Alcatel-Lucent Enterprise OmniAccess® Stellar WLAN GOLDEN RFP

Alcatel·Lucent
Enterprise

Release Version	Date	Comments
4.0.1	November 2020	Release sync with AWOS4.0.1.44, OVE 4.5R2, and OVC 4.5.2
4.0.3	January 2022	Release sync with AWOS 4.0.3.2054, OVE 4.6R2, and OVC 4.6R2 “large deployment” or “Cloud deployment” for any deployment (single or multi-site) with Centralized Management.
4.0.5	November 2022	Release sync with AWOS 4.0.5.23, OVE 4.7R1, and OVC 4.7R1 AP1451 Wi-Fi 6E access point
4.0.7	November 2023	Release sync with AWOS 4.0.7.1019, OVC 10.4.1, OVE/OVC 4.8R1 AP1411 Wi-Fi 6E access point AP1431 Wi-Fi 6E access point
5.0.1	November 2024	Release sync with AWOS 5.0.1.27, OVC 10.4.3, OVE/OVC 4.9R2 AP1511 Wi-Fi 7 access point AP1521 Wi-Fi 7 access point

Alcatel·Lucent Enterprise

Contents

Figures

Tables

1. Introduction

Omnivista Cirrus 10 is designed for Stellar XL/multi-tenant cloud deployments in *Enterprise Mode*. Omnivista Cirrus 10.3 and its further versions represent the first releases that provide native SaaS cloud-based management and advanced monitoring for Stellar access points, complete with easy-to-read dashboard displays.

This document outlines various "Cloud deployment" scenarios for XL/multi-tenant deployments supported by Omnivista Cirrus 10 SaaS cloud solution. These deployments are described in a dedicated section for Omnivista Cirrus 10. Otherwise all supported Stellar features in *Enterprise Mode* are described through Omnivista 2500 NMS or Omnivista Cirrus 4 menus.

This edition introduces the OmniAccess Stellar Wi-Fi 7 AP1511 and AP1521 access points in *Enterprise mode* with OmniVista Cirrus 10.4.3, OmniVista Cirrus and Omnivista 2500 NMS 4.9.2, and AWOS version 5.0.1.

2. Solution & Architecture Overview

1.	The wireless LAN solution shall be based on IEEE 802.11 and shall be WFA certified for Data and Voice.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess® Stellar WLAN Access Points are Wi-Fi Alliance® certified for 802.11a/b/g/n/ac/ax/be and for extended implementation of 802.11ax to 6GHz band and for Multilink Operation (MLO) across the 2.4/5/6 GHz bands with the 802.11be standard, ensuring interoperability with other 802.11a/b/g/n/ac/ax products. The Alcatel-Lucent Enterprise OmniAccess® Stellar WLAN solution is also WFA 802.11e WMM certified, ensuring proper prioritization of real-time voice and audio/video traffic and applications.

Alcatel-Lucent Enterprise proposes standard-based only products and solutions and will continue to pursue Wi-Fi certification as new products and standards arise:

- IEEE 802.11a/b/g/n/ac/ax/be
- 2.4 GHz Spectrum Capabilities
- 5 GHz Spectrum Capabilities
- 6 GHz Spectrum Capabilities
- Wi-Fi CERTIFIED 6®
- Wi-Fi CERTIFIED 7™
- WMM®
- Wi-Fi Agile Multiband™
- Wi-Fi Vantage™

- Passpoint® release 3
- WPA, WPA2 & WPA3™-Enterprise
- Spectrum & Regulatory

By supporting a solution based on open standards, certifications, and a device-agnostic approach, Alcatel-Lucent Enterprise can ensure support for the heterogeneous set of mobile device types common to all environments. Learn more about Wi-Fi certifications at: www.wi-fi.org/certification/programs

AP1101	802.11ac wave1	Certificate-WFA6831 2-OAW-AP1101.pdf
AP1201	802.11ac wave2	Certificate-WFA8006 1-OAW-AP1201.pdf
AP1201H	802.11ac wave2	Certificate-WFA7830 0-OAW-1201H.pdf
AP1220	802.11ac wave2	Certificate-WFA7333 1-OAW-AP1221.pdf Certificate-WFA7333 5-OAW-AP1222.pdf
AP1230	802.11ac wave2	Certificate-WFA7426 3-OAW-AP1231.pdf Certificate-WFA7426 4-OAW-AP1232.pdf
AP1251	802.11ac wave2	Certificate-WFA7406 1-OAW-AP1251.pdf
AP1311	802.11ax	Certificate-WFA1091 88-OAW-AP1311.pdf
AP1320	802.11ax	Certificate-WFA9731 1-OAW-AP1321.pdf Certificate-WFA9731 0-OAW-AP1322.pdf
AP1360	802.11ax	Certificate-WFA9730 7-OAW-AP1361.pdf Certificate-WFA9730 9-OAW-AP1361D.pdf Certificate-WFA9730 8-OAW-AP1362.pdf
AP1301	802.11ax	Certificate-WFA1091 89-OAW-AP1301.pdf

AP1301H	802.11ax	Certificate-WFA116640-OAW-1301H.pdf
AP1331	802.11ax	Certificate-WFA117761-OAW-AP1331.pdf
AP1351	802.11ax	Certificate-WFA114310-OAW-AP1351.pdf
AP1261	802.11ac	Certificate-WFA122372-OAW-AP1261.pdf
AP1451	802.11ax	Certificate-WFA121231-OAW-AP1451.pdf
AP1411	802.11ax	WFA128051 (OAWAP1411).pdf
AP1431	802.11ax	WFA128049 (OAWAP1431).pdf
AP1521	802.11be	WFA132830 (OAWAP1521).pdf

2.	The wireless LAN solution shall propose a distributed control function (no centralized controller) with native support for redundancy, elimination of traffic bottlenecks, and lowered latency.	C/PC/NC

The OmniAccess Stellar WLAN solution relies on a distributed control architecture that provides all the functions of a centralized controller and eliminates architecture complexity, single points of failure, traffic bottlenecks, latency, and high operational costs.
Eliminating the previously required controller from wireless deployment architectures offers many potential benefits to organizations and their IT departments:

Lower CapEx
Controller-based architectures involve high upfront capital expenses. They also involve high licensing and maintenance costs. The most apparent benefit of the distributed control architecture is that CapEx is

reduced since no controller is required. The saving is even more significant for deployments that involve multiple controllers for redundancy or load sharing purposes.
Additionally, the Alcatel-Lucent Enterprise licensing model foresees one single license per AP for management. This single license includes all features required today for a state-of-the-art wireless network (intrusion detection, firewalling, deep packet inspection, L7 Application monitoring, and enforcement, …), thus reducing software & licensing costs. It also brings simplicity and clarity compared to traditional licensing models that come with controllers and charge licensing fees per feature.

Lower operating costs
No controllers mean less equipment to operate and manage, providing several costs benefits: less rack space, less power, and cooling requirements, no maintenance fees (especially for unused backup controllers), and less equipment to be monitored by the IT department.

Increased resiliency
In a centralized controller-based architecture, the controller is a single point of failure for the entire wireless network impacting all wireless traffic when the controller fails. The only way to minimize the impact is to add additional redundant controllers, but this comes with a high cost. With a distributed control architecture, that single point of failure does not exist. Indeed, the controller function is no longer centralized but shared by all APs in the domain of management. When an AP fails, the neighboring AP will detect that and react by increasing their transmit power, thus avoiding any radio coverage hole. The impact will be purely local: only clients associated with the failed AP will associate to the neighboring AP and authenticate again.

Optimized latency and QoE (Quality of Experience)
A WLAN network is now a critical and indispensable asset for an organization. Wi-Fi is no longer only a comfort option. Today, the WLAN is expected to connect bandwidth-hungry and latency-sensitive applications (Voice or Audio/Video over IP, video streaming…). Over the years, the technology has improved throughput with IEEE standards 802.11a/b/g, 802.11n, 802.11ac, and now 802.11ax, which provides more Multi-Gigabit throughput over the air. To fully leverage the capabilities of 802.11ax APs, such APs will be connected to the LAN with the IEEE 802.3bz 2500BASE-T link providing up to 5G connectivity.
Tunneling all that traffic from each AP towards the controller will be challenging to sustain and will create a throughput bottleneck and increased latency. In the Stellar WLAN distributed architecture, the traffic is no longer tunneled to centralized equipment but directly bridged into the local Ethernet switch.
By design, OmniAccess Stellar WLAN will use the Ethernet fabric as the data plane. However, in some circumstances, it may be needed to tunnel some traffic to a central position. Using latest tunneling protocols (L2GRE and Wireguard), Stellar APs can terminate tunnels in OmniSwitch or a third-party device, including the OmniAccess WLAN Controllers, Nokia 7750 Service Routers, and other.
The key differentiator between controller-based solutions and Stellar WLAN is ONLY selected traffic will be tunneled towards the central position. In controller-based solutions, all traffic from APs is sent to the central site, creating bottlenecks, delays, and latency. In contrast, the Stellar WLAN solution can tunnel only specific traffic, like guest traffic, improving the QoE and Security.

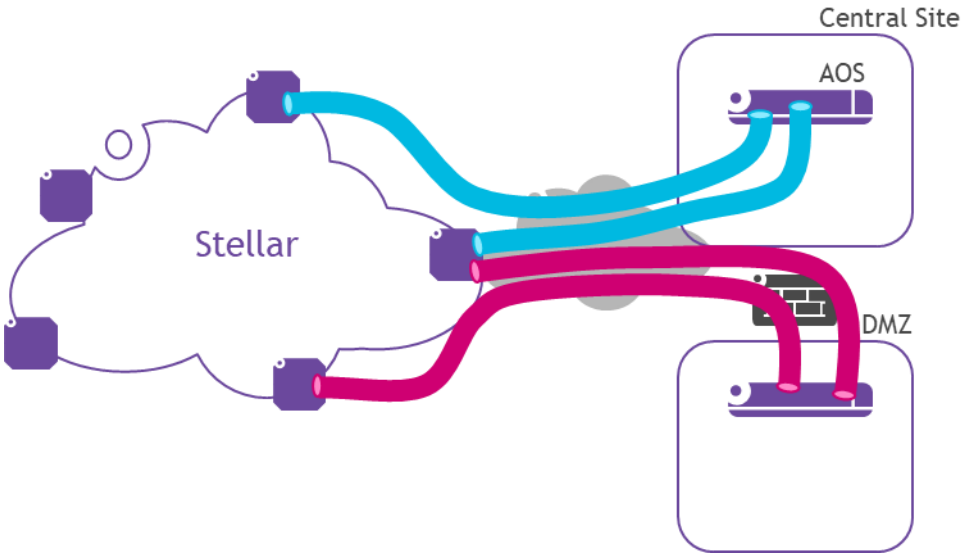


Figure 1: Stellar WLAN Distributed Forwarding with specific traffic tunneled

Better scalability

When the maximum number of APs that a controller can manage is reached, deploying new APs requires an additional controller. The distributed control architecture offers much better scalability: no controller equipment is needed, regardless of the deployment size.

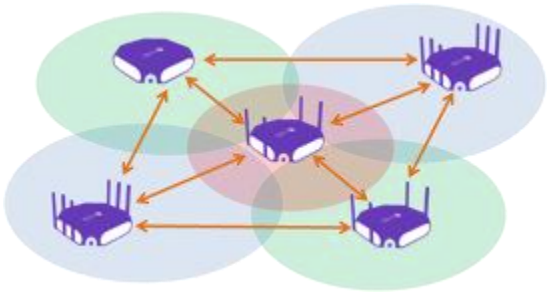


Figure 2: Stellar WLAN distributed control plane

The control plane of the OmniAccess Stellar WLAN solution relies on communications between neighbor only APs. Each AP communicates with its adjacent APs with:

- "Over the air" exchanges to discover each other by announcing essential information like AP management IP addresses through the *Neighbor Management Protocol*
- "Over the LAN" exchanges (a mix of L2 broadcast/multicast and IP connectivity between AP management IP addresses) to agree on RF parameters (e.g., channel utilization and transmit power) and to share roaming clients' contexts.

With this information exchange, each AP will create a "view" of its surrounding Radio neighborhood. That information includes details about trusted-Stellar-APs of the same Group, trusted-Stellar-APs managed by the same OmniVista, Wi-Fi clients in neighboring APs (to speed up hand-over when the client is on mobility), radio interferences, etc.

The distributed control architecture is undoubtedly the shortest route to a sustainable development of enterprise wireless technology in the cloud.

3.	The wireless LAN solution shall rely on a distributed data plane.	C/PC/NC

The data plane of the OmniAccess Stellar WLAN solution is fully distributed, and there is no need for a centralized controller.

The OmniAccess Stellar AP will manage all WLAN user traffic, from encryption/decryption to Firewall rules and Layer 7 (L7) application monitoring and enforcement. Once the traffic is cleaned and secured, it is forwarded to the switched network.

The OmniAccess Stellar WLAN solution's advantage is the traffic can be tunneled using either L2GRE or Wireguard uses for traffic encryption for RAP (Remote AP) for specific use cases. Depending on the ARP (Access Role Profile) assigned to the user, the traffic will:

- Use the L2 data plane (tagged or untagged traffic) of the existing Switching and Routing network.
- Use an L2GRE tunnel ending in OmniSwitch or 3rd party devices supporting L2GRE, like a controller-based architecture.
- Use a WireGuard encrypted tunnel crossing an untrusted network (Internet, Service Provider, External campus, etc.) and ending in the Alcatel-Lucent Enterprise Virtual Appliance.

In the native way of operation, wireless data (IEEE 802.11) is converted to Ethernet (IEEE 802.3) in the AP and sent to the rest of the network through the AP uplink. The AP does not operate any routing on wireless client data. The LAN infrastructure shall handle this L3 function. The AP just tags (IEEE 802.1q) traffic at Layer 2 before sending it on the uplink. The VLAN tag is applied depending on the SSID or ARP (Access Role Profile) configuration. Different clients in the same SSID may have different ARP assignment (VLAN, QoS, FW rules, L7 application control, etc.).

In L2GRE mode, the ARP applied to the client will inform the Stellar AP to L2GRE tunnel the client's traffic towards the Tunnel terminator. This approach has important benefits compared with traditional controller-based solutions, as ONLY specific traffic will be tunneled, leaving the rest of traffic to flow with the lowestdelays while supporting VLAN tagging. The Stellar APs will stablish L2GRE tunnels per ARP. That means that all users with the same ARP will share the same tunnel, improving AP performance. ARP security filters are applied to the traffic as enters the AP, so security is still applied at the EDGE of the network, to properly stops attacks and misbehavior as closer to the source as possible.

In RAP mode, the AP will stablish a SECURE connection with a central tunnel terminator. The GRE tunnel carrying VLANs is encrypted, so the tunnel can flow crossing any unsecure network with support for L2 ethernet services over GRE. Wireguard is the state-of-the-art security protocol used in the RAP communications. The central tunnel terminator is a Virtual Appliance (VA-RAP) provided by Alcatel-Lucent Enterprise. RAP functionality allows for split-tunneling, meaning some traffic can be directly resolved locally and sent using the Internet connection, while protected traffic will take the WireGuard tunnel towards the central site.

4.	The wireless LAN solution shall allow two types of deployment with a Centralized Management: ▪ "Large deployment" for a multi-site deployment with Access Points spread over multiple management VLANs, and that may operate in a different RF environment ▪ "Cloud deployment" for any deployment (single or multi-site) with Centralized Management in the cloud. For both deployment types, the solution shall offer advanced features like Intrusion Detection/Prevention or a Captive Portal to manage guests' or BYOD connections without additional third-party components. For both deployment types, the solution shall support advanced wireless services, using Bluetooth LE and ZigBee technologies or advanced servers included in the solution. This without addition of third-party components.	C/PC/NC

The OmniAccess Stellar WLAN solution fully complies with this requirement. OmniAccess Stellar WLAN solution can be deployed in two distinct ways.

The first one is called Stellar *Wi-Fi Express* and is meant for smaller deployments with up to 255 APs of any model in the current Stellar WLAN portfolio. OmniAccess Stellar WLAN Access Points operate by default in Wi-Fi *Express* mode and provides simplified plug-and-play deployments with standalone clusters, deployed with a common management VLAN and common RF environment (e.g., same *Country Code* for all APs).
Wi-Fi *Express* mode is generally not subject of RFP proposals and then will be not detailed within this document.

The second one is called *Wi-Fi Enterprise*, and it can scale up to 4096 APs right now and many more with the development of the cloud-based WLAN solution. In the latest cloud deployment model, the Alcatel-Lucent Enterprise Omnivista Cirrus Network Management System (NMS) is deployed on top of the Access Points infrastructure to take care of management and configuration of all the APs for maximum scalability. The Omnivista 2500 NMS remains fully supported in *Wi-Fi Enterprise* mode and fully compatible with cloud-based management models.

Both Omnivista 2500 mode (also called *Enterprise* mode) and Omnivista Cirrus mode are requesting proposals for Wireless LAN solution for Enterprise and are described within this RFP document.

"Large & Cloud" deployment projects are multi-site/multi-tenants projects and reach the limits of the *Wi-Fi Express* solution. For instance, when the deployment needs more than 255 APs, several Radio Frequency domains (a company spread in EU and US), advanced functionality including user access roles, complex and highly personalized captive portals, or the need for a Centralized Management.

For these projects, the solution is either Omnivista 2500 and Omnivista Cirrus modes. In both modes, the access points are managed as one or more AP Groups (a logical grouping of one or more access points with similar settings) by Omnivista.

Stellar Enterprise mode with Omnivista 2500 embeds a visionary controller-less architecture, providing user-friendly workflows for Unified Access together with integrated *Unified Policy Authentication Manager* (UPAM), which helps define authentication strategy and policy enforcement for Employees, Guest Access and BYOD.
Omnivista 2500 offers advanced features and capabilities as a Zero Trust Access with L7 application recognition and enforcement, providing real-time classification and control of flows at application level or local heatmap feature for WLAN to prepare site planning.

Omnivista 2500 offers advanced Stellar location services (when using BLE radio), other third-party IoT management with IoT applications (Assa Abloy application with using Zigbee radio etc.) or any other location applications (RTLS applications) by providing the connectivity to different types of servers:

- RTLS type (OmniVsta Cirrus Wi-Fi RTLS or Aeroscout)
- Assa Abloy type; with management of Zigbee application through Zigbee Control Service module (ZCS) and using ZigBee technology. Stellar Asset Tracking server type; with Stellar Asset Tracking and Contact Tracing server using BLE technology.
- OmniVista Cirrus Advanced Analytics type; with analytics tasks provided by OmniVista Cirrus 10 Cloud solution.

Omnivista 2500 manages the on-boarding of IoT equipment and thus brings from the administrator point of view a complete control of IoT in the managed network by OV2500. Once IoT equipment is discovered its acceptation is done by Omnivista Enterprise to be effectively operational in the network

Stellar *Enterprise* mode offers, with the combination of OmniVista Cirrus release 10, advanced analytics services dedicated to statistical and analytical tasks and Quality of Experience (QoE) monitoring for any Stellar XL/Multi-Tenant deployment.

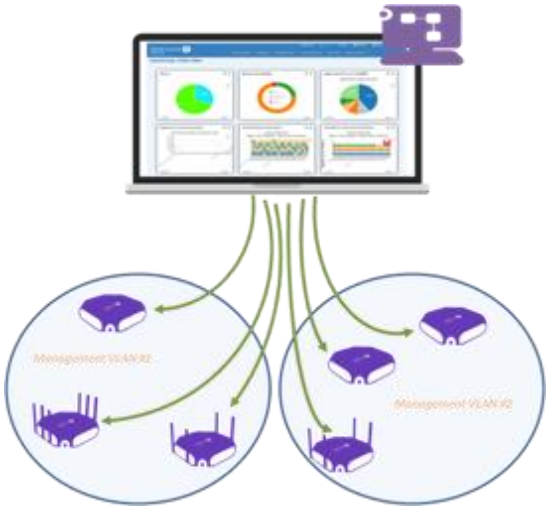


Figure 3: OmniAccess Stellar WLAN Enterprise

Note the cloud-based version of the OmniAccess Stellar Enterprise deployment model exists in two versions and is called OmniAccess **Stellar Cloud**.
In legacy cloud versions, Stellar WIFI Access Points are provisioned and managed by the cloud-based OmniVista **Cirrus** Network Management System in its release 4. OmniVista Cirrus release 4 is a scalable, resilient, secure cloud-based network management for unified access offered as a subscription service. It is functionally equivalent to OmniVista 2500 Enterprise but hosted in the cloud. OmniVista Cirrus 4 provides an easy to deploy, effective way to manage and monitor Alcatel-Lucent Enterprise OmniSwitch and Alcatel-Lucent OmniAccess Stellar access point infrastructure. Like OmniVista 2500 in *Wi-Fi Enterprise* mode, it provides advanced policy capabilities for guest access and BYOD.

OmniVista Cirrus release 4 is a subscription-based service, facilitating alignment with new business imperatives. Ease of purchasing, provisioning and ongoing daily operations are at the core of OmniVista Cirrus. This facilitates digital transformation, allows to be quick to respond to new business needs, but without high upfront costs or complex infrastructure changes or software deployments. Shifting to a cloud-based network management solution with OmniVista Cirrus can simplify digital transformation by reducing cost and administrative IT burden.

Stellar Cloud mode evolves with release 10 of OmniVista Cirrus, by leveraging the latest technologies available in the Cloud. Omnivista Cirrus 10 enables:

- Centralize the wireless visibility & management for WLAN
- Provide Cloud SaaS NMS solution with Multi-tenant/Multi-organisation support
- Provide scalable, resilient, secure, cloud-native solution
- Provide advanced analytics
- QoE monitoring
- IoT enablement
- Manage ALE network devices, introducing OmniAccess Stellar access points management (from release 10.3)
- Will provide network assistance and preventive maintenance in its further versions.

As a Cloud SaaS NMS solution Omnivista Cirrus 10 is requesting for proposals for wireless LAN for Enterprise and is subject to a complete and separated RFP Golden document: *ALE Omnivista Cirrus 10 Golden RFP*. For any proposal preparation with Omnivista Cirrus 10 please refer to this document related to Enterprise mode for ALE equipment managed in the cloud.

Figure 4: OmniAccess Stellar WLAN Cloud & OmniVista Cirrus

The idea in general for network design with Omnivista (multi-site/multi-tenant) is to manage the Access Points as one or more AP-Groups (a logical grouping of one or more Access Points with similar settings) by Omnivista to form distincts groups of Wi-Fi 5 (802.11ac) and/or Wi-Fi 6/6E (802.11ax) and/or Wi-Fi 7 (802.11be) versions, to form IoT-enabled AP-Groups as required and several Radio Frequency domains, this in varied scales. There is no specific role for access points for their management. For all the management, security or fault tasks, Stellar Access Points and Omnivista communicate using Wireless Management Application (WMA) of Omnivista. WMA is performed on Stellar management plans and remains active as long as one Omnivista instance stays reachable.

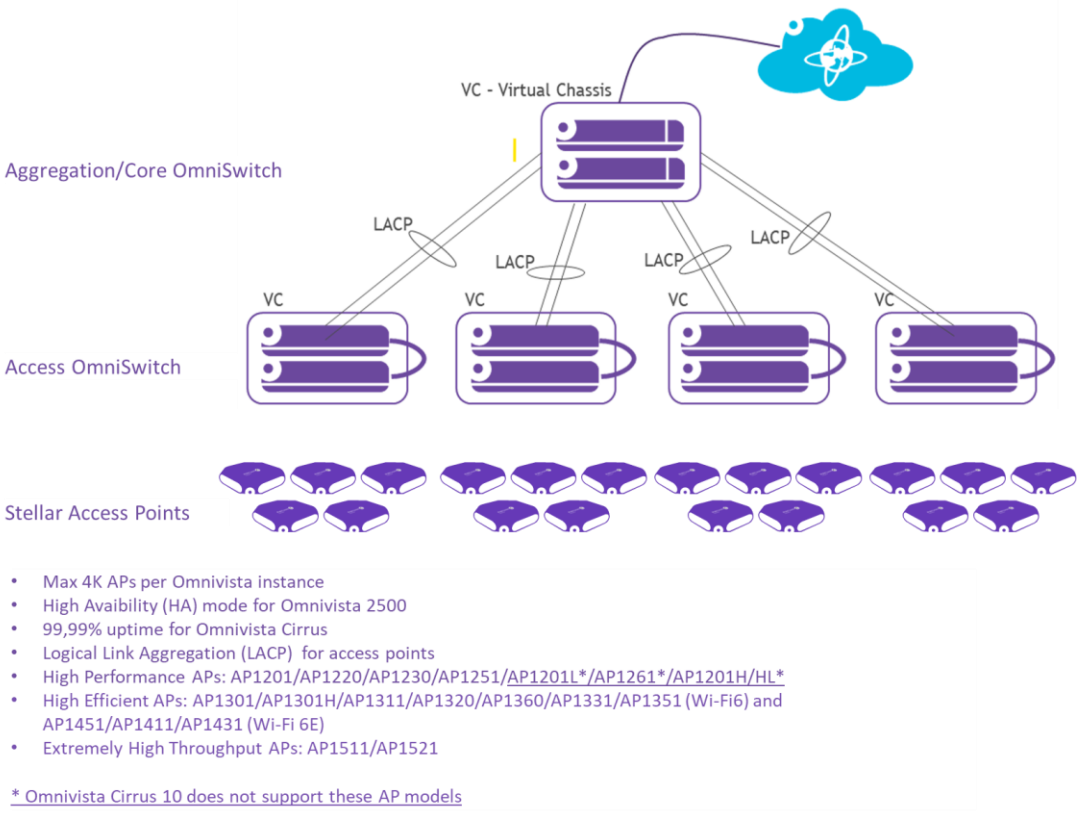


Figure 5: Wi-Fi Enterprise sizing

Within this document the **Stellar Enterprise mode** and **Stellar Cloud mode** deployment models will generally be described interchangeably as "*Stellar Enterprise mode*", "*Wi-Fi Enterprise mode*" or "*Enterprise mode*" for simplicity purposes.

5.	The wireless LAN solution shall propose a centralized management function, irrespective of the deployment model ("Large" or "Cloud"), as described previously [4].	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement for all deployment models (*Enterprise and Cirrus*). Please refer to requirement [6].In Enterprise and Cirrus models, OmniVista is the central point of management.

6.	The wireless LAN solution shall propose a centralized management function based on an embedded and secure WEB GUI, irrespective of the deployment model ("Large" or "Cloud") as described previously [4].	C/PC/NC

The *Enterprise* deployment model allowed by the OmniAccess Stellar solution offer a secure (HTTPS) web based centralized management function relying on following Omnivista depending on Large or Cloud management mode chosen in *Stellar Wi-fi Enterprise mode*:

- The Alcatel-Lucent Enterprise OmniVista 2500 Network Management System
- The Alcatel-Lucent Enterprise OmniVista Cirrus 4 and Omnivista Cirrus 10 cloud-based Network Management System

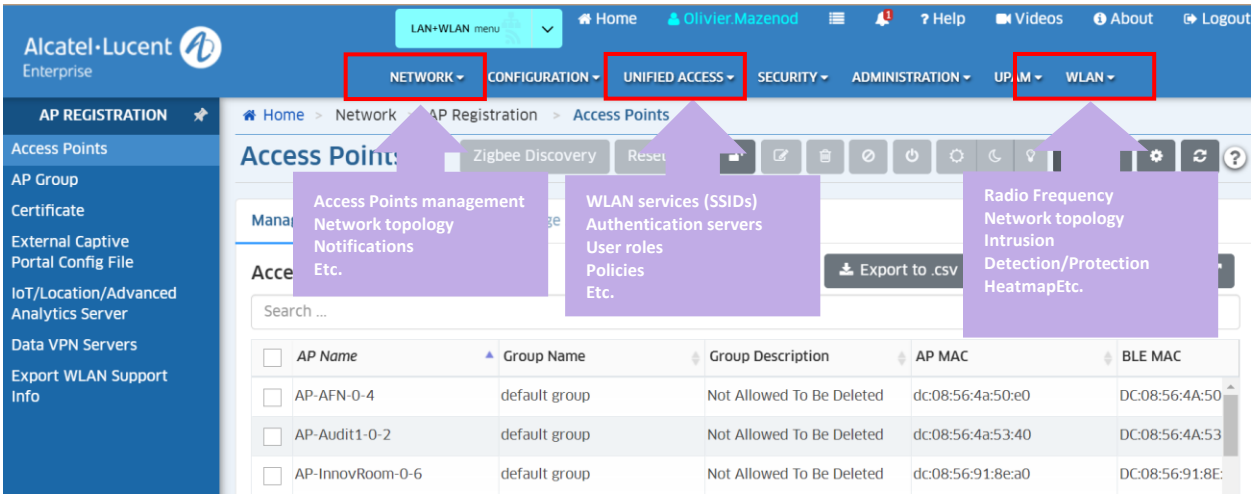


Figure 6: On-premise centralized management - Enterprise mode – Omnivista 2500

7.	In addition to a centralized management function, all Access Points of the wireless LAN solution shall propose a dedicated web interface to monitor and configure a single AP in the global infrastructure, irrespective of the deployment model ("Large" or "Cloud") as described previously [4].	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement in *Wi-Fi Enterprise mode*. Each AP provides a dedicated web interface called "AP UI" (*Access Point User Interface*) to monitor and configure a single AP in the global infrastructure for tasks like:

- Learning the WLANs status, connecting clients on the AP
- Configuring DHCP/DNS/NAT services on the AP
- Configuring wireless Mesh/Bridge feature for the AP
- Maintenance (Upgrade/Reset/Reboot the AP)
- Dedicated scanning mode activation
- Wireless capture feature activation
- Configuring neighboring APs

The access to the AP UI is via the *AP Web* "action" in OmniVista:

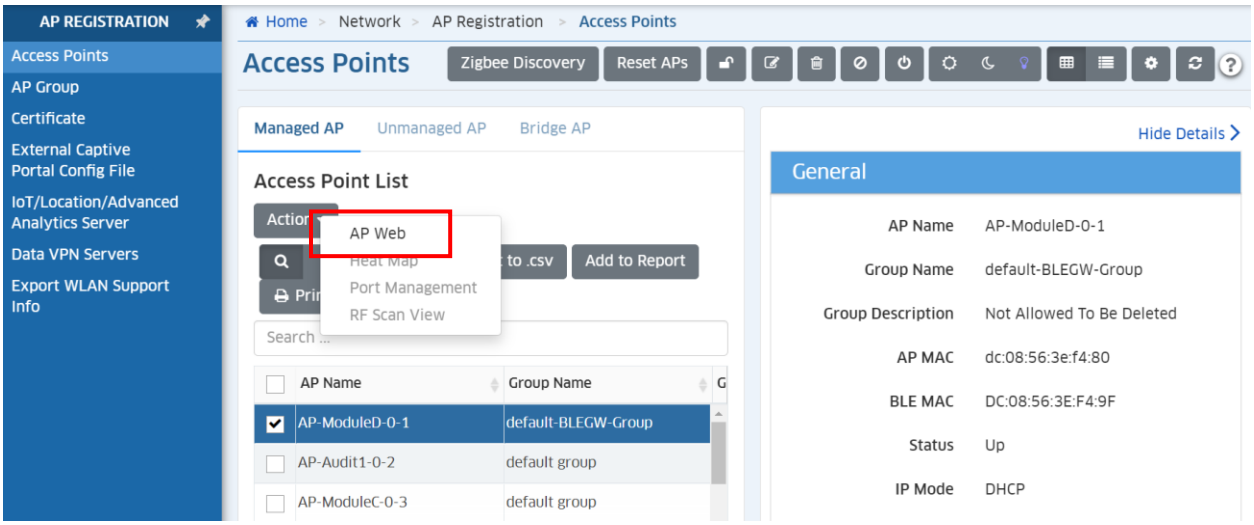


Figure 7: Link to AP UI - Enterprise mode – Omnivista 2500 (Access Points)

8.	At least for a "Large or Cloud deployment" scenario as described previously [4], the centralized management function shall be able to handle wired equipment (switches) management for a "unified management" approach.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniVista 2500 NMS and Omnivista Cirrus 4 that are part of the OmniAccess Stellar WLAN solution in *Wi-Fi Enterprise mode*, provides unified management of your whole network with Alcatel-Lucent switches and third-party network equipment. That "unified management" approach provides a Single Pane of Glass for the entire network (wired/wireless), with a single management platform, same cohesive (wired or wireless) workflows and applications for maximum operational value.

Subsequent versions of Omnivista Cirrus 10 introduced in this document, will expand the management of Alcatel-Lucent switches, as part of the ongoing evolution of "unified WLAN/LAN management" in the cloud.

9.	The wireless LAN solution shall scale up to 4096 Access Points for the "Large or Cloud deployment" models [4] and thousands of users while guarantee ease of deployment and expansion (to be described).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement for all deployment models (*Enterprise and Cirrus*). Please refer to requirement [4]. This value is not a limit in term of architecture for deployment with Omnivista Cirrus 10.

10.	The "Large or Cloud deployment" option previously described [4] shall rely on a licensing model that is as simple as possible, with one license per AP, including all functions (basic or advanced) handled by the AP.	C/PC/NC

While WLAN solutions proposed by Alcatel-Lucent Enterprise competitors (especially controller-based solutions) rely on a complex and feature-dependent licensing model, the OmniAccess Stellar licensing model in Wi-Fi *Enterprise* mode foresees one single license per AP for management. This single license includes all features required today for a state-of-the-art wireless network (intrusion detection, firewalling, L7 application recognition and enforcement…, BLE/ZigBee radios management for IoT), thus reducing software & licensing costs. It also brings simplicity and clarity in comparison with traditional licensing models that come with controllers and that charge licensing fees per feature.
The only additional licenses that may be required based on the deployment requirements are "Guest Access" and "BYOD" (*Bring Your Own Device*) licenses.

AP management (1 → 4096)	per AP
RF Management	Included
Floor Pan/Heatmap	Included
wIDS/wIPS	Included
Authentication & Policy Enforcement	Included
Application Visibility	Included
Client Monitoring	Included
IoT Inventory	Included
Guest Access (20 → 10K)	per Device
BYOD (20 → 10K)	per Device

Table 1: Stellar Enterprise/Cloud licensing model description

11.	At least for a "Large or Cloud deployment" scenario as described previously [4], and especially for XL deployments, the centralized management function shall offer integrity of the WLAN solution by supporting optimal monitoring, management and security features for WLAN.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. OmniVista NMS monitors the network and manages OmniAccess Stellar access points using the *Single Node Management Protocol* (SNMP). Stellar APs monitoring is now secured with SNMP version 3 for all APs models (AWOS release 4.0.5 minimum) to collect, organize APs information (based on OmniAccess Stellar MIB structure) and verify activity of APs registered in OmniVista. SNMPv3 will also be advantageously used for monitoring Stellar WLAN network with 3th-party Network hypervisor. Legacy SNMPv2 and standard SNMP versions are still supported.

OmniVista NMS optimizes also the security of registered access points with several features. Omnivista allows to provide additional information on the attachment of APs (AWOS release 4.0.5 minimum) by inserting specific data into the DHCP option 82. In particular, the DHCP relay will support the *Circuit ID* information to identify the AP attachment point.

Omnivista NMS also frees the WLAN network from any impersonation of Stellar APs (known as rogue APs attack) by fully managing switch port-based 802.1x identification for APs, applying an access role (port-based ARP) and involving the built-in RADIUS server of UPAM module in Omnivista.

The customer can then either use the built-in Stellar PKI and certificate or import customer's PKI and certificate(s) into Omnivista for a totally private site configuration for APs identification.

12.	The centralized management function shall allow access to all wIPS/wIDS features.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement in *Wi-Fi Enterprise mode*. Please refer to chapter 5.

13.	At least for a "Large or Cloud deployment" scenario as described previously [4], the centralized management function shall offer, on the basis of an application signature file, insight at application layer (e.g. *facebook.com*, *youtube.com*, *salesforce.com*…) even if the applications run on top of the HTTP or HTTPs protocols. It shall also allow control of those applications.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Please refer to requirement [108].

14.	At least for a "Large or Cloud deployment" scenario as described previously [4], the centralized management function shall be collocated with the Guest and BYOD management applications.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement by collocating the three functions on the OmniVista 2500 Network Management System. Please refer to chapter 1 and requirement [28].

15.	Moving from Wi-Fi Express option (255 APs) shall allow an easy migration to a "Large deployment" (4096 APs) when needed.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution has been thought and designed with future evolution in mind. Indeed, Wi-Fi *Express* and Wi-Fi *Enterprise* mode are mutually exclusive, but moving from a Stellar *Express* architecture to a Stellar *Enterprise/Cloud* architecture is very easy.

