

ClearPass Guest 3.9

(Amigopod 3.9)



Release Notes

Copyright

© 2012 Aruba Networks, Inc. Aruba Networks trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

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. 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.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Chapter 1	Release Overview	5
	Supported Browsers.....	5
	Virtual Appliance.....	5
	System Requirements	6
	VMware Requirements	6
	VMware Player / VMware Workstation.....	6
	Configuring VMware Player	7
	Timekeeping in Virtual Machines	7
	Evaluation License.....	7
	Contacting Support	7
Chapter 2	What's New in This Release	9
	Introducing ClearPass Guest and ClearPass Onboard	9
	Administrative.....	9
	Default Login Access Setting Now HTTPS	9
	Multiple Syslog Collectors Supported	9
	Packet Capture Size Increased.....	9
	Plugins Renamed	10
	Customization.....	10
	Multi-File Content Upload	10
	Configurable Page Elements.....	11
	Default Guest Receipt Enhanced	11
	Documentation	11
	General	11
	Configuration Changes Logged	11
	Amigopod Name Changes.....	11
	Integration with Other ClearPass Servers Configurable	12
	Guest Management	13
	Single Password for Multiple Accounts Supported	13
	Sponsor Confirmation for Role Selection	15
	MAC Authentication.....	16
	Caching During User Authentication.....	16
	Mobile Device Provisioning Services.....	17
	Mobile Device Provisioning Services (MDPS) is now ClearPass Onboard ...	17
	Device Enrollment Support	18
	Operating Systems Support.....	18
	Android Support.....	18
	Obtaining Device Serial Number	18
	Security Types Applicable for All Devices.....	18
	Windows Device Support.....	18
	User/Password Authentication for iOS and OS X.....	18
	RADIUS Services	18
	MAC Auto-Registration in ClearPass Policy Manager	18
	SMS Services	19
	Support for Conversion to 16-Bit Hex Encoding	19
	POST Method Supported	19

	SMTP Services	20
	Email Format Cleanup Supported.....	20
Chapter 3	Fixed Issues	21
	Administrator	21
	DNS Server Configuration	21
	Network Settings Issue on Chrome Browser	21
	Packet Capture	21
	Customization.....	21
	Custom Field Creation	21
	General	22
	Login Page	22
	SMS and Email	22
	Guest Manager	22
	Editing Guest Account Username	22
	Large-Import Failure	22
	High Availability Services.....	22
	Domain Join and Leave Operations	22
	RADIUS Disconnect Requests	23
	Kernel.....	23
	“No favicon” Log Messages	23
	“Undefined Index” PHP Message	23
	Mobile Device Provisioning Services.....	23
	Changing From Intermediate to Root CA Mode	23
	Mac OS X Lion Provisioning	23
	iOS 5 Devices Were Not Detected as Unique	23
	Operating System.....	24
	Kernel Package Security Updates	24
	libpng Package Security Updates	24
	RPM Package Security Updates	24
	OpenSSL Package Security Updates	24
	RADIUS Services.....	25
	Active Sessions Username Display and Disconnect Issues	25
	EAP Server Certificate Import Failure	25
	Login Page Support for Motorola Controllers	25
	Parsing Value Error	25
	Scrolling Behavior on Apple Devices	25
	Skins	25
	HTML Error on iPhone During Device Provisioning	25
Chapter 4	Known Issues.....	27
	General	27
	Mobile Device Provisioning Services.....	27
	SMS Services	27
Chapter 5	Upgrade Procedure	29
	Important Points to Remember	29
	Before you Upgrade	29
	Setting System Memory	29
	Configuration Backup	30
	Snapshot of the Virtual Machine	31
	Upgrading Amigopod Software.....	32

ClearPass Guest release 3.9 is a major software release that introduces new features and fixes to previous outstanding issues. This release note contains the following chapters:

- [Chapter 2, “What’s New in This Release” on page 9](#)—Describes the new features introduced in this release
- [Chapter 3, “Fixed Issues” on page 21](#)—Lists the issues fixed in this release
- [Chapter 4, “Known Issues” on page 27](#)—Lists the known issues in this release
- [Chapter 5, “Upgrade Procedure” on page 29](#)—Provides new upgrade instructions



It is important that you read the procedures in the Upgrade chapter to ensure a successful upgrade.

Supported Browsers

ClearPass Guest best practices recommend updating your browser to the latest version available for the best user experience. Supported browsers for ClearPass Guest are:

- Microsoft Internet Explorer 7.0 and later on Windows XP, Windows Vista, and Windows 7
- Mozilla Firefox 3.x and later 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



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

Virtual Appliance

The ClearPass Guest visitor management software is delivered as a pre-installed virtual appliance. For additional information refer to the sections [“System Requirements” on page 6](#) and [“VMware Requirements” on page 6](#). The files for this release are:

2012-04-30-ClearPassGuest-VirtualAppliance-3.9.0-x86_64.zip:

- Use this image with VMware ESXi version 4.0+, or VMware ESXi version 5.0+.
- This virtual machine image is built using a 64-bit architecture.

2012-04-30-ClearPassGuest-ESX3Appliance-3.9.0-x86_64.zip

- Use this image with VMware ESX Server 3.5.
- This virtual machine image is built using a 64-bit architecture.

2012-04-30-ClearPassGuest-VmwarePlayer-3.9.0-i386.zip

- Use this image with VMware Workstation, VMware Player 3.0+ or VMware Server 2.0.
- This virtual machine image is built using a 32-bit architecture. Use of virtualization software allows this image to run on either a 32-bit or 64-bit platform.

System Requirements

When deploying a ClearPass Guest virtual machine, the following minimum system resources are required:

Table 1 *Virtual Machine Requirements*

Resource	Minimum Recommended Configuration
CPU	1 virtual CPU
Memory	1024 MB
Storage	8 GB virtual disk
Network Adapters	2 virtual NICs



This configuration is the minimum recommended and is suitable only for very small-scale deployments or to support basic evaluation and testing. For production networks or larger-scale testing, you will need to increase the resources allocated to the virtual machine according to the load you expect to support. Refer to the ClearPass Guest Sizing Guide for detailed information about sizing the ClearPass Guest virtual machine for your deployment.

