Release Notes – Rev. B

OmniAccess Stellar AP

AWOS Release 4.0.4 – MR1 Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 4.0.4 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://myportal.al-enterprise.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://myportal.al-enterprise.com/.

Hardware Supported

- AP1101, AP1201, AP1220 series, AP1230 series, AP1251, AP1251-RW-B, AP1261-RW-B, AP1201H, AP1201L, AP1201HL, AP1320 series, AP1360 series, AP1201BG, AP1301, AP1301H, AP1311, AP1351

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
AP1301H Management (OVE&OVC)	
AP 802.1x Client (OVE&OVC)	Except AP1101
AP Support Preemption for Backup Radius (OVE&OVC)	All
Support for DS-Lite ISP connections at Stellar RAP(OVE&OVC)	Except AP1101
WCF Enhancement (OVE&OVC)	Except AP1101, AP1201H, AP1201HL, AP1201L, AP1261-RW-B

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 Problem Reports Between Build 4.0.4.1029 and 4.0.4.9

Notes: No customer issues reported on 4.0.4.9 (GA release dedicated to new model OAW-AP1301H), All the customer issues fixed in AWOS 4.0.3 MR4 are contained in this build.

PR	Description
Case: 00590006 ALEISSUE-1190	**Summary:** AP can't work at 802.11ax mode in Russia country code. **Explanation:** Modify AP boarddata to support 802.11ax mode in Russia country code. Click for additional information
Case: 00592179 ALEISSUE-1194	**Summary:** WiFi user can't get portal page at sometimes. **Explanation:** Sometimes when the client does not interact with the AP by sending 802.11 messages, AP cannot obtain information about the client and cannot delete the relevant access policy resulting of issue when redirecting to Captive Portal page Click for additional information

Case: 00588845 ALEISSUE-1169	**Summary:** AP send deauth to clients with reason 2 when clients disassociated with AP. **Explanation:** When AP received clients offline event, it wrongly didn't clear relevant resource, and after the client's resource timer expired AP send deauth reason 2 to this client. Click for additional information
Case: N/A ALEISSUE-1158	**Summary:** Record Syslog message after AP crashed. **Explanation:** Generate a Syslog message "`[sysreboot]: =Power Off`" after rebooting and detecting AP crash. This kind of reboot is usually observed when a LANPOWER defect is observed on switch, for OmniSwitch please ensure the capacitor-detection is disabled
Case: 00586612 ALEISSUE-1175	**Summary:** AP-1201BG management SSID not able to disable. **Explanation:** The front-end page is missing the relevant configuration, as a workaround we can add any Stellar AP model supporting Wi-Fi within the cluster, once this AP will be elected as PVM administrator can disable the Management SSID. As of AWOS 4.0.4 MR-1 if all APs models are AP1201BG we expose on the Cluster management page the possibility for deactiving the Management SSSID Click for additional information
Case: 00582383 ALEISSUE-1192	**Summary:** WiFi clients traffic are forwarded to Management VLAN **Explanation:** IP forward function is turned on in the AP, the use's broadcast traffic will be the AP's management vlan, discard such traffic on the management bridge. Click for additional information
Case: N/A ALEISSUE-1159	**Summary:** No Syslog message generated when client is added to blocklist. **Explanation:** Adding following syslog message when client's MAC Address is added in the blocklist: `<NOTICE> [AP <AP_MAC_Address>@<AP_IP_Address>] : [tid:xx] [ Add blacklist mac is <device_mac_addresss> ]`
Case: 00574007 ALEISSUE-1138	**Summary:** Vulnerability check

