Release Notes - Rev. D

OmniAccess AP1101

AOS-WNG Release 2.1

These release notes accompany AOS-WNG Release 2.1 software for the OAW-AP1101. This document provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

IMPORTANT: Prior to deploying any OAW-APs shipped with software version 2.1.0.67 you **MUST** first upgrade the software to the version available on the Service & Support website. Please review the Prerequisite section for additional information.

Table of Contents

Related Documentation

The release notes should be used in conjunction with the associated manuals as listed below.
User manuals can be downloaded at:
http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

OAW-AP Quick Start Guide
The Quick Start Guide assists you in quickly connecting to and configuring the OAW-AP.

OAW-AP Installation Guide
Provides technical specifications and installation procedures for the OAW-AP.

OAW-AP Configuration Guide
Includes procedures for managing and configuring all aspects of the OAW-AP using the built-in web interface.

Technical Tips, Field Notices, Upgrade Instructions
Contracted customers can visit our customer service website at: support.esd.alcatel-lucent.com.

Prerequisites

Please note the following important release specific information prior to upgrading or deploying this release.

- 2.1.0.67 – Previous factory default software version shipped on some units during September, 2016.
- 2.1.0.78 – Previous factory default software version shipped on some units during October, 2016.
- 2.1.0.79 – Current factory default software being shipped on all units.

System Requirements

OAW-AP1101

Software Release	Note
2.1.0.67	This was the factory default version shipped on some units during the month of September, 2016. It's strongly recommended to upgrade to version 2.1.0.79 which is the current factory default version and is also available on the service & support site.
2.1.0.78	This was the factory default version shipped on some units during the month of October, 2016.
2.1.0.79	This release fixed SR# 1-199557608: Not possible to broadcast only 5GHz SSID from wizard. The AP-1101 was not broadcasting single radio only 5GHz SSID when configured from the wizard. However, if the SSID was configued as dual radio, then the SSID was visible in 5GHz. Additionally, when configured as dual-radio, the 5GHz SSID experienced a delay before showing up as compared to the 2.4GHz SSID.
IMPORTANT: Review the detailed explanation and follow the upgrade instructions in Appendix A prior to deploying the OAW-AP1101.	

New Hardware Supported

OAW-AP1101

The OAW-AP1101 is a dual-band, 2x2 MIMO, indoor wireless access point supporting the 802.11ac standard.

- Based on an AP group network architecture with support for up to 16 APs.
- Software configurable for dual-radio or single-radio working status.
- Multi-core CPU processor that has the fastest encoding and decoding capability and ensures reliability of multiple users access with heavy traffic.
- Supports up to 1.2Gbps wireless data rate.
- Equipped with 3dBi antenna.
- Capable of covering 50 meters distance in line-of-sight environment.

New Software Features and Enhancements

The following software features are new with this release, subject to the feature exceptions and problem reports described later in these release notes:

Feature	Platform
Group Network Architecture	OAW-AP1101
RF Management	
- Radio Dynamic Adjustment (RDA)	OAW-AP1101
- Manual RF Management	OAW-AP1101
- Background Scanning	OAW-AP1101
- Band Steering	OAW-AP1101
Roaming	
- L2 Roaming	OAW-AP1101
- Opportunistic Key Caching	OAW-AP1101
- Fast BSS Transition (802.11r Roaming)	OAW-AP1101
Authentication	
- 802.1x/WPA2	OAW-AP1101
- Captive Portal Authentication (Internal Portal Server)	OAW-AP1101
- EAP types supported: PEAP, EAP-TLS, EAP-TTLS,EAP-GTC	OAW-AP1101
- Local User Database	OAW-AP1101
Bandwidth Capping per User	OAW-AP1101
NTP Client	OAW-AP1101
Wireless QoS	
- WMM to DSCP/802.1p	OAW-AP1101
- Voice&Video aware wireless	OAW-AP1101
Multicast Optimization	
- IGMP Snooping	OAW-AP1101
- Multicst to Unicast	OAW-AP1101
Security	
- Rogue AP Detection and Containment	OAW-AP1101
- Whitelisting/Blacklisting	OAW-AP1101
- Walled Garden	OAW-AP1101
- OS Fingerprinting	OAW-AP1101
ACLs	OAW-AP1101
Configuration Backup and Restore	OAW-AP1101
Firmware Upgrade and Restore	OAW-AP1101
Factory Default	OAW-AP1101
Syslog	OAW-AP1101
Ping/Traceroute/TCPDUMP	OAW-AP1101
Zero Touch Provisioning	OAW-AP1101

