

Release Notes - Rev. A

OmniAccess Stellar AP

AWOS Release 3.0.6 - GA Release

These release notes accompany the OmniAccess Stellar Operating System (AWOS) Release 3.0.6 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 | 3 |
| Hardware Supported..... | 4 |
| New Software Features and Enhancements | 4 |
| AP Supported Modes | 4 |
| Fixed field problems in build 3.0.6.28 | 5 |
| Limitations and/or Dependencies..... | 6 |
| New Software Feature Descriptions..... | 8 |
| Appendix A - Upgrade Instructions | 25 |
| Technical Support | 28 |

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, AP1220 series, AP1230 series, AP1251, AP1201H, AP1201

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 |
|---|---|
| | OmniAccess Stellar AP1101/AP1220/AP1230/AP1251/AP1201H/AP1201 |
| Range of Tx Power | All |
| Fixed Channel Width setting | All |
| Support "Collect Support Info" on Stellar APs | All |
| IPv6 Client Support | All |
| WPA3 Support | All |
| User Behavior Tracking Syslog Support | All |
| Express Cluster Scale to 255 APs | All (natively on AP1220/AP1230/AP1251) |
| Client detail roaming & RSSI history | All |
| Long Interval background-scanning | All |
| DHCP Option 82 Support | All |
| Captive Portal redirection IP | All |
| AP1201H - trust tag support on downlink ports | AP1201H |
| Radius Access Request Called-Station-ID Setting | All |
| mDNS Multicast Control | All |
| Log Improvements | All |

AP Supported Modes

Wi-Fi Express

Wi-Fi Enterprise

- OmniVista 2500
- OVCirrus

Fixed field problems in build 3.0.6.28

Note: All fixes from prior releases are included up to AWOS 3.0.5.2060

Note: OmniAccess Stellar AP reserves an SSID (On 2.4G & 5GHz band). It is used to perform background scanning for wIPS/wIDS services to alert and take preventive actions on any security threat. NO clients can connect to this SSID.

Limitations and/or Dependencies

1. Express Cluster Scale to 255 APs

Limitation:

When AP1101/AP1201H is PVC/SVC, max cluster size supported is 32.

When AP1201 is PVC/SVC, max cluster size supported is 64.

When AP1220 series, AP1230 series or AP1251 is PVC/SVC the max cluster size supported is 255.

- With mixed AP models in any cluster of size > 64, recommendation is for every 64 APs to include at least 2 APs from either AP1220 series, AP1230 series or AP1251.

2. Upgrade in Web UI

Limitation:

The upgrade input select boxes won't show up after AP has been running several days, need to refresh the upgrade page to make them show up.



| Firmware | AP Quantity | |
|----------|-------------|--------|
| 3.0.6.26 | 1 | Expand |


Upgrade Firmware

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

Image File Image File URL

← The firmware Input Select boxes not exist

Remove All Upload All

172.16.101.2 

Web Management Upgrade

Refresh the upgrade page




| AP Quantity | |
|-------------|------------------------|
| 1 | Expand |

Upgrade Firmware

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

Image File Image File URL

AP1101  After refresh, the select box show up

New Software Feature Descriptions

Range of Tx Power

The network admin with Power Setting still set as Auto, can configure a range of TX power per band (min & max). The auto power selection algorithm then selects TX power of the AP within the minimum and maximum specified.

1. Open up wireless RF configuration page

Wireless

RF 2.4GHz 5GHz

2.4GHz Channel Distribution

1

wIDS/wIPS

Rogue Suppress: off

Dynamic Blacklist: off

Wireless Attack Detection: off

Unknown AP

Interfering AP 34:E

Rogue AP

0 100 200

2. Click the green pen in desired AP item.

RF Configuration

Global: 5G Channel Width(MHz) 20 Save

| AP | 2.4GHz Channel | 2.4GHz Power(dBm) | 5GHz Channel | 5GHz Power(dBm) |
|----------|----------------|-------------------|--------------|-----------------|
| AP-91:20 | auto(1) | auto(20) | auto(52) | auto(23) |

Click Here

3. Range of Tx power can be configured for 2.4G Channel and 5G Channel. Scroll down the “Edit RF Information” window to find 2.4G Channel power box or 5G Channel power box. Enable APC, and set Auto Power Range, at last, click Save.

Set 2.4G power range:

Edit RF Information

2.4GHz

Channel

ACS: ON OFF

Channel: 11

Channel Width: 20 (MHz)

Power

1. Enable APC

APC: ON OFF

Power: 20 (3-40)dBm

Auto Power Range: 6 - 30 (3-40)dBm

2. Set Min & Max power

Set 5G power range:

Edit RF Information

5GHz

Channel

ACS: ON OFF

Channel:

Channel Width: (MHz)

Channel List:

Power

1. Enable APC

APC: ON OFF

Power: (3-40)dBm

Auto Power Range: - (3-40)dBm

2. Set Min & Max power

Save configuration:

Edit RF Information

Power

APC: ON OFF

Power: (3-40)dBm

Auto Power Range: - (3-40)dBm

Others

Short GI:

Note : The RF configuration requires 30 seconds to take effect on the AP after you click 'Save', it is not recommended to make other RF changes on this AP during this period.

