ClearPass 6.0.2 Patch 2

Release Notes

Copyright

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

ARUBA® networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Preface

ClearPass 6.0.2 Patch 2 is a cumulative monthly patch release that introduces new features and provides fixes to previous outstanding issues. These release notes contain the following chapters:

- Chapter 2, "Upgrade Procedure" on page 9—Provides upgrade instructions and considerations.
- Chapter 3, "What's New in This Release" on page 11—Describes new features and issues introduced in this 6.0.2 release as well as issues fixed in this 6.0.2 release.
- Chapter 4, "Enhancements in Previous 6.x Releases" on page 15—Describes new features introduced in earlier 6.0.x releases.
- Chapter 5, "Issues Fixed in Previous 6.x Releases" on page 21—Lists issues fixed in previous 6.0 releases.
- Chapter 6, "Known Issues Identified in Previous Releases" on page 25—Lists extant known issues identified in previous 6.0 releases.
- Chapter 7, "Introducing the Integrated Platform" on page 29—Introduces the integrated ClearPass platform for users migrating from Amigopod 3.9.x.

Supported Browsers

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

- Microsoft Internet Explorer 7.0 and later on Windows XP, Windows Vista, and Windows 7
- Mozilla Firefox on Windows XP, Windows Vista, Windows 7, and Mac OS
- Google Chrome for Mac OS and Windows
- Apple Safari 3.x and later on Mac OS
- Mobile Safari 5.x on iOS

NOTE

Microsoft Internet Explorer 6.0 is now considered a deprecated browser. You might encounter some visual and performance issues when using this browser version.

System Requirements

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

Virtual Appliance Requirements

The following specifications are recommended in order to properly operate Aruba ClearPass Policy Manager in 64-bit VMware ESX or ESXi server environments. To ensure successful deployment and maintain sufficient performance, verify that your hardware meets the following minimum specifications.

Supported ESX/ESXi Versions

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

CP-VA-500

- 2 Virtual CPUs
- One (1) - 250 GB disk space
- 4 GB RAM
- 2 Gigabit virtual switched ports (Only 1 needed if not using separate ports for data and management)

Table 1 *Disk I/O Performance Requirements for the Hardware Appliance*

Number of Disks:	1
Capacity:	500 GB (7.2K rpm)
RAID:	No RAID
Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 75	

CP-VA-5K

- 8 Virtual CPUs
- 512 GB disk space
- 8 GB RAM
- 2 Gigabit virtual switched ports (Only 1 needed if not using separate ports for data and management)

Table 2 *Disk I/O Performance Requirements for the Hardware Appliance*

Number of Disks:	2
Capacity:	500 GB (7.2K rpm)
RAID:	RAID 1
Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 105	

CP-VA-25K

- At least 12 Virtual CPUs (Aruba hardware appliances ship with 24 cores)
- 512 GB disk space
- At least 24 GB RAM (Aruba hardware appliances ship with 48GB RAM)
- 2 Gigabit virtual switched ports (only 1 needed if not using separate ports for data and management)

Table 3 *Disk I/O Performance Requirements for the Hardware Appliance*

Number of Disks:	4
Capacity:	300 GB (10K rpm)
RAID:	RAID 10
Functional IOP rating for a 40-60 read/write profile for 4K random read/write = 350	

Note: In order for a CP-VA-25K virtual appliance to properly support up to 25,000 unique authentications with full logging capability, customers should match the number of CPUs and RAM that ship in our hardware appliances. If you do not have the VA resources to support a full workload, please consider ordering the Policy Manager hardware appliance.

Evaluation version

- 2 Virtual CPUs
- 40 GB disk space
- 4 GB RAM
- 2 Gigabit virtual switched ports (only 1 needed if not using separate ports for data and management)

Note: VMware Player is not supported. Please contact Aruba customer support at support@arubanetworks.com with any further questions or if you need any additional assistance.

Use of Cookies

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

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

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
End of Support information	www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Chapter 2

Upgrade Procedure

This chapter provides instructions and considerations for upgrading to the 6.0.2 release.

Upgrading to ClearPass Policy Manager 6.0.2

- You can upgrade to ClearPass Policy Manager 6.0.2 only from ClearPass Policy Manager 6.0.1 at **Administration > Agents and Software Updates > Software Updates**.
- Direct upgrades are not supported from any versions prior to ClearPass Policy Manager 6.0.1. Customers with prior versions must upgrade to ClearPass Policy Manager 6.0.1 first before upgrading to 6.0.2.
- You cannot upgrade to 6.0.2 from any evaluation version.

Before You Upgrade

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

- User modifications on default services (dynamically received data such as Guest SSID) will not be carried forward after the upgrade. You must configure these inputs again after you upgrade.
- Data filter and Syslog Export filter configurations will be removed after the upgrade. You may have to reconfigure them.
- If you are upgrading a ClearPass Policy Manager 6.0.1 production virtual machine, you must add an additional hard disk (SCSI 0:2) to the VM before you upgrade. Please refer to the ClearPass VMware installation instructions Tech Note available in the Deployment Guides section at support.arubanetworks.com.

NOTE

Due to a known issue in this release, the subscription ID is not retained when you upgrade to CPPM 6.0.2. After you upgrade, you must re-enter the subscription ID at **Administration > Agents and Software Updates > Software Updates**. This is the same subscription ID that was used for 6.0.1, and is required in order to receive software updates.

Chapter 3

What's New in This Release

This chapter provides a brief summary of the new features and changes in the ClearPass 6.0.2 Patch 2 release.

This chapter contains the following sections:

- "Release Overview" on page 11
- "New Features and Enhancements in the 6.0.2 Patch 2 Release" on page 11
- "Issues Resolved in the 6.0.2 Patch 2 Release" on page 11
- "New Known Issues in the 6.0.2 Patch 2 Release" on page 13

Release Overview

In ClearPass 6.0.x, all ClearPass applications - ClearPass Policy Manager (CPPM), Profile, OnGuard, Guest, and Onboard—run on a common platform, using common platform services, and have a common look and feel.

New Features and Enhancements in the 6.0.2 Patch 2 Release

Policy Manager

Subscription-Based Application License Generation

Policy Manager now generates licenses for all platform applications based on subscription information. License duration units are displayed in the **Duration** column of the **Servers** tab at **Administration > Server Manager > Licensing**. (#12668)

Hourly Certificate Revocation Lists Supported

ClearPass Policy Manager now supports more frequent Certificate Revocation List (CRL) checks. New CRLs may be issued on an hourly basis. (#12640)

Issues Resolved in the 6.0.2 Patch 2 Release

The following issues have been fixed in the ClearPass 6.0.2 Patch 2 release.

Policy Manager

Table 4 below lists resolved issues in Policy Manager 6.0.2 Patch 2:

Table 4 *Policy Manager Issues Fixed in 6.0.2 Patch 2*

Bug ID	Description
11994	Corrected an issue where restoring from a 6.0.1 backup could lead to duplicate intermediate CA certificates being installed in the CPPM trust list, and one was empty.
12714	Corrected an issue where, during the upgrade from 6.0.1 to 6.0.2, the order of services was changed, causing authentications to fail.
12728	The Web login vendor settings for Ruckus were updated to support ZoneDirector 8.0.

Table 4 *Policy Manager Issues Fixed in 6.0.2 Patch 2 (Continued)*

Bug ID	Description
12778	Corrected an issue where, in a few cases where a machine was at peak memory capacity, a page's HTML was displayed before the java applet user interface page could be launched.
12816	Corrected an issue where the Administrator user interface was not accessible due to a race condition during database re-indexing.
12912	Corrected an issue where after applying a cumumlative patch to CPPM (using HTTP proxy) the Administrator user interface could not be accessed.
12988	Integration with MobileIron now allows CPPM's Mobile Device Management to detect an asset's compromised status and save it to the Endpoint.
13002	Corrected an issue where the update frequency interval under the Endpoint Context Servers did not poll as per the configured interval, although manual updates were successful.

AirGroup

Table 4 below lists resolved issues in AirGroup 6.0.2 Patch 2:

Table 5 *AirGroup Issues Fixed in 6.0.2 Patch 2*

Bug ID	Description
12521	Corrected an issue where editing an AirGroup device did not send a CoA request to configured AirGroup controllers.