	Explanation: The vulnerability exists in DHCP Server service, in this release DHCP Server service is running only when this is enabled, by default, AP does not run this service. Click for additional information
Case: 00573237 ALEISSUE-1136	**Summary:** callhome_hash.json file is empty **Explanation:** Call home configuration file is found empty, it is enhanced by adding backup mechanism when previous configuration is empty, backup file will recover. Click for additional information
Case: 00571709 ALEISSUE-1131	**Summary:** Radius Shared Secret with special characters doesn't work a**fter AP reboot** **Explanation:** It is due to character '\' and ':' are not supported on AWOS 4.0.3 builds, it is solved by adding support for those characters. Click for additional information
Case: 00570454 ALEISSUE-1126	**Summary:** OmniVista does not allow backslash as PSK/Passphrase **Explanation:** It is due to character '\' and ':' are not supported on AWOS 4.0.3 builds, it is solved by adding support for those characters. Click for additional information
Case: 00564932 ALEISSUE-1106	**Summary:** Nessus scan discovered a few vulnerabilities for stellar APs. **Explanation:** Remove TLS1.0 and TLS1.1 support of MQTT broker service due to TLS1.0 and TLS1.1 is not secured Click for additional information
Case: 00544344 ALEISSUE-1017	**Summary:** RADIUS Authentication Requests are not redirected to OV/UPAM HA Active Node when back into service **Explanation:**

	Adding the support of RADIUS Server preemption, AP is checking every 5 minutes (introduced Radius Authentication Server Down timer) the status of the Radius Primary Server. Once active back, Primary Radius Server will preempt over Backup
	[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-990	Deauthentication reason 34(Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged due to AP transmissions and\/or poor channel conditions). Use the command `grep deauth /proc/kes_debug` for listing the deauthentication messages	Will be fixed in AWOS 4.0.4 MR2
ALEISSUE-1028	802.11 Frame Aggregation and Fragmentation Vulnerabilities.	Will be fixed in AWOS 4.0.4 MR2
WCF	WCF Feature is not supported when WLAN Client is running behind an HTTP Proxy	No workaround
WCF	WCF Feature is not supported when WLAN Client is using mobile applications, there is no restrictions (packets are not dropped by AP, no redirection to Restricted Web page)	No workaround
802.1x_wpa3 client connection	On OV mode, when configured enterprise with WPA3_AES, client configured with 1x_wpa3 only can't connect to this WLAN. For now, WPA3_AES is intended to satisfy WPA2 and WPA3 transition mode.	In AWOS 4.0.5, Will add one more WPA2 and WPA3 transition mode, and WPA3_AES changes to WPA3 connection only.
802.1P	802.1P downlink direction does not take effect on 11AX products.	Will be fixed on AWOS 4.0.5.
Management VLAN	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.
DPI	[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.

AP stateful ipv6 address	The ipv6 address of the dual-stack AP, AP is a stateful address. After configuring the open type of 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	Create one policy list binding and two policies, results that the user cannot access the ftp	There is no known workaround at this time.

Limitations and/or Dependencies

| Feature	AP Model	Limitations and/or Dependencies
Tagged VLAN	AP1301H	It's not supported in this release, will be supported in next AWOS 4.0.4 MR
Bypass VLAN	AP1301H	It's not supported in this release, will be supported in next AWOS 4.0.4 MR
VMM 802.1p mapping	AP1301H	It's not supported in this release, will be supported in next AWOS 4.0.4 MR
VMM DSCP mapping	AP1311/AP1301	Wireless client can not use Guest Tunnel or RAP on AP1301/AP1311 for L2GRE tunnel forwarding problem, this issue will be fixed on AWOS 404-MR2.
DPI	AP1311/AP1301/AP1301H	DPI is not supported on AP1301 & AP1311 products, it will be supported in future release.
WCF	All	1. WCF does not support http over proxy scenario. 2. WCF does not support blocking mobile applications access. Client's packets are not restricted (packet not dropped by AP, no redirection to Restricted Web Page) 3. WCF does not support RAP scenario.
RAP	All	RAP does not support tagged VLAN on the Downlink ports
HTTPs CP over proxy	All	For iOS does not support to configure URL to bypass the proxy, this function does not work on iOS devices.
AP 802.1x client	All	Wireless clients can't connect to internet on untag VLAN with AOS switch due to AOS switch treat all untag devices as 802.1x client.
Wired Port	AP1201HL	AP1201HL switches to a Group with downlink configuration, wired client cannot access it.
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	All Stellar Wi-Fi 6 AP Models	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	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 /AP1301H	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.
mDNS	AP1201H/ AP1201HL /AP1261- RW-B	AP1201H/1201HL/AP1261-RW-B 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.
Management VLAN Static IP LACP	AP1351	When configure LACP + Management VLAN + Static IP for AP1351, the network will not be reachable after AP reboot if LACP aggregated link is formed, the workaround of this issue should be disable LACP on switch side.
Link aggregation	All	Link aggregation with management VLANs has a certain probability of failure

