Release Notes – Maintenance

OmniAccess AP1101

Release 2.1.0.100

The following is a list of issues that have been identified and corrected in this AOS-WNG software release. This document is intended to be used as a pre-upgrade guide and does not replace the GA Release Notes which are created for every GA release of software.

Alcatel-Lucent Enterprise

Contents

Fixed Problem Reports Between Builds 92 and 100

The following issues were fixed between AOS-WNG Release 2.1.0.92 and 2.1.0.100.

PR	Description
R21ISSUE-32	**Summary:** Rogue AP "Black List" does not have SSID information. How do we detect a rogue? **Explanation:** The SSID field has been added to the "Black List" of Rouge AP.

Fixed Problem Reports Between Builds 83 and 91

The following issues were fixed between AOS-WNG Release 2.1.0.83 and 2.1.0.91.

PR	Description
R21ISSUE-7	**Summary:** Redefine the priorities of log messages. **Explanation:** Improvements to syslog capability to provide filtering of messages sent to syslog based on priority levels.
R21ISSUE-12	**Summary:** "support" user needs ability to change password. **Explanation:** The AP supports a “support” account for troubleshooting purposes in CLI. If a user logs into the AP with the support account, he now has the ability to change the “support” account password.
R21ISSUE-13	**Summary:** Country code list for time zone setting needs to be updated. Eg. Malta/Sweden not available. **Explanation:** Additional country codes added: Belgium – BE; United Kingdom – GB; Guam – GU; Hungary – HU; Ireland – IE; Monaco – MC; Macedonia – MK; Malta – MT; Malaysia – MY; Nigeria – NG; Panama – PA; Russia – RU; Sweden – SE; Thailand – TH; Turkey – TR; Vietnam - VN
R21ISSUE-29	**Summary:** Captive Portal customization should allow JPG format. **Explanation:** JPG format is now supported. Additional sizing and dimension enhancements added.
R21ISSUE-30	**Summary:** (Accidently) Hitting the "backspace" key outside of a text-field will redirect the administrator to the login page of the AP management (login page). **Explanation:** Pressing the “backspace” key outside of a text field no longer redirects to the login page.

R2ISSUE-54	**Summary:** Add the option for SVC to take over as PVC. **Explanation:** Option added to have SVC takeover as PVC.
R21ISSUE-55	**Summary:** In the "Monitoring" pane, show the AP name instead of the MAC address. **Explanation:** "Monitoring" pane displays the AP name.

Fixed Problem Reports Between Builds 79 and 82

The following issues were fixed between AOS-WNG Release 2.1.0.79 and 2.1.0.82.

PR	Description
R21ISSUE-15	**Summary:** Max length of email field in local user creation screen is too short (30 characters). **Explanation:** It has been increased to 64 characters.
R21ISSUE-16	**Summary:** Max length of first & last name is too short in local user creation screen (10 characters). **Explanation:** It has been increased to 35 characters each (according to US Government standards).
R21ISSUE-17	**Summary:** Captive Portal restrictions: 1) Special characters are not allowed in passwords 2) Last name does not allow hyphens or spaces 3) First name does not allow spaces or hyphens 4) Company name does not allow spaces and is limited to 30 characters **Explanation:** 1) Special characters are allowed for captive portal users passwords 2) First names like Jean-Claude and last names e.g. Le-Fleur are allowed. 3) Spaces are allowed for last names, e.g. "John Doe" 4) Company name is allowed 64 characters and spaces. e.g. "Alcatel-Lucent Enterprise Corporation, Argentina".
R21ISSUE-46 R21ISSUE-47	**Summary:** WLAN changes security mode from Enterprise (WPA) to OPEN on its own. **Explanation**: Neither encrypt nor decrypt an empty password to keep the same value of password, avoid creating wrong type of WLAN.

Open Problem Reports and Known Issues

The following issues are identified in AOS-WNG 2.1.0.100 Release.

PR	Description	Workaround
	Microsoft Internet Explorer does not support https login with IP address like 'https: //192.168.20.100', it only support login with the URL 'https: //mywifi.al-enterprise.com'.	Recommend to use Google Chrome and Mozilla Firefox for https management.

New Features Introduced - 2.1.0.100

The following new features were introduced.

