Release Notes – Rev. B

OmniAccess Stellar AP

AWOS Release 4.0.2.1033 – MR-1 Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 4.0.2 software for the Stellar APs. 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.

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: https://businessportal2.alcatel-lucent.com.

Stellar AP Quick Start Guide

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

Stellar AP Installation Guide

Provides technical specifications and installation procedures for the Stellar AP.

Stellar AP Configuration Guide

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

Technical Tips, Field Notices, Upgrade Instructions

Contracted customers can visit our customer service website at: https://businessportal2.alcatel-lucent.com.

Hardware Supported

- AP1101, AP1201, AP1220 series, AP1230 series, AP1251, AP1251-RW-B, AP1201H, AP1201L, AP1201HL, AP1320 series, AP1360 series, AP1201BG, AP1301, AP1311

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 Support
DRM Improvement: Change auto channel selection interval from 6 hours to 12 hours	All

Notes:

- OmniAccess Stellar AP reserves two SSIDs (One on 2.4G band, and one on 5G band). They perform background scanning for WIPs/WIDs services to alert and take preventive actions on any security threat. It is secure and NO clients can connect to these SSIDs.

Fixed field problems between build 4.0.2.21 and build 4.0.2.1033 (MR-1)

PR	Description
Case: 00540308 ALEISSUE-985	**Summary:** Stellar AP stuck (no Web UI access, clients not able to associate) **Explanation:** The root cause for this problem is rtnetlink module was stuck after a long time running. To prevent this issue, a defense mechanism is added
Case: N/A ALEISSUE-984	**Summary:** Policy List is not been loaded after a successful External Captive Portal authentication **Explanation:** The root cause for this problem is when wam receive portal auth success messsage, it will apply new ARP. But if the policy list was empty, it did not update, the previous value was still effective. Change to update the ARP whether the policy list is empty or not to fix this problem.
Case: 00539824 ALEISSUE-994	**Summary:** ARP on the AP uplink is not forwarded to the wireless interface causing no voice call **Explanation:** When WIFI Phone A calls WIFI Phone B, call is established but there is no voice. ARP received on the AP uplink is not forwarded to Wireless ATHxx, as a consequence, WIFI Phone does not receive IP Address where to forward RTP packets Click for additional information
Case: 00540480 ALEISSUE-1002	**Summary:** client cannot connect to Device specific PSK SSID if we have 802.11r enable **Explanation:** The Device Specific PSK obtains the key from the mac authentication packet, so it must wait for the mac authentication result to start the key exchange. When 11r is enabled, the key exchange starts without waiting for the mac authentication result, causing the connection to fail. Click for additional information
Case: 00544707 ALEISSUE-1012	**Summary:** Stellar AP ACL stop working logs shows policy: create set error: **Explanation:** The workflow sequence of POLICY module is incorrect sometimes when L2 isolation is enabled. When a client is connecting to SSID, WAM module will send this client info to POLICY and GATEWAY module. GATEWAY module obtains gateway info through the ARP message sent by this client, and then sends it to POLICY module. In normal case, POLICY module receives the client info sent by WAM module first, and then receives the gateway info sent by GATEWAY module. But if not, the client list in POLICY module may be confused, which cause POLICY module to crash. Fix Solution:

	1. Initialize the iptables rule when an exception occurs in policy and the user information is reloaded 2. When an error occurs in iptables rule, policy clear ipset multiple times to ensure the success of the operation. Click for additional information
Case: 00557674 ALEISSUE-986	**Summary**: APs showing 23 dbm power on the OV even max power level is configured to 15 dbm on the AP **Explanation**: This is only a display issue Click for additional information
Case: 00550837 ALEISSUE-1064	**Summary:** Static IP is missing after applying the untagged VLAN. **Explanation**: When AP switches from Express mode to OV mode, there is a problem with the netmgr configuration file, which leads to other problems (such as missing static IP when applying untagged VLAN). Fix Solution: When switching from Express mode to OV, synchronize the configuration of netmgr.
Case: 00551172 ALEISSUE-1073	**Summary:** Stellar Mesh AP loses static IP address after reboot **Explanation**: In mesh mode on AWOS 4.0.2 release, the default is dhcp by netmgr although static is configured. Fix Solution: Change to use correct DHCP configuration for mesh mode to fix this problem.
Case: 00543690 ALEISSUE-1020	**Summary:** OmniAccess Stellar WLAN - AP1201BG cannot be upgraded when using sshpass command **Explanation**: During the upgrade process, all processes will be killed to prevent the upgrade from being affected. But there will be some processes that will be protected from being dropped by kill process, the osupgrade command is not in the protection directory, which causing the sshpass upgrade fail. Fix solution: Add [osupgrade] command in the protection list for AP1201BG. Click for additional information
Case: 00538360 ALEISSUE-1014	**Summary:** Stellar AP no longer sending the custom certificate that is enabled after upgrade to 4.0.2 **Explanation**:

	The issue was introduced when fixing another security vulnerabilities issue, the wrong path for certificate used for express mode and cause the ap_manage process not loading the certificate after AP reboot , and then AP used the default certificate. Click for additional information
Case: 00520520 ALEISSUE-919	**Summary:** Stellar client getting disconnected randomly. **Explanation**: The probe frame sent by the client is used as the basis for determining whether to kick the client offline, but there is a situation in which the rssi frame value of the probe is very small, but the actual rssi of the client is normal. Fix solution: Only when the rssi of the wireless frame of the client is less than the set value will the logic of kicking the client be triggered, instead of relying on the rssi of the probe frame as the basis for judgment.
Case: 00552674 ALEISSUE-1062	**Summary:** Users cannot connect to an SSID on Stellar AP **Explanation**: The number of clients on radio is greater than the maximum set value, but this value will only be modified when the client becomes online or offline. This count will cause AP to reject all new users associating to SSID Fix solution: When the value is greater than the set maximum number of clients, calculate the real number of clients on the radio, and then reset the value to the real number of clients Click for additional information
Case: N/A ALEISSUE-1011	**Summary:** AP became mesh mode after upgrade from R4.0.0.9177 to R4.0.1.3091 **Explanation**: Version 4.0.0 of AP does not have the automesh feature. If the user does not enable the mesh feature, there will be no mesh configuration file. When upgrading to version 4.0.1.3091, the default automesh configuration will be created because the detection logic of the OV mode of the automesh feature is that there is no mesh configuration, and the default automesh configuration will be detected when the configuration is created. If the network status is down, the automesh created will be configured with mesh, enabled and leaf node. If there is no root node, the AP will restart, after the upgrade, the mesh will be enabled and there is no root node, it will cause the AP to restart indefinitely.
Case: 00530585 ALEISSUE-952	**Summary**: Neighboring APs are running on the same channel **Explanation**: Optimize the auto channel selection mechanism to exclude channels used by neighboring AP, and then choose the best channel to obtain better channel distribution among the network. Click for additional information
Case: N/A	**Summary**: filter-id attribute is not considered when using an External Captive Portal

ALEISSUE-949	**Explanation**: EAG did not process the filter-id attribute. Add processing of filter-id attribute to fix this problem
Case: 00550449 ALEISSUE-1038 ALEISSUE-1044 ALEISSUE-1045 ALEISSUE-1001	**Summary**: APs are showing as DOWN in the OV2500. **Explanation**: When the connection between mosquitto of AP and activateMQ is abnormal, it will cause AP to display Down, and cannot receive configuration messages from OV. Fix solution: A detection mechanism has been added to restart the MQTT process when an mosquitto exception is detected to ensure normal communication with OV
Case: 00515838 ALEISSUE-942 ALEISSUE-904 ALEISSUE-914	**Summary**: AP rebooted with unknown reason **Explanation**: This is a stability issue, and the root cause still needs to be investigated, but there can be some effective fixes. Fix solution: 1. Support disable DDR power mode, 2. Support adjust CPU clock speed 3. Use the netlink socket option NETLINK_NO_ENOBUFS to ignore the ENOBUFS messages returned by the system. Click for additional information
Case: 00524409 ALEISSUE-931	**Summary**: Wifi stations unable to connect - netlink: recvfrom failed: No buffer space available **Explanation**: The frequent ARP messages sent by kernel module arpd to wam through netlink may result in insufficient buffer from kernel to netlink, which leads to this problem [No buffer space available]. Fix solution: Only send arp reply messages to wam to reduce netlink buffer consumption Click for additional information
Case: 00544719 ALEISSUE-1013	**Summary**: sta_list shows no client connected while OV 2500 shows 17 clientx associated on same AP **Explanation:** The data displayed by OV came from the user manager module. The number of clients displayed by sta_list did not consistent with that displayed by user manager module.

