully reboots and the admin and **Async network services** services are up, the ClearPass user interface is not automatically refreshed. The error message "Server will be accessible after reboot and DB migration (if any) is complete. This may take a while… UI will refresh automatically" is displayed but the system continues to hang. **Workaround:** Manually refresh the page.

Dissolvable Agent

Table 44: *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 macOS 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 macOS 10.9. **Scenario:** New security restrictions in macOS 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	Users should be aware that the OnGuard applet needs to run in Safari's "Unsafe mode" in order 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	Users should be aware that 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.

Table 44: *Known Issues in the Dissolvable Agent (Continued)*

Bug ID	Description
#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 macOS. **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, macOS 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 macOS, 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 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 macOS, 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 macOS 10.6.
	Workaround: On macOS 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 macOS 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 macOS 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.

Table 44: *Known Issues in the Dissolvable Agent (Continued)*

Bug ID	Description
	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 macOS 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: macOS 10.6, 10.7, and 10.8.

Guest

Table 45: *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.
#39889	**Symptom:** When attempting a Web login to Guest on an iOS device, the first attempt consistently fails but the second attempt succeeds. **Scenario:** This issue occurs if a self-signed certificate is used for the Aruba controller. This is only an issue on iOS devices; it is not an issue on other device types. **Workaround:** Always use an external (public) certificate for an Aruba controller.

Insight

Table 46: *Known Issues in Insight*

Bug ID	Description
#31048	**Symptom/Scenario:** When the Internet Explorer browser is refreshed, icons on the Insight Dashboard are displayed as text. **Workaround:** Navigate to any other page in Insight and then come back to the Dashboard page.
#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.

Table 46: *Known Issues in Insight (Continued)*

Bug ID	Description
#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	**Symptom/Scenario:** If the report period is more than one month, the PDF report does not show the X,Y data table below the 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

Bug ID	Description
	widget visibly changes the pointer to a click pointer, but no action occurs if the pointer is clicked.
#33667	Users should be aware that Insight configurations from Insight versions earlier than ClearPass 6.6 are not retained during migration or upgrade, and will need to be manually recreated after upgrading to ClearPass 6.7.0.
#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 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.
#40250 #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.
#42796	**Symptom:** The endpoint counts shown on Insight's **Dashboard** and **Endpoint Unique Trend** graph do not match. **Scenario:** If one week, one month, or a custom date is selected for viewing the endpoint count on Insight's **Dashboard**, and the user then drills down to view the data on the **Endpoints Unique Trend** graph, the counts might not match. Users should be aware that this is because if an endpoint is authenticated multiple times, the **Dashboard** shows only the most recent authentication; however, on the **Endpoint Unique Trend** graph, unique endpoints are counted on an hourly basis.

Licensing

Table 47: *Known Issues in Licensing*

Bug ID	Description
#43007	**Symptom:** Service configuration is not allowed because an Access License that was never activated has expired. **Scenario:** This may occur after an Access License expires in a situation where multiple Access Licenses are installed but not activated, and they are valid for different durations. **Workaround:** Users should be aware that, if multiple Access Licenses are installed, they should be activated as soon as they are installed. This ensures that even if one activated license is expired, service configuration will still be allowed if the other Access Licenses have not yet reached their expiration dates. Otherwise, if service creation is blocked when an Access License that was not activated expires: 1. Activate the expired license. 2. Verify whether the other Access Licenses are still within their validity date range. 3. Activate any others that have expired.

Onboard

Table 48: *Known Issues in Onboard*

Bug ID	Description
#9897	**Symptom:** ClearPass Onboard does not update the Policy Manager endpoints table with an endpoint record when provisioning an iOS 5 device. **Scenario:** This is because the iOS 5 device does not report its MAC address to ClearPass Onboard during device provisioning.
#10667	**Symptom/Scenario:** When using Onboard to provision a OS X system with a system profile, an administrator user must select the appropriate certificate when connecting to the provisioned network for the first time. The administrator should also ensure that the system's network settings are configured to automatically prefer connecting to the provisioned network, if the intent is for non-administrator users to always use that network. **Workaround:** The process to provision an OS X system with a system profile is: 1. The administrator should log in to the OS X system and connect to the provisioning SSID. Do not select the "Remember this network" option. 2. Use Onboard to provision the device with an EAP-TLS profile, ignoring the username/password prompt. 3. Connect to the provisioned network, selecting EAP-TLS as the mode and selecting the provisioned certificate, but ignoring the username field. 4. When the system connects and authorizes to the network, use Network Preferences to place the EAP-TLS network first in the priority list. 5. After the administrator logs out, users logging in are connected by EAP-TLS and cannot modify those settings.
#20983	**Symptom:** HTC Android asks the user to enter a certificate name to be installed when onboarding. **Scenario:** HTC Androids running Android version less than Android 4.3 and greater than Android 2.3 ask the user to enter a name for the certificate to be installed while onboarding. Authentication will fail if the user does not enter the exact certificate name as QuickConnect application instructs in a message prior to the certificate installation dialog. **Workaround:** None. This issue is due to a limitation in the Android phone's firmware.
#23287	**Symptom:** Embedding Admin credentials for onboarding does not work in Windows 8 and above. The system hangs and there is no error message. **Scenario:** When onboarding Windows systems with Windows 8 and above, if operations requiring admin privileges are configured, then the end user doing the onboarding needs to have admin privileges on the

Table 48: *Known Issues in Onboard (Continued)*

Bug ID	Description
	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:** macOS disconnects before it completes a certificate renewal. **Scenario:** On macOS, 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 macOS 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	**Symptom/Scenario:** 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.
#43070	**Symptom:** After onboarding an Ubuntu system, the error message "Your system has been successfully configured for secure access to network. QuickConnect could not automatically connect <SSID> to the network..." is displayed. **Scenario:** This issue might occur after an Ubuntu system is successfully onboarded and even though it is able to reconnect to the SSID through TLS. **Workaround:** This error message can be ignored. The connection to the SSID will happen automatically in the background.