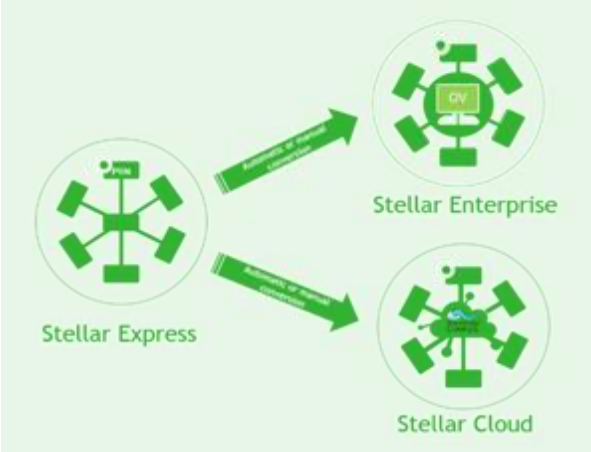


Figure 8: Stellar Wi-Fi Express or Enterprise/Cloud - Evolutive design

The operating mode of an AP is hardcoded at first boot: if the AP gets a DHCP lease with option 138 (which gives the IP address of the OmniVista 2500 server), the operating mode of the AP is permanently set to Stellar *Enterprise*. Otherwise (no option 138), the AP first tries to contact OV Cirrus in the cloud. If the AP can join OV Cirrus and if the AP is provisioned (serial number and MAC address) in some Cirrus instance, then the operating mode of the AP is permanently set to *cloud*. If the AP gets a DHCP lease with no option 138, and the AP cannot contact OV Cirrus in the cloud (or the AP is not provisioned in OV Cirrus), then the operating mode is permanently set to Stellar *Express*.

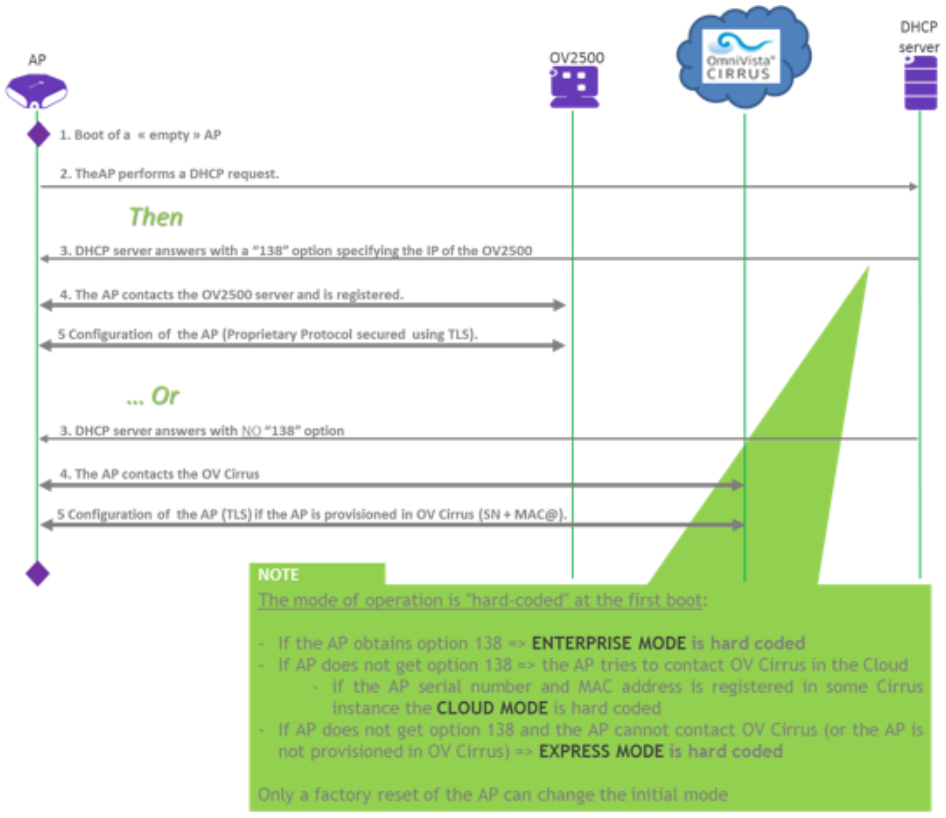


Figure 9: Stellar AP boot sequence and DHCP option 138

If a Stellar AP is configured in *Express* mode, it can be easily migrated to *Enterprise* or *Cloud* mode by performing a factory reset after having configured the option 138 in the DHCP server, or having configured @IP of Enterprise server manually, for the management scope. A factory reset can be done manually on each AP by pressing a factory reset button on the back of the AP, or centrally through the centralized Web GUI.

Figure 10: Express to Enterprise migration (factory reset button)

When a Stellar AP is running in *Express* mode, it can also be easily converted to *Enterprise* or to *Cloud mode* by selecting appropriate option in Stellar Express WEB management interface:

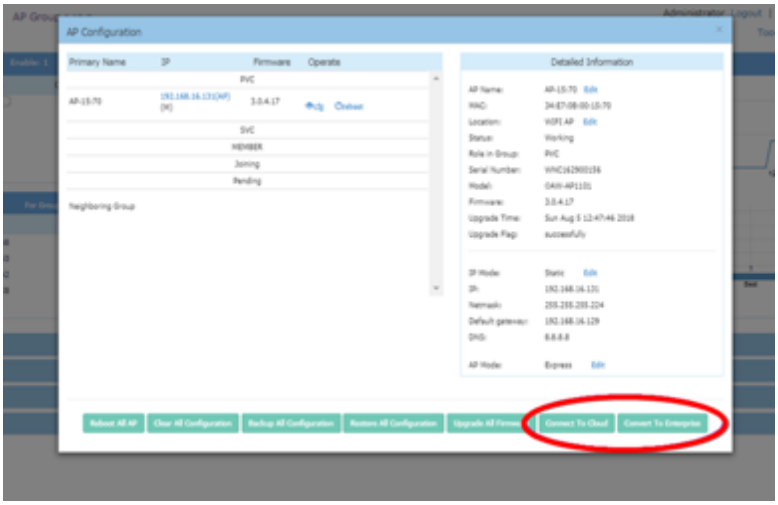


Figure 11: Express to Enterprise migration (Web GUI based conversion)

16.	The wireless LAN solution shall have been designed with scalability in mind to allow the 4096 APs limit without requiring new equipment or deployment design change.	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution fully complies with this requirement. While competitors' controller-based or even controller-less solutions (in that case, an AP is usually elected and handles the control function) rely on a centralized control function, the control function of the OmniAccess Stellar WLAN solution is fully distributed. In theory, the number of APs that the OmniAccess Stellar WLAN solution can support is even unlimited by design. Competitors' solutions rely on a central point that concentrates "control information" for the entire wireless network and which capabilities are physically limited. In Alcatel-Lucent Enterprise's proposal, the "control information" is not concentrated but shared only between neighboring APs to handle some functions like roaming. That allows maximum scalability and investment protection. Alcatel-Lucent Enterprise will regularly proceed to new validation tests to formally validate and announce new maximum number of APs the *Stellar Enterprise mode* can support.

17.	For the "Cloud deployment" model [4] the WLAN solution shall be designed to allow APs to be purchased in a subscription-based model for customers who do not wish to own their Wi-Fi equipment. The subscription offer will be included in the solution and will be fully managed by the supplier of the WLAN equipment.	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution fully complies with this requirement in *Wi-Fi Enterprise mode*, offering a NaaS (Network as a Service) service for Cloud deployment with a hybrid Capital Expenditure (CAPEX) /Operating Expenditure (OPEX) registration mode for Stellar access points.

This service provides an all-in-one service that combines OmniAccess Stellar support where partners purchase access points upfront in CAPEX at an attractive price, transferring hardware ownership from ALE to the partners. A Right to Use (RTU) license for the device is available through a subscription model (OPEX) between ALE and the partner. The partner has two options for end-customers:

- Option 1 - resell the hardware in CAPEX with a RTU license, suitable for customers who want equipment ownership.
- Option 2 - include the hardware in partner's managed service offer for a nominal monthly fee, providing a fully OPEX service. This option excludes the purchase and acquisition of Stellar access points by the end-customer, who only bears the operating costs, the support and the subscription to the service.

NaaS subscription is taken out with the customer's partner as service provider.

For any Cloud deployment, Omnivista Cirrus 10 sets the CAPEX/OPEX ownership mode when registering the AP, and also updates the number of NaaS device licenses used for the site.

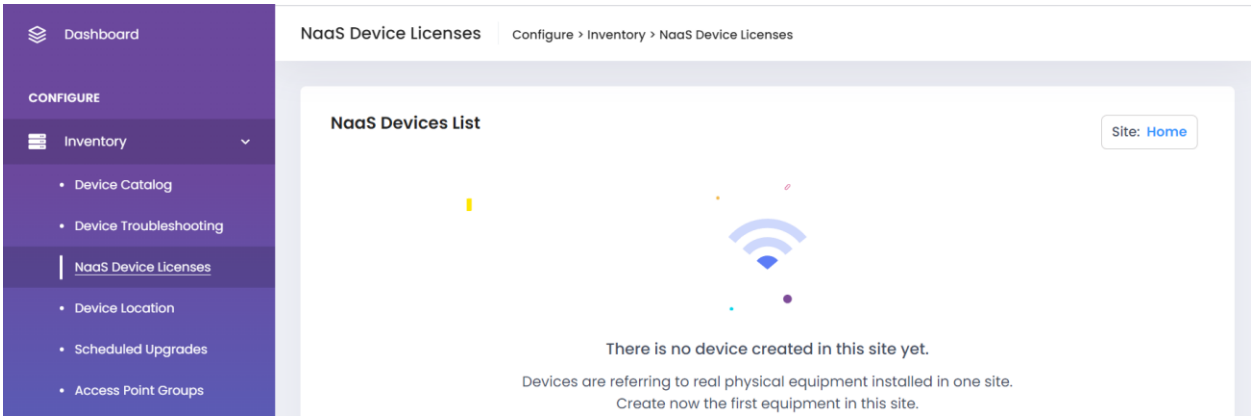


Figure 12: NaaS Device Licenses – Enterprise mode – Omnivista Cirrus 10 (Inventory)

18.	For the "Cloud deployment" model [4] the customer's partner specifies the NaaS duration offer for the Stellar WLAN solution. NaaS terms and conditions with options are described in a service description document provided by ALE.	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution fully complies with this requirement in *Wi-Fi Enterprise mode* with Omnivista. The end-customer chooses to purchase his WLAN equipment as a Service in exchange for periodic monthly/quarterly/annual or term payments from his partner. The supplier indicates a duration period from 24 months to 60 months. Fees natively embed the support of equipment: including advanced repair replacement (faulty hardware), technical assistance, software upgrades/updates, security patches and access to the Knowledge Hub.

The current version of the NaaS service (version 3.1) is described in the *"Network-as-a-Service by ALE" Service Description* document for partners and is available under ALE MyPortal. NaaS subscription chosen by end-customer simply adds to the AP license model detailed in [10], that includes all functions (basic or advanced) handled by the APs.

19.	The WLAN solution shall allow to connect two distant sites over a wireless point-to-point link.	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution fully complies with this requirement in Wi-Fi *Enterprise mode* with two OmniAccess Stellar Access Points configured in "bridge" mode:

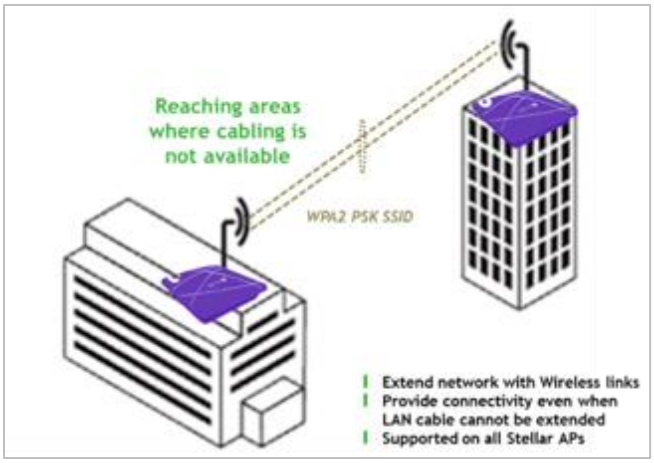


Figure 13: Point-to-Point bridge mode

All OmniAccess Stellar Access Points can be configured in "bridge" mode, thus allowing to connect two separate networks wirelessly when LAN cable cannot be extended. In that mode, no WLAN services can be configured on the APs connecting the two sites for clients association (all radios links are aggregated to build the point-to-point radio link) and the wireless point-to-point connection is established by configuring and broadcasting a WPA2 or WPA3 PSK SSID. With Omnivista easy bridge/mesh feature, APs dedicated to bridge link can be configured directly from the devices list.

20.	The WLAN solution shall allow to connect multiple distant sites over wireless (Mesh Network)	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution fully complies with this requirement in Wi-Fi *Enterprise* mode by configuring and deploying multiple OmniAccess Stellar Access Points configured in "mesh" mode:

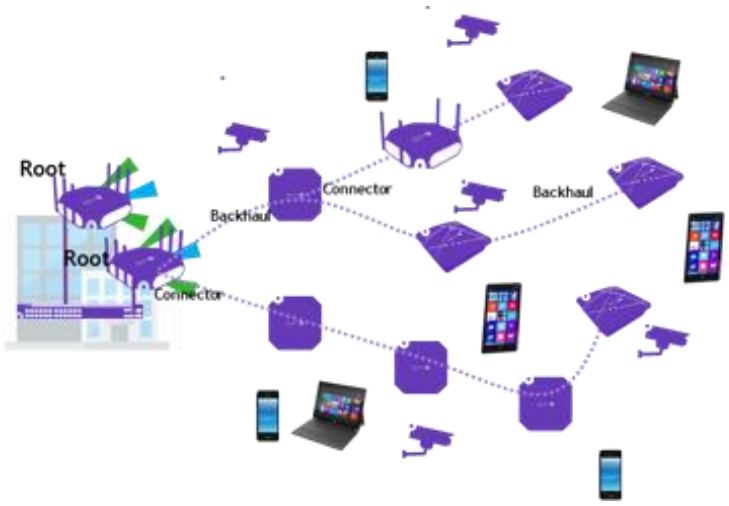


Figure 14: Point-to-Multipoint mesh mode

All OmniAccess Stellar Access Points can be configured in “mesh” mode, thus allowing to connect multiple sites. In that mode, Access Points which have a wired connection to a LAN are “mesh root” APs and Access Points which do not have a wired connection are pure “mesh” APs. Each “mesh” AP works in a parent-leaf mode with repeater. All APs can broadcast up to 5 WLAN services (SSIDs) for clients association and can establish up to 5 direct Point-to-Multipoint to other APs considering that the whole mesh setup can include up to 16 APs and considering that a chain can include up to 8 APs from a mesh root to furthest mesh AP. With Omnivista easy bridge/mesh feature, APs dedicated to mesh links can be configured directly from the devices list.

21.	The WLAN solution shall allow easier deployment of Mesh Networks.	C/PC/NC

The OmniAccess Stellar Access Points support Auto-Mesh. With this functionality, Admin only has to enable the Mesh-Root functionality in the wired APs. When Mesh-Point AP boots up, if it is not connected to the wired network, it will automatically start the process of joining to the Mesh Network, automatically establishing the radio links with the neighboring Mesh-Points and Mesh-Roots.

The easy/mesh configuration menus are provided for both Enterprise and Cloud deployment models.

22.	The WLAN solution shall support IPv6 for wireless clients.	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution fully complies with this requirement in Wi-Fi *Enterprise* mode, thus enabling next generation large-scale IP networks by supporting addresses that are 128 bits long. The support of IPv6 includes:

- IPv6 address of the client
- IPv6 based ACL for client traffic
- White list for IPv6 address (“Walled Garden”)

The support of IPv6 for wireless clients in Wi-Fi E*nterprise* mode also includes communications between wireless clients and the Captive Portal for guest authentication, depending on the IP address of the redirection URL. Following table describes in detail the support of IPV6 and its options:

Authentication & Accounting	Support
IPv6 Radius Client	Yes
MAC authentication for IPv6 or IPv4/IPv6 client	Yes
802.1x for IPv6 or IPv4/IPv6 client	Yes
Captive Portal for IPv6 or IPv4/IPv6 client	Yes
RADIUS Accounting (MAC-Auth/802.1x/Captive Portal) for IPv6 or IPv4/IPv6 client	Yes

IPv6 Security, QoS, Firewall, Policy	Support
IPv6 Policies (Enterprise)	Yes
Application Visibility (DPI)	No
White list for IPv6 addresses	Yes
Walled Garden for FQDNs using IPv6 address	Yes
Client isolate for IPv6 traffic	Yes
IPv6 Forwarding	
ICMPv6	Yes
IPv6 Bandwidth Setting	Yes
IPv6 forward mode - Layer 2 bridging	Yes
IPv6 forward mode - Layer 3 routing	Yes
IPv6 forwarding over IPv4 L2 GRE Tunnels	Yes
Roaming	**Support**
L2 Roaming for IPv6 or IPv4&IPv6 client	Yes
L3 Roaming for IPv6 or IPv4&IPv6 client	Yes
IPv6 client Information, Management	**Support**
IPv6 addresses of the client in User Interface/API	Yes
OS fingerprint of IPv4/IPv6 dual-stack client	Yes
OS fingerprint of IPv6 only client	No
Client IPv6 Behavior Tracking	Yes

Table 2: IPv6 support for wireless clients

Please note that IPv6 traffic crossing Layer 2 domains or visiting the Internet requires an IPv6/IPv4 dual-stack gateway.

23.	The WLAN solution shall support L2GRE tunneling with a highly flexible architecture.	C/PC/NC

OmniAccess Stellar is fully compliant with this requirement.

In today's WLAN networks, it is pretty common to send traffic to a central device or site, avoiding mixing different traffic types.

Some examples are:

- Guest Access. Enterprise companies usually prefer to isolate guest user traffic from the enterprise's network completely.

- For Service Providers to move data traffic out of 4G/5G networks to WLAN, is a technique called WLAN-offload.
- In Multi-tenant networks, the same WLAN infrastructure has to provide service to many different tenants, each with specific security configurations, AAA servers, etc.

Stellar APs can use L2GRE to tunnel specific traffic towards a central device. Currently supported devices are:

- Alcatel-Lucent OmniSwitch 6860.
- Alcatel-Lucent OmniSwitch 6900.
- Alcatel-Lucent OmniAccess WLAN Controllers.
- HPE Controllers.
- Nokia 7750 WLAN-GW.

Stellar APs will L2GRE tunnel traffic according to the ARP assigned to the connected device. The same AP may have different L2GRE tunnels ending in different tunnel terminators while natively forwarding traffic at L2 to the local switch. For example, an AP may have a single SSID, and five (5) ARP applied to devices, based on authentication or role derivation rules. Three of these ARPs are L2GRE and, for instance, two of them are ending in the same tunnel terminator, while the third is ending in another endpoint. The other two ARP are native, meaning the AP is just performing L2 bridging between 802.11 WLAN and 802.3 Ethernet.

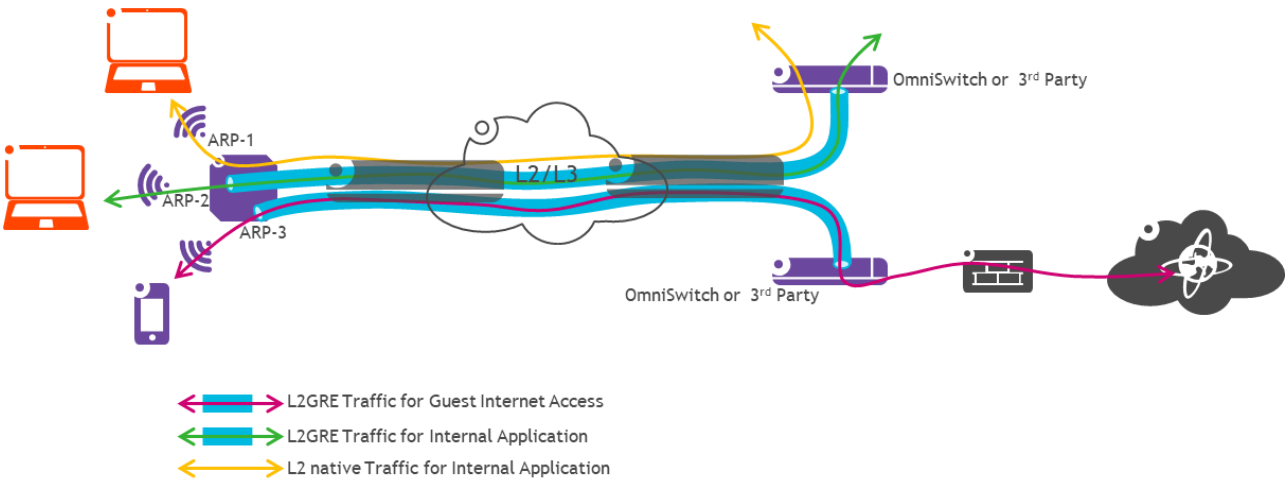


Figure 15: Stellar L2GRE Tunneling

Stellar Enterprise mode handles also a full GRE tunnel resiliency for OmniAccess Stellar access points, with an active/backup configuration of GRE tunnels termination points. This High GRE tunnel resiliency management is added in ARP assigned to the connected device (AWOS release 4.0.5 minimum).

OmniVista configures the ARP and SSIDs from an integrated service view.

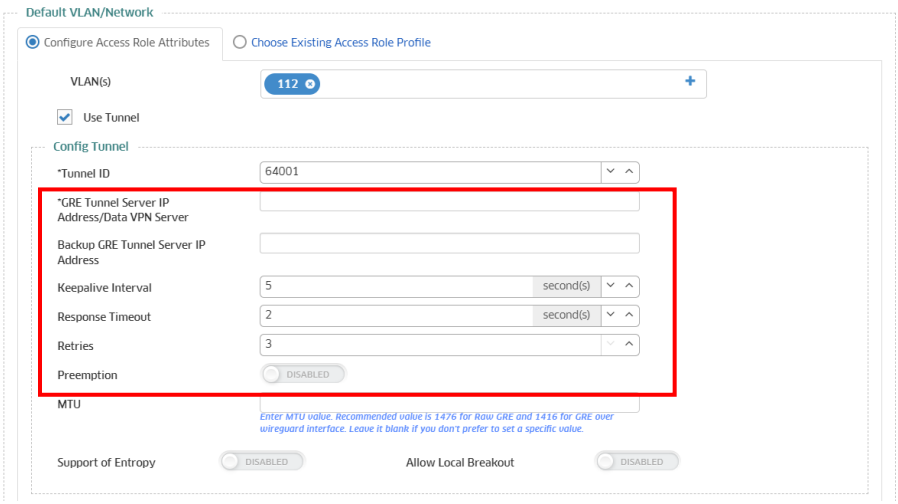


Figure 16: OmniVista L2GRE configuration – Enterprise mode – Omnivista 2500 (SSID)

24.	The WLAN solution shall support RAP functionality, allowing an AP to secure the traffic sent over an untrusted network like the Internet. Should use the latest security standards like WireGuard.	C/PC/NC

OmniAccess Stellar is fully compliant with this requirement. Alcatel-Lucent Enterprise is one of the first vendors to adopt the new state-of-the-art security protocol: WireGuard.

In some circumstances, the connectivity between the users and applications must cross an untrusted network, where the IT administrators cannot guarantee security, authenticity, integrity, or confidentiality. For those cases, the connectivity between the users and the applications must be secured.

Stellar Remote AP (RAP) functionality allows deploying Stellar APs in an untrusted network and providing a secure communication channel. Stellar is using WireGuard for this purpose. WireGuard is a free and open-source software application and communication protocol that implements virtual private network (VPN) techniques to create secure point-to-point connections in routed or bridged configurations. It is run as a module inside the Linux kernel and aims for better performance and more power saving than the IPsec and OpenVPN tunneling protocols.

Stellar RAP tunnels end in a WireGuard tunnel terminator virtual appliance, provided by Alcatel-Lucent Enterprise as part of the solution.

Stellar RAP working in *Enterprise* mode, adds security to the management plane. When APs are in OVC (OmniVista Cirrus), they already have a secured connection with the OVC in the cloud.

RAP functionality includes two kinds of tunnels: One “management” tunnel so that the OVE can manage the AP and the “Data” tunnel for clients’ secure communications. APs can leverage the RAP functionality for “Data” tunnels ending in the Wireguard VPN concentrator in OVC deployments.

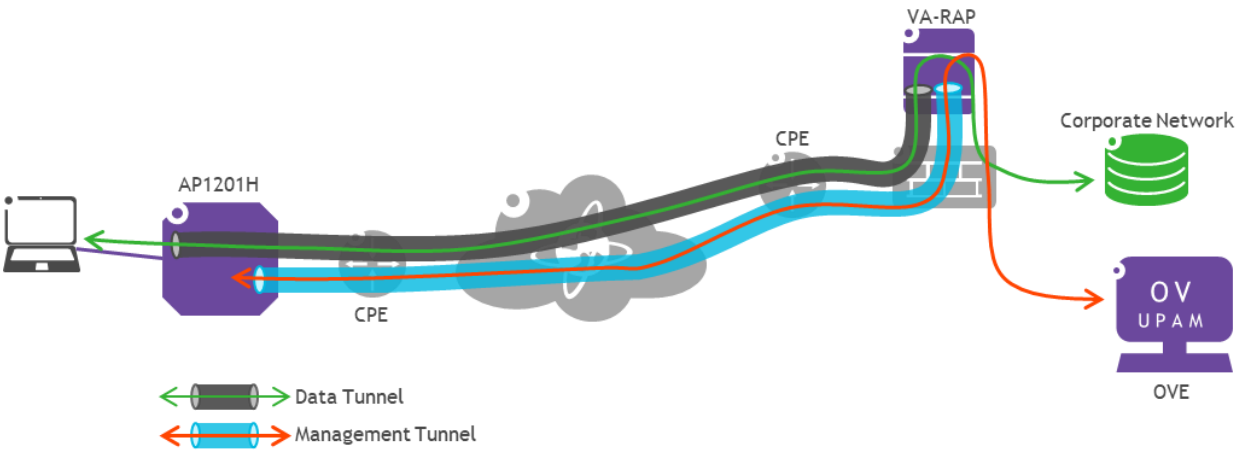


Figure 17: Stellar RAP Management VPN and Data VPN

Stellar RAP allows split-tunneling in the Data tunnel. This technique makes it possible to select which traffic is sent through the secured tunnel and which one will be locally resolved. For example, consider a remote worker at home, using an FTTH connection (Fiber To The Home, GPON). All Internet traffic (O365, Internet browsing, etc.) can be locally resolved and sent directly to the FTTH connection. In contrast, the Corporate traffic (Intranet resources) will take the tunnel towards the tunnel terminator, located at the corporate’s DMZ.

With Stellar APs supporting downlink ports, like AP1201H or AP1301H (Wi-Fi 6), wireless and wired clients can benefit from RAP functionality. Stellar *Enterprise* mode supports the VLAN tagging on the downlink ports of RAP access point, to transport any type of VLAN for different applications for wired clients (AWOS release 4.0.5 and AP1301H minimum)

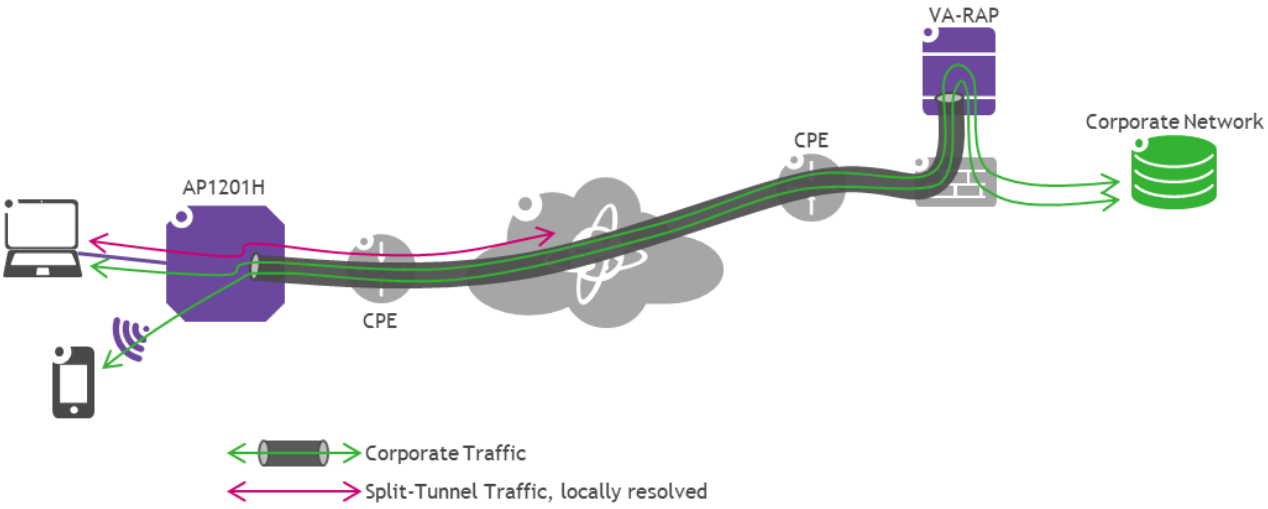


Figure 18: Stellar RAP functionality. Split-tunnel

25.	At least for a "Large or cloud deployment" scenario as described previously [4], the WLAN solution shall provide RAP functionality as a complete multi-site solution to support different offices extensions and providing equivalent network functionality to that managed in the main office. The WLAN solution shall provide the equivalent RAP level of service to operators that support different remote WLAN configurations for different customers.	C/PC/NC

OmniAccess Stellar WLAN is fully compliant with this requirement. Stellar RAP is a multi-site solution, fitting different sites in size or customers, deployed in data center, and entirely managed in *Enterprise mode*. Stellar Remote Access Point (RAP mode) is an affordable way to connect different remote sites over Internet like small branch offices, temporary offices, home workers or nomadic workers.

Stellar Enterprise mode brings the complete WLAN management to remote offices:

- Use of corporate SSIDs at remote location
- Local/Internet routing on SSIDs basis, with corporate traffics default back to main office
- Use of WLAN/LAN parent company access Role Profiles (ARP)
- Use of parent company Application Monitoring with use of Deep Packet Inspection (DPI) of RAP
- Use of parent company Profile Access Manager (UPAM) function of OmniVista for advanced access
- Forward of corporate VLANs and downlink ports management on RAP

In cloud mode and specifically with Omnivista Cirrus 10, Stellar RAP solution takes in account the most use cases encountered by MSP providers to support their remote configurations and users for different clients:

- Multi-organisation support with RAP organisation (Omnivista Cirrus 4 equivalent account is OVC Freemium with RAP list)
- Connection behind DS-Lite ISP routers for remote offices
- Configuration of downlink ports and direct VLAN forwarding on each RAP port, any type of VLAN

3. Omnivista 2500 requirements

3.1. Access Control, Authentication and Encryption

26.	At least for a “Large” scenario as described previously [4], the wireless LAN solution shall support MAC based authentication.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode*. MAC-based authentication, a common authentication method that is used to authenticate devices based on their physical *Media Access Control* (MAC) address, is fully supported with an Alcatel-Lucent Enterprise OmniAccess Stellar solution (*Enterprise*). While not

the most secure and scalable method, MAC-based authentication implicitly provides an addition layer of security and is often used to authenticate and allow network access to certain devices while denying access to the rest.

27.	At least for a "Large" scenario as described previously [4],the wireless LAN solution shall support 802.1x based authentication.	C/PC/NC

Alcatel-Lucent Enterprise fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode* and recommends indeed using 802.1x for wireless and even wired user authentication.
802.1x authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop or a smartphone) that wants to attach to the WLAN. The authentication server is typically a host running software supporting the RADIUS and EAP protocols. In the framework of the OmniAccess Stellar WLAN solution, the authenticator is the OmniAccess Stellar Access Point itself that acts like a security guard to the protected network. The wireless client device is not allowed access through the authenticator/AP to the protected side of the network until its identity has been validated and authorized.

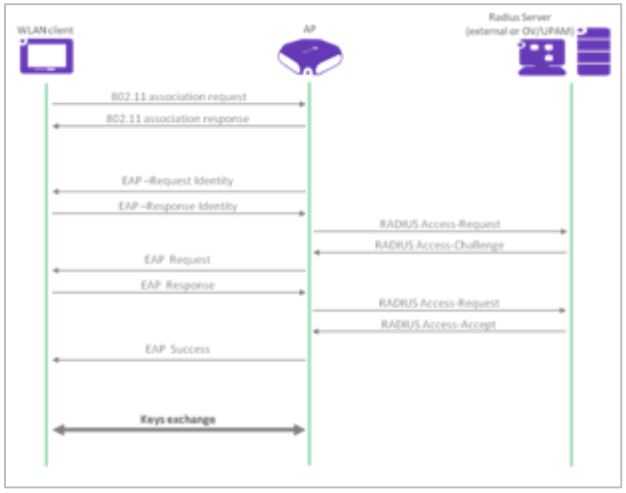


Figure 19: OmniAccess Stellar and 802.1x

28.	At least for a "Large" scenario as described previously [4], the WLAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication that shall not be proposed as a separate product.	C/PC/NC

As shown in the following figure, the Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista 2500 by offering an embedded Radius server in *Wi-Fi Enterprise mode* for 802.1x and MAC authentication. This embedded server is called *Unified Policy Access Manager* (UPAM-NAC) and is inherent to the global solution. While ALE's competitors' proposals consist of an additional appliance or server/VM, UPAM-NAC comes in an integrated software module with the OmniVista Network Management System.

Figure 20: Unified Policy Access Manager – Enterprise mode

Much more than a built-in Radius server, UPAM-NAC is a Policy Manager that consists of a Guest Access application for visitor network access and a BYOD access solution for employee device secure onboarding.

UPAM-NAC allows for a highly flexible service model:

- RADIUS requests from a NAS (ALE or any 3rd party vendor) are checked against "Access Policies", trying to find a match between the RADIUS request parameters and the configured Access Policy parameters.
- Once a match is found, the Access Policy specifies which "Authentication Strategy" must be taken to process the information in the RADIUS request.
- Once the request has been processed, either with authentication with the local database, external AAA servers, external LDAP/AD, internal CP, or external CP, the RADIUS response is prepared and sent to the NAS device.

The following picture allows a better understanding:

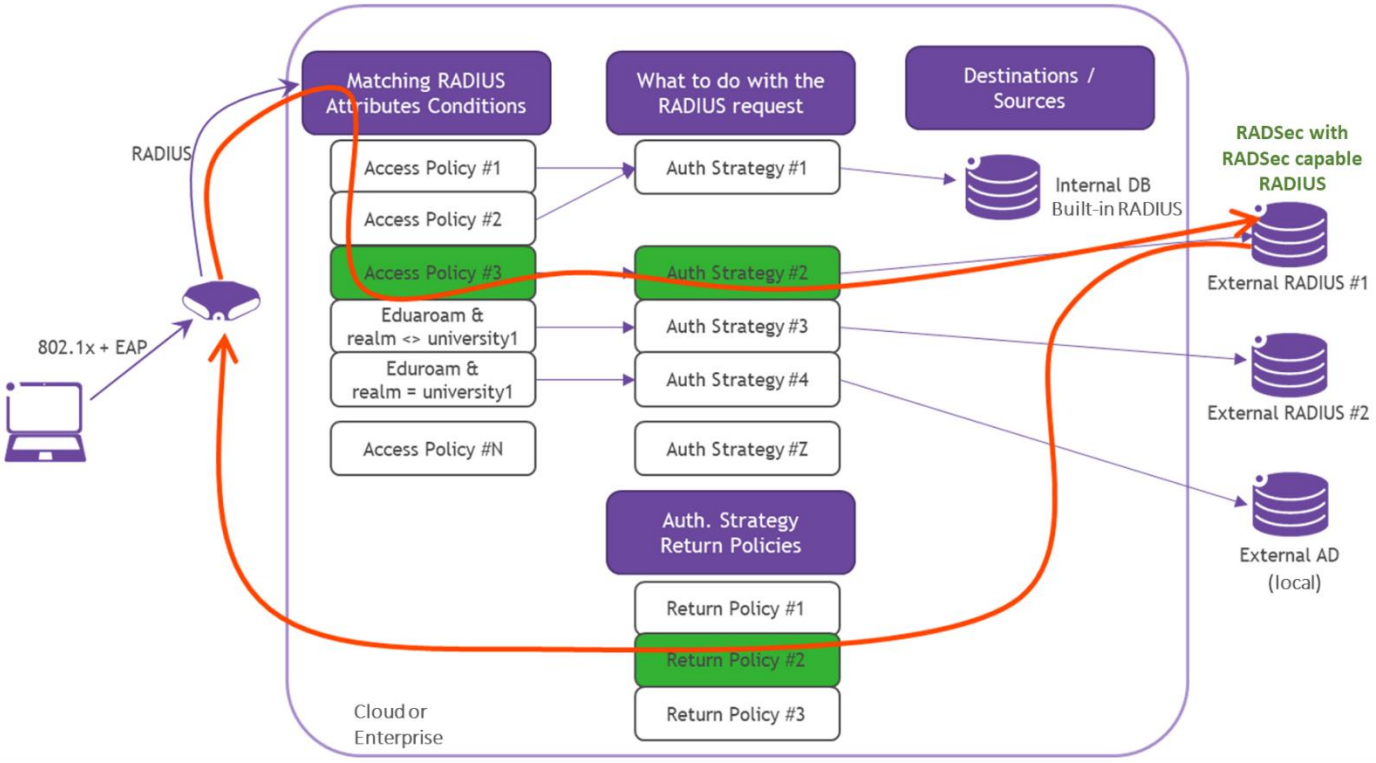


Figure 21: UPAM-NAC - How it works

29.	At least for a "Large" scenario as described previously [4], built-in RADIUS server as described previously [28] shall be able to interface with an external authentication server (Radius, LDAP, Active Directory, Microsoft Azure AD): FreeRadius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP etc.	C/PC/NC

As depicted in previous *Figure 20: Unified Policy Access Manager*, the UPAM module can be used as a "local" Radius database but can also interface with an external Radius server or with the company corporate Microsoft Active Directory or LDAP server.
Connecting to an external authentication source allows centralized user management with the possibility to assign user or device "role profiles" (VLAN, QoS and security ACL) based on AD/LDAP attributes.

