


ClearPass 6.0 Common issues encountered during deployment



Technical Note

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®, RFPProtect®, 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. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site::

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

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

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



www.arubanetworks.com
1344 Crossman Avenue
Sunnyvale, California 94089
Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

1.	Preface:	4
2.	ClearPass 6.0 General Tips	5
3.	Joining ClearPass 6.0 to an AD domain	6
4.	CPPM 6.0 Authentication sources (AD/LDAP):	7
5.	ClearPass Guest 6.0: “/guest/” in URLs	8
6.	ClearPass Guest 6.0 Account Display: passwords are invisible	9
7.	ClearPass 6.0 Onboard: no certificate available	10
8.	ClearPass 6.0 Onboarding: common SSL issues	11
9.	ClearPass 6.0 Onboard: iOS certificate invalid error	12
10.	ClearPass Onboard: Certificate Retention/Revocation	13
11.	ClearPass 6.0 Onboard: whitelisting URLs	14
	Apple CNA:	14
	Kindle Fire CNA:	14
	Google Play (aka Android Market)	14
	Amazon Market	14
	ArubaOS netdestination config:	14

1. Preface:

This document contains some common issues and the resolutions for these issues that are often encountered during initial deployment of ClearPass 6.0 in a production environment. The target audiences are System Engineers/administrators who are deploying the ClearPass 6.0 Solution (Guest and/or Policy Manager) and have knowledge of AD/LDAP authentication infrastructure as well as an understanding of and experience with Public Key Infrastructure (PKI) concepts and implementation.

This technote is **NOT** intended to be a design reference or instruction guide and is only intended to provide quick reference for some issues commonly encountered while deploying the ClearPass 6.0 product.

2. ClearPass 6.0 General Tips

Here are some tips for avoiding common issues when deploying ClearPass.

- Make sure the system time is set correctly.
- Use NTP to avoid clock issues caused by clock drift or power outages.
- Exercise caution when integration systems operating in different time zones.
- Only the management IP address is required for operation of the ClearPass server. Use the secondary interface if out-of-band management is desired.
- Clear the cache on authentication servers when changing users (for example group membership).

3. Joining ClearPass 6.0 to an AD domain

Here are some tips when integrating ClearPass with Active Directory.

- Joining ClearPass 6.0 to an AD domain is only necessary when performing EAP-PEAP authentication.
- Ensure that all server clocks, (Including AD and ClearPass) are set correctly with preferred NTP synchronization.
- Ensure that the ClearPass DNS configuration is configured to send requests to the Active Directory server.
- Use the Fully Qualified Domain Name (FQDN) of a Domain Controller (using only the domain name or IP address are likely to fail).
- When entering the domain name during the join process, use the format: username@domain (DOMAIN\username will fail).
- The ClearPass join account requires privileges to add computers to the domain. Full domain administration rights will also work.
- The Active Directory account used to join the domain is not stored by ClearPass and may be **disabled** or even deleted once the join operation is completed.