New Software Feature Descriptions

AP 802.1x Client

This function provides a method for allowing only APs authenticated over 802.1x for trusting WLAN clients on OmniSwitch, chart blow describes the main workflow of this function.
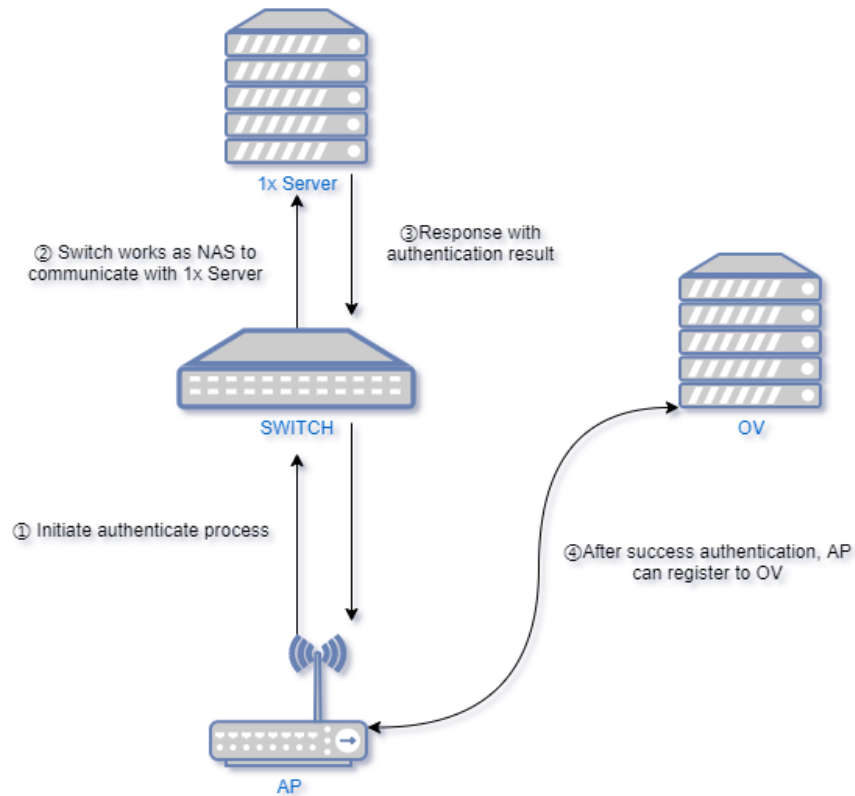
Configurations needs to be done on both AP/AP Group (thru OV management) and Switch side, for details please refer to OmniVista user guide.

AP Support for DS-Lite ISP connections at Stellar RAP

In this release, data VPN of MTU and TCPMSS are configurable, please refer to the screenshot below:

1. MTU of data VPN is configurable on OVE/OVC SSID Settings:

2. TCPMSS of data VPN is configurable on OVE/OVC Data VPN Servers settings:

3. TCPMSS of management VPN is configurable on GOV Device Catalog(freemium tenant):

VPN Settings

○ Create New VPN Settings   ● Choose Existing VPN Settings

*Choose VPN Setting	GOV-RAP ▼		
*Server's Public IP	106.38.8.234 [GOV-RAP]	*Port	2222
*Server's VPN IP	22.0.0.1		
AP's VPN IP	22.0.0.2		
*OmniVista Enterprise Server IP	192.168.40.20		
ⓘ TCPMSS	1362		

Enter TCPMSS value. Recommended value is 1362. Leave it blank if you don't prefer to set a specific value.

