Release Notes – Maintenance

OmniAccess AP1101

Release 2.0.1.82

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.

Contents

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 this AOS-WNG Release.

PR	Description	Workaround
R21ISSUE-49	NTP does support daylight-savings.	There is no known workaround at this time. Planned to be supported in next release.
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.

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:

1) Click the PMD link in the main page

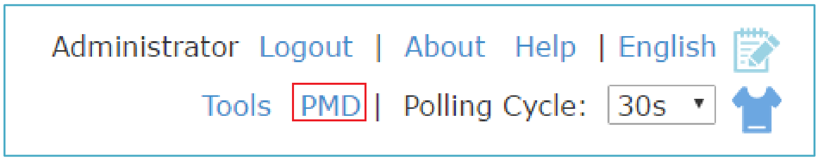
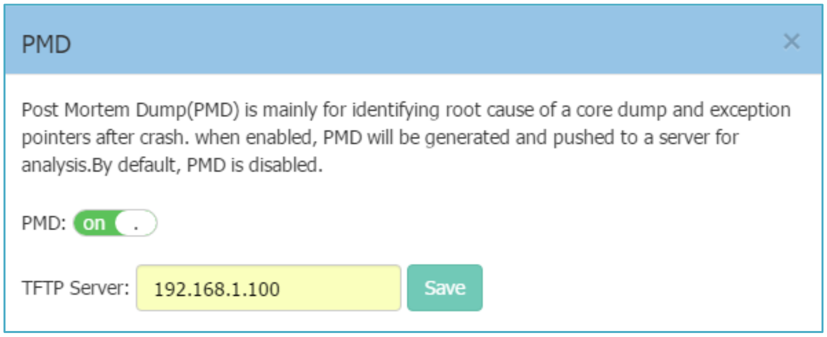


Figure 1 PMD link

2) Configure PMD



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:

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 “led_ctrl.11. core”, “led_ctrl” is the application crashed.
3) 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 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

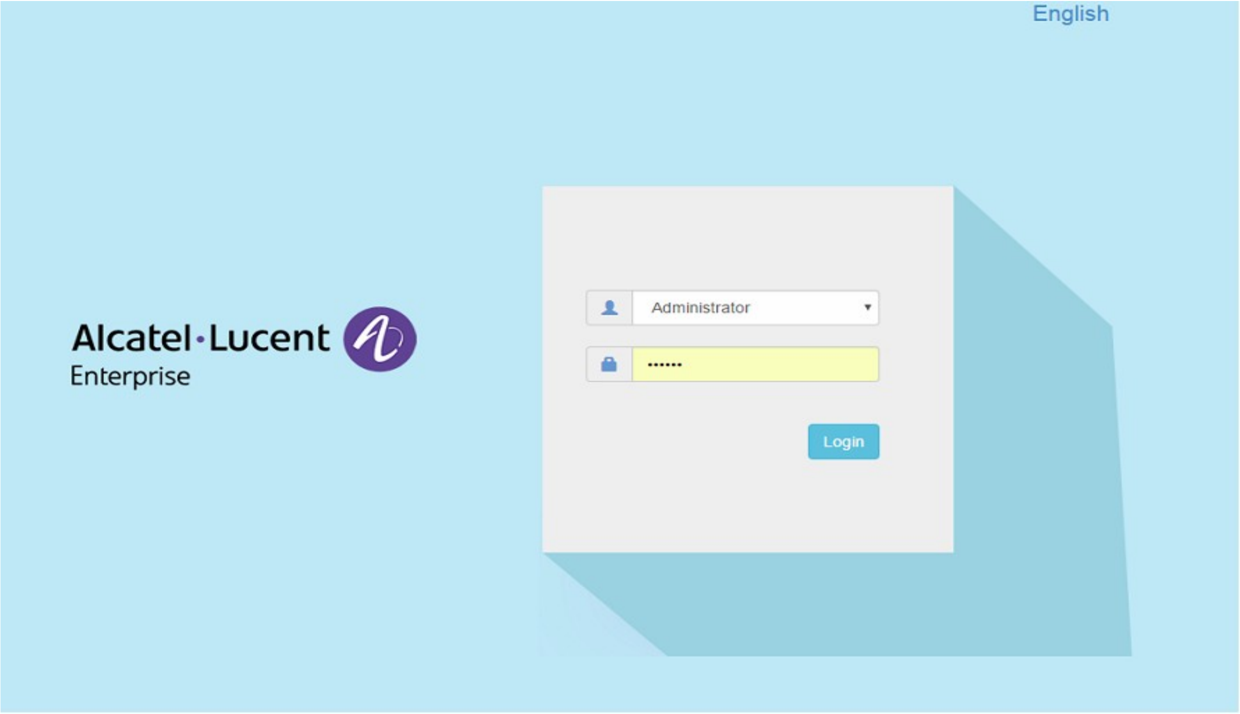
Passwords related to the operation of the OAW-AP1101 are not stored securely in software version 2.1.0.67. To resolve this issue the OAW-AP1101 software MUST be upgraded to the latest software version available from customer support. Please Visit https://support.esd.alcatel-lucent.com/ to get the latest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