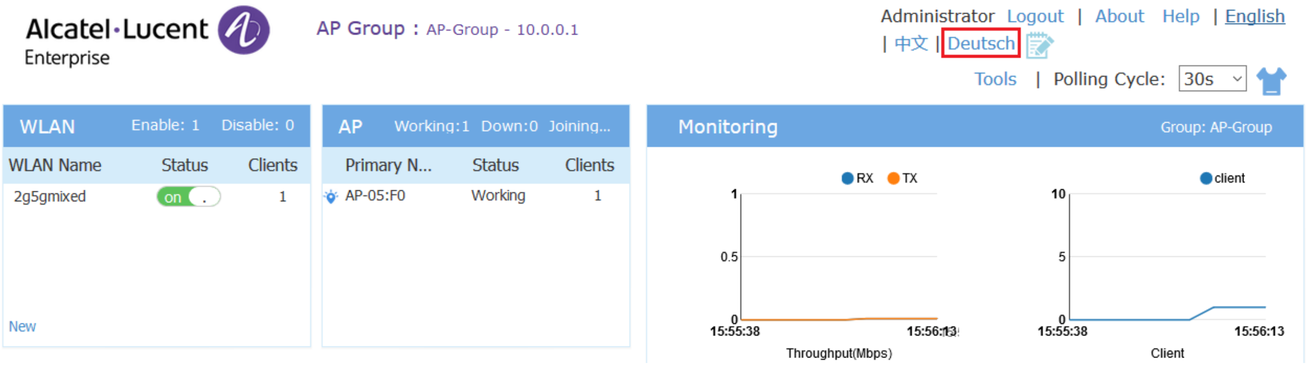
1. HTTPS Support

Web pages now support HTTPS. By importing a root certificate, users can login without any untrusted warning and all communication is protected.
First steps to begin using HTTPS:
1) Download the root certificate file from the AP;
2) Install the certificate for the web browser according to operating system;
3) Login with HTTPS to manage the AP group.

Usage Guidelines:
1) Google Chrome and Mozilla Firefox are recommended for the HTTPS management. Microsoft Internet Explorer is NOT recommended for use because it does not support HTTPS login through IP address, however HTTPS access via a URL is supported.
2) If an AP in the group is reset to the factory default, it is highly recommended to close and reopen the browser for rebuilding the HTTPS connection between the AP and the browser.

2. German Language Support

German is supported for web management, user can switch to German by selecting ‘Deutsch’ in the main page.


Alcatel·Lucent Enterprise
AP Group : AP-Group - 10.0.0.1
Administrator Logout | About Help | English
| 中文 | Deutsch
Tools | Polling Cycle: 30s
WLAN Enable: 1 Disable: 0
AP Working:1 Down:0 Joining...
Monitoring Group: AP-Group
New
RX TX
1
0.5
0
15:55:38
15:56:13
Throughput(Mbps)
client
10
5
0
15:55:38
15:56:13
Client

WLAN Name	Status	Clients
2g5gmixed	on	1

Primary N...	Status	Clients
AP-05:F0	Working	1

New Features Introduced - 2.1.0.91

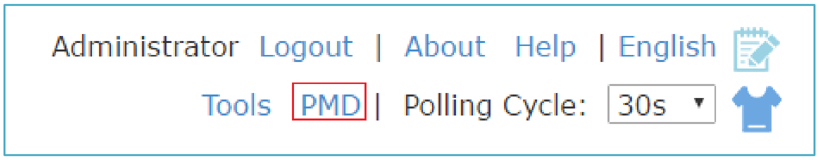
The following new features were introduced.

1. Post Morten Dump - PMD

Post Mortem Dump (PMD) is a troubleshooting method which helps to identify root cause of a core dump and exception pointers after a fatal crash. If PMD is enabled and configured, the AP will send PMD files to a specific TFTP server immediately when there is a key process crashing on the AP.

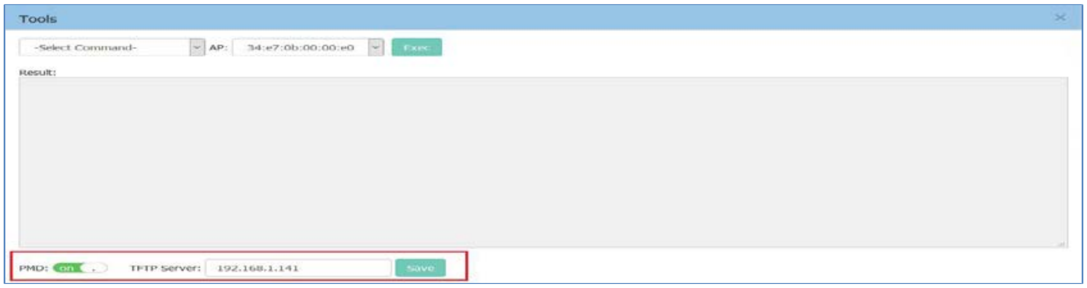
Web UI Usage:

1) Click the Tools link in the main page


Administrator Logout | About Help | English
Tools PMD | Polling Cycle: 30s

Tools link

2) Configure PMD



AP: 34:e7:0b:00:00:e0

PMD: on

TFTP Server: 192.168.1.141

PMD Configuration Window

Table: Key word specification in PMD Window

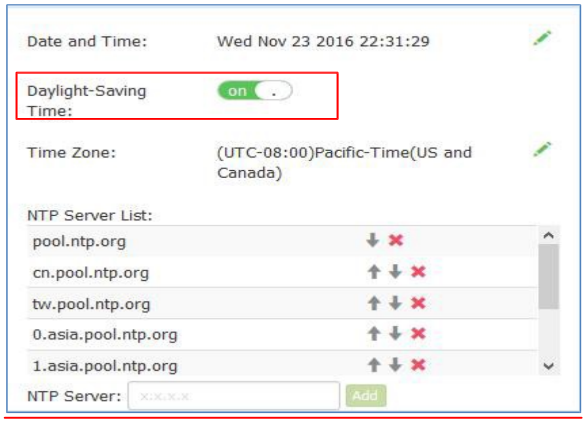
PMD: on	Enable/Disable PMD files sending.
TFTP Server	Specify the TFTP server to which PMD files will be sent.