Guest

Table 6 below lists resolved issues in Guest 6.0.2 Patch 2:

Table 6 *Guest Issues Fixed in 6.0.2 Patch 2*

Bug ID	Description
12439	Guest accounts without a specific activation time were previously created with an activation time set to the UNIX epoch (1970-01-01 00:00 UTC). The activation time is now set to the account creation time instead.
12664	Corrected an issue where the guest self-registration action "Display a link enabling a guest receipt via email/SMS" was not displayed.
12808	Corrected an issue where a guest-sponsored self registration on a subscriber generated an incorrect link in the confirmation email. Clicking on the link resulted in an Internal Error message.
12852	Corrected the behavior of ClearPass Guest to always use the HTTP proxy settings that have been configured in ClearPass Policy Manager. (This configuration is set in CPPM at **Administration > Server Manager > Server Configuration > select server > Service Parameters > ClearPass System Services > HTTP Proxy**).
12886	Corrected an issue where the Mobile Carrier (visitor_carrier) field was not being loaded on the Create Account (create_user) and List Accounts > Edit Account (guest_edit) forms.
12903	A security enhancement ensures that the session cookie's ID is always changed when the user logs in or out.
12977	Corrected a database query error shown on the Active Sessions page if the operator filter was set to "Only show accounts created by the operator."

Onboard

Table 7 below lists resolved issues in Onboard 6.0.2 Patch 2:

Table 7 *Onboard Issues Fixed in 6.0.2 Patch 2*

Bug ID	Description
12655	Corrected an issue when Onboard was used to install the ClearPass OnGuard agent on the Windows operating system. The client error message displayed was “Could not read the source FSX. Invalid window handle.”

New Known Issues in the 6.0.2 Patch 2 Release

No significant new issues have been identified since the last release. For a list of known issues found in previous 6.0.x releases, see Chapter 6, “Known Issues Identified in Previous Releases” on page 25.

Chapter 4

Enhancements in Previous 6.x Releases

This chapter provides a brief summary of the features and enhancements introduced in previous ClearPass 6.0.x releases.

Features and Enhancements in Previous 6.0.x Releases

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

Policy Manager

- ClearPass Policy Manager now includes the ability to integrate with various MDM vendors such as Mobile Iron, Maas360, AirWatch, JAMF, and SOTI. ClearPass Policy Manager can fetch mobile endpoint information to make policy enforcements from these MDM servers. A new screen, “Endpoint Context Servers,” is available under the Administration menu.
- ClearPass Policy Manager can now be configured to pull AP related context from Aruba Activate. This allows CPPM to maintain a white list of APs that can be used to authenticate them into the network.
- Authorization attributes can now have data types associated with them (for example, AD:Department = String). This ensures that the correct operator (LESS_THAN, EQUALS, CONTAINS, etc.) is used for that attribute while creating policies in CPPM.
- ClearPass Policy Manager now supports remote authentication survivability for 802.1X (PEAP) authentications in an Aruba Instant network.
- ClearPass Policy Manager’s administration GUI has been localized to the following languages – Japanese and Simplified Chinese.
- RADIUS CoA actions can now be sent for multiple endpoints (MAC addresses) via the Command Line and Control API.
- Custom SQL support is included for Data filters and Syslog Export filters.
- Product version, engine version, and data-file version checks can be enabled generally to any product that is installed on the client without having to select a specific anti-virus/anti-spyware vendor. These options are added using the “Allow any Product” check box in the ClearPass Windows Universal System Health Validator. These options are also available for “ClearPass Linux Universal System Health Validator” and “ClearPass Mac OS X Universal System Health Validator” plugins also.
- The CPPM Access Tracker is now restricted to viewing authentication/authorization information for 7 days. Insight can be used to generate reports for authentication/authorization information for up to 2 years in the past.
- A new “API Administrator” privilege level was added. An API Administrator has access to only the configuration API operations and not the UI itself.
- Licensing framework is enhanced to include ClearPass Guest, ClearPass Onboard, and the all-new Advanced Technology license. A separate Profile license no longer exists; it is part of the base platform license. Associated with this is a new, consolidated view of all licensing information. This can be found on the **Administration > Server Manager > Licensing** page.
- ClearPass has switched from disk-based encryption to file/directory-based encryption. This enables ClearPass to support variable sized disks and upgrades in a VM environment.

- ClearPass now supports pushing per-session dynamic roles (via the Aruba Downloadable Role Enforcement Profile) to both the Mobility Access Switches (version 7.2) and the Controllers.
- Post-authentication rules (implemented via post-authentication Enforcement Profiles) are new in CPPM 6.0.1. The enforcement profiles support use cases such as MAC caching and session and bandwidth restrictions.
- ClearPass Policy Manager now supports Oracle DB as a SQL-based Authentication and Authorization Source.
- ClearPass now supports creating GRE tunnels and VLAN interfaces from the **Server Configuration** page.
- VM upgrades are now supported. Note that this is only applicable to versions starting with 6.0. VM upgrades from versions prior to 6.0 are not supported.
- Software patches and upgrades are supported from within the user interface. Anti-virus, anti-spyware, Windows hotfixes, and fingerprint updates have been consolidated with firmware and patch updates into a single page under **Administration > Agents and Software Updates > Software Updates**.
- Remote Desktop Sessions to the Windows clients can now be controlled (Allow/Deny) via ClearPass OnGuard. This was not supported in previous versions.
- ClearPass Audit Viewer now includes create and update events from the Guest and Onboard applications.

AirGroup

The AirGroup feature was added to the ClearPass platform. AirGroup allows users to register their personal mobile devices on the local network and define a group of friends or associates who are allowed to share them. The ClearPass Policy Manager base license includes AirGroup functionality.

AirGroup configuration is distributed across ClearPass Policy Manager and ClearPass Guest. You use ClearPass Guest to define AirGroup administrators and operators. AirGroup administrators can then use ClearPass Guest to register and manage an organization's shared devices and configure access according to username, role, or location. AirGroup operators (end users) can use ClearPass Guest to register their personal devices and define the group who can share them. AirGroup operators can also be authenticated via LDAP.

For complete AirGroup information, refer to the ClearPass Guest Deployment Guide and the AirGroup Deployment Guide.

Guest

- The following methods are available for use with the {nwa_radius_query} function: GetUserFirstLoginTime, GetUserCumulativeUsage, GetIpAddressCurrentSession, and GetUserActiveSessionCount. (#11046, #11976)
- Application log data retention is now controlled by a cluster-wide parameter. Events are stored in the Application Log for seven days by default. To review a record of significant runtime events and configuration changes prior to the last seven days, go to **ClearPass Policy Manager > Monitoring > Audit Viewer**. (#12121)
- The Application Log user interface was enhanced to provide better search, export, and navigation capabilities. The Search tab was replaced by a filter and keyword features. You can use the filter to view events and messages from a different time frame, can filter by time or severity, and can use keywords or phrases in a search. Export options are more efficient, and allow you to specify a range of pages and a download limit. (#11113)
- New icons were added to the Guest Manager module's List Accounts, Edit Account, and List Devices pages to indicate the state of the user or device account. (#11126)