	Fix solution: Update sta_list statistic mechanism for online client and solve the problem of abnormal number of clients obtained by sta_list. Click for additional information
Case: N/A ALEISSUE-1026	**Summary**: Beacon Interval can't be changed on the WIFI6 AP's when using the code 4.0.2.21 at least **Explanation:** Beacon interval did not be supported in MESH mode on build 4.0.2.21 Fix solution: Adding configuration to support beacon interval in mesh mode
Case: 00544586 ALEISSUE-1037	**Summary:** User suddenly not able to get IP **Explanation:** WLAN service module is restarted due to a driver exception, some of the interfaces failed to load. Fix solution: Adding mechanism to guarantee WLAN interfaces created correctly when WLAN service module restarted. Click for additional information

Fixed field problems between build 4.0.2.18 and build 4.0.2.21

PR	Description
Case: 00542268 ALEISSUE-1005	**Summary**: AP-1321 loss its static ip when upgrade to 4.0.2.18 **Explanation**: In some cases, the configuration parameter read by netmgr is empty, but the IP address is still configured, resulting in the correct configuration file being removed, which causes AP loss static IP after next reboot Click for additional information
Case: 00540923 ALEISSUE-999	**Summary**: After upgrade to 4.0.2.18, AP is running in dynamic instead of static mode **Explanation**: When configuring the access role of untaged VLAN, the netifd module creates the untag-related interface and reconfigures the WAN port after AP booting up, resulting of AP losing the static IP information during the process, which causes AP to work in DCHP mode. Click for additional information
Case: 00520456 ALEISSUE-918	**Summary**: Create wired network interface failed when vlanpool is null **Explanation**: In some cases, AP would receive empty vlanpools message from OV which causing AP failed to create network interface. Solution: Added a mechanism to handle the null vlanpool message to fix this problem.

Fixed field problems in build 4.0.2.18

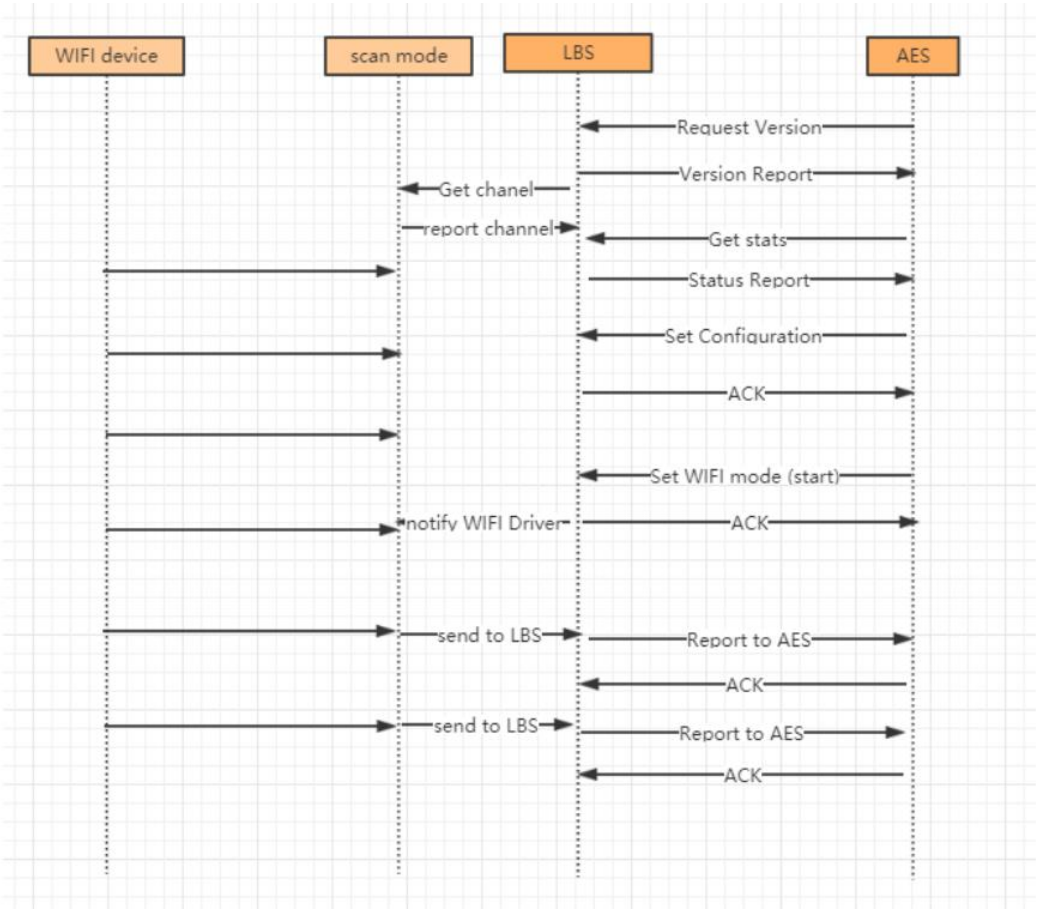
PR	Description
Case: 00523696 ALEISSUE-933	**Summary**: after upgrading the Stellar AP's from 3.0.6.3074 to 4.0.2.x, the MESH no longer works. **Explanation**: The issue is introduced by “Out-of-box Mesh” feature, system will disable mesh interface automatically once AP has wired connection with switch. With new release of 4.0.2, only when in the factory state, the “out-of-box mesh” will be disabled if there’s wired connection. Click for additional information

Case: 00530735 ALEISSUE-951	**Summary**: BYOD - After logging out of the session the user can still access to the network. **Explanation**: 1. User connects to the BYOD SSID with PSK key. Configured with untagged VLAN. Default Access role profile 2. User gets IP but not able to access the network before authentication. 3. Open browser login using Employee credentials. User is able to access the network. 4. Now user clicks on the logout button on the screen. 5. User is still able to access the network. 6. We do not have remembered device enabled on the BYOD strategy. 7. Expectation is user do not have access to the network if he clicks on the logout button. AP was removing the history of authentication and was not applying the data quota limitation Click for additional information
Case: 000062679 ALEISSUE-955	Summary: Guest User is not kicked off automatically when after account validity period Explanation: 1. User connects to the Guest SSID. Configured with untagged VLAN. Default Access role profile 2. User gets IP but not able to access the network before authentication. 3. Open browser login using Guest credentials. User is able to access the network. 4. Now after account expiry User is still able to access the network. 5. We do not have remembered device enabled on the Guest strategy. 6. Expectation is user do not have access to the network after account expiry. AP was removing the history of authentication and was not applying the data quota limitation Click for additional information
Case: 00531505 ALEISSUE-954	**Summary**: Quota does not work for guest access **Explanation**: 1. User connects to the Guest SSID. Configured with untagged VLAN. Default Access role profile 2. User gets IP but not able to access the network before authentication. 3. Open browser login using Guest credentials. User is able to access the network. 4. Then account's Quota limit is expired 5. User is still able to access the network. 6. Expectation is user do not have access to the network after Quota expiry. AP was removing the history of authentication and was not applying the data quota limitation Click for additional information
Case: 00532213	**Summary**: 802.11k does not work as expected

