ClearPass Guest 3.9.7

(Amigopod 3.9.7)

Release Notes

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Release Overview

ClearPass Guest 3.9.7 is a patch release that provides fixes to outstanding issues. These release notes include the following chapters:

- Chapter 2, "What's New in This Release" on page 9—Describes new features and issues introduced in this 3.9.7 release, as well as features introduced in previous 3.9 releases.
- Chapter 3, "Enhancements in Previous 3.9.x Releases" on page 11—Describes new features introduced in earlier 3.9.x releases.
- Chapter 4, "Issues Fixed in Previous 3.9.x Releases" on page 15—Lists issues fixed in previous 3.9 releases.
- Chapter 5, "Known Issues Identified in Previous 3.9.x Releases" on page 29—Lists extant known issues identified in previous 3.9 releases.
- Chapter 6, "Upgrade Procedure" on page 31—Provides upgrade instructions for previous versions of Amigopod.

Supported Browsers

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

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

ClearPass Guest software is delivered as a pre-installed virtual appliance. For additional information refer to "System Requirements" on page 6 and "VMware Requirements" on page 6. The files for this release are:

2013-2-27-ClearPassGuest-VirtualAppliance-3.9.7-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.

2013-2-27-ClearPassGuest-ESX3Appliance-3.9.7-x86_64.zip

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

2013-2-27-ClearPassGuest-VmwarePlayer-3.9.7-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 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, increase the resources allocated to the virtual machine according to the load you expect to support.

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+

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. 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 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.

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

What's New in This Release

This chapter provides a brief summary of changes in the 3.9.7 release, as well as features introduced in previous 3.9.x releases.

This chapter contains the following sections:

New Features and Enhancements in the 3.9.7 Release

No new features were introduced in this release.

Issues Resolved in the 3.9.7 Release

The following issues have been fixed in the ClearPass Guest 3.9.7 release. For a list of issues fixed in previous 3.9 releases, see Chapter 4, "Issues Fixed in Previous 3.9.x Releases" on page 15.

ClearPass Platform

Table 2 below lists issues resolved in the ClearPass Platform in 3.9.7.

Table 2 *ClearPass Platform Issues Fixed in 3.9.7*

Bug ID	Description
12728	The Web login vendor settings for Ruckus were updated to support ZoneDirector 8.0.

Kernel

Table 3 below lists issues resolved in the Kernel in 3.9.7.

Table 3 *Kernel Issues Fixed in 3.9.7*

Bug ID	Description
12903	A security enhancement ensures that the session cookie ID is always changed when logging in or out.

New Known Issues in the 3.9.7 Release

No significant new known issues have been identified since the last release. For a list of known issues found in previous 3.9.x releases, see Chapter 5, "Known Issues Identified in Previous 3.9.x Releases" on page 29.

Chapter 3

Enhancements in Previous 3.9.x Releases

This chapter provides a brief summary of the features and enhancements introduced in previous 3.9.x releases.

Features and Enhancements in Previous 3.9.x Releases

Administrator

- **SMS SMTP carriers enhancements:** 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. (#12119)

  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.
- **SSL parameters editable**: SSL protocols and supported SSL cipher suites may be edited to allow fine-grained control over security policy. Default values for these fields allow SSL access using only high-strength ciphers (128-bit encryption or better), which should be acceptable for most installations. (#10066)
- **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, best practices is to 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. (#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 were renamed. (#2049)

Customization

- **Multi-file content upload:** You can now upload multiple content asset files and folders or a Web deployment archive. 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 upload 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. (#501)
- **Configurable page elements:** From the **Customization > 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 **Page Properties** area at the bottom of the **Edit Properties** form. (#2307)
- **Default guest receipt enhanced:** The default Guest Manager Receipt print template’s format and is enhanced for optimum display and compatibility in more email clients. (#2333)

General

- **Introducing ClearPass Guest and ClearPass Onboard:** The 3.9 release introduced the integration of Amigopod with Aruba Networks' QuickConnect and the ClearPass Policy Manager platform. As part of the changes, the Amigopod Visitor Management Solution was renamed, and is now called ClearPass Guest. Mobile Device Provisioning Services (MDPS) is now called ClearPass Onboard. These names are updated throughout the application, documentation, and various programmatic elements.
- **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 and other name changes:** The Amigopod name was changed throughout the application. (#2043, #2241) In addition to 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.
- **Integration with other ClearPass servers configurable:** Support was added for controlling integration with ClearPass Policy Manager and ClearPass Profile, letting you send information about account registration or device provisioning. (#2238)