VMware Requirements

The recommended virtualization products compatible with this release are:

- VMware ESXi 5.0 Server
- VMware ESX Server 4i, version 4.1.0+
- VMware Workstation (all versions)
- VMware Player 3.0+
- VMware Server 2.0+

The ClearPass Guest virtual appliance is shipped with a single virtual network adapter configured to obtain an IP address using DHCP.

When importing the virtual appliance, ensure that you connect the virtual machine's network adapter to a physical network that has an available DHCP server. The current IP address of the appliance is shown on the appliance console at the login prompt.

For more information on VMware products, including free downloads, go to: <http://www.vmware.com/>

VMware Player / VMware Workstation

The ClearPass Guest virtual appliance is shipped with two virtual network adapters; both are configured to obtain an IP address using DHCP.

The virtual appliance's first Ethernet adapter is connected to the VMware NAT virtual adapter; this enables the virtual machine to reach the Internet using the host's IP address.

The virtual appliance's second Ethernet adapter is connected to the VMware Bridged adapter; this enables external access to the virtual machine using the physical network connected to the bridged adapter. The current IP address of the appliance is shown on the appliance console at the login prompt.

Configuring VMware Player

If you are using VMware Player and your host machine has more than one Ethernet adapter installed, you might encounter difficulties obtaining a DHCP network address if the Ethernet adapter selected for automatic bridging is not the correct adapter.

Although VMware Player does not have a menu option to configure virtual networks, the network configuration can be viewed and modified using the Virtual Network Configuration application. This program is called **vmnetcfg.exe** and can be found in the VMware Player program files directory. If the default installation path was selected, this program is:

C:\Program Files\VMware\VMware Player\vmnetcfg.exe

Timekeeping in Virtual Machines

If running an AMD dual-core (X2) processor, the AMD Dual-Core Optimizer must be installed on the host to avoid timekeeping problems in the virtual appliance. The download address is:

http://www.amd.com/us-en/Processors/TechnicalResources/0_30_182_871_9706,00.html

Other hosts with dual-core or SMP systems may also experience timekeeping problems unless the virtual machine's processor affinity is set to a specific CPU. For more details on timekeeping best practices in VMware virtual machines, refer to <http://kb.vmware.com/kb/1006427>.



Running NTP within the ClearPass Guest virtual machine is NOT recommended, as this may conflict with VMware's internal clock synchronization. Instead, run NTP or another time synchronization client on the host, and use VMware's clock synchronization (enabled by default) to keep the virtual machine's time accurate.

Evaluation License

The evaluation license, which ships with the ClearPass Guest appliance, permits the creation of guest accounts with a maximum lifetime of 15 minutes. After 15 minutes, the guest account expires and is deleted.

Contact your ClearPass Guest reseller to purchase a subscription ID that allows for unlimited guest account lifetimes, or to obtain a time-limited evaluation license that provides complete functionality for a defined period.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.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
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com

EMEA

emea_support@arubanetworks.com

WSIRT Email

Email details of any security problem found
in any Aruba product.

wsirt@arubanetworks.com

This chapter provides a brief summary of the new features in this release.

Introducing ClearPass Guest and ClearPass Onboard

With the 3.9 release, we are proud to introduce the integration of Amigopod with Aruba Networks' QuickConnect and the ClearPass Policy Manager platform.

As part of the changes, the Amigopod Visitor Management Solution has been renamed, and is now called ClearPass Guest. Mobile Device Provisioning Services (MDPS) also has a new name, and is now called ClearPass Onboard. These names are updated throughout the application, documentation, and various programmatic elements. For more information on name changes associated with the ClearPass Guest rebranding, see [“Plugins Renamed” on page 10](#), [“Amigopod Name Changes” on page 11](#), and [“Mobile Device Provisioning Services \(MDPS\) is now ClearPass Onboard” on page 17](#).

In addition to numerous other features and fixed issues, this release has focused on the following major enhancements:

- Integration of QuickConnect Enterprise with Amigopod's Mobile Device Provisioning Services (MDPS)—For more information, see the [Mobile Device Provisioning Services](#) section on page 17.
- MAC Authentication user interface enhancements—For more information, see [“Caching During User Authentication” on page 16](#) and [“MAC Auto-Registration in ClearPass Policy Manager” on page 18](#).
- Additional integration with ClearPass Policy Manager—For more information, see [“Integration with Other ClearPass Servers Configurable” on page 12](#) and [“MAC Auto-Registration in ClearPass Policy Manager” on page 18](#).
- New Guest Print Receipt (GuestManager Receipt)—For more information, see [“Default Guest Receipt Enhanced” on page 11](#).

Administrative

Default Login Access Setting Now HTTPS

The default login access settings now require HTTPS for both operators and guests. This change only affects new installations. (2260)

Security Recommendation: For existing installations, we strongly recommend you enable HTTPS for operators and guests. To do so, go to **Administrator > Network Setup > Login Access** and mark the check boxes in the **Security** rows for operators and for guests.