OnConnect Enforcement

Table 49: *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,

Table 49: *Known Issues in OnConnect Enforcement (Continued)*

Bug ID	Description
	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 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

NOTE

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 50: *Known Issues in OnGuard*

Bug ID	Description
#12342	**Symptom/Scenario:** 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 macOS, 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 macOS. It does not occur on Windows OS.
#13929	**Symptom/Scenario:** At times, OnGuard may fail to detect peer-to-peer applications, such as /uTorrent, on Windows 2008 R2.
#13935	**Symptom/Scenario:** OnGuard does not support enabling or disabling the Windows Update Agent Patch Management Application.
#13970	**Symptom/Scenario:** After anti-virus software is installed, the system must be rebooted before using ClearPass OnGuard.

Table 50: *Known Issues in OnGuard (Continued)*

Bug ID	Description
#14196	**Symptom/Scenario:** ClearPass OnGuard will not be able get the correct status of 'Software Update' PM application on macOS, if "Check for updates" and "Download updates automatically" are not toggled at least once.
#14673	Users should be aware that the OnGuard Agent for macOS does not support bouncing of a VPN Interface other than the Aruba VPN Interface (version 6.1).
#14760	**Symptom/Scenario:** 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	**Symptom/Scenario:** Installing the ClearPass OnGuard Unified Agent removes an existing VIA installation. **Workaround:** 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	**Symptom/Scenario:** If McAfee VE is running on Windows XP, the ClearPass OnGuard Unified Agent VPN will not work.
#15072	Users should be aware that VIA connection profile details are not carried forward after upgrading from VIA 2.0 to ClearPass OnGuard Unified Agent 6.1.1.
#15097	Users should be aware that the ClearPass OnGuard Unified Agent does not support installation of a VPN component on macOS 10.6.
#15156	**Symptom/Scenario:** VPN configuration is not retained after upgrading to the ClearPass OnGuard Unified Agent using MSI Installer on a 64-bit Windows system.
#15233	**Symptom/Scenario:** On Windows 7 (64 Bit), upgrading an existing VIA 2.1.1.X to the ClearPass OnGuard Unified Agent can lead to an inconsistent state. **Workaround:** 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 macOS 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 macOS: 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	**Symptom/Scenario:** 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 macOS. **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

Table 50: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	state using the MacKeeper (ZeoBIT LLC) Disk Encryption Product on macOS. 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.
#18341	**Symptom/Scenario:** OnGuard cannot start a process on macOS for non-administrative users. **Workaround:** The user must have root privileges to start process-level health checks by OnGuard on macOS.
#19019	**Symptom:**The network interface will be bounced twice (once immediately, and once after the configured interval) when the log-out/bounce delay parameter is configured. **Scenario:**Users should be aware that this is expected behavior; the first bounce is required to end the existing session.
#20316	Users should be aware that 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 macOS. **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.
#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 macOS, the native and Java dissolvable agents do not get the RTP status of ESET Cyber

Bug ID	Description
	Security Antivirus 6.x. **Scenario:** Users should be aware that the ClearPass OnGuard Native Dissolvable Agent for macOS 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. **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.

Table 50: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	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 **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 macOS 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 macOS. **Workaround:** When the agent is launched for the first time , click "Launch ClearPass OnGuard Agent" to launch it manually.
#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

Table 50: *Known Issues in OnGuard (Continued)*

Bug ID	Description
	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. **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 macOS 10.10 and 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 updating a cluster from 6.6.4 to 6.6.5, or if you are upgrading it from 6.6.4 to 6.7.0, 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, or when upgrading from 6.6.4 to 6.7.0. 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.

Table 50: *Known Issues in OnGuard (Continued)*

Bug ID	Description
#42850	Users should be aware of the following behaviors: • Manual installation of the ClearPass OnGuard Agent Library for the Persistent Agent on Windows will restart the OnGuard Agent and services. • If multiple users are logged in at the time of the installation, then after the installation the installer will launch the OnGuard Agent only for the current active user. OnGuard Agents for non-active users will be closed and will need to be launched manually.
#43080	**Symptom/Scenario:** On systems configured for non-English languages, the ClearPass OnGuard Persistent Agent and Native Dissolvable Agents show the End User License Agreement in the English language.

Policy Manager

Table 51: *Known Issues in Policy Manager*

Bug ID	Description
#10881	**Symptom/Scenario:** Entity updates with PostAuth enforcement fail if the publisher is down.
#12316	Users should be aware that Syslog Filters and Data Filters configurations will be removed after an upgrade. Policy Manager does not carry these configurations forward. Only default data is migrated.
#13645	**Symptom/Scenario:** Authorization attributes are not cached for the Okta authentication source.
#13999 #13975	Users should be aware that, 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	**Symptom/Scenario:** ClearPass does not currently support posting of Palo Alto Networks (PANW) user ID information when the PAN OS uses Vsys.
#19826	Users should be aware that Palo Alto Networks (PANW) devices accept only the backslash (\ )