Guest Manager

- **Login provided in receipt URL**: SMS receipts can now include the guest's username and password in the login URL, letting the guest click Login once and have their login info automatically populated on Guest login pages. This avoids having to copy-paste or remember a password between screens. (#11821)
- **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. To use this feature, go to **Customization > Forms & Views**, click the **create_multi** row, then click its **Edit Fields** link. (#2291)
- **Sponsor confirmation for role selection:** The sponsored self-registration workflow now allows the sponsor to choose the role for the user account when the sponsor approves the self-registered account. To use this feature, go to **Customization > Guest Self-Registration**, click the **Guest Self-Registration** row, then click **Edit**. In the **Receipt Page** area of the diagram, click **Actions**. (#2151)

Kernel

- **Ruckus Wi-Fi controllers supported for device onboarding:** Support was added for onboarding devices that use a Ruckus Wi-Fi controller and MAC address. (#10633)
- **Disabling credentials caching supported:** A global toggle option for disabling autocomplete was added to the Kernel plugin configuration form, allowing credential caching to be turned off. (#10201)
- **Form navigation enhanced:** Usability of certain list views within the application is improved. Inserted rows and rows with inline editing capabilities are now automatically selected when editing. (#10234)

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. To use these options, go to **RADIUS > User Roles** and click the **Edit** link for the role. (#2170)

Onboard (Mobile Device Provisioning Services)

- **Windows 8 supported:** Support for Windows 8 clients was added to ClearPass Onboard. (#11526)
- **Code-signing certificate import supported:** ClearPass Onboard supports the import of a code-signing certificate chain and private key for signing the Windows provisioning application. Certificates can be uploaded as PFX, PKCS-12, SPC, or PKCS-7, and can include a chain of certificates. An operator's profile must include the Import Code-Signing Certificate privilege in order to access this feature. (#9860)
- **MDPS is now ClearPass Onboard:** Mobile Device Provisioning Services (MDPS) has merged with QuickConnect and is now called ClearPass Onboard. In the 3.9.0 release, it also supports configuration and provisioning for all "bring your own device" (BYOD) and IT-managed devices, including Windows, Android, OS X 10.5+, and wired clients. For more information, please refer to the ClearPass Onboard documentation on the Aruba Support Center. (#2176, #2177, #2183, #2203, #2204)
- **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)
- **Certificate trust chain and certificate bundle options:** A new option on the **Export Certificate** form lets you include the certificate trust chain when you export a certificate in PEM format. You can use this option to create and export a certificate bundle that includes the Intermediate CA and Root CA and can be imported in ClearPass Policy Manager as the server certificate. ClearPass Policy Manager does not accept PKCS#7. (#2355)
- **Certificate bundle downloads:** You can now download the root CA certificate together with any intermediate certificates as a bundle. (#2287)
- **Custom certificate trust settings:** A new option for Android devices lets you provision a custom certificate to an Android device that is provisioned using ClearPass Onboard. When this option is not selected, the default behavior is to provision the ClearPass Onboard Root CA certificate. (#2375)
- **Tag for username included in device information**: The **Owner** tag is now included in the Onboard device information that is sent to ClearPass Policy Manager when a device is provisioned. This tag contains the username of the person who enrolled the device. This allows some functions that operate on tags to perform username-based queries. (#2376)
- **Enhanced device profiling supported in CPPM:** During mobile device provisioning enrollment, Onboard now sends device classification explicitly to ClearPass Policy Manager (CPPM) by POST syntax, rather than indirectly through http_user_get. Device classification information includes category, family, and name. Profile support requires ClearPass Policy Manager 5.2.0 or later. (#10144, #10162)

- **Wired configuration profiles for OS X Lion device provisioning:** Support was added for provisioning wired network profiles for OS X 10.7 and later. (#10089)

Operator Logins

- **Operator profile included in application log:** When an operator logs in, their operator profile is now included in application logging. (#10643)
- **CLI Reset Administrator Password option enhanced:** The **Reset web password for admin** option in the command line interface now restores the administrator account's operator profile if necessary. (#10649)

RADIUS Services

- **Logging enhancements:** Logging details now include the reason for authorization failures when processing a RADIUS request. This can aid in troubleshooting the exact cause of an Access-Reject. (#11808)
- **MAC auto-registration in CPPM:** Support was added for automatically registering guest MAC addresses as endpoint records in ClearPass Policy Manager (CPPM) 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)
- **Internal authorization type configuration option:** A new configuration option, **Internal Auth Type**, was added to the RADIUS Services plugin. This option lets you specify the authentication method to use for internally-generated RADIUS requests such as Web login page authentication or device provisioning requests. Previously, these requests used PAP for authentication, which had displayed the user's password in cleartext to the administrator in the RADIUS debugger. The new Internal Auth Type option lets the administrator select either PAP, CHAP, or MSCHAP as the authentication mode to use for internal RADIUS requests. (#2356)
- **Extra spaces trimmed from values on Web login:** Leading and trailing spaces are now automatically removed from all values submitted on the Web login and account setup pages. This prevents issues where a login attempt would fail if the user had entered extra spaces in a field—for example, following a username or email address. (#2348)

SMS Services

- **Additional text with phone number supported:** Support was added for sending SMS via SMTP when the carrier's email address requires additional text before or after the phone number. To use this feature, use a template that contains the uppercase word **NUMBER**—for example, **NUMBER.msg@carrier.example.com**. (#11538)
- **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)
- **POST method supported:** Support was added for specifying the HTTP method to use—either GET or POST—when creating a custom SMS handler. (#2163)

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 previous 3.9.x releases. For a list of issues resolved in the 3.9.7 release, see the What's New in This Release chapter.