Feature Summary Table

Feature Descriptions

Group Network Architecture

The AOS-WNG solution is based on a group architecture which allows multiple APs to work together and be configured using one virtual IP address for the group. All APs that have the same group ID should be in the same VLAN and will belong to the same group. The group will select a Primary Virtual Controller (PVC) and Secondary Virtual Controller (SVC) based on the MAC address, the one with the highest MAC address will be selected as the PVC and the one with the second highest MAC address will become the SVC. The PVC is responsible for the group management, such as configuration synchronization, usage data statistics, firmware upgrading, etc. and the SVC is the backup of the PVC. An AP Group supports Zero Touch Provisioning, a mechanism by which all APs of a group can obtain bootstrap data securely from a system on-premise and be provisioned with a boot image and configuration once installed and powered up.

- 16 APs per group.
- 256 concurrent clients and 16 WLANs
- AP communication based on multicast.
- Automatically selects PVC (highest MAC) and SVC (next highest MAC address).
- Zero-touch provisioning

RF Management

- **Radio Dynamic Adjustment:** Radio Dynamic Adjustment (RDA) technology automatically adjusts channel and power settings, provides Automatic Channel Selection (ACS) and Automatic Power Control (APC), and ensures that APs stay clear of all sources of radio frequency interference (RFI) to deliver reliable, high-performance WLANs.
- **Background Scanning**: The OAW-AP can be configured to provide part-time or dedicated air monitoring for spectrum analysis and wireless intrusion protection.
- **Band Steering**: The OAW-AP supports prefer 5GHz and user load balancing. Prefer 5GHz feature assigns the clients to the 5 GHz band prior to the 2.4G band. This can reduce co-channel interference and increase available bandwidth for clients due to the additional channels available on the 5 GHz band. User load balancing is based on the amount of adjacent APs, clients are steered from a busy AP to an idle AP.

Roaming

Supports L2 roaming, clients can roam among APs in the same broacast domain.

- **OKC**: If OKC (Opportunistic Key Caching) is enabled, a cached pairwise master key (PMK) is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication.
- **Fast BSS Transition (802.11r Roaming)**: The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same group.

Authentication and Encryption

When creating WLAN the following types of authentication and encryption can be configured:

- **Open**: No Authentication and encryption method is used for this WLAN. User data will be transmitted as plain text transmit mode.
- **Personal**: There will be several WPA, WPA2, AES and TKIP combinations available once you select Personal. This does not require an external RADIUS Server.
- **Enterprise**: Authentication method will be based on WPA Enterprise Architecture. Encryption method TKIP or AES is selected. An external RADIUS server is required.

EAP types supported: PEAP, EAP-TLS, EAP-TTLS, and EAP-GTC.

Captive Page Authentication is used for Open type WLAN, especially useful for guest networks which use a splash page to allow the user to enter his/her user account and password for authentication. The GuestOperator can add users to the local user database.

Bandwidth Capping per User

Provides the capability to set the bandwidth limitation per user, including downstream and upstream. This can prevent excessive bandwidth use by a single user.

NTP Client

Network Time Protocol (NTP) is a networking protocol for time synchronization between the elements across the network. You can specify a list of NTP server to be synchronized by OAW-AP in the group.

Wireless QoS

- **WMM to DSCP/802.1p:** To support different applications such as VOIP, encrypted video conferencing and desktop sharing, the OAW-AP fully supports 802.11e and WMM. 802.11e defines the quality of service (QoS) of wireless local area network and WMM works with 802.11a, b, g, and n physical layer standards to distinguish Voice, Video, Best effort and Background traffic categories. Voice/Video can be distinguished and served with higher priority. Also the the OAW-AP supports QoS mapping between 802.11 and 802.3 mapping of WMM values to 802.1p/DSCP.
- **Voice & Video aware wireless**: Background scanning needs to be aware of existing traffic on the OAW-AP. If there is an ongoing voice/video service, scanning should not be done to ensure uninterrupted traffic; scanning can be resumed when there are no active voice/video sessions.