Usage Guidelines:

1) By default, sending PMD files to an external TFTP server is disabled.
2) The PMD file name gives the application that crashed. For example a PMD file named “pmd-led_ctrl-2016.11.20-16:57:45”, “led_ctrl” is the application crashed.
3) PMD files are coding level information, it is suggested to send them to service & support for analysis.

2. Daylight Saving Time

An option has been added to enable/disable daylight saving time on the System main page.



Date and Time: Wed Nov 23 2016 22:31:29

Daylight-Saving Time: on

Time Zone: (UTC-08:00)Pacific-Time(US and Canada)

NTP Server List:

pool.ntp.org
cn.pool.ntp.org
tw.pool.ntp.org
0.asia.pool.ntp.org
1.asia.pool.ntp.org

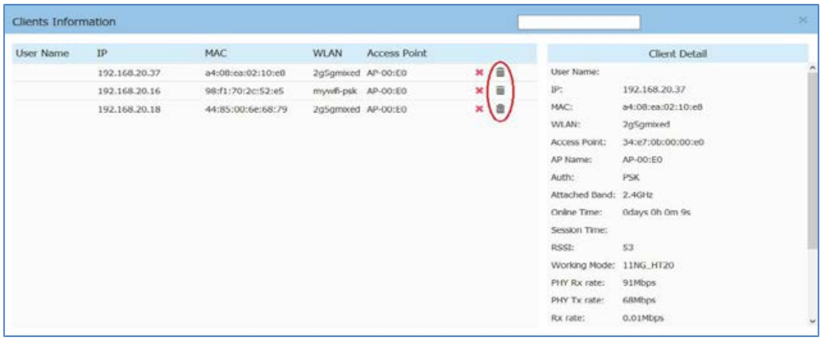
Daylight-Saving Time

The daylight saving time (DST) varies from different time zones. The DST of supporting time zones is enabled automatically by default, while other time zones are not editable on DST.

3. Disconnect a client from the wireless network

Previously there was no method to force a user or device disconnection without having to put that user or device in the Black List. This resulted in that user or device never being able to connect again until the administrator manually removed it from the Black List. An option to easily disconnect a user or device has been added.

Click the Client bar in the main page to enter the Clients Information Window.



Clients Information

User Name	IP	MAC	WLAN	Access Point	
	192.168.20.37	a4:08:ea:02:10:e8	2g5gmixed	AP-00:E0	✖ 🗑
	192.168.20.16	98:f1:70:2c:52:e5	mywifi-psk	AP-00:E0	✖ 🗑
	192.168.20.18	44:85:00:6e:68:79	2g5gmixed	AP-00:E0	✖ 🗑

Client Detail	
User Name:	
IP:	192.168.20.37
MAC:	a4:08:ea:02:10:e8
WLAN:	2g5gmixed
Access Point:	34:e7:0b:00:00:e0
AP Name:	AP-00:E0
Auth:	PSK
Attached Band:	2.4GHz
Online Time:	0days 0h 0m 9s
Session Time:	
RSSI:	53
Working Mode:	11NG_HT20
PHY Rx rate:	91Mbps
PHY Tx rate:	68Mbps
Rx rate:	0.01Mbps

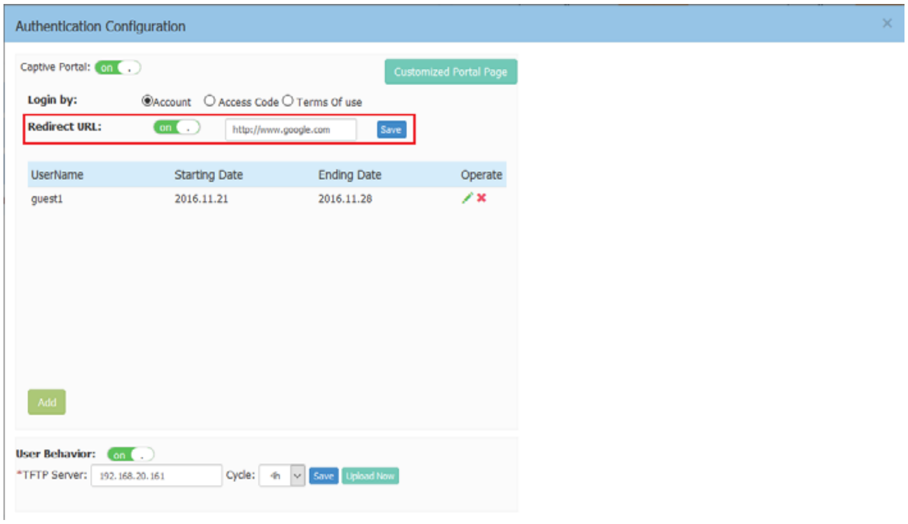
Disconnect a Client

4. Redirect to ADMIN-specified page after successful login

Administrator can specify the web page after successfully logging in.