- When exporting guest accounts, a new format is used that is compatible with the ClearPass Policy Manager import/export format. The new default XML format consists of a <GuestUsers> element containing a <GuestUser> element for each exported guest account. The numeric ID of the guest account is provided as the "id" attribute of the <GuestUser> element. (#11887)
- Two SMS SMTP carrier enhancements were made to SMS Services (#12119):
  - When SMS over SMTP is selected as the SMS Gateway service on the Create SMS Gateway form, the form expands to include the new Carrier Selection field. Options in this field let you choose how the carrier will be determined. You can configure carrier settings on the Create SMS Gateway form, specify a carrier, or let the visitor enter their carrier on the registration form.
  - When the SMS over SMTP option is used, a new list view, SMTP Carriers, is added to the left navigation. The Create tab on this list opens the new SMS SMTP Carrier Editor form. You can use the list and editor to manage the list of SMTP carriers that are included in the Mobile Carrier drop-down list on the SMS Services > SMS Gateways > Edit SMS Gateway form. Options in the editor also let you create an SMS gateway that sends a hardcoded email address or include a mobile phone number in the subject line.
- The new Import Configuration form lets you import selected items from a ClearPass Guest 3.9.x configuration. (#11090)
- A new logging level, **Debug**, was added to the configuration options for the Guest Services plugin. When this option is selected, the application log includes details of ClearPass Policy Manager API requests and responses. (#10414)
- The AirGroup Services plugin was added to the plugin list. AirGroup administrators can add and configure AirGroup controllers. (#10232, #10459, #10590)
- A new form, Authentication, allows you to configure HTTP and RADIUS authentication options for the ClearPass Guest application. (#10560)
- The {nwa_radius_query} function is enhanced to also return the corresponding user and role information (in the _user and _role keys, respectively) when performing a query that returns a single session. (#11587)
- When a Web login page is configured to perform a pre-authorization check using RADIUS, the RADIUS vendor-specific attribute **Aruba-Port-Id** will be set to the name of the Web login page. This allows services defined in Policy Manager to determine which captive portal page is being used for authentication. (#11757)
- AirGroup allows users to register their personal mobile devices on the local network and define a group of friends or associates who are allowed to share them. If AirGroup Services is enabled, AirGroup administrators can provision their organization's shared devices and manage access, and AirGroup operators can register and provision a limited number of their own personal devices for sharing.
- The Guest Manager plugin configuration provides more options for random passwords. You can specify special characters, numbers, and letters to exclude from random passwords as well as user-generated passwords—for example, letters and numbers that can look similar, such as i, l, 1, 0, O, o, 5, S. (#11423)
- SMS receipts can now include the guest's username and password in the login URL. This allows the guest to click the Login button once and have their login info automatically entered, and not have to copy and paste or remember their password between screens. (#11821)
- The following tasks are described in the "Operator Logins" chapter of the "ClearPass Guest Deployment Guide":
  - Create AirGroup administrators—See the "Local Operator Authentication" section
  - Create AirGroup operators—See the "Local Operator Authentication" section
  - Configure an operator's device limit— See the "Creating an Operator Profile" section

  - Authenticate AirGroup users via LDAP and define the LDAP server—See the “LDAP Operator Authentication” section
  - Define appropriate translation rules—See the “LDAP Translation Rules” section
- Support was added for more complex email address formatting for SMS and SMTP, such as addresses that prepend the phone number to the email address using the "." character as a separator—for example, 4085551212.myname@domainname.com. (#11538)

Insight

- Insight 2.0 is a completely revamped version of the Policy Manager reporting, analytics, and alerting tool. This new version also includes Guest and Onboard reporting. The ClearPass Policy Manager built-in reporting tool (Activity Reports) is deprecated and removed from the UI. Report configuration and generation will be part of Insight.

Onboard

- The Network Settings editor now includes an **Enabled** check box, allowing you to set the enabled or disabled status while configuring the network. (#10096)
- 6.0.2 provides the option to generate the certificate on the client for iOS devices. The default provisioning setting is to generate the certificate on the client, which will not create an Onboard Device entry in ClearPass Policy Manager. On the **General** tab of the **Onboard > Provisioning Settings** page, select a “**created by server**” option for the Key Type to generate Onboard Device accounts in ClearPass Policy Manager.
- Enhancements for uploading trusted certificates were added in two places (#10710):
  - Trusted certificates can now be imported from the Certificate Management page.
  - Trusted certificates can also be uploaded directly from the **Trust** tab of the **Network Settings** form when you are configuring the network settings that will be provisioned to a network’s devices. To use this feature, go to **Onboard > Network Settings**, click the network’s row in the list, then click its **Edit** link. On the **Trust** tab, choose to configure trust settings manually, then use the options in the **Upload Certificate** row.
- Checks are now made for potentially insecure network configurations in the **Onboard > Network Settings** form. A warning message is displayed if selections are made in the **Dynamic Trust** or **Windows Trust** rows that could potentially expose the user to security problems. (#11114)
- When exporting a certificate from the Certificate Management list, the Open SSL text format is now available. This option allows you to view advanced details such as X509v3 extensions. It also includes the certificate in .pem format appended to the .txt file. (#12006)
- Support was added for Android rootkit detection. Onboard can be configured to prevent Android devices with a rootkit from being provisioned. This option is available on the **Android** tab of the **Provisioning Settings** form. (#12071)
- Onboard can now automatically detect the appropriate certificate trust settings for your deployment. When this option is selected on the **Trust** tab of the **Network Settings** editor, the Trusted Certificates, Upload Certificate, Dynamic Trust, Android Trust, and Windows Trust fields are automatically configured and are not displayed on the form. In the new Configure Trust drop-down list, you can choose this option or you can choose to configure trust settings manually. Automatic configuration is the default. (#12178)
- The new **Applications** form supports installation of applications during device provisioning. You can mark individual Windows applications for installation, and can specify whether they should be restarted when the device is provisioned. If restart is selected, you can specify whether the restart should take effect when the installation is complete or at a later time. This feature is currently available for Windows devices. (#9903)

- ClearPass OnGuard is now available in the **Onboard > Applications** list as an application that may be installed during device provisioning for Windows devices.
- The text that is displayed to users of different types of devices before, during, and after provisioning their device can now be customized using the **Onboard > Provisioning Settings** form. (#9990)
- The **Provisioning Settings** form is now organized in tabs. The iOS & OS X, Legacy OS X, Windows, and Android tabs include the fields for customizing the text displayed to the user in the onboarding process. The General and Onboard Client tabs contain provisioning settings that apply to all devices. (#9990)
- Onboard now supports multiple network configurations. A network configuration can be wired-only, wireless-only, or both wired and wireless. (#9900)
- A new column, **Device Type**, was added to the Certificate Management view. This column shows the type of device associated with the certificate in the same row. An identifying icon is also displayed for each device type. (#11123)
- To clarify certificate usage, the term **tls-server** was replaced with the term **trusted** in the **Type** column for the certificate. (#10709)
- A new row, **Profile Type**, was added to the **iOS and OS X** tab of the **Provisioning Settings** form, allowing you to select the type of profile to create when an OS X 10.7 (or later) device is provisioned. The drop-down list in this row includes two options. The **User** option creates a per-user profile; the **System** option creates a system profile. The System option can be used in settings where the device has several users and a single profile might be preferred to individual user profiles—for example, where an iMac in a high school classroom is used by all the students. (#10667)
- Support was added for having a device automatically join a network when it is provisioned. When this option is chosen, if only one network is available to the user, the device will be connected automatically. If multiple networks are available, the user will be able to choose the network to connect to. If the Automatically join network option is not chosen, an option to manually connect to the network will be shown to the user. To use this feature, go to **Onboard > Network Settings**, click the **Edit** link for the network, and click the **Access** tab. (#10127)
- The ClearPass Policy Manager server certificate is automatically listed in the Onboard certificate management list view as a trusted certificate. This simplifies the process of setting up an 802.1X network configuration where CPPM is the authentication server and EAP termination point. Updates to the server certificate are also automatically reflected in Onboard's certificate management list. (#11607)

OnGuard

- ClearPass OnGuard now supports the Windows 8 operating system.
- Remote Desktop Sessions to the Windows clients can now be controlled (Allow/Deny) via ClearPass OnGuard. This was not supported in previous versions.
- ClearPass Audit Viewer now includes create and update events from the Guest and Onboard applications.
- The ClearPass OnGuard Agent can now perform remediation actions (Disable/Allow) against the type of networks connections that are not to be allowed on a client machine.
- Support for health checks through ClearPass OnGuard in Windows XP SP2 is discontinued with the 6.0.1 release.
- The ClearPass OnGuard agent now supports the Windows Security Health Validator plugin. This was supported only in the NAP Agent in prior releases.
- ClearPass OnGuard can now check for clients hosting virtual machines and can make remediation actions accordingly.

Issues Fixed in Previous 6.x Releases

The following issues were fixed in previous 6.x releases. For a list of issues resolved in the 6.0.2 Patch 2 release, see the What’s New in This Release chapter.