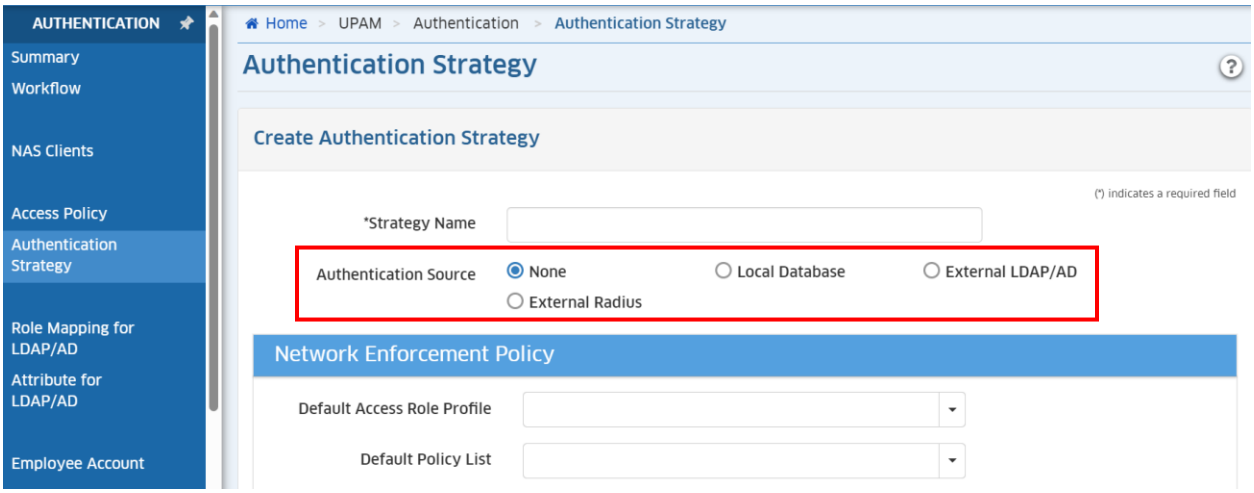


Figure 22: UPAM-NAC Access Policies – Omnivista 2500 (Authentication strategy)

Omnivista Cirrus 10 fully support backup to on-premise AD server of customer and can manage preemption to this server if required.

30.	The built-in RADIUS server as described previously [28] shall support following EAP types: EAP-MD5, EAP-TLS, EAP-AKA, EAP-PEAP, EAP-FAST, EAP-SIM, EAP-TTLS, EAP-GTC.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode*.

31.	At least for a "Large" scenario as described previously [4], the wireless LAN solution shall have the ability to utilize RADIUS attributes to assign each authenticated user/device to a specific ROLE. A role defines a VLAN and enforces security and QoS through the use of role-based ACLs and QoS policies that can be directly integrated with the roles defined within existing authentication servers.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 and supports role-based access control. OmniAccess Stellar APs utilize radius attributes to assign users or devices to roles. Once the role of the user is learned (accomplished by interfacing with existing backend authentication servers such as RADIUS, LDAP, and Active Directory) authenticated users or devices can be assigned to a specific VLAN. The OmniAccess Stellar APs have firewall capabilities and the role-based access control can even go beyond basic VLAN assignment. A pre-defined profile can be applied to set the VLAN but also security (network ACLs) and Quality of Service (QoS) policies for the authenticated user or device. The AP embedded firewall is identity-aware and can take permit/deny, and Quality of Service (QoS) decisions (such as setting DSCP/802.1p bits or placing the packet into a priority queue) based on the identity of the user or device and application. By applying granular policies tailored to the role of the particular user, the OmniAccess Stellar WLAN solution restricts network privileges to those appropriate to the user's role, and also greatly decreases exposure in the event that a device or user were compromised by limiting the amount of damage that can be done.

32.	At least for a “Large” scenario as described previously [4], the wireless LAN solution shall include and handle a flexible and adaptive RADIUS attributes dictionary allowing to add an IETF or any vendor specific RADIUS attribute.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. As depicted in following figure, the UPAM embedded RADIUS server available in *Wi-Fi Enterprise mode* can store multiple RADIUS attributes defined by the IETF, by *Alcatel-Lucent Enterprise*, or by any other vendor:

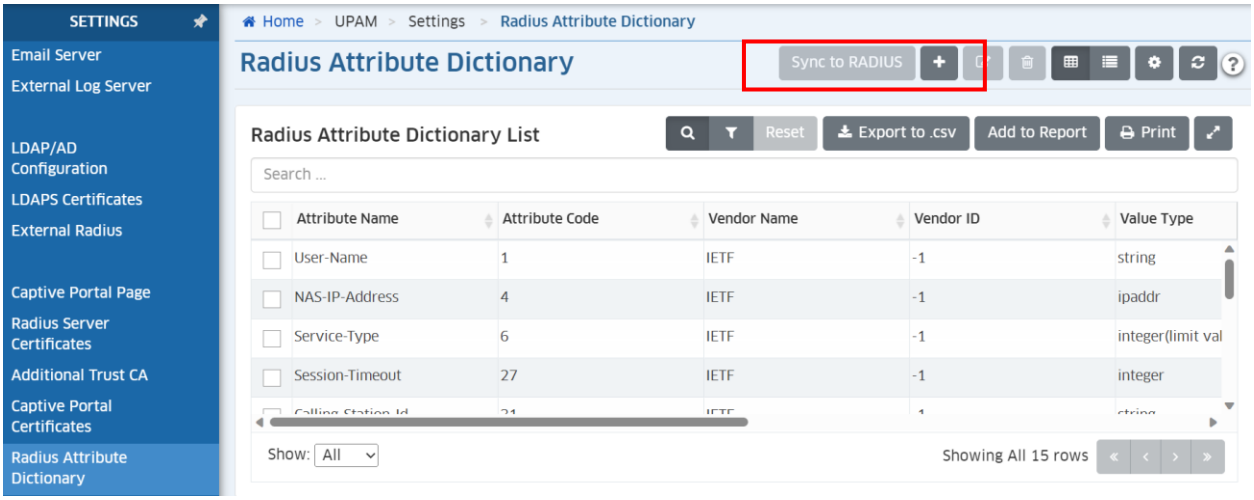


Figure 23: UPAM-NAC- Access Policies – Omnivista 2500 (RADIUS Attributes)

The RADIUS Attribute Dictionary enables UPAM to integrate with other vendor’s network infrastructure and allows UPAM to act as a RADIUS server to authenticate user requests from Third-Party devices.

33.	If the built-in RADIUS server as described previously ([302]) shall interface with an external RADIUS server, then it shall be able to interface with multiple and distinct RADIUS servers depending on specific access conditions (SSID name, Access Point IP address, identity of the connecting user…)	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. The *Wi-Fi Enterprise mode* and its UPAM module allow to define multiple external RADIUS servers as shown in following figure:

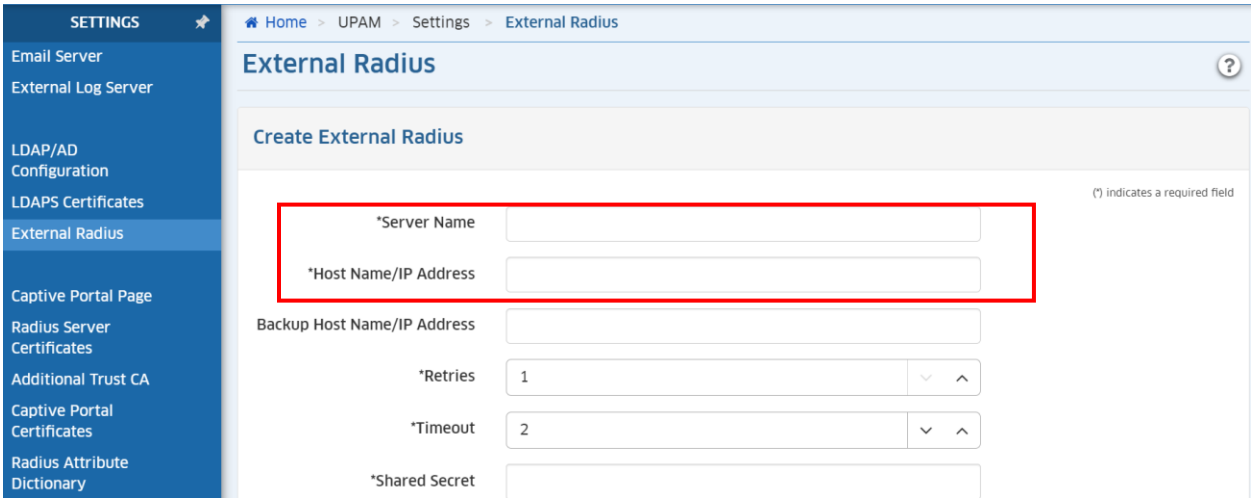


Figure 24: UPAM-NAC External RADIUS server – Omnivista 2500 (Create external RADIUS server)

The backend RADIUS server used to authenticate connecting users can be selected based on conditions defined in an "Access Policy", like the connecting SSID, the IP address or name of the connecting AP (or AP-Group), the identity of the connecting user (according to the IETF "User-Name" attribute) or any other relevant RADIUS attribute defined in the UPAM "Radius Attribute Dictionary" as described previously [92]. The defined condition can then be processed with "comparison" operators which can additionally ignore case-sensitivity:

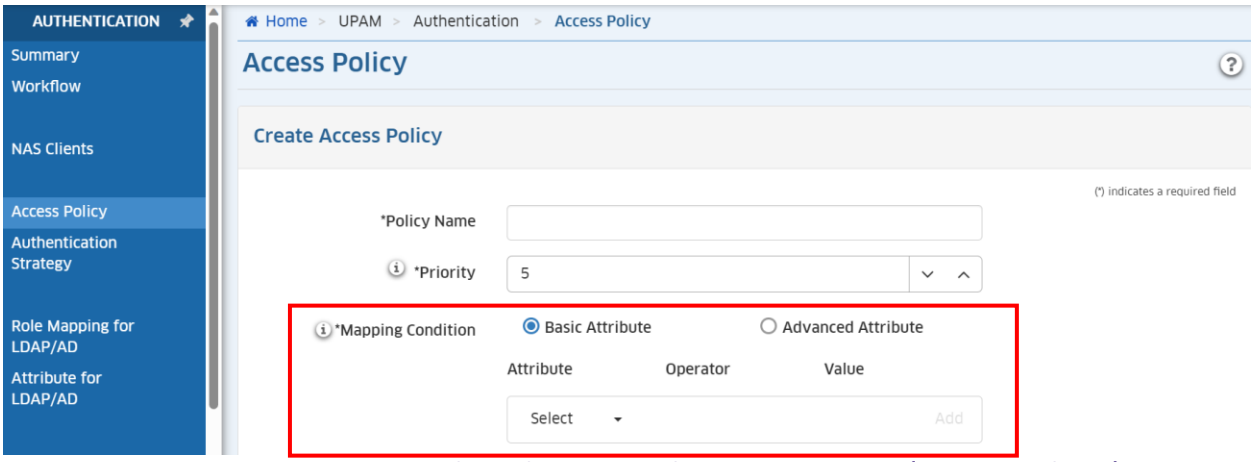


Figure 25: UPAM-NAC-Access Policy and mapping condition – Omnivista 2500 (mapping conditions)

The "Authentication Strategy" selected in the "Access Policy" will finally define the external backend RADIUS server used for user authentication:

34.	At least for a "Large" scenario as described previously [4], the wireless LAN solution shall support following link layer encryption standards: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES,	C/PC/NC

	WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP, WPA3_PSK_SAE_AES, WPA3_SAE_AES, OWE_PMF.	

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode*.

35.	At least for a "Large" scenario as described previously [4], the wireless LAN solution shall support the latest WPA3 encryption standard.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 because wireless is the primary method to access the network, and enhanced Wi-Fi security becomes a 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. WPA3 comes in two versions:

1. WPA3-Personal

It will utilize *Simultaneous Authentication of Equals* (SAE) 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 is required and can be negotiated for all WPA3 connections providing an additional layer of protection from deauthentication and disassociation attacks.

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. Additionally, WPA3 also offers an optional CNSA 192-bit cryptographic security.

Following table describes the support of the WPA3 standard according to the Access Point models in the OmniAccess Stellar portfolio:

WPA3	AP1101	A01201H	AP12XX /AP13XX /AP14XX*	
WPA3-Personal transition mode	Yes	Yes	Yes	128-bit CCMP PMF negociated
WPA3-Enterprise mode (AWOS release 4.0.5 minimum)	Yes	Yes	Yes	128-bit CCMP PMF required
WPA3 Enterprise with CNSA option	No	5GHz only	Yes	SuiteB92 mode with 256-bit GCMP PMF required

* Latest WPA3 encryption standard is the only encryption that can be used on 6GHz band used by AP14XX Wifi-6^{E} access points

Table 3: WPA3 support

36.	At least for a "Large" scenario as described previously [4], the wireless LAN solution shall support OWE encryption standard with open Wi-Fi networks	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. OmniAccess Stellar provides enhanced security and privacy for open ssids in WLAN networks (AWOS release 4.0.5 minimum), with support of the new Wi-Fi Enhanced Open security standard based on Opportunistic Wireless Encryption (OWE)

Thus, the OWE standard enables access to WLAN for users where encryption is needed but authentication is not required; like in public venues, schools, coffee shops, bars etc. OWE capable users connect to a hidden SSID and will get Protected Management Frames (PMF), otherwise known as 802.11w, that is mandatory with Opportunistic Wireless Encryption.
OmniAccess Stellar provides legacy and OWE SSID (BSSIDs) to users by default.

37.	At least for a "Large" scenario as described previously [4], the wireless LAN solution shall support following 802.1x supplicants: Windows 7, 10 (and more), MAC OS, IOS, Android, Chromebook…	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode*.

38.	At least for a "Large" scenario as described previously [4], the wireless LAN solution shall support time-based policy access to a SSID.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*.
In *Wi-Fi Enterprise mode* a time-based policy access to a SSID can be defined when Period Policy is defined as attribute in SSID "Access Role Profile". The period policy can specify a time window for all or specific days of the week during which the SSID will broadcasted by the APs of the AP-Group:

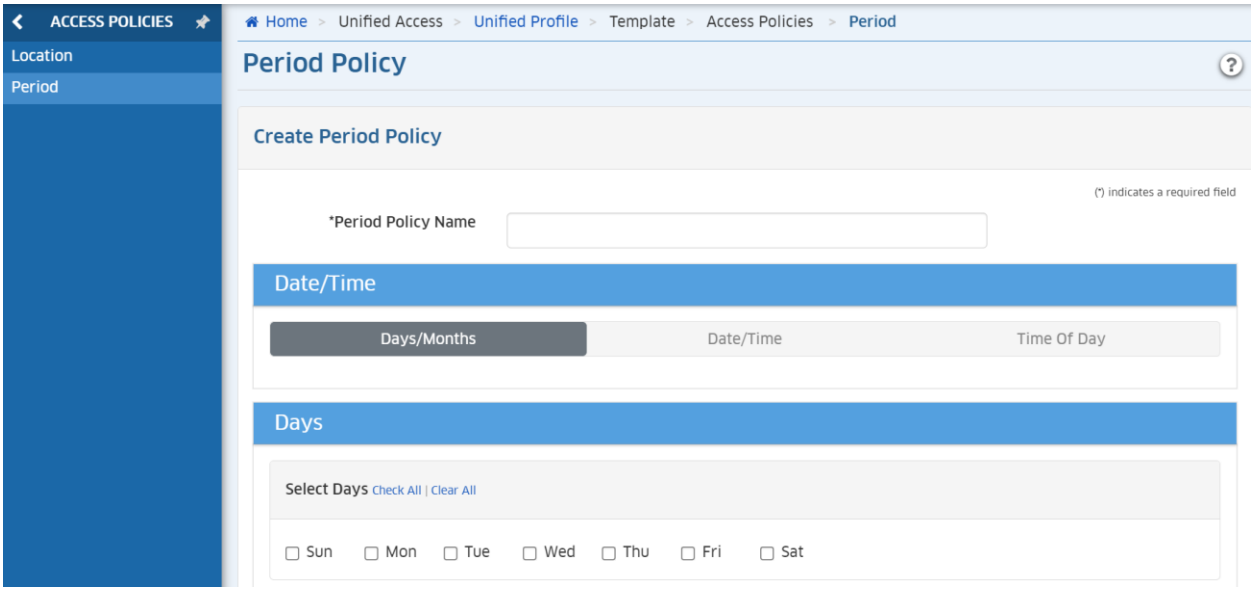


Figure 26: SSID time-based policy access - Omnivista 2500 (Period Policies)

39.	For the "Large" deployment model as described previously [4], the wireless LAN solution shall propose a "Guest" management solution based on an embedded and built-in Captive Portal providing web-based authentication for guests and visitors.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*.

In *Wi-Fi Enterprise mode*, the guests access function is handled by the UPAM-NAC module which provides an advanced and sophisticated Captive Portal with maximum customization capabilities and various access methods (employee sponsored guest access, guest self-registration…).
Descriptions [40] to [55] depict the Guest access management with Omnivista 2500.

Figure 27: OV/UPAM-NAC Captive Portal and Guest Access - Enterprise mode

40.	The Guests Captive Portal included in the wireless LAN solution shall allow a customizable look & feel.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*.

The Captive Portal provided by UPAM-NAC in Wi-Fi *Enterprise mode* is fully customizable. The logo and background page be personalized, and a "welcome" message may also be displayed:

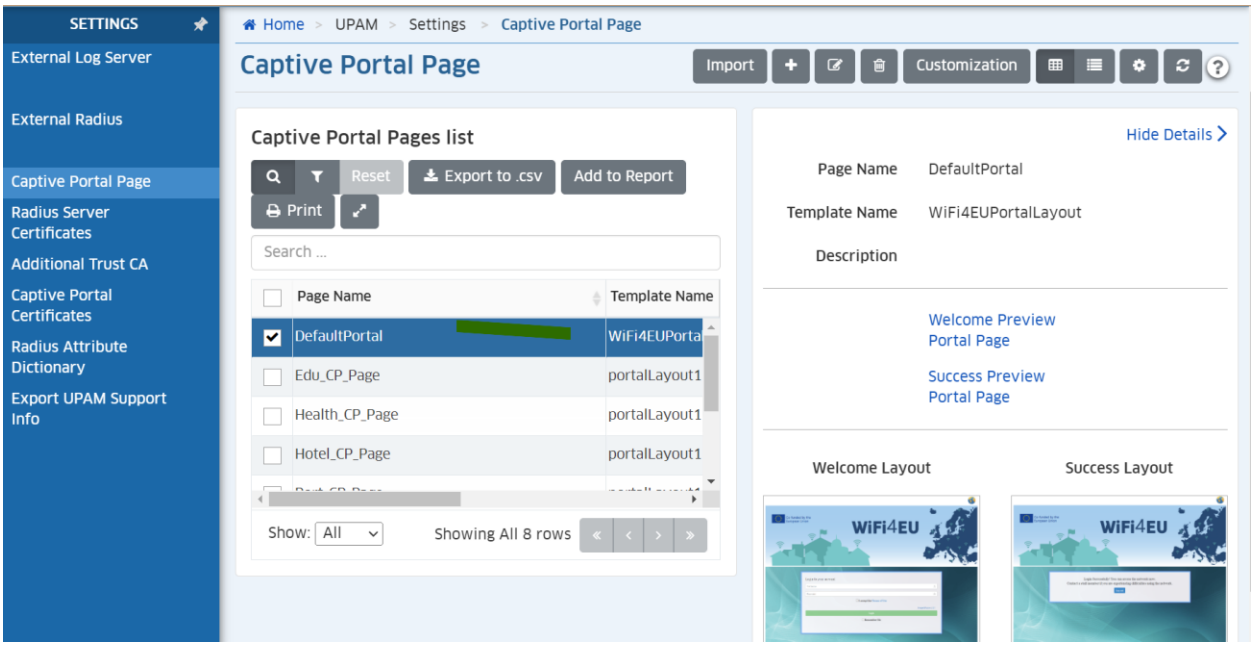


Figure 28: UPAM-NAC Captive Portal customization – Omnivista 2500 (Captive Portal Page)

Additionally, the “success page” that is displayed after a successful authentication may also be modified for a personal look & feel:

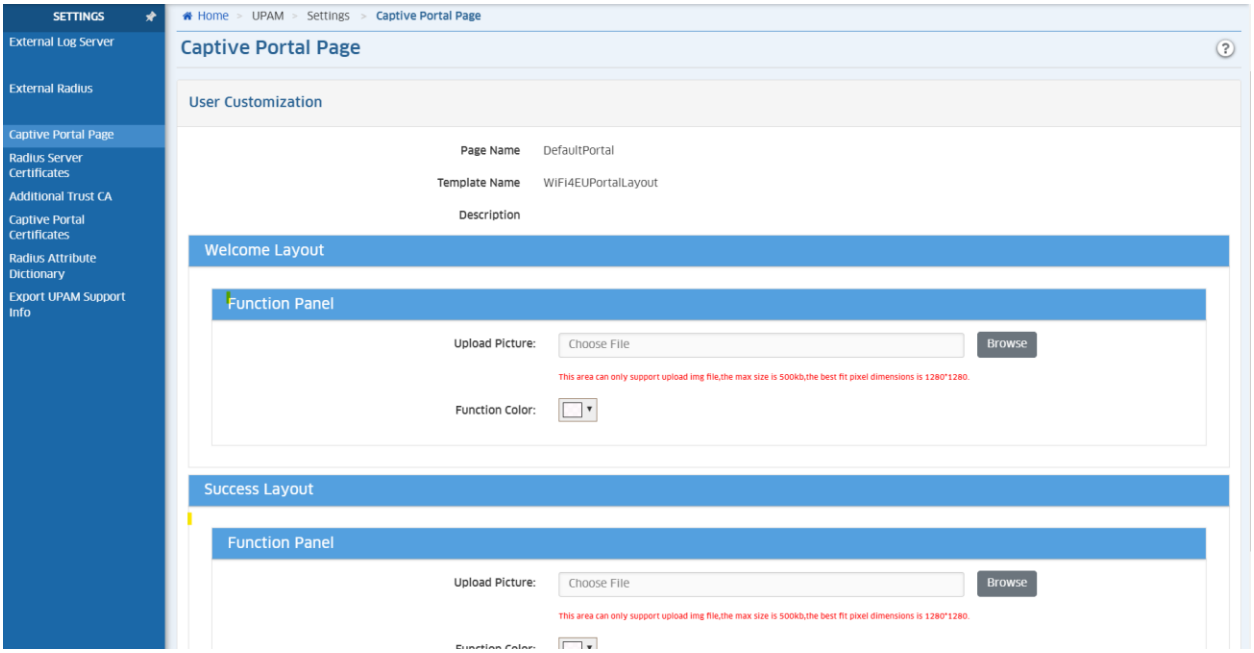


Figure 29: UPAM-NAC “success page” customization – Omnivista 2500 (Captive Portal Page)

To allow customization with maximum flexibility, a Captive Portal template can be downloaded as a zip file containing all files building the portal for individual modification. The files can then be zipped again and uploaded to the UPAM server for a new and totally customized Captive Portal:

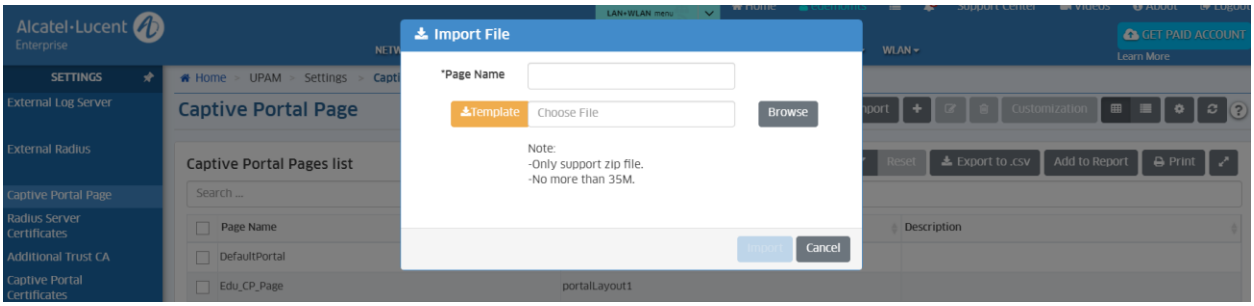


Figure 30: UPAM-NAC Captive Portal full customization – Omnivista 2500 (Captive Portal page)

41.	The Guest management solution shall allow, at least, following authentication methods: ▪ Username & Password ▪ Access Code ▪ Simple Term & Condition acceptance	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*.

42.	A least for a "Large" scenario as described previously [4], the Guest management solution shall allow guests to authenticate using their favorite social network account (supported social networks shall be listed).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. That is one of the advanced options offered by the UPAM Guest management application:

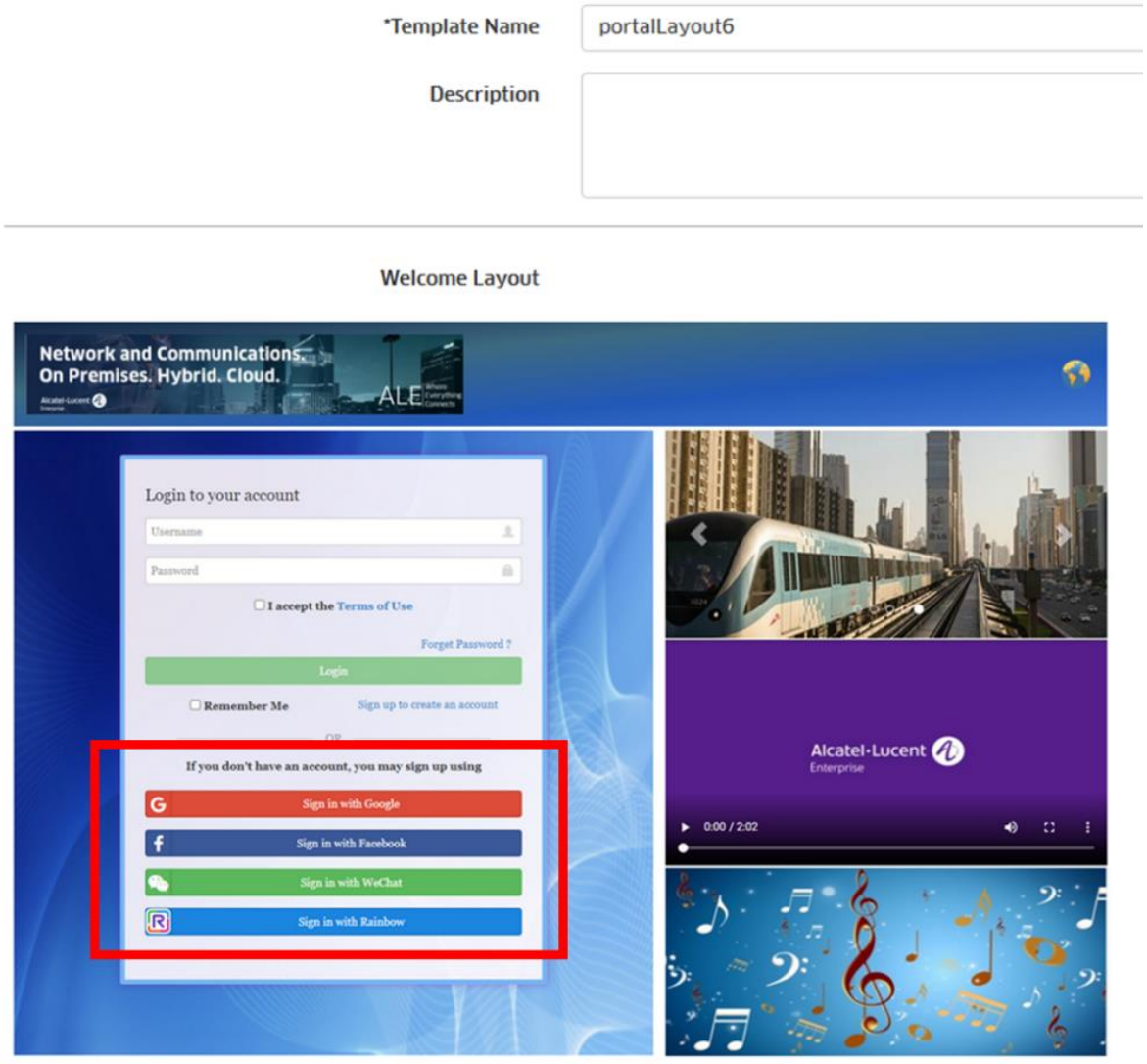


Figure 31: UPAM-NAC Guest social login – Omnivista 2500 (Captive Portal page)

Indeed, Guests expect today a quick and simple process when they log in to the Wi-Fi network and case studies reveal that social Wi-Fi login is the preferred user interaction method that provides them Internet access: users are always logged-in on their devices so it usually takes a single click to authenticate.

Facebook, *Google* and *Twitter, WeChat*, Alcatel-Lucent Enterprise *Rainbow* and *Office 365* (Microsoft Azure) are the social networks supported today.

The social login option is made available on the UPAM-NAC embedded Captive Portal if "*Social Media Account*" is enabled in the "Guest Access Strategy".

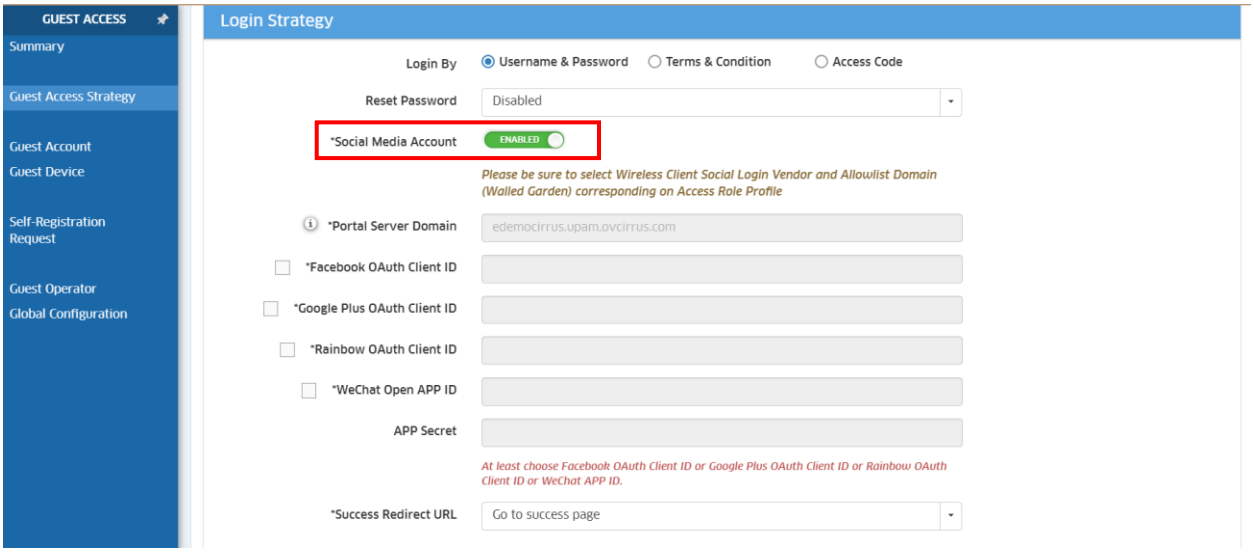


Figure 32: Guests Social Login method – Omnivista 2500 (Guest Access Strategy)

43.	For the "Large" deployment model as described previously [4], the wireless LAN solution shall offer the possibility to build a walled garden environment (with configured domain names) for guest users before they authenticate.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Any domain name may be entered as a "Whitelist Domain" to allow a guest to connect to authorized sites over the Internet without authentication:

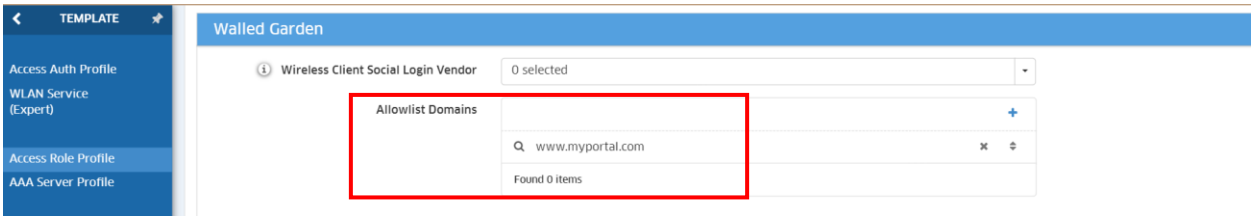


Figure 33: Walled Garden – Omnivista 2500 (Access Role Profile)

Walled Garden environments may be useful in a situation where, for instance, a hotel wants to allow a guest to connect to their website without authentication.

44.	The Guest management solution shall allow non-IT staff (e.g., a receptionist) to create temporary guest accounts.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*.

In Wi-Fi *Enterprise mode*, and from the OmniVista 2500 NMS, the administrator can create multiple "Guest Operators" accounts to manage guests' access:

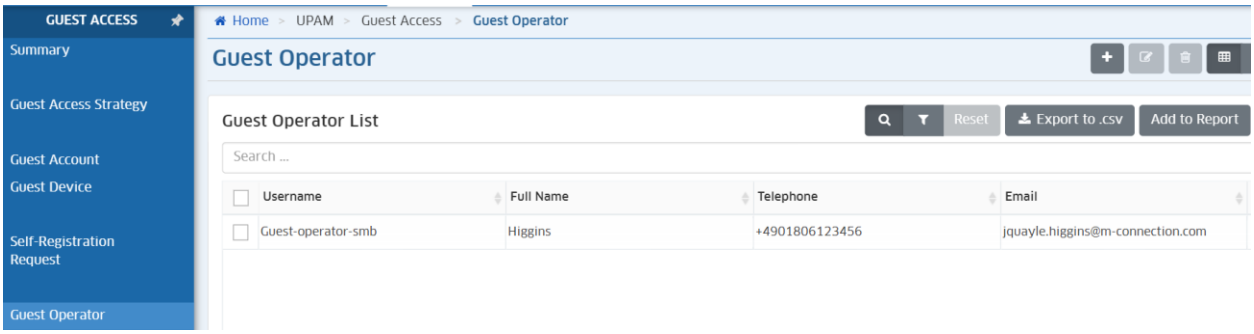


Figure 34: Guests Operator accounts creation – Omnivista 2500

45.	A least for a "Large" scenario as described previously [4], the WLAN solution shall allow guest self-registration and employee sponsored access.	C/PC/NC

Guests accounts can be created by a Guest Operator as previously described. In addition, and in Wi-Fi *Enterprise mode*, guests accounts can also be self-created by guests when they are redirected to the Captive Portal if "Self-Registration" is enabled in the "Guest Access Strategy":

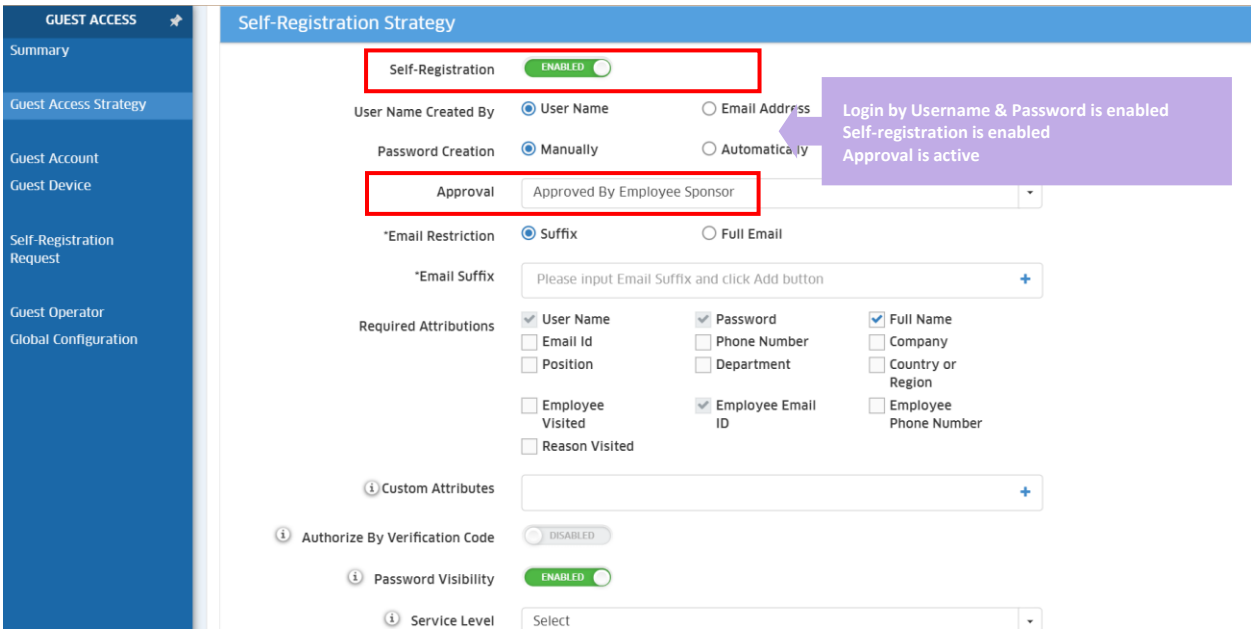


Figure 35: Guest self-registration – Omnivista 2500 (Guest Access Strategy)

The self-registered guest account will not be usable immediately if "*Approved by Sponsor*" is enabled in the "Guest Access Strategy". The account will be usable after either:

- it is approved by an "Employee Sponsor" which must have been provisioned in the UPAM "Employee" internal database or must "exist" on an external AD/LDAP server interfacing with UPAM.
- or it is approved by a Guest Operator.