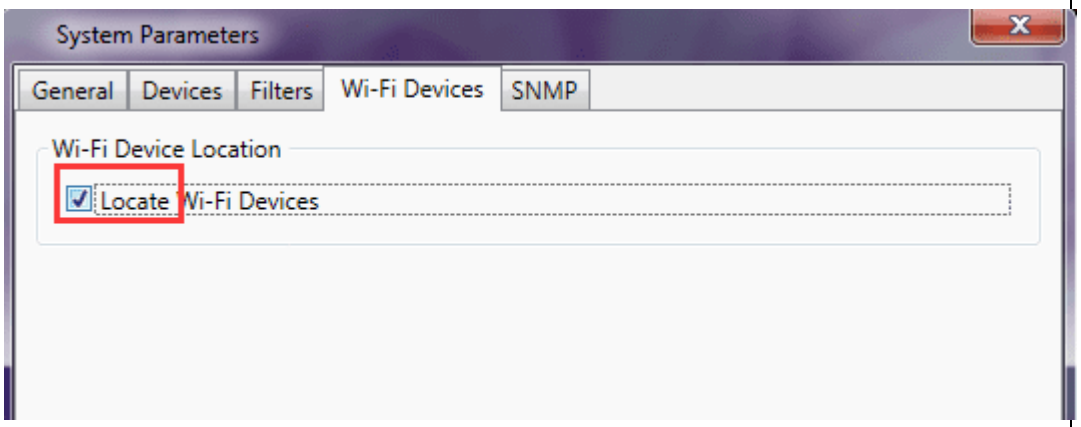
ALEISSUE-960	**Explanation:** AP has an aging mechanism to manage neighbor information, but the aging time interval is very short. With this release, once neighbor device is scanned, the data can be stored in AP for longer time. Click for additional information
Case: 00532506 ALEISSUE-962	**Summary:** 2.4GHz clients cannot connect to AP **Explanation:** The reason is that the counter of associated users is incorrect in WIFI driver. So far we don't find out the root cause, but a protection mechanism has merged into the new build, when each client access to AP, WIFI driver will re-calibrate the actual number of clients Click for additional information
Case: 00528037 ALEISSUE-940	**Summary:** Several APs upgrade failed from 4.0.0 to next releases **Explanation:** 1. A protection scheme has been added to ensure that there is sufficient memory during the upgrade and that there is no interference from kernel data. 2. If the AP upgrade fails, we can check the cause of the failure through the log collect by take_snapshot.sh
Case: 00510989 ALEISSUE-916	**Summary:** 802.11ax Wifi-6 Stellar APs 1362 when connected with fiber ports do not have LLDP link discovered on OV 2500/OV Cirrus **Explanation:** Stellar OAW-1362 when connected with fiber port (powered using PoE Adapter) is sending a different chassis and port MAC IDs, as a consequence link is not discovered/not displayed on OV topology map Click for additional information
Case: 00512196 ALEISSUE-924	**Summary:** Stellar RTLS IOT location service is not working for Wifi-6 devices **Explanation:** 'IOT/location service' is configured but Stellar AP does not send any packets to location server, AP can ping the server but cannot capture any RTLS packets/information

For AX devices, we did not initialize the mac when we obtained it, resulting in an error in calling the ubus API of IoT

Note that AES Server must be configured in order to send the first request (get channel) and then AP will start to send data as per the following call flow:



On AES Server -> System Parameters, select “Locate Wi-Fi Devices”:



Click for additional information

Fixed Problem Reports Between Build 1057(MR-1) and Build 2073 (MR-2)

PR	Description
Case: 00522531 ALEISSUE-927	**Summary:** Unable to disable scan mode option **Explanation:** The problem only happened on 11AX platform (AP1320, AP1360 Series). When configuring ALWAYS scanning mode, the parameter value in the AP was set incorrectly, which causes AP not be able to stop scanning. Click for additional information
Case: 00521061 ALEISSUE-920	**Summary:** AP1201 High CPU utilization **Explanation:** There was timer conflict for DRM module causing the high CPU utilization. Optimization of different timers fixed the issue Click for additional information
Case: N/A ALEISSUE-892	**Summary:** AP rebooted with core-mon reboot due to wam memory leak **Explanation:** Issue fixed by limiting the number of client synchronous entries in WAM module
Case: 00512929 ALEISSUE-894	**Summary:** AP-1221 crash with out of memory when around 50 to 60 users connected to it **Explanation:** Wrong parameter was pushed to wireless driver by application when large amount of clients connected Click for additional information
Case: 00516305 ALEISSUE-907	**Summary:** Multicast stream not broadcasted by stellar AP1221 **Explanation:** The problem is caused by wrong configuration on the wireless driver for untagged multicast traffic. Workaround on previous version (mcsctl -s br-wan state disable) Click for additional information
Case: 00515422 ALEISSUE-911 ALEISSUE-912	**Summary:** Unable to upgrade AP's and download logs from the AP assigned with the Management tagged VLAN IP, getting error (Failed to communicate with the backend server) **Explanation:** The issue does not happen when using management VLAN and dynamic IP. Issue is observed when configuring static IP Address on br-wan

	Click for additional information

Fixed Problem Reports Between Build 44(GA) and Build 1057(MR-1)

PR	Description
Case: 00510741 ALEISSUE-887	**Summary:** Client Blacklisting Does Not Work on AP1320/AP1360 **Explanation:** Modify the interface between software and Wi-Fi driver to set correct parameters in Wi-Fi driver to make client blacklist working. Click for additional information
Case: N/A	**Summary:** SSID is not created on 11ax device after changed group on OV **Explanation:** After change group operation, AP loaded wrong RF profile, causing not broadcasting SSID. Modified the internal configuration logic to fix this problem.
Case: 00500298 ALEISSUE- 836	**Summary:** AP1360 series Tx-Power went from 50 mW to 25mW after upgrading **Explanation:** Since AP takes some time to create wireless interface after booting up, during this period the static Tx-Power cannot be set correctly. Optimize to reduce the wireless interface creation time and add a waiting timer to ensure RF profile is loaded correctly after wireless interfaces completely created. Click for additional information
Case: 00492998 ALEISSUE-781	**Summary:** AP is taking more than 10 min to come UP in OVE. **Explanation:** The issue happened when large configuration existed on AP with maximum SSIDs as well as nearly hundred VLANs. The previous logic of interface creation was only suitable for small configuration and it contained some redundant operation. Optimize the interface call relationship and removed some waiting timer to fix this problem. Click for additional information
Case: 00514750 CROVAE-65	**Summary:** APs status is DOWN on Asset Tracking when running AWOS 4.0.1.44 **Explanation:** The BLE module initialization sequence was after the report module, it caused the AP reporting message with wrong BLE mac. Adjust the module initialization sequence to fix this problem. Click for additional information

Fixed Problem Reports in build 4.0.1.44

PR	Description
Case: **00494467** ALEISSUE-796/ ALEISSUE-806/ ALEISSUE-819/ ALEISSUE-831/ ALEISSUE-842/ ALEISSUE-846/ ALEISSUE-856/ ALEISSUE-865/ ALEISSUE-868	**Summary**: Unknow reason reboot. **Explanation**: Root cause : With the “memory-access error”, the kes logs might overwrite the data of the area/address for Linux system, that could lead to different abnormal reboots. Solution: Reallocate the memory usage for “kes log” to reserve a special area to avoid the Memory out of bounds by “kes log”. Click for additional information
Case: **00492778** ALEISSUE-810/ ALEISSUE-807	**Summary**: AP reboot with policy exception. **Explanation**: Fix a policy process crash issue. Click for additional information
Case: **00502500** ALEISSUE-857	**Summary**: Heatmap with AP-1321 is not displayed. **Explanation**: After AP bootup OV will get the AP RF information from AP once, but sometimes the wireless interface is not ready and causes the OV get null information. Optimization of the software to ensure OV can get the correct information. Click for additional information
Case: N/A ALEISSUE-820	**Summary**: Channel 144 missing in OV for Singapore County code. **Explanation**: Wireless driver add support for channel 144. Click for additional information
Case: N/A ALEISSUE-861	**Summary**: Stellar AP Data tunnel not able to support packet size more than 1354 Bytes. **Explanation**: The management frame doesn’t support IP fragmentation, so it will be dropped during transmission due to MTU. Management interface MTU set to 1420 by default, also the value can be configured in SUPPORT account.
Case: N/A ALEISSUE-408	**Summary**: Information disclosure via Rsync default credentials in Express mode. **Explanation**: Rsync credentials encrypted to enhance security.
Case: N/A ALEISSUE-713	**Summary**: Configured SSID detected as interference AP by the same AP’s scanning function(AP13xx). **Explanation**: Fixed this scanning issue.