Multiple Syslog Collectors Supported

System log messages can now be sent to multiple syslog collectors. In the Syslog Server row of the System Log Configuration page, you may enter multiple syslog collectors as a comma-separated list of hostnames or IP addresses. To navigate to this form, go to **Administrator > System Control > System Log**. (2109)

Packet Capture Size Increased

In the packet capture tool, the maximum size of a packet capture was increased to 100,000 packets. (2095)

Plugins Renamed

As part of the ClearPass platform rollout, several plugins have been renamed, as shown in [Table 3](#). To view the list of available plugins, go to **Administrator > Plugin Manager > Manage Plugins**. (2049)

Table 3 *Plugins Renamed in ClearPass Guest Rollout*

Original Plugin Name	New Plugin Name
Aruba Amigopod Skin	Aruba ClearPass Skin
amigopod Administrator	Administrator
amigopod Deployment Guide	Deployment Guide
amigopod Kernel	Kernel
amigopod Operator Logins	Local Operator Logins
amigopod LDAP Operator Logins	LDAP Operator Logins
amigopod RADIUS Operator Logins	RADIUS Operator Logins
amigopod Hotspot Manager	Hotspot Manager
amigopod OS	Operating System
amigopod RADIUS Services	RADIUS Services
amigopod Support Services	Support Services
amigopod Translation Assistant	Translation Assistant
GuestManager Plugin	Guest Manager
LDAP Sponsor Lookup Plugin	LDAP Sponsor Lookup
MAC Authentication Plugin	MAC Authentication
Mobile Device Provisioning Services	ClearPass Onboard
SMS Services Plugin	SMS Services

Customization

Multi-File Content Upload

You can now upload multiple content asset files and folders, or a Web deployment archive. (501)

To upload multiple assets, first compress the files as a “tarball” or zip file, then upload it on the Content Manager’s Upload New Content form. Allowed file formats are .tgz, .tar.gz, .tb2, .tar.bz2, or .zip. After you have uploaded the file, the Extract option lets you create the new directory, navigate into it, and view and extract the files. Directory structure is preserved when extracting.

Configurable Page Elements

From the Customize Forms and Views page, you can now customize the page title, header HTML, and footer HTML for many of the application's forms and views, including the Create Guest Account form, Edit Guest Accounts view, and others. These options are in the new Page Properties area at the bottom of the Edit Properties form. (2307)

Page Properties

Page Title:	<input type="text"/>
	The title to display on the page. Leave blank to use the default title.
Header HTML:	<input type="text"/>
	HTML template code displayed before the form or view. Leave blank to use the default text, or enter a hyphen "-" to remove the default text.
Footer HTML:	<input type="text"/>
	HTML template code displayed after the form or view. Leave blank to use the default text, or enter a hyphen "-" to remove the default text.

 Save Changes

Default Guest Receipt Enhanced

The default Guest Manager Receipt print template has a new, improved format and is designed for optimum display and compatibility in more email clients. Unless you use a customized receipt template, you will receive the updated version. (2333)

To see this feature, go to **Customization > Print Templates**. Click the **GuestManager Receipt** row, then click the **Preview** link.

Documentation

The Deployment Guide content in the application's online help has been updated to version 3.7. (2096)

General

Configuration Changes Logged

A log message is now written to the Application Log for all configuration changes made in the ClearPass Guest and ClearPass Onboard user interfaces. (877)

Amigopod Name Changes

All occurrences of the Amigopod name have been changed throughout the application. (2043, 2241)

In addition to the updating the name to ClearPass Guest in all application screens, documentation, subscription IDs, and translations, the following items are also updated:

- **Default hostname**—The default hostname for the application is now **clearpass-guest.localdomain** instead of **amigopod.localdomain**. This only affects new deployments.
- **Default initial password**—The default password used to log in for the first time is now **admin** instead of **amigopod**.

- **Command line interface (CLI) default reset password**—When using the CLI option “Reset web password for admin to default”, the password is now reset to **admin** instead of amigopod.
- **Application plugins**—Many plugin names are updated. These are described in [Plugins Renamed](#) in this chapter.

Integration with Other ClearPass Servers Configurable

Support was added for controlling integration with ClearPass Policy Manager and ClearPass Profiler, letting you send information about account registration or device provisioning. (2238)

To use these options:

1. Go to **Administrator > Network Setup** and choose the new **ClearPass** option.



The ClearPass Servers form opens.

Manage ClearPass Servers	
ClearPass Policy Manager These options control ClearPass Policy Manager integration.	
Enable Policy Manager:	<input type="checkbox"/> Send device information to ClearPass Policy Manager Notify a ClearPass Policy Manager server when a device is enrolled or a certificate revoked.
ClearPass Profiler These options control ClearPass Profiler integration.	
Enable Profiling:	<input type="checkbox"/> Send device information to ClearPass Profiler Notify a ClearPass Profiler server when devices connect to ClearPass Guest.
<input type="button" value="Save Changes"/>	

2. To configure integration with ClearPass Policy Manager, mark the **Enable Policy Manager** check box. The form expands to include options for specifying the Policy Manager hostname, username, and password.

Manage ClearPass Servers	
ClearPass Policy Manager These options control ClearPass Policy Manager integration.	
Enable Policy Manager:	<input checked="" type="checkbox"/> Send device information to ClearPass Policy Manager Notify a ClearPass Policy Manager server when a device is enrolled or a certificate revoked.
* Host:	<input type="text"/> The hostname or IP address of the Policy Manager publisher node.
* Username:	<input type="text"/> The username used to log into the Policy Manager server.
* Password:	<input type="text"/> The password used to log into the Policy Manager server.

3. To configure integration with ClearPass Profiler, mark the **Enable Profiling** check box. The form expands to include options for sending device error, event, and profile interval information, as well as the hostname, username, and password for the primary and secondary Profiler servers.

ClearPass Profiler

These options control ClearPass Profiler integration.

Enable Profiling:	<input checked="" type="checkbox"/> Send device information to ClearPass Profiler Notify a ClearPass Profiler server when devices connect to ClearPass Guest.
Profiler Errors:	<input type="checkbox"/> Report Profiler errors to the client Treat failure to contact the Profiler server as an error.
Profiling Events:	<input type="checkbox"/> When client submits a web login form <input type="checkbox"/> When client requests a guest-facing page <input type="checkbox"/> When client registers a guest account <input type="checkbox"/> When client provisions a device The events on which to send device information to the Profiler server.
* Profiling Interval:	60 minutes Interval between sending duplicate updates to the Profiler server. Set to 0 to send all updates.