The self-registered guest account will be usable immediately if "*Approved by Sponsor*" is disabled in the "Guest Access Strategy".

The Guest Operator and the Employee Sponsor can access to the same User Interface to approve the self-registered guest account:

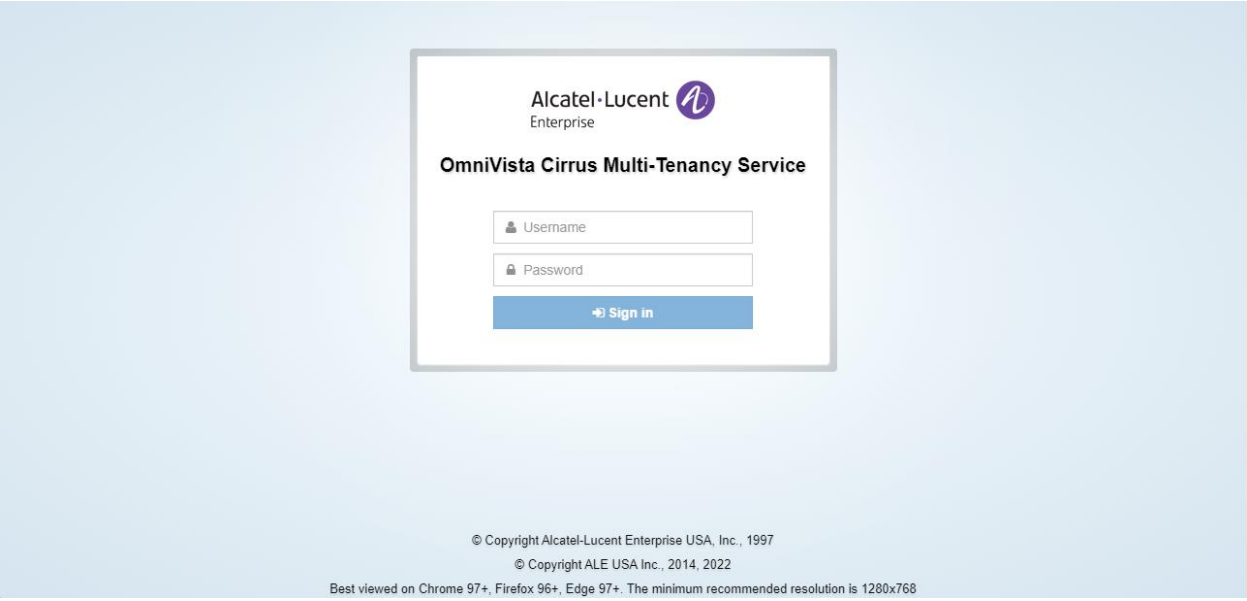


Figure 36: Guest Operator & Employee Sponsor UI – Omnivista 2500

46.	The WLAN solution shall allow guests accounts bulk provisioning by importing a file containing guest accounts information and shall propose a template import file.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in Wi-Fi *Enterprise mode* as depicted in following figure:

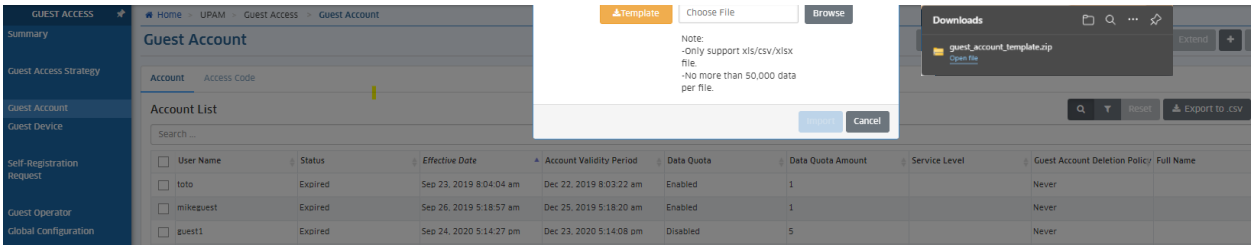


Figure 37: Guests accounts bulk import - Omnivista 2500 (Guest Account)

47.	A least for a "Large" scenario as described previously [4], the WLAN solution shall allow to create batch of guests accounts just by specifying a guest prefix and a number of accounts to be created.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution, in Wi-Fi *Enterprise mode*, fully complies with this requirement when managed by Omnivista 2500 as depicted in following figure:

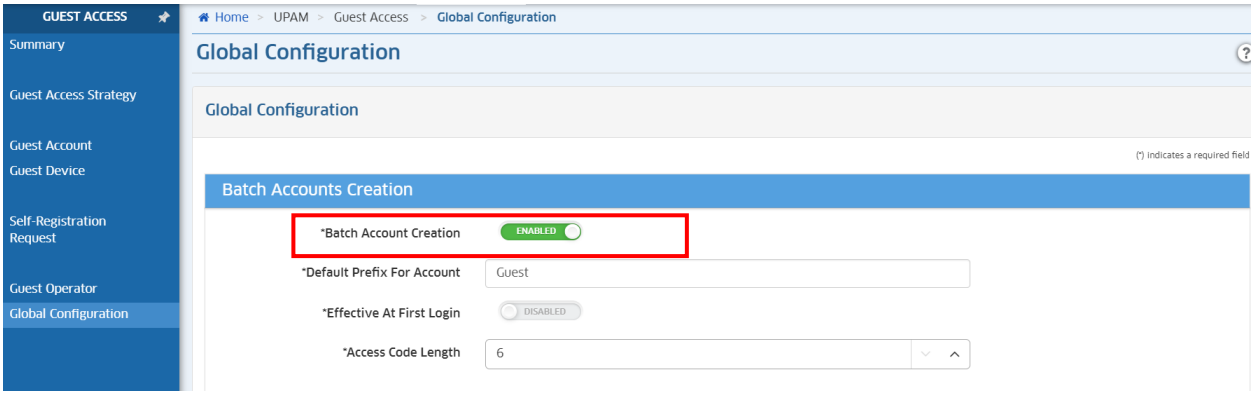


Figure 38: Guest accounts batch creation – Omnivista 2500 (Global Configuration)

Additionally, tickets for those guests can be immediately printed when they are created.

48.	A least for a "Large" scenario as described previously [4], the WLAN solution shall allow to define networking SLAs (security, QoS…) to be applied to guest network connections.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In Wi-Fi *Enterprise mode*, the network administrator can configure "Service Levels". A "Service Level" can specify a user role as previously defined [31] or a "Policy List" that will be applied to the network connection and that will apply security ACLs or QoS rules:

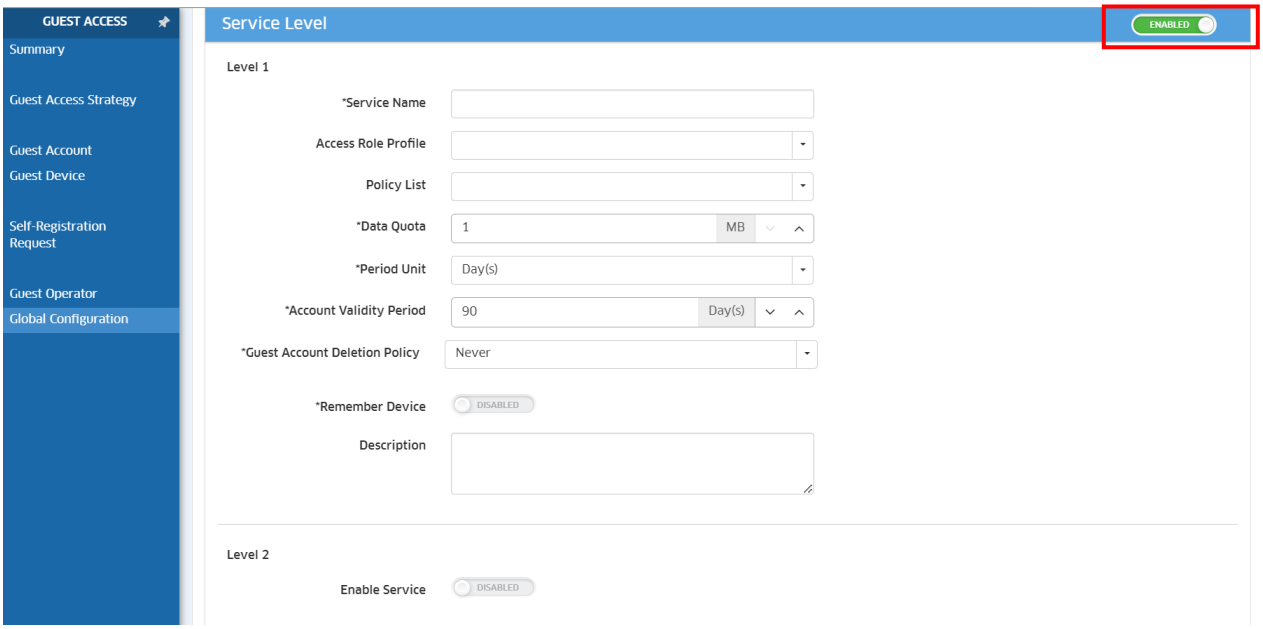


Figure 39: Service Levels - Omnivista 2500 (Global Configuration)

A maximum of five “Service Levels” can be defined. A “Service Level” can then be applied to a specific guest when his account is created:

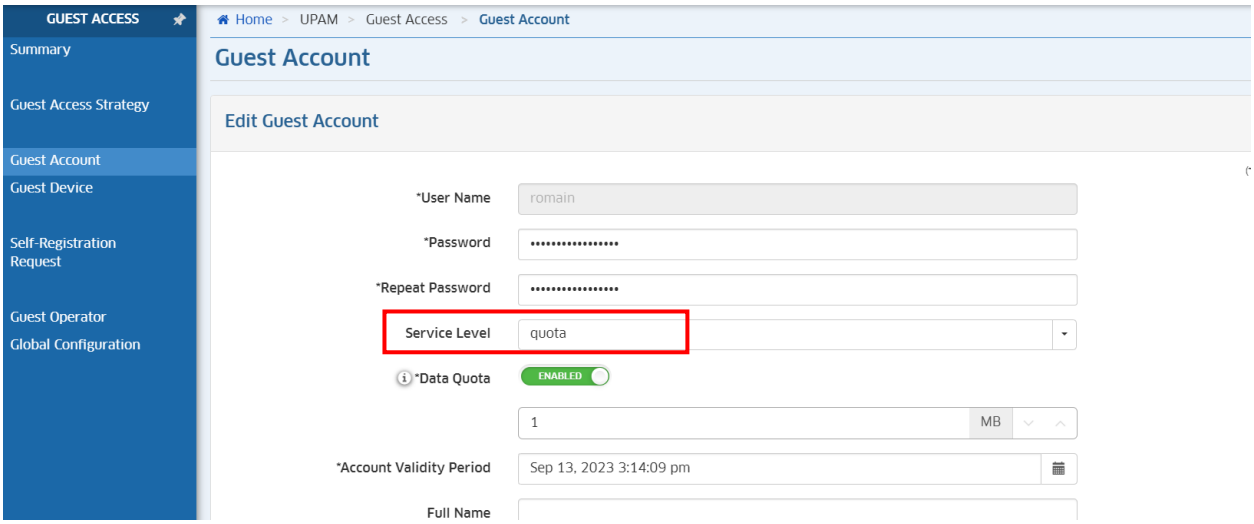


Figure 40: Service Level and Guest account - Omnivista 2500 (Guest Account)

49.	A least for a “Large deployment” scenario as described previously [4], the WLAN solution shall allow to define and apply “data quotas” to guests to limit access based on total traffic consumed.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In Wi-Fi *Enterprise mode*, the network administrator can configure a data quota at global configuration level that will be applied to all guest users. Additionally, each “Service

Level" as previously described [48] can specify a data quota that will be applied to a category of guests, or a data quota can be defined at guest level when his account is created:

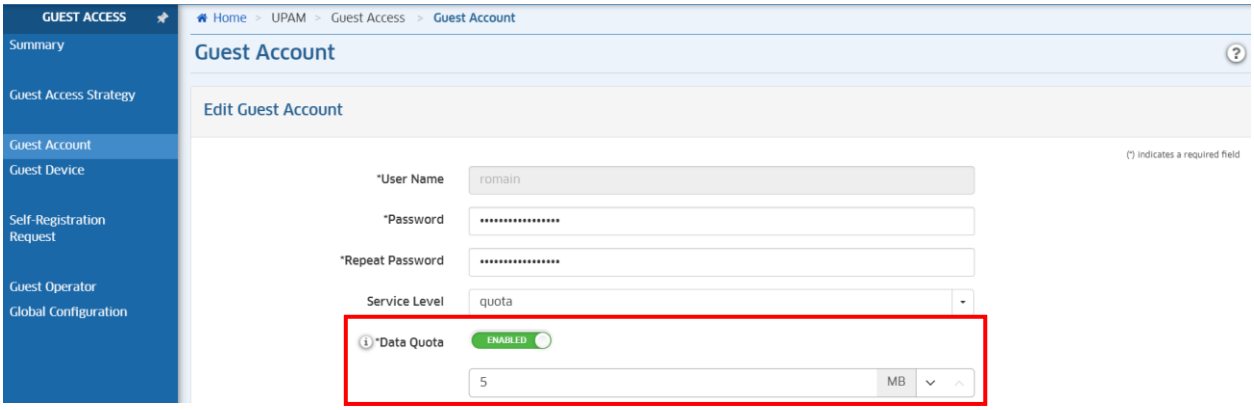


Figure 41: Guest data quota – Omnivista 2500 (Guest Account)

Data quotas are applied with a priority order: "Guest Account" first, then "Service Level", and finally, "Global Configuration". When no data quota is defined, no traffic limit is imposed and when the quota exhausts, the guest may be redirected to a pre-configured URL or to the Captive Portal login page.

50.	A least for a "Large deployment" scenario as described previously [4], the WLAN solution shall allow guests SMS notification.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. The *Wi-Fi Enterprise mode* offers the "SMS gateway" feature which allows to connect to a SMS Provider to send SMS messages (containing login credentials) to new guests when their accounts are created.

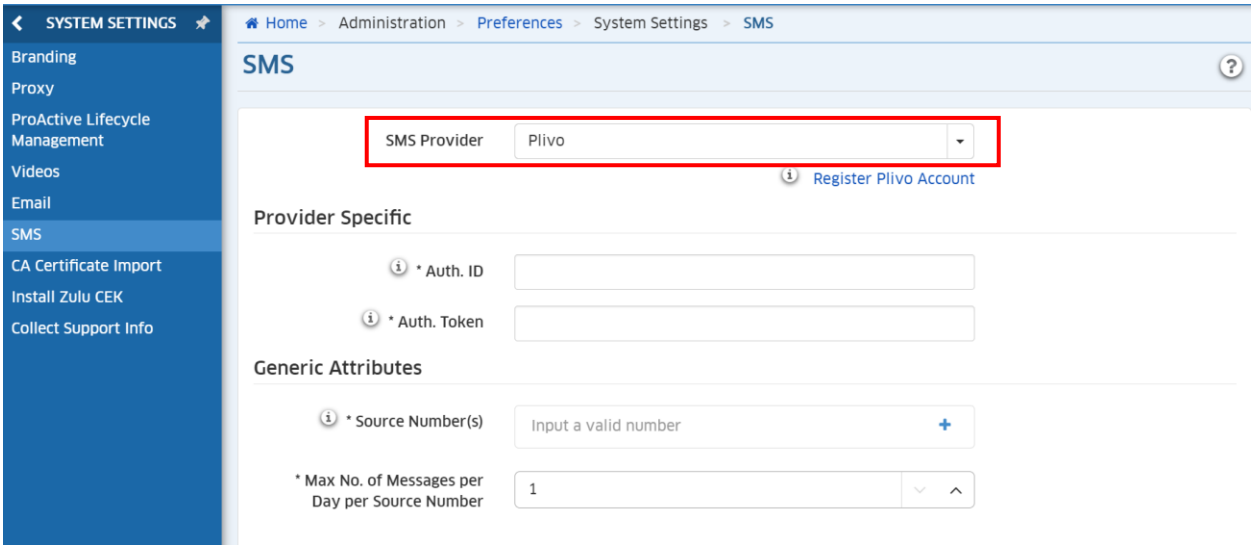


Figure 42: SMS gateway – Omnivista 2500 (System Settings)

OmniVista allows to configure a connection to a third-party SMS provider (*Plivo*) to process SMS messages and set SMS preferences. A *Plivo* account can be created at: https://www.plivo.com.

51.	For the "Large" deployment model as described previously [4], the wireless LAN solution shall offer the possibility to interface with a third-party external Captive Portal for guest authentication, without necessarily forcing the traffic to through any server or appliance.	C/PC/NC

In Wi-Fi *Enterprise mode*, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 by using a standard approach of HTTP(s) redirection and Radius authentication:

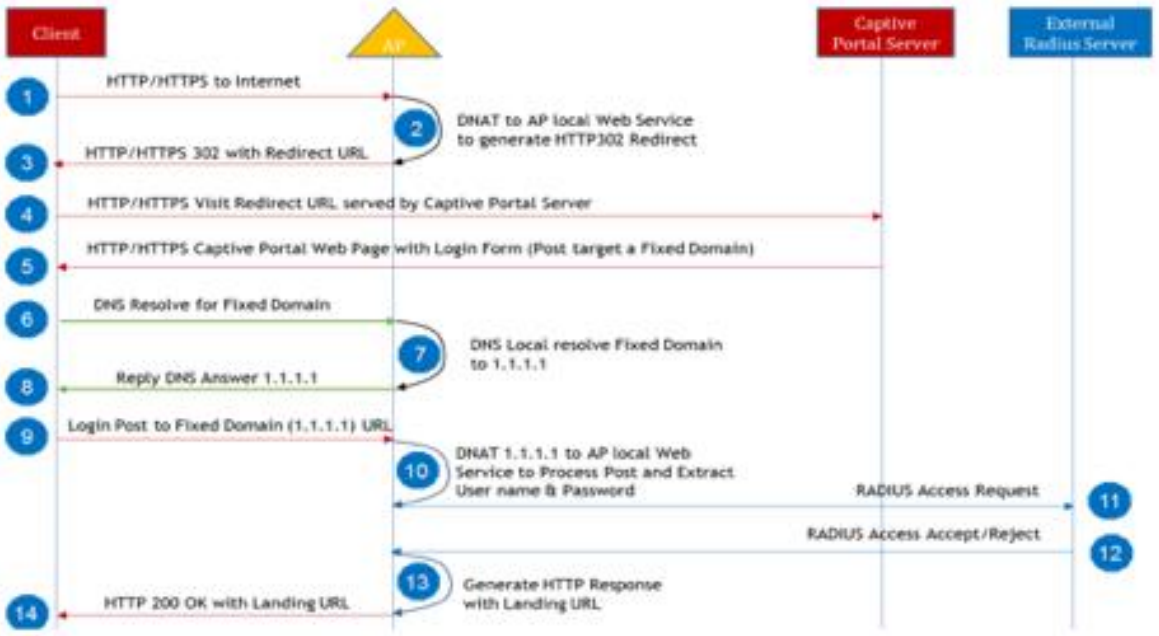


Figure 43: External Captive Portal Process Flow

Alcatel-Lucent Enterprise is constantly working to open the OmniAccess Stellar solution by performing interoperability tests with other third-party external Captive Portals on the market. Today, the OmniAccess Stellar solution is certified to work with following third-party Captive Portal solutions: *Ucopia*, *Octopus*, *Ohmyfi*, *Aislelabs*, *Zoox Wi-Fi*, *Adypsis, Antamedia, Weblib, Boundless, Cloudi-Fi* and *Encapto Wi-Fi* or Aruba *Clearpass*.

52.	For a "Large deployment" scenario as described previously [4], the licensing model of the Guest management solution shall be based on the number of devices.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

53.	For a "Large deployment" scenario as described previously [4], the Guest management solution shall allow setting a validity period for an authenticated device, in order to avoid entering credentials each time a guest access the network.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

54.	A least for a "Large deployment" scenario as described previously [4], the WLAN solution shall implement strict Guests traffic isolation.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In Wi-Fi *Enterprise mode*, a dedicated OmniSwitch® 6860 or 6900 switch handles the Guest Isolation feature. The switch acts, indeed, as a GRE tunnel gateway, terminating the guests GRE tunnels established by the APs and applying firewalling rules for a strict control of the guest traffic, thus blocking traffic between guests even if guests are in the same VLAN, and isolating the guest network from the rest of the network:

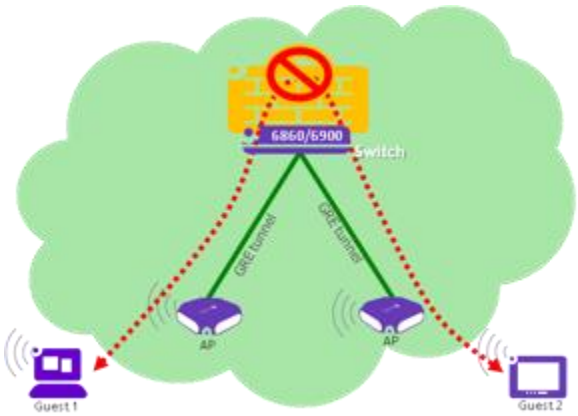


Figure 44: Guests traffic isolation

The OmniSwitch 6860 switch (for up to 750 GRE tunnels) and the OmniSwitch 6900 switch (for up to 1000 GRE tunnels) are equipment from the Alcatel-Lucent Enterprise OmniSwitch LAN portfolio and are inherent parts of the OmniAccess WLAN Stellar global solution.

Please note that in *Wi-Fi Enterprise mode*, the configuration at SSID level allows to prevent two clients that are associated to the same Access Point from communicating with each other even without a dedicated GRE gateway:

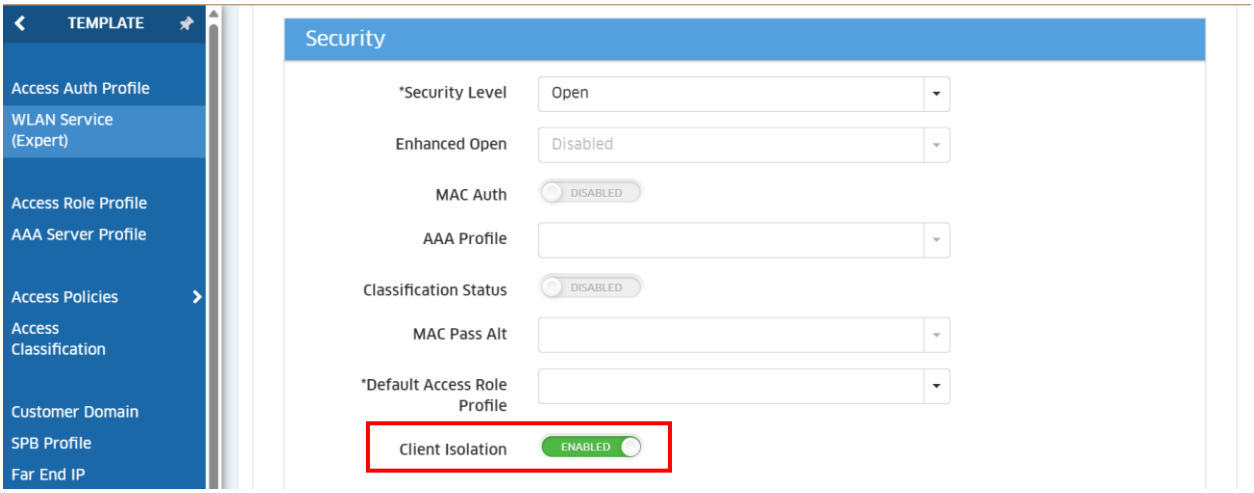


Figure 45: Guests isolation from each other – Omnivista 2500 (WLAN Service Expert)

In that case, the rest of the network is not isolated from guests' traffic (and vice versa) and if isolation between guests is required even if they are associated to different APs, then an ACL (at SSID level) may be configured and applied to block traffic between guest clients.

Stellar Enterprise (AWOS release 4.0.5 minimum) can also configure the ACL (at SSID level) with an additional list of @MAC for which clients will be allowed to communicate with.

Otherwise client isolation only allow communications with GRE gateways.

55.	The WLAN solution shall allow data retention on user sessions when providing Guest Wi-Fi.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. The OmniAccess Stellar WLAN solution allows to track guests' connections and to log detailed guest traffic information at TCP, UDP and HTTP/HTTPs level by recording the domain names of the websites visited by users.

The following picture shows how "client behavior" tracking can be configured in *Wi-Fi Enterprise mode*:

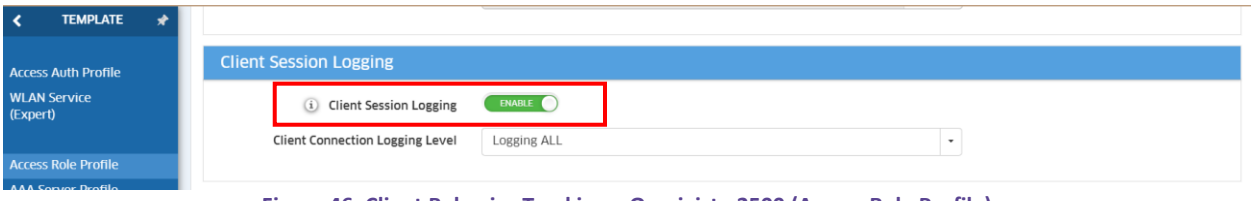


Figure 46: Client Behavior Tracking – Omnivista 2500 (Access Role Profile)

The client behavior log storage requires an additional and external TFTP or sFTP or Syslog logging server in *Enterprise Wi-Fi mode*.

56.	In the framework of a "Large deployment" scenario as described previously [4], the WLAN solution shall support BYOD and be able to provide device on-boarding that is as simple as possible and without requiring additional third-party components.	C/PC/NC

As depicted in following figure, the UPAM-NAC module of the OmniAccess Stellar WLAN solution (*Wi-Fi Enterprise mode*), includes a BYOD application that allows easy device on-boarding with Captive Portal registration for employees.

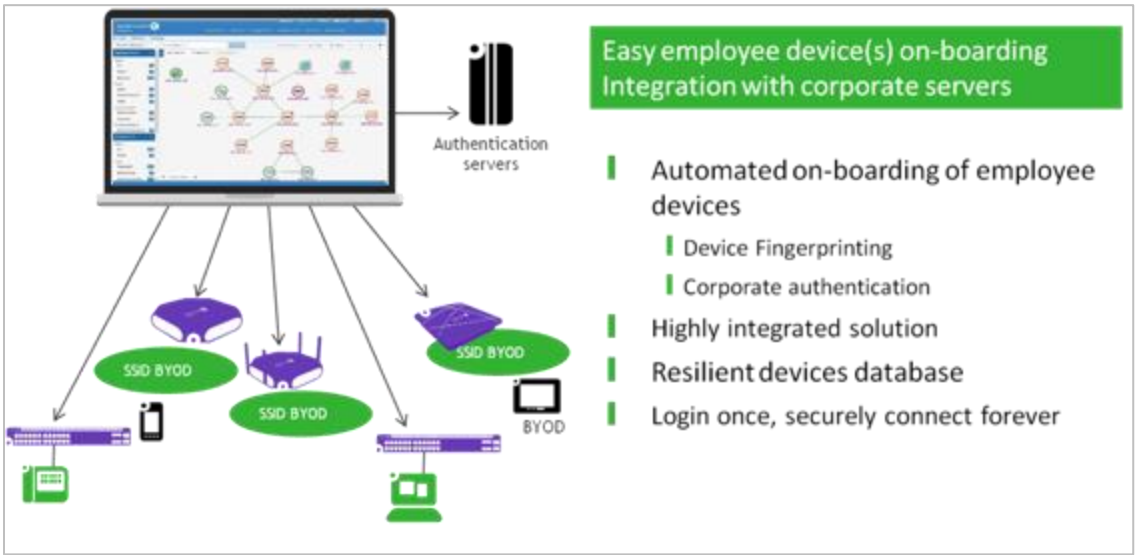


Figure 47: OV/UPAM-NAC Captive Portal and BYOD - Enterprise mode

57.	The on-boarding process of employee devices shall be based on employee corporate accounts.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, the BYOD Captive Portal asks the employee to provide his corporate login/password in order to authenticate and on-board his device. This is possible thanks to the capability of the UPAM module to interface with the company corporate authentication server like a LDAP server or a Microsoft Active Directory server. Nevertheless, the employee account can be locally created.

58.	The BYOD application shall allow setting the validity period for the device, and the maximum number of devices per account.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

59.	The licensing model of the BYOD application shall be based on the number of on-boarded devices.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

60.	A least for a "Large" scenario as described previously [4], the WLAN solution shall support DSPSK to allow the use of different Pre-Shared Keys (PSK) for WPA2 encryption standard in the same SSID at the same time	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. The basic PSK per SSID poses a security risk in having a common PSK for network access for all users. With DSPSK (Device-Specific PSK) supported for WPA2 PSK security modes administrator can now assign a secure PSK for each end device or a group of end-devices in the same SSID.

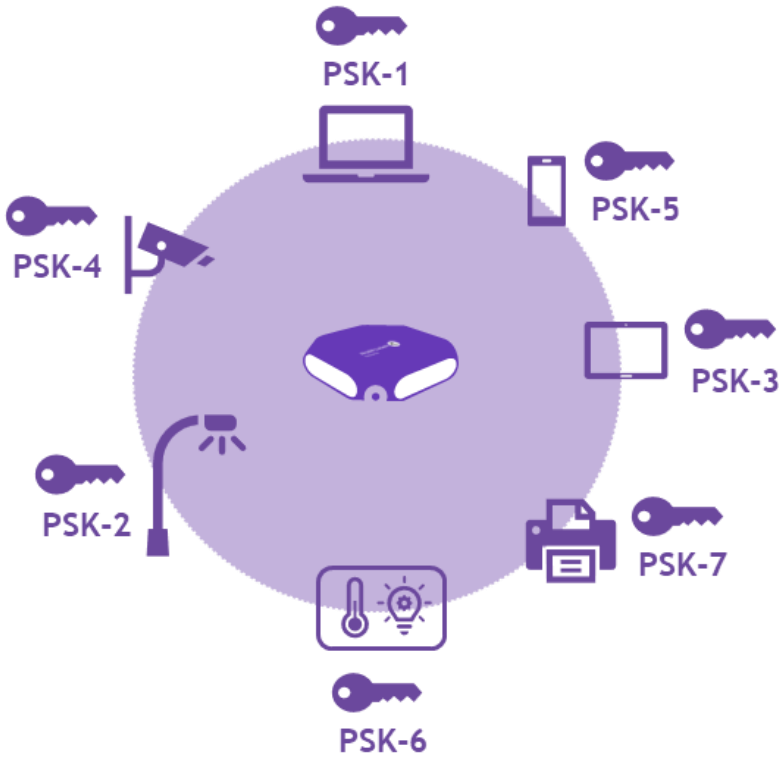


Figure 48: Stellar AP support for DSPSK

The SSID has to be configured for "Device Specific PSK" with this, MAC-auth also gets enabled. DSPSK works with UPAM authentication service in Omnivista 2500.
UPAM needs a new database for "Device Specific PSK" and the entries will be tied with SSID (BSSID). For every MAC-Auth failure, UPAM will record in the database the MAC & SSID & time of the request. Administrator can decide either to allow assisted key generation or manually specify a device-specific key for the device. Administrator via manual provisioning can configure two or more devices with the same

PSK if needed. The administrator can print a ticket with the MAC address, SSID & PSK, and the same can be printed in a QR code.

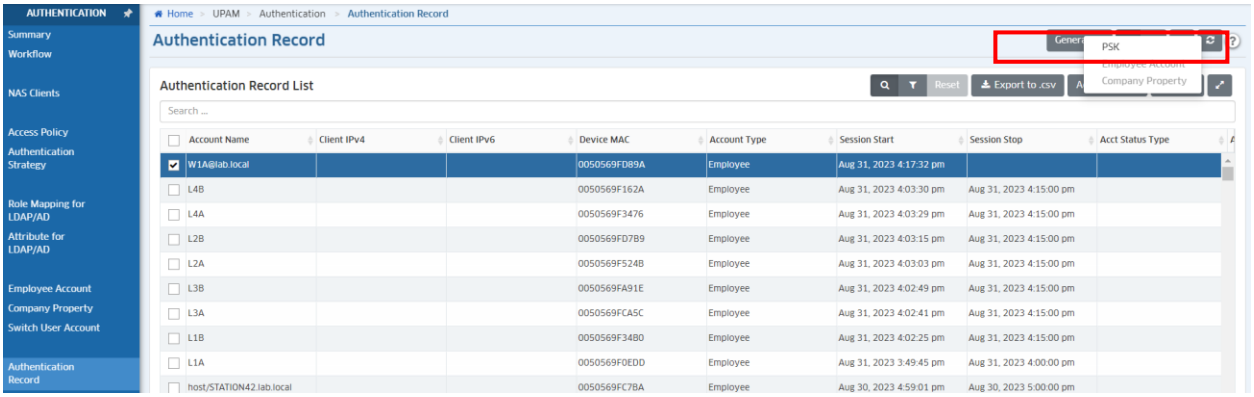


Figure 49: DSPSK generation with device MAC – Omnivista 2500 (Authentication Record)

61.	A least for a “Large” scenario as described previously [4], the WLAN solution shall support the WIFI4EU initiative from the EU. That includes support for Hotspot 2.0 (Passpoint® release 3 Wi-Fi Alliance certification program)	C/PC/NC

OmniAccess Stellar WLAN is fully compliant with this requirement when managed by Omnivista 2500.

The WiFi4EU initiative promotes free access to Wi-Fi connectivity for citizens in public spaces, including parks, squares, public buildings, libraries, health centers, and museums in municipalities throughout Europe.

Any WiFi installation network participating in WiFi4EU should comply with the conditions stated in the applicable Grant Agreement and annexes. This implies compliance with specific requirements regarding EU visual identity, usage, and network quality. The European Commission (EC) is verifying the compliance of the participating networks by providing a “Policy Enforcement Component”, also known as “the snippet”. The snippet is a piece of JavaScript code that needs to be integrated into the captive portal page of the participating network. It verifies the captive portal's compliance in terms of visual identity, counts the number of users, and measures connection speed and latency. The EC collects this data to monitor the WiFi installation's operational state and usage, allowing operational validation before voucher payment or potential recovery in case of non-compliance.

OmniAccess Stellar WLAN and OmniVista solution incorporate the Policy Enforcement Component (snippet) in the WIFI4EU Captive Portal template (WiFi4EuPortalLayout). One of the multiple Captive Portal templates OmniVista has pre-defined is the WIFI4EU. This Captive Portal profile incorporates the Policy Enforcement Component (snippet).