Case: **00486920** ALEISSUE-770	**Summary**: Multicast traffic flooded on all SSID's with different VLANs. **Explanation**: In order to roam faster, all the traffic will be forwarded when a client roams to a new AP even if it doesn't finish authentication. But that also causes all packets to be leaked between VLANs since forwarding logic in macvlan layer doesn't distinguish VLAN-ID. In 4.0.1 build packets will be dropped if the VLAN-ID is not the same as the interface VLAN-ID. Click for additional information
Case: **00490818** ALEISSUE-785	**Summary**: AP eth1,2 and 3 are coming up even before the AP is completely up. **Explanation**: The downlink port stays disabled if the link between AP and OV is not established completely. Click for additional information
Case: N/A ALEISSUE-818	**Summary**: AP1231 does not disable 5g High radio even though its unchecked in RF profile. **Explanation**: Optimize code logic, AP does not upload radio information if this band is disabled.
Case: **00498265** ALEISSUE-826	**Summary**: Default STP priority for mesh root AP's. **Explanation**: STP function is disabled in 4.0.1 build. Click for additional information
Case: **00459427** ALEISSUE-666	**Summary**: Even if the inactive time is disabled, the captive portal users are getting disconnected after 15 minutes. **Explanation**: The inactivity timeout setting is restricted by wireless driver and the maximum value is 12000 seconds, increase the range from [1-1200s] to [1-12000s]. Click for additional information
Case: **00484996** OVE-7859/ OVE-8174	**Summary**: Stellar WLAN – reduce DPI manager memory consumption. **Explanation**: Fixed the bug that memory of DPI process increased when loading preconfig messages. Click for additional information
Case: **00467457** OVE-8881	**Summary**: The data can be forwarded from VPN VA when guest tunnel with vlan. **Explanation**: Because VLAN-ID field in the packet takes 4-bytes the data interface MTU is set to 1542 by default. Also the value can be configured in SUPPORT account. Click for additional information

Open/Known Problems

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.

PR	Description	Workaround
ALEISSUE-882	**Summary:** When connecting with WPA3-AES-Enterprise (802.1x + AES), it is almost unusable, the speed is dramatically low.	Will be optimized in AWOS 4.0.3
ALEISSUE-949	**Summary:** When an External Captive Portal is configured the Stellar AP is not processing properly any filter-id sent by the Radius server instead of that always will assign any accepted connection to the SSID Default ARP.	Will be fixed in 402MR1
ALEISSUE-931	**Summary:** SSID is not visible and clients are disconnected. Wifi clients are unable to reconnect.Reason netlink: recvfrom failed: No buffer space availabl	Will be fixed in 402MR1
WCF limitations	Cache is done at the AP level and is limited to 2000 entries, cache is removed every 12 hours, this is not configurable An AP will allow any URL to be accessed by the first time a user visits that URL, while the AP tries to determine whether this URL is to be restricted for this Access Role Profile or not. If the URL is to be restricted, subsequent users belonging to the same Access Role Profile will then be blocked from visiting this restricted URL. So, on any given AP, Web Content Filtering will not be effective for the first visitor of a restricted URL. Web Content Filtering rules will be effective for such first visitors only after DNS cache expires on the user device • if we consider only one user is connecting behind RAP or AP, this user will never be restricted • if we consider the above limitation, every 12 hours one user will be able to access the website	
WCF limitations	When a client tries to access a website (category) that is restricted for access	In OV 2500 4.6R01/AWOS 4.0.3 if user is trying to reach a

	by admin, the client will see the page fails to load, and the browser will finally display a generic error.	HTTP website, we will redirect client to a specific block page
Management VLAN	**Summary:** when the management VLAN is enabled, setting the static IP may fail	The static IP must be set first, and then enable the management VLAN
Reboot by Target Assert	**Summary:** The AP reboot by WIFI chipset bug	Continuously optimizing CPU management and reducing CPU utilization to avoid CPU exception. Target: AWOS-4.0.3
Unknown reason reboot	**Summary:** for some reason, AP reboot with unknown reason sometimes	Continuously optimizing CPU management and reducing CPU utilization to avoid CPU exception. Target: AWOS-4.0.3
Static IP address	**Summary:**[BBNL]The static IP address for the br-vlan sometimes disappeared if we set it just after finishing changing the vlan id of the WLAN.	Modify the vlan id of wlan and wait a little longer before setting the br-vlan static IP.
AP1220 reboot due to out of memory	**Summary:** When unicast traffic is large, AP may cause OOM, due to a sharp drop in available memory, especially for AP with less than 40m of available memory.	Reduce unicast traffic scenarios
Device type and operate system	**Summary:** The Samsung client terminal device type and system reported by AP are incorrect. Notice: Occasional problem.	Use the client to access the web page for a period of time, and then refresh the display on OV
LED state abnormal	**Summary:** After AP boot up, the blue light is on after the network is connected, and when network is unreachable due to LACP, the red light begins to flash. After waiting for the network to be connected, the blue light is detected again. Notice: Occasional problem.	Because of the LACP function, this is the normal design logic, and the state of the lamp will be optimized later.
802.1x_WPA3_AES	**Summary:** Configure 1x_wpa3_aes VLAN:56 WLAN,iPhone11 and iPhone7 access, and then the client iPhone11	Change the wlan to untag, and re-send it to the Group. Client can be accessed normally, and then the wlan can be changed

	prompts that you cannot join the network	to tagged, client for normal access. Target: AWOS-4.0.3
LDAP	**Summary:** Configure on-premise ldap with special characters for AP, clients to connect to the wlan, page to prompt authentication failure	1. Rebind the issued configuration globally. This problem can be solved. 2. Special characters cause, if there are no special characters, there is no this problem
Portal authentication	**Summary:** When "/ # /\ / &" exists in the userparameters value of the AD server, and the client connects to wlan, to launch the portal page, the login jump exception occurs.	Special characters cause, if there are no special characters, there is no this problem
Portal authentication	**Summary:** When the authentication source is ldap/ad.portal authentication, AP will send a lot of mac authentication, and portal authentication will not be able to jump to the authentication success page for a long time.	
DPI	**Summary:** [reflexive] configure link tracking. DPI_DROP does not take effect.	After modifying the reflexive, the client needs to go online and offline again, which can return to normal.
Apple device connection issue on 1320/1360 series	**Summary:** When the VLANID in SSID is modified, all clients will be kicked off, but Apple device may not send DHCP request when reconnecting with this SSID, that will cause to keep using old IP address and unable to connect to the network.	Disconnect and re-join this network with the Apple device
AP1201H is in downlink bridge mode, and the client cannot get IP when it is associated with tag wlan.	**Summary:** AP1201H is downlink bridge mode. When the client is associated with tag wlan, it cannot get IP, that is, AP1201H and other models of AP,. Tag bridge mode is not supported.	AP1201H has low performance and is not recommended as a bridge AP
Short GI	**Summary:** The configuration on the web side of shortgi does not seem to take effect. In the case of more WLAN, it only takes effect on some WLAN.	Target: AWOS-4.0.3

Configuration synchronization	**Summary:** After changing AP1231 from tagged to untag, there is a problem with configuration synchronization	If you separate the cluster by tagger and want to return to the original cluster, you need to manually firstboot, and then add the original cluster synchronization configuration.
Express Login	**Summary:** [Cluster/AP] Downgrade version 4.0.2.x to version 4.0.0.x Actual result: log in to the cluster page after the upgrade is completed, and the password is changed to admin.	Login with default password and reconfigure it.
AP stateful ipv6 address	**Summary:** The ipv6 address of the dual-stack AP,AP is a stateful address. After configuring the open type wlan, to associate the wlan, with the wireless network card of win 7 11n set to single-stack V6, check the network on-off condition of the V6 address.	When you manually configure a V6 address of the same network segment on the client as the gateway address, you can communicate with the same network address.
DPI FTP policy	**[reflexive]** Create one policy list binding and two policy, results that the user cannot access the ftp	

Limitations and/or Dependencies

Feature	AP Model	Limitations and/or Dependencies
Wired Port	AP1201HL	AP1201HL switches to a Group with downlink configuration, wired client cannot access it.
Change Group	AP1301/AP1311/AP1320 Series/AP1360 Series	For AX devices, when there are a large number of wlan interfaces, frequent group-cutting operations may lead to the emergence of target assert in wireless drivers.
DRM	All	In some cases, when the channel utilization reaches more than 90%, the channel does not switch automatically, which seriously affects the user experience.
IGMP Snooping	AP1301/AP1311/AP1320 Series /AP1360 Series	For 11AX devices, if there is no multicast querier in the environment, the conversion from multicast to unicast may fail. We recommend that the switch of IGMP Snooping feature be turned on by default.
Mesh	All	Multicast to unicast is not supported in Mesh mode.