Fixed in 3.9.6

Administrator

Table 4 below lists issues resolved in the Administrator module in 3.9.6.

Table 4 *Administrator Issues Fixed in 3.9.6*

Bug ID	Description
12013	In certain failure situations the built-in process monitor did not automatically restart the Apache Web server, leading to the failure message "httpd failed to start" in the system log.

Guest Manager

Table 10 below lists issues resolved in the Guest Manager module in 3.9.6.

Table 5 *Guest Manager Issues Fixed in 3.9.6*

Bug ID	Description
12223	Creating a new account from the List Accounts page now works correctly after the create form is overridden by a guest self-registration form.

RADIUS Services

Table 13 below lists issues resolved in RADIUS Services in 3.9.6.

Table 6 *RADIUS Services Issues Fixed in 3.9.6*

Bug ID	Description
12133	In certain authorization failure conditions, the error message “PHP Notice: Undefined index: message” was logged in the application log. This message was accompanied by another error similar to “Authorization failed for ‘username’: %2”, which did not include details about the authorization failure.

Translations

Table 7 below lists issues resolved with translations in 3.9.6,

Table 7 *Translation Issues Fixed in 3.9.6*

Bug ID	Description
12120	The application log message "PHP Notice: Language not supported: ja" was repeatedly logged when using the Japanese Translations plugin. This notice was benign and did not indicate a problem.

Fixed in 3.9.5

ClearPass

Table 9 below lists issues resolved in ClearPass in 3.9.5.

Table 8 *ClearPass Issues Fixed in 3.9.5*

Bug ID	Description
11762	An endpoint could be profiled into the category "Smartdevice" instead of "SmartDevice".

Customization

Table 9 below lists issues resolved in Customization in 3.9.5.

Table 9 *Customization Issues Fixed in 3.9.5*

Bug ID	Description
11587	The {nwa_radius_query} function was 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.

Guest Manager

Table 10 below lists issues resolved in Guest Manager in 3.9.5.

Table 10 *Guest Manager Issues Fixed in 3.9.5*

Bug ID	Description
11259	An account that required sponsorship approval and that was scheduled to be activated at a future time was incorrectly activated at the time the sponsor approved the account.
11423	Random usernames and passwords now have visually similar characters removed—for example, depending on the method, a mix of characters such as: i l 1 0 O o 5 S 2 Z 8 B The list of characters entered in the **Disallowed Password Characters** field in the Guest Manager plugin configuration will now be excluded from any randomly generated password.

Onboard

Table 11 below lists issues resolved in Onboard in 3.9.5.

Table 11 *Onboard Issues Fixed in 3.9.5*

Bug ID	Description
11089	A PHP notice, “Undefined variable: args,” was sometimes displayed during device provisioning with Onboard. The message was harmless and did not indicate a provisioning problem.
11151	Profile would incorrectly classify an Android device as a Windows device when the device was provisioned using Onboard.
11249	In certain circumstances, provisioning a device using Onboard did not honor a Session-Timeout attribute returned from the device authorization RADIUS request, which could have led to Onboard calculating an incorrect certificate expiration time.
11725	Attempting to reprovision a device sometimes resulted in a “404 Page Not Found” error.
11742	Added support for using Onboard for a 802.1X wired network on Windows 7 SP1 and later. **Note:** Versions of Windows earlier than Windows 7 SP1 do not support this capability. Also note that 802.1X credentials can be set only for users with administrator privileges, which means that non-administrator users can't use Onboard to get on to the wired network.
11812	An issue introduced with an earlier fix (#10144) had caused ClearPass Profile to fail when used with ClearPass Guest 3.9.

Operating System

Table 12 below lists issues resolved in the operating system in 3.9.5.

Table 12 *Operating System Issues Fixed in 3.9.5*

Bug ID	Description
11288	The Apache Web server component was updated to address CVE-2012-0053. For more information on CVE-2012-0053, refer to http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053.

RADIUS Services

Table 13 below lists issues resolved in RADIUS Services in 3.9.5.

Table 13 *RADIUS Services Issues Fixed in 3.9.5*

Bug ID	Description
11047	A security update was applied for CVE-2012-3547, affecting users of EAP-TLS, EAP-TTLS, and PEAP. For more information on CVE-2012-3547, refer to http://freeradius.org/security.html.
11902	A user account was incorrectly paired with a MAC caching account even when the MAC account had expired and was deleted.