Multicast Optimization

- **IGMP snooping**: IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows APs to listen in on the IGMP conversation between hosts and server. By listening to these conversations the AP maintains a table of multicast receivers.
- **Multicast to Unicast**: This feature allows APs to convert multicast streams into unicast streams over the wireless network based on the IGMP snooping table. Enabling Multicast to Unicast can enhance the quality and reliability of video streams, while preserving the bandwidth available to the non-video services.

Security

The OAW-AP provides leading wireless technology and extensive IEEE802.11 WLAN standard, enhanced WPA/WPA2 security and Portal/RADIUS/EAP type of authentication methods to secure all types of wireless devices connecting to the network. Integrated wireless intrusion protection offers threat protection and mitigation and eliminates the need for separate RF sensors and security appliances.

- **Rogue AP Detection and Containment**: A rogue AP is an unauthorized AP plugged into the wired side of the network or a foreign interfering AP broadcasting the same SSID with the AP group. Rogue AP is considered a security threat to the AP group. The OAW-AP is able to detect the rogues nearby and send DEAUTH packets to the clients connected to the rogue AP, keeping them away from the unsafe wireless network.
- **Whitelisting/Blacklisting**: When a client is blacklisted, the client is no longer allowed to associate with any AP in the network. When a client is in the whitelist, it can access the network without passing the captive portal authentication.
- **OS Fingerprinting**: The OAW-AP is able to discover the device type and operating system type when a client connecting to the wireless network.

Access Control Lists

The OAW-AP supports L2 and L3 access control lists.

Configuration Backup and Restore

The OAW-AP supports backup and restore capability for the configuration file through HTTP or TFTP.

Firmware Upgrade and Restore

The OAW-AP supports the upgrade and restore capability for firmware through HTTP or TFTP.

Factory Default

Press and hold the reset button for approximately 5 seconds then release. The LED will turn off and then turn red as the AP reboots to the factory default settings.

Syslog

The OAW-AP supports generating Syslog messages in a local file which can also be sent to a remote TFTP server.

Zero Touch Provisioning

An AP Group supports Zero Touch Provisioning, a mechanism by which all APs of a group can obtain bootstrap data securely from an ALE OXO server on-premise and be provisioned with a boot image and configuration once installed and powered up.

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product’s release. Any problems not discussed in this section should be brought to the attention of the Service and Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at the time of release.

System

PR	Description	Workaround
163608	Tools -> show history syslog Info may return: “No log information found”	Reloading the AP resolves the problem.
163505	Multiple syslog messages are logged as critical & error level syslog messages.	Majority of these messages are not critical and should be regarded as “informational”.
163202	NTP does not support daylight-savings.	There is no known workaround at this time.

WLAN

PR	Description	Workaround
BUG-779	Some combinations of special characters are not supported when creating a WLAN name.	1.**Avoid** using the following special character combinations in the WLAN name: “`”, ”=”, ”\”, ” **space**” 2. **Avoid** using the following special characters combinations in the WLAN name:”.*”, ”???” 3.**Suggest** using combination of letters ,numbers and single special character from the set of {~!@#$%^&*()_+|[];’:”,.<>/}, such as ”www.al-enterprise.com”.”{“ and ”}” are included. 4.Avoid using contiguous special charaters, like ”www.@#al-enterprise.com”.[.@# are the contiguous special charaters]

RF Management

PR	Description	Workaround
	Voice and video aware functions do not work when two phone terminals in the conversation attach to same AP and same WLAN.	There is no known workaround at this time.
163405	When changing and saving the WMM values the error messages "Failed to communicate with the backend server" may appear.	This is a display issue only, the configuration is applied. This happens when the configuration is slow to take effect.
	Some of the old phones do not support channel 161/165 at 5.8 GHz, so they can only use 2.4GHz if the auto channel selection on OAW-AP is selected on those channels.	There is no known workaround at this time.
	Setting the bandwidth mode is not supported in this release.	The default mode of 2.4G is HT20, and default mode for 5G is VHT80, however bandwidth compatibility for 5G can be supported for those clients who can only support HT20/HT40.

Captive Portal

PR	Description	Workaround
BUG-896	Client remains online when an "Open+Portal" type SSID is deleted and then recreated with the same name. The recreated SSID does not have authentication enabled.	Enable the "Captive portal" attribute for the SSID.
BUG-684	Captive portal doesn't support HTTPs redirect, splash page doesn't support URL using HTTPs protocol.	Enter the splash page using the URL format http://www.example.com instead of the format https://www.example.com.