Client VPN IP Address Pool

● IP Range   ○ Shorthand Mask

*IP Range   22.0.0.2   -   22.0.0.20

*Subnet Mask   255.255.255.0

Encryption Keys

|	
AP's Public Key	PnYn5bC0LrBChvK1BrG20yx/5CiKE8UUA8UbxQ8v0xw=
AP's Private Key	B2vNsqI1K7Znzuy1a0fcDb2wdys+3X7ONPNTLmPzBII=
Server's Public Key	uPKa5KHxOpqehDUyIAini77MN+a8DGg37CTpilw2VT0=
Server's Private Key	r8atfeeFCBuGLQYE0ngA/pxEb7VLsU1gd0mXJGWTKJI=

WCF Enhancement

In this release, when a page is blocked by WCF, End user is notified when redirected to Restricted Web Page embedded on Stellar AP
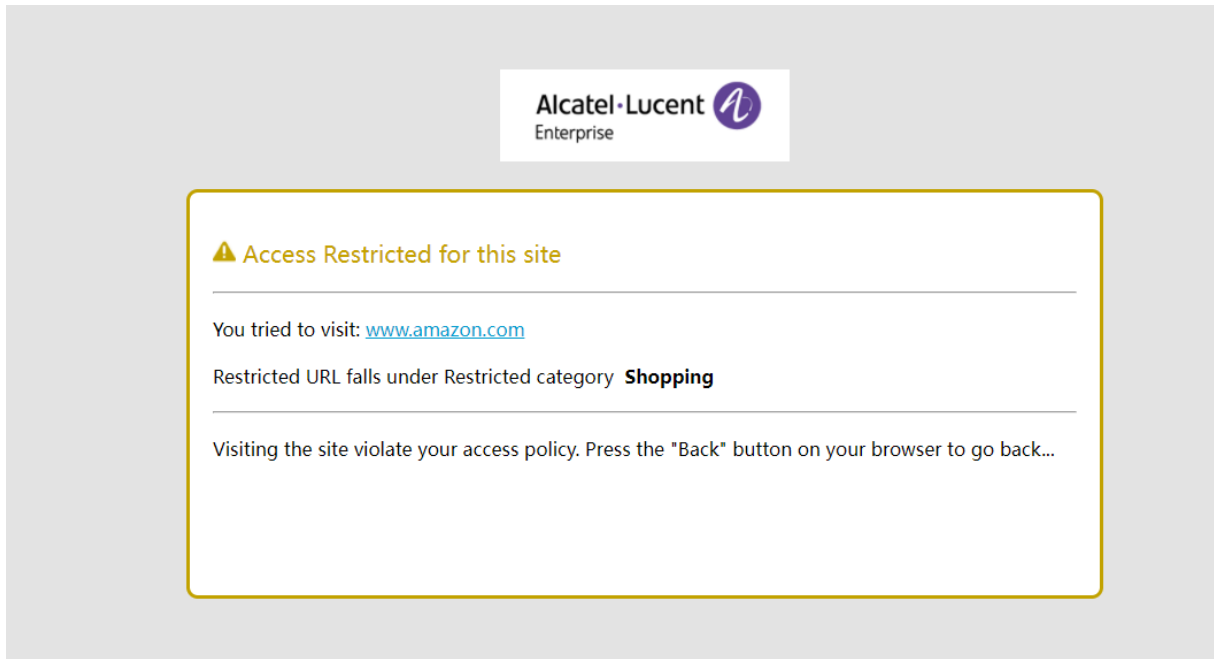
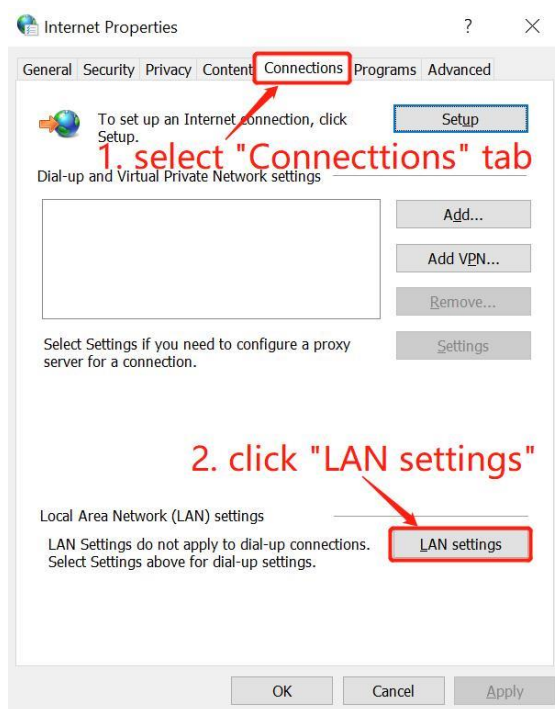## AP Support HTTPS CP Redirection over Proxy