Skins

Table 14 below lists issues resolved with skins in 3.9.5,

Table 14 *Skin Issues Fixed in 3.9.5*

Bug ID	Description
11304	In certain conditions, one or more of the <html>, <head> or <body> elements were duplicated in an email message. This could have led to incorrect rendering of HTML-formatted emails.

SMS Services

Table 15 below lists issues resolved in SMS Services in 3.9.5.

Table 15 *SMS Services Issues Fixed in 3.9.5*

Bug ID	Description
11750	A new SMS gateway, **Clickatell (Mobile Origination)**, was added for use when you are using the Clickatell SMS gateway and require the Mobile Origination flag to be set (MO=1).
11811	If the account balance was negative, the error message “Error retrieving account balance” was displayed. Gateways with a negative credit balance are now displayed correctly.

Fixed in 3.9.4

Kernel

Table 16 below lists issues resolved in the kernel in 3.9.4.

Table 16 *Kernel Issues Fixed in 3.9.4*

Bug ID	Description
10795	Corrected a potential cross-site scripting (XSS) issue affecting multiple pages in the application.

MAC Authentication

Table 17 below lists issues resolved in MAC Authentication in 3.9.4.

Table 17 *MAC Authentication Issues Fixed in 3.9.4*

Bug ID	Description
10784	Values for the **mac** field in guest accounts were not updated when the MAC Authentication plugin was configured. Now when the MAC Authentication plugin configuration is edited, all MAC fields included on forms are updated with the current format.

Onboard

Table 18 below lists issues resolved in Onboard in 3.9.4.

Table 18 *Onboard Issues Fixed in 3.9.4*

Bug ID	Description
10746	Deleting a certificate could leave a reference to it in the network configuration. Now when a certificate is deleted, any references to it in the network configuration are also removed.

Operating System

Table 19 below lists issues resolved in the operating system in 3.9.4.

Table 19 *Operating System Issues Fixed in 3.9.4*

Bug ID	Description
10778	PHP was upgraded to the latest 5.3.16 version. This version of the PHP scripting language addresses the following security issues: CVE-2012-1172 CVE-2012-1823 CVE-2012-2143 CVE-2012-2311 CVE-2012-2688 CVE-2012-3365

RADIUS Services

Table 20 below lists issues resolved in RADIUS Services in 3.9.4.

Table 20 *RADIUS Services Issues Fixed in 3.9.4*

Bug ID	Description
10687	An error message was displayed if incorrect root password details were entered and saved on the **Edit RADIUS Data Source** page. For both the user account and the root account, validation was added to allow changes to be saved only if the entered credentials are correct.
10688	Resetting the database to default settings did not work after the database root password was changed.

Reporting Manager

Table 21 below lists issues resolved in Reporting Manager in 3.9.4.

Table 21 *Reporting Manager Issues Fixed in 3.9.4*

Bug ID	Description
10723	A case mismatch between RADIUS accounting records and the visitor account resulted in empty fields displayed in a report.

Fixed in 3.9.3

Kernel

Table 22 below lists issues resolved in the kernel in 3.9.3.

Table 22 *Kernel Issues Fixed in 3.9.3*

Bug ID	Description
10264	Plugin updates sometimes failed with a message similar to `Cannot open source file for copy....`

Onboard

Table 23 below lists issues resolved in Onboard in 3.9.3.

Table 23 *ClearPass Onboard Issues Fixed in 3.9.3*

Bug ID	Description
10186	Using the `Reinitialize ClearPass Guest Database` option from the command line interface caused subsequent attempts to save changes from Onboard's Provisioning Settings and Network Settings pages to fail with the message `Failed to load the Mac OS X JNLP template file`.
10312	In the **Network Settings > Trust** page, the information for Android custom certificate trust settings was clarified.
10371	Uploading a certificate signing request (CSR) with a subject ALT name caused PHP warnings in the log files.
10418	The configured "Max Devices" limit was not applied to user accounts authenticated with Active Directory.
10458	Deleting certificates on the Reset to Factory Defaults page produced an error message. The certificates were deleted correctly.

Palo Alto Network Services

Table 24 below lists issues resolved with Palo Alto Network Services in 3.9.3.

Table 24 *Palo Alto Network Services Issues Fixdd in 3.9.3*

Bug ID	Description
10515	For usernames in the format DOMAIN\username, the username sent to the Palo Alto Networks user ID agent contained a double backslash (\\) instead of a single backslash.

SMS Services

Table 25 below lists issues resolved in SMS Services in 3.9.3.

Table 25 *SMS Services Issues Fixed in 3.9.3*

Bug ID	Description
10465	When using the SMS over SMTP gateway, the "Send SMS receipt" page was missing the Mobile Carrier drop-down list.