Primary Profiler Server

* Host:	<input type="text"/> The hostname or IP address of the primary Profiler publisher node.
* Username:	<input type="text"/> The username used to log into the primary Profiler server.
* Password:	<input type="text"/> The password used to log into the primary Profiler server.

Secondary Profiler Server

Host:	<input type="text"/> The hostname or IP address of the secondary Profiler publisher node.
* Username:	<input type="text"/> The username used to log into the secondary Profiler server.
* Password:	<input type="text"/> The password used to log into the secondary Profiler server.

Guest Management

Single Password for Multiple Accounts Supported

Support was added for the password field on the Create Multiple Guest Accounts form (`create_multi`). After you customize this form to include the password field, you can create multiple accounts that have the same password. (2291)

To use this feature:

1. Go to **Customization > Forms & Views**, click the `create_multi` row, then click its **Edit Fields** link. The Customize Form Fields view opens, showing a list of form fields and their descriptions.
At this point, the Password field is not listed because the `create_multi` form has not yet been customized to include it. You will create it for the form in the next step.
2. Click on any field in the list to expand a row, then click the **Insert After** link. The Customize Form Field form opens.
3. In the **Field Name** row, choose **password** from the drop-down list, and mark the **Enable this field** check box in the **Field** row. You may also enter a number in the **Rank** field to sort the password field on the form.

- In the **User Interface** row, choose **Password text field** from the drop-down list. The **Field Required** check box should now be automatically marked, and the **Validator** field should be set to **IsNotEmpty**.
- Click **Save Changes**. On the Customize Form Fields view, the password field is now included and can be edited.
- Go to **Guests > Create Multiple**. The Create Accounts form opens, and includes the Visitor Password field.

Create Guest Accounts

* Number of Accounts:	<input style="width: 80%;" type="text" value="3"/> <small>Number of visitor accounts to create.</small>
* Visitor Password:	<input style="width: 80%;" type="password" value="●●●●●●"/> <small>Select the length of generated visitor account usernames.</small>
Account Activation:	<input style="width: 80%;" type="text" value="Now"/> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	<input style="width: 80%;" type="text" value="1 day from now"/> <small>Select an option for changing the expiration time of this account.</small>
* Expire Action:	<input style="width: 80%;" type="text" value="Delete and logout at specified time"/> <small>Select an option for controlling the expiration of this account. Note that a logout can on</small>
Account Lifetime:	<input style="width: 80%;" type="text" value="N/A"/> <small>The amount of time after the first login before the visitor account will expire and be del</small>
* Account Role:	<input style="width: 80%;" type="text" value="Contractor"/> <small>Role to assign to this visitor account.</small>

- In the **Number of Accounts** field, enter the number of accounts you wish to create. In the **Visitor Password** field, enter the password that is to be used by all the accounts. Complete the other fields, then click **Create Accounts**. The Finished Creating Guest Accounts view opens. The password and other account details are displayed for each account.

Account Details	
	Username 42754093
	Password ouhIU99j9
	Role Contractor
	Account Expiration Saturday, 28 April 2012, 05:40 PM
Account Details	
	Username 52004616
	Password ouhIU99j9
	Role Contractor
	Account Expiration Saturday, 28 April 2012, 05:40 PM
Account Details	
	Username 19630172
	Password ouhIU99j9
	Role Contractor
	Account Expiration Saturday, 28 April 2012, 05:40 PM

Sponsor Confirmation for Role Selection

The sponsored self-registration workflow now allows the sponsor to choose the role for the user account at the time the sponsor approves the self-registered account. (2151)

To use this feature:

1. Go to **Customization > Guest Self-Registration**, click the **Guest Self-Registration** row, then click its **Edit** link. The Customize Guest Registration diagram opens, providing links to the various forms available for the configuration process.
2. In the **Receipt Page** area of the diagram, click the **Actions** link.



The Receipt Actions form opens.

3. In the **Enabled** row of the **Sponsorship Confirmation** area, mark the check box for **Require sponsor confirmation prior to enabling the account**. The form expands to let you configure this option.

Sponsorship Confirmation	
Enabled:	<input checked="" type="checkbox"/> Require sponsor confirmation prior to enabling the account
Authentication:	<input checked="" type="checkbox"/> Require sponsors to provide credentials prior to sponsoring the guest <small>If checked, the sponsor will need to successfully authenticate prior to sponsoring the user. The sponsor's operator profile must have the Guest Manager > Remove Accounts privilege.</small>
* Email Field:	(Use Default: sponsor_email) <input type="text"/> <small>The field containing the sponsor's email address.</small>
* Email Confirmation:	Sponsorship Confirmation <input type="text"/> <small>The plain text or HTML print template to send to the sponsor.</small>
* Email Skin:	(Use Default: No skin – HTML only) <input type="text"/> <small>The format in which to send email receipts.</small>
* Send Copies:	Do not send copies <input type="text"/> <small>Specify when to send visitor account receipts to the recipients in the Copies To list.</small>
UI Overrides:	<input type="checkbox"/> Display fields to override UI text and labels
Role Override:	(Prompt) <input type="text"/> <small>Change the guest's role upon a successful confirmation from the sponsor.</small>
Extend Expiration:	<input type="text"/> <small>Extend the account's expiration time. Leave blank to use the original expiration time. For example: +12h, +30d, or +1y.</small>
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>	

4. In the **Authentication** row, mark the check box for **Require sponsors to provide credentials prior to sponsoring the guest**.

- In the **Role Override** row, choose (**Prompt**) from the drop-down list.
- Complete the rest of the form, then click **Save Changes**. You are returned to the Customize Guest Registration diagram. Click the **Launch this guest registration page** link at the upper left to preview.



The Guest Registration login page is displayed as the guest would see it.

When a guest completes the form and clicks the **Register** button, the sponsor receives an email notification.