4. CPPM 6.0 Authentication sources (AD/LDAP):

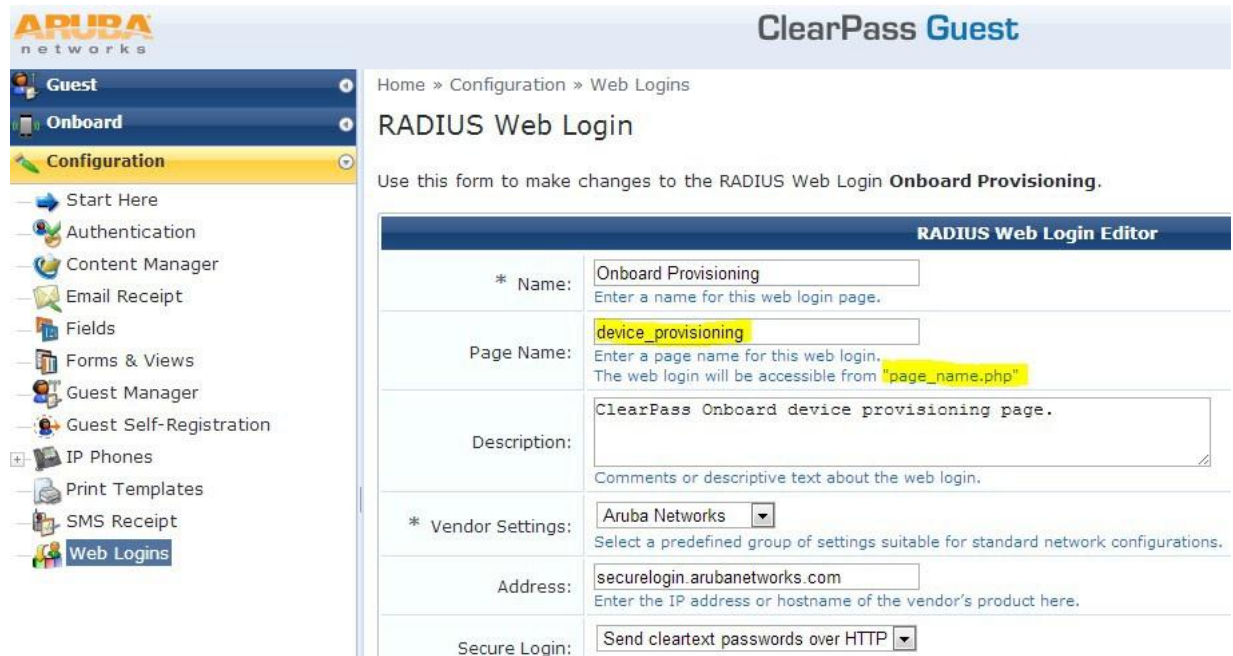
Here are some tips when using AD/LDAP as an authentication source.

- An AD/LDAP account is required for EAP-PEAP authentication, for group membership, and etc.
- The account used for ClearPass requires read rights to the folders/information you want to use in role mapping.
- The account used must also **remain active**, and should not be required to change or update its password regularly (setup as a service account).
- DO NOT use a regular user's account for production ClearPass deployments. Think of what happens when the original user leaves the organization and their account is deactivated. You should always use a dedicated service account for production ClearPass deployments!

5. ClearPass Guest 6.0: “/guest/” in URLs

With ClearPass Policy Manager (CPPM) v6.0, guest page URLs are preceded with /guest/. The page device provisioning is located at:

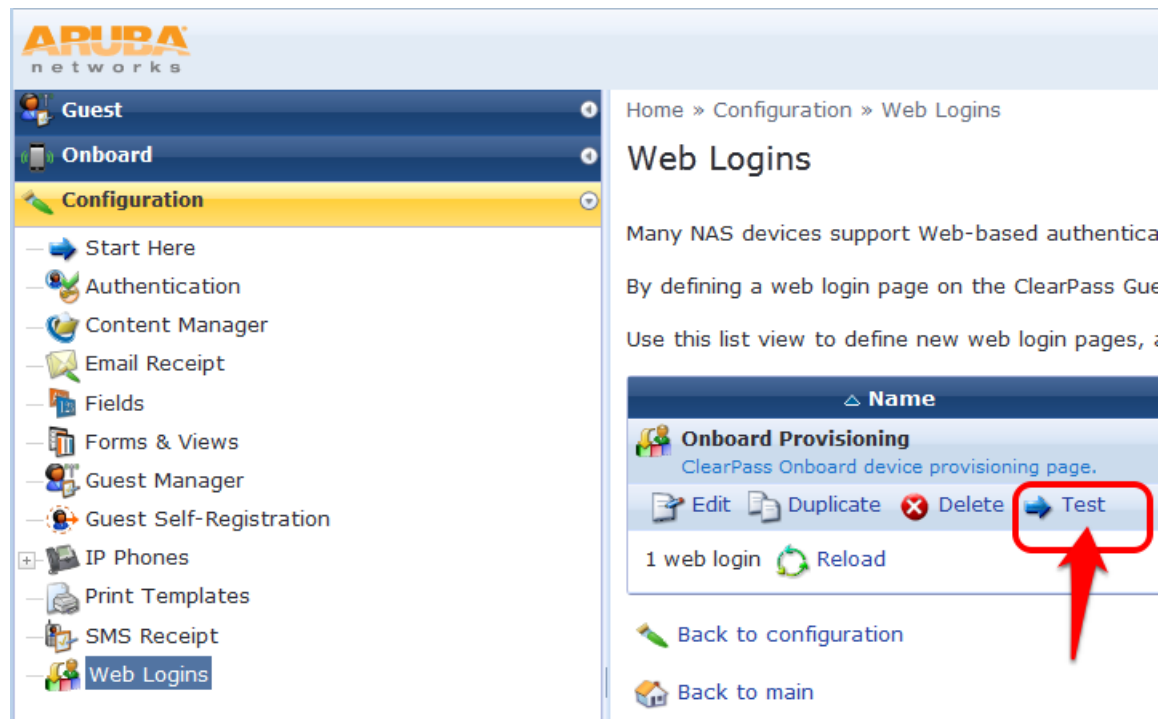
`https://<hostname>/guest/device_provisioning.php`