Table 25 *SMS Services Issues Fixed in 3.9.3 (Continued)*

Bug ID	Description
10464	Cool SMS DK acknowledges a successful transmission appropriately in either English (“success”) or Danish (“korrekt”) depending on the location.
10463	Content in the message body was URL-escaped by the custom HTTP SMS handler in POST mode.

Support Services

Table 26 below lists issues resolved in Support Services in 3.9.3.

Table 26 *Support Services Issues Fixed in 3.9.3*

Bug ID	Description
10437	Corrected a directory traversal vulnerabilty in the online documentation browser.

Fixed in 3.9.2

High Availability

Table 27 below lists issues resolved in High Availability in 3.9.2.

Table 27 *High Availability Issues Fixed in 3.9.2*

Bug ID	Description
10091	Trying to set up a High Availability cluster when using a shared key with a hash symbol (#) caused the setup to stall at initializing remote node service. When the hash symbol was removed, cluster setup continued.

Kernel

Table 28 lists issues resolved in the kernel in 3.9.2.

Table 28 *Kernel Issues Fixed in 3.9.2*

Bug ID	Description
10121	The color picker was sometimes hidden on pages whose skin had a z-index set.

Onboard

Table 29 lists issues resolved in Onboard in 3.9.2.

Table 29 *ClearPass Onboard Issues Fixed in 3.9.2*

Bug ID	Description
10090	When the Maximum Devices limit was set to “1”, a previously-provisioned device whose profile had been deleted could not be re-provisioned under the same username. The error message said the user had already provisioned the maximum number of devices.

Table 29 *ClearPass Onboard Issues Fixed in 3.9.2 (Continued)*

Bug ID	Description
10094	During Win-XP onboarding, the error `Cannot authenticate with wireless` was displayed although the device connected and authenticated successfully.
10104	The Hidden Network setting can now be enabled for Windows Vista and Windows 7+ devices on the Network Settings page. This setting lets you provision hidden (non-broadcast) wireless networks for these devices.
10129	An error was produced on a Korean Windows 7 laptop system when the Quick1x app ran during Onboard system configuration.
10134	Deleting a certificate in ClearPass Guest did not delete the corresponding Onboard device from ClearPass Policy Manager. Device credentials are now deleted in Policy Manager when the certificate is deleted in Guest. Users should also be aware that if Onboard is reset, the Onboard device is not automatically deleted from Policy Manager, and needs to be removed by the user.
10151	Windows laptops sometimes failed to Onboard with the wired network setting. Users should be aware that the network settings name may not contain any special characters.
10162	Endpoint Fingerprint details of onboarded devices were not shown correctly in Policy Manager.

RADIUS Services

Table 30 lists issues resolved in RADIUS Services in 3.9.2.

Table 30 *RADIUS Services Issues Fixed in 3.9.2*

Bug ID	Description
10109	Using the **Log In** button on the **Guest Registration Receipt** page (guest_register_receipt.php) did not record the MAC address in the Endpoints table.

Security

Table 31 lists security issues resolved in 3.9.2.

Table 31 *Security Issues Fixed in 3.9.2*

Bug ID	Description
10173	A cross-site scripting (XSS) flaw was identified and fixed. This flaw affected several pages in the application.
10174	A validation error caused by insufficient checking of input data was corrected. This error was harmless but could lead to error messages indicating an invalid SQL query.

Fixed in 3.9.1

Administrator

Table 32 lists issues resolved in Administrator in 3.9.1.

Table 32 *Administrator Issues Fixed in 3.9.1*

Bug ID	Description
2373	On the **Administrator > Network Setup > HTTP Proxy** page, if an HTTP proxy URL contained an @ character, the characters following it were not masked, and the latter half of the password was displayed.

Guest Manager

Table 33 lists issues resolved in Guest Manager in 3.9.1.

Table 33 *Guest Manager Issues Fixed in 3.9.1*

Bug ID	Description
2350	Updating plugins on a system that had numerous guest self-registration forms caused an out-of-memory condition.

Kernel

Table 34 lists issues resolved in the kernel in 3.9.1.

Table 34 *Kernel Issues Fixed in 3.9.1*

Bug ID	Description
2370	Uploading a single plugin file sometimes caused an Internal Server Error and the plugin update operation would fail.

LDAP Sponsor Lookup

Table 35 lists issues resolved in LDAP in 3.9.1.

Table 35 *LDAP Issues Fixed in 3.9.1*

Bug ID	Description
2304	LDAP sponsor lookup matches were case-sensitive, which was unexpected behavior. Sponsor detail matching is not case-sensitive now.

Onboard

Table 36 lists issues resolved in Onboard in 3.9.1.