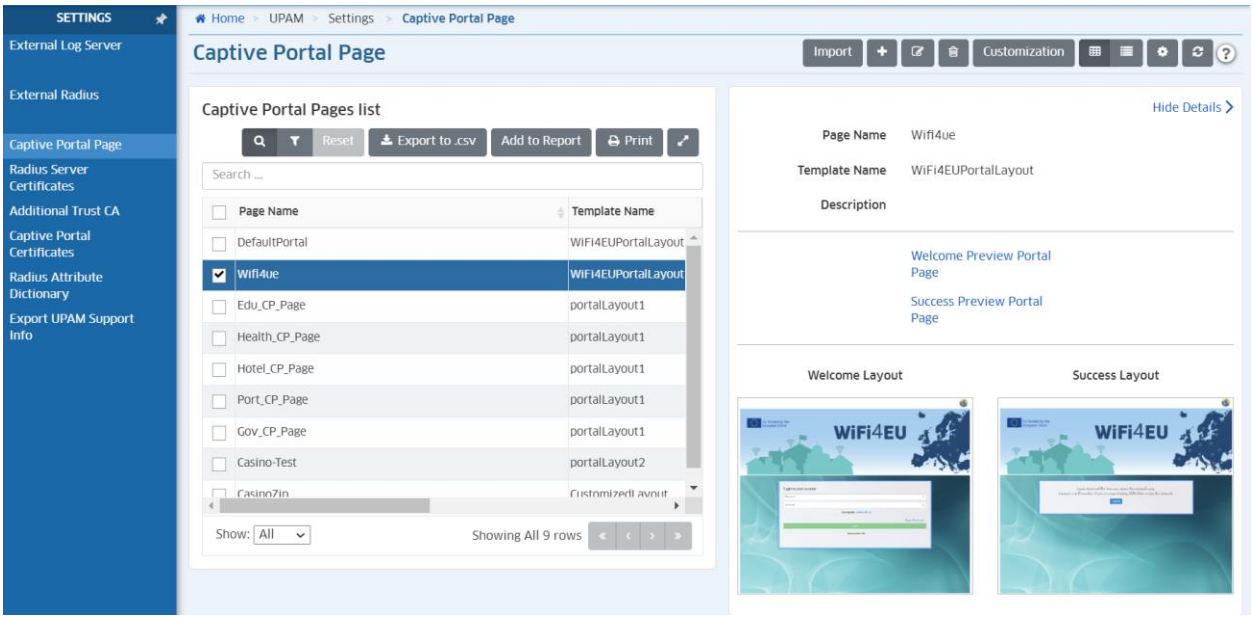


Figure 50: WIFI4EU Captive Portal template – Omnivista 2500 (Captive Portal page)

OmniVista allows to configure the snippet parameters:

- WiFi4EU network UUID: the Universally Unique Identifier (UUID) that the EC attributed to this WiFi4EU network installation. It is generated when the network installation is created in the Installation Report and cannot be changed.
- IP Address/Range: the public IP address or IP address range from which the snippet will send the monitoring data to the EC. This address/range will be whitelisted in the EC data collection firewall to exclude unknown sources' communication.
- Captive portal name: the snippet's Uniform Resource Locator (URL) of the captive portal page. The EC will verify the compliance of this page with the WiFi4EU requirements.

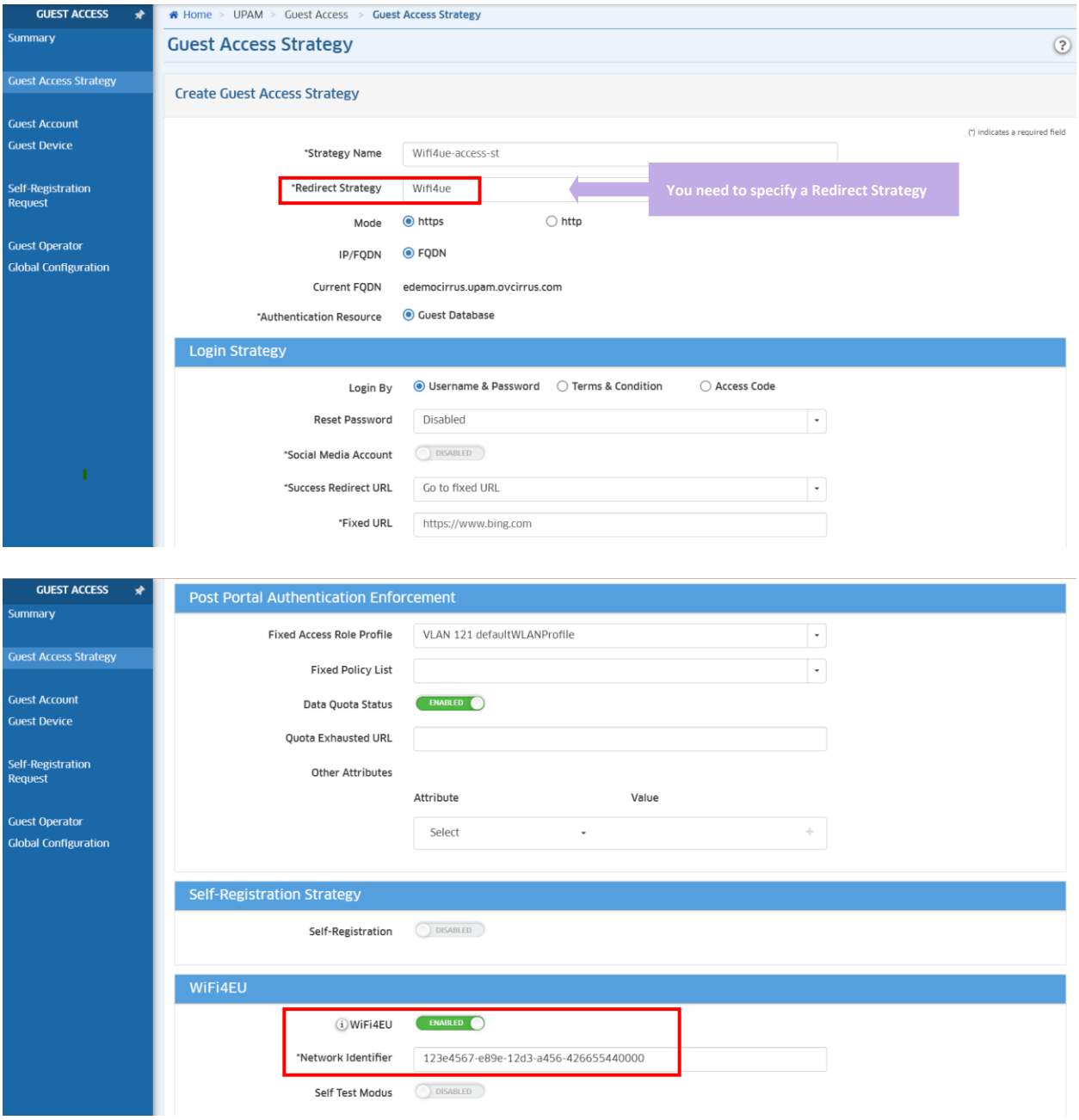


Figure 51: WIFI4UE Captive Portal snippet configuration – Omnvista 2500 (Guest Access Strategy)

EC mandates that the APs for WIFI4EU must fulfill the following requirements:

- Supports concurrent dual-band (2,4GHz – 5GHz) use
- Has a support cycle superior to 5 years
- Has a Mean Time Between Failure (MTBF) of at least five years
- Has a dedicated and centralized single point of management for all APs of each WiFi4EU network
- Supports IEEE 802.1x
- Complies with IEEE 802.11ac Wave I
- Supports IEEE 802.11r

- Supports IEEE 802.11k
- Supports IEEE 802.11v
- Can handle at least 50 concurrent users without performance degradation
- Has at least 2x2 multiple-input-multiple-output (MIMO)
- Complies with Hotspot 2.0 (Passpoint® release 3 Wi-Fi Alliance certification program).

All Stellar APs satisfy these requirements.

62.	A least for a "Large" scenario as described previously [4], the WLAN solution shall support the EDUROAM authentication hierarchy for Universities and Research Centers	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista 2500 are fully compliant with this requirement.

The EDUROAM Authentication Hierarchy provides the authentication service for Universities and Research Centers. Students, researchers, teachers, and other community members may reside in different universities, campuses, or premises. It is critical to define an authentication service that could facilitate access to the network resources while maintaining high-security access control.

EDUROAM is a hierarchy of RADIUS servers. All starts with a RADIUS-request coming from a Stellar AP when a new user wants to access the WLAN. The local RADIUS server in the university receives the RADIUS-request and checks the "realm". If the realm matches the local university, then the local RADIUS will send the authentication request to the local users' database (LDAP, AD, etc.). If the user is in the local university users' database, the RADIUS returns an Access-Accept to the Stellar AP, and the user is allowed to access the network. The Access-Accept may contain the VLAN or ARP (Access Role Profile) to apply to the user traffic.

If the user is not in the local users' database, the RADIUS responds with a REJECT, and the Stellar AP will not allow the user to access the network.

Until now, this is a regular RADIUS transition.

When the realm does not match with the local university, EDUROAM comes into play. The local RADIUS acts as a Proxy-RADIUS and sends the RADIUS-Request to the EDUROAM hierarchy, which will follow the path searching for the university that matches the realm in the RADIUS-Request.

Once the RADIUS-Request reaches the user's university RADIUS, it checks with the user's database. If it is a valid user, the RADIUS returns an Access-Accept to the local RADIUS, which Proxies the response to the Stellar AP. The user is allowed to enter the network.

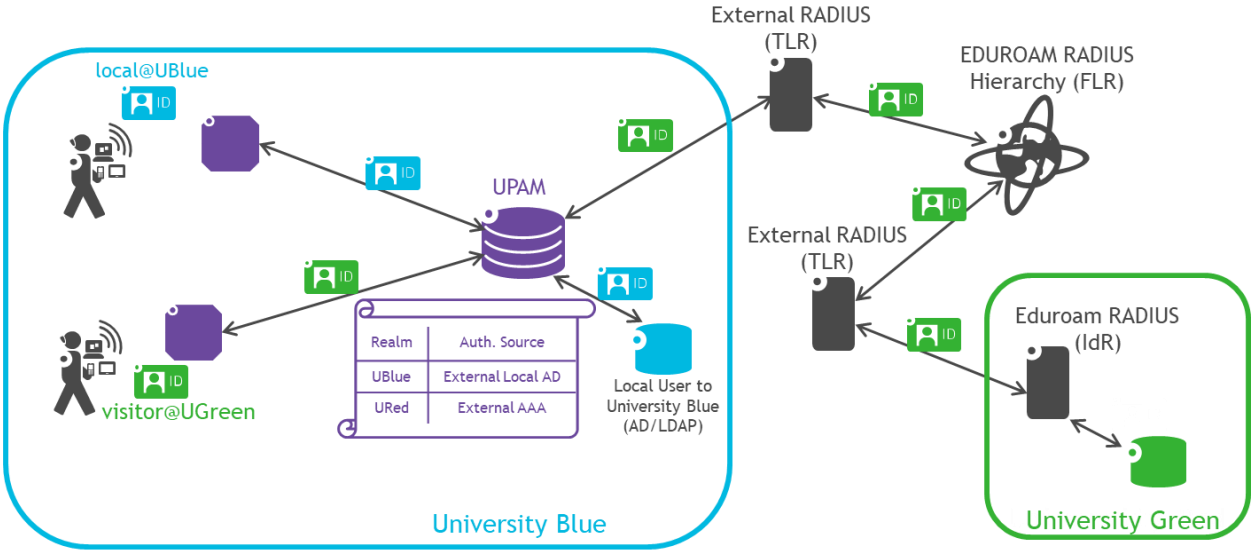


Figure 52: Stellar AP and UPAM for EDUROAM

The Stellar AP and UPAM-NAC (OmniVista) framework allow for:

- Stellar directly pointing to the Local RADIUS server, usually a FreeRADIUS server. In this case, UPAM-NAC is not needed. Local RADIUS will receive the RADIUS-Requests from Stellar APs and process them. If the university wants to leverage the ARP framework, the RADIUS server must return the ARP for the user in the Filter-ID RADIUS parameter.
- UPAM-NAC as Local RADIUS. In this case, UPAM-NAC is the only Local RADIUS. It will use the RADIUS-Request realm to resolve the authentication, either with local LDAP/AD or by sending the request to the EDUROAM hierarchy.
- UPAM-NAC as Proxy-RADIUS. In this case, there is an existing Local RADIUS (usually FreeRADIUS). UPAM-NAC will just act as a Proxy-RADIUS, sending all RADIUS-Requests from Stellar APs towards the Local RADIUS. This scenario is preferred to the first one, as UPAM-NAC has visibility about the Authentication results and will simplify troubleshooting in case of problems.

63.	A least for a "Large deployment" scenario as described previously [4], the WLAN solution shall support Web content filtering for users that connect to the Internet	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista 2500 are fully compliant with this requirement.

Stellar AP and built-in policy access manager (UPAM-NAC) as described previously [28] enable a web content access control in Enterprise mode. OmniVista 2500 manages Web Content Filtering (WCF) feature to allow/deny client access through Stellar APs to web sites based on specific security or content conditions (e.g. Malware Sites, Gambling etc). OmniVista 2500 connects to a Cloud-based Web Content Filtering Service to determine access to filtered URLs.

When the connection to WCF Cloud Service is up in UPAM module, end users are notified that a web page is blocked by OmniVista Web content filtering. A WCF Cloud Service license is consumed for each AP in AP-Groups that support web content filtering if necessary WCF feature can be disabled per AP to reduce the number of WCF licenses.

The following picture shows how a web content filtering can be configured in *Wi-Fi Enterprise mode*, WCF profile must apply to Access Role Profile or SSID managed for APs that have to support WCF Cloud service.

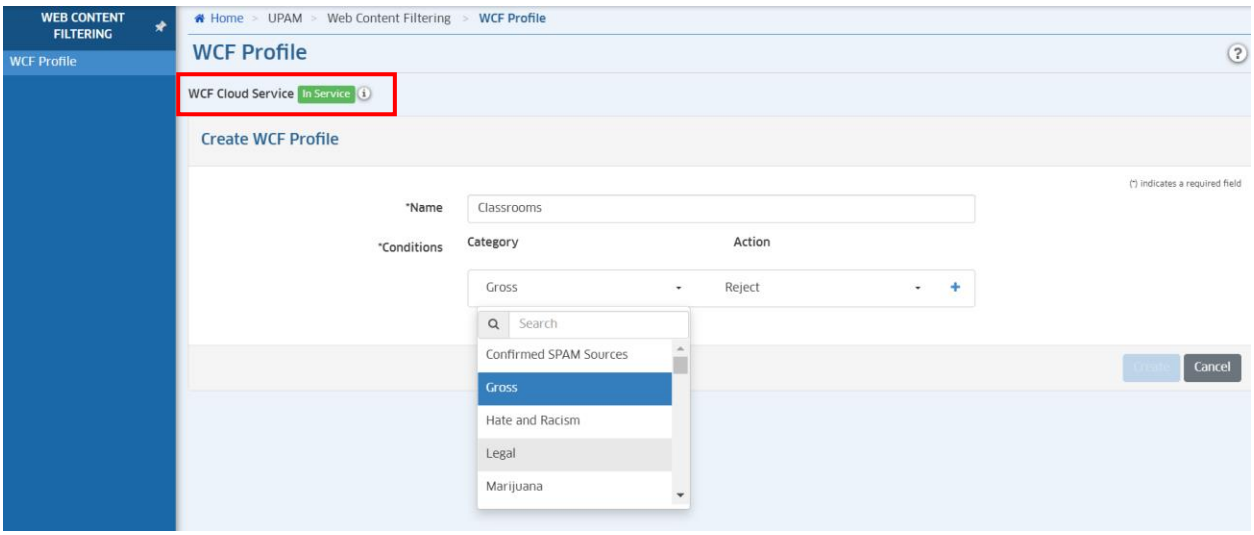


Figure 53: Web content filtering configuration – Omnivista 2500 (WCF Profile)

3.2. RF Management

64.	In the framework of a "Large deployment" scenario as described previously [4], the WLAN solution shall allow automatic and/or manual RF management (channel and power).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. The OmniAccess Stellar APs implement the *Radio Dynamic Adjustment™* (RDA) technology that automatically assigns channels and power settings, provides *Dynamic Frequency Selection /Transmit Power Control* (DFS/TPC), and ensures that Access Points stay clear of all radio frequency interference (RFI) sources to deliver reliable, high-performance wireless LANs.

The control plane of the OmniAccess Stellar WLAN solution is fully distributed. The automation (when activated) of the RF parameters settings of the OmniAccess Stellar APs occurs between adjacent/neighbor APs only (even if they belong to different AP-Groups and even if they are located within different management VLANs), in a fully distributed manner. Each AP communicates with its neighbor APs with "over the air" exchanges through the *Neighbor Management Protocol* in order to discover each other and, then, with "over the LAN" exchanges for RF management. This allows RF context sharing (Channel utilization & interference, number or clients per band, radio & AP, power…) and each AP can take RF actions:

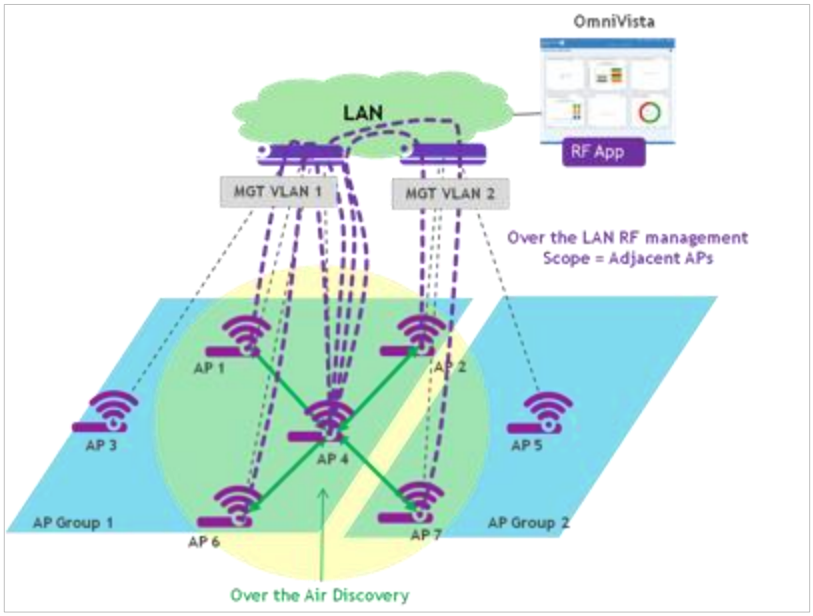


Figure 54: Automated RF management between adjacent APs

After the APs have discovered each other, each AP will declare starting auto-channel & auto-power process and, in case of collision, will wait for a while and retry. The AP that can proceed will listen to the RF environment for a while, then choose the best channel based on certain algorithm. After a while, each AP in the neighborhood should have tried once at least, and all APs will be in a channel distribution with as less interference as possible. The auto-channel process will work only when there is no client attached to the radio.

Regarding the auto-power process, each AP will send transmit power setting to its neighbor APs that will compare the RSSI and transmit power in order to adjust their own transmit power based on certain algorithm. After several rounds of this process, the power of all APs will be adjusted to the most appropriate setting.
The channel width cannot be set automatically and must be set manually for each band. The Channel width is used to control how broad the signal is for transferring data. By increasing the channel width, the speed and throughput can be increased. However, larger channel width brings more unstable transmission in crowded areas with a lot of frequency noise and interference.

OmniAccess Stellar WLAN 802.11ax access points (e.g AP13xx series and AP14xx series) and 802.11be access points (e.g AP15xx) make the use of available frequency space efficiently with OFDMA-based communications, then 20MHz channel width consisting of 256 subcarriers are grouped into smaller subchannels (known as Resource Units). Stellar WLAN 802.11ax/be access points dictates use of RUs and their combination within 20HMz channel. 802.11ax/be APs can communicate with one client using entire 20MHz bandwidth or can communicate with several clients using different sets of subchannels.

OmniAccess Stellar WLAN 802.11ax/be access points operating in the 6GHz band, or Wi-Fi 6E access points (e.g. AP1451/AP1411/AP1431 supported from AWOS release 4.0.7) or Wi-Fi 7 access points (e.g. AP1511/AP1521 supported from AWOS release 5.0.1), now use the 6GHz-7GHz frequency band available for Wi-Fi for OFDMA-based communications. 500MHz or 1200MHz bandwidth is added depending on regions worldwide.

- The UNII-5 band available for Wi-Fi (Wi-Fi 20MHz channels numbered from 1 to 93; see tables on Internet for the detailed list) is adopted by EU, UK, Australia, UAE and Malaysia.
- The UNII-6 to 8 bands available for Wi-Fi (Wi-Fi 20MHz channels numbered from 97 to 233 (see tables on Internet for the detailed list) are also adopted by US, Canada, Brazil, Chile, South Korea, UAE.

Channel & Power	▪ Auto-mode enabled by default ▪ It is recommended to use auto channel & power instead of static setting ▪ Channel sets by region/local regulation ▪ Lower power in case of dense AP deployment *Guidelines for statically setting channels*: **WLAN 802.11 channels-2.4GHz,3.6GHz,5GHz channel to frequency converter (rfwireless-world.com)** **WLAN 802.11ax RU | RU-26,RU-52,RU-106,RU-242,RU-484,RU-996 (rfwireless-world.com)** **WLAN 802.11 channels-6GHz channel to frequency converter (wikipedia.org/wiki/List_of_WLAN_channels#6_GHz)**
Channel Width	▪ Keep Default settings ▪ Narrow width for dense AP deployment ▪ Smaller subchannels for efficient AP deployment with 802.11ax ▪ Large width for sparse AP deployment
Short Guard Interval	▪ Enabled by default ▪ If RF environment requires it or clients not crowded, then Long Guard Interval can be enabled

Table 4: OmniAccess Stellar WLAN per-band wireless information

A time window can be defined for RDA operation (from Omnivista release 4.8) outside which the automatic power and channel assignment is stopped, thus avoiding any disruption of high client traffic during the day - typically suitable for high-density installations.

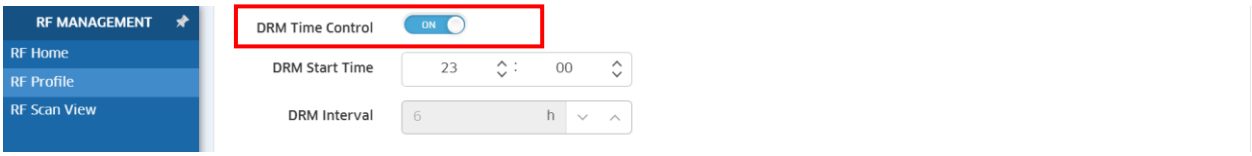


Figure 55: DRM Time Control – Omnivista 2500 (RF Profile)

65.	The WLAN solution shall support IEEE 802.11d standard in order to adapt channel and power levels to specific regulations of the geographical regions and countries to cover	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Stellar Access Points support country information, to identify the regulatory domain where the access point is installed, along with other radio parameters such Frequency Hopping (FH). Stellar HW models exist to specifically support regulations for regions such as US HW model (US, Japan), ME HW model (Egypt, Israel) or RW HW model for any other country worldwide.

66.	The WLAN solution shall support IEEE 802.11h standard in order to adapt to regulatory constraints related to the use of the 5GHz frequency band	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Stellar Access Points implement *Channel Switch Announcement* (CSA) in beacons to announce to the connected clients the channel switch to be performed when a radar equipment is detected in *Dynamic Frequency Selection* 5GHz sub-bands (DFS). The CSA operates on channels 52 to 140 of the UNII-II and UNII-II extended bands, which are usually shared with radar equipment. CSA announcements allows not to interfere with such equipment that have priority in this frequency band.

OmniAccess Stellar WLAN solution allows the management of the transmitted power and the configuration of a power range per band (min & max) including the DFS band. Stellar *Dynamic Frequency Selection/Transmit Power Control* (DFS/TPC) feature allows to stay in compliance with local regulations regarding the transmitted power and allows to control the consumption of access points in the 5GHz band.

67.	The WLAN solution shall comply with different WLAN coverage classes defined for next-generation services deployed in the 6GHz frequency band	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully meets this requirement when managed by OmniVista 2500. The Stellar Wi-Fi 7 AP1511 and AP1521 access points manage transmit power and a power range per band (min & max) in the 6GHz band using the Transmit Power Control (TPC) feature, ensuring compliance with regulations regarding the emitted power in the 6GHz band.

- WLAN Class compliant with Low Power Indoor (LPI Class) in the UNII-5 band for fixed services with a maximum of 1 watt per AP (Standard Power AP)
- WLAN Class Low Power Indoor only (LPI) in the UNII-6 band for mobile services with a maximum of 250 mWatt per AP (Low Power AP)
- WLAN Class Standard Power (SP) in the UNII-7 band for fixed services with a maximum of 1 Watt per AP (Standard Power AP). Automated Frequency Coordination equipment is required for this band shared with other wireless equipment (e.g., satellite services)
- WLAN Class Low Power (SP) in the UNII-8 band for fixed and mobile services with a maximum of 250 mWatt per AP (Low Power AP). No SP APs in this band.

68.	The WLAN solution shall support large width for sparse AP deployment	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

With IEEE 802.11ax OFDMA-based communications starting from Stellar AP13xx series, the possibility of having up to 160MHz of channel width in the 5GHz band and up to 320MHz channel width in the 6GHz band with 802.11be standard is introduced, instead of the typical 80MHz of channel width in 802.11ac. Having a larger channel width means greater actual speed, especially for locations where Wi-Fi clients compatible with the 5 GHz and/or 6 GHz bands require such speeds.

The High-Efficient AP1320 and AP1360 series support and can adjust this larger channel width in RF, for areas with a well-known context in term of interference and frequency noise. 160MHz channel width is supported in a 80MHz + 80MHz mode on both APs while the full 160MHz mode is supported on high-end WiFi 6 AP1331 and AP1351 offering 160MHz bandwidth on channels 50 and 114 in the 5GHz band.

Wi-Fi 6E and high-end AP1451 (AWOS 4.0.5), AP1411, AP1431 (AWOS 4.0.7), seven new 160MHz channels are supported in full 160MHz mode and make AP14xx perfect for such deployments. They operate on UNII-5, 6, 7 and 8 bands and are assigned according to regions worldwide. The 160MHz channels 15, 47 and 79 (UNII-5 band), channel 111 (UNII-6 band), channels 143, 175 (UNII-7) and channel 207 (UNII-8) can be used for sparse AP deployment in a very precise RF context where interferences and radio spectrum use are perfectly known for these channels. For example, channels 15, 47, 79 and 111 can be used to deploy a Low Power Indoor (LPI) class WLAN.

With the introduction of Wi-Fi 7 and the tri-radio AP1511 and AP1521 access points (AWOS 5.0.1), OmniAccess Stellar supports three new 320 MHz channels in full 320 MHz mode, making the AP15xx series perfectly suited for Extremely High Throughput (EHT) deployments. They operate on the UNII-5, 6, 7, and 8 bands, which are allocated based on global regions. For example, 320 MHz channels 31 and 63 (UNII-5 band) can be used for sparse access point deployment in next-generation, speed-demanding applications, in a highly specific RF context where interference and radio spectrum usage are well understood, for the deployment of a Low Power Indoor (LPI) Class WLAN.

The 2.4GHz, 5GHz or 6GHz bands to be used for these deployments can be directly specified on dual radio access points (ie. Wi-Fi 6E AP1411 model).

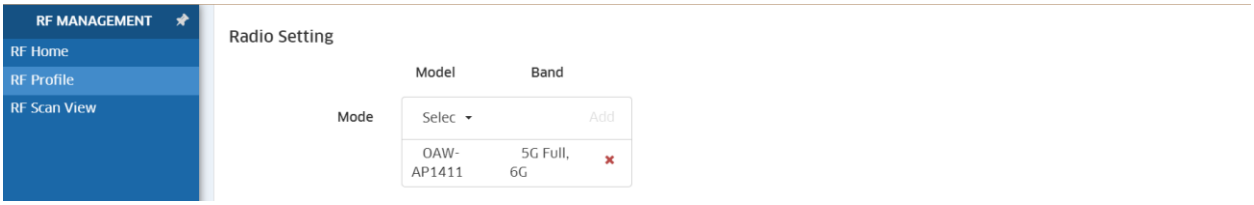


Figure 56: Sparse AP deployment on dual radio – Omnivista 2500 (RF Profile)

69.	The WLAN solution shall support preamble puncturing for better use of wideband channels in the presence of interference within the band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by OmniVista 2500 for Stellar Wi-Fi 7 AP15xx access points (AWOS 5.0.1). The Preamble Puncturing feature optimizes the use of wideband channels, even in the presence of in-band interference (e.g. in the presence of 20/40 MHz access points). Combined with multi-Rus feature, which offer flexible resource allocation across the channel, Preamble Puncturing skips subcarriers affected by interference, ensuring efficient use of the unaffected portions of the band and thereby improving the network spectral efficiency.

70.	The WLAN solution shall support most recent modulations for latest dual-band and tri-band clients	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. With IEEE 802.11ax OFDMA-based communications starting from Stellar AP13xx/AP14xx series, the possibility of using 1024-QAM modulation to bring more throughput for dual-band clients supporting this modulation is introduced. A new 10 bits per data symbol scheme enables a raw speed increase of 39% for the client with IEEE 802.11ax.

The OmniAccess Stellar WLAN AP1511 and AP1521 access points introduce 4096-QAM modulation with IEEE 802.11be for increased throughput with tri-band clients supporting this modulation. A new 12 bits per data symbol scheme enables a gross speed increase of 20% for clients supporting IEEE 802.11be.

71.	The WLAN solution shall support power saving functions for battery consuming clients or for clients with specific data transmission	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. With Unscheduled Automatic Power Save Delivery (U-APSD) of WMM 802.11e and Target Wake Time (TWT) for 802.11ax OFDMA-based communications, the possibility for clients to wake up at a time and save more battery while connected to the WLAN by entering in standby or sleep mode is introduced.

Stellar WLAN solution is able to buffer data and hold it for clients running real-time applications (like phones), WMM U-APSD feature allows smooth transition in and out of sleep mode and is implemented per SSID on Stellar WLAN solution.
Stellar WLAN solution is able to negotiate a waking schedule with IoT clients running data transmission “on demand” and is implemented using TWT setup frames of 802.11ax.

802.11be introduces support for dynamic Power Save MU SMPS (Spatial Multiplexing Power Save) for MIMO clients, allowing the client to save energy by disabling some MIMO antennas when maximum performance is not needed, while automatically reactivating them when performance demand performance increases.

72.	The WLAN solution shall minimize the airtime consumption in extremely dense environments where cell overlap is significant	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.
With Basic Service Set coloring (BSS coloring) for 802.11ax and 802.11be OFDMA-based communications, Stellar WLAN 802.11ax/be radios differentiate between BSSs using a BSS color identifier when radios are transmitting on a same channel. 802.11ax/be Clear Channel Assessment (CCA) is re-adjusted based on BSS color code and provides spatial reuse operation to decrease co-channeling contentions issue in high dense environments where cell overlap is significant.

73.	The WLAN solution must be compatible with previous 802.11ax (Wi-Fi 6/6E), 802.11ac (Wi-Fi 5) and 802.11b/g/n (Wi-Fi 4) standards and remains compatible in case of clients do not support fully the latest standards.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. When Stellar WLAN 802.11ac access points (e.g AP1101 or AP12xx serie), Stellar 802.11ax (AP13xx/AP14xx) or Stellar 802.11be (AP15xx) are mixed, there is backward compatibility with 802.11ax (Wi-Fi 6/6E), 802.11ac (Wi-Fi 5) and 802.11b/g/n (Wi-Fi 4).

There is the possibility to disable the extremely high throughput (EHT) 802.11be, the efficient 802.11ax OFDMA-based network or even the Multi-User MIMO in case of clients cannot fully operate with 802.11be, 802.11ax or even MU-MIMO functions on sustained 2.4G/5GHz frequency bands.

Figure 57: 802.11be, 802.11ax and MU-MIMO operation – Omnivista 2500 (RF Profile)

Thus, the AP12xx, AP13xx, AP14xx, and AP15xx series are backward compatible with a WLAN 802.11ac wave 1, while offering, for each series, the new features specific to 802.11be, 802.11ax, or even 802.11ac wave 2.

74.	The WLAN solution shall support Short Guard Interval.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In IEEE 802.11 OFDM-based communications, the guard interval is at a very basic level, time spacing between data symbols to prevent inter-symbol interference. The *Short Guard Interval* allows to reduce the transmit interval in order to increase overall throughput but may also

increase packet error rate. The standard guard interval per the 802.11n standard is 800 nanoseconds and has been carried over to 802.11ac/ax/be. To increase data rate, the optional support for a 400 nanoseconds guard interval has been added providing approximately an 11% increase in data rates, but it results in a higher packet error rate when the delay spread of the channel exceeds the guard interval and/or if timing synchronization between the transmitter and receiver is not precise.

In the framework of the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution, the *Short Guard Interval* is enabled by default and should be disabled if the RF environment is not good or in clients crowded environments.

75.	The WLAN solution shall support Long Guard Interval and Long symbol duration	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In IEEE 802.11ax OFDMA-based communications, the guard interval time spacing between data symbols can be increased to provide an answer for topologies where propagation delays, echoes and reflections are significant. *Long Guard Interval* in 802.11ax/be allows to improve certain radio links jointly with *longer symbol duration* and new preambles. 1.6 microseconds and 3.2 microseconds Guard Interval values have been added to standard 400/800 nanoseconds in the framework of the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN 802.11ax and 802.11be solution, providing better robustness of radio links without increasing the packet error rate.

Long Guard Interval can be enabled for Stellar 802.11ax/be outdoor configurations such as Bridging and Meshing, within not clients crowded environments.

76.	The WLAN solution shall be smart enough to guide a new client to the optimal band/channel (2.4GHz/5GHz and 6GHz) considering, at a given time, both the number of associated clients on each band, and the medium utilization.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, the OmniAccess Stellar WLAN solution can do smart clients load balancing, including Band Steering. *Load balancing including band guidance* controls the behavior of multi band clients according to the utilization of a wireless channel and users connected to the AP and can guide a client accessing the network to the optimal band/channel. Band guidance considers, at a given time, two parameters:

- the client count per radio (the difference between the number of associated clients on each radio/channel)
- the channel/band load, considering that any channel/band is overloaded when its average medium utilization over the span of a minute exceeds 70%

Band guidance rules apply to the entire Alcatel-Lucent Enterprise OmniAccess Stellar dual-band access points series, as well as to the tri-radio Access Points AP123X, AP1351, AP1431, AP1451, AP1511 and AP1521. The band guidance feature shall consider three bands/channels in the case of tri-radio APs (2.4G, 5G-Low and 5G-High, or 2.4G, 5G and 6G, either separated or aggregated) instead of two in the case of dual-band APs.

77.	If no channel (2.4GHz/5GHz/6GHz) is overloaded (high medium utilization) or crowded (high client count), an AP shall by default guide a new client to the 5GHz/6GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

78.	Even if the 5GHz/6GHz band is not overloaded but is crowded (high client count), an AP shall guide a new client to the 2.4GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

79.	If a channel (2.4GHz/5GHz/6GHz) is overloaded (high medium utilization) and even if it is not crowded, an AP shall guide a new client to the less loaded band/channel.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

80.	If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilization) and no band/channel is crowded, an AP shall guide a new client to the 5GHz/6GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

81.	If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilization) and the 5GHz is crowded, an AP shall guide a new client to the 2.4GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

82.	The WLAN solution must be able to guide a new client to the appropriate channel (5GHz/6GHz) when connecting to access points supporting the 6GHz band separately (Wi-Fi 6E), considering the capability of client to connect to this frequency band separately.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In case of connection on 5GHz/6GHz bands with Wi-Fi 6E Stellar AP14xx series (from AWOS release 4.0.5) the priority is given to the connection on 6GHz band channels for clients which have the capability to use Wi-Fi 6E channels.

- AP1451 is a tri-radio access point with two separate 5GHz and 6GHz radios.

- AP1411 is a dual radio access point operating in different modes on the 3 bands: modes 2.4GHz + 5GHz; 2.4GHz + 6GHz and 5GHz + 6GHz can be selected
- AP1431 is a tri-radio access point operating in the 2.4GHz, 5GHz and 6GHz bands separately.

Band steering on AP14xx series prioritizes the 6GHz band, followed by the 5GHz, depending on the management done at SSID level and depending on the capability of the client to connect to Wi-Fi 6E channels. When 6GHz is enabled, AP14xx access points broadcast 6GHz channels it operates on by transmitting a *802.11k Reduced Neighbor Report* tag (802.11k RNR) and channel in beacons. Thus the client wishing to fully exploit 6GHz channels can associate to the AP.