Click Save

Global Fixed Channel Width Setting

It is important to have all the APs operate with channels of equal width. This is to ensure optimal user experience when roaming. The network admin in auto mode can still specify the channel width for 5GHz band. The channel selection algorithm ensures all APs configured with the same RF profile get assigned channels that abide by the configured channel width.

Enter the “RF Configuration” Page, and configure global 5g channel width.

1. Select Channel Width

2. Click to save

| AP | 2.4GHz Channel | 2.4GHz Power(dBm) | 5GHz Channel | 5GHz Power(dBm) |
|----------|----------------|-------------------|--------------|-----------------|
| AP-91:20 | auto(11) | auto(20) | auto(52) | auto(23) |

IPv6 Support

IPv6 protocol enables next generation large-scale IP networks by supporting addresses that are 128 bits long. It contains three main functions in Web UI:

1. IPv6 address of the client.
2. IPv6 based ACL for client traffic.
3. White list for IPv6 address.

The following snapshots show how they are used or configured.

1. IPv6 address of the client.

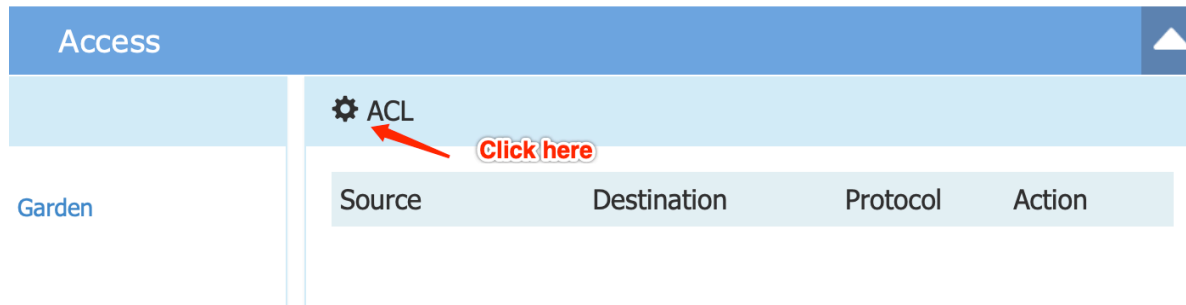
Clients For Group: AP-Group Total:2

| User Name | IP | MAC | WLAN | Auth |
|-----------|-------------------|-------------------|------------|------|
| | 172.16.101.57/... | e4:a7:a0:23:f1:ef | 152-open5g | OPEN |
| | 172.16.101.34 | e0:ac:cb:b9:1d:b6 | 152-open5g | OPEN |

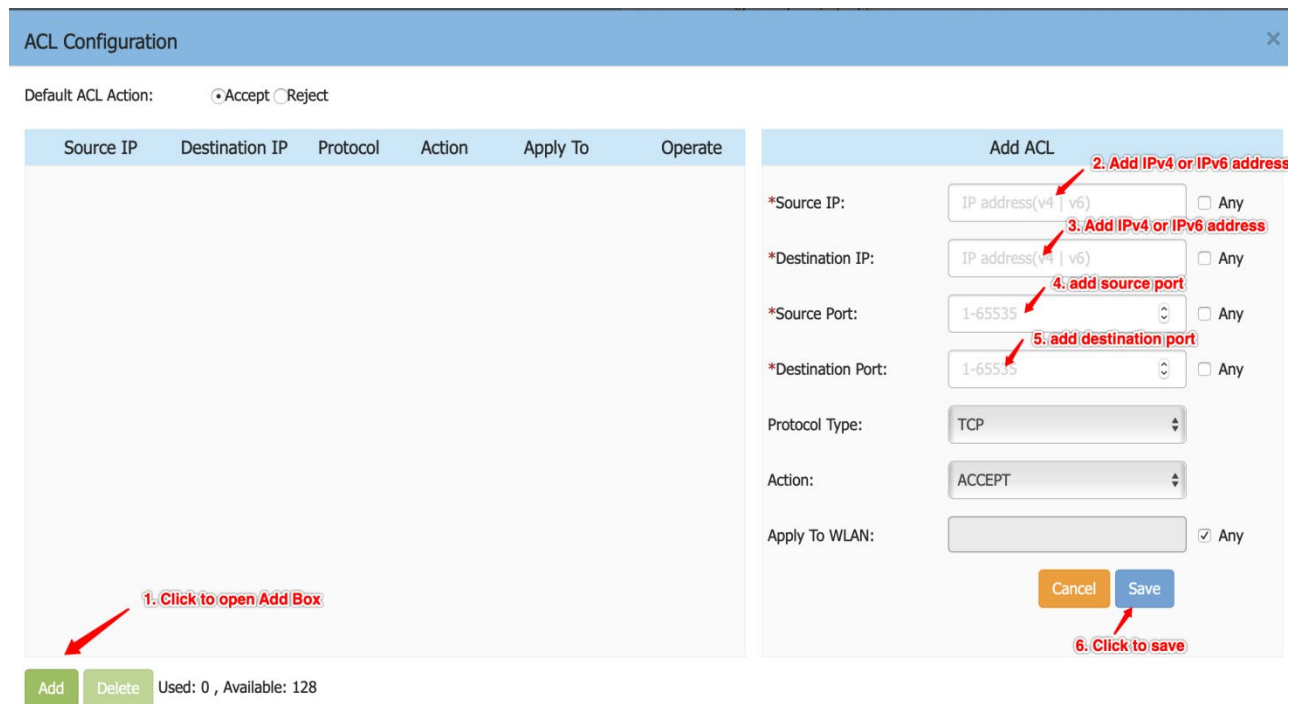
Hover mouse above, the IPv6 address can show up