Table 36 *ClearPass Onboard Issues Fixed in 3.9.1*

Bug ID	Description
2317	For certain combinations of devices, the number of devices that could be provisioned exceeded the limit set in the **Maximum Devices** field of the **Provisioning Settings** page.
2357	Re-provisioning an iOS device with the same user name would incorrectly create a new TLS client certificate, although the existing certificate was still valid.
2366	Deleting the unique device credentials from ClearPass Policy Manager would fail when revoking a client certificate.
2368	If Onboard was configured to use the Intermediate CA mode, using the Reset to Factory Defaults option to delete all Onboard certificates sometimes generated the message `Internal error: the certificate with ID... does not have a valid fingerprint.`
2378	Certain certificates could not be uploaded on the **Onboard > Network Settings > Trust** tab. The system displayed the error message `Error parsing certificate: Unexpected identifier (0x82) when looking for [2] at offset 0.`
2379	For non-iOS devices, the RADIUS Session-Timeout attribute returned during authorization for device provisioning was not reflected in the resulting device certificate's expiration time.
2380	Enrolling the same device multiple times using different user names would incorrectly reuse an existing device certificate with a different user name.
2389	The Onboard left navigation is now arranged alphabetically.

Fixed in 3.9.0

Administrator

Table 37 lists issues resolved in Administrator in 3.9.0.

Table 37 *Administrator Issues Fixed in 3.9.0*

Bug ID	Description
1588	Changing network interface or DNS settings would not redirect correctly on the Chrome browser.
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.
2277	Under certain conditions, manually configured DNS servers could be omitted from the system's DNS configuration.

Customization

Table 38 below lists issues resolved in Customization in 3.9.0.

Table 38 *Customization Issues Fixed in 3.9.0*

Bug ID	Description
2172	It was possible to create a new custom field with the same name as an existing field, and the existing field was overwritten. A new field is now validated for a unique name and cannot overwrite an existing field.

General

Table 39 lists general issues resolved in 3.9.0.

Table 39 *General Issues Fixed in 3.9.0*

Bug ID	Description
2171	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.
2255	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

Table 40 lists issues in resolved Guest Manager in 3.9.0.

Table 40 *Guest Manager Issues Fixed in 3.9.0*

Bug ID	Description
1923	Renaming an existing user account to have the same name as a previously deleted user account failed with the error message `ERROR: duplicate key value violates unique constraint 'useraccount_username'.`
1992	An out-of-memory condition was sometimes caused 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

Table 41 lists issues resolved in High Availability in 3.9.0.

Table 41 *High Availability Services Issues Fixed in 3.9.0*

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

Kernel

Table 42 lists issues resolved in the kernel in 3.9.0.

Table 42 *Kernel Issues Fixed in 3.9.0*

Bug ID	Description
2048	System log error messages logged a non-existent file named `favicon.ico`.
2332	A PHP message that referred to “Undefined index: P27” (and similar numbers) was sometimes logged during a plugin update. These messages did not indicate the presence of a problem.

Onboard

Table 43 lists issues resolved in Onboard in 3.9.0.

Table 43 *ClearPass Onboard Issues Fixed in 3.9.0*

Bug ID	Description
2024	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.
2056	The allowable clock skew for the Mobile Device Provisioning Services certificate authority could be set to a negative number.
2083	Device provisioning on OS X 10.7 (Lion) is now supported.

Operating System

Table 44 lists issues resolved in the operating system in 3.9.0.

Table 44 *Operating System Issues Fixed in 3.9.0*

Bug ID	Description
2075	The Linux kernel is now updated with security fixes from RHSA-2012:0007. For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHSA-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 RHSA-2012:0107. For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHSA-2012-0107.html.
2337	The RPM package is now updated with security fixes from RHSA-2012:0451. For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHSA-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.
2338	The OpenSSL package is now updated with security fixes from RHSA-2012:0426 (Moderate) and RHSA-2012:0518 (Important). For more information on the issues addressed by these updates, see https://rhn.redhat.com/errata/RHSA-2012-0426.html and https://rhn.redhat.com/errata/RHSA-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.
2339	The libpng package is now updated with security fixes from RHSA-2012:0407 (Moderate) and RHSA-2012:0523 (Moderate). For more information on the issues addressed by these updates, see https://rhn.redhat.com/errata/RHSA-2012-0407.html and https://rhn.redhat.com/errata/RHSA-2012-0523.html. The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Table 44 *Operating System Issues Fixed in 3.9.0 (Continued)*

Bug ID	Description
2340	The kernel is now updated with security fixes from RHSA-2012:0480-1 (Important). For more information on the issues addressed by this update, see https://rhn.redhat.com/errata/RHSA-2012-0480.html.

RADIUS Services

Table 45 lists issues resolved in RADIUS Services in 3.9.0.