		Because, root AP to non-root AP does not implement the function of multicast to unicast in mesh mode, even if the client on non-root AP implements multicast to unicast, the efficiency is still not high.
DPI	AP1311/AP1301	When the DPI feature is enabled and the DPI configuration is loaded at the same time, when clients continue to connect, the remaining memory will be reduced and cannot be reclaimed. When the remaining memory is lower than a certain value, AP may restart due to insufficient memory. It is recommended that turn off DPI, or do not load the relevant DPI configuration
DPI	AP1201 AP1220 series, AP1251	When DPI function is enabled, it is recommended to have an initial free memory size of about 30MB after AP booting up for system stable running. If the booting up free memory size is far less than 30MB, suggest removing unnecessary WLAN/VLAN/Policy/DPI rule on AP1201/AP1220/AP1251.
Bypass vlan	AP1201H/AP1201HL	If the bypass vlan function is enabled, setting vlan id A, and setting the management vlan to tag vlan id is also A, which will cause the AP itself to be inaccessible and affect the operation of AP. Therefore, there is a restriction here that the tag for managing vlan cannot be the same as bypass.
ALEISSUE-882	All	When connecting with WPA3-AES-Enterprise (802.1x + AES), it is almost unusable, the speed is dramatically low.
	AP1311/AP1301	There is the problem of packet loss in the wired port of AP1311/AP1301,because driver upgrade is involved, it will be fixed in 4.0.3
Wlan	AP1311/AP1301	For devices with a non-US/CN country code, the 2.4G signal of AP1311 may not be scanned, or may even be scanned but the connection fails.
mDNS	AP1201H/AP1201HL	AP1201H/1201HL Downlink Terminal does not support mDNS message forwarding
Show device name	All	When some clients connect to wlan, there is no option12 field in the dhcp message, so its hostname cannot be displayed.
Login	All	[Cluster/AP] cluster login password is changed to admin after cross-version upgrade of AP

.

Application support matrix:

	AP1101	AP1201	AP1201H AP1201L	AP1220 Series	AP1230 Series	AP1251	AP1320 Series	AP1360 Series	AP1311

			AP1201HL						
Application Visibility (DPI)	N	Y	N	Y	Y	Y	Y	Y	Y
IoT Profiling	Y	Y	Y	Y	Y	Y	Y	Y	Y
mDNS Edge	N	Y	Y	Y	Y	Y	Y	Y	Y
Mesh/Bridge	Y	Y	Y	Y	Y	Y	Y	Y	Y

Restrictions on Mesh / Bridge AP

We support up to 8 slave APs, and the chain is up to 4 hops and the max AP number is up to 16 APs in a mesh network.

The WLAN limits is 5 with single frequency on mesh AP.

If AP works in bridge mode, it will not broadcast wireless signals.

Users can only change the channel of root AP

Hardware Limit:

	AP1101	AP1201	AP1201H AP1201L AP1201HL	AP1220 Series	AP1230 Series	AP1251	AP1320 Series	AP1360 Series	AP1311
No of SSID max	7	7	7	7	7	7	7	7	7
No of VLANs max	16	32	16	64	64	64	64	64	64
No of Policy max	64	128	64	256	256	256	256	256	256
BLE Gw	N	Y	N	N	Y	N	Y	Y	Y
Zigbee Gw	N	Y	N	N	N	N	Y	Y	Y
LinkAgg	N	N	N	N	Y	N	Y	N	Y
WPA3	Y (1)	Y	Y (1)	Y	Y	Y	Y	Y	Y

(1): AP1101 does not support WPA3_AES256 full band and AP1201H(L) does not support WPA3_AES256 on 2.4GHz band

Best practice recommendations:

	AP1101	AP1201	AP1201H AP1201L AP1201HL	AP1220 Series	AP1230 Series	AP1251	AP1320 Series	AP1360 Series	AP1311
No of SSID	4	5	4	5	5	5	5	5	5
No of VLANs	4	16	4	32	32	32	32	32	32
No of ARP	8	32	8	64	64	64	64	64	64
No of Policy	32	64	32	64	64	64	64	64	64
Multicast traffic (Mbps)	1Mbps	2Mbps	1Mbps 20Mbps for wired port	2Mbps	2Mbps	2Mbps	2Mbps	2Mbps	2Mbps

Note: the multicast traffic depends of interface in AP and it is recommended to enable the IGMP Snooping function in case of multicast scenario

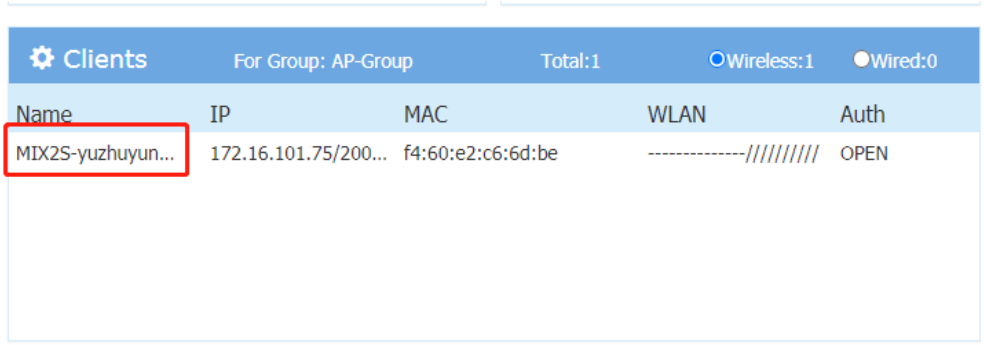
New Software Feature Descriptions

Show Device Name

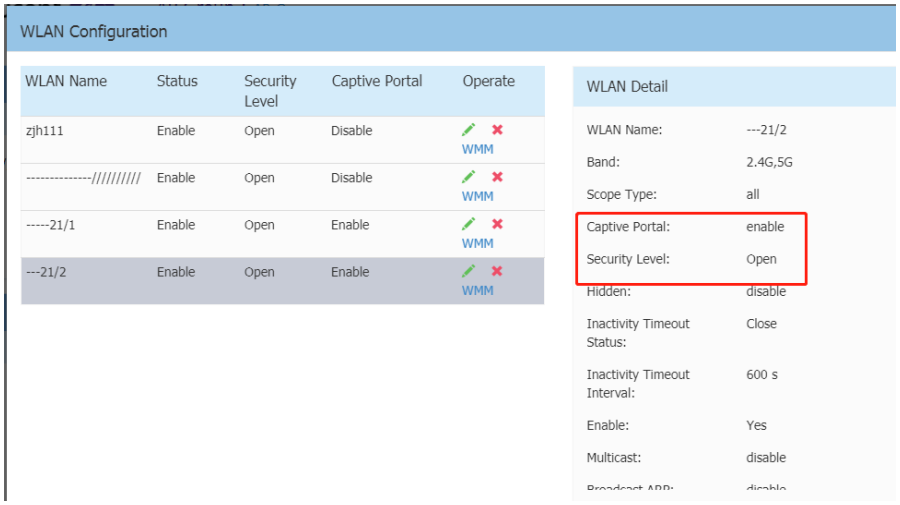
Show device name is support in 4.0.2 release, when there is a portal certified username, the username is displayed, and in other cases, the client's hostname is displayed.