Go to Access in the main page and click to open the Authentication Configuration Window.

The administrator can enable the URL redirect function and specify the redirect page in the Authentication Configuration Window.



Authentication Configuration

Captive Portal: on

Login by: ● Account ○ Access Code ○ Terms Of use

Redirect URL: on http://www.google.com Save

UserName	Starting Date	Ending Date	Operate
guest1	2016.11.21	2016.11.28	✎ ✖

User Behavior: on

*TFTP Server: 192.168.20.161 Cycle: 4h Save Upload Now

Redirect to ADMIN-specified URL

New Features Introduced - 2.1.0.82

The following new features were introduced.

1. Post Mortem Dump - PMD

Post Mortem Dump (PMD) is a troubleshooting method which helps to identify root cause of a core dump and exception pointers after a fatal crash. If PMD is enabled and configured, the AP will send PMD files to a specific TFTP server immediately when there is a key process crashing on the AP.

Web UI Usage:

3) Click the PMD link in the main page

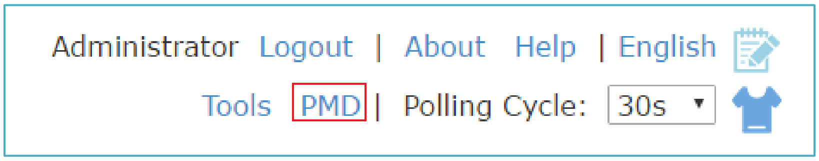
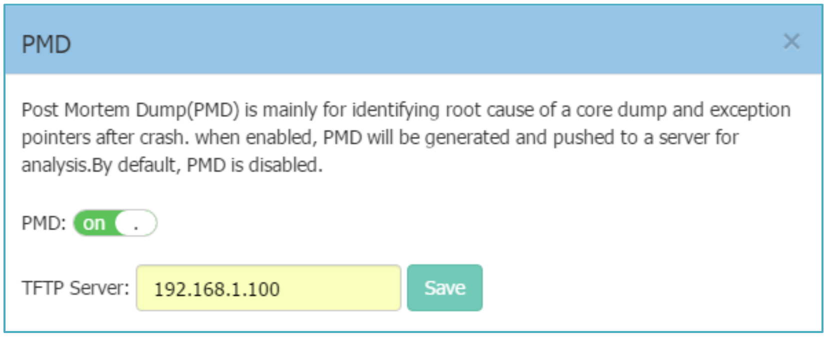


Figure 1 PMD link

4) Configure PMD



Post Mortem Dump(PMD) is mainly for identifying root cause of a core dump and exception pointers after crash. when enabled, PMD will be generated and pushed to a server for analysis.By default, PMD is disabled.

PMD: on

TFTP Server: 192.168.1.100

Figure 2 PMD Configuration Window

Table: Key word specification in PMD Window

PMD: on	Enable/Disable PMD files sending.
TFTP Server	Specify the TFTP server to which PMD files will be sent.

Usage Guidelines:

4) By default, sending PMD files to an external TFTP server is disabled.
5) The PMD file name gives the application that crashed. For example a PMD file named “led_ctrl.11. core”, “led_ctrl” is the application crashed.
6) PMD files are coding level information, it is suggested to send them to service & support for analysis.

Note: PMD file naming format is planned to be changed to “pmd-process name-date-time”, such as “pmd-led_ctrl-2016.11.20-16:57:45” in the next release.

2. Guest Operator Account Privileges

Added a new web GUI for the guest operator account that only allows for the creation and deletion of guest users for the AP.

3. Syslog Error Messages

To reduce the many error level syslog messages after configuring or modifying a VLAN ID, the log messages of the WAM module have been downgraded to Debug level.

Technical Support

Alcatel-Lucent technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	1-800-995-2696
Latin America	+1-877-919-9526
European Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email : ebg_global_supportcenter@alcatel-lucent.com

Internet: Customers with service agreements may open cases 24 hours a day via the support web page at: support.esd.alcatel-lucent.com.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1 - Production network is down resulting in critical impact on business—no workaround available.

Severity 2 - Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 - Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 Information or assistance on product feature, functionality, configuration, or installation.

Appendix A: Upgrade Instructions

Passwords related to the operation of the OAW-AP1101 are not stored securely in software version 2.1.0.67. To resolve this issue the OAW-AP1101 software MUST be upgraded to the latest software version available from customer support. Please Visit https://support.esd.alcatel-lucent.com/ to get the latest software and follow the upgrade instructions below.

The two cases below describe the Syslog messages that will be seen when an AP running software version 2.1.0.67 is detected in a group with another AP running software version 2.1.0.68 or higher.