Table 45 *RADIUS Serivces Issues Fixed in 3.9.0*

Bug ID	Description
2072	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.
2148	Attempting to import an EAP server certificate failed 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.
2156	Added Web login page support for Motorola controllers that use version 6.0 code.
2197	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.
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

Table 46 lists issues resolved with skins in 3.9.0.

Table 46 *Skin Issues Fixed in 3.9.0*

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

The following known issues were identified in previous releases. Workarounds are included when possible. For a list of known issues identified in the 3.9.7 release, see the What's New in This Release chapter.

General

Table 47 below lists general known issues in previous releases.

Table 47 *Known Issues, General*

Bug ID	Description
1956 (9651) 1973 (9668)	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. **Workaround**: Avoid connecting multiple network adapters to the same physical network, or having the same subnet assigned to multiple network adapters.

Onboard (Mobile Device Provisioning Services)

Table 48 below lists known issues in Onboard in previous releases.

Table 48 *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.
10229	QuickConnect cannot process passwords that contain the ampersand (&), backslash (\), or equal-to (=) characters. If a password contains one of these characters, the special character and all characters trailing it are ignored and login fails. For example, if the password provided is "Password123&", QuickConnect sends "Password123" to Onboard. If the password is "Password&123", it sends "Password". **Workaround**: Do not use the ampersand (&), backslash (\), or equal-to (=) characters in a password.
10525	Wired clients fail to connect to an 802.1x port that is also being used for wireless provisioning.

SMS Services

Table 49 below lists known issues in SMS Services in previous releases.

Table 49 *Known Issues in SMS Services*

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.

Chapter 6

Upgrade Procedure

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 minimum of 1 GB (1024 MB) if system memory for a virtual machine, and 256 MB for the Web Application.

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

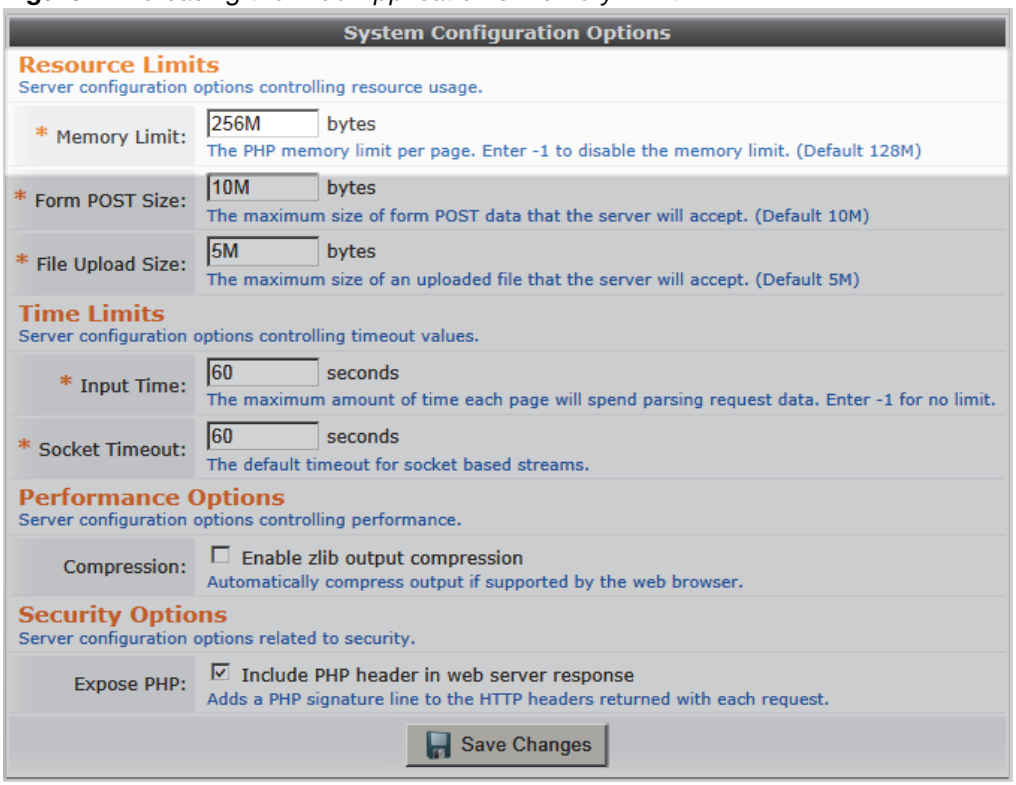
Ensure the following before performing an upgrade.

- Verify that the memory limit is set to at least 256M (see "Setting System Memory" on page 32).
- Back up your configuration (see "Configuration Backup" on page 32).
- If you are running a virtual machine, take a snapshot of it (see "Snapshot of the Virtual Machine" on page 33).