The screenshot shows the ClearPass Guest configuration interface. The left sidebar contains a navigation menu with options: Guest, Onboard, Configuration (selected), Start Here, Authentication, Content Manager, Email Receipt, Fields, Forms & Views, Guest Manager, Guest Self-Registration, IP Phones, Print Templates, SMS Receipt, and Web Logins. The main content area displays the breadcrumb path: Home » Configuration » Web Logins. Below this is the title "RADIUS Web Login" and a sub-header "RADIUS Web Login Editor". The form contains the following fields:

- Name:** Onboard Provisioning (with a note: "Enter a name for this web login page.")
- Page Name:** device_provisioning (with a note: "Enter a page name for this web login. The web login will be accessible from 'page_name.php'")
- Description:** ClearPass Onboard device provisioning page. (with a note: "Comments or descriptive text about the web login.")
- Vendor Settings:** Aruba Networks (with a note: "Select a predefined group of settings suitable for standard network configurations.")
- Address:** securelogin.arubanetworks.com (with a note: "Enter the IP address or hostname of the vendor's product here.")
- Secure Login:** Send cleartext passwords over HTTP

Use the **Test** feature to easily find to the correct URL.



The screenshot shows the ClearPass Guest configuration interface in list view. The left sidebar is the same as in the previous image. The main content area displays the breadcrumb path: Home » Configuration » Web Logins. Below this is the title "Web Logins" and a sub-header "Many NAS devices support Web-based authentication. By defining a web login page on the ClearPass Guest, you can use this list view to define new web login pages, etc." Below the sub-header is a table with the following columns and rows:

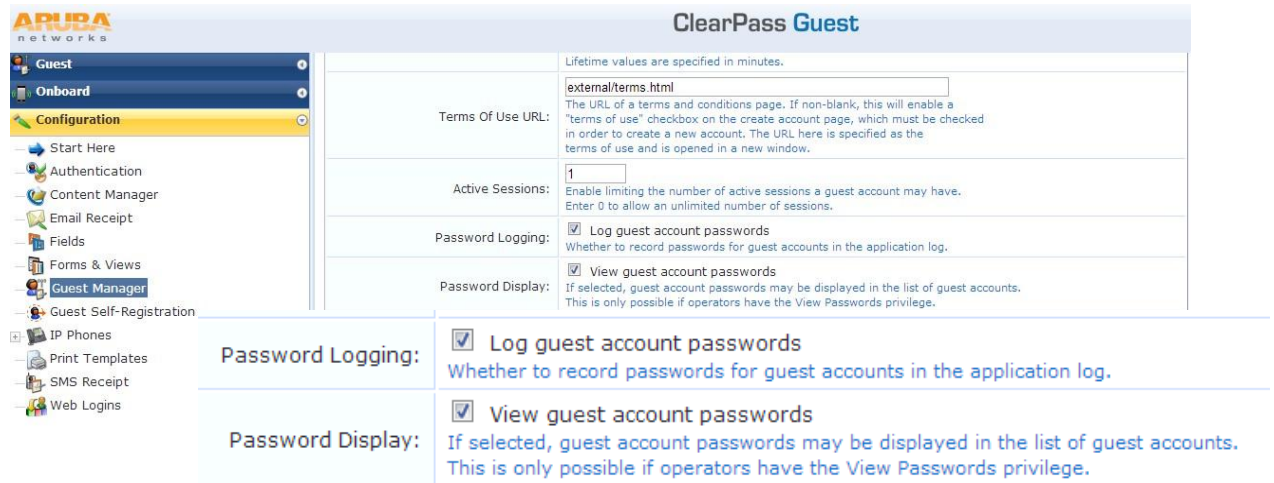
Name
Onboard Provisioning ClearPass Onboard device provisioning page.
Edit Duplicate Delete Test
1 web login Reload

At the bottom of the page, there are two buttons: "Back to configuration" and "Back to main". A red arrow points to the "Test" button in the table.

6. ClearPass Guest 6.0 Account Display: passwords are invisible

By default in ClearPass v6.0, guest passwords are only visible when initially created.

Previous behavior for displaying visible guest passwords in the list of guest accounts can be enabled in the ClearPass Guest configuration UI: **Configuration>Guest Manager>Password Display:**



The screenshot shows the ClearPass Guest configuration interface. On the left is a navigation menu with options like Guest, Onboard, Configuration, Start Here, Authentication, Content Manager, Email Receipt, Fields, Forms & Views, Guest Manager, Guest Self-Registration, IP Phones, Print Templates, SMS Receipt, and Web Logins. The main area is titled 'ClearPass Guest' and contains several configuration sections. A table below the main configuration area highlights two specific settings:

Password Logging:	<input checked="" type="checkbox"/> Log guest account passwords Whether to record passwords for guest accounts in the application log.
Password Display:	<input checked="" type="checkbox"/> View guest account passwords If selected, guest account passwords may be displayed in the list of guest accounts. This is only possible if operators have the View Passwords privilege.

7. ClearPass 6.0 Onboard: no certificate available

Switch back to HTTP! HTTPS will not work without a valid certificate!

You should also use HTTP when OnBoarding via IP (when no DNS is available).

The screenshot shows the Aruba ClearPass Guest configuration interface. The left sidebar contains navigation options: Guest, Onboard, Configuration (selected), Start Here, Authentication, Content Manager, Email Receipt, Fields, Forms & Views, Guest Manager, Guest Self-Registration, IP Phones, Print Templates, SMS Receipt, and Web Logins. The main content area is titled 'Authentication' and includes a breadcrumb trail: Home » Configuration » Authentication. Below the title is a description: 'Use this page to modify authentication settings for ClearPass Guest.' The 'Authentication Settings' form contains the following fields:

Authentication Settings	
Dynamic Authorization:	<input checked="" type="checkbox"/> Send a disconnect/re-authorization message to the NAS Global to automatically send disconnects when enabled/role values change. Requires a NAS Type supporting RFC-3576.
NAS Type:	Aruba Networks (RFC 3576 support) [v] Select the default type for network access servers.
RFC-3576 Bind Address:	0.0.0.0 Force a specific bind address for RFC-3576 requests. This may be needed in an AirGroup environment.
* Internal Auth Type:	PAP [v] Controls the RADIUS authentication type used for internal RADIUS authentication requests.
Security:	<input checked="" type="checkbox"/> Require HTTPS for guest access [red arrow] If checked, HTTP access by guests will be redirected to use HTTPS instead.