- To confirm the guest's access, the sponsor clicks the **click here** link in the email, and is redirected to the Guest Registration Confirmation form.

- In the **Account Role** drop-down list, the sponsor chooses the role for the guest, then clicks the **Confirm** button.

MAC Authentication

Caching During User Authentication

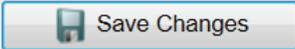
The RADIUS Role Editor includes new options to control MAC caching during user authentication without the need to write complex expressions within the role. (2170)

To use these options:

- Go to **RADIUS > User Roles** and click the **Edit** link for the role. The RADIUS Role Editor form opens, and includes the new MAC Cache area at the bottom of the form.

MAC Cache
 Enable guests to have their device cached for subsequent connections.
 Requires a NAS capable of MAC authentication and captive portal fallback.

Enabled: Enable MAC caching



- To configure MAC device caching, mark the **Enabled** check box. The form expands to include options for the role override, expiration, and device limit settings.

MAC Cache
 Enable guests to have their device cached for subsequent connections.
 Requires a NAS capable of MAC authentication and captive portal fallback.

Enabled: Enable MAC caching

Role: (No override)
 Override: Apply a separate role to the MAC device.

Expiration: 24h
 Enter how long the MAC accounts shall remain valid.
 For example: 12h, 24h, 30d.

Device Limit: Limit the number of devices a single guest can cache

* Limit: 1
 Enter the maximum number of accounts to create.

* Limit Action: Reject authentications once the limit is reached
 Allow authentications but no longer cache the device
 Enter the maximum number of accounts to create.



Mobile Device Provisioning Services

Mobile Device Provisioning Services (MDPS) is now ClearPass Onboard

Mobile Device Provisioning Services has merged with QuickConnect and is now called ClearPass Onboard. It also supports configuration and provisioning for all BYOD and IT-managed devices, including Windows, Android, OS X 10.5+, and wired clients. (2176, 2177, 2183, 2203, 2204)

This component of the application has moved to the top level of the navigation: From the Home page, click the **ClearPass Onboard** link, or look for the **Onboard** link in the left navigation.

- Customization
- Onboard
- RADIUS
- Reporting
- Support
- Logout



ClearPass Onboard
 Manage provisioning for "bring your own device" networks.

- Create, view and revoke certificates
- Configure the certificate authority
- Configure provisioning settings
- Configure the network profile

For more information, please refer to the ClearPass Onboard documentation on the Aruba Support Center.

Device Enrollment Support

Additional device enrollment support was implemented for the QuickConnect Enterprise product. (2004)

Operating Systems Support

As part of the merge with QuickConnect and support for all device types in ClearPass Onboard, the MDPS Wi-Fi settings Proxy Username and Proxy Password are no longer necessary and have been removed. Any field or section of a form that is applicable to only a subset of devices is clearly identified in the application. (2209)

Android Support

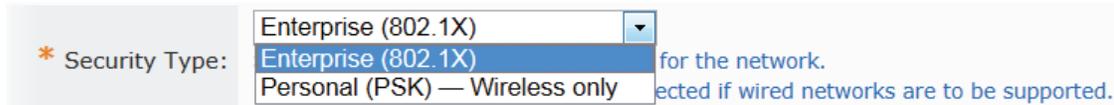
ClearPass Onboard now supports Android devices. (2203)

Obtaining Device Serial Number

Support was added for obtaining and storing a device's serial number during ClearPass Onboard device provisioning. (1965)

Security Types Applicable for All Devices

The list of security types available on the Network Settings page is updated to include only options that are applicable to all devices. Deprecated options are removed, and the Security Type field includes only the Personal and Enterprise options. Enterprise (802.1X) is selected by default if wired networks are to be supported. A new Security Version field lets you set the encryption version for the wireless network to WPA or WPA2. (2266)



Windows Device Support

ClearPass Onboard now supports Windows devices. Support is included for the Windows XP, Windows Vista, and Windows 7 (and later) clients. (2177)

User/Password Authentication for iOS and OS X

Support was added for unique device credential provisioning for iOS and OS X devices. (2233)

RADIUS Services

MAC Auto-Registration in ClearPass Policy Manager

Support was added for automatically registering guest MAC addresses as endpoint records in ClearPass Policy Manager when using a Web login page or a guest self-registration workflow. This option is available in Customization on the Web Logins and Guest Self-Registration pages if a valid Local or RADIUS pre-authentication check was performed. (2215)

Post-Authentication
Actions to perform after a successful pre-authentication.

Policy Manager:	<input checked="" type="checkbox"/> Register the guest's MAC address with ClearPass Policy Manager If selected and a ClearPass Policy Manager has been enabled, the username will be linked to the MAC.
Advanced:	<input checked="" type="checkbox"/> Advanced ClearPass Policy Manager options
Endpoint Attributes:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>List of name value pairs to pass along. user_field Endpoint Attribute.</p>

SMS Services

Support for Conversion to 16-Bit Hex Encoding

Unicode support for custom SMS handlers was added. You can now specify that the message format should be converted to hex-encoded UTF-16. (2272)

To use the Message Format option, go to **Administrator > SMS Services > SMS Gateways**.

Confirm Password:	<input type="text"/> Your authorization password for the SMS service provider.
Message Format:	<input checked="" type="checkbox"/> Convert text to hex-encoded UTF-16 If selected, the message will be converted to hex-encoded UTF-16. Refer to your handlers documentation if this is necessary.

Mobile Number Settings

POST Method Supported

Support was added for specifying the HTTP method to use—either GET or POST—when creating a custom SMS handler. (2163)

To use this feature:

1. Go to **Administrator > SMS Services > Manage SMS Gateways**, then click the **Create new SMS Gateway** link at the bottom of the page. The Create SMS Gateway form opens.
2. In the **SMS Gateway** field, choose **Custom HTTP Handler** from the drop-down list.

* SMS Gateway:
Select the SMS gateway you have service with.