Fixed in 6.0.2

Policy Manager

Table 8 below lists resolved issues in Policy Manager 6.0.2:

Table 8 *Policy Manager Issues Fixed in 6.0.2*

Bug ID	Description
	CPPM now supports downloadable ACLs for Cisco ASA.
	Access tracker now displays more details about why a client is deemed unhealthy, such as a list of missing hotfixes or antivirus protection not being up-to-date.
	Support was added for Certificate Revocation Lists (CRLs) through HTTP proxy.
	The CPPM Read Only administrator can now download and install software through the Software Update portal.
	Evaluation license counts for applications (OnGuard, Onboard, Guest) are removed from the total count available after the evaluation period expires.
	Syslog Export filters now can send RADIUS accounting information to Syslog servers from switches, WLCs that do not send class attribute in their RADIUS accounting exchange with CPPM.

AirGroup

Table 8 below lists resolved issues in AirGroup 6.0.2:

Table 9 *AirGroup Issues Fixed in 6.0.2*

Bug ID	Description
11924	The description of the airgroup_shared_user field was updated, and the Quick Help text for the AirGroup Operator and AirGroup Administrator list views was improved. The available user-based and role-based sharing options are now more accurately described in ClearPass Guest's AirGroup forms.
11933	The default UDP port number for new AirGroup controllers was changed to 5999 to match the default settings of Aruba Instant and Aruba OS 6.3.

Guest

Table 10 below lists resolved issues in Guest 6.0.2: Onboard

Table 10 *Guest Issues Fixed in 6.0.2*

Bug ID	Description
9241	To enhance security, Cross-Site Request Forgery (CSRF) protection was implemented.
10535	Hotspot Manager was not available in the 6.0 and 6.0.1 releases. It was restored in the 6.0.2 release.
11799	The functionality to send a test email message was not available in the 6.0 and 6.0.1 releases. It was restored in the 6.0.2 release. To use this feature, go to **Configuration > Email Receipt**.

Table 10 *Guest Issues Fixed in 6.0.2 (Continued)*

Bug ID	Description
11800	If both the CPPM and Guest session cookies timed out, the Guest login page was displayed for an operator even after they logged back in to ClearPass Policy Manager.
11844	Changing the expiration time of a MAC device updated the account information correctly, but displayed the account incorrectly in the user interface.
11846	Support was added for **Guest Manager > Import Accounts** to automatically recognize and accept the XML format generated when saving guest accounts from ClearPass Policy Manager. The Key Type field now includes the following options: ● 1024-bit RSA – created by device ● 2048-bit RSA – created by device ● 1024-bit RSA – created by server ● 2048-bit RSA – created by server ● 4096-bit RSA – created by server The “created by device” options use SCEP to provision the EAP-TLS device certificate, so the private key is known only to the device rather than also known by the user. When a “created by device” option is selected, the generated key is used instead of a username/password authentication defined in Network Settings.
11873	TLS was added as a supported option for Onboard provisioned network settings for Windows, Legacy S X, and Android, enabling provisioning of the client certificate through Onboard enrollment for these platforms.
11951	Disconnecting an active session failed if the cluster password was different from the administrator account password.
11961	The default values for File Upload size and Form Post maximum size were updated to 15 MB.
12085	The functionality to create an SMS service when a subscription ID was entered was not available in the 6.0 and 6.0.1 releases. It was restored in the 6.0.2 release. A ClearPass Guest SMS Service entry is automatically created on the Administration > SMS Services > SMS Gateways list when the subscription ID is entered in ClearPass Policy Manager. The subscription ID is used as the username and password.
12109	Matching pre-registration fields for a guest account failed under certain circumstances.
12120	An application log message “PHP Notice: Language not supported: ja” was repeatedly logged when using the Japanese Translations plugin. This notice was harmless and did not indicate a problem.
12162	The error message was improved that is shown when a disconnect action from the Active Sessions list cannot be completed by the controller.
12223	Overriding a Create form with a self-registration form now works for List Accounts > New Visitor Account.
12384	An NAS login used HTTPS for submitting user credentials even when it was configured to use HTTP.

Table 11 below lists resolved issues in Onboard 6.0.2:

Table 11 *Onboard Issues Fixed in 6.0.2*

Bug ID	Description
11216	For HTC phones running Android 3.x and later, a self signed certificate for the CPPM server is not sufficient for proper trust setting. **Workaround**: Do one of the following: ● Have the CPPM server certificate issued by the Onboard CA, then push the Onboard CA root certificate to the phone as a trusted certificate. To do this, on the **Onboard > Network Settings > Trust** tab, use the **Configure Trust Settings Automatically** option. ● Have the CPPM server certificate issued by an external CA, then push the external CA root certificate to the phone as trusted certificate.
11725	Attempting to reprovision a device could result in a 404 Page Not Found error.
11978	A “Profile could not be decrypted” error was sometimes shown when trying to onboard an iOS device.
12011	It was not possible to change back to the “None” setting for the Android Trusted Certificate in Onboard.

Table 11 *Onboard Issues Fixed in 6.0.2 (Continued)*

Bug ID	Description
12036	On the Certificate Management page, trusted certificates that were imported into Onboard can now be deleted at any time after import.
12103	The Aruba QuickConnect client on Android 4.1.2 generated an error if the device's lock-screen password was not already set.

Fixed in 6.0.1

Policy Manager

Table 12 lists resolved issues in Policy Manager 6.0.1.

Table 12 *Policy Manager Issues Fixed in 6.0.1*

Bug ID	Description
	Cluster passwords can contain special characters within them. These special characters will no longer affect cluster join operations.
	Alert notifications can be added in Access Tracker if Crypto binding TLV is disabled on the CPPM server side but enabled on client side.
	This version includes enhanced support for multiple AD domains along with some fixes for issues found in previous versions.
	Fixed several issues that caused Machine Authentication Caching to be purged due to time out failures.
	Fixed issues relating to Access Tracker, System Monitoring, and Analysis and Trending records not being shown due to delays in DB write.
	Online Help documentation has now been updated for all the new features released in ClearPass Policy Manager 6.0.1.
	Online Help documentation for Insight is now available.
	The browser-based OnGuard dissolvable agent can now collect health data on Windows 7 64-bit OS platforms.

Guest

Table 13 lists resolved issues in Guest in 6.0.1.

Table 13 *General ClearPass Guest Issues Fixed in 6.0.1*

Bug ID	Description
10798	Error handling is improved for certain SQL errors that could be generated.

Onboard

Table 14 lists resolved issues in Onboard in 6.0.1.

Table 14 *Onboard Issues Fixed in 6.0.1*

Bug ID	Description
11186, 11249	CPPM now correctly returns the Session-Timeout RADIUS attribute by default, and QuickConnect device enrollments now correctly process the Session-Timeout attribute. For Android and Windows XP devices, the maximum validity period setting no longer overrides the session timeout value. This corrects an issue that could have resulted in guest accounts with short expiration times being permitted access to the network beyond their account's configured expiration time.
10229	QuickConnect now correctly processes passwords that contain the ampersand (&), backslash (\), or equal-to (=) characters.

Chapter 6

Known Issues Identified in Previous Releases

The following known issues for this release were identified in previous releases. Workarounds are included when possible. For a list of known issues identified in the 6.0.2 Patch 2 release, see the What's New in This Release chapter.

Policy Manager

Table 15 lists known issues in Policy Manager found in previous releases.

Table 15 *Known Issues in Policy Manager*

Bug ID	Description
	The subscription ID is not retained when you upgrade to CPPM 6.0.2. After you upgrade, you must re-enter the subscription ID at **Administration > Agents and Software Updates > Software Updates**. This is the same subscription ID that was used for 6.0.1, and is required in order to receive software updates.
	After a restore operation, the EAP-FAST master keys is generated and updated in 30 minutes on the restored machine. During this period, authentications using EAP-FAST mechanism might fail.
	Alert messages in the access tracker might be missing for some failed RADIUS authentication requests.
	OCSP URLs cannot be accessed through HTTP proxy from CPPM.
	Upgrading from previous versions to 6.0.1 will fail if ClearPass Policy Manager is already joined to the domain. **Workaround**: Perform a "leave domain" before starting an upgrade.
	If Profile is enabled, cleanup intervals for Known/Unknown/Disabled endpoints in the Cluster Wide Parameters must not be configured. This is known to cause issues with the cleanup process.
	Domain join operations will fail if the domain password contains special characters such as a space, quotation marks, or a "$" symbol.
11906	The Aruba dictionary becomes disabled by default after upgrading from Policy Manager 4.x to 6.0.1. **Workaround:** Customers who run into this issue must enable the Aruba dictionary manually from the **Administration > Dictionaries** page.
12422	After upgrading from 6.0.1 to 6.0.2, the Server License Summary table on the **Administration > Licensing** page may be blank. If you notice this behavior, simply execute the `system refresh-license` CLI command, and the table will repopulate with the correct information.