Security

PR	Description	Workaround
BUG-918	Rogue AP can not be suppressed on 5G band.	There is no known workaround at this time.
BUG-533	When a client accesses the Wi-Fi network and works as a rogue DHCP server, other clients may not be able to obtain IP addresses correctly.	There is no known workaround at this time.

Wireless QoS

163405	When changing and saving the WMM values the error message "Failed to communicate with the backend server" may appear.	This is a display issue only, the configuration is applied. This can happen when the configuration is slow to take effect.

User Interface

PR	Description	Workaround
BUG-879	Firefox browser compatibility issues with Windows Server 2012.	Recommended browsers: - Google Chrome 38 and later - Mozilla Firefox 48 and later - Internet Explorer 11 and later Recommended OS: - Windows7/Windows8/Windows10/MAC OS X 10.9/MAC OS X10.10

Technical Support

Alcatel-Lucent Enterprise 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
Europe Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: ebg_global_supportcenter@al-enterprise.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's 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 - Mandatory Upgrade of the OAW-AP1101

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.

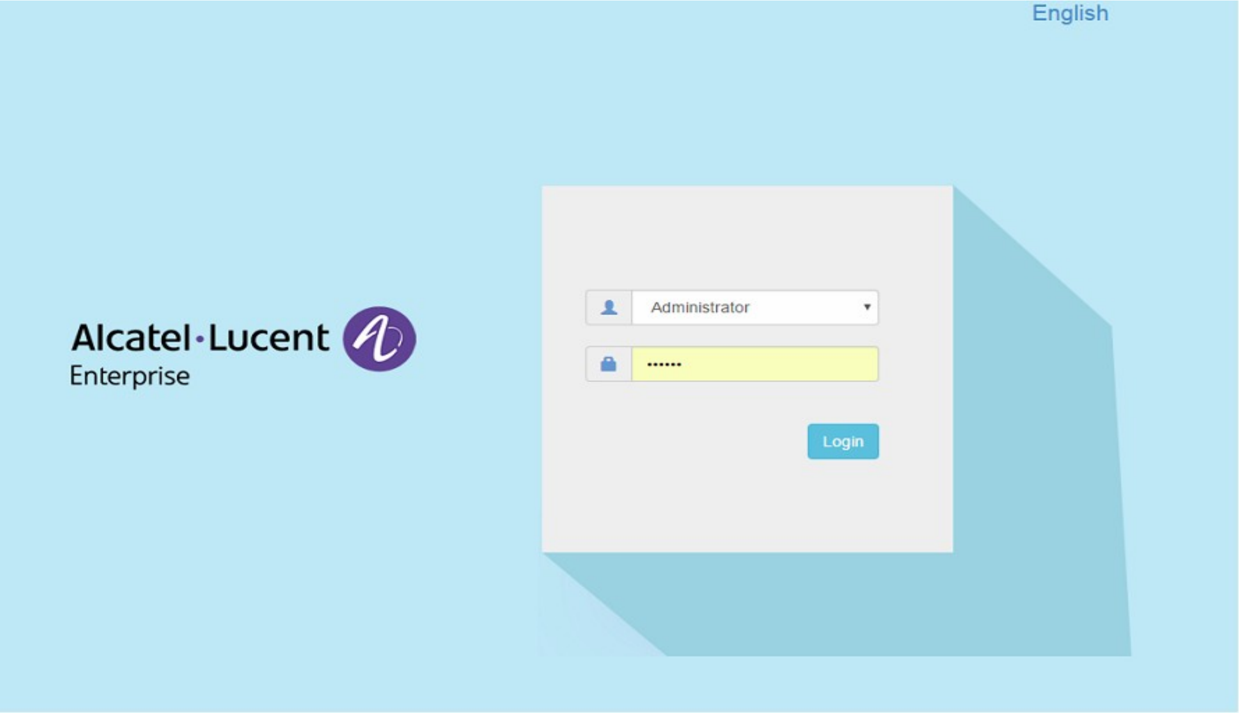
The two cases below describe the Syslog messages that will be seen when an AP running software version 2.1.0.67 is detected in a group with another AP running software version 2.1.0.68 or higher.