The form displays the configuration options for that gateway type, and the **Service Method** row includes the GET and POST options. When you select the **POST** option, The HTTP Headers and HTTP Post rows are added. You can use the text fields in these rows to override HTTP headers and enter the text to post.

* Service Method:	<input type="radio"/> GET <input checked="" type="radio"/> POST The HTTP method to access the processor
HTTP Headers:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>Override the HTTP headers. For example: Content-Type: text/xml</p>
* HTTP Post:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>Enter the text to POST. See the Service URL for available substitutions.</p>

SMTP Services

Email Format Cleanup Supported

The email and sponsor_email fields were updated to remove display and other formatting passed with the email address by some email clients. Now when an address is passed by applications such as Outlook or Mail.app in a format such as *mailto: Alice Pleasance Liddel <alice@wonderland.org>*, the extraneous elements are stripped away and the format is converted to the plain email address, *alice@wonderland.org*. (1370)

The following issues were fixed in this release.

Administrator

DNS Server Configuration

Bug ID	Description
2277	Resolved an issue where, under certain conditions, manually configured DNS servers could be omitted from the system's DNS configuration.

Network Settings Issue on Chrome Browser

Bug ID	Description
1588	Resolved an issue where changing network interface or DNS settings would not redirect correctly on the Chrome browser.

Packet Capture

Bug ID	Description
2128	Packet capture files downloaded from the user interface now use the “.pcap” extension, rather than “.cap”, for compatibility with the latest version of Wireshark.

Customization

Custom Field Creation

Bug ID	Description
2172	Resolved an issue where a new custom field could be created with the same name as an existing field and the existing field would be overwritten. A new field is now validated for a unique name and cannot overwrite an existing field.

General

Login Page

Bug ID	Description
2171	Resolved an issue where, on certain Web browsers, if the username and password were automatically populated from the browser's credential store, the Submit button of the login page would be disabled, preventing a user from logging in.

SMS and Email

Bug ID	Description
2255	Resolved an issue where versions 3.3 through 3.7 disabled the ability to send an SMS or email to disabled users, including those with an activation time set.

Guest Manager

Editing Guest Account Username

Bug ID	Description
1923	Corrected an issue where renaming an existing user account to have the same name as a previously deleted user account would fail with the error message "ERROR: duplicate key value violates unique constraint 'useraccount_username'".

Large-Import Failure

Bug ID	Description
1992	Resolved an issue that sometimes led to an out-of-memory condition when importing a large number of guest accounts. The total number of user accounts that can be imported in a single operation is now limited to the maximum number of accounts that can be created with the create_multi form.

High Availability Services

Domain Join and Leave Operations

Bug ID	Description
2169	Removed the ability to join or leave the Active Directory domain when a node is part of a High Availability cluster.

RADIUS Disconnect Requests

Bug ID	Description
1749	Added a configuration item to allow specifying the bind address for RFC 3576 disconnect messages. This allows a disconnect operation to work when using a virtual IP address in High Availability cluster mode. In Administrator > Plugin Manager, the Configuration form for the High Availability plugin now includes an option for specifying a particular bind address for RFC-3576 requests. The default setting for this option lets the system choose the address.

Kernel

“No favicon” Log Messages

Bug ID	Description
2048	Resolved an issue where system log error messages would be logged about a non-existent file named “favicon.ico.”

“Undefined Index” PHP Message

Bug ID	Description
2332	Resolved an issue where a PHP message had referred to “Undefined index: P27” (and similar numbers) was sometimes logged during a plugin update. These messages were benign and did not indicate the presence of a problem.

Mobile Device Provisioning Services

Changing From Intermediate to Root CA Mode

Bug ID	Description
2056	Resolved an issue where the allowable clock skew for the Mobile Device Provisioning Services certificate authority could be set to a negative number.

Mac OS X Lion Provisioning

Bug ID	Description
2083	Support was added for device provisioning on OS X 10.7 (Lion).

iOS 5 Devices Were Not Detected as Unique

Bug ID	Description
2024	Resolved an issue where iOS 5 devices were not detected as unique devices for the purpose of limiting the maximum number of devices a user is able to provision.

Operating System

Kernel Package Security Updates

Bug ID	Description
2075	The Linux kernel is now updated with security fixes from RHTSA-2012:0007. For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHTSA-2012-0007.html . The kernel packages contain the Linux kernel, the core of any Linux operating system.
2157	The Linux kernel is now updated with security fixes from RHTSA-2012:0107. For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHTSA-2012-0107.html .
2340	The kernel is now updated with security fixes from RHTSA-2012:0480-1 (Important). For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHTSA-2012-0480.html .

libpng Package Security Updates

Bug ID	Description
2339	The libpng package is now updated with security fixes from RHTSA-2012:0407 (Moderate) and RHTSA-2012:0523 (Moderate). For more information on the issues addressed by these updates, see https://rhn.redhat.com/errata/RHTSA-2012-0407.html and https://rhn.redhat.com/errata/RHTSA-2012-0523.html . The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

RPM Package Security Updates

Bug ID	Description
2337	The RPM package is now updated with security fixes from RHTSA-2012:0451. For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHTSA-2012-0451.html . The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

OpenSSL Package Security Updates

Bug ID	Description
2338	The OpenSSL package is now updated with security fixes from RHTSA-2012:0426 (Moderate) and RHTSA-2012:0518 (Important). For more information on the issues addressed by these updates, see https://rhn.redhat.com/errata/RHTSA-2012-0426.html and https://rhn.redhat.com/errata/RHTSA-2012-0518.html . The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

RADIUS Services

Active Sessions Username Display and Disconnect Issues

Bug ID	Description
2197	Corrected an issue where Active Directory user accounts authenticated by RADIUS Services were displayed in the Active Sessions list view with a double backslash separating the domain name and the username. This issue also caused RFC 3576 disconnections to fail for these sessions.