At the bottom of the form is a 'Save Changes' button. Below the form, there is a legend: '* required field', a green arrow icon labeled 'Back to configuration', and a house icon labeled 'Back to main'.

8. ClearPass 6.0 Onboarding: common SSL issues

- If you enable HTTPS, you are required to have a valid DNS entry, resolvable from the Onboarding device
- Onboarding via HTTPS via IP address will fail because a trusted certificate can no longer be issued for an IP address.
- Use NTP so that you do not have any server failures based on timing discrepancies caused by clock drift or other timing issues.
- In the Onboard configuration, make sure you Configure Minimum Data retention of certificates to Zero, so that they can be deleted. Otherwise the delete button will not be visible.
- Use the following command on ArubaOS CLI:
`aaa user delete or CoA` to reset a running connection.

9. ClearPass 6.0 Onboard: iOS certificate invalid error

Onboarding on iOS will fail if the server certificate does not contain all intermediates to the CA root. Windows may work because of cert caching but may also experience issues if intermediate certificates are missing.

Check that the intermediate certificate is visible with the server certificate:

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar contains navigation options like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Administration > Certificates > Server Certificate'. A dropdown menu shows 'Select Server: 192.168.32.16'. Below this, there are two certificate sections. The first is 'Server Certificate' with details: Subject: EMAILADDRESS=postmaster@arubalab.com, CN=clearpass.nl.arubalab.com, C=NL, OID.2.5.4.13=7g7w91XlQJxKVDA; Issued by: CN=StartCom Class 1 Primary Intermediate Server CA, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL; Issue Date: Nov 13, 2012 02:39:16 CET; Expiry Date: Nov 14, 2013 05:02:28 CET; Validity Status: Valid. The second section is 'Intermediate CA Certificate', which is highlighted with a red arrow. Its details are: Subject: CN=StartCom Class 1 Primary Intermediate Server CA, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL; Issued by: CN=StartCom Certification Authority, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL; Issue Date: Oct 24, 2007 22:54:17 CEST; Expiry Date: Oct 24, 2017 22:54:17 CEST; Validity Status: Valid. On the right side, there are buttons for 'Create Self-Signed Certificate', 'Create Certificate Signing Request', 'Import Server Certificate', and 'Export Server Certificate'.

If intermediate certificates are not visible in the UI, then in

the certificate file, before importing, concatenate the

following two together (see example below):

- server-cert
- intermediate

```
-----BEGIN CERTIFICATE-----
MIIGbDCCBVsgAwIBAgIDCAz4MA0GCSqGSIb3DQEBBQUAMIGMMQswCOYDVQQGEwJJ
TDEWMBQGA1UEChMNU3RhcncRDb20gTHRkLjErMCKGA1UECXMtU2VjdXJlIERpZ210
YWwgQ2VydG1maWNhdG1vbiBBdXR0b20gTHRkLjErMCKGA1UECXMtU2VjdXJlIERpZ210
MSBQcm1tYXJ5IElucyBkaW50b20gTHRkLjErMCKGA1UECXMtU2VydG1maWNhdG1vbiBBdXR0b20gTHRkLjErMCKGA1UECXMtU2VjdXJlIERpZ210
fr3fRSRG7xkHC+kLoybaq1qt29DVPgGqCwj4HAsjFvt5wORHGqDp3hms5qwKimHnX
yK8RmG9yK/p0Acq/eB446+KzKF6lKzD2/H6CQ/ySOsoF9slzVqFlv+C5Euyg/Sxh
izH+T65B14YSbYspMrsB9Q==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGNDCCBBygAwIBAgIBGDANBgkqhkiG9w0BAQUFADB9MQswCOYDVQQGEwJJTDEW
MBQGA1UEChMNU3RhcncRDb20gTHRkLjErMCKGA1UECXMtU2VjdXJlIERpZ210YWwg
Q2VydG1maWNhdG1vbiBBdXR0b20gTHRkLjErMCKGA1UECXMtU2VjdXJlIERpZ210
dG1vbiBBdXR0b20gTHRkLjErMCKGA1UECXMtU2VjdXJlIERpZ210YWwgQ2VydG1maWNh
SRXNiTE8kMByIzVLojwRRHfLd1zORgWMIIMEXANERK2wNRBd1o640ucQP12Eg7PD
wuTSxv0JS3QJ3fGz0zk+gA2iCxnw00fFwq/iI9th4plcbiCJSS4jarJiwUW0n6+L
p/EiO/h94pDQehn7Skzj0n1fSoMD7SfWI55rjbrZotnviIip3XUZPD9MEI3vu3Un
0q6Dp6jOW6c=
-----END CERTIFICATE-----
```