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#24781	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.
#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	**Symptom/Scenario:** 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	Users should be aware that, in order for ClearPass to have complete data to post to Palo Alto Networks devices in HIP reports, profiling must be turned on. This is the expected behavior.
#20455	**Symptom/Scenario:** When doing an SSO & ASO flow in Safari browsers, the certificate needs to be added in the trust list of the browser. **Workaround:** Please follow these steps: 1. Open the Safari browser and enter the SP URL. 2. After you enter the SSO application in the browser, the Show Certificate option is provided in a popup window. 3. Click **Show Certificate** and select the **"Always trust 'FQDN of SP machine' when connecting to IPaddress"** check box, and then click the **Continue** button.
#20456	**Symptom:** SNMP bounce fails. **Scenario:** When only the SNMP bounce in the SNMP Enforcement profile of a Web auth service is configured, SNMP bounce functionality does not work. **Workaround:** Also configure a VLAN ID along with the SNMP bounce in the SNMP enforcement profile.
#20484	**Symptom:** Dropping the Subscriber and then adding it back to the cluster may fail at times. **Scenario:** ClearPass system time might not have been synchronized with an NTP source. **Workaround:** Configure an NTP server. ClearPass will synchronize its time with the NTP source. Attempt the cluster operation.
#20489	**Symptom/Scenario:** ClearPass 6.3 does not allow a server certificate with a Key Length of 512 bits as seen in the Self-Signed Certificate and Certificate Signing Request UIs. Earlier ClearPass versions did not have this restriction, hence their server certificate may use one with a 512 bit Public Key. After upgrade, these servers will not work properly. **Workaround:** The admin must manually fix the server certificate to allow a minimum of 1024 bits long Public Key prior to upgrade.
#21334	**Symptom:** ClearPass does not launch. **Scenario:** The ClearPass user interface will not launch from Firefox or from older versions of Internet Explorer (IE) browsers if an EC-based HTTPS server certificate is used. On Firefox, the error message "Secure Connection Failed. An error occurred during a connection to *<server>*. Certificate type not approved for application" is displayed. On older versions of IE, the error message "Internet Explorer cannot display the Web page" is displayed. **Workaround:** Use the latest version of IE, or the Chrome browser instead.
#22023	**Symptom/Scenario:** Launching the customer's ClearPass user interface through a proxy does not

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	work on the Internet Explorer or Safari browsers. **Workaround:** Use the Chrome or Firefox browser instead.
#23581	**Symptom:** A database connection error occurs in the Access Tracker UI when it is updated to 6.3.2 with MD2 server certificates. **Scenario:** This is a database connection problem because of the MD2 certificate available for PostgreSQL. MD2 is not supported. **Workaround:** After updating to 6.3.2 (patch installation from 6.3.0), if Access Tracker or Analysis & Trending show errors relating to database query errors, it can be due to an invalid Server Certificate. 1. Go to Server Certificate and select the certificate for the server and RADIUS service. 2. Click View Details for each certificate in the chain. 3. Look for the Signature Algorithm and check to see if it uses MD2. 4. Download the certificate that is MD5 or 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. **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.
#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.
#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

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	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.
#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.
#30486	**Symptom:** Custom filters in an Auth Source do not work after upgrading to ClearPass 6.6. **Scenario:** As part of enhancements to tag mappings, the schema for storing the tag values has changed, and all default filters were migrated to the new schema. It is not possible, however, to automate the migration of custom filters. **Workaround:** If you have custom filters, contact Support to have the custom filters migrated to the new schema.
#30569	**Symptom/Scenario:** The Guest Portal name in the ClearPass portal is unchanged after updating the name in the ClearPass Guest application. **Workaround:** When you change Guest Portal names in the ClearPass Guest application, the admin must manually update the ClearPass Portal settings if the guest portal is used in that configuration.
#30968	Users should be aware that VMware ESX hosts are not profiled by SNMP CDP based profiling. The Profiler needs a host MAC or IP address in order to identify the device. ESX servers might not report the management IP address and MAC address in the CDP announcements, causing the Profiler to ignore neighbor CDP information for the host.
#31208	**Symptom:** Multiple entries for the same device can be seen in the endpoints page. **Scenario:** Users should be aware that, during the network discovery scan, if devices have multiple endpoints those endpoints will be listed separately in the endpoints page.
#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.

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#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 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: Restoring Log DB and Access Tracker Records" on page 105). 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**.
#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

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
	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 > Server Manager > Server Configuration > Services Control** tab.
#35167 #35735 #35282	**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 network services** 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 network services** 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.
#36397	Users should be aware that, now that OnGuard uses only Plugin Version 2.0 (V4 SDK) and the V3 SDK is deprecated, the **Display Update URL** option cannot be selected for the **AntiVirus** health class at **Configuration > Posture > Posture Policies**.

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#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. 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.
#40661	**Symptom:** A Change of Authorization (CoA) for the [ArubaOS Switching - Bounce Switch Port] (called [HPE Bounce Host Port] in version 6.6.x and earlier) reauthorization profile does not work if the session reauthorization is submitted through ClearPass Guest's **Active Sessions** form or through the ClearPass API, although it does work through the **Access Tracker** when **Change Status** is selected for the profile. **Scenario:** This has been observed for wired devices connected to an Aruba 3810 and 2930. **Workaround:** Submit the CoA for the [ArubaOS Switching - Bounce Switch Port] reauthorization through the Access Tracker's **Request Details > Change Status** option instead of through the **Active Sessions** form or the API.
#40880	**Symptom:** In FIPS mode, trying to create a new Certificate Authority (CA) fails with connection errors. **Scenario:** At Onboard > Certificate Authorities > Create new certificate authority, trying to create a new CA sometimes fails and a connection error message is displayed. The error message is different on different browsers, but some examples are "Security Connection Failed" or "This page is not working". This issue only occurs in FIPS mode. It is not an issue if FIPS mode is not enabled. **Workaround:** Restart ClearPass services from the CLI using the command **service restart all**.
#41698	**Symptom:** After upgrading a virtual appliance to 6.7.0 on a Hyper-V or VMware ESXi hypervisor, network connectivity is not restored. **Scenario:** This is only an issue when upgrading to ClearPass 6.7.0, and only on a Hyper-V virtual appliance, or on a VMware ESXi virtual appliance *only* if the MAC address of its Network adapter1 is higher than that of its Network adapter2. **Workaround:** A new CLI command, **system refresh network**, can be used to refresh and associate the network adapters with ClearPass during a Hyper-V or ESXi upgrade. Customers who are upgrading to 6.7.0 on a Hyper-V virtual appliance, or on an ESXi virtual appliance as described above, need to use this command when they upgrade. Full instructions are provided in the "After You Upgrade" sections of the Upgrade and Update Information chapter.
#42218	**Symptom:** Under certain conditions a ClearPass backup fails and the error message "ERROR - Failed to back up 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.
#42285	**Symptom/Scenario:** Users should be aware that when configuring an Aruba downloadable role enforcement profile in advanced mode, the secondary role name must not exceed 64 characters. If the secondary role name is longer than 64 characters, the enforcement might fail on the switch side. This is a limitation in the switch, not in ClearPass. This is not an issue in standard mode.