2. IPv6 based ACL for client traffic.

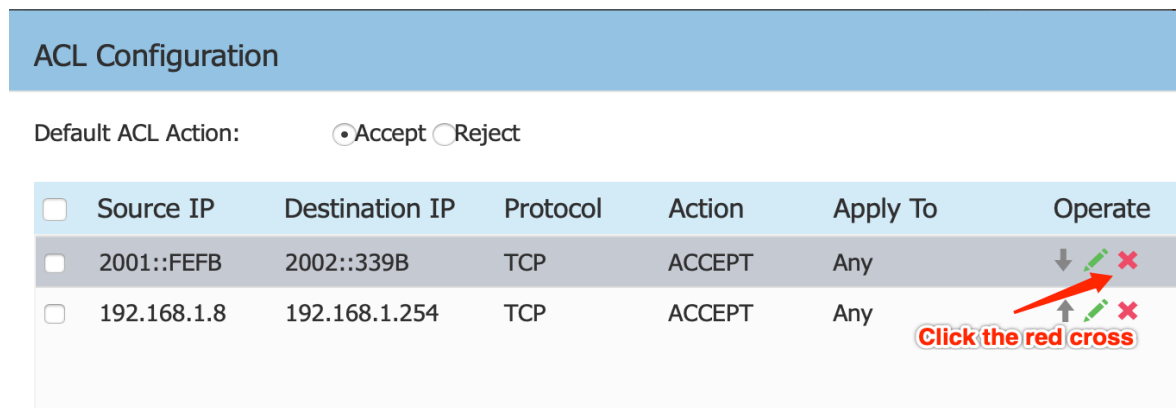
Enter ACL Configuration page:



For adding ACL rule:



For deleting single ACL rule:



For deleting group ACL rule:

ACL Configuration

Default ACL Action: Accept Reject

| <input type="checkbox"/> | Source IP | Destination IP | Protocol | Action | Apply To | Operate |
|-------------------------------------|--------------|----------------|----------|--------|----------|---------|
| <input checked="" type="checkbox"/> | 2001::FEFB | 2002::339B | TCP | ACCEPT | Any | ↓ ✓ ✗ |
| <input checked="" type="checkbox"/> | 192.168.1.8 | 192.168.1.254 | TCP | ACCEPT | Any | ↑ ↓ ✓ ✗ |
| <input type="checkbox"/> | 192.168.1.99 | 192.168.1.222 | TCP | ACCEPT | Any | ↑ ✓ ✗ |

Select which to delete

Click to delete

Add Delete Used: 3 , Available: 125

ACL Configuration

Default ACL Action: Accept Reject

| <input type="checkbox"/> | Source IP | Destination IP | Protocol | Action | Apply To | Operate |
|--------------------------|--------------|----------------|----------|--------|----------|---------|
| <input type="checkbox"/> | 2001::FEFB | 2002::339B | TCP | ACCEPT | Any | ↓ ✓ ✗ |
| <input type="checkbox"/> | 192.168.1.8 | 192.168.1.254 | TCP | ACCEPT | Any | ↑ ↓ ✓ ✗ |
| <input type="checkbox"/> | 192.168.1.99 | 192.168.1.222 | TCP | ACCEPT | Any | ↑ ✓ ✗ |

Click here to select all

Click to delete

Add Delete Used: 3 , Available: 125

3. White list for IPv6 address

For adding walled garden item:

Access

Black List & White List

Black List **White List** **Walled Garden**

Multicast Control

1 Click here

IP **Operate**

Domain: IP:

Starting IP:

Ending IP:

Add

Click to Add

Select IP

Input v4 or v6 address

Input v4 or v6 address

For deleting walled garden item:

Black List & White List

Black List **White List** **Walled Garden**

Multicast Control

IP **Operate**

1110::2233-1110::4455 **×**

192.168.1.8-192.168.1.233 **×**

Click the red cross to delete

Domain: IP:

Starting IP:

Ending IP:

Add

WPA3 Support

Security is a concern for any network admin but with wireless being the primary method to access the network, enhanced Wi-Fi security becomes a very critical requirement. With the changing threat landscape, the Wi-Fi Alliance® announced new security enhancements for Wi-Fi Protected Access. These new enhancements are released under the WPA3 umbrella, all aiming at better protecting Wi-Fi communications. Also of important note is WPA3 is backward compatible with WPA2.