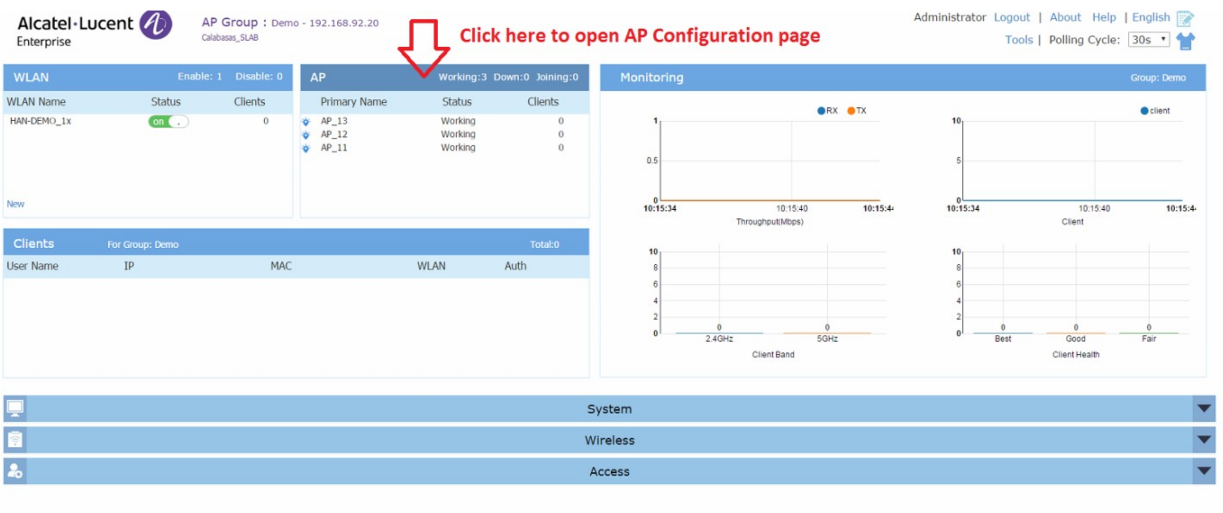
- Case1: In a group, AP-00:e0 is acting as the PVC running software version 2.1.0.68 or higher; AP-05:30 running software version 2.1.0.67 is detected in the group:
  PVC generates an Error level log message: “AP-05:30 with incompatible software is trying to join the group, please upgrade it!”
- Case2: 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