- 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!"

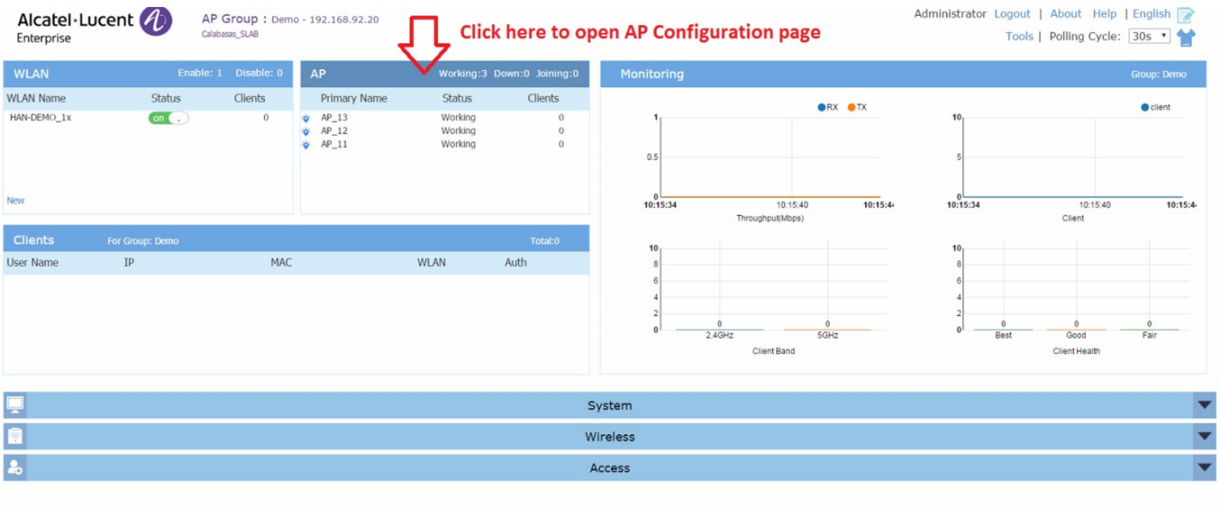
- Case2: In a group, AP-05:30 is acting as the PVC running software version 2.1.0.67; AP-00:e0 running software version 2.1.0.68 or higher is detected in the group:
  AP-00:e0 generates a Critical level log message: "Some APs in the network are running incompatible software. To avoid network interruptions, 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

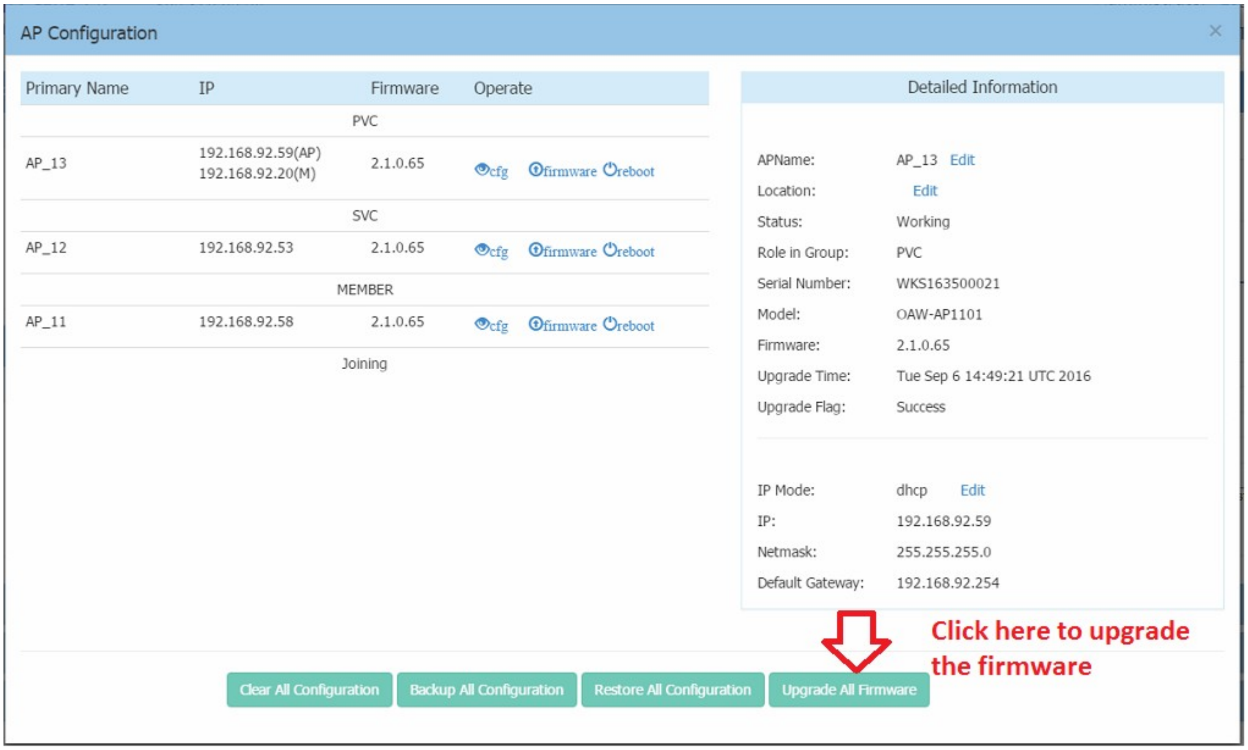
Alcatel·Lucent Enterprise
AP Group : Demo - 192.168.92.20
Calabasas_SLAB
Administrator Logout | About Help | English
Tools | Polling Cycle: 30s
WLAN Enable: 1 Disable: 0
New
AP Working:3 Down:0 Joining:0
Monitoring Group: Demo
RX TX
Throughput(Mbps)
client
Client
2.4GHz 5GHz
Client Band
Best Good Fair
Client Health
Clients For Group: Demo Total:0
System
Wireless
Access