Subsequently 2.4GHz/5GHz load balancing on AP14xx operates accordingly to the same rules as for the 2.4GHz/5GHz/6GHz load balancing rules described before.

83.	The WLAN solution must be able to guide a new tri-band client to the appropriate resources and channels (2.4GHz/5GHz/6GHz) when connecting to access points that support aggregation of these bands (Wi-Fi 7 access points), considering the capability of client to connect to these aggregated resources.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully meets this requirement when managed by OmniVista 2500. For the Wi-Fi 7 tri-radio Stellar access points (AP1511 and AP1521 with AWOS 5.0.1), it supports Multi-Link Operation (MLO), allowing clients to simultaneously use the 2.4GHz, 5GHz, and/or 6GHz bands based on SSID-level management in OmniVista 2500. This is achieved through the management of data links at Layer 2 of Wi-Fi; the aggregation of MPDUs at the physical layer allows clients to choose between two link aggregation modes supported by OmniAccess Stellar to optimize latency and bandwidth:

- EMLSR Mode (Enhanced Multi-Link Single Radio) supported by the AP15xx series utilizes a single link at a time for transmission and reception. It promotes reliability and simplifies data management, making it useful for environments where network conditions change and where a single stable link is preferred.

- STR Mode (Simultaneous Transmission and Reception) supported by the AP15xx series allows for the simultaneous use of multiple links for both transmission and reception, maximizing bandwidth and improving latency for faster and more responsive connections. This mode is particularly suited for next-generation equipment such as Virtual Reality (VR) devices that transmit and receive on different bands.

Figure 58: MLO operation on Wi-fi 7 tri-band radio Access Points – Omnivista 2500 (SSID)

84.	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Clients are typically in control of connectivity decisions such as which AP to associate with. Unfortunately, clients do not have a system view of the network and often make poor decisions such as connecting to the first AP they hear, regardless of whether it matches their needs. The OmniAccess Stellar WLAN solution allows smart load balancing of clients between APs. The client information like the client count per AP is shared between APs so that an AP can know the load of its neighbor AP and decide whether or not to permit client access based on a timer set up according to its current associated client count:

Figure 59: WLAN clients load-balancing

85.	The WLAN solution shall force clients to the 5GHz (or 6GHz) only when they are dual band capable. The WLAN solution shall force clients to the 5GHz only or shall force clients to the 6GHz only (Wi-Fi 6E capable) when they are dual band capable.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500, in *Wi-Fi Enterprise mode* as depicted in following figures:

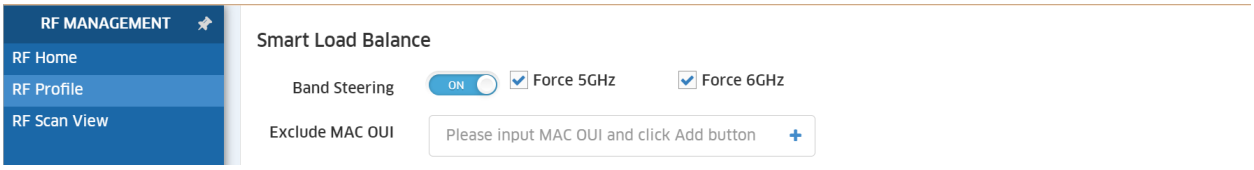


Figure 60: 5GHz and 6GHz forcing for dual band clients – Omnivista 2500 (RF Profile)

This band selection remains compatible with Stellar tri-radio AP1511 and AP1521 access points that support Multi-Link Operation, regardless of MLO configuration across the 2.4GHz, 5GHz and 6GHz bands.

86.	The WLAN solution shall deny connection to an AP when the signal of the client becomes too weak and disconnect a client to force it to roam when the signal becomes too weak.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, the OmniAccess Stellar WLAN solution allows to set RSSI (*Received Signal Strength Indication*) thresholds in decibels in order to optimize connectivity by forbidding client access to the network when the signal is too weak or by disconnecting a client (forcing it to roam) when the signal becomes too weak.

The thresholds are set for each radio band, considering also dual 5GHz-low and 5GHz-high bands supported by the OmniAccess Stellar 123X series, AP1351 tri-radio and 6GHz band supported by Stellar AP14xx access points and by Stellar tri-radio AP15xx access points:

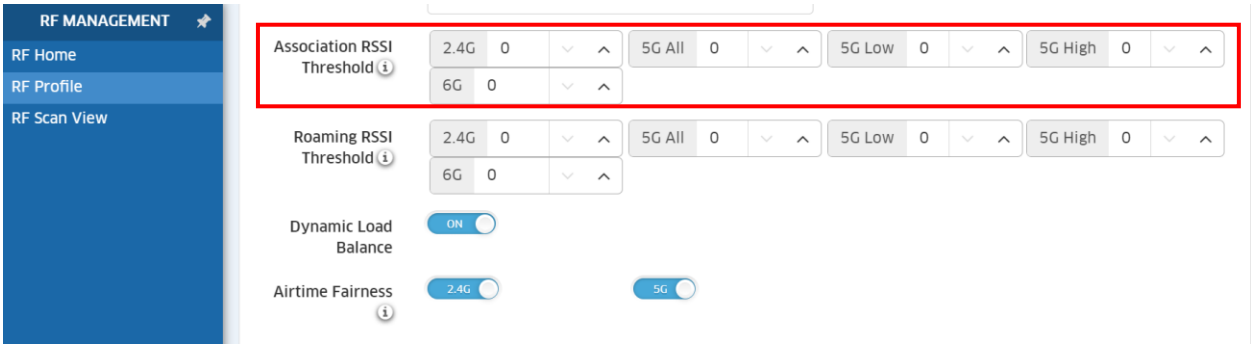


Figure 61: Per-band Association and Roaming RSSI Thresholds – Omnivista 2500 (RF Profile)

87.	The WLAN solution shall support the IEEE 802.11v and 802.11k standards to facilitate network guided roaming.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, as Wi-Fi clients roam, they tend to hang on to the original access point they associated with rather than move to a nearby AP that would generally be a better choice. Clients generally MUST monitor indicators of the health of their wireless connection, such as the signal strength (RSSI) of their connection, their signal to noise ratio, and the number of errors/retries they are experiencing on that connection. Once these indicators start to degrade, they MUST ideally begin to probe for alternative access points, ready to make the jump to a new access point that will provide a better-quality connection.

IEEE 802.11k standard includes a range of mechanisms for performing various measurements of the WLAN station's environment and allows a client to request information about that environment. One of the most useful tools from a client roaming perspective is the *Neighbor Report*. A client requests a *Neighbor Repor*t to obtain the list of the known or neighboring APs of its current AP. Having this information significantly improves a client's ability to make a roaming decision. The use of 802.11k is dependent on client support for this feature, but it is becoming well supported amongst newer mobile devices.

IEEE 802.11v standard defines a service that allows stations on a WLAN (APs and clients) to exchange data that provides them with awareness of network conditions. One of the mechanisms provided in 802.11v is "BSS Transition Management". 802.11v mechanism allows for example a client to request a set of preferred APs, at any time, according to its own operating criteria. This without waiting for a new association to further AP to know the radio context and neighboring APs.

Both standards are supported in *Wi-Fi Enterprise mode* as depicted in the following figure:

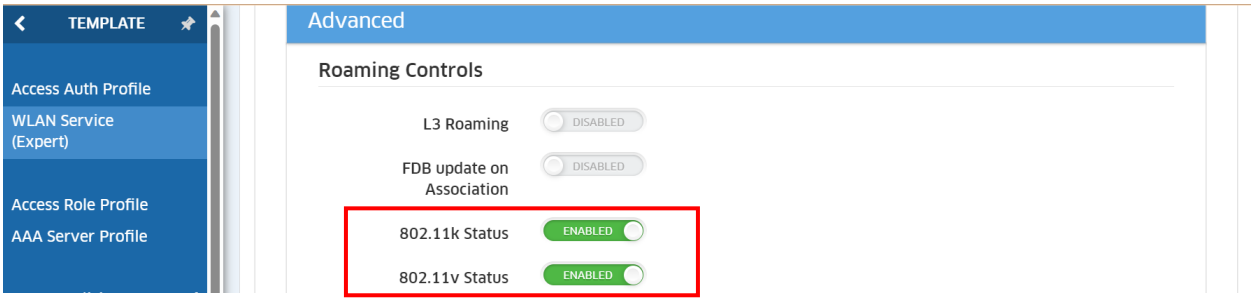


Figure 62: IEEE 801.11k & 802.11v support – Omnivista 2500 (WLAN Service Expert)

IEEE 802.11k and 802.11v are supported in 2 modes that are directly managed in RF profile that applies to any AP model in an AP group:

- Background scan mode for AP12xx series (Wi-Fi 5)
- Full scan mode for AP13xx/AP14xx series (Wi-Fi 6/6E)
- Full scan mode for AP15xx series (Wi-Fi 7)

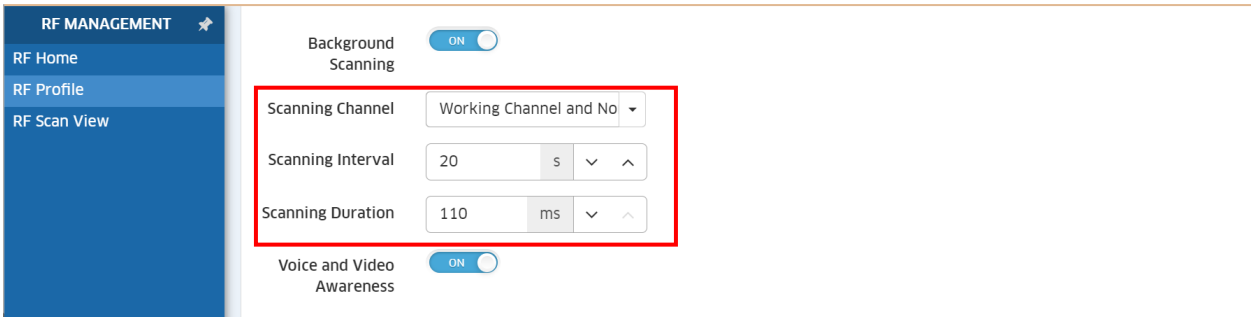


Figure 63: Background scanning for 802.11k/v support – Omnivista 2500 (RF Profiles)

88.	The WLAN solution shall support data rate control to encourage clients to roam at higher rates.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, clients can be forced to roam to a better AP by not allowing clients to connect at low speeds. This mechanism is used to encourage clients to roam at higher rates. By switching off support for lower connection rates that are generally available from an AP, a client simply does not have the option to use lower rates and is forced to roam to another AP much sooner.

The Stellar APs by default, support connection rates all the way from very high-end speeds (e.g perhaps 12.2Gbps for 802.11be Wi-Fi 7, perhaps 9.6Gbps for 802.11ax Wi-Fi 6E, perhaps 4.8Gbps for an 802.11ax AP and perhaps 1.7Gbps for an 802.11ac AP) down to very low legacy speeds (e.g 6Mbps on 5GHz, or 1Mbps on 2.4GHz). By limiting support for the lower rates through, a client simply cannot "hang on" to an AP over such a large area.

A common approach is to keep lowest support speed on 2.4GHz to perhaps 12Mbps or 24Mbps. For 5GHz or 6GHz, to perhaps 27Mbps or 54Mbps are often selected. A client will be aware from AP beacon information which rates an AP supports, so will know that it must find a new AP once it reaches the minimum supported rates (e.g. 12Mbps) – it will have to roam much sooner than if it had the option to drop to 1Mbps.

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution complies with this requirement in *Wi-Fi Enterprise mode* as depicted in following figure:

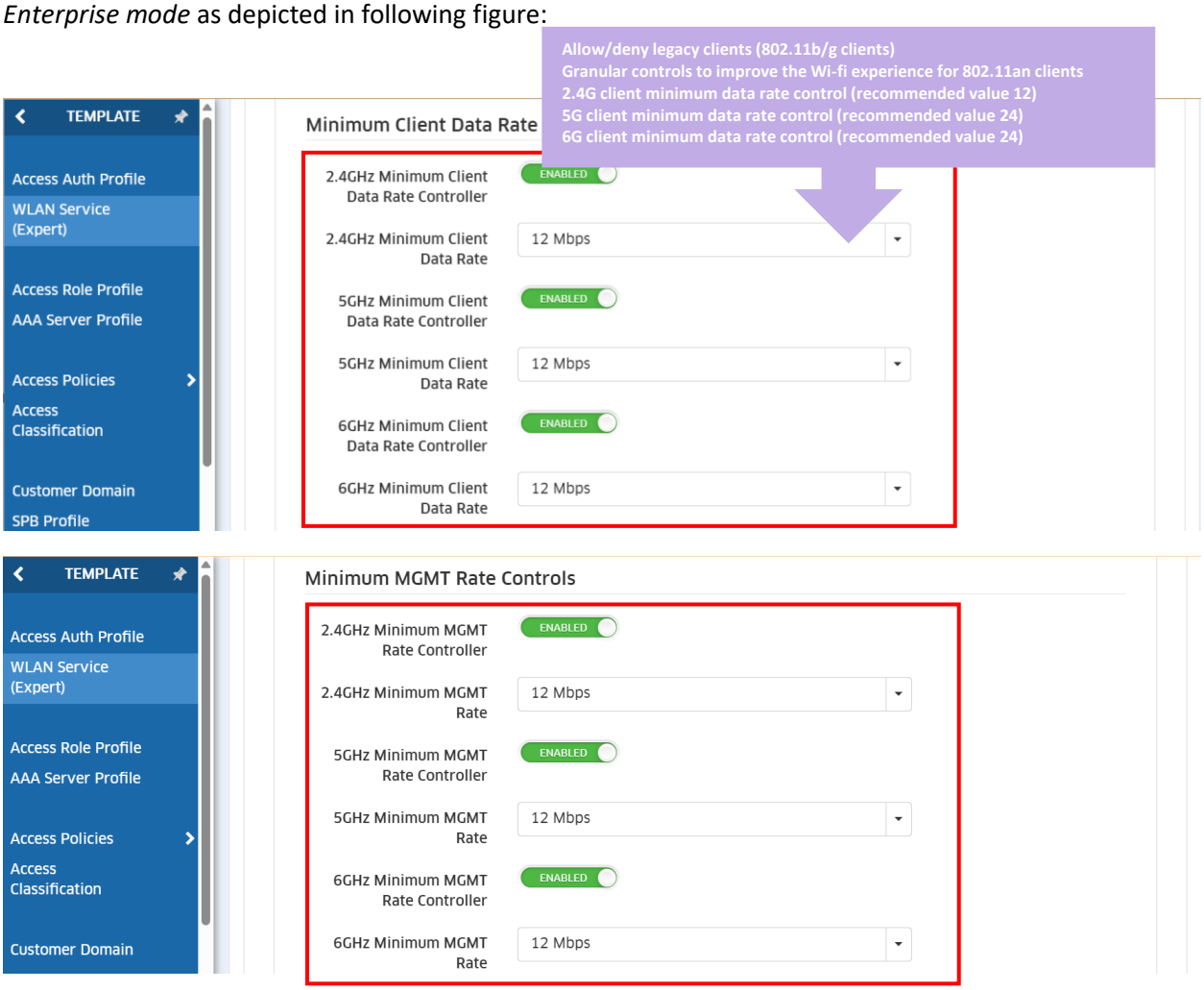


Figure 64: Minimum Data Rates Control - Omnivista 2500 (WLAN Service Expert)

89.	The WLAN solution shall propose APs that have the ability to scan the air in order to provide interfering/rogue APs and wireless attacks detection and shall not rely on external scanning equipment.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, all OmniAccess Stellar Access Points have background scanning capabilities, and the OmniAccess Stellar WLAN solution does not require any specific and external scanning equipment.
Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference or even attacks.

Background Scanning is used to examine the *Radio Frequency* (RF) environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks. Background scanning is the basis of some advanced features such as wIDS/wIPS (*Wireless Intrusion Detection/Protection System*) or RDA (*Radio Dynamic Adjustment*). When background scanning is turned off, the foreign AP detection and rogue containment will stop, and the precision of the RDA feature may be affected.

Background Scanning operates only on working channels of OmniAccess Stellar Wi-Fi 5 (e.g AP12xx access points) and can be done through dedicated 1x1 full band radio (non-working channels) on OmniAccess Stellar Wi-Fi 6, Wi-Fi 6E or Wi-Fi 7 (eg. AP13xx, AP14xx and AP15xx acces Points), both modes are supported by OmniAccess Stellar solution.

Background scanning settings on Wi-Fi 5 working channels have an impact on real-time clients, by default background scanning is enabled with default scanning interval (20 seconds, with a 5 to 10799 second range) and a default scanning duration (50 ms, with a 50 to 110 ms range).

Background Scanning	▪ Enabled by default
Scanning Interval	▪ Keep Default settings
Scanning Duration	▪ Keep Default settings ▪ Higher scanning interval or lower scanning duration means intrusions are less likely being detected but client performance will be better with AP12xx access points ▪ Lower scanning interval or higher scanning duration means intrusions are more likely being detected but client performance will be lower with AP12xx access points
Voice and Video Awareness	▪ Enabled by default

Table 5: Background scanning information for Wi-Fi 5 access points

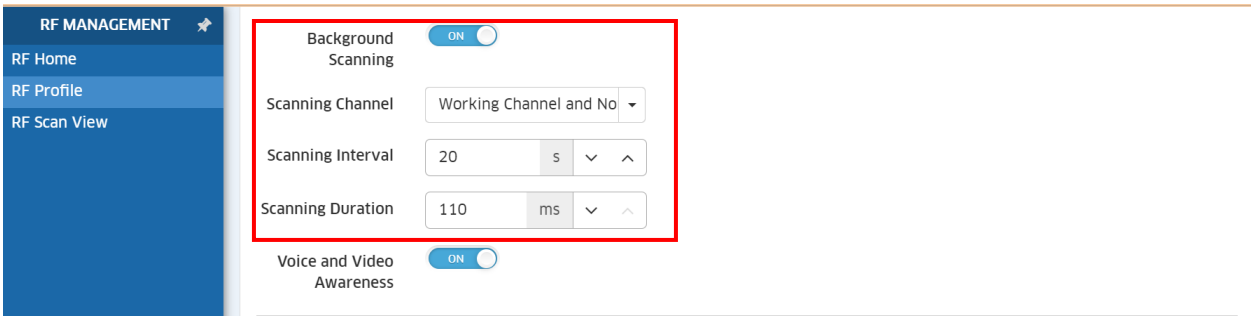


Figure 65: Background Scanning support – Omnivista 2500 (RF Profile)

90.	The scanning function of the APs shall not impact active voice or video calls (SIP and H.323). The scanning function of the APs shall not impact active voice or audio/video calls (SIP, H.323 or proprietary)	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. During scanning on working channels (AP12xx access points) wireless clients are impacted and the Access Points cannot process 802.11 data. Background scanning needs to be aware of existing traffic on the AP. If there is an ongoing voice (SIP or proprietary like NOE) or audio/video (SIP or H.323) scanning must not be performed to ensure uninterrupted traffic; and scanning must resume when there is no active voice/audio/video session. As mentioned on *Table 5: Background scanning information*, the "Voice and Video Awareness" feature is enabled by default for AP12xx access points

There is no impact on active voice/audio/video calls (SIP, H.323 or NOE) with scanning function on non-working channels (AP13xx, AP14xx and AP15xx access points) and with specific settings for the Background scanning.

91.	At least for the 5GHz and 6GHz bands, the WLAN solution shall allow to define the list of channels which can participate in dynamic configuration.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

The list of authorized channels can be defined in *Wi-Fi Enterprise mode* through *RF profiles* which can then be applied to OmniAccess Stellar Access Points directly or via AP-Groups:

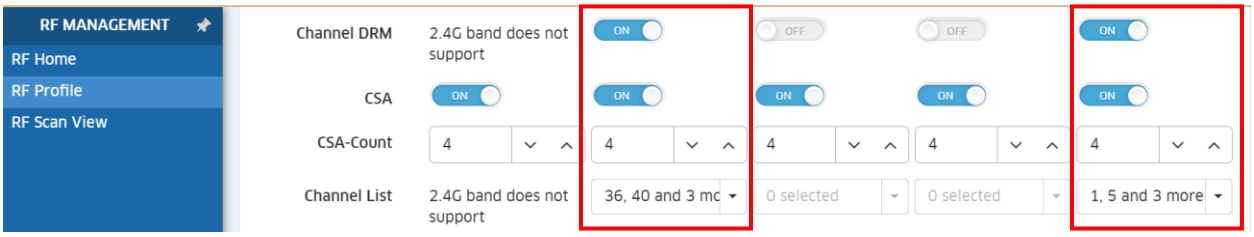


Figure 66: Authorized Channel List definition – Omnivista 2500 (RF Profile)

92.	The WLAN solution shall allow to define a range of transmit power per band (min & max) even if power settings are configured for automatic and dynamic assignments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Both *Enterprise* modes, with power settings set as "automatic", allow to configure a range of transmit power per band (min & max). The auto power selection algorithm then selects the transmit power of the AP within the minimum and maximum specified.

The range of transmit power per band can be defined in *Wi-Fi Enterprise mode* through *RF profiles* which can then be applied to OmniAccess Stellar Access Points directly or via AP-Groups:

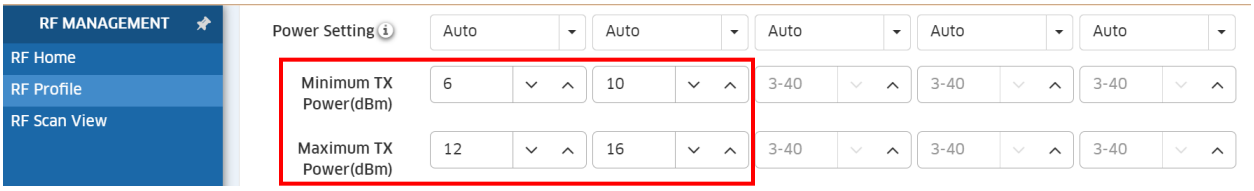


Figure 67: Min & max automatic transmit power – Omnivista 2500 (RF Profile)

OmniAccess Stellar transmit power management feature is also known as DFS/TPC feature for the control of transmitted power for outdoor using the UNII-2 5GHz DFS sub-band.

93.	The WLAN solution shall propose Access Points which can all be configured and deployed in a dedicated scanning mode.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In *Wi-Fi Enterprise mode*, OmniAccess Stellar AP15xxs, AP14xxs, AP13xxs and AP12xxs can be set to examine the radio frequency environment in which the Wi-Fi network is operating by analyzing all channels, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel. In *Wi-Fi Enterprise mode*, scanning mode can be enabled permanently or for a one-shot scan.

The two pictures below show an AP managed by Omnivista 2500 appliance, with dedicated scanning enabled

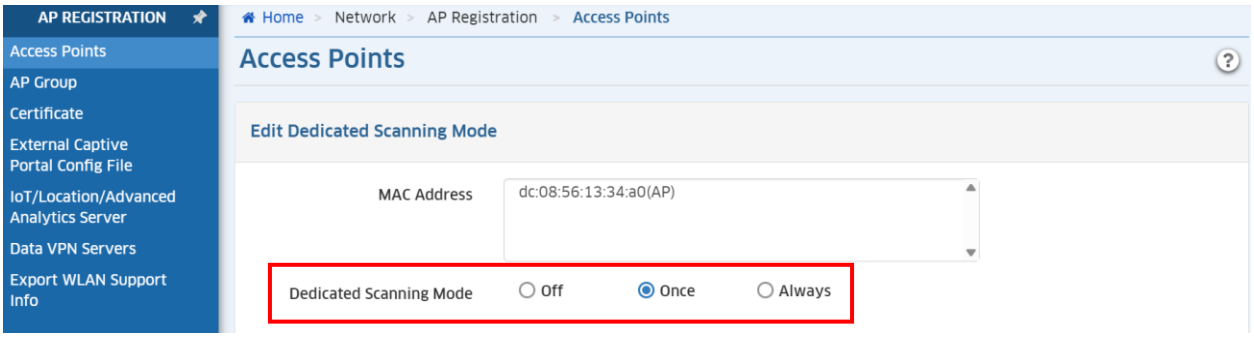


Figure 68: AP dedicated scanning mode activation – Omnivista 2500 (Access Points)

With more hardware resources the *Wi-Fi Enterprise mode* offers a "Real Time" and a "History" display mode:

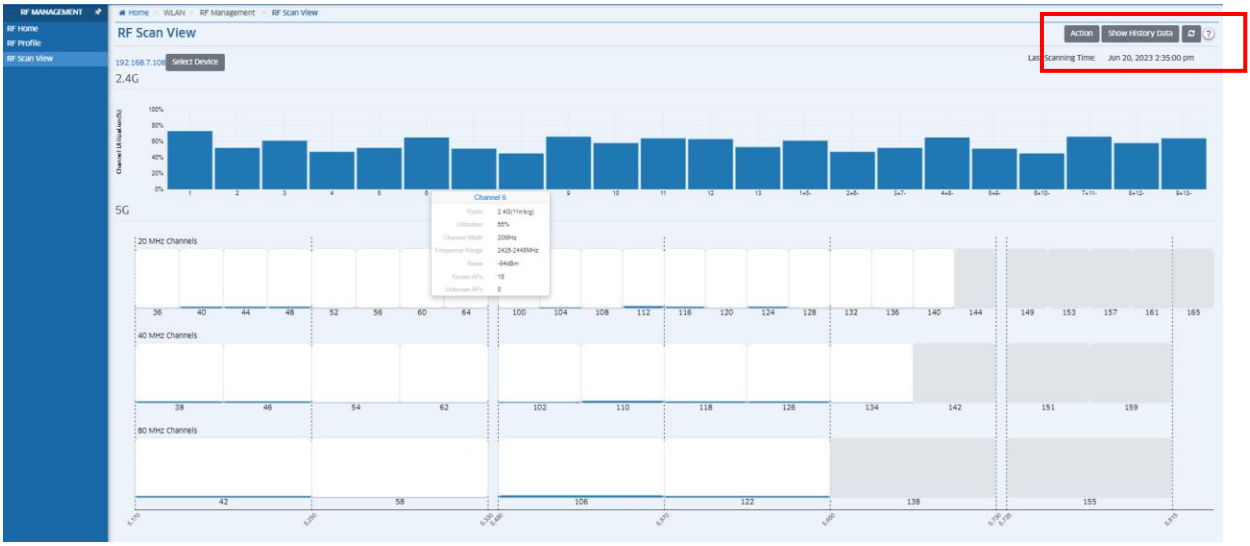


Figure 69: RF Scan display – Omnivista 2500 (RF Scan View)

94.	The WLAN solution shall propose Access Points with wireless packet capture capabilities.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In *Wi-Fi Enterprise mode*, OmniAccess Stellar AP15xxs, AP14xxs, AP13xxs and AP12xxs can perform wireless packet capture for further analysis. Access to the Wireless capture feature is via the *AP UI* (AP dedicated web interface, as described below [7]) as depicted in following figure:

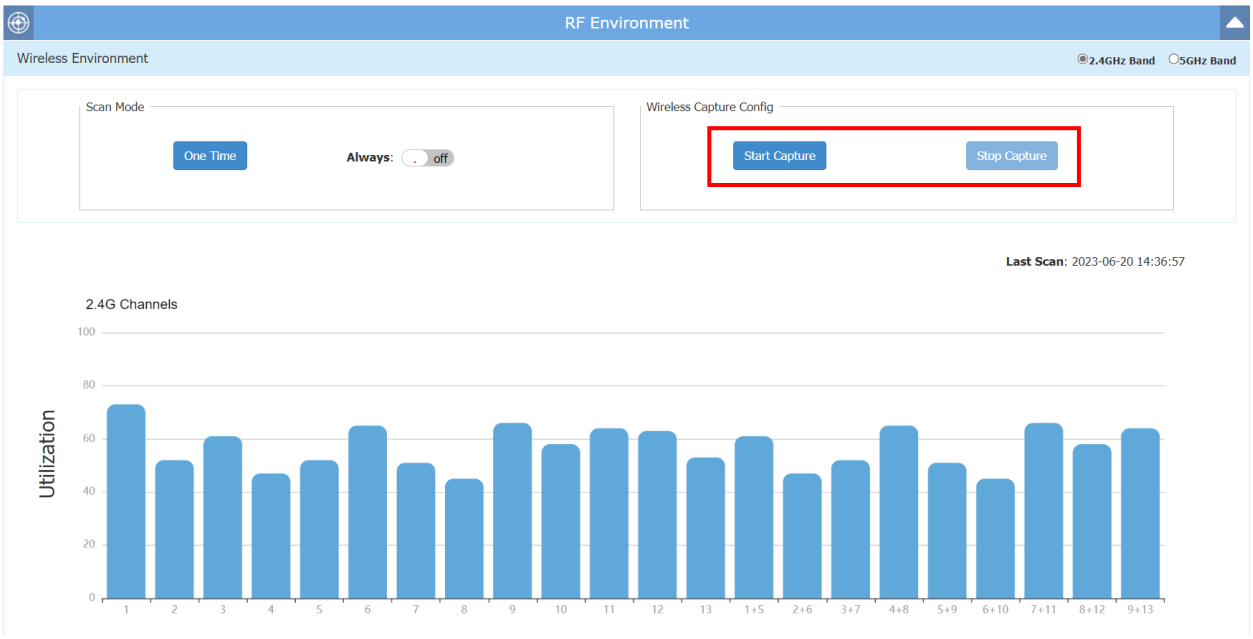


Figure 70: Wireless capture feature – Enterprise mode (AP UI)

In Large Wi-Fi Enterprise deployments, capturing wireless traffic requires specifying a local TFTP server to store the captured data as depicted in following figure:

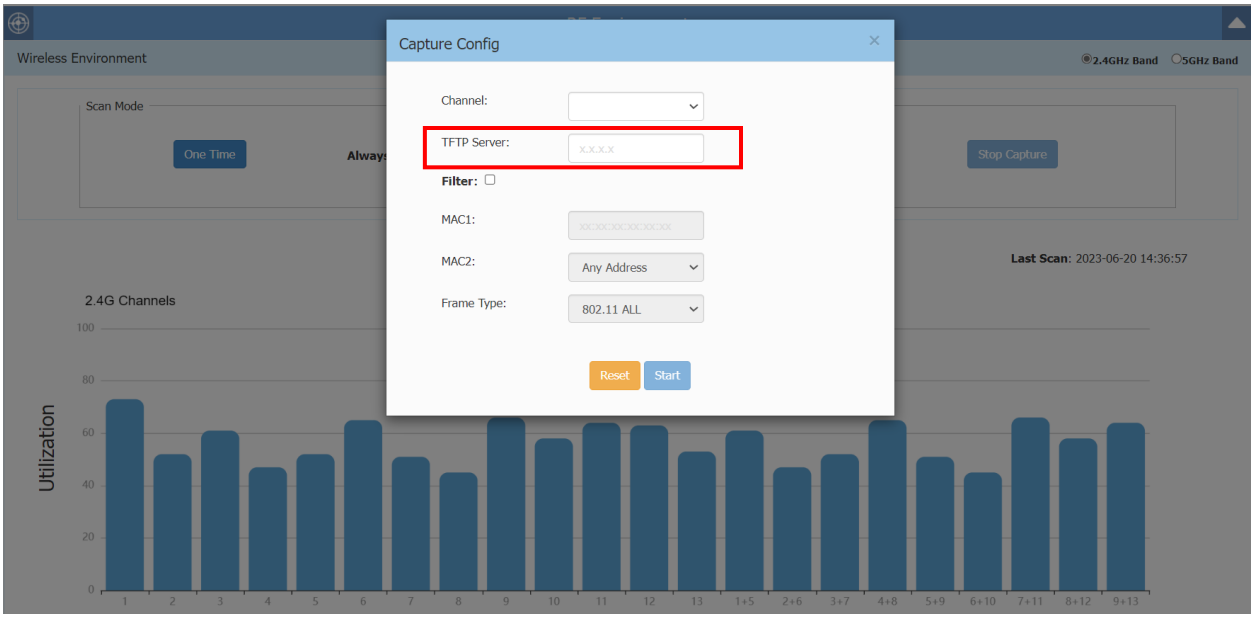


Figure 71: Wireless capture configuration – Enterprise mode (AP UI)

95.	The WLAN solution shall make it simple to review the roaming history for a given client device.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 by allowing to easily trace clients roaming behavior and Quality of

Experience (QoE) for devices connectivity. As shown in following figure with Omnivista 2500, the *Wi-Fi Enterprise mode* provides the time of roaming and RSSI historical information over a completely customized time range. For each roaming occurrence, Roaming AP, Association Time, Band and RSSI are recorded. With more resources in the Cloud *Wi-Fi Enterprise mode* offers Up to 30 days of roaming & RSSI history:

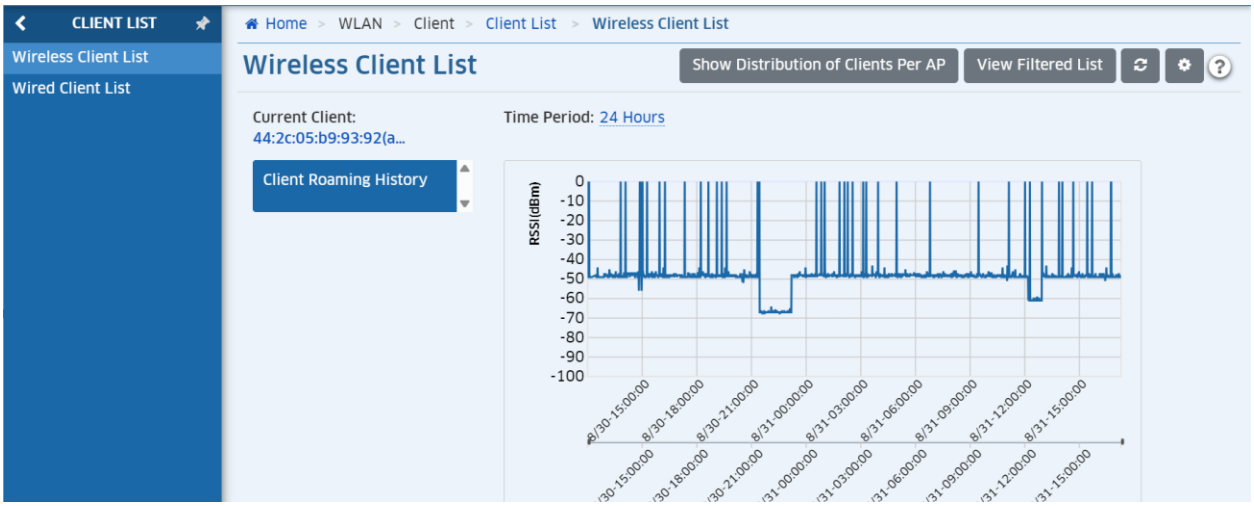


Figure 72: Roaming History – Omnivista 2500 (Wireless Client List)

96.	The WLAN solution shall allow long interval background scanning.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Some environments, such as healthcare, have indeed health monitoring equipment which have 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 on working channels (scanning mode of AP12xx access points) the client 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.

OmniAccess Stellar Access Points can be configured to analyze the environment every 3 hours at most, as shown by following figure in *Wi-Fi Enterprise mode*:

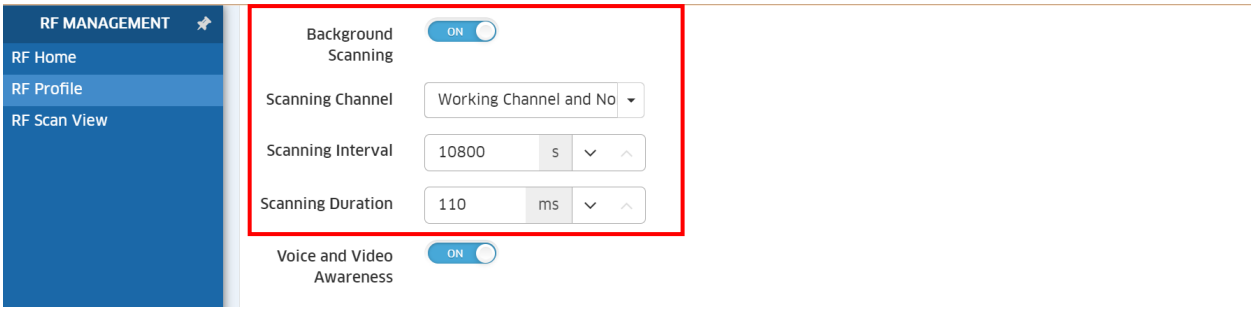


Figure 73: Long Interval Background Scanning – Omnivista 2500 (RF Profile)

3.3. Intrusion Detection and Prevention

97.	At least for a "Large scenario deployment" as described previously [4], the WLAN solution have wIDS/wIPS capabilities with no additional and dedicated equipment nor additional license.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, OmniAccess Stellar Access Points integrate *wireless Intrusion Detection and Prevention* (wIDS/wIPS) capabilities and reduce deployment and management costs by using Access Points to simultaneously serve clients and contain wireless threats.
With OmniAccess Stellar, there is no need for a costly overlay IDS with dedicated sensors. Automatic threat mitigation protects the network from unauthorized clients or APs and attacks. Integrated wIDS/wIPS capabilities allow to protect the WLAN better than an overlay deployment by virtue of being able to analyze and correlate 802.11 frames inline. It is possible to monitor the wireless radio spectrum for the presence of unsafe Access Points or unsafe clients, and countermeasures can be taken to mitigate the impact of foreign intrusions.