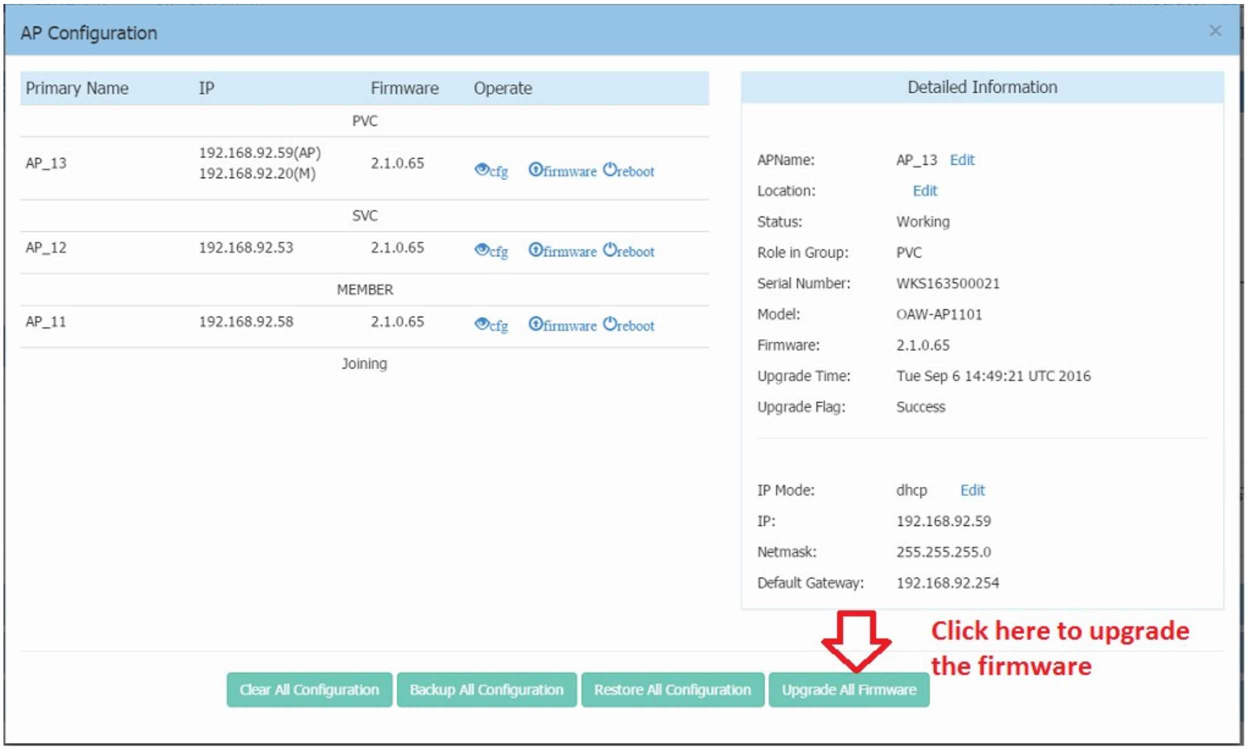
AP Working:3 Down:0 Joining:0

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.**



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

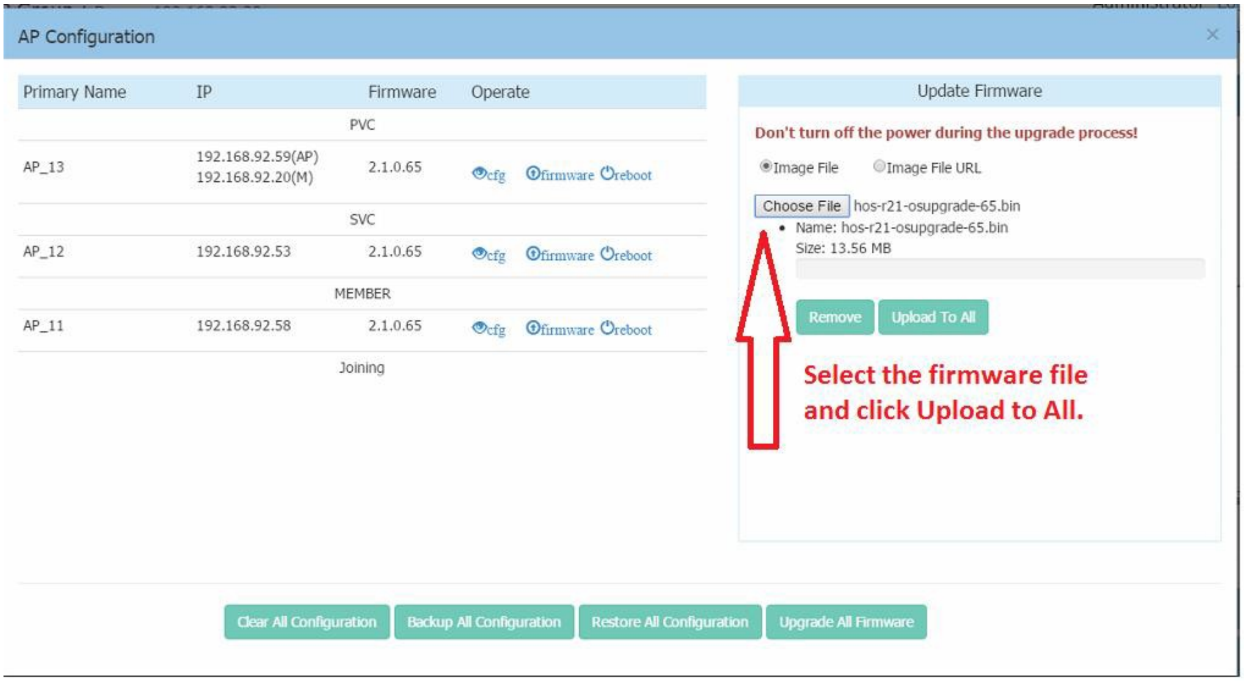
	SVC		
AP_12	192.168.92.53	2.1.0.65	cfg firmware reboot
	MEMBER		
AP_11	192.168.92.58	2.1.0.65	cfg firmware reboot
	Joining		