As follows:

1. Host name is displayed when there is no username in non-portal mode



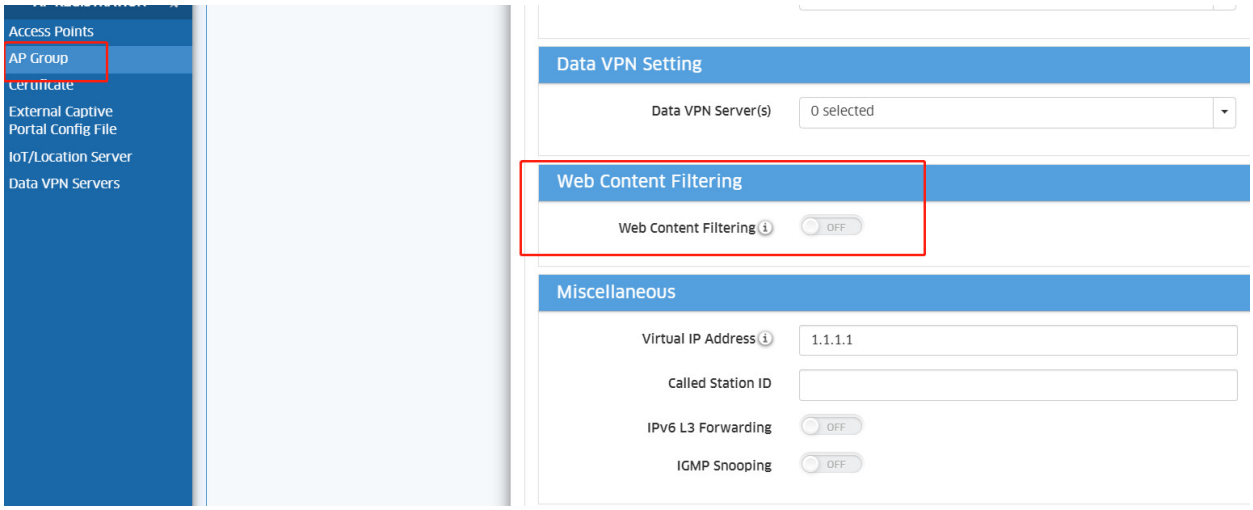
2. When portal mode and username are present, username is displayed



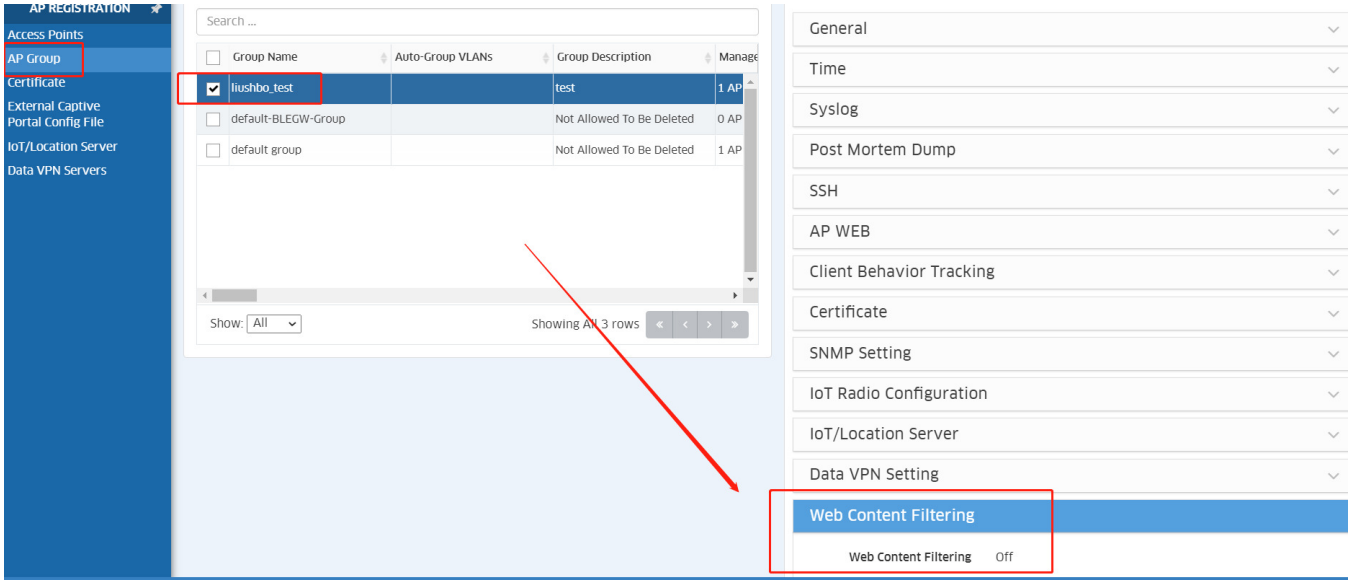
Web Content Filter

The WCF function is the Web Content Filter function, which mainly filters the url to be accessed by client and adds release and deny rules so that it can only access the URL specified by the administrator.