EAP Server Certificate Import Failure

Bug ID	Description
2148	Resolved an issue where attempting to import an EAP server certificate would fail with the error message "Private key is invalid or passphrase is incorrect (error:0906A068:PEM routines:PEM_do_header:bad password read)" if the certificate's private key was encrypted.

Login Page Support for Motorola Controllers

Bug ID	Description
2156	Added Web login page support for Motorola controllers that are using version 6.0 code.

Parsing Value Error

Bug ID	Description
2072	Resolved an issue where the message "ERROR: Failed parsing value "" for attribute FreeRADIUS-Client-IPv6-Address: failed to parse IPv6 address string "": ip_hton: Name or service not known" was displayed in the RADIUS Debugger. This message is benign and did not indicate an actual error, and has been removed.

Scrolling Behavior on Apple Devices

Bug ID	Description
2264	Support is now added for detecting the Captive Network Assistant in iOS 5.1, which has some changes in behavior compared to iOS 5.0 and iOS 4.x.

Skins

HTML Error on iPhone During Device Provisioning

Bug ID	Description
2034	Corrected an issue with several skins that could cause an HTML error to be displayed for iPhone devices in the Safari Debug Console.

The following are known issues and caveats. Applicable bug IDs and workarounds are included when possible.

General

Bug ID	Description
1956 1973	<p>Connecting multiple network adapters to the same physical network, or having the same subnet assigned to multiple network adapters is not recommended. This configuration may cause errors such as “IP address already in use” when changing network interface settings, or bringing one of the network interfaces up or down.</p> <p>Workaround: Avoid connecting multiple network adapters to the same physical network, or having the same subnet assigned to multiple network adapters.</p>

Mobile Device Provisioning Services

Bug ID	Description
2202	<p>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.</p>

SMS Services

Bug ID	Description
1877	<p>From the Edit Accounts page: if multiple accounts share the same phone number and all are selected, then SMS is received multiple times.</p> <p>Workaround: Avoid selecting multiple accounts that share identical phone numbers.</p>
2272	<p>Unicode SMS messages are limited to 70 Unicode characters. The ClearPass Guest user interface will still display 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. If you plan to use Unicode SMS messages, check your SMS receipt carefully to ensure it is not over 70 characters in length.</p>

This chapter contains information and procedures for successfully updating to this software release as well as upgrading the appliance.



The upgrade procedure and requirements are the same as they were in the 3.7 release. To ensure a successful upgrade, read the contents in this chapter completely before upgrading.

The basic upgrade is:

1. Verify that your system's memory is sufficient to upgrade.
2. Perform a complete configuration backup.
3. Update the software using the Plugin Manager.

Important Points to Remember

- Best practices recommends upgrading during a maintenance window. This will limit the troubleshooting variables.
- Verify your system's memory configuration. We recommend a virtual machine's system memory minimum of 1 GB (1024 MB), and a minimum for the Web Application of 256 MB.



Recovering the appliance from an "out of memory" state may require rebuilding your server from a recent configuration backup.

- Best practices recommends backing up your configuration at regular intervals.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- Read all the information and procedures in this chapter before upgrading.

Before you Upgrade

Ensure the following before performing an upgrade.

- Verify that the memory limit is set to at least 256M (see "[Setting System Memory](#)" on page 29).
- Backup your configuration (see "[Configuration Backup](#)" on page 30)
- If you are running a virtual machine, take a snapshot of it (see "[Snapshot of the Virtual Machine](#)" on page 31)

Setting System Memory

To increase the memory limit, navigate to **Administrator > System Control > Web Application** and change the "Memory Limit" to read **256M**. Click **Save Changes** to save your setting and restart the web server so that the changes takes effect (see [Figure 1](#)).

Figure 1 Increasing the web application's memory limit

The screenshot shows the 'System Configuration Options' dialog box. It is divided into four sections: 'Resource Limits', 'Time Limits', 'Performance Options', and 'Security Options'.
- **Resource Limits:** Includes 'Memory Limit' (256M bytes), 'Form POST Size' (10M bytes), and 'File Upload Size' (5M bytes).
- **Time Limits:** Includes 'Input Time' (60 seconds) and 'Socket Timeout' (60 seconds).
- **Performance Options:** Includes a checkbox for 'Enable zlib output compression' (unchecked).
- **Security Options:** Includes a checkbox for 'Include PHP header in web server response' (checked).
A 'Save Changes' button is located at the bottom right.

Configuration Backup

Perform a complete configuration backup and virtual machine snapshot (if applicable) before upgrading your software. The configuration backup and virtual machine snapshot will provide a restore point in the event a restore is required.

Navigate to **Administrator > Backup & Restore > Configuration Backup** (see [Figure 2](#)) and download a complete backup configuration.

Figure 2 Configuration Backup dialog prior to a system update.

The screenshot shows the 'Configuration Backup' dialog box. It has two main fields: 'Backup Mode' and 'Backup Name'.
- **Backup Mode:** A dropdown menu is set to 'Complete backup'.
- **Backup Name:** A text field contains 'amigopod67.support-ad.corp.airwave.com 2012-01-05-1814'.
A 'Download Backup' button with a downward arrow icon is located at the bottom center.