Last but not least, in *Wi-Fi Enterprise mode*, the OmniAccess Stellar APs embedded wIDS/wIPS capabilities do not require any additional license to protect the wireless network.

98.	The WLAN solution shall be able to identify Interfering APs.	C/PC/NC

A wireless network is a borderless network and always works in an open environment which can be interfered with and attacked. It is useful to discover the surrounding wireless conditions, and based on that, provide instructions and tools to help administrators improve the quality of the wireless network. Usually there are two types of foreign unknown APs having a negative effect on the wireless network; they are interfering APs and rogue APs.

An **interfering AP** is an AP seen in the wireless environment but not connected to the wired network. The interfering AP can provide RF interference potentially, but it is not considered a direct security threat, because it is not connected to the wired network. However, some interfering APs may have an impact on network quality and can interfere with valid clients accessing the network.

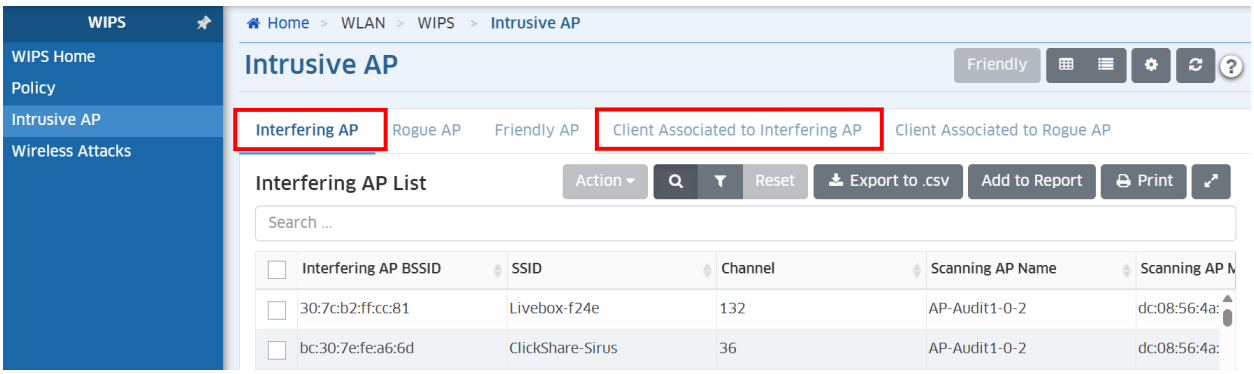


Figure 74: wIDS/wIPS – Omnivista 2500 (Intrusive Access Points)

99.	The WLAN solution shall be able to identify and contain Rogue APs.	C/PC/NC

Beyond potential RF interference it can cause, a **rogue AP** is considered as a security threat to the WLAN network. This is typically the case of an unauthorized AP plugged into the wired side of the network (in that case, the MAC address of the scanned interfering AP is identified in the Forwarding Database of the scanning AP) or a foreign interfering AP broadcasting a SSID that is configured and set in the WLAN network.

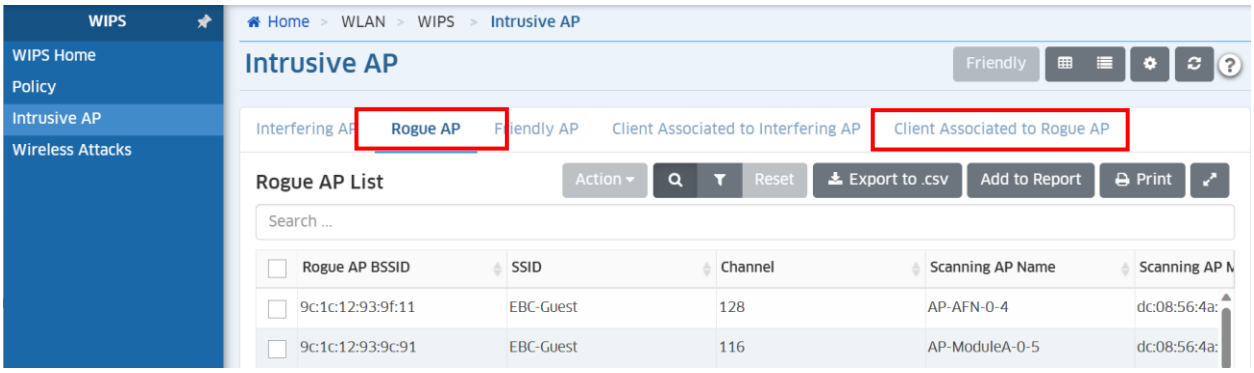


Figure 75: Rogue APs containment – Omnivista 2500 (Intrusive Access Points)

When an AP is classified as a rogue AP and when containment is enabled (disabled by default), the detecting AP (the one that detected the rogue AP) will send DEAUTH frames to clients that have associated to the rogue AP, keeping the clients away from the unsafe wireless network.

100.	A least for a “Large deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible policies to classify an AP as a Rogue AP.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, beyond the detection of a valid SSID, and as described in table below, the OmniAccess Stellar WLAN solution can consider several other parameters for rogue AP classification:

Rogue AP policy	Description	Wi-Fi Enterprise
Unauthorized AP detected on LAN	▪ When an intrusive AP is plugged into the wired side of the network	Y

Detect Valid SSID	▪ When an intrusive AP plugged on the wired network is advertising a SSID that is already configured and set in the WLAN network	Y
	▪ When an intrusive AP not plugged on the wired network is advertising a SSID that is that is already configured and set in the WLAN network and a known station MAC is detected associating with it.	Y
Signal Strength Threshold	▪ The detected AP signal in dbm is too strong and above the threshold ▪ Default: – 70 dbm (Range: -95 to -50 dbm)	Y
Detect Rogue SSID Keyword	▪ The detected AP is advertising a SSID name that matches one of the string set in this policy (SSID blacklist)	Y
Rogue OUI	▪ The detected AP is having a OUI that matches one of the OUI set in this policy	Y

Table 6: Rogue AP policy

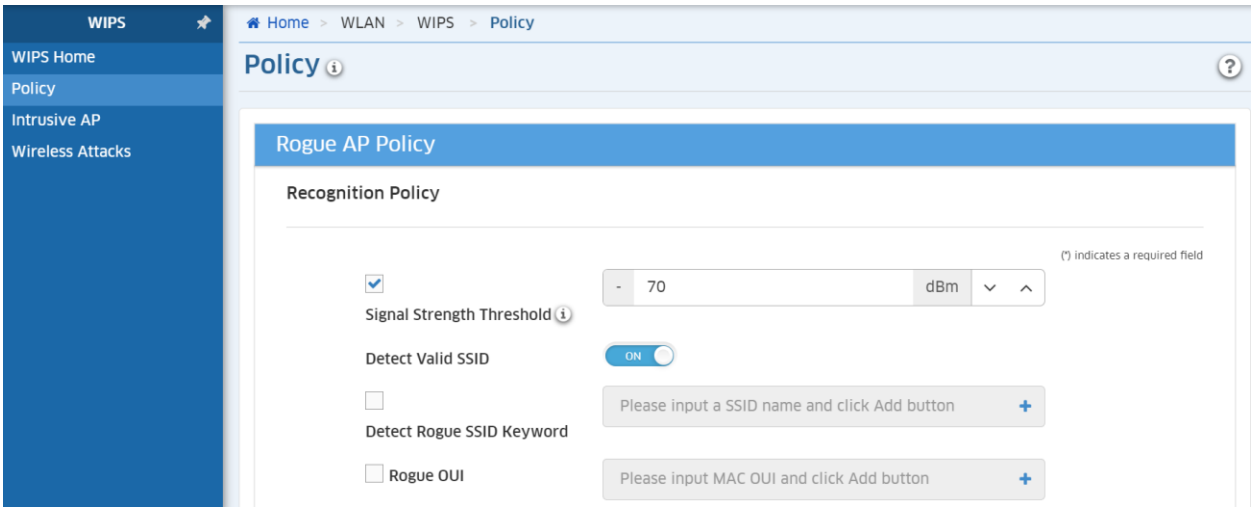


Figure 76: Rogue APs policy – Omnivista 2500 (Policy)

101.	A least for a "Large deployment" scenario as described previously [4], the WLAN solution shall allow the definition of flexible AP attacks detection policies.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In *Wi-Fi Enterprise mode*, the OmniAccess Stellar solution allows to create flexible policies to detect and react to AP wireless attacks. When an attack is detected based on the policy, the detected AP is displayed with details for review and action. An AP Attack Detection Policy detects multiple attacks originating from foreign APs. The following detection methods are available:

AP Spoofing	An AP Spoofing attack involves an intruder sending forged frames that are made to look like they are from a valid AP.
AP Impersonation	In AP impersonation attacks, an AP assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a *Honeypot* attack.
Broadcast De-authentication	A de-authentication broadcast attempts to disconnect all clients in range. Rather than sending a spoofed de-authentication frame to a specific MAC address, this attack sends the frame to a broadcast address.
Broadcast Disassociation	By sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF), an intruder can disconnect all stations on a network for a widespread DoS.
Adhoc networks using a valid SSID	If an unauthorized adhoc network is using the same SSID as an authorized network, a valid client may be tricked into connecting to the wrong network. If a client connects to a malicious adhoc network, security breaches or attacks can occur.
Long SSID	802.11 allows a maximum of 32 bytes for the SSID. Over-sized SSIDs are indicative of an attack attempting to exploit vulnerabilities in several drivers
Adhoc Networks	An adhoc network is a collection of wireless clients that form a network among themselves without the use of an AP. If the adhoc network does not use encryption, it may expose sensitive data to outside eavesdroppers. If a device is connected to a wired network and has bridging enabled, an adhoc network may also function like a rogue AP. Additionally, adhoc networks can expose client devices to viruses and other security vulnerabilities.
Wireless Bridge	Wireless bridges are normally used to connect multiple buildings together. However, an intruder could place (or have an authorized person place) a wireless bridge inside the network that would extend the corporate network somewhere outside the building. Wireless bridges are somewhat different from rogue APs in that they do not use beacons and have no concept of association. Most networks do not use bridges. In these networks, the presence of a bridge is a signal that a security problem exists.
Null Probe Response	A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving such a probe response.
Invalid Address Combination	In this attack, an intruder can cause an AP to transmit de-authentication and disassociation frames to its clients. Triggers that can cause this condition include the use of broadcast or multicast MAC address in the source address field.
Reason Code Invalid of De-authentication	The 802.11 specification defines valid reason codes for disconnect and de-authenticate events. De-authentication packets with invalid reason code will be classified as an attack.

Reason Code Invalid of Disassociation	The 802.11 specification defines valid reason codes for disconnect and de-authenticate events. Disassociation packets with invalid reason code will be classified as an attack.

Table 7: AP attack policy - Enterprise mode

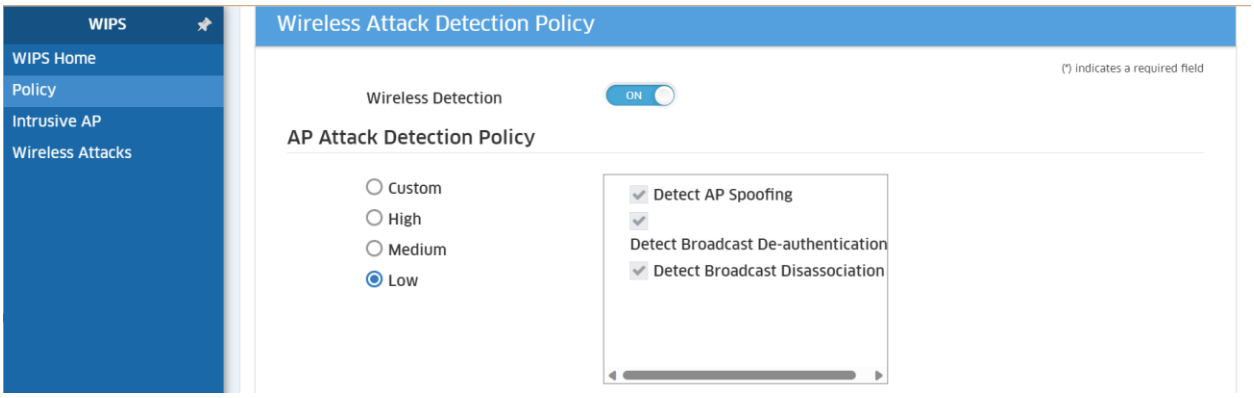


Figure 77: AP attack detection policy – Omnivista 2500 (WIPS Policy)

102.	A least for a "Large deployment" scenario as described previously [4], the WLAN solution shall allow the definition of flexible client attacks detection policies.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In *Wi-Fi Enterprise mode*, the OmniAccess Stellar solution allows to create flexible policies to detect and react to client wireless attacks. When an attack is detected based on the policy, the detected client is displayed and can be automatically blacklisted (its MAC address is not allowed to associate to any AP of the WLAN). The following detection methods are available:

Valid Station Misassociation	This feature does not detect attacks, but monitors authorized (valid) or innocent wireless clients associated to a rogue AP.	not blacklisted
Omerta Attack	Omerta is an 802.11 DoS tool that sends disassociation frames to all stations on a channel in response to data frames. The Omerta attack is characterized by disassociation frames with a reason code of 0x01. This reason code is "unspecified" and is not be used under normal circumstances.	blacklisted
Unencrypted Valid Client	This feature does not detect attacks, but monitors authorized (valid) or innocent wireless clients associated to an open (no encryption) SSID. A valid client that is passing traffic in unencrypted mode is a security risk. An intruder can sniff unencrypted traffic (also known as packet capture) with software tools known as sniffers. These packets are then reassembled to produce the original message.	not blacklisted
802.11 40Mhz Intolerance setting	When a client sets the HT capability "intolerant bit" to indicate that it is unable to participate in a 40MHz BSS, the	blacklisted

	AP must use lower data rates with all of its clients. Network administrators often want to know if there are devices that are advertising 40MHz intolerance, as this can impact the performance of the network.	
Active 802.11n Greenfield Mode	When 802.11 devices use the HT operating mode, they can't share the same channel as 802.11a/b/g clients. Not only can they not communicate with legacy devices, the way they use the transmission medium is different, which would cause collisions, errors and retransmissions.	blacklisted
DHCP Client ID	A client which sends a DHCP DISCOVER packet containing a Client-ID tag (Tag 61) which doesn't match the source MAC of the packet may be doing a DHCP denial-of-service to exhaust the DHCP pool.	blacklisted
DHCP Conflict	Clients which receive a DHCP address and continue to use a different IP address may indicate a mis-configured or spoofed client.	blacklisted
DCHP Name Change	The DHCP configuration protocol allows clients to optionally put the hostname in the DHCP Discover packet. This value should only change if the client has changed drastically (such as a dual-boot system). Changing values can often indicate a client spoofing/MAC cloning attack.	blacklisted
Malformed Frame Association Request	A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving such a probe response.	blacklisted
Sticky Client	Client keep trying to authenticate with too much authentication failure.	blacklisted
Detect Long SSID in Client detection	The 802.11 specification allows a maximum of 32 bytes for the SSID. Over-sized SSIDs also in probe request frame or associate request frame are indicative of an attack attempting to exploit vulnerabilities in several drivers.	blacklisted
Detect Reason Code Invalid	The 802.11 specification defines valid reason codes for disconnect and de-authenticate events. Invalid reason code in disassociation frames and de-authentication frames indicates an attack attempt.	blacklisted

Table 8: Client attack policy - Enterprise mode

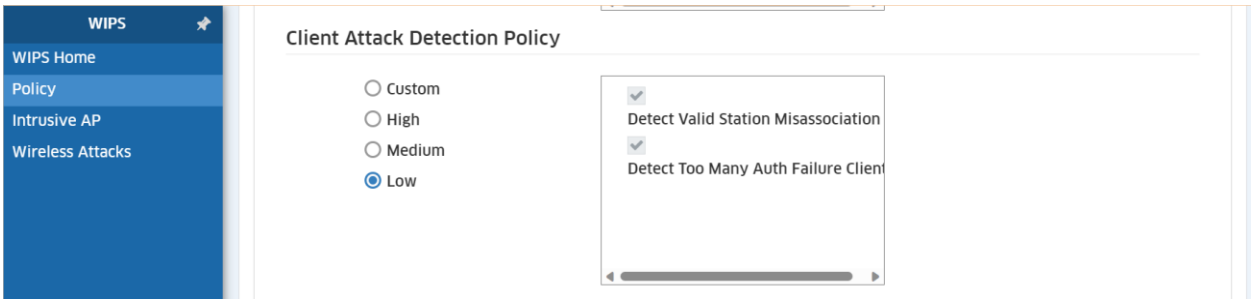


Figure 78: Client attack detection policy – Omnivista 2500 (WIPS Policy)

103.	A least for a “Large deployment” scenario as described previously [4], the WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In *Wi-Fi Enterprise mode*, the OmniAccess Stellar solution allows to blacklist a client manually or automatically. If a wireless attack has been detected the intruder identified (MAC address) by the wIDS/wIPS application is prevented from associating with the network.

104.	A least for a “Large deployment” scenario as described previously [4], the WLAN solution shall allow to configure a blacklist duration.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode*.

105.	A least for a “Large deployment” scenario as described previously [4], the WLAN solution shall allow to configure an authentication failure times threshold.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode*. When a client fails to pass the authentication in the associated phase for too many times in a brief period, it will be classified as an intruder and added into the “Client Blacklist”. (Ranges: 3 - 10 times per 5 - 3600 seconds, Default: 10 times per 60 seconds).

The picture below summarizes the policies on client blocklist.

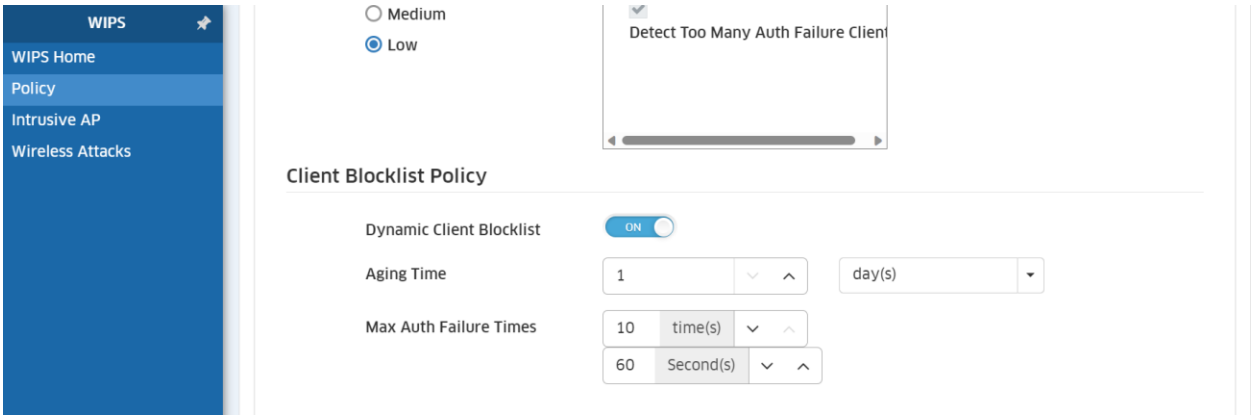


Figure 79: Client Blocklist policy – Omnivista 2500 (WIPS Policy)

3.4. Quality of Service

106.	At least for a "Large deployment" scenario as described previously [4], the WLAN solution shall offer WLAN Access Points that shall support fine-tuned Quality of Service (QoS) allowing following actions based on the identity of the connecting user: - ACL based (source/destination IP address and TCP/UDP ports) permit/deny decision - QoS priority marking and queuing	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Each time a user connects to the WLAN network, a role is assigned to that user and connection. That role assigns a VLAN to the user. It also defines and applies network security ACLs and a QoS policy to the user connection. The security ACLs (based on source/destination IP address and TCP/UDP ports) allow to restrict the resources the user can access like critical financial servers.

The QoS policy defined in the user role allows to assign the QoS markings (802.1p/DSCP on the wired side, and WMM over the air) within the AP based on the user identity in order to apply user specific treatment to the traffic originating from or destined for that user, thus providing appropriate QoS for each application such as voice, video and desktop sharing.

107.	The wireless LAN solution shall comply with the 802.11e WMM standard and shall allow for custom QoS tag (802.1p/DSCP) to WMM queue mapping.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. The OmniAccess Stellar solution and Access Points are indeed WFA 802.11e WMM certified, ensuring proper prioritization of real-time voice and video traffic and applications according to four categories: "Voice", "Video", "Best Effort" and "Background".

In the downstream portion of the WLAN network (AP to the device), prioritization is handled in the AP. Delay sensitive traffic is identified by the AP based on the 802.1p MAC header field or the DSCP IP header field of the inbound traffic. Upon receiving priority-tagged frames, the AP places these frames into a high-priority queue. Frames are transmitted using a strict queuing method, ensuring that high priority frames are always transmitted before low-priority frames.
In the upstream portion of the WLAN network (device to the AP), devices transmitting priority-sensitive traffic can use WMM (Wi-Fi Multimedia) - a derivative of IEEE 802.11e -to provide preferential access to the wireless media. WMM also provides a mechanism for client devices to tag frames with a relative priority, allowing the AP to recognize the relative priority of the received frame.

The OmniAccess Stellar solution, in Wi-Fi *Enterprise* mode, allows for use of customized DSCP/802.1p to WMM queue mapping to accommodate already existing assignments used within the wired LAN. The OmniVista 2500 NMS allows granular WMM-802.1p/DSCP mapping:

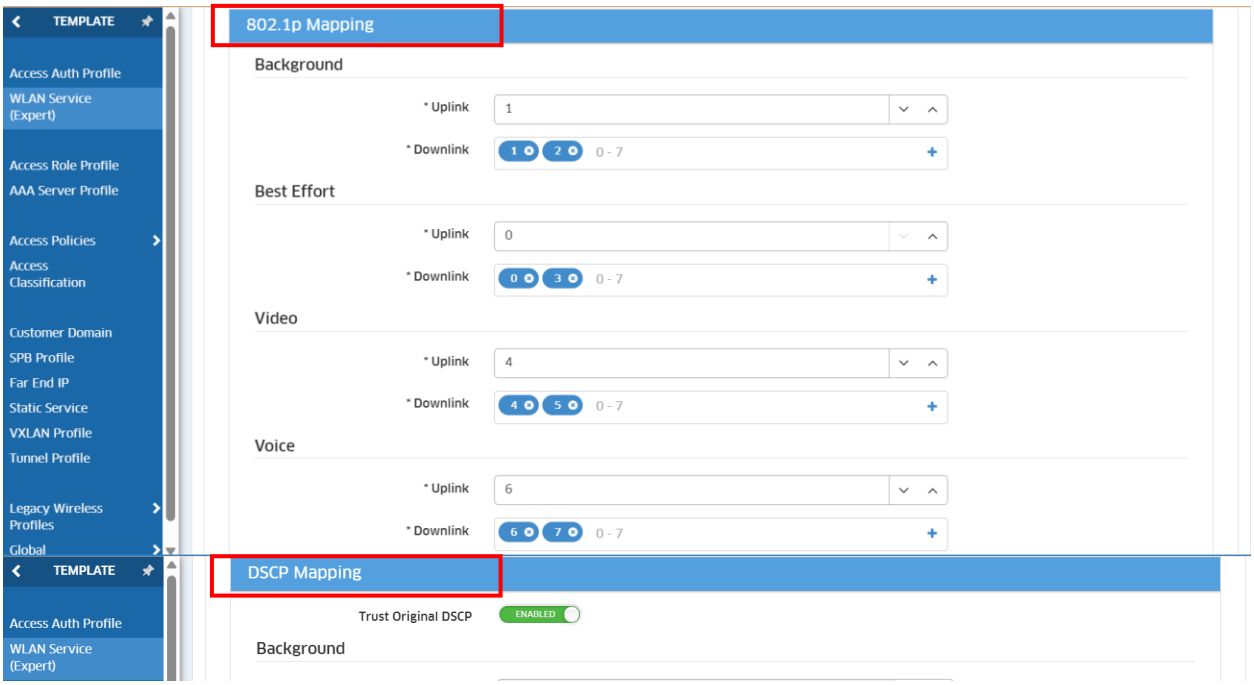


Figure 80: WMM/802.1p-DSCP mapping - Omnivista 2500 (WLAN Service Expert)

The recommended WMM/802.1p-DSCP mapping settings are described in following table:

WMM	802.1p	DSCP
Best Effort	3	18 – AF 2x
Background	2	18 – AF 2x
Voice	6	46 - EF
Video	4	26 – AF 3x

Table 9: WMM/802.1p-DSCP recommended mapping

108.	A least for a "Large deployment" scenario as described previously [4], the WLAN solution shall have traffic L7 Application fingerprinting (aka *Deep Packet Inspection* (DPI) capabilities allowing an administrator to take control of applications (even if they all run on top of the HTTP or HTTPs protocols), including not only blocking applications, but also allowing to prioritize and rate-limit applications.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution in Wi-Fi *Enterprise* mode fully complies with this requirement when managed by Omnivista 2500. Indeed, the AP12xx series (except AP1101 and AP1201H) , Wi-Fi 6 AP13xx series, Wi-Fi 6E AP14xx series and Wi-Fi 7 AP15xx series, have a built-in DPI technology that provides real-time applications classification and role-based control capabilities: The

Application Visibility and Enforcement feature. With *Wi-Fi Enterprise mode,* the network administrator can obtain a comprehensive view of applications running in the network and apply adequate control to optimize the performance of the network for business-critical applications. It is also possible to prevent harmful or non-compliant applications from being utilized and also create a space for employees to explore new applications and also use personal apps, harmonizing the coexistence of both business and personal applications.

Figure 81: Application Visibility & Enforcement - Enterprise mode

Application Visibility and Enforcement is an answer to the challenge of application "webification". More and more applications - even corporate application - use the same port to communicate and appear as HTTP(S) traffic. Based on a signature application file and its DPI capability, the *Application Visibility and Enforcement* feature allows identifying unique applications (even when encrypted) and apply different prioritization and QOS (with QoS policy lists defined in the applied user/device role) to critical applications like Salesforce, SAP, Rainbow and IP telephony against some personal services like Facebook, YouTube etc.

109.	At least for a "Large deployment" scenario as described previously [4], the wireless LAN solution shall be able to define and guarantee bandwidth on basis of a SSID. It shall also be able to define and guarantee bandwidth based on a user/device role.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, in *Wi-Fi Enterprise mode*, a "bandwidth contract" may be defined and set at user/device role level based on the QoS Policy List defined within the role. Moreover, the Policy List can embed an Application/DPI rule as previously introduced [108]. As depicted in *Figure 81* below, a "bandwidth contract may also be set at SSID level (the bandwidth is then shared for all users, per radio) by specifying:

- the upstream (Ingress) bandwidth (and depth) for the SSID
- the downstream (Egress) bandwidth (and depth) for the SSID

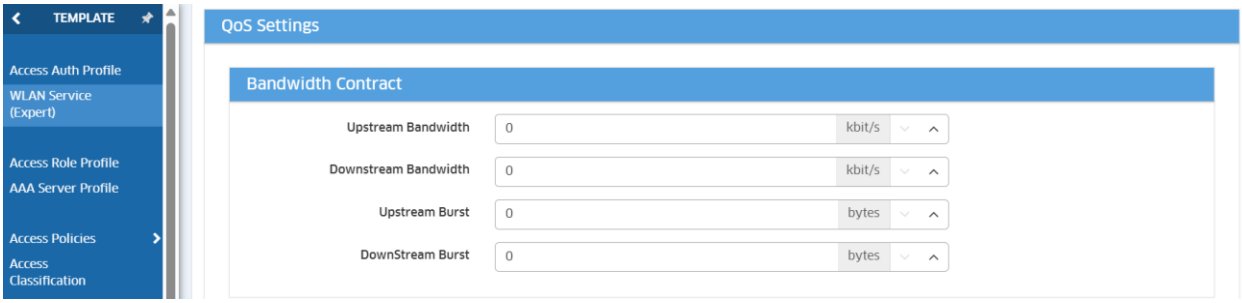


Figure 82: SSID Bandwidth Contract – Omnivista 2500 (WLAN Service Expert)

In *Wi-Fi Enterprise mode*, a WLAN service or SSID is always configured with an associated "Access Role Profile" that defines a default role that will be applied to a user if the authentication process for that user has succeeded but has not returned a role. In that case the connected user will be assigned the VLAN, the security ACLs and the QoS Policy List defined in the SSID "Access Role Profile":

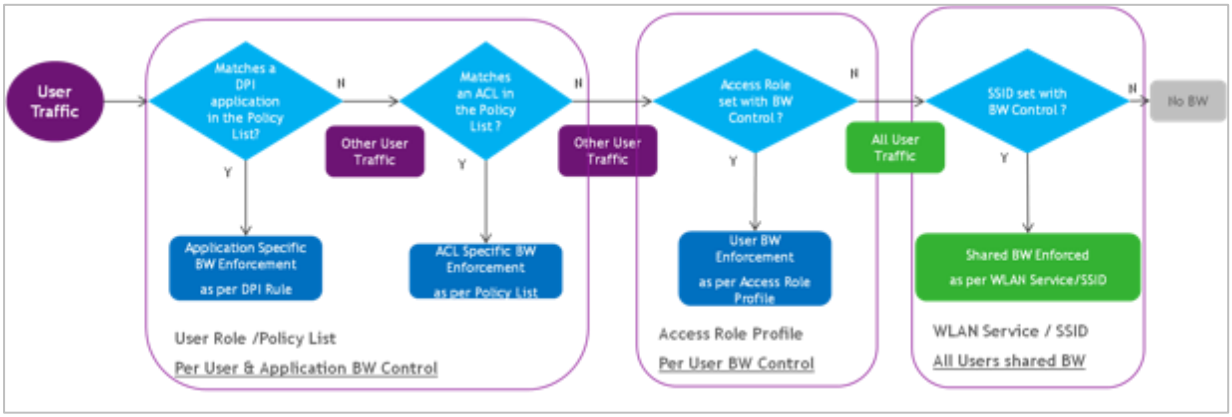


Figure 83: User bandwidth control Precedence

110.	At least for a "Large deployment" scenario as described previously [4], the WLAN solution shall allow to set the maximum number of clients per band/radio and per AP for a specific SSID.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

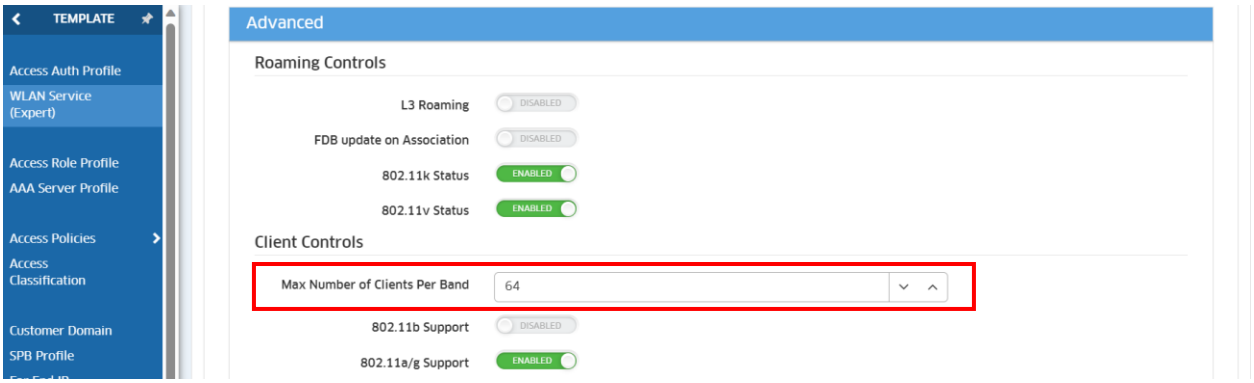


Figure 84: Maximum number of clients per band per SSID – Omnivista 2500 (WLAN Service Expert)

111.	The wireless LAN solution shall propose broadcast traffic optimization mechanisms (including Broadcast filtering and Broadcast/Multicast Key rotation).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

Below, the OmniAccess Stellar WLAN solution, in *Wi-Fi Enterprise mode*, allows to filter broadcast traffic by dropping all broadcast packets except DHCP & ARP. It allows also to convert broadcast ARP to unicast and proxy ARP for known devices:

Figure 85: Broadcast traffic Optimization – Omnivista 2500 (WLAN Service Expert)

The OmniAccess Stellar WLAN solution allows to activate "*Broadcast Key Rotation*" (with WPA, WPA2 or Dynamic WEP encryption only) and set the broadcast key rotation time (default value: 15 min, Range: 1 min – 24 hours):

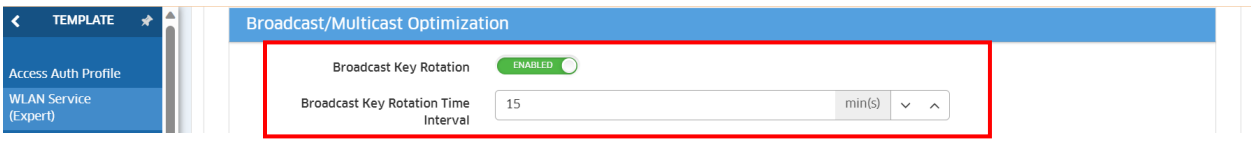


Figure 86: Broadcast Key Rotation – Omnivista 2500 (WLAN Service Expert)

When "*Broadcast Key Rotation*" is enabled, encryption keys constantly rotate, making them much harder for hackers to sniff with a protocol analyzer. But the faster the keys rotate, the more potential there is for transmission latency while the key resets. It is recommended to start with a small value, and, if performance issues are encountered, increase it until the performance issues stop.

112.	Leveraging its IGMP snooping capabilities, the wireless LAN solution shall be able to optimize multicast traffic by converting multicast traffic to unicast traffic.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In an OmniAccess Stellar deployment, multicast traffic is appropriately controlled to ensure that proper bandwidth exists for all connected devices/users. IGMP snooping, enabled on the APs in *Wi-Fi Enterprise mode*, allows to reduce the amount of traffic replication within the network infrastructure. IGMP Snooping is enabled by default and ensures that the wired infrastructure sends multicast traffic, such as video traffic, only to those APs that have active subscribers.

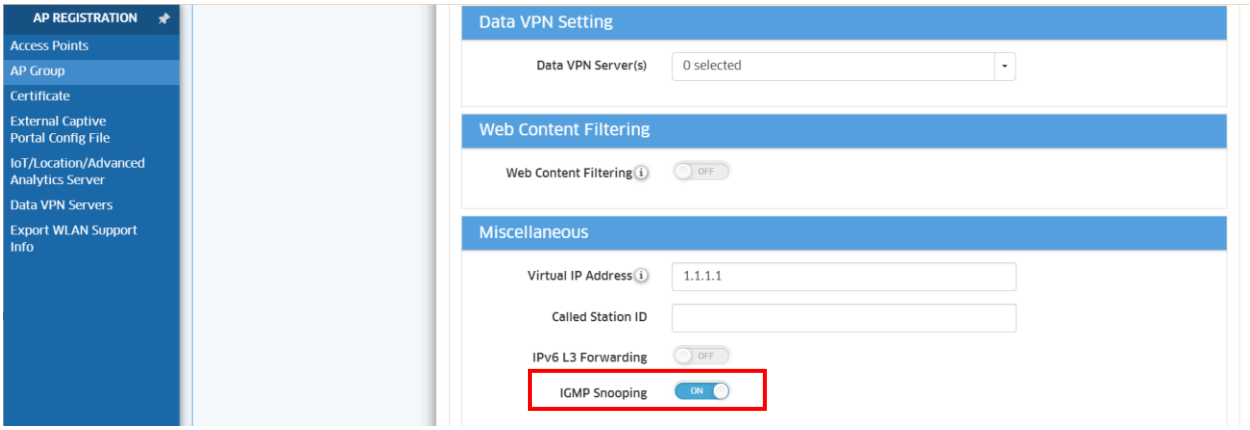


Figure 87: IGMP snooping – Omnivista 2500 (AP Group)

Wireless multicast transmissions occur at broadcast rates. Broadcast and multicast frames are not acknowledged, so these transmission methods use lower (slower) data rates to provide a better chance of reception. The 802.11 standard states that multicast over WLAN must be transmitted at the lowest supported rate so that all clients can decode it. The low transmission rate results in increased airtime utilization, and therefore decreased overall throughput for transmissions. Because of the slower speed, it is desirable to transform multicast traffic to unicast when a few clients have subscribed to a multicast stream. Transforming multicast traffic to unicast increases the speed of wireless transmissions by using the higher unicast rates.