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#42601	**Symptom:** ClearPass 6.7.0 performance is degraded on a KVM virtual appliance (VA). **Scenario:** ClearPass 6.7.0 shows greatly reduced performance on KVM hypervisors. This is not an issue on Hyper-V or VMware hypervisors. **Workaround:** Customers using KVM should not upgrade to 6.7.0 at this time. This issue will be resolved in a future patch release.
#42807 #42808	**Symptom:** On a ClearPass 6.5.X system, after installing the Upgrade Preparation Patch for 6.7.0, any 6.6.0 upgrades and 6.5.X patch updates do not work. **Scenario:** Users should be aware that the public/private key pair used to sign and verify an upgrade image has been changed. Because of this, a 6.5.X system cannot be upgraded directly to 6.7.0. Instead, an Upgrade Preparation Patch must first be installed in order to update the keys, after which it can be upgraded to 6.7.0. However, after installing the Upgrade Preparation Patch, the system can only be upgraded to 6.7.0, and cannot be upgraded to 6.6.0. **Workaround:** To upgrade from 6.5.X to 6.6.0, do not apply the patch. Instead, upgrade to 6.6.0 and then upgrade to 6.7.0.
#43734	Due to a problem identified within IP-MIB, the following OIDs have been temporarily removed from ClearPass 6.7.2: ● ipAdEntAddr ● ipAdEntIfIndex ● ipAdEntNetMask ● ipAdEntBcastAddr ● ipAdEntReasmMaxSize ● ipv4InterfaceIfIndex ● ipv4InterfaceReasmMaxSize ● ipv4InterfaceEnableStatus ● ipv4InterfaceRetransmitTime ● ipv6InterfaceIfIndex ● ipv6InterfaceReasmMaxSize ● ipv6InterfaceIdentifier ● ipv6InterfaceEnableStatus ● ipv6InterfaceReachableTime ● ipv6InterfaceRetransmitTime ● ipv6InterfaceForwarding
#43757	**Symptom/Scenario:** While doing a postauth disconnect for an endpoint and with OnGuard disconnected, the error message "Insightdb failed to connect to dbhost" was displayed. **Workaround:** At **Administration > Server Manager > Server Configuration**, whenever you enable or disable Insight for the server, be sure to restart **Async network services**.
#43839	**Symptom:** Under certain conditions, a patch rollback operation fails with the error message "ERROR: Patch rollback operation failed. Error retrieving information for the installed patch," and the system remains in the pre-rollback version. **Scenario:** This occurs if, before the rollback, a custom skin had been installed by uploading it through **Administration > Agents and Software Updates > Software Updates > Import Updates** and then clicking **Install**. **Workaround:** If this occurs, please contact Customer Support to assist you with executing the rollback operation.
#44148	**Symptom:** On a 6.7.0 system that was upgraded from 6.5.3, the **system boot-image** command throws an error and the system cannot be switched back to the 6.5.3 partition. **Scenario:** After a system that is running a fresh 6.5.3 version (no update patches applied) is upgraded to 6.7.0, the **system boot-image** command displays the error message "Failed to set specified boot-image". This issue occurs when trying to switch back from a 6.7.0 or 6.7.X partition to 6.5.3. **Workaround:** Contact Customer Support to help you recover the 6.5.3 partition.

Table 51: *Known Issues in Policy Manager (Continued)*

Bug ID	Description
#44288	**Symptom:** The **Event Viewer** sometimes does not log messages indicating that the usage level for an Application license has returned to within the allowed range. **Scenario:** This issue occurs if the **Administration > Server Manager > Licensing > Refresh Count** link is clicked within the fifteen-minute interval since the last license computation. This issue also occurs if new license capacity is added within the fifteen-minute interval since the last license computation.
#44374	**Symptom:** Changing the enabled or disabled value of the **Post-Auth v2** cluster-wide parameter does not restart the **Async network services** service or clear the existing connections. **Scenario:** When the status of the **Post-Auth v2** cluster-wide parameter is changed, the **Async network services** service must be restarted, but this is not happening automatically and no message is shown in the user interface. Also, the current user session information in the external server is not cleared. **Workaround:** Whenever the **Post-Auth v2** parameter's value is changed: • You must manually restart the **Async network services** service. Go to **Administration > Server Manager > Server Configuration** and double-click the appropriate ClearPass appliance. On the **Services Control** tab, click **Stop** and then click **Start** in the **Async network services** row. • Make sure there are no active user sessions in the Palo Alto Networks (PANW) server.
#44399	Users should be aware that when the new **Post-Auth v2** cluster-wide parameter is enabled, only the GET and POST context server actions are supported by the new PostAuth module.

Profiler and Network Discovery

Table 52: *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 53: *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 6.7.