10. ClearPass Onboard: Certificate Retention/Revocation

The delete certificate button is **invisible by design!**

Home » Onboard » Certificate Management

Certificate Management

Use this list view to manage certificates.

- Upload a certificate signature
- Generate a new certificate
- Upload a code-signing certificate

Common Name	Serial Number	Type	Valid From	Valid To	Device Type
clearpass.nl.arubalab.com	0x00a3bf6956f190b1d9	trusted	2012-11-12 16:41:22+00	2013-11-12 16:41:22+00	None
ClearPass Onboard Local Certificate Authority	1	ca	2012-11-12 16:40:50+00	2022-11-13 17:10:50+00	None
ClearPass Onboard Local Certificate Authority (Signing)	2	ca	2012-11-12 16:40:50+00	2022-11-13 17:10:50+00	None
Device Enrollment (Profile Signing)	3	profile-signing	2012-11-12 16:40:50+00	2022-11-13 17:10:50+00	None
ronald	5	tls-client	2012-11-25 20:53:41+00	2013-11-25 21:23:41+00	iOS
StartCom Class 1 Primary Intermediate Server CA	24	trusted	2007-10-2		

Actions for row 5: View certificate, Export certificate, Revoke certificate, **Delete certificate**

When testing, set the minimum period for Onboard to zero weeks to allow immediate removal.

ARUBA networks ClearPass Guest

Home » Administration » Data Retention

Data Retention Policy

Use this form to control how long data should be retained by the system.

Manage Data Retention

- * Enable: Enable data retention policy
If enabled, records will be deleted after the period set below.
- Time of Day: 3 : 0
Select the time of day at which data retention will run.
- Onboard Device Certificates**
 - Minimum Period: 0 weeks
The minimum delay required before an expired certificate (or a rejected request) can be deleted. Leave blank to allow certificates and requests to be deleted at any time, including before expiration.
 - Maximum Period: 52 weeks

Onboard Device Certificates

- Minimum Period: 0 weeks
The minimum delay required before an expired certificate (or a rejected request) can be deleted. Leave blank to allow certificates and requests to be deleted at any time, including before expiration.

11. ClearPass 6.0 Onboard: whitelisting URLs

Here are some example URLs that commonly need to be whitelisted for Onboarding to succeed as they are accessed by the client device as part of network setup/detection by the Captive Network Assistant (CNA).

Apple CNA:

- <http://www.apple.com/library/test/success.html>

Kindle Fire CNA:

- <http://spectrum.s3.amazonaws.com/kindle-wifi/wifistub.html>

Google Play (aka Android Market)

- android.clients.google.com - google play access
- [.ggpht.com](http://ggpht.com) - download app from google play store

Amazon Market

- amzdigitaldownloads.edgesuite.net

ArubaOS netdestination config:

```
netdestination onboard-whitelist
  name www.apple.com
  name android.clients.google.com
  name .ggpht.com
!
aaa authentication captive-portal "WLAN_WPA2_onboard"
  login-page "http://<server>/device_provisioning.php"
  white-list "onboard-whitelist"
  white-list "ocsp.comodoca.com"
  white-list "ocsp.startssl.com"
!
```

NOTE! Don't forget to whitelist the Online Certificate Status Protocol (OCSP) servers used in your certificate otherwise certificate validation will fail!