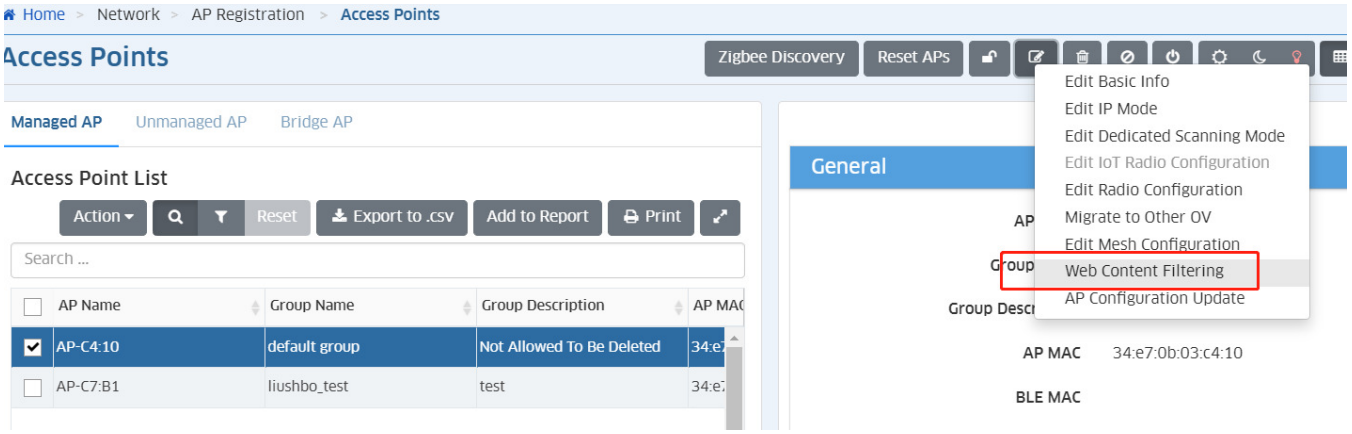
1. Group WCF configuration



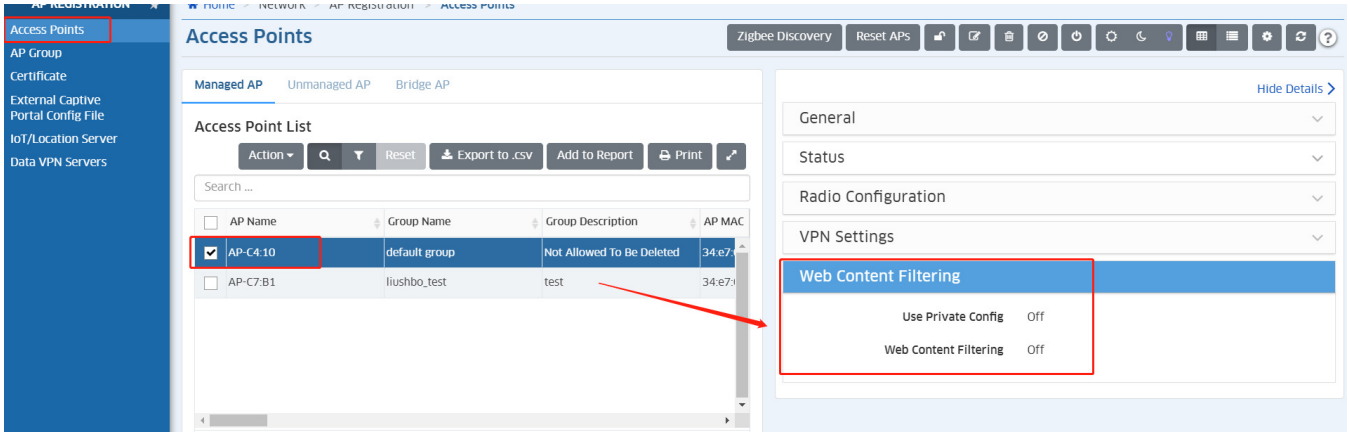
2. Check group wcf status



3. Private WCF configuration (for signal device)



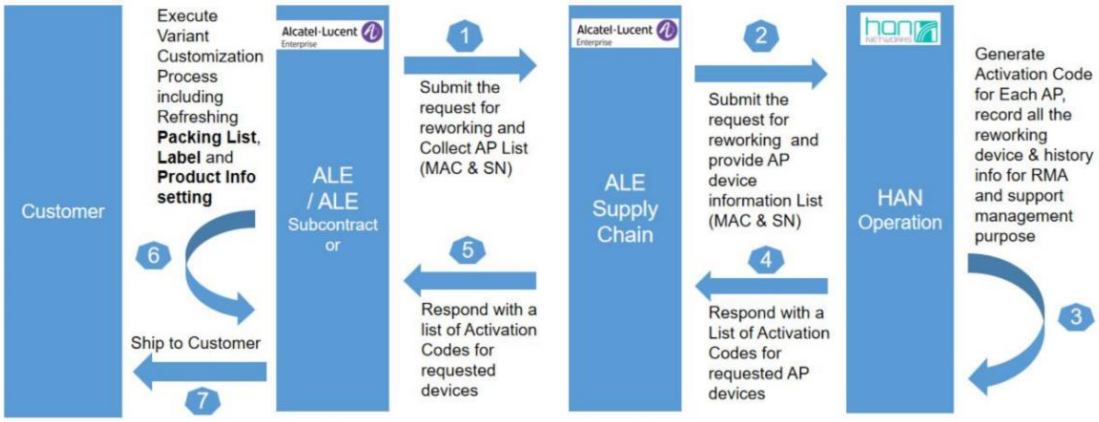
4. Check private wcf status



AP Reworking

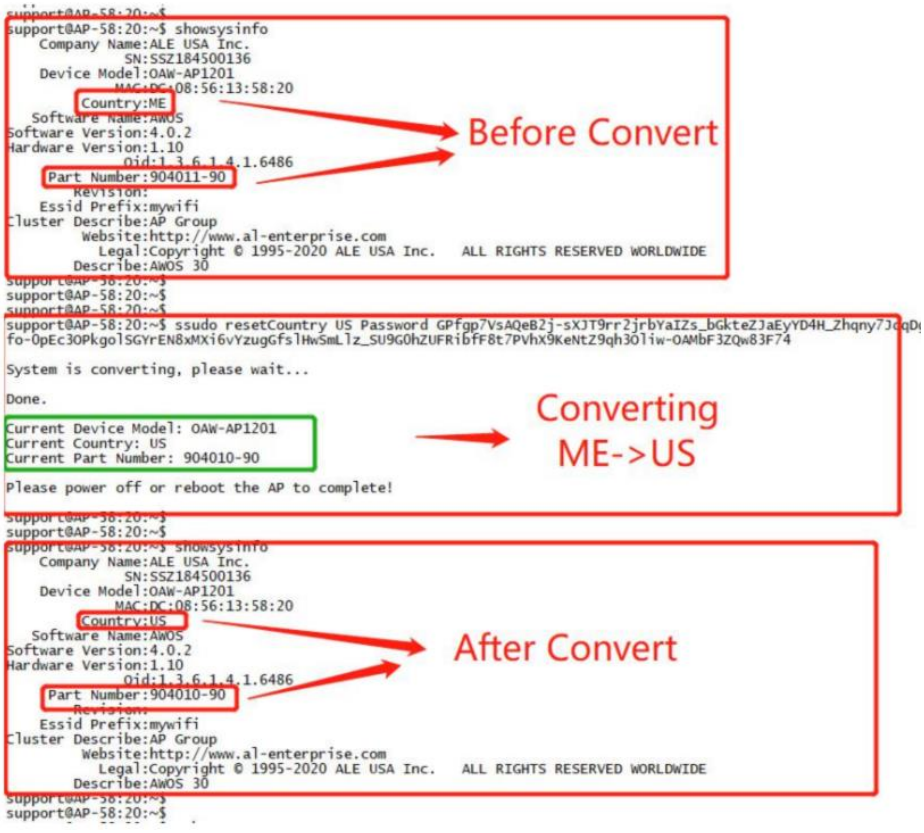
Provide variant customization requirements for ALE-branded AP. Partner must open an eSR, ALE Customer Support team will apply the procedure