Guest

Table 16 lists known issues in Guest found in previous releases.

Table 16 *Known Issues in Guest*

Bug ID	Description
	Advertising Services is not available in this version of ClearPass Guest. It will be restored in a future release.
	User names are treated case-sensitively by ClearPass Policy Manager. **Workaround**: Be aware that authentication is always case-sensitive and enter your username accordingly.

Table 16 *Known Issues in Guest (Continued)*

Bug ID	Description
1877 (9572)	From the **Edit Accounts** page, if multiple accounts share the same phone number and all are selected, then SMS is received multiple times. **Workaround**: Avoid selecting multiple accounts that share identical phone numbers.
2272 (9967)	Unicode SMS messages 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.
10334	Filtering on the Guest Manager List Accounts page (guest_users) might not work when non-standard columns are displayed. You might see the message "Internal error: NwaClearPassApi does not support this query: Complex queries using _Build are not supported". **Workaround**: Use default columns, or disable searching on additional columns that are added to the view (customize the view, edit the column, and deselect the **Include values when performing a quick search** check box).
10442	The expire_postlogin field and expire_usage field are not supported in this version of Guest. **Workaround**: There is no workaround at this time.
10625	iOS and OS X 10.7+ devices do not report their MAC address during the Onboard process. As a result, these devices will always show as an "Unknown" endpoint.
10985	The Guest Manager List Accounts page (guest_users) cannot be sorted or searched by the Role Name or Status columns. **Workaround**: There is no workaround at this time.
11109	The do_expire field for ClearPass Guest is not supported in this release. ClearPass Guest accounts are always disabled when the expiration time is reached. There is no option to delete the account, or to logout the account. **Workaround**: Manually delete expired accounts, or wait for a scheduled database cleanup to delete the expired accounts.
11250	Editing a guest account for which there is an already active session will not generate a CoA-Request to update the properties of the active session, even if the Dynamic Authorization check box is selected on the Configuration > Authentication form.
11522	The expire_postlogin field cannot be used with ClearPass Policy Manager. This functionality will be available in a future release.
11523	The ability to generate session warning messages prior to the expiration of a guest's session was removed from the 6.0 release. This functionality will be restored in a future release.

Insight

Table 17 lists known issues for Insight found in previous releases.

Table 17 *Known Issues in Insight*

ID	Description
	The previous configuration for the Report Analytics selection is not retained when a report is edited. **Workaround:** Select the appropriate Analytics columns again before you click Save.
	Data tables are not populated in HTML & PDF reports if the CSV file size is > = 1MB. However, any associated analytics are produced in the corresponding HTML & PDF reports.
	Insight is not supported on Internet Explorer 8 (IE8).

Table 17 *Known Issues in Insight (Continued)*

ID	Description
	HTML reports do not show embedded images.
	Data tables are not populated in HTML or PDF reports when the CSV file size is > = 1MB. However, any associated analytics will be produced in the corresponding HTML and PDF reports.
11827	Insight is not supported in Internet Explorer 8 (IE8).

Onboard

Table 18 lists known issues for Onboard found in previous releases.

Table 18 *Known Issues in Onboard*

Bug ID	Description
2202 (9897)	ClearPass Onboard does not update the Policy Manager endpoints table with an endpoint record when provisioning an iOS 5 device. This is because the iOS 5 device does not report its MAC address to ClearPass Onboard during device provisioning.
10127	Auto-reconnect does not work for Mac OS X 10.7. This client will reconnect using the original credentials that were used to connect to the SSID (PEAP instead of TLS). This happens even if the "Remember this Network" option is NOT selected when connecting to the provisioning network.
10525	Wired clients fail to connect to an 802.1x port that is also being used for wireless provisioning.
10667	When using Onboard to provision a OS X system with a system profile, an administrator user must select the appropriate certificate when connecting to the provisioned network for the first time. The administrator should also ensure that the system's network settings are configured to automatically prefer connecting to the provisioned network, if the intent is for non-administrator users to always use that network. The process to provision an OS X system with a system profile is: ● The administrator should log in to the OS X system and connect to the provisioning SSID. Do not select "Remember this network." ● Use Onboard to provision the device with an EAP-TLS profile, ignoring the username/password prompt. ● Connect to the provisioned network, selecting EAP-TLS as the mode and selecting the provisioned certificate, but ignoring the username field. ● When the system connects and authorizes to the network, use Network Preferences to place the EAP-TLS network first in the priority list. ● After the administrator logs out, users logging in are connected by EAP-TLS and cannot modify those settings.
11334	Device provisioning fails with a "page not found" error if a user attempts to use Onboard on a subscriber node when the publisher is not reachable or offline. **Workaround**: Bring the publisher back online, or promote one of the subscribers in the cluster to become the new publisher.
11825	Users cannot specify which network settings to provision to devices, either from a device provisioning page or from Onboard's provisioning settings. **Workaround**: There is no workaround at this time.

OnGuard

Table 19 lists known issues for OnGuard found in previous releases.

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 19 *Known Issues in OnGuard*

ID	Description
	Peer-to-Peer check and Process check against the uTorrent application do not work in this version of OnGuard.
	OnGuard is known to have issues with Sophos 10.0.4 Anti-Virus installed on Windows XP SP3.
	OnGuard fails to collect health on Windows 8 OS if VMWare Server 2.0.2.X is installed.
	Upgrading ClearPass OnGuard from versions 3.5, 4.0, 5.0, 5.0.1, 5.1.1, and 5.2 to 6.0 will fail if the OnGuard installer is invoked without administrative privileges on the client. **Workaround**: Execute the `msciexec/I ClearPassOnGuardInstall.msi` command from the windows command prompt as the administrator user.
	Disabling USB storage devices on Windows 2008 server (64-bit) is not supported.
	Migration of Posture Policies from earlier versions of ClearPass Policy Manager to 5.1.x/5.2.0/6.0 is not supported. **Workaround**: Add/configure posture policies directly on the upgraded version of CPPM again.
	ClearPass OnGuard does not display remediation messages for Windows OS Service Pack checks. This is applicable only if OS-based checks are enabled through the “Windows System Health Validator” plugin.
	Live updates for Windows Defender is not supported on Windows 8, and users cannot browse the URL provided in the OnGuard remediation messages.
	Auto-Remediation fails if the OnGuard agent is installed by a domain user (non-administrator). Two workarounds are available: **Workaround 1**: Install OnGuard using administrator privileges from the command prompt. Command to execute: `msiexec /i ClearPassOnGuardInstall.msi` **Workaround 2**: Use the EXE version of the installer (ClearPassOnGuardInstall.exe) to install OnGuard.

Chapter 7

Introducing the Integrated Platform

The ClearPass 6.0 release integrated the ClearPass Guest and ClearPass Onboard applications as options with the ClearPass Policy Manager platform. A single login gives access to all ClearPass applications. If you are migrating from Amigopod to ClearPass 6.x, this chapter helps you know what to expect. It describes what's new, what's changed, and what's the same in your applications.

This chapter contains the following sections:

- "Integrated Platform Overview" on page 29
- "Using ClearPass Guest in the Integrated Platform" on page 30

Integrated Platform Overview

The ClearPass 6.0 release fully integrated the ClearPass Guest and ClearPass Onboard applications as options with the ClearPass Policy Manager platform. A single login gives access to all ClearPass applications.

What has Changed in Guest? What's the Same?

This section briefly summarizes the changes in ClearPass Guest. For detailed information about changes to each functionality area, see "Using ClearPass Guest in the Integrated Platform" on page 30 of this chapter.