1. WPA3-Personal

It will utilize Simultaneous Authentication of Equals as defined in the IEEE 802.11-2016 standard. With SAE, the user experience is the same (choose a passphrase, use it to connect), but SAE automatically adds a step to the “handshake” that makes brute force attacks ineffective. With SAE, the passphrase is never exposed, making it impossible for an attacker to find the passphrase through brute force dictionary attacks. The other added benefit of WPA3-Personal is that Protected Management Frames (PMF) are required to be utilized for all WPA3 personal connections. In the past PMF was an optional capability that was left up to the user to enable. With WPA3, PMF must be negotiated for all WPA3 connections providing an additional layer of protection from de-authentication and disassociation attacks. (Mandatory)

2. WPA3-Enterprise

Within the enterprise, one of the subtle changes that will be evident to end users is in keeping in line with the WPA3 goal for PMF to be enabled and negotiated for all WPA3 connections. WPA3 also introduces a 192-bit cryptographic security suite B.

When create WLAN, the WPA3 is supported for Personal and Enterprise mode.

Enter WLAN Configuration page:

| WLAN | | | |
|------------|--------|------------|--|
| Enable: 3 | | Disable... | |
| WLAN Name | Status | Clients | |
| 1212 | off | 0 | |
| xin | on | 0 | |
| 1111test | on | 0 | |
| 152-open5g | on | 1 | |

New

Enable WPA3 for Personal WLAN:

WLAN Configuration

| WLAN Name | Status | Security Level | Captive Portal | Operate |
|------------|--------|----------------|----------------|---------|
| 152-open5g | Enable | Open | Disable | WMM |

1 Click to open Create window

Create New WLAN

WLAN Name:

Security Level: 2 Select Personal

Key Management: 3 Select wpa3-personal

Password Format:

Password:

Confirm:

Inactivity Timeout Status: **off**

Inactivity Timeout Interval:

Enable WPA3 for Enterprise WLAN:

WLAN Configuration

| WLAN Name | Status | Security Level | Captive Portal | Operate |
|------------|--------|----------------|----------------|---------|
| 152-open5g | Enable | Open | Disable | WMM |

1 Click to open Create window

Create New WLAN

WLAN Name:

Security Level: 2 Select Enterprise

Key Management: 3 Select wpa3-enterprise

CNSA:

AuthServer:

AuthPort:

AuthSecret:

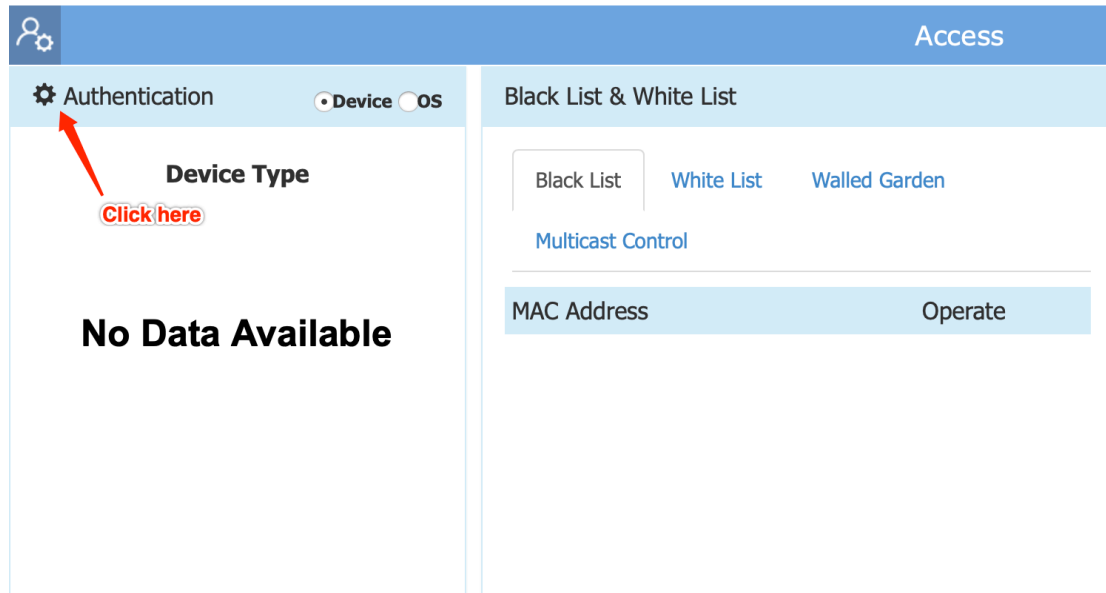
Nas Identifier:

Radius Accounting:

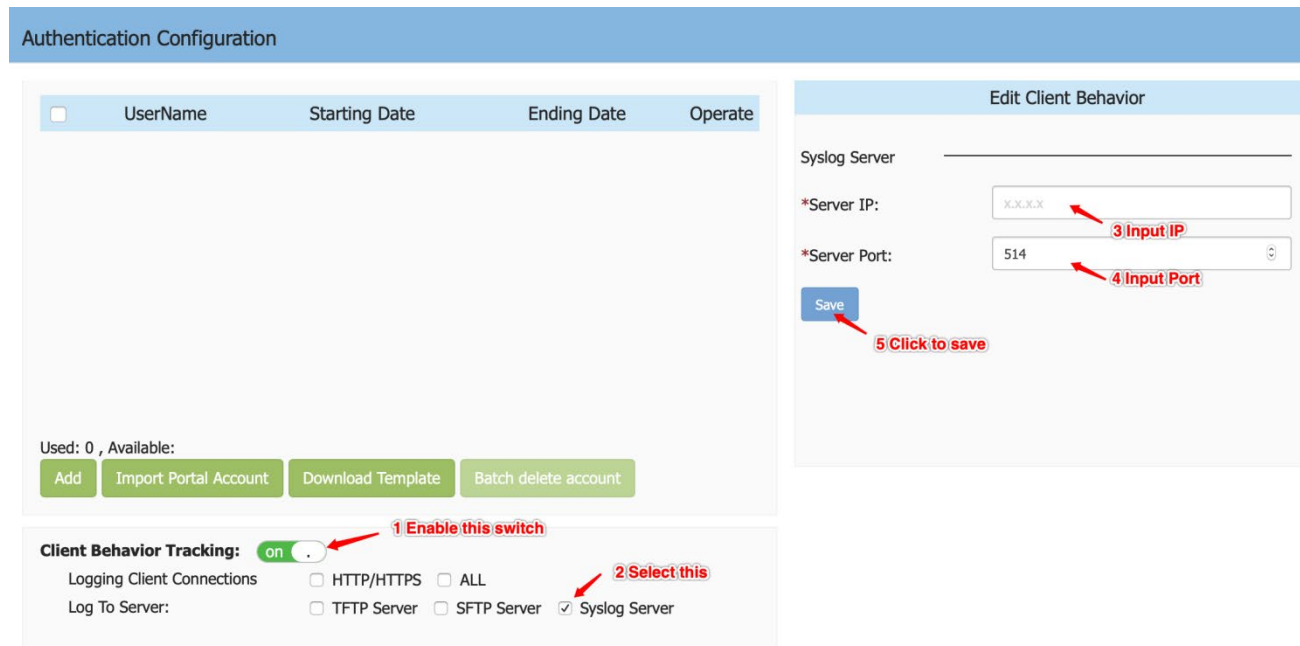
User Behavior Tracking Syslog Support

UCOPIA requires that the AP must send the client behavior message via syslog.

Enter Authentication Configuration page:



Scroll down to find “Client Behavior Tracking”:



Client Detail Roaming & RSSI History

Now one can easily trace clients roaming behavior and connectivity QoE. For each client/AP association we should maintain a record with “AP Name, AP MAC, Association time, VLAN, min RSSI, min RSSI time recorded, max RSSI time recorded, and Avg RSSI).

Now one can see days of roaming & RSSI historical information. Each block represents roaming during active session period. For each roaming occurrence we record Roaming AP, Association Time, Band, RSSI.

Enter “Clients Information” page:

| Clients | | | | |
|---------------------|----------------|-------------------|------------|------|
| For Group: AP-Group | | Total:2 | | |
| User Name | IP | MAC | WLAN | Auth |
| | 172.16.101.34 | e0:ac:cb:b9:1d:b6 | 152-open5g | OPEN |
| | 172.16.101.106 | 38:f9:d3:de:10:e8 | 152-open5g | OPEN |

Show the roaming history:

Clients Information

| User Name | IP | MAC | WLAN | Access Point | |
|----------------|-------------------|------------|----------|--------------|--|
| 172.16.101.34 | e0:ac:cb:b9:1d:b6 | 152-open5g | AP-91:20 | | |
| 172.16.101.106 | 38:f9:d3:de:10:e8 | 152-open5g | AP-91:20 | | |

1 Click to select specified AP

Client Detail

Attached Band: 5G

Online Time: 1 m 48 s

RSSI: 40

Working Mode: 11AC_VHT80

PHY Rx rate: 234.00Mbps

PHY Tx rate: 650.00Mbps

Rx rate: 0.00Mbps

Tx rate: 0.00Mbps

Download: 165kB

Upload: 130kB

Device Type: Unknown

OS Type: Unknown

Rx Error: 0

Tx Retry: 38

Roaming History

2 Click the + button

Scroll to see the full roaming history:

The screenshot shows a web interface for 'Clients Information'. On the left is a table with columns: User Name, IP, MAC, WLAN, Access Point, and icons for delete and refresh. Two rows are visible, both with IP addresses starting with 172.16.101. On the right is a 'Client Detail' sidebar with a 'Roaming History' section. This section contains two sessions, each with details like Associated SSID (152-open5g), AP (AP-91:20), Associated Time, Band (5GHz), RSSI (49), and Status (Online). A red box highlights the Roaming History section.

| User Name | IP | MAC | WLAN | Access Point |
|-----------|----------------|-------------------|------------|--------------|
| | 172.16.101.34 | e0:ac:cb:b9:1d:b6 | 152-open5g | AP-91:20 |
| | 172.16.101.106 | 38:f9:d3:de:10:e8 | 152-open5g | AP-91:20 |

Long Interval Background-scanning

Some environments, such as healthcare, have health monitoring equipment which has very low thresholds for packet loss over time.

By default, background scanning runs every 10 seconds for a duration of up to 110ms. During background scanning clients traffic is not served. The health telemetry monitors transport the data as UDP, so there is no retransmission. In such environments configuring a Long Interval is required.