1. Configure http/https proxy on the wireless client (Windows OS for example).

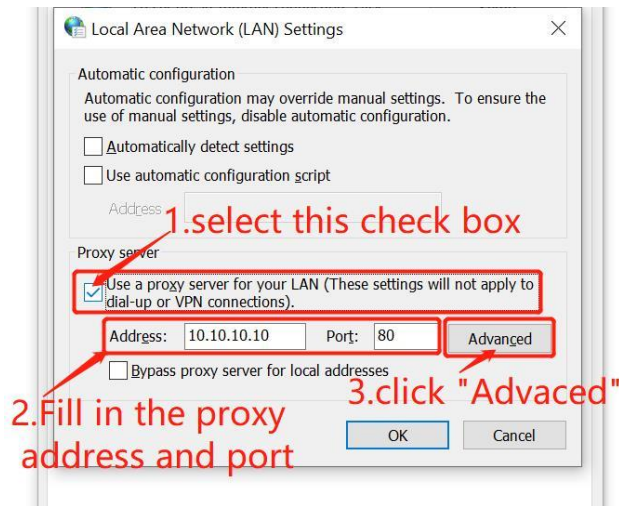1.1 Open "Control Panel"> "Network and Internet"> "Internet Options"
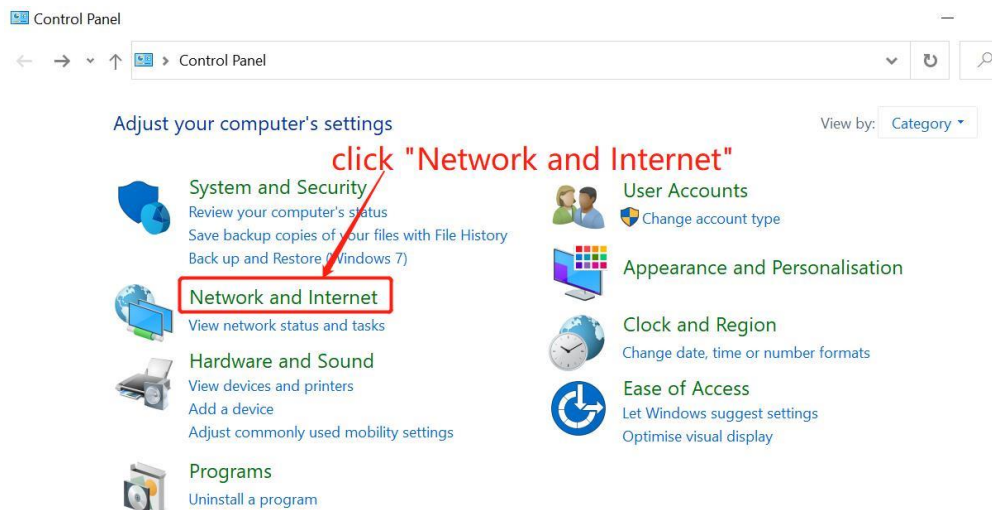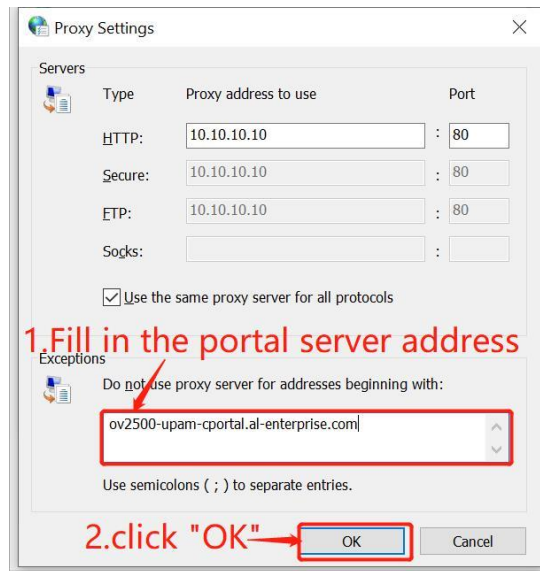
1.2 The "Internet Properties" window pops up, select the "Connections" tab, and click "LAN Settings"