- Because ClearPass Policy Manager (CPPM) centralizes and automates many access, policy, provisioning, and security management features, most of ClearPass Guest's system-level administrative features have moved to the underlying Policy Manager platform. The RADIUS and Reporting modules, as well as some sections within the Administration and other modules, no longer appear in ClearPass Guest because their features are now managed in CPPM.
- Application-level administrative and configuration features are still managed within the ClearPass Guest application.
- The features within the Guest Manager, Onboard, and Customization modules are mostly unchanged except for some additions.
- ClearPass Policy Manager's skin is used for all its applications, so ClearPass Guest has a new "look and feel," including a slightly different behavior for its left navigation links.
- There are some changes to login and navigation:
  - You can log in directly to ClearPass Guest or, if you will also be working in ClearPass Policy Manager, a single login provides access to all your applications from the CPPM dashboard.
  - The URL has changed slightly.
  - The order of ClearPass Guest's modules has changed slightly in the left navigation, but navigation within each module is much the same.
  - While navigating in ClearPass Guest, you will notice a couple of name changes: The Administrator module is now Administration, and the Customization module is now Configuration.

  See "Navigation" on page 34 for details of login and navigation changes.
- Advertising Services is not available in this version of ClearPass Guest. It will be restored in a future release.

Where Can I Find the Features I'm Used To?

Most of the features you use regularly are in their familiar locations in ClearPass Guest. See the module descriptions under "Using ClearPass Guest in the Integrated Platform" on page 30 for overviews of feature locations. If you log in through ClearPass Policy Manager, the first page that opens is CPPM's Dashboard. To access ClearPass Guest, look for the Quick Links pane on the Dashboard page and click the Guest link. See "Navigation" on page 34 for details of login and navigation changes.

To perform system-level administrative tasks that you used to do in ClearPass Guest's RADIUS or Reporting Manager modules or sections of the Administrator module, please refer to the ClearPass Policy Manager documentation.

Does My Licensing Status Change?

ClearPass Policy Manager's basic license includes a minimum user count for each of the Guest, Onboard, and OnGuard applications. Each of these applications also has a product-specific license. The user count for each product-specific license is in addition to the count provided by CPPM's basic license, so your ClearPass Guest user limit will now be slightly higher.

ClearPass Guest now follows CPPM's method of measuring and enforcing its user count. Prior to the 6.0 release, ClearPass Guest enforced the user count as the number of concurrent users at any time. In other words, with a license for 500 users, Guest would allow 500 concurrent users but would not authenticate another user until one of the 500 had dropped off.

ClearPass Policy Manager measures usage per day and monitors the average of the past seven days. With this method, occasional spikes that exceed the licensed user count tend to be balanced by times of low usage and produce a seven-day average below the licensed limit. At the end of a month, if the average for any seven days exceeded the licensed count, a notice is displayed to the administrator. If the average continues to be high, licensing needs can be reevaluated. Users will still be authenticated, and enforcement takes the form of limiting the tasks the administrator can perform in CPPM.

Can I Upgrade an Existing ClearPass Guest 3.9 to 6.x?

Upgrading from an existing ClearPass Guest 3.9.x is not available with this release. Support for migrating from 3.9.x will be added in a future release.

Using ClearPass Guest in the Integrated Platform

This section provides details of user interface and process changes, including documentation and navigation changes. Issue tracking IDs are included when available.

Administration

User Interface Changes

- The module's name was changed from Administrator to Administration.
- The Data Retention page was moved up to the first level in the Administration module's left navigation.
- The Support section used to be a top-level module in the left navigation; it is now part of the Administration module. System logs are no longer included in ClearPass Guest's support items because they are in ClearPass Policy Manager.
- The Operator Logins list view was removed from ClearPass Guest. It is replaced by the Configuration > Identity > Local Users screen in ClearPass Policy Manager.
- Subscription management, plugin additions, update checks, and OS updates are now handled in ClearPass Policy Manager. The Available Plugins List and plugin configuration are still in ClearPass Guest.

- Some AirGroup processes were added. The Administration module is used to configure the AirGroup plugin, create AirGroup administrators and operators and set operators' device limits, and to authenticate AirGroup operators via LDAP.
- The following functionality was removed from the Administration module and is now managed entirely in ClearPass Policy Manager:
  - Backup and Restore
  - High Availability
  - Network Setup
  - Notifications
  - SSL Certificate
  - OS Updates
  - Server Time
  - System Log

AirGroup Services

AirGroup is a new feature in the ClearPass platform. AirGroup allows users to register their personal mobile devices on the local network and define a group of friends or associates who are allowed to share them. The ClearPass Policy Manager base license includes AirGroup functionality.

AirGroup configuration is distributed across ClearPass Policy Manager and ClearPass Guest. You use ClearPass Guest to define AirGroup administrators and operators. AirGroup administrators can then use ClearPass Guest to register and manage an organization's shared devices and configure access according to username, role, or location. AirGroup operators (end users) can use ClearPass Guest to register their personal devices and define the group who can share them. AirGroup operators can also be authenticated via LDAP.

For complete AirGroup information, refer to:

- The "AirGroup Deployment Process" section in the ClearPass Guest Deployment Guide's "Overview" chapter
- The "AirGroup Services" section in the Deployment Guide's "Administration" chapter
- The "AirGroup Device Registration" section in the Deployment Guide's "Guest Manager" chapter
- The "Local Operator Authentication" section in the Deployment Guide's "Operator Logins" chapter
- The "AirGroup Deployment Guide" and the ClearPass Policy Manager documentation

Customization

User Interface Changes

- The module's name was changed from Customization to Configuration.
- The Authentication form was added.

Home Module

The Home module was removed from ClearPass Guest and all its functionality was moved to ClearPass Policy Manager. For complete information on these features, refer to the ClearPass Policy Manager documentation.

Operator Logins

User Interface Changes

The Operator Logins list and the Create Operator Logins form were removed from ClearPass Guest's Administration module. This functionality is now distributed across ClearPass Policy Manager and ClearPass Guest. See "Procedure Change: Creating a ClearPass Guest User" on page 32.

Procedure Change: Creating a ClearPass Guest User

The procedure for creating an operator has changed. Some steps are now performed in CPPM, and some are performed in ClearPass Guest, as described below. (#10047, #11127)

To create a new ClearPass Guest operator:

1. Create an operator profile in ClearPass Guest, or use an existing one. (To create AirGroup users, choose either the AirGroup Administrator or AirGroup Operator profile, as appropriate. These profiles are automatically included in ClearPass Guest when the AirGroup Services plugin is installed.) See the "Operator Profiles" section in the "Operator Logins" chapter of the "ClearPass Guest Deployment Guide".
2. Create a CPPM role for the operator: In ClearPass Policy Manager (CPPM), go to **Configuration > Identity > Roles** and create a role that matches the operator profile. Refer to the ClearPass Policy Manager documentation for information on creating the role.
3. Create a local user for the operator: In CPPM, go to **Configuration > Identity > Local Users**. Select the CPPM role defined for the user. Refer to the ClearPass Policy Manager documentation for information on creating the local user.
4. Create a translation rule to map the CPPM role name to the ClearPass Guest operator profile:
   a. In ClearPass Guest, go to **Administration > Operator Logins > Translation Rules**.
   b. In the **Translation Rules** list, choose the profile, then click its **Edit** link.
   c. Edit the fields appropriately to match the CPPM role name to the ClearPass Guest operator profile. See the LDAP Translation Rules section in the Operator Logins chapter of the ClearPass Guest Deployment Guide.
   d. Click **Save Changes**.

RADIUS Services

RADIUS Services functionality was moved to ClearPass Policy Manager. For complete information on functionality that is now in CPPM, refer to the ClearPass Policy Manager documentation.

Reporting Manager

Reporting functionality was moved to ClearPass Policy Manager, and includes the ClearPass Insight application. For complete information on functionality that is now in CPPM, refer to the ClearPass Policy Manager documentation.