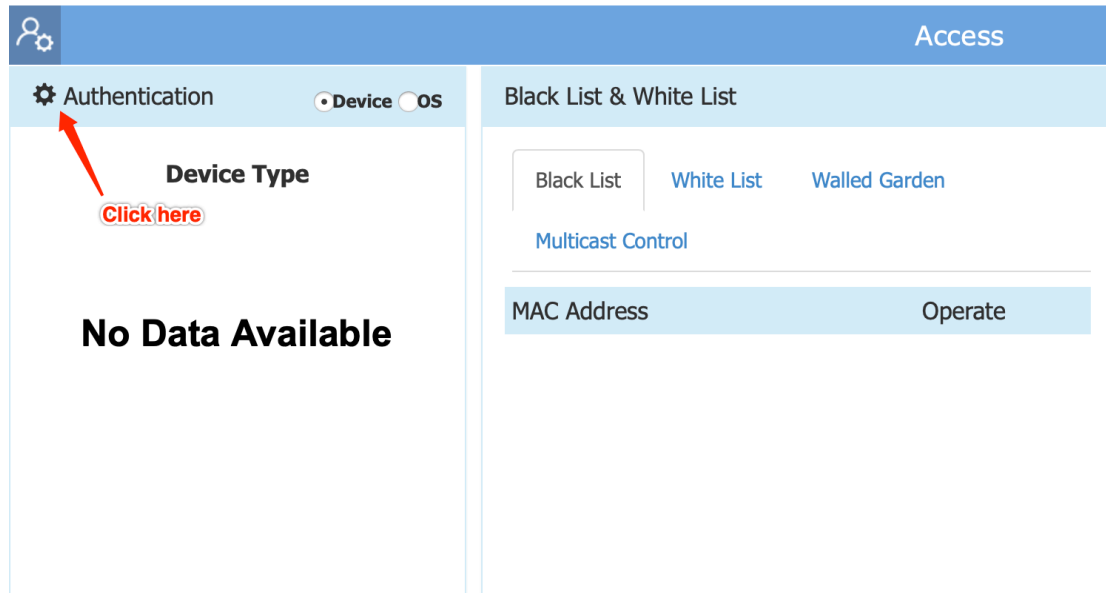
AP can configure at most 3 hours in minutes. Check below:

The screenshot shows the 'Wireless' configuration page. The 'wIDS/wIPS' section has three toggle switches for 'Rogue Suppress', 'Dynamic Blacklist', and 'Wireless Attack Detection', all set to 'off'. An arrow labeled '1 Click here' points to the 'Wireless' header. The 'Performance Optimization' section has a 'Background Scanning' toggle set to 'on'. Below it, the 'Scanning Interval' is set to 0 minutes and 10 seconds. A red box highlights the 'Scanning Interval' label. Arrows labeled '2 set minutes', '3 set seconds', and '4 click to save' point to the respective input fields and the 'save' button. The 'Scanning Duration' is set to 110ms on a scale from 20 to 110.

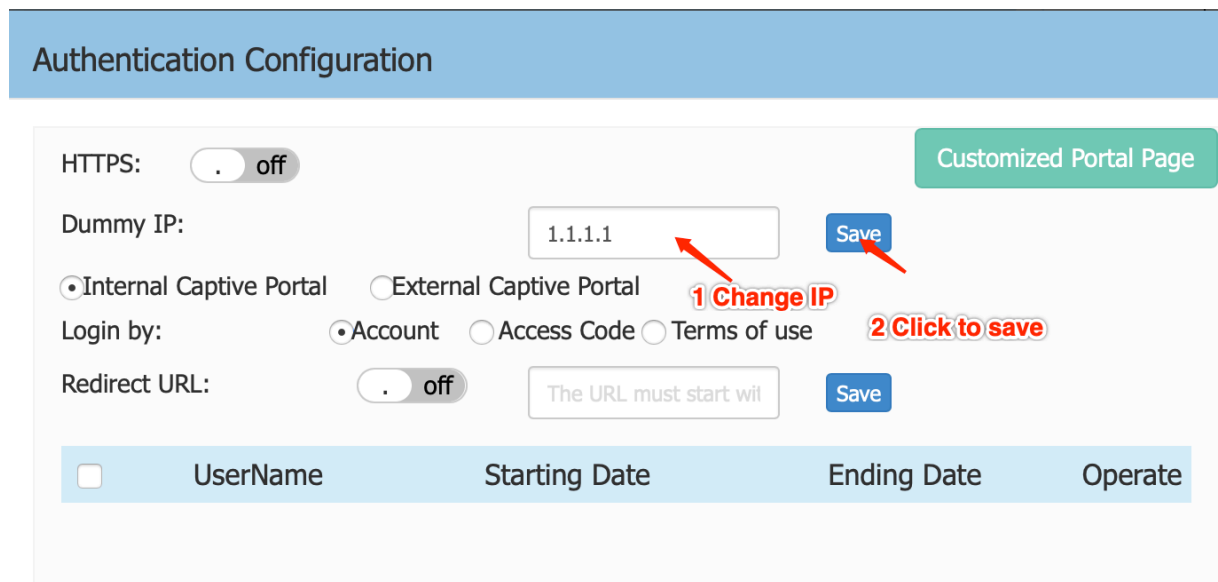
Captive Portal Redirection IP

Internal IP address used for portal redirection can be configured.