1.3 The "Local Area Network (LAN) Settings" window pops up, check "Use a proxy server for your LAN", fill in the proxy server address and port, and click the "Advanced" button

1.4 The "Proxy Settings" window pops up, fill in the portal server address in "Exceptions", and click "OK"
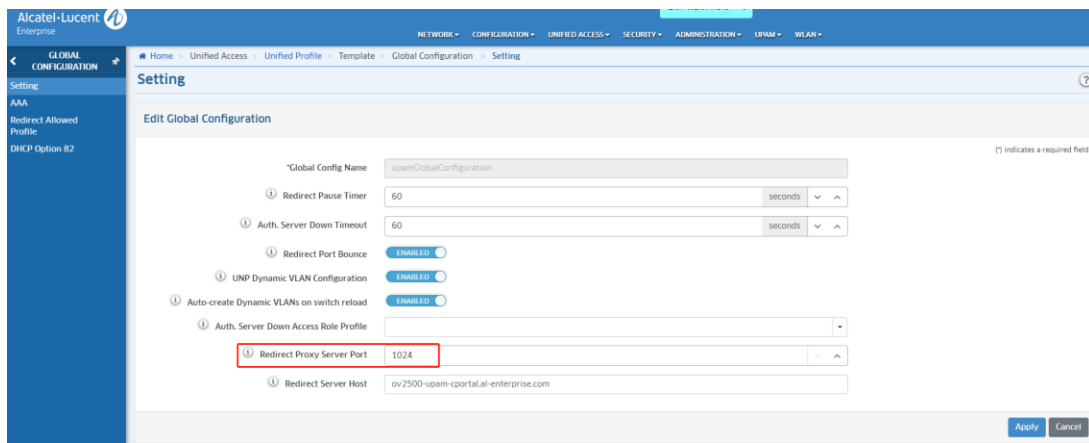

The client http/https proxy setting is complete.

2. Set the proxy port on the AP.

2.1 Log in to the OV management page and go to Home > Unified Access > Unified Profile > Template > Global Configuration > Setting。

Modify or create Global Configuration and fill in the proxy port used by the client in "Redirect Proxy Server Port".

After the modification is completed, click "apply", and then click "Apply to Devices", select the AP's group, and send it to the AP.
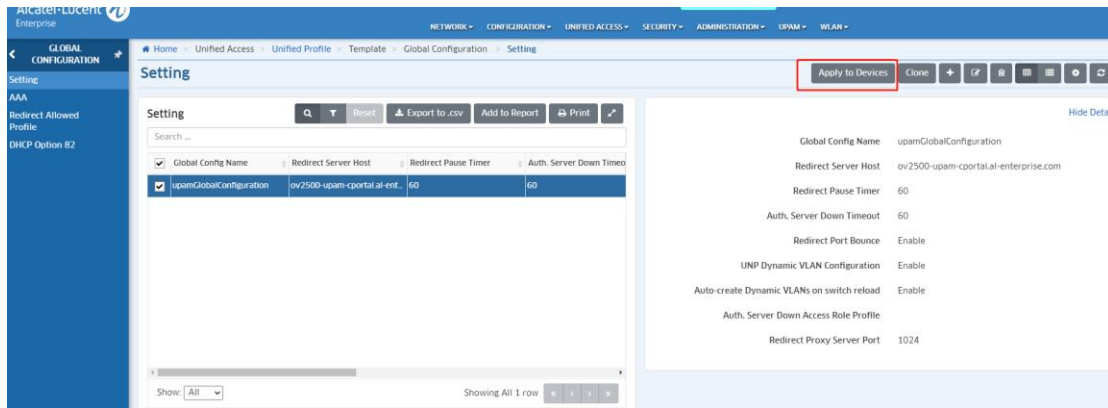
Technical Support

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://myportal.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.