SMTP Services

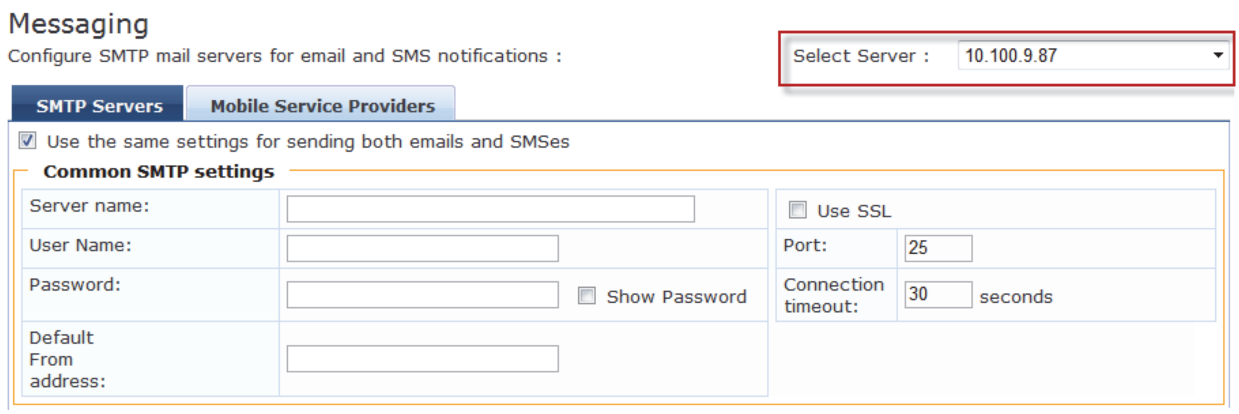
Procedure Change: Configuring SMTP Servers in CPPM

Before sending email receipts, you must now configure the SMTP server in ClearPass Policy Manager. (#10287)

To configure an SMTP server:

1. In **ClearPass Policy Manager**, go to **Administration > External Servers > Messaging Setup**. The Messaging form opens with the SMTP Servers tab displayed.

Figure 1 *The SMTP Servers Tab of CPPM's Messaging Setup Form*



Messaging

Configure SMTP mail servers for email and SMS notifications :

Select Server : 10.100.9.87

☑ Use the same settings for sending both emails and SMSes

Common SMTP settings

Server name:		☐ Use SSL	
User Name:		Port:	25
Password:	☐ Show Password	Connection timeout:	30 seconds
Default From address:			

2. In the **Select Server** drop-down list in the upper-right corner, select the server to configure for email receipts.
3. To configure the same settings for both SMTP and SMS email servers, mark the **Use the same settings** check box.
4. Complete the rest of the fields with the appropriate information. Include the username and password if your email, then click **Save**.

NOTE

If the SMTP server is not configured in CPPM, Guest emails will not be sent.

Documentation

Reflecting the distribution of functionality across the ClearPass Policy Manager platform, some chapters were removed, and some sections were moved to different places within the Deployment Guide. Changes resulting from integration with ClearPass Policy Manager are summarized below. For complete information on functionality that is now in CPPM, refer to the ClearPass Policy Manager documentation.

The following sections were moved to new locations in the Deployment Guide:

- The Content Manager section is now in the Configuration chapter. It used to be in the Administrator Tasks chapter.
- Managing Data Retention is now a top-level section in the Administration chapter. It used to be a subsection within the System Control section.

The following chapters and sections were removed from the Deployment Guide. These tasks are now managed through ClearPass Policy Manager:

- Setup Guide chapter
- High Availability Services chapter
- RADIUS Services chapter
- Report Management chapter
- Administrator Tasks chapter, sections removed:
  - Network Setup section
  - SSL Certificate section
  - Backup and Restore section
  - Notifications section
  - OS Updates section

  - Parts of Plugin Manager section
  - Server Time section
  - System Log section
- Operator Logins chapter, section removed:
  - LDAP Operator Authentication section
- Onboard chapter, section removed:
  - Configuring ClearPass Servers for Device Provisioning section
- Reference chapter, sections removed:
  - Standard RADIUS Request Functions section
  - RADIUS Server Options section
  - List of Standard RADIUS Attributes section

Navigation

There are now two ways you can log in to ClearPass Guest. You can log in to the Guest application by itself, or, to work in ClearPass Guest and ClearPass Policy Manager concurrently, you can use a single login to access all your ClearPass applications from the CPPM dashboard. The URLs for each login and changes to navigation are described below.

Logging in Directly to ClearPass Guest

To log in directly to ClearPass Guest:

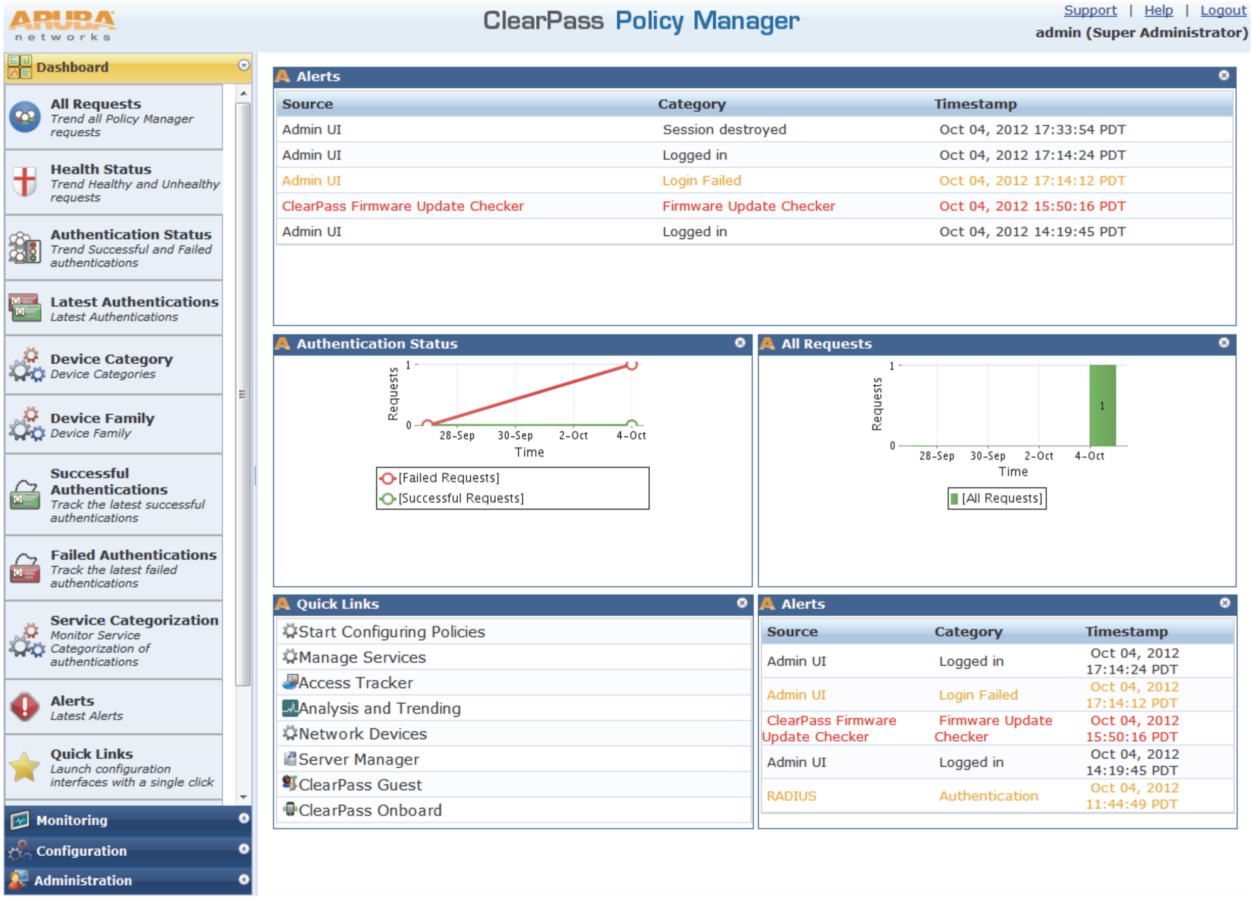
1. Using the hostname or IP address for your installation, point your browser to **https://<hostname or IP address>/guest**. The ClearPass Guest login page opens.
2. Enter your username and password and click **Log in**. The ClearPass Guest application opens with the Start page of the Guest Manager module displayed.
3. These login credentials are defined in ClearPass Policy Manager at **Configuration > Identity > Local Users**.