- Case1: In a group, AP-00:e0 is acting as the PVC running software version 2.1.0.68 or higher; AP-05:30 running software version 2.1.0.67 is detected in the group:

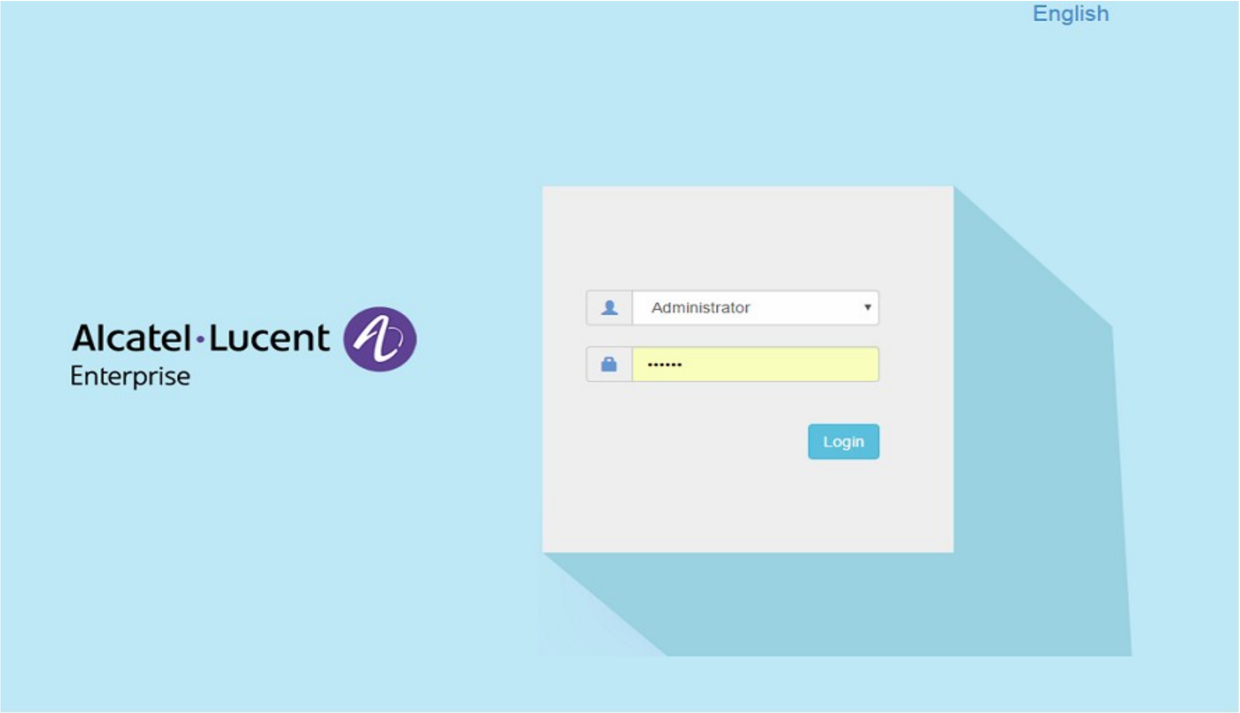
  PVC generates an Error level log message: "AP-05:30 with incompatible software is trying to join the group, please upgrade it!"

- Case2: In a group, AP-05:30 is acting as the PVC running software version 2.1.0.67; AP-00:e0 running software version 2.1.0.68 or higher is detected in the group:

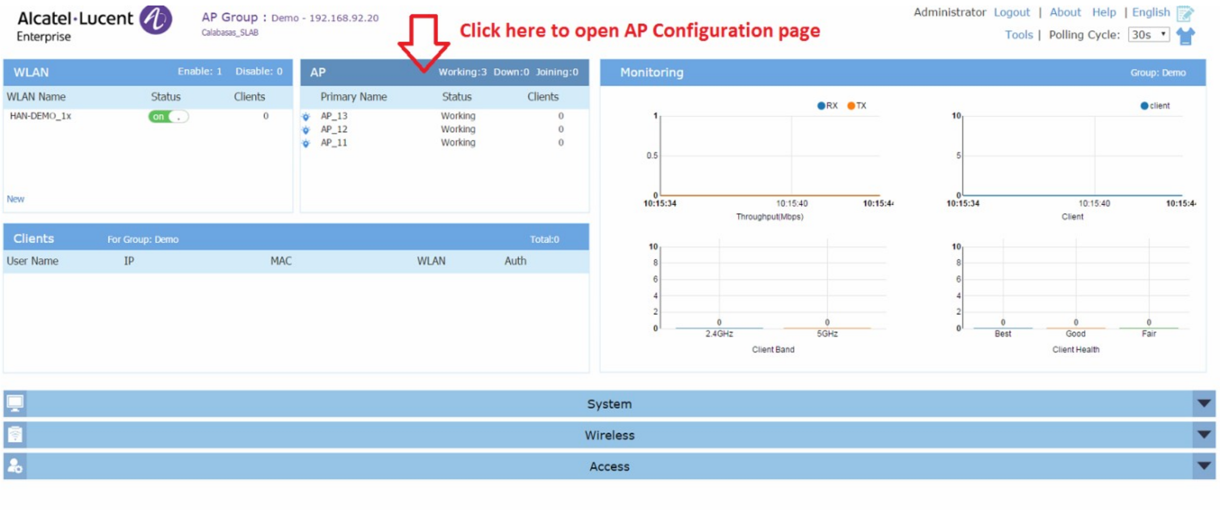
  AP-00:e0 generates a Critical level log message: "Some APs in the network are running incompatible software. To avoid network interruptions, an upgrade to the latest software is strongly recommended!".