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!

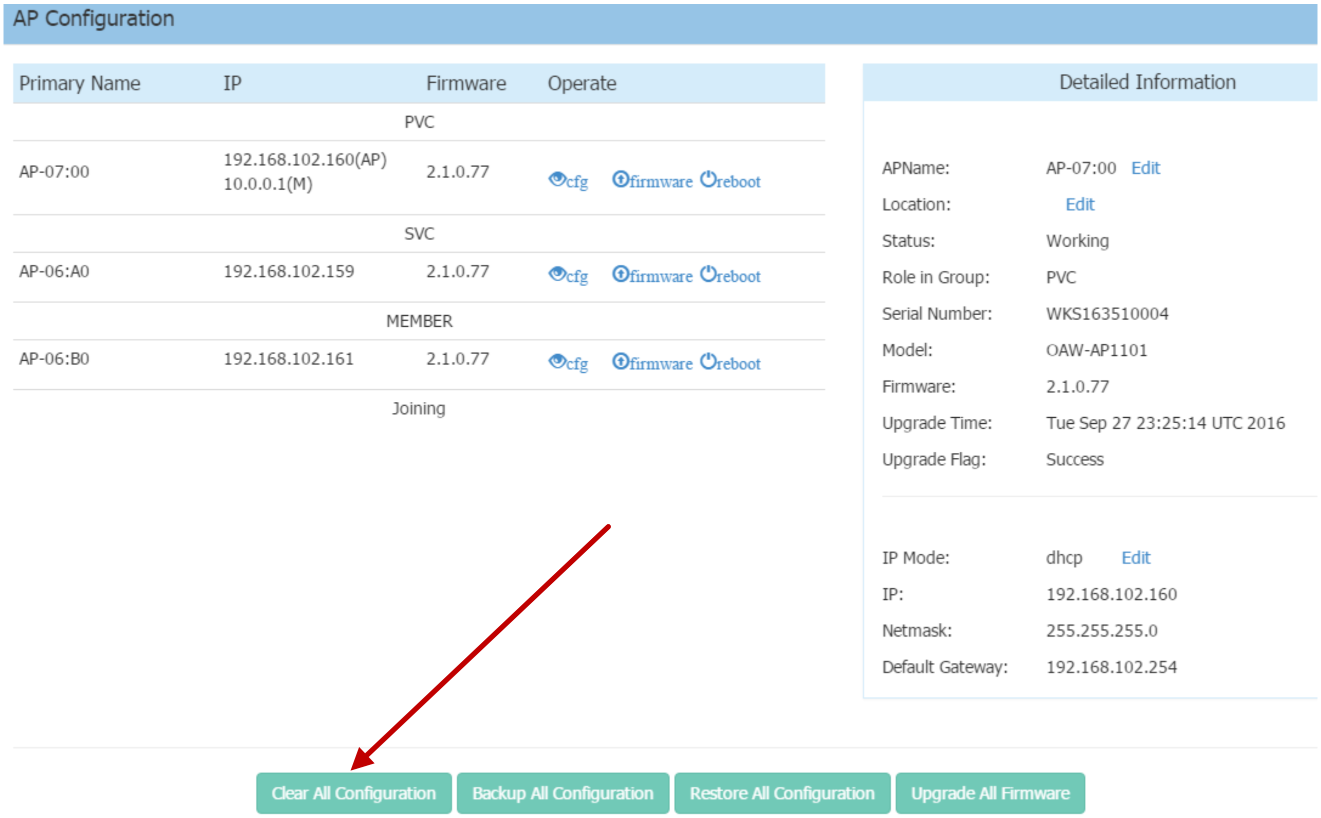
● Image File ○ Image File URL

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.