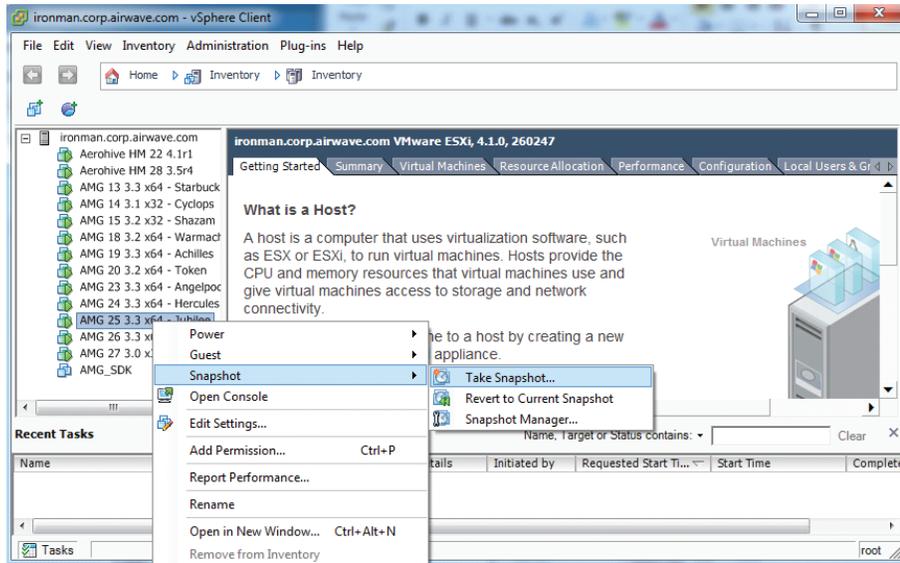
Snapshot of the Virtual Machine

If the appliance is running a VMware virtual machine, we recommend that you take a snapshot of the virtual machine to preserve its state.



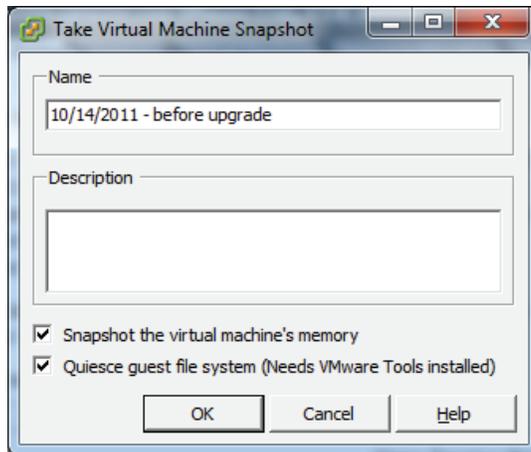
Select the “Quiesce guest file system (Needs VMware Tools installed)” option when taking a snapshot of the virtual machine (Figure 3). This ensures that the state of the file system is captured at a point in time where it is safe to do so.

Figure 3 A virtual machine snapshot prior to update.



Enter the name and date of this snapshot and click “OK” (see Figure 4)

Figure 4 Take Virtual Machine Snapshot dialog



To free space on the VMware host, you can remove this snapshot after a successful upgrade. Maintaining multiple snapshots may reduce performance of the virtual machine.

Upgrading Amigopod Software

If you are running Amigopod 3.3 or 3.5, follow the instructions in this section.

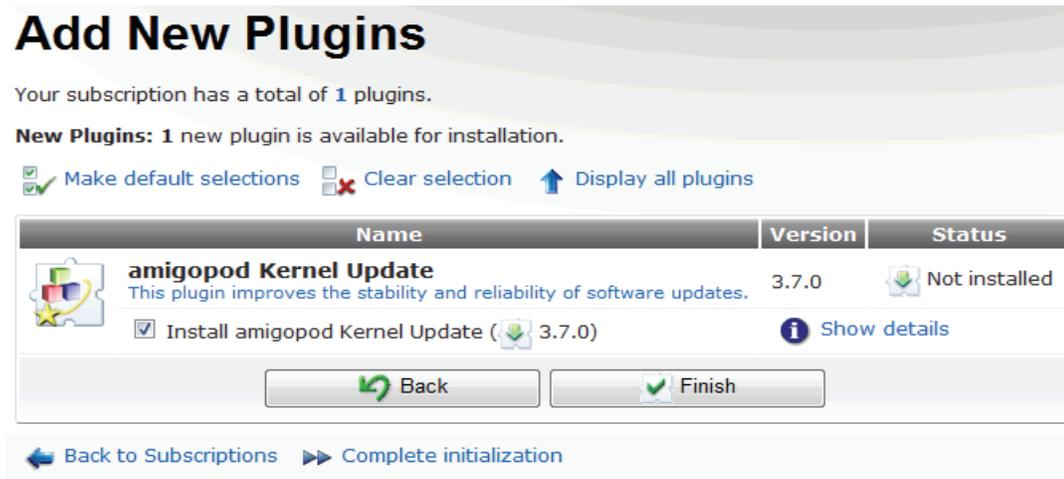
Use the Plugin Manager to upgrade your Amigopod software. Navigate to **Administrator > Plugin Manager > Update Plugins**. When upgrading from a previous version of Amigopod, initially only one plugin is available to install; the Amigopod Kernel Update (see [Figure 5](#)). Once the kernel is installed, you can update the other plugins.

1. Verify that the “Install amigopod Kernel Update...” is clicked.
2. Click **Finish** to download and install the software upgrade.
3. Re-enter the Plugin Manager (**Administrator > Plugin Manager > Update Plugins**) and check for any other plugin updates for Amigopod 3.7.2. Select your plugins and click **Finish**.
4. Restart your system services or reboot the server before your software upgrade takes effect.



When upgrading a High Availability cluster, the cluster must be destroyed prior to updating any plugins. Repeat the plugin update on both nodes of the cluster, and rebuild the cluster after the software update has been completed successfully.

Figure 5 Add New Plugins

The screenshot shows a web interface titled "Add New Plugins". It states "Your subscription has a total of 1 plugins." and "New Plugins: 1 new plugin is available for installation." Below this are three links: "Make default selections" (checked), "Clear selection", and "Display all plugins". A table lists the available plugin:

Name	Version	Status
 amigopod Kernel Update This plugin improves the stability and reliability of software updates.	3.7.0	 Not installed

Below the table, there is a checked checkbox for "Install amigopod Kernel Update (3.7.0)" and a "Show details" link. At the bottom of the table are "Back" and "Finish" buttons. Below the table are two navigation links: "Back to Subscriptions" and "Complete initialization".