1. The functional flow of AP Reworking is as follows



2. The AP side of the Reworking function is implemented as follows

Reworking Command: `ssudo resetCountry [Country] Password [ActivationCode]`

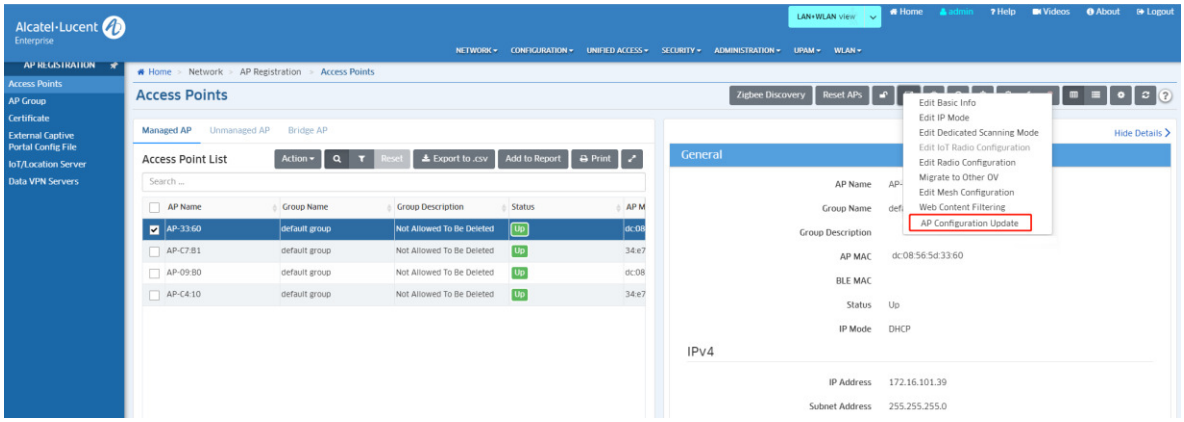


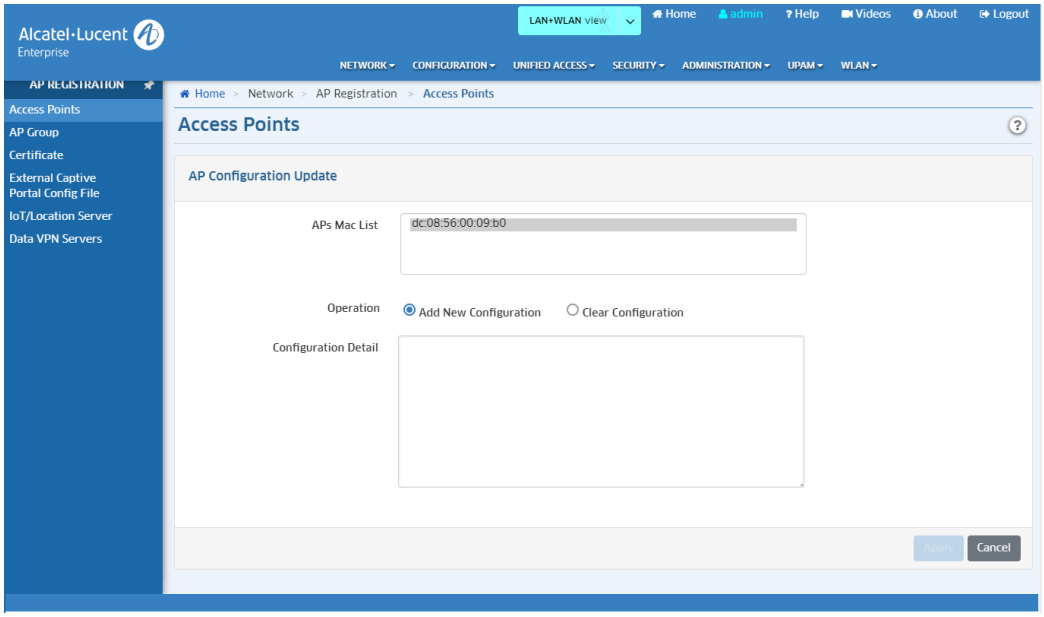
Extend Config Channel

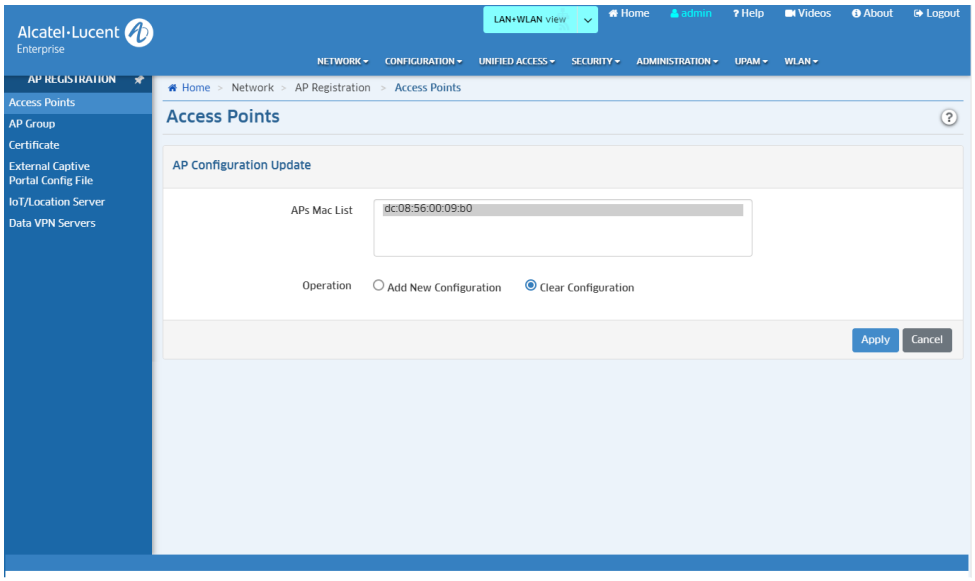
Stellar AP supports pushing new profiles to a single AP (including, but not limited to, the RF profile), AP will take effect accordingly.

It will help the support team use the new OV version to temporarily resolve customer issues before the new AP is officially released.

Here are the configuration methods:



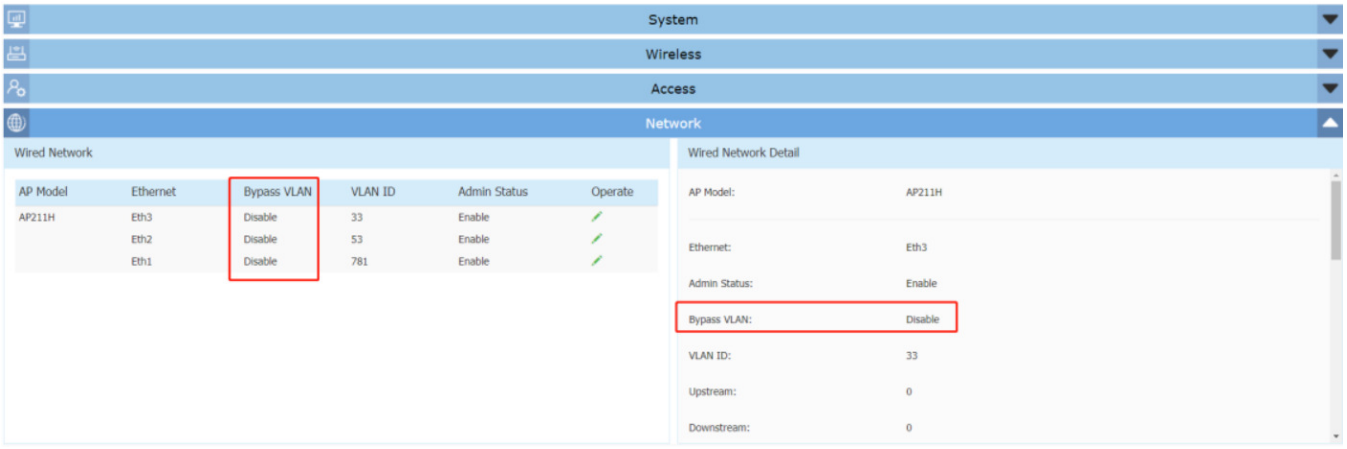




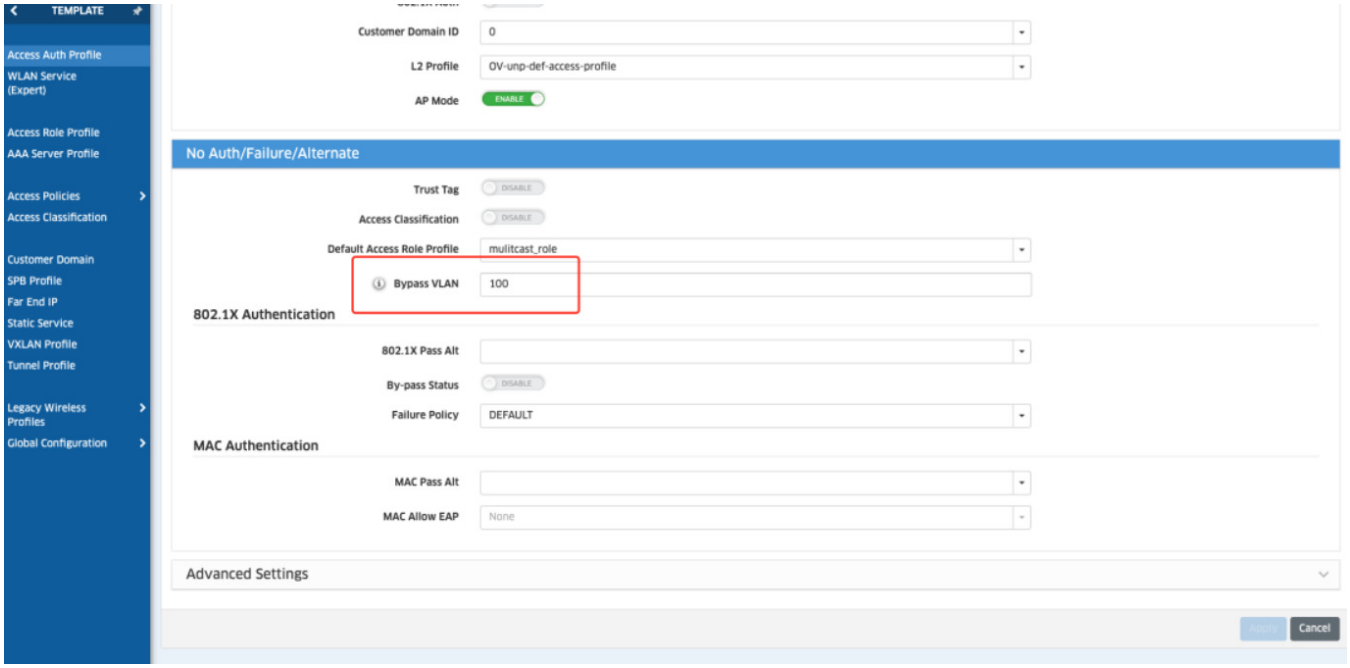
AP1201H Wired Port Multicast Optimization

Support configuration through UI pages to control whether multicast messages are forwarded by CPU to meet different application scenarios.

1. For cluster mode, the configuration and status check methods are as follows:



2. For OV mode, the configuration method is as follows



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: https://businessportal.al-enterprise.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.