This chapter provides the following information:

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 6.7 Milestones

- Release Date: December 4, 2017
- End of Development: December 4, 2019
- End of Support: December 4, 2020

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 6.7 Deprecated Features

The following features are no longer supported in ClearPass 6.7:

- Java for the Windows or macOS ClearPass OnGuard Dissolvable Agents.
- The following TipsAPI (XML), Guest SOAP APIs, and Guest XML-RPC APIs are no longer supported, and are replaced by the indicated RESTful APIs:
  - **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
- VMware ESX 5.1 and earlier.

ClearPass 6.7 Deprecation Notice

The following features will not be supported after ClearPass 6.7:

- ClearPass continually builds on the unified REST API framework to support a wide variety of use cases. All future R&D will focus on this framework. Customers are encouraged to migrate any planned or existing applications to interface with the new API framework. If you still use the TipsAPI (XML),Guest SOAP APIs, or Guest XML-RPC APIs, we recommend that you migrate to the appropriate RESTful API as soon as possible.

- ClearPass 6.7 is the last release to include the Nessus server functionality in the Audit Servers posture category. ClearPass includes the 2.2 release of Nessus Server, which was available as open source software. After the acquisition of Nessus by Tenable Network Security, the project was moved to a proprietary license. ClearPass will continue to work with external Nessus server products, but after 6.7.x it will no longer include the open source version of the code on the shipping product .

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
  - Window Vista — April 11, 2017
- Apple, Inc:
  - macOS 10.6 (Snow Leopard) — February 26, 2014
  - macOS 10.7 (Lion) — October 2014
  - macOS 10.8 (Mountain Lion) — September 2015
  - macOS 10.9 (Mavericks) — September 2016
- Ubuntu:
  - Ubuntu 12.04 (Precise Pangolin) — April 28, 2017

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.

To ensure scalability, dedicate or reserve the processing and memory to the ClearPass virtual appliance instance. You must also ensure that the disk subsystem can maintain the IOP's throughput as detailed below. Most virtualized environments use a shared disk subsystem assuming that each application will have bursts of I/O without a sustained high I/O throughput. ClearPass requires a continuous sustained high data I/O rate.

> **NOTE**
> Starting with the 6.7.0 release, the names of the ClearPass appliance types have changed:
> - CP-SW-EVAL is now CLABV
> - CP-VA-500 is now C1000V
> - CP-VA-5K is now C2000V
> - CP-VA-25K is now C3000V

The CLABV appliance image is for training, configuration testing, and demonstrations. The C1000V, C2000V, and C3000V appliance images should be used for performance and scale testing or to mimic a production environment.

This section includes the following:

- "Supported Hypervisors" on page 92
- "VMware vSphere Hypervisor (ESXi) Requirements " on page 92
- "Hyper-V Requirements " on page 93
- "KVM Requirements" on page 94

For complete information on installing, configuring, or morphing an ESXi™, Hyper-V®, or KVM hypervisor, see the *Tech Note: Installing or Upgrading to 6.7 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, 6.5, or 6.5 U1.
- 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

CLABV (Evaluation OVF)

- 2 reserved virtual CPUs
- 6 GB RAM
- 80 GB disk space required

C1000V (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

C2000V (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

C3000V (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

CLABV (Evaluation VHDX)

- 2 reserved virtual CPUs
- 6 GB RAM
- 80 GB disk space required

C1000V (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

C2000V (5K Virtual Appliance VHDX)

- 8 reserved virtual CPUs
  - Underlying is recommended to have a [PassMark](#)® of 9600 or higher
- 8 GB RAM
- 1000 GB disk required
- 2 Gigabit virtual switched ports

- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105

C3000V (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 required
- 2 Gigabit virtual switched ports
- Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 350

KVM Requirements

Virtual appliance customers who use KVM hypervisors are advised to not apply the ClearPass 6.7.0 upgrade at this time. Our tests have shown a negative performance impact when 6.7.0 is installed on a KVM virtual appliance. To prevent this happening to our customers, at the time of this release we have not posted the virtual appliance image for KVM with the other 6.7.0 images. We are working to resolve the issue in a future patch release. We will then repost the KVM virtual appliance image and let users know we again recommend upgrading to 6.7.0 on KVM hypervisors. (#42601)

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 7, Windows 8.x, Windows 10, and macOS 10.10 and later.
- Google Chrome for macOS and Windows.
- Apple Safari 3.x and later on macOS.
- 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 macOS 10.6, 10.7, 10.8, or 10.9 operating systems. These systems are no longer supported by Apple or by ClearPasss.

The Google Chrome browser no longer supports the Windows XP, Windows Vista, or macOS 10.6, 10.7, 10.8, or 10.9 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

- macOS 10.10 – 10.13

- Ubuntu 12.04 LTS, 14.04 LTS, and 16.04 LTS

- Windows 7, Windows 8.x Pro, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016 are all supported with no service pack requirements. OnGuard does not support Windows 8.x RT or Windows 8.x Phone.

> **CAUTION**
>
> 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.

OnGuard Supported Third-Party Products

> **NOTE**
>
> 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 6.7.3, 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 54: *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)

Table 54: *Third-Party Software Summary*

Product Type	Product Name
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)

> **NOTE**
> 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. To compare to products that were supported by the deprecated 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 the Native Dissolvable Agent. For more information on the Dissolvable Agent, refer to the ClearPass Policy Manager online help.

> **NOTE**
> Users should be aware that the Dissolvable Agent flow might not work on the macOS 10.6, 10.7, 10.8, or 10.9 operating systems because Mozilla no longer supports Firefox on these platforms. (#37967)

> **NOTE**
> The Google Chrome browser stopped supporting updates on the Windows XP, Windows Vista, and macOS 10.6, 10.7, 10.8, or 10.9 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)

> **NOTE**
> 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 these operating systems in this and future releases.