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*

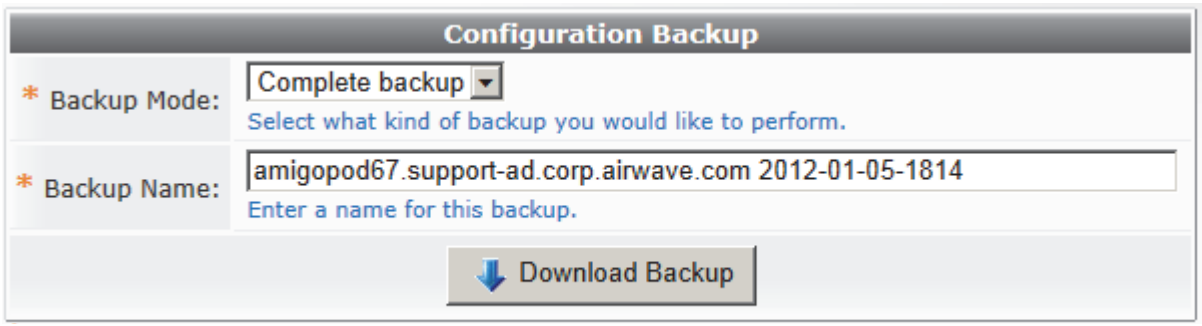


Configuration Backup

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 restoring is required.

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

Figure 2 *The Configuration Backup Dialog Prior to a System Update*



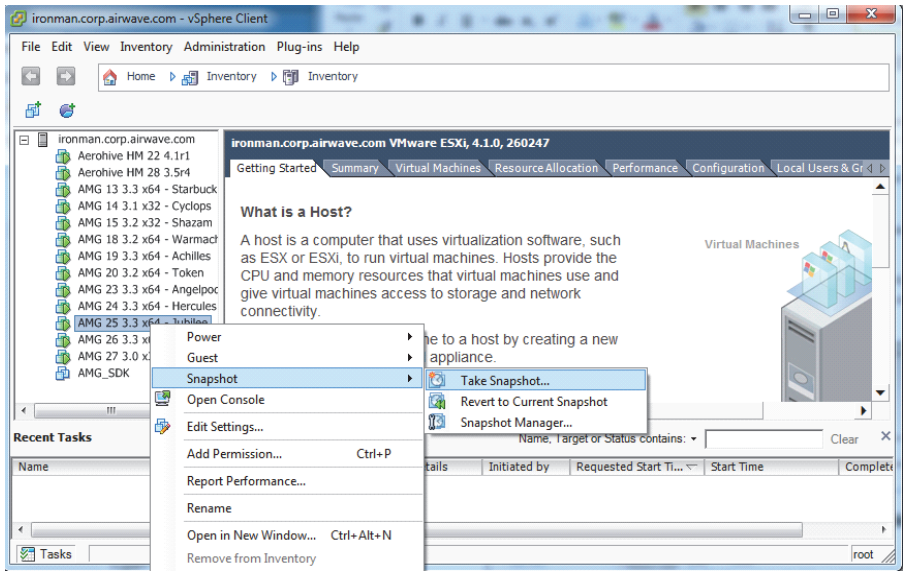
Snapshot of the Virtual Machine

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

NOTE

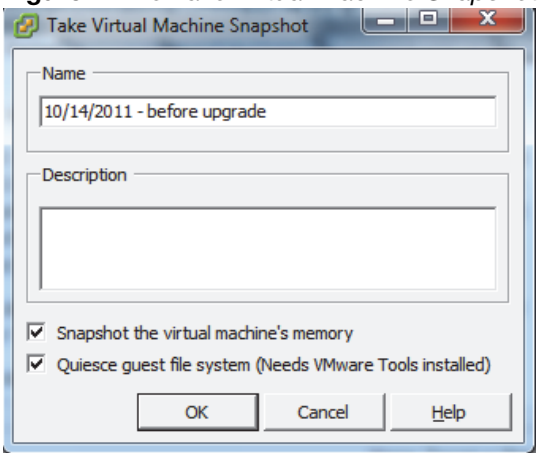
Select the “Quiesce guest file system (Needs VMware Tools installed)” option when taking a snapshot of the virtual machine (Figure 3). This ensures that the state of the file system is captured at a point in time where it is safe to do so.

Figure 3 *A Virtual Machine Snapshot Prior to Update*



Enter the name and date of this snapshot, then click **OK** (see Figure 4)

Figure 4 *The Take Virtual Machine Snapshot Dialog*



NOTE

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). When the kernel is installed, you can update the other plugins.

1. Verify that **Install Amigopod Kernel Update** is selected.
2. Click **Finish** to download and install the software upgrade.
3. Go to **Administrator > Plugin Manager > Update Plugins** again and check for any other plugin updates. Select your plugins and click **Finish**.
4. Restart your system services or reboot the server for your software upgrade to take effect.

NOTE

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 *The Add New Plugins Page*