Software Upgrade Instructions

1. Login to AP using Administrator account with default password 'admin'.



2. Click on the AP tab to open up the AP Configuration page.



Click here to open AP Configuration page

WLAN Enable: 1 Disable: 0

WLAN Name	Status	Clients
HAN-DEMO_1x	on	0

New

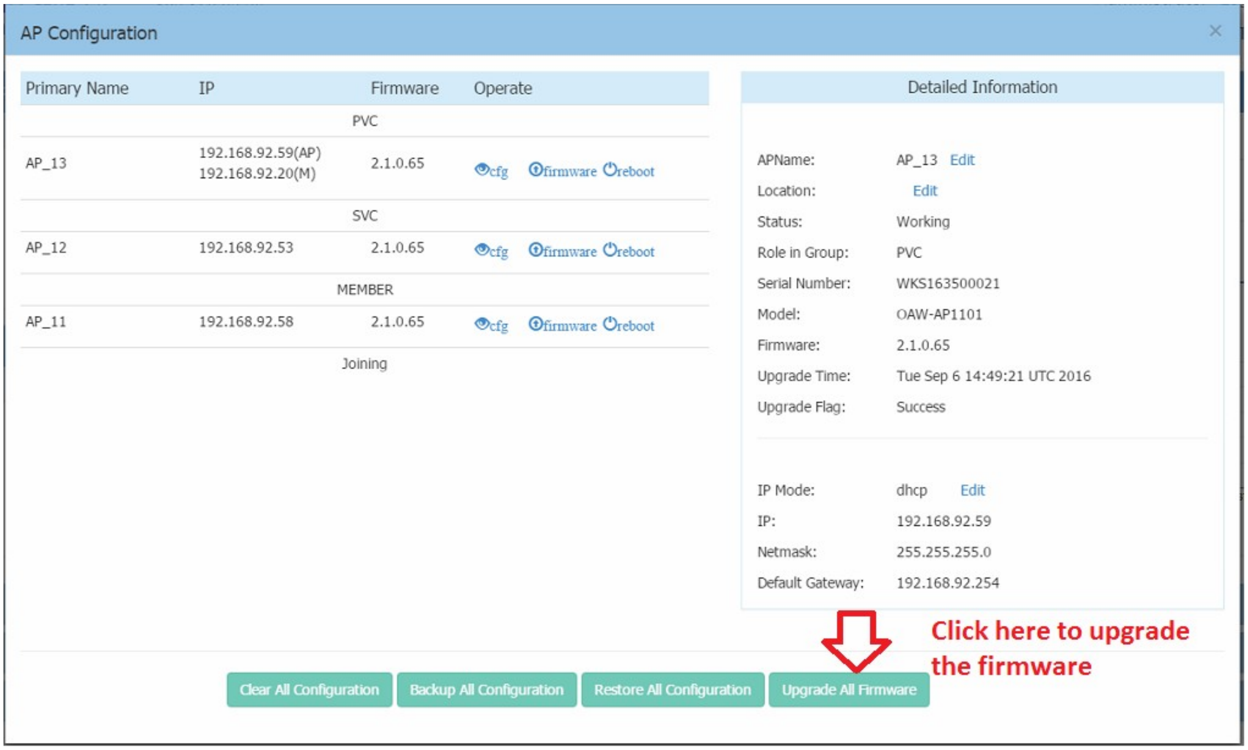
AP Working:3 Down:0 Joining:0

Primary Name	Status	Clients
AP_13	Working	0
AP_12	Working	0
AP_11	Working	0

Clients For Group: Demo Total:0

User Name	IP	MAC	WLAN	Auth

3. On AP Configuration Page, click **Upgrade All Firmware.**



AP Configuration

Primary Name	IP	Firmware	Operate
		PVC	

AP_13	192.168.92.59(AP)
	192.168.92.20(M)
		2.1.0.65	cfg firmware reboot

		SVC	
AP_12	192.168.92.53	2.1.0.65	cfg firmware reboot
		MEMBER	
AP_11	192.168.92.58	2.1.0.65	cfg firmware reboot
		Joining	