WLAN Name	Status	Clients
HAN-DEMO_1x	on	0

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

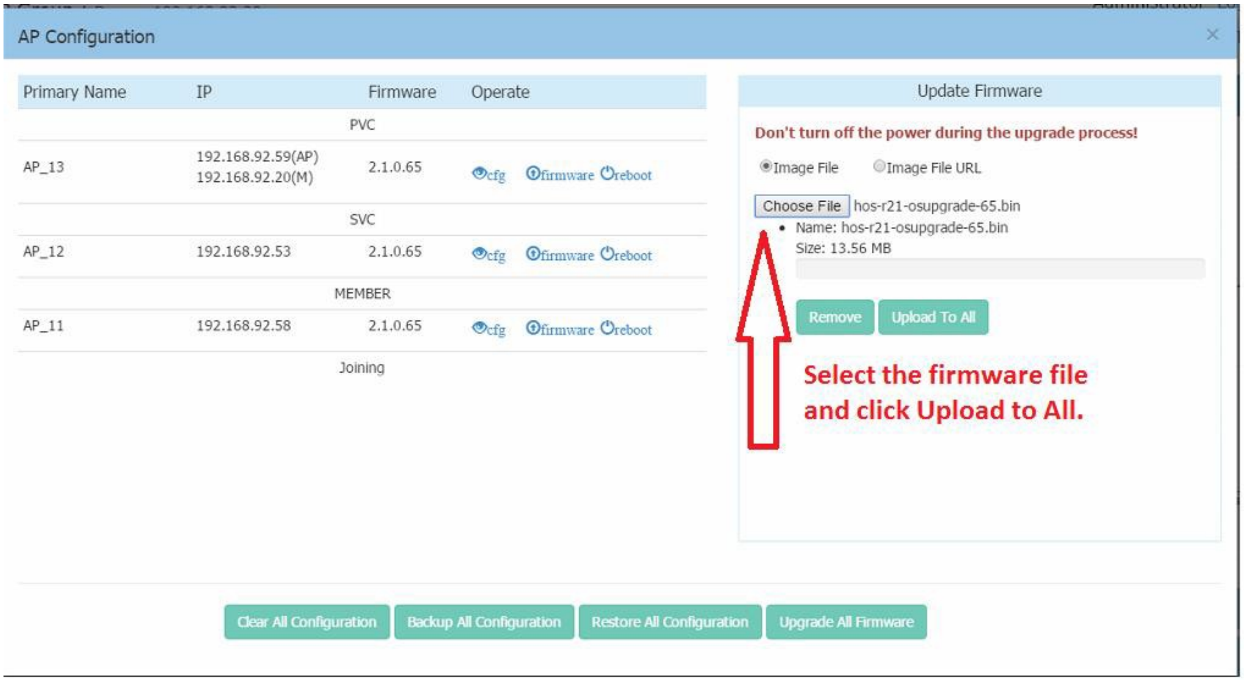
	SVC		
AP_12	192.168.92.53	2.1.0.65	cfg firmware reboot
	MEMBER		
AP_11	192.168.92.58	2.1.0.65	cfg firmware reboot
	Joining		