Accessing ClearPass Guest Through CPPM

To use a single login to log in to ClearPass Policy Manager and navigate to ClearPass Guest and your other ClearPass applications:

1. Using the hostname or IP address for your installation, point your browser to **https://<hostname or IP address>/tips**. The ClearPass Policy Manager login page opens.
2. Enter your username and password and click **Log In**. ClearPass Policy Manager opens with the Dashboard page displayed. The panes on this page display a variety of system information.

Figure 2 *The Dashboard Page and CPPM Left Navigation*

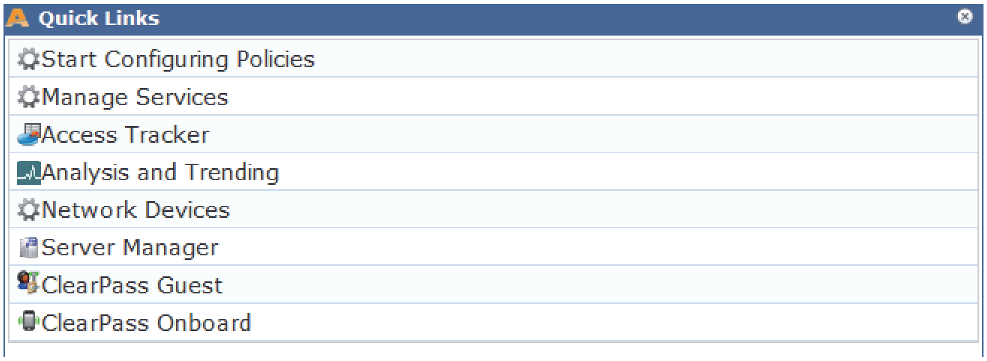

ARUBA networks
ClearPass Policy Manager
Support | Help | Logout
admin (Super Administrator)
Dashboard
All Requests
Trend all Policy Manager requests
Health Status
Trend Healthy and Unhealthy requests
Authentication Status
Trend Successful and Failed authentications
Latest Authentications
Latest Authentications
Device Category
Device Categories
Device Family
Device Family
Successful Authentications
Track the latest successful authentications
Failed Authentications
Track the latest failed authentications
Service Categorization
Monitor Service Categorization of authentications
Alerts
Latest Alerts
Quick Links
Launch configuration interfaces with a single click
Monitoring
Configuration
Administration
Alerts

Source	Category	Timestamp
Admin UI	Session destroyed	Oct 04, 2012 17:33:54 PDT
Admin UI	Logged in	Oct 04, 2012 17:14:24 PDT
Admin UI	Login Failed	Oct 04, 2012 17:14:12 PDT
ClearPass Firmware Update Checker	Firmware Update Checker	Oct 04, 2012 15:50:16 PDT
Admin UI	Logged in	Oct 04, 2012 14:19:45 PDT

Source	Category	Timestamp
Admin UI	Logged in	Oct 04, 2012 17:14:24 PDT
Admin UI	Login Failed	Oct 04, 2012 17:14:12 PDT
ClearPass Firmware Update Checker	Firmware Update Checker	Oct 04, 2012 15:50:16 PDT
Admin UI	Logged in	Oct 04, 2012 14:19:45 PDT
RADIUS	Authentication	Oct 04, 2012 11:44:49 PDT

3. Look for the **Quick Links** pane in the lower left of the Dashboard. This pane contains top-level navigation links to some areas of CPPM, as well as links to ClearPass Guest and Onboard. Click the **ClearPass Guest** link.

Figure 3 *The Quick Links Pane*



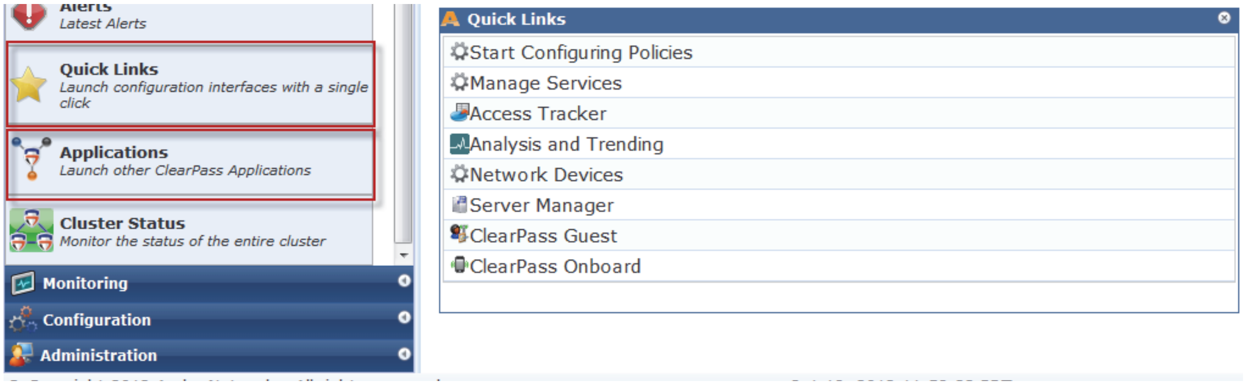
The ClearPass Guest application opens in a new browser tab, with the Guest Manager module displayed. ClearPass Policy Manager stays open in the first tab so you can work in both ClearPass Guest and ClearPass Policy Manager concurrently.

Using CPPM's Dashboard Page

When you first log in to ClearPass Policy Manager, the Dashboard page is displayed by default. The Dashboard link in the left navigation is expanded to show options, and CPPM's other left-navigation links are below.

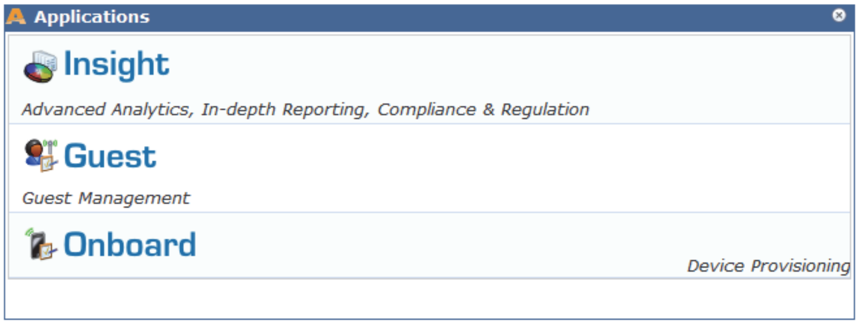
The Dashboard is an interactive page: Its left-navigation options are not clickable links; instead, they are drag-and-drop items you can display in any pane on the Dashboard. When you drag an option to a pane, it replaces the option that was there. To restore an option you replaced, simply drag it from the left navigation again.

Figure 4 *Drag-and-Drop Items Highlighted in CPPM's Left Navigation*



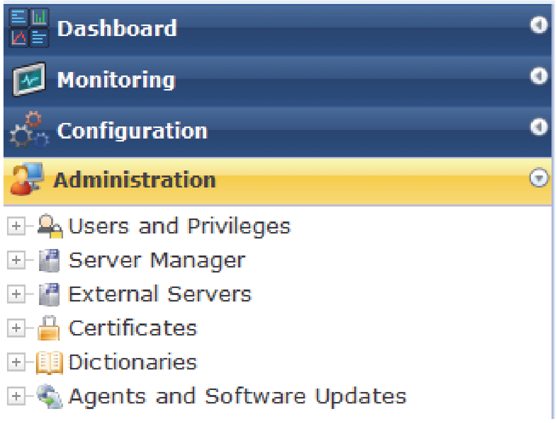
For example, the Quick Links pane has a corresponding option in the left navigation. Just below it in the left navigation is an Applications option. If you drag the **Applications** option over the Quick Links pane, a list of links to your licensed applications replaces the list of platform links, and the name of the pane changes. You can use either the **Applications** list or the **Quick Links** list to access your ClearPass applications.

Figure 5 *The Applications Pane*



ClearPass Policy Manager's other top-level left-navigation links are Monitoring, Configuration, and Administration. The Configuration and Administration modules in CPPM are for system-level changes that apply to the ClearPass platform as a whole. The Configuration and Administration modules within ClearPass Guest are for application-level changes, and affect only the Guest application.

Figure 6 *ClearPass Policy Manager's Left Navigation*


Dashboard
Monitoring
Configuration
Administration
Users and Privileges
Server Manager
External Servers
Certificates
Dictionaries
Agents and Software Updates