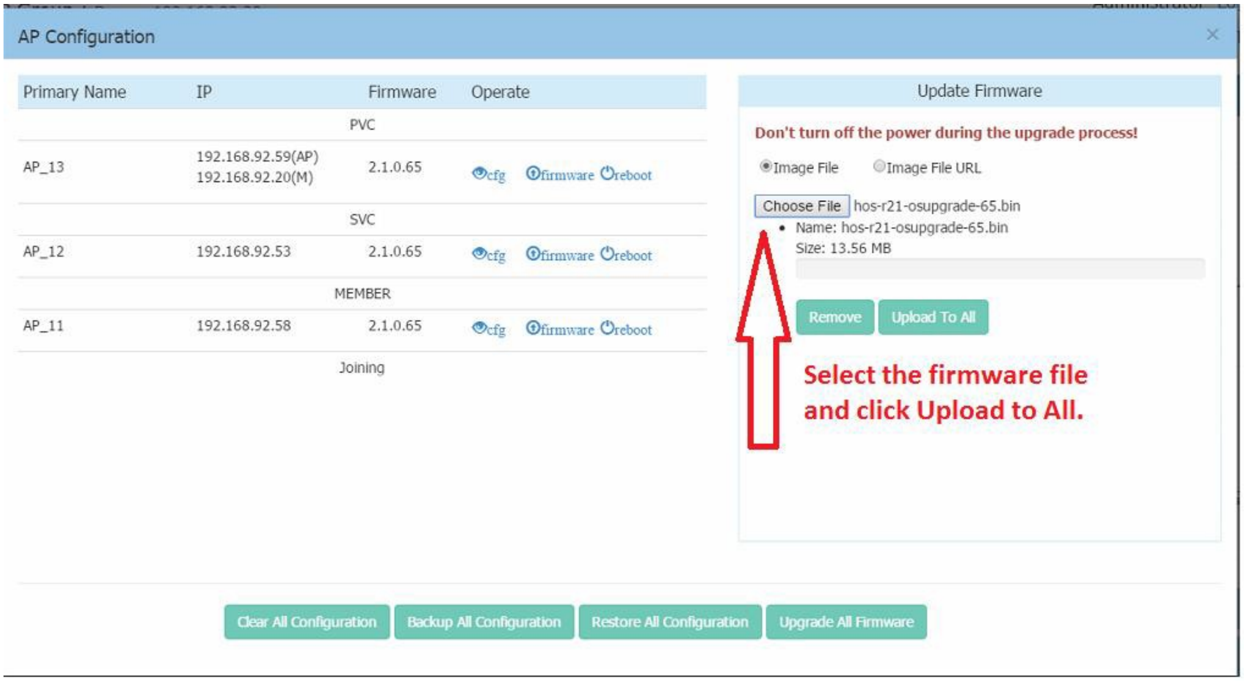
Detailed Information

APName: AP_13 Edit
Location: Edit
Status: Working
Role in Group: PVC
Serial Number: WKS163500021
Model: OAW-AP1101
Firmware: 2.1.0.65
Upgrade Time: Tue Sep 6 14:49:21 UTC 2016
Upgrade Flag: Success

IP Mode: dhcp Edit
IP: 192.168.92.59
Netmask: 255.255.255.0
Default Gateway: 192.168.92.254

Click here to upgrade the firmware

4. Select the firmware file and click **Upload To All**, this will upgrade the firmware and reboot the AP.



AP Configuration

Primary Name	IP	Firmware	Operate
		PVC	

AP_13	192.168.92.59(AP)
	192.168.92.20(M)
		2.1.0.65	cfg firmware reboot

		SVC	
AP_12	192.168.92.53	2.1.0.65	cfg firmware reboot
		MEMBER	
AP_11	192.168.92.58	2.1.0.65	cfg firmware reboot
		Joining	

Update Firmware

Don't turn off the power during the upgrade process!