This section includes the following:

- "OnGuard Native Dissolvable Agent Version Information " on page 97
- "OnGuard Java-Based Agent Version Information" on page 98

OnGuard Native Dissolvable Agent Version Information

In current laboratory tests for ClearPass 6.7.3, the browser versions shown in Table 55 were verified for the ClearPass OnGuard Native Dissolvable Agent. 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.

NOTE

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

Table 55: *Native Dissolvable Agent Latest Supported Browser Versions for This Release*

Operating System	Browser
macOS 10.13	Safari 11.x
	Chrome 66.x (#24518, #24986)
macOS 10.12	Safari 11.x
	Chrome 66.x (#24518, #24986)
macOS 10.11	Safari 9.x
	Chrome 66.x (#24518, #24986)
macOS 10.10	Safari 9.x
	Chrome 66.x (#24518, #24986)
Windows 10 64-bit	Chrome 65.x (#24518, #24986)
	Internet Explorer 11.x
	Microsoft Edge 38.x
Windows 10 32-bit	Chrome 65.x (#24518, #24986)
	Internet Explorer 11.x (#25827)
	Microsoft Edge 38.x
Windows 8.1 64-bit	Chrome 65.x (#24986)
	Internet Explorer 11.x
Windows 8.1 32-bit	Chrome 65.x (#24986)
	Internet Explorer 11.x
Windows 8 64-bit	Chrome 65.x (#24986)

Table 55: *Native Dissolvable Agent Latest Supported Browser Versions for This Release (Continued)*

Operating System	Browser
	Internet Explorer 10.x
Windows 8 32-bit	Chrome 65.x (#24986)
	Internet Explorer 10.x
Windows 7 64-bit	Chrome 65.x (#24518, #24986)
	Internet Explorer 11.x (#25827)
Windows 7 32-bit	Chrome 65.x (#24518, #24986)
	Internet Explorer 11.x
Windows 2016 64-bit	Chrome 65.x (#24986)
	Internet Explorer 11.x
Windows Server 2012 R2 64-bit	Chrome 65.x (#24986)
	Internet Explorer 11.x
Windows Server 2012 64-bit	Chrome 65.x (#24986)
	Internet Explorer 10.x
Windows 2008 64-bit	Chrome 65.x (#24986)
	Internet Explorer 8.x (#24766)

OnGuard Java-Based Agent Version Information

In current laboratory tests for ClearPass 6.7.3, the browser and Java versions shown in Table 56 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.

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

> **NOTE** 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 56: *Supported Browser and Java Versions for This Release*

Operating System	Browser	Java Version
Linux - RedHat	Firefox 17.0.10	JRE 1.8 Update 161
Linux - SUSE	Firefox 52.2.0	JRE 1.8 Update 161

ClearPass Onboard Requirements

Onboard's QuickConnect wizard does not support over-the-air provisioning for Windows RT, Windows Phone, or Windows 10 S. Certificate provisioning and enrollment for these devices can be configured through Onboard's **Device Provisioning** pages.

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 6.6.x to 6.7.0.
  - To upgrade a cluster to 6.7.0, we recommend using the **Cluster Upgrade** interface. For more information, see the About the Cluster Upgrade Tool 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 6.7.2 to 6.7.3.
  - To update a cluster to 6.7.3, we recommend using the **Cluster Update** interface. For more information, see the About the Cluster Update Tool 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 6.7

An upgrade is the process of moving from one major release version to another—for example, from 6.6.x to 6.7.0. This section describes accessing upgrade images, considerations to be aware of, and instructions for restoring the log database after the upgrade (optional).

For complete upgrade instructions, please refer to the *Installing or Upgrading to 6.7 on a Virtual Appliance* Tech Note and the *Upgrading to ClearPass 6.7* Tech Note.

- 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**.

This section includes the following:

Upgrade Paths and Version Considerations

Direct upgrades to 6.7.0 are only supported from 6.6.x, 6.5.7, and 6.5.3, with some caveats as described in this section.

For all other versions, direct upgrades are not supported. The specific patch update and upgrade paths described below must be followed instead.

Before you proceed with any upgrade, you should always apply the latest available patch updates for your current release. For information on the patch update procedure, see "Updating Within the Same Major Version" on page 107.

From 6.6.x

Through the Software Updates Portal — Direct upgrades to 6.7.0 are supported for all 6.6.x versions when the upgrade is done through the Software Updates portal's **Import Upgrade Image** option or downloaded or installed through the Web service.

Through the Cluster Upgrade Portal — If a 6.6.7 or 6.6.8 version is upgraded to 6.7.0 through the **Cluster Upgrade** portal, an upgrade preparation patch is required first, and must be applied only to the publisher. This patch is not required for versions 6.6.0 through 6.6.5. The **ClearPass 6.7.0 Upgrade Preparation Patch** specific to 6.6.7 and 6.6.8 is available through the Support site or through the **Software Updates** portal.

> If you are using any ClearPass Extensions, you must first update to 6.6.8 or higher before. upgrading to 6.7.0. Otherwise, extensions will not be backed up and restored to the new version.

From 6.5.7

Direct upgrades to 6.7.0 are supported from 6.5.7, but an upgrade preparation patch is required first. The **ClearPass 6.7.0 Upgrade Preparation Patch** specific to 6.5.7 is available through the Aruba Support site or through the **Software Updates** portal. In a cluster, the preparation patch must be applied to all the appliances in the cluster.

> If you will be using the Cluster Upgrade Tool to upgrade from 6.5.7 to 6.7.0, you must first download and install the Cluster Upgrade Tool Patch for 6.5.7 from either the Support site or through the **Software Updates** portal. This is only required on 6.5.7; it is not needed if you are upgrading from 6.6.x.

From 6.5.3

Direct upgrades to 6.7.0 from 6.5.3 are *only* supported on hardware appliances that were shipped new with 6.5.3 as the base version. An upgrade preparation patch is required first. The **ClearPass 6.7.0 Upgrade Preparation Patch** specific to 6.5.3 is available through the Aruba Support site or through the **Software Updates** portal. In a cluster, the preparation patch must be applied to all the appliances in the cluster.