Enter Authentication Configuration page:



Set the Dummy IP:



AP1201H - Trust Tag Support on Downlink Ports

This feature now allows reception of tagged traffic on downlink port of AP1201H.

| AP Model | Ethernet | VLAN ID | Admin Status | Operate |
|-------------|----------|---------|--------------|---------|
| OAW-AP1201H | Eth3 | | Enable | |
| | Eth2 | | Enable | |
| | Eth1 | | Enable | |

Wired Network Configuration

AP Model: OAW-AP1201H

Ethernet: Eth2

Admin Status: on

VLAN ID: (0,2-4090)

Upstream: (0-1024000)kbps

Downstream: (0-1024000)kbps

Tagged Vlan: (2-4090)

Buttons: Cancel, Save

Radius Access Request Called-Station-ID Setting

By default the Radius Access Request fills the Called-Station-ID field with AP-MAC:Location. However, UCOPIA which supports multizone portal/authentication & DHCP services can use this field to identify a zone.

Allow optional Per AP Group advanced setting string up to 64 bytes.

Enter Authentication Configuration page:

Authentication Device OS

Device Type [Click here](#)

No Data Available

Black List & White List

Black List White List Walled Garden

Multicast Control

| MAC Address | Operate |
|-------------|---------|
|-------------|---------|

Scroll Down to bottom, and set the Called-Station-ID:

Authentication Configuration

| <input type="checkbox"/> | UserName | Starting Date | Ending Date | Operate |
|--------------------------|----------|---------------|-------------|---------|
| | | | | |

Used: 0 , Available:

AddImport Portal AccountDownload TemplateBatch delete account

Client Behavior Tracking: on

Logging Client Connections HTTP/HTTPS ALL

Log To Server: TFTP Server SFTP Server Syslog Server

RADIUS Setting:

Called-Station-ID:

Save

1 input Called-Station-ID

2 Click to save

mDNS Multicast Control

mDNS multicast traffic source from wired network (switch ports) towards AP can be controlled. When enabled, only traffic from the configured multicast source in the white list can be forwarded by AP to the clients connecting to it.

Maximum 8 items of multicast white list are supported.

When Multicast White List is disabled, the mDNS multicast traffic is forwarded without conditions.

AP can recognize mDNS packets and drop or transfer them according to configured rule.

For adding multicast white list:

1 Click here

2 Click here

3 Enable this switch

4 Input mac

5 Click to add

| Multicast Type | Destination IP | Source MAC | Operate |
|----------------|----------------|-------------------|---------|
| mDNS | 224.0.0.251 | 11:22:33:44:55:60 | ✘ |

For deleting multicast white list:

Click the red cross to delete

| Multicast Type | Destination IP | Source MAC | Operate |
|----------------|----------------|-------------------|---------|
| mDNS | 224.0.0.251 | 11:22:33:44:55:60 | ✘ |

Log Improvement

Three aspects of logging have been improved:

1. Split the logs based on Group.
2. More granular user debug logs.
3. More logs related to the ACS and APS.

Set syslog group level.

Note that: Ap-Debug used to control the global syslog level. E.g. If Ap-Debug's level is Notice, the left groups' syslog whose level lower than Notice (Debug, Info) cannot show up.

The screenshot shows the 'System' configuration page. The 'System Time' section is on the left, and the 'Syslog & SNMP' section is on the right. The 'Syslog & SNMP' section has a red box around the 'Log Level' dropdowns. Annotations include: '1 Click here' pointing to the 'System' header, '2 Click here' pointing to the 'Syslog & SNMP' header, '3 Set group level' pointing to the 'Log Level' dropdowns, and '4 Click to save' pointing to the 'Save' button.

System 1 Click here

System Time

Date and Time: Wed Jun 19 2019 04:16:34 ✎

Daylight-Saving Time: off

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

NTP Server List:

| | |
|---------------------|-------|
| pool.ntp.org | ↓ × |
| cn.pool.ntp.org | ↑ ↓ × |
| tw.pool.ntp.org | ↑ ↓ × |
| 0.asia.pool.ntp.org | ↑ ↓ × |
| 1.asia.pool.ntp.org | ↑ × |

NTP Server: Add

Syslog & SNMP 2 Click here

Log Level:

Ap-Debug: Notice ▾

System: Debug/ALL ▾

Security: Debug/ALL ▾

Wireless: Debug/ALL ▾

Network: Debug/ALL ▾

User: Debug/ALL ▾

3 Set group level

4 Click to save

Save

Log Remote: off Run

Log File: AP-91:20 ▾ Download

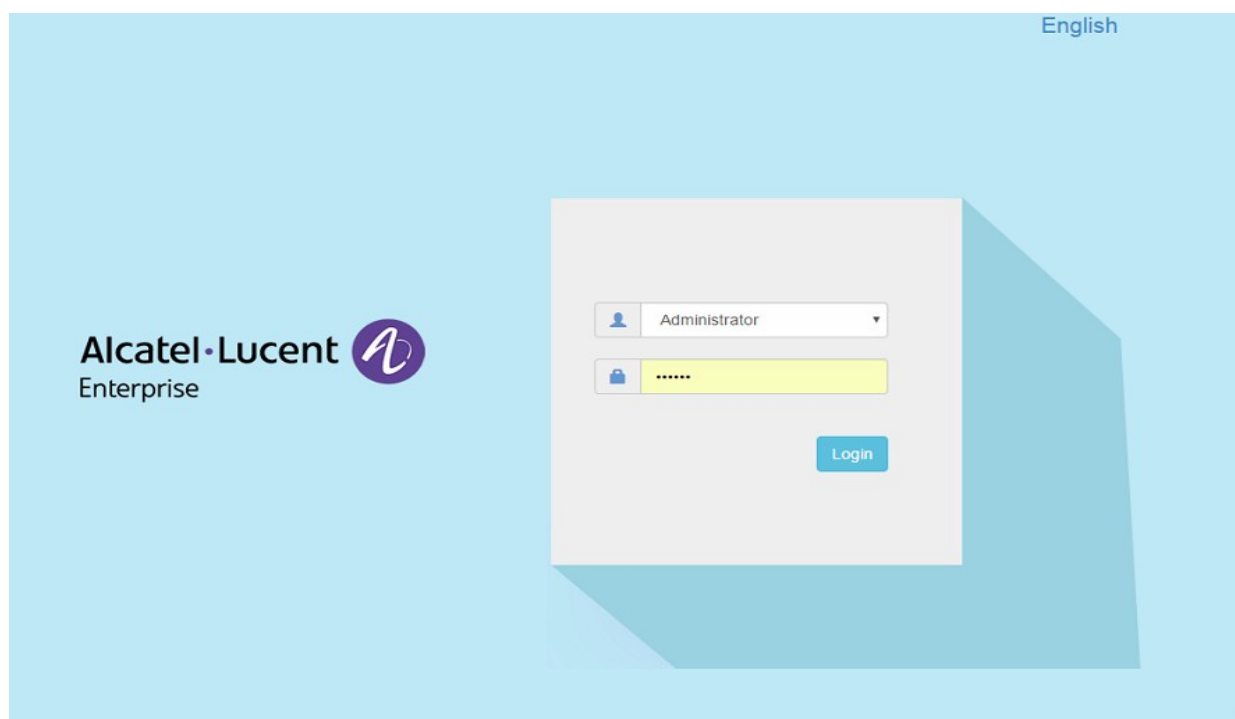
Appendix A - Upgrade Instructions

Mandatory Upgrade of the OAW-AP1101

Release 2.1 is not compatible with Release 3.0. All the Stellar AP1101 APs running R2.1 MUST be upgraded to the latest software release version available from customer support so that all the APs can form a cluster with release 3.0 or can be managed by OmniVista. Please Visit <https://businessportal2.alcatel-lucent.com> to get the latest software and follow the upgrade instructions below.

General Software Upgrade Instructions (WiFi Express)

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



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

The screenshot shows the Alcatel-Lucent Enterprise management interface. At the top left, the logo and 'Enterprise' text are visible. The main navigation bar includes 'WLAN', 'AP', and 'Monitoring' tabs. The 'AP' tab is selected, and a red arrow points to it with the text 'Click here to open AP configuration page'. Below the tabs, there are several panels: 'WLAN' with status controls, 'Clients' with a table, and 'Monitoring' with four charts showing throughput, client distribution, and wireless client health. At the bottom, there are three expandable sections: 'System', 'Wireless', and 'Access'.

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

The screenshot shows the 'AP Configuration' page. It features a table of APs with columns for Primary Name, IP, Firmware, and Operate. The table lists AP-1A:10, AP-42:20, and AP-DD:50. To the right of the table is a 'Detailed Information' panel for AP-1A:10, showing fields like AP Name, MAC, Location, Status, Role in Group, Serial Number, Model, Firmware, Upgrade Time, and Upgrade Flag. At the bottom of the page, there is a row of buttons: 'Reboot All AP', 'Clear All Configuration', 'Backup All Configuration', 'Restore All Configuration', 'Upgrade All Firmware', 'Connect To Cloud', and 'Convert To Enterprise'. A red arrow points to the 'Upgrade All Firmware' button with the text 'Click here to upgrade'.

| Primary Name | IP | Firmware | Operate |
|-------------------|---------------------------|------------|---------|
| PVC | | | |
| AP-1A:10 | 192.168.20.119(AP) (M) | 3.0.5.23 | |
| SVC | | | |
| AP-42:20 | 192.168.20.111 | 3.0.5.27 | |
| MEMBER | | | |
| AP-DD:50 | 192.168.20.128 | 3.0.5.6 | |
| Joining | | | |
| Pending | | | |
| Neighboring Group | | | |
| AP-32:30 | 192.168.20.237 | 3.0.4.2052 | |

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

Multi-model Upgrade

| Model | Firmware | AP Quantity | |
|--------|----------|-------------|--------|
| AP1250 | 3.0.5.23 | 1 | Expand |
| AP1101 | 3.0.5.6 | 1 | Expand |
| AP1220 | 3.0.5.27 | 1 | Expand |

Upgrade Firmware

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

Image File Image File URL

AP1101 **1. Select corresponding AP model and upload right image**
 No file chosen

AP1220
 No file chosen

AP1250 **2. Then upload all here**
 No file chosen

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://businessportal2.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.