● Image File ○ Image File URL

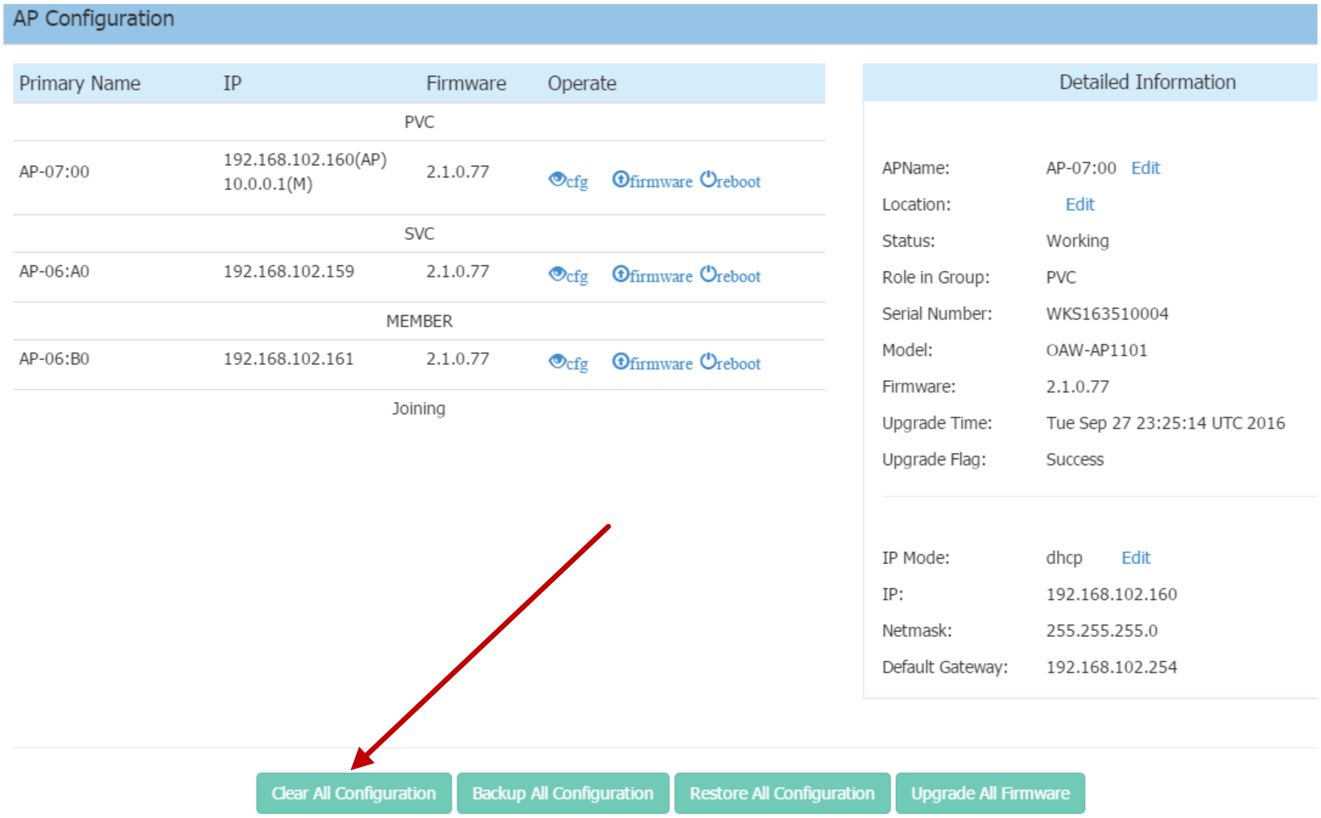
Choose File hos-r21-osupgrade-65.bin

- Name: hos-r21-osupgrade-65.bin

Size: 13.56 MB

Select the firmware file and click Upload to All.

5. Log into the AP group and clear the configuration by clicking **Clear All Configuration** and confirm the reboot. **NOTE**: This step erases the configuration for all the APs in the group. It is only MANDATORY when upgrading an AP from software version 2.1.0.67 to a higher version.



AP Configuration

Primary Name	IP	Firmware	Operate
		PVC	

AP-07:00	192.168.102.160(AP)
	10.0.0.1(M)
		2.1.0.77	cfg firmware reboot

		SVC	
AP-06:A0	192.168.102.159	2.1.0.77	cfg firmware reboot
		MEMBER	
AP-06:B0	192.168.102.161	2.1.0.77	cfg firmware reboot
		Joining	

Detailed Information

APName:	AP-07:00 Edit
Location:	Edit
Status:	Working
Role in Group:	PVC
Serial Number:	WKS163510004
Model:	OAW-AP1101
Firmware:	2.1.0.77
Upgrade Time:	Tue Sep 27 23:25:14 UTC 2016
Upgrade Flag:	Success
IP Mode:	dhcp Edit
IP:	192.168.102.160
Netmask:	255.255.255.0
Default Gateway:	192.168.102.254

Additional Upgrade Information for APs with software version 2.1.0.67

When adding an AP(s) with software version 2.1.0.67 to an existing group of APs with a software version higher than 2.1.0.67, the APs with software version 2.1.0.67 must be upgraded and the configuration cleared.

There are two scenarios for adding APs to an existing AP group:

A) The existing group has a minimal configuration which can be easily cleared and reconfigured. In this case perform the following steps:
   1) Add the new APs to the group.
   2) Upgrade the APs to the newer software version.
   3) Clear the configuration and reboot as described earlier.

B) The existing group has an extensive configuration that needs to be preserved. In this case, there are 2 options.

   Option 1:

   1) Backup the existing configuration.
   2) Add the new APs to the group.
   3) Upgrade the APs to the newer software version.
   4) Clear the configuration and reboot as described earlier.
   5) Restore the configuration.

   Option 2:

   1) Use an isolated network, not connected to the existing AP's network.
   2) Power up the APs and allow them to form their own group.
   3) Upgrade the APs to the newer software version.
   4) Clear the configuration and reboot as described earlier.
   5) Move the APs to the existing network.

   NOTE: The backup and restoration of an existing configuration is only supported with a software version higher than 2.1.0.67. All APs with a configuration based on 2.1.0.67 must have their configuration cleared.