From Other 6.5.x Versions

From all 6.5.x versions other than 6.5.7 or the 6.5.3 HW appliance, you must first update to 6.5.7 and then follow the 6.7.0 upgrade procedure provided above from 6.5.7.

From 6.4.x

For 6.4.x upgrades, direct upgrades are not supported. You must first update to 6.4.7, then upgrade to either 6.5.7 or 6.6.x, and then follow the appropriate 6.7.0 upgrade procedure provided above from 6.5.7 or 6.6.x.

From 6.3.x

For 6.3.x upgrades, direct upgrades are not supported. You must first update to 6.3.6, then upgrade to either 6.5.7 or 6.6.x, and then follow the appropriate 6.7.0 upgrade procedure provided above from 6.5.7 or 6.6.x.

From 6.2.x or 6.1.x

For 6.2.x and 6.1.x, direct upgrades are not supported. Customers on 6.2.x or 6.1.x must intermediately upgrade to 6.5.7 or 6.6.x first and then follow the appropriate 6.7.0 upgrade procedure provided above from 6.5.7 or 6.6.x.

From 5.2.0

For appliance upgrades from 5.2.0, direct upgrades are not supported. You must upgrade to 6.5.7 or 6.6.x before upgrading to 6.7.0.

Other Upgrade Path Considerations

Insight configurations from Insight versions earlier than ClearPass 6.7 are not retained during migration or upgrade. You will need to manually recreate the pre-6.7 configurations after upgrading to ClearPass 6.7.0.

Before You Upgrade

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

- The stand-by-publisher value should be set to false during the upgrade process to avoid a false failover.

- 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 Table 57 in "Sample Times Required for Upgrade" on page 103.

- Review the hypervisor disk requirements. These are described in "Virtual Appliance Requirements" on page 91 of the "System Requirements for ClearPass 6.7" chapter.

- Any log settings that were modified prior to the upgrade are not retained, and are reset to the default. The administrator should configure any custom log settings again after the upgrade.

> **NOTE**
>
> Log Database and Access Tracker records are not restored as part of the upgrade. If required, you can manually restore them after the upgrade. For more information, please review "After You Upgrade: Restoring Log DB and Access Tracker Records" on page 105.

- 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: Restoring Log DB and Access

---

Tracker Records" on page 105). Please contact Customer Support for configuration recommendations to move away from using the session log database as an authentication source.

- Beginning with the ClearPass 6.7.0 release, ClearPass natively uses a MariaDB connector. The MariaDB Connector/ODBC replaces the mysql-connector package that was installed separately. The MariaDB connector comes with a GLPL license. After you upgrade to ClearPass 6.7.0, you should set the MariaDB connector as the driver for any authentication sources that were mapped to the MySQL driver prior to the upgrade.

- Virtual appliance (VA) 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 6.7.0 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 91.

CAUTION | Never remove SCSI 0:0

Sample Times Required for Upgrade

To help you estimate how much time the upgrade might take, the tables in this section show 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 virtual appliance (VA) installations, upgrade times vary significantly based on the IOPS performance of your VA 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.

The following table shows examples of upgrade times for standalone appliances. Test results are shown for hardware appliances and for virtual appliances.

Table 57: *Standalone Appliances — Sample Total Times Required for Upgrade, Hardware and Virtual Appliances*

Appliance Type	Total Backup Size	Config DB Size	Insight DB Size	Log DB Size	Total Upgrade Time
C2000 (HW)	450 MB	470 MB	120 MB	500 MB	54 minutes
	1 GB	175 MB	6 GB	18 GB	56 minutes
	2.25 GB	200 MB	19 GB	15 GB	75 minutes
C3000 (HW)	450 MB	470 MB	120 MB	500 MB	31 minutes
	1 GB	175 MB	6 GB	18 GB	32 minutes
	2.25 GB	200 MB	19 GB	15 GB	46 minutes

Appliance Type	Total Backup Size	Config DB Size	Insight DB Size	Log DB Size	Total Upgrade Time
C2000V (VA)	450 MB	470 MB	120 MB	500 MB	61 minutes
	1 GB	175 MB	6 GB	18 GB	72 minutes
	2.25 GB	200 MB	19 GB	15 GB	90 minutes
C3000V (VA)	450 MB	470 MB	120 MB	500 MB	39 minutes
	1 GB	175 MB	6 GB	18 GB	45 minutes
	2.25 GB	200 MB	19 GB	15 GB	65 minutes

The following table shows examples of upgrade times for appliances in a cluster. Test results are shown for publishers and subscribers, and for various combinations of hardware appliances and virtual appliances.

Table 58: *Cluster Appliances — Sample Total Times Required for Upgrade, Hardware and Virtual Appliances*

Example #	Publisher or Subscriber?	Config DB Size	Insight DB Size	Appliance Type	Total Upgrade Time
1	Publisher (WAN)	100 MB	—	VA-5K to C2000V (VA)	22 minutes
	Subscriber	100 MB	20 GB (Insight Master)	HW-25K to C3000 (HW)	41 minutes
	Subscriber	100 MB	20 GB	HW-5K to C2000 (HW)	37 minutes
2	Publisher	300 MB	25 GB (Insight Master)	HW-25K to C3000 (HW)	43 minutes
	Subscriber	300 MB	25 GB	HW-5K to C2000 (HW)	39 minutes
	Subscriber (WAN)	300 MB	—	VA-5K to C2000V (VA)	23 minutes
3	Publisher	500 MB	60 GB (Insight Master)	HW-25K to C3000 (HW)	1 hour 5 minutes
	Subscriber 1	500 MB	60 GB	HW-25K to C3000 (HW)	53 minutes
	Subscriber 2 (WAN)	500 MB	—	VA-5K to C2000V (VA)	23 minutes
4	Publisher	1 GB	70 GB (Insight Master)	HW-25K to C3000 (HW)	1 hour 36 minutes