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

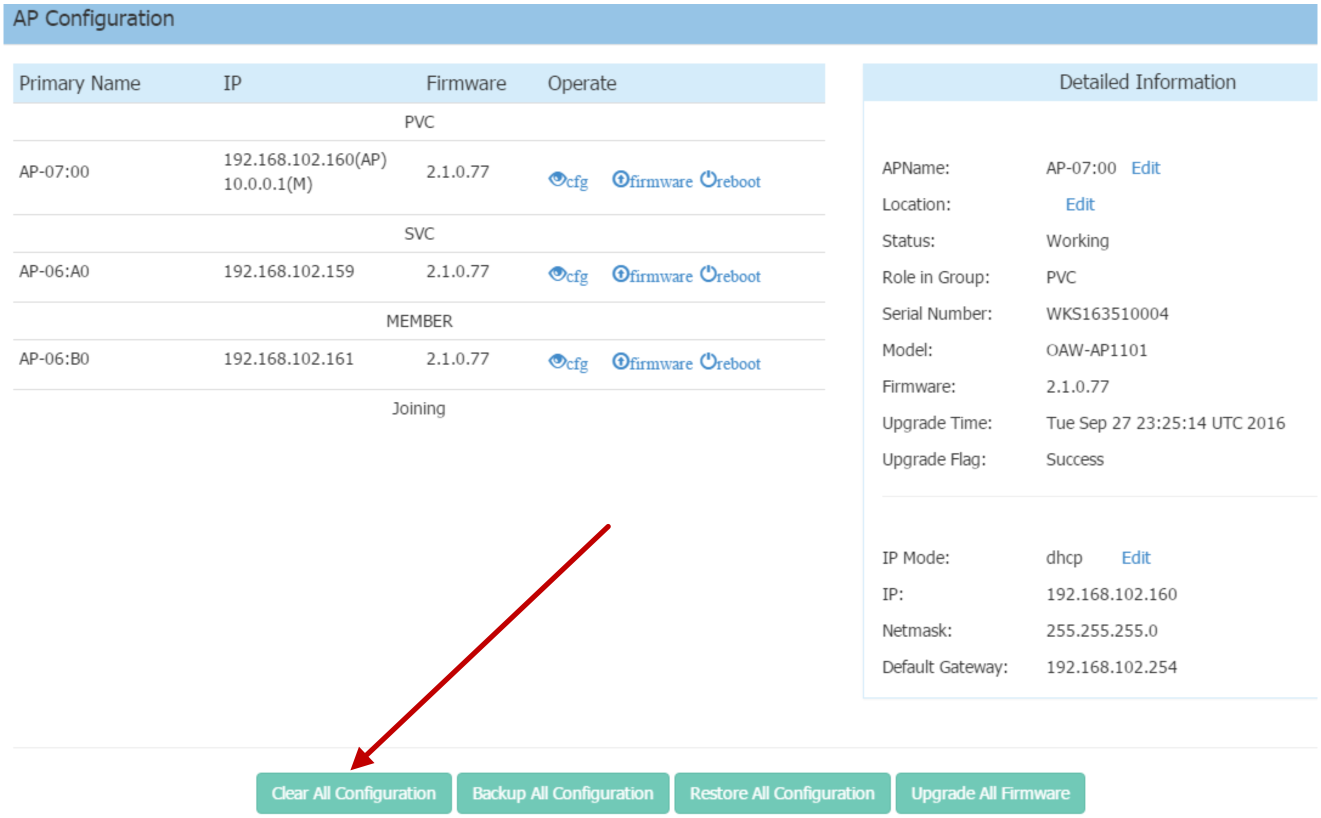
Choose File hos-r21-osupgrade-65.bin

- 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.