Example #	Publisher or Subscriber?	Config DB Size	Insight DB Size	Appliance Type	Total Upgrade Time
	Subscriber 1	1 GB	70 GB	HW-25K to C3000 (HW)	1 hour 7 minutes
	Subscriber 2 (WAN)	1 GB	—	VA-5K to C2000V (HW)	26 minutes

After You Upgrade: Restoring Log DB and Access Tracker Records

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
```

After You Upgrade on ESXi Servers: Establishing NW Connectivity

If you are upgrading ClearPass from 6.5.x or 6.6.x to 6.7.0 on a VMware ESXi server, and only if the MAC address of **Network adapter1** is higher than that of **Network adapter2**, additional steps are required after the upgrade. (#41698)

After upgrading, follow the steps below in order for ClearPass to have network connectivity:

1. After you upgrade to 6.7.0, log in to the console as appadmin and use the CLI command **<system shutdown>** to shut down the ClearPass server. This step must be done only through the console.

2. After the command is executed, wait for the virtual appliance to shut down completely.

3. Edit the ClearPass virtual appliance settings in the vSphere client and remove the two Ethernet adapters that are named **Network adapter1** and **Network adapter2**.

4. Add two new network adapters with the names **Network adapter1** and **Network adapter2** and of type **Ethernet Adapter**. Network adapter1 should be the management port connected to SwitchManagement, and Network adapter2 should be the data port connected to SwitchData.

5. Save the new settings and start the ClearPass virtual appliance.

6. Log in to the ClearPass console using the appadmin account, and then run the following CLI command to refresh the network settings:

   `system refresh-network`

7. After the refresh command is executed, reboot the ClearPass virtual appliance to establish network connectivity.

After You Upgrade on Hyper-V Servers: Establishing NW Connectivity

If you are upgrading ClearPass from 6.5.x or 6.6.x to 6.7.0 on a Hyper-V server, additional steps are required after the upgrade. (#41698)

ClearPass 6.5.x and 6.6.x Hyper-V images were shipped with network adapters of type "Legacy Network Adapter". CentOS version 7 does not support the Legacy Network Adapter type, therefore ClearPass 6.7.0 Hyper-V images do not support the Legacy Network Adapter type. After upgrading from ClearPass 6.5.x or 6.6.x to 6.7.0, you must follow the steps below in order for ClearPass to have network connectivity:

1. After you upgrade to 6.7.0, log in to the console as appadmin and use the CLI command **<system shutdown>** to shut down the ClearPass server. This step must be done only through the console.

2. After the command is executed, wait for the virtual appliance to shut down completely.

3. Edit the ClearPass virtual appliance settings in the Hyper-V manager and remove all three network adapters (these are named **NIC0**, **NIC1**, and **Network Adapter**).

4. Add two new network adapters with names of type **Network Adapter**.

5. Edit the network adapters. Make the first one the management port connected to SwitchManagement, and make the second one the data port connected to SwitchData.

6. Save the new settings and start the ClearPass virtual appliance.

7. Log in to the ClearPass console using the appadmin account, and then run the following CLI command to refresh the network settings:

```
system refresh-network
```

8. After the refresh command is executed, reboot the ClearPass virtual appliance to establish network connectivity.

> **NOTE**
>
> Do not use the Cluster Upgrade Tool to upgrade ClearPass clusters from 6.5.x or 6.6.x to 6.7.0 on a Hyper-V server. Doing so will cause the appliance to lose network connectivity after the upgrade and will require manual intervention from the administrator to regain connectivity.

After You Upgrade: Restoring Insight Configurations

If you are upgrading from a version earlier than ClearPass 6.6, Insight configurations are not retained during the migration or upgrade. After the upgrade, you must manually recreate the Insight configurations.

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 6.7.2 to 6.7.3. 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" on page 108

> The stand-by-publisher value should be set to false during the patch update process to avoid a false failover.

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.

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.

After You Update: Performing a Patch Rollback

After a cumulative patch is applied, the CLI command **system patch-rollback** allows administrators to revert to the last version that was installed on the system. For example:

- if a system was at 6.7.2 and cumulative update 6.7.3 is applied, it can be reverted to 6.7.2 through the **system patch-rollback** command.

- If a system was at 6.7.0 and cumulative update 6.7.3 is applied, it can be reverted to 6.7.0 because that was the last installed version. It cannot be reverted to 6.7.2.

This command can be used if a problem is found after the patch update, such as an issue identified in production that was not identified during testing, resulting in a degradation of capabilities.

Before using this command to revert from 6.7.3 to the last installed 6.7.x version, you must first download the **ClearPass 6.7 Rollback RPM Package** from the **Software Updates** portal and install it.

As part of the patch rollback feature, users should be aware of the following:

- As best practice, users should always take a data backup before an update.

- This command cannot be used after an upgrade to revert to an earlier major version (for example, 6.6.x).

- Although you can only roll back to the last version that was installed on the appliance, if multiple hotfix patches are included within the cumulative patch version you are rolling back from, then you can roll back multiple hotfix patches, one at a time, to a specific hotfix within the current version. To roll back to the previously installed version, you must first roll back each intervening hotfix patch.

- When this command is used in a cluster, it must be done to all the appliances in the cluster. The publisher must be rolled back first, followed by each subscriber individually. The rollback must be completed on all appliances in the cluster within 24 hours after the publisher rollback is initiated in order to maintain the cluster status.

- Any custom skins that are installed in the current version are retained after the rollback to the earlier version.

- System rollback events are logged in the **Event Viewer**.