113.	At least for a "Large deployment" scenario as described previously [4], Multicast optimization shall stop on high load.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. In general, unicast traffic can be transmitted at higher transmission rates and an acknowledgement ensures consistent delivery. However, after a certain number of clients have been reached, it is more efficient to revert to multicast transmissions.

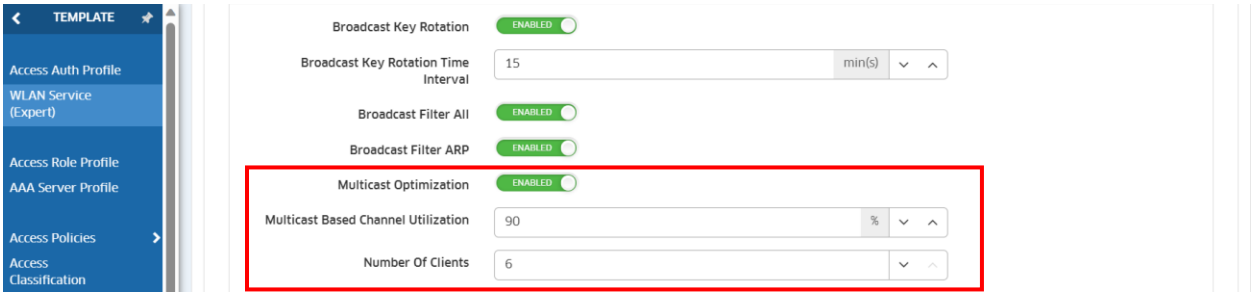


Figure 88: Multicast optimization – Omnivista 2500 (WLAN Service Expert)

Two parameters can be considered to stop multicast optimization on high load:

- Channel Utilization (RF environment too poor to have optimization): the default value is 90% (range: 85% to 95%)
- Number of Clients (CPU load too high to support optimization): the default value is 32 (range: 16 to 64)

114.	The wireless LAN solution shall propose the WMM *Automatic Power Save delivery* (APSD) feature to allow clients conserve battery life.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution and Access Points fully comply with this requirement when managed by Omnivista 2500, allowing mobile WLAN client (especially devices like phones running real time applications) to save more battery while connected to the WLAN network by entering standby or sleep mode. The WMM APSD feature allows smooth transition in and out of sleep mode by allowing the client to signal the AP of its status. Whenever the clients enter power saving mode or “sleep” mode, the AP can buffer data and hold it for the client. The client chooses the time to wake up and receive data packets to maximize power conservation without sacrificing Quality of Service.

As already seen in [71] WMM U-APSD is now implemented per SSID on Stellar WLAN solution. Stellar WLAN solution complements the power saving feature for 802.11ax OFDMA-based communications with TWT feature for clients with specific data transmission.

115.	The wireless LAN solution shall by default identify Voice and Audio/Video calls and provide appropriate treatment.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. It is indeed Voice and Video over IP aware and can dynamically classify

real-time traffic in appropriate Class of Service. In addition, this level of voice awareness enables OmniAccess Stellar APs to know that a voice/audio/video call is taking place and not to scan channels for RF management or intrusion detection purposes until the call is terminated.

3.5. Mobility

116.	The WLAN solution shall support Layer 2 roaming capabilities across APs with no special client-side software required.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode*. Mobility and roaming are a necessity. In an Alcatel-Lucent Enterprise Stellar deployment, roaming is always transparent and seamless to both the client and the network (the end goal is that the client's view of the network does not change and the network's view of the client does not change). With very high roaming performances, delay-sensitive and persistent applications such as voice and audio/video do not suffer interruption.

L2 roaming between APs means the roaming client remains in the same VLAN when associating to the new AP and its IP address does not change. Roaming between APs occurs on the same subnet and all traffic goes through standard Layer 2 learning to allow a WLAN client to move from one AP to another. L2 roaming is always enabled.

Roaming relies on "client contexts" sharing between adjacent APs and L2 or L3 roaming decision is based on client VLAN between the "home" and the "foreign" AP. All APs learn about their neighboring APs through "over-the-air" exchanges allowing to announce to each other their respective IP management on the wired side of the network. The adjacent APs can then share dynamically client contexts that contain client specific information allowing the APs to handle roaming properly. "Client contexts" exchange evolves starting from AWOS 5.0.1 for the AP13xx, AP14xx, and AP15xx series with secured exchanges with DTLS encryption. The user then provides a roaming domain for all client context exchanges.

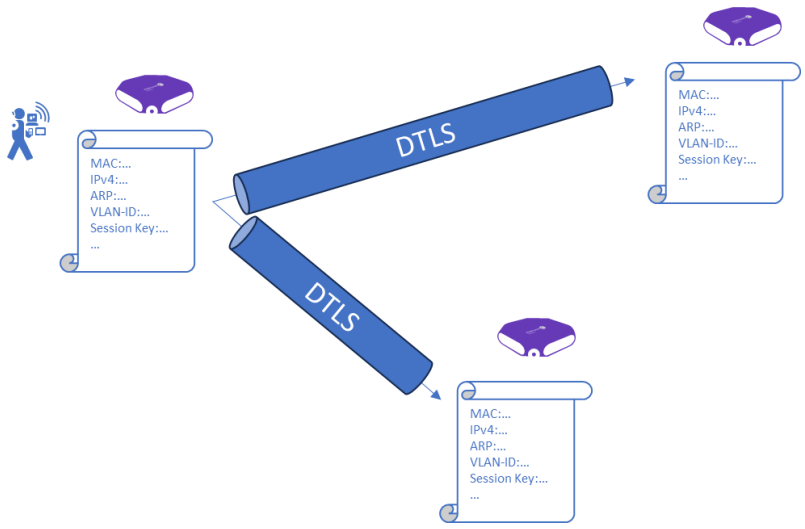


Table 10: Client contexts

Upon roaming, the adjacent AP implement a client context removal mechanism. On client association, the new AP sends an *Add message* to all adjacent APs, and, on client dis-association, the AP sends a *Delete message* to all adjacent APs. On a receiving AP, *Add*/*Delete* messages are discarded when the AP is not managed by the same OV, or when the AP does not have the WLAN service (SSID).

The following figure illustrates the *Add* messages that are sent by an AP to its adjacent APs upon association of a client on the move (*Delete* messages are not depicted):

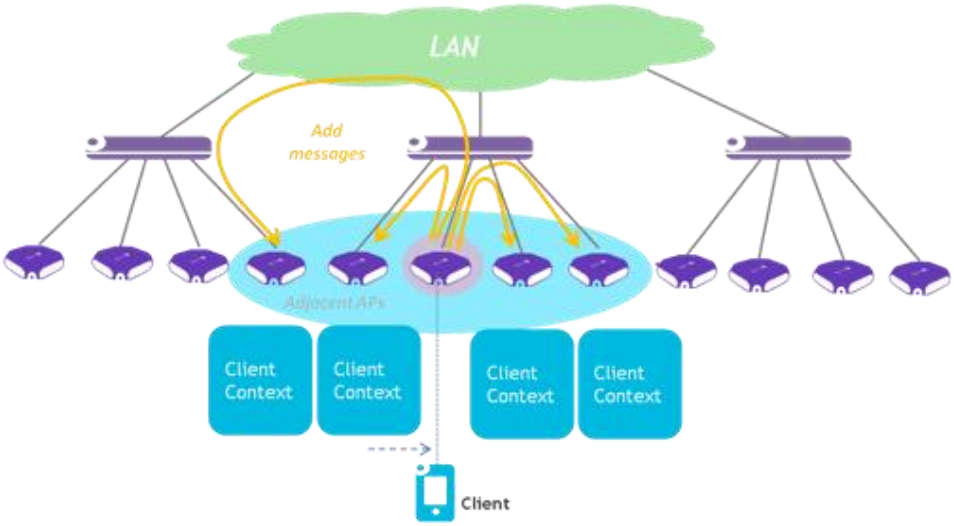


Figure 89: client context sharing

The roaming conditions may be summarized as follows:

Client Context exists on the new AP?	Client Context WLAN service and Access Role Profile exist on new AP?	Client Context VLAN ID = VLAN ID mapped to the Access Role Profile on new AP?	Roaming Results
No	-	-	No Roaming, new client
Yes	No	-	No Roaming, new client
Yes	Yes	Yes	L2 Roaming
Yes	Yes	No	L3 Roaming

Table 11: Client roaming conditions

117.	At least for a "Large deployment" scenario as described previously [4], the WLAN solution shall support Layer 3 roaming across APs with no special client-side software required.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution, in *Wi-Fi Enterprise mode*, fully complies with this requirement when managed by Omnivista 2500.

In campus WLAN deployments, there have to be multiple user VLANs that need to be provisioned since the number of IP addresses available per VLAN are restricted by the subnet size (for instance, 255 for 255.255.255.0 or /24 address space) and there are more mobile users in a WLAN deployment than the provisioned address space. WLAN deployment hence require provisioning of different APs, supporting the same SSID, assigned with different user VLANs. A wireless user that roams across APs that are assigned with different user VLANs is regarded as performing L3 roaming – as it is roaming across different user VLANs. The *Enterprise mode* of the OmniAccess Stellar WLAN solution allows to automatically tunnel the traffic of a roaming client from the "Foreign" AP (the new associating AP) to the "Home" AP (the former associating AP). A L2 GRE tunnel is indeed established by the Foreign AP to the Home AP at early stage of roaming and the client traffic is transparently tunneled to the Home AP where it is then processed locally. This allows users to roam the enterprise without a change of IP address as depicted in following figure where the same SSID is broadcasted in two floors of a same building but with specific user VLANs per floor:

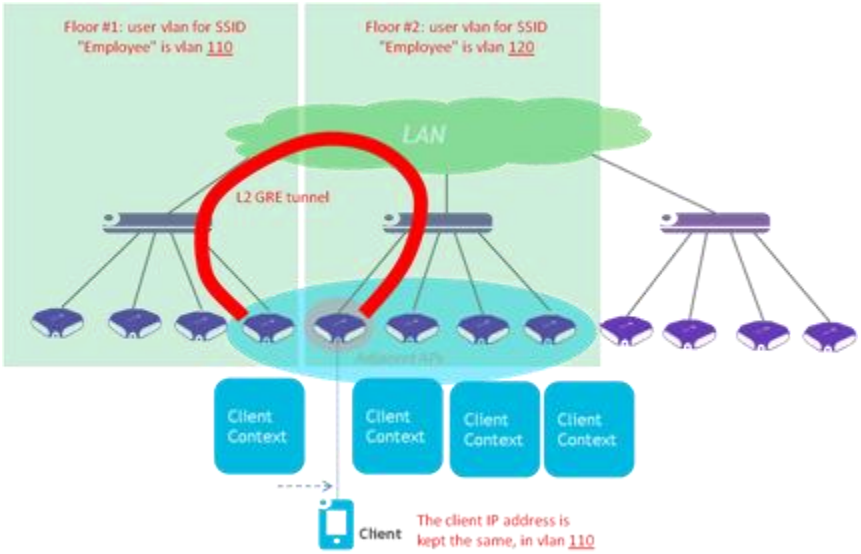


Figure 90: L3 roaming

All policies including QoS and security ACLs, are maintained as the user roams and L3 roaming (disabled by default) shall be enabled at SSID ("WLAN service") level:

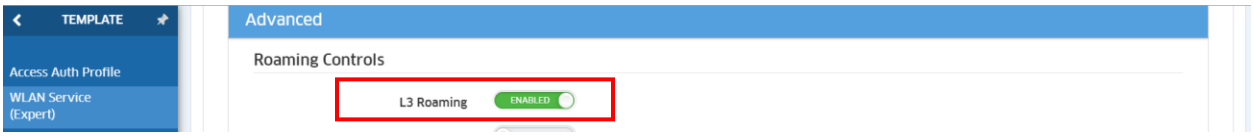


Figure 91: L3 roaming activation – Omnivista 2500 (WLAN Service Expert)

118.	The WLAN solution shall support 802.11r Fast Roaming and OKC - *Opportunistic Key Caching.*	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

802.11r Fast Roaming simplifies the handoff process by reducing the 802.1X negotiation steps when moving from the existing AP to the new one.

802.11r has been designed to create a more seamless roaming experience for WLAN clients. 802.11r is particularly useful for VoIP or other real-time applications where long roaming times can result in a very noticeable impact on performance. 802.11r uses *Fast Basic Service Set Transition* (FT) to allow encryption keys to be stored on all APs in a network.

This way, a client doesn't need to perform the complete authentication process to an authentication backend server every time it roams to a new AP within the network. They are hence avoiding a significant amount of latency that would have previously delayed network connectivity.

802.11r reduces roaming delay by pre-authenticating clients with multiple target APs before client roams to an AP.

Opportunistic key caching (OKC, part of 802.11i), supported on Enterprise SSIDs only (802.1X), helps reduce the time needed for authentication. When OKC is used, multiple APs share *Pairwise Master Keys* (PMKs, resulting from the initial 802.1X client authentication), and the WLAN client can roam to a new AP that has not visited before reusing the derived PMK of the current AP. OKC allows the client to roam quickly to an AP it has never authenticated with, eliminating the 802.1X process. OKC helps stations to handover faster by caching the PMK. When the PMK is cached, stations can bypass 802.1X authentication and derive new encryption keys when they roam between APs.

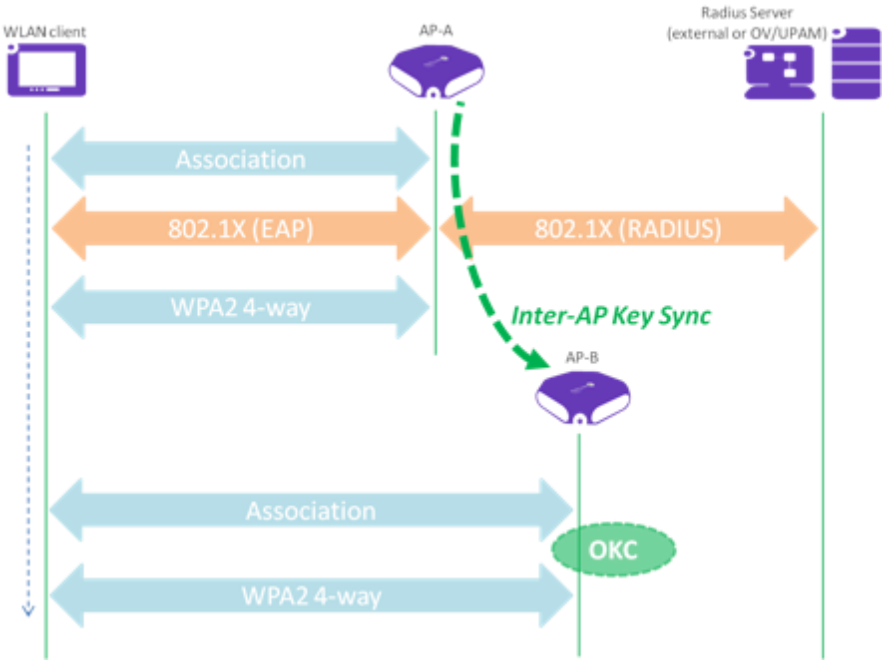


Figure 92: 802.11r fast roaming and OKC

119.	The WLAN solution shall comply with the 802.11k Radio Resource Management standard.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

The 802.11k standard provides information to discover the best available access point.

The 802.11k protocol enables Stellar APs and clients to measure the available radio resources dynamically. When 802.11k is enabled, Stellar APs and clients send reports containing:

- Beacon
- Neighbor Report
- Link Measurement

With the Neighbor Report, the Stellar AP informs the station about other APs in the RF Neighborhood to create a list. Using the Beacon Reports, the station tells the Stellar AP about the signal level (RSSI) of the beacons received from the other Stellar APs. The Channel Reports allows the Stellar AP to inform the station about the channels in use for the WLAN network.

With this information, already associated stations will build up a table with the optimized list of alternative APs. When the signal strength of the current AP fades out below a transition level, the station will scan for target APs from the list that are the best candidates to handover. This mechanism provides a faster transition as the scanning is limited to some APs and assures the station will connect with the best possible AP, drastically reducing the “sticky client” problem.

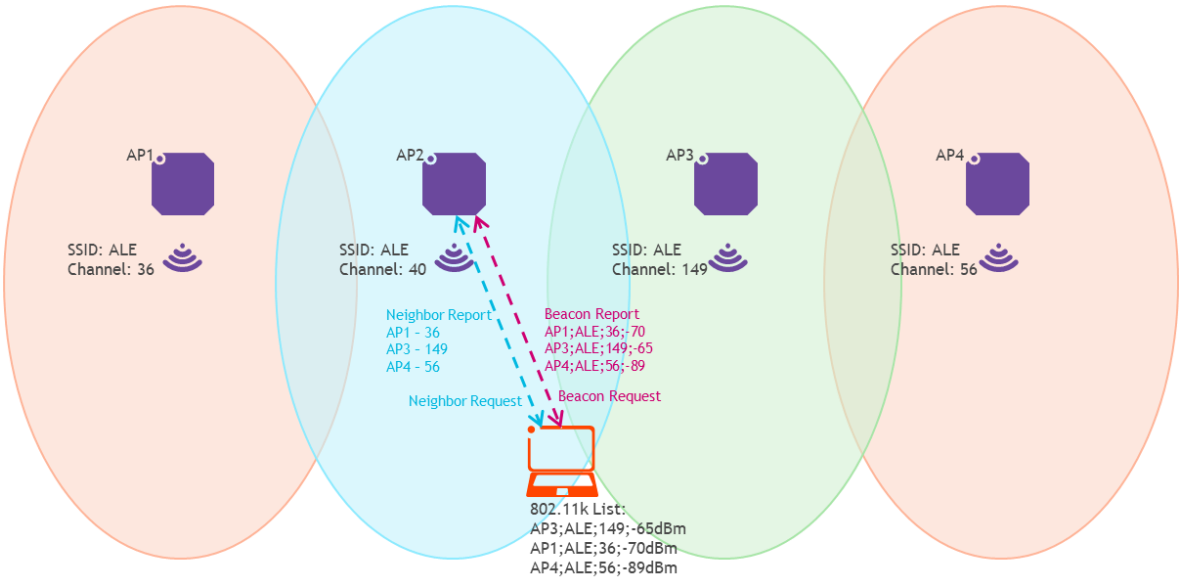


Figure 93: OmniAccess Stellar 802.11k support

802.11k is supported differently depending on the AP model, and is activated with channel scanning set on *working and non-working channels* mode in RF profile.

- Background scan mode for AP12xx series (Wi-Fi 5)

- Full scan mode for AP13xx/AP14xx/AP15xx series (Wi-Fi 6/6E/7)

120.	The WLAN solution shall comply with the 802.11v BSS Transition Management standard.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables a Stellar AP to request a client to transition to a specific Stellar AP or suggest a set of preferred Stellar APs to a client due to network load balancing or BSS termination. BSS transition mechanism allows also a client to request a set of preferred APs, at any time, according to its own operating criteria, and this without waiting for a new association to know the radio context and neighboring APs.

Stellar APs with 802.11v enabled can now direct devices to roam to another AP that it deems will provide a better WLAN experience for the device. Stations can now accept and respond to these Basic Service Set (BSS) Transition Management frames, leading to improved WLAN quality when connected to a network that supports 802.11v.

Enabling 802.11v in Stellar APs brings the following benefits:

- Network assisted Power Savings – Connected stations safe power by exchanging information with the WLAN network to stay longer in power-safe mode.
- Network assisted Roaming on AP's decision – The current AP will send information to associated stations about better APs, with lower network load. Stations may use this information to handover alternative, better AP.
- Network assisted roaming on client's decision - The client will request for a set of preferred APs, at any time, this without waiting for a new association to know the radio context.

Combining 802.11r, k and v WLAN will provide fast handovers for multimedia applications, eliminate "sticky client" problems, and balance the network load between the APs.

802.11v is supported differently depending on the AP model, and is activated with channel scanning set on *working and non-working channels* mode in RF profile.

- Background scan mode for AP12xx series (Wi-Fi 5)
- Full scan mode for AP13xx/AP14xx/AP15xx series (Wi-Fi 6/6E/7)

121.	The WLAN solution shall inform the wired side of the network about roaming across APs.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Ominivista 2500. *Forward Data Base Update* (FDB Update) *on association* enables, when a device roams to a new AP, to generate Gratuitous Address Resolution Protocol packet (Gratuitous

ARP) to the uplink switch. This to notify the switch to update the downstream forwarding port for device traffic, based on this new generated GARP.
This to enable location-based services to identify Stellar access points on which mobile device is actually connected, when conducting live or historical search of where the device is/has been connected to and through (ie. Ray Baum's Act step 2 law for location of mobile VoIP devices). Stellar FDB Update helps for devices that silently roam across APs without provide an ARP update by their own.

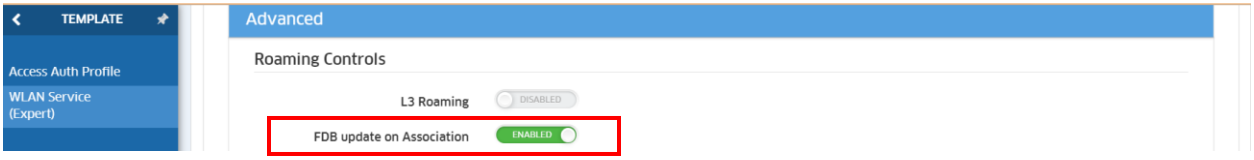


Figure 94: FDB Update disable option – Omnivista 2500 (WLAN Service Expert)

3.6. Wireless LAN Services

122.	In the framework of a "Large deployment" scenario as described previously [4], the solution shall provide BYOD Zeroconf services for mDNS	C/PC/NC

The OmniAccess Stellar WLAN solution provides a comprehensive solution for new trends like Bring Your Own Device (BYOD) and zero-configuration networking when managed by Omnivista 2500.

In some WLAN deployments, users are "bringing" their devices and connecting to available services. For instance, in Education, teachers may use their laptops and use the university smart screens to present content. Or in Hospitality, some guests will stream their favorite series to the big screen in the room.
Zeroconf or zero-configuration networking enables automatic discovery of devices and services on a network using industry-standard IP protocols. Zeroconf makes it easy to discover, publish, and resolve network services in a network.

Zeroconf, also known as Apple Bonjour, DLNA (UPnP), and other names, is based on standard protocols like mDNS (Multicast DNS) and SSDP (Simple Service Discovery Protocol).
One of the main drawbacks of these protocols is they rely on non-routable multicast groups. So a system advertising a service in one subnet (usually linked with a VLAN) will not be seen by a potential client of such service located in a different VLAN/subnet. Even using PIM routing, multicast communication will not flow, as the multicast IP addresses used by mDNS/SSDP are non-routable.

To overcome such drawbacks, Alcatel-Lucent Enterprise OmniAccess Stellar and OmniSwitch work together to deliver a smart and secure solution. The OmniSwitch product range offers two ways of solving this problem:

- OmniSwitch as mDNS/SSDP Gateway. In this mode of operation, the AOS8 will forward the zeroconf (mDNS and SSDP) multicast traffic between the configured VLANs. This simple mode allows all devices to discover all services in the network.
- OmniSwitch as mDNS/SSDP Responder. In this mode of operation, the AOS8 will forward the zeroconf multicast traffic between the configured L2GRE tunnels based on control policies. By

default and as a security feature, if there are no Service Rules configured, the AOS Responder will learn all the Services but will not process any zeroconf client request. There must be a defined Service Rule to forward client requests so that they can discover new services. A Service Rule is composed of a Client Rule and Server Rule. The Client Rules specify the clients, while Server Rules do the same with Servers publishing services. At least one of these parameters must be present in each rule: VLAN, ARP or Role, Location, Username, or MAC-address.

UPAM-NAC can dynamically assign VLAN and ARP, introducing another security layer by authenticating the users entering the network. For instance, if a user has both clients and servers, the service rule will allow only clients and servers with the same ARP to communicate.
Once a client discovers the service published by a server using multicast traffic (mDNS or SSDP), the communication is unicast and will flow according to the QoS and FW/ACL rules in the network.

OmniAccess Stellar WLAN supports both modes of operation when managed by Omnivista 2500.

- In the *AOS-Gateway mode* Stellar APs will place the traffic of the users in its corresponding VLAN, according to the ARP (Access Role Profile). The traffic will reach the OmniSwitch acting as Zeroconf gateway, forwarding Zeroconf multicast traffic between the configured VLANs.

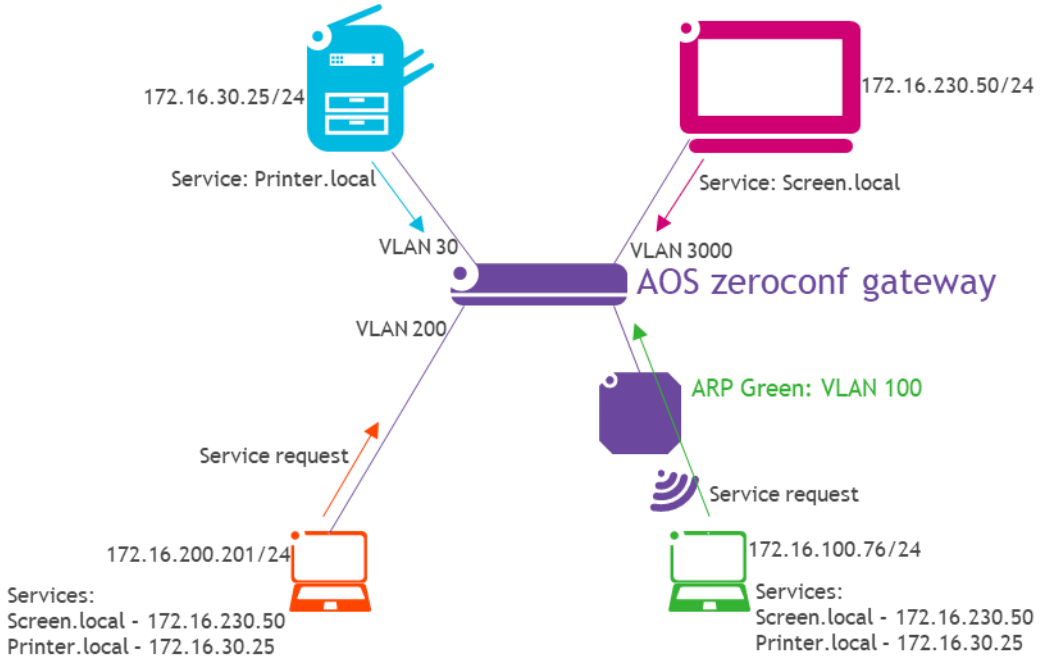


Figure 95: Stellar Zeroconf (mDNS/SSDP) in Gateway Mode

- In the *AOS-Responder mode* Stellar APs configuration captures ONLY Zeroconf traffic and sent if through a L2GRE tunnel towards the Responder. Responder will apply the Service Policies and forward the information to other edge devices. In the reverse path, the Responder will send zeroconf traffic to the Stellar APs using a L2GRE tunnel. At the end of this process, Servers have published their services and Clients have discovered the services.

When the client consumes a service, traffic is unicast. The Stellar AP sends the traffic directly to the switch, tagging the traffic with the corresponding VLAN.

L2GRE traffic is ONLY zeroconf (mDNS multicast traffic). Service traffic is sent out off the tunnel to be switched/routed by the network.

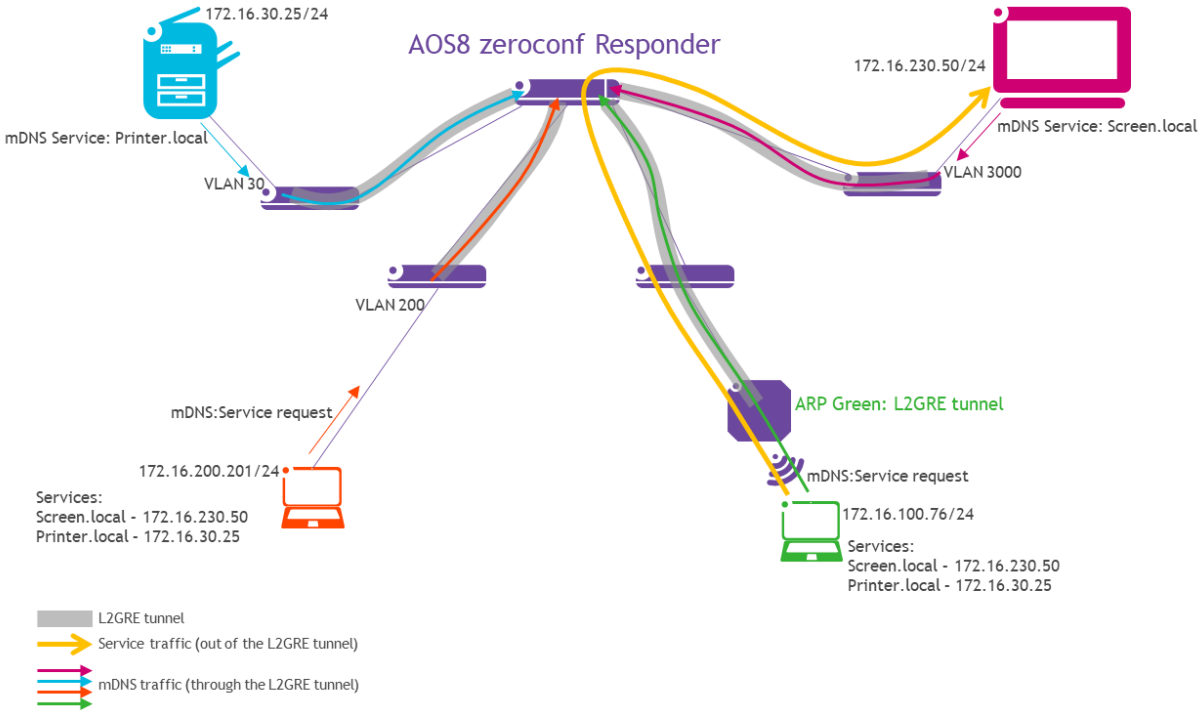


Figure 96: Stellar Zeroconf (mDNS/SSDP) in Responder Mode

In the Responder Mode, Stellar APs can terminate L2GRE tunnels not only in Alcatel-Lucent OmniSwitch AOS8 product families but in OmniAccess WLAN Controllers as well. In this case, the behavior of the OmniSwitch as Responder is the same as the Controller.

When the solution is based on OmniSwitch and Stellar, OmniVista can configure all the Zeroconf edge devices, responders, clients, server and service rules in the network. So OmniVista will have a full view of your Zeroconf services.

Configuring the responder is done under Unified Access -> Multimedia Services in Omnivista 2500:

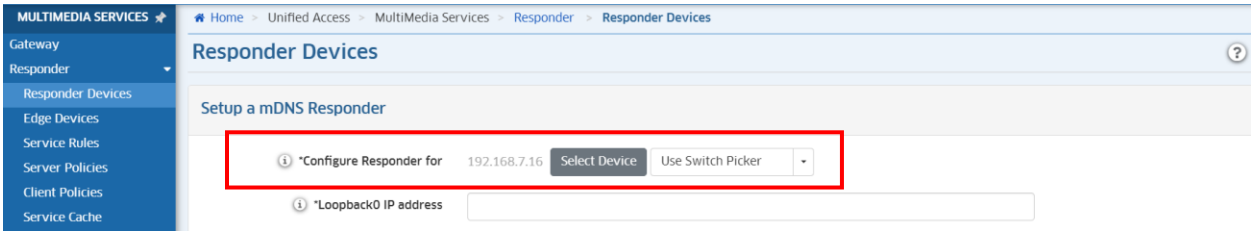


Figure 97: OmniVista Zeroconf configuration – Omnivista 2500 (Responder Devices)

The following menu configures Zeroconf gateways for AOS8 in *AOS-Gateway mode* in Omnivista 2500:

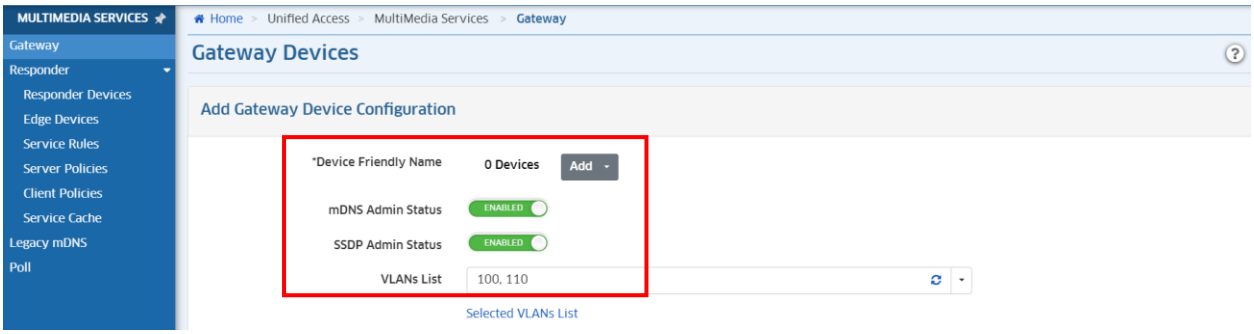


Figure 98: OmniVista Zeroconf gateway configuration – Omnivista 2500 (Gateway)

In the following example, VLANs 100 and 110 will exchange Zeroconf multicast traffic, so clients and servers in both VLANs can publish and discover them.

In Responder mode, there is an overview in Omnivista 2500 about the current status of the Zeroconf network:

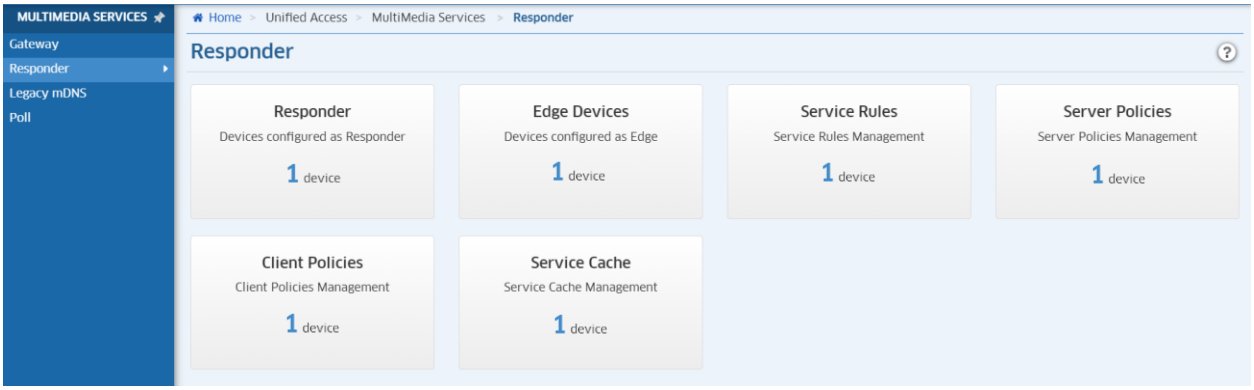


Figure 99: OmniVista Zeroconf Responder overview – Omnivista 2500 (Responder)

Responder devices configuration:

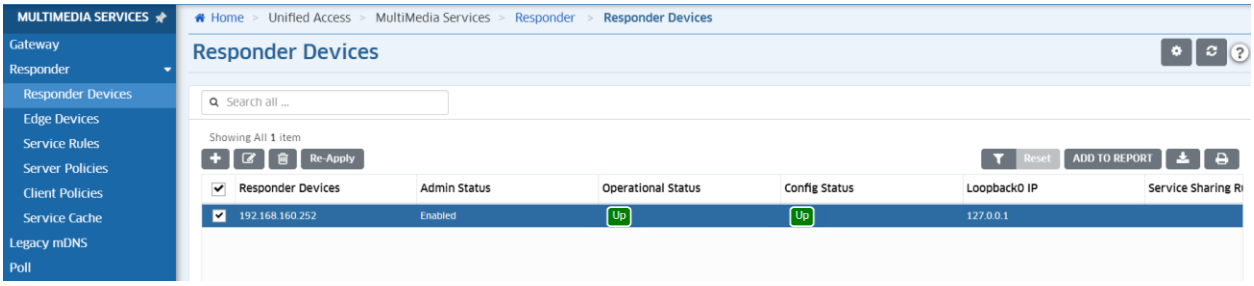


Figure 100: OmniVista Zeroconf Responder Configuration – Omnivista 2500 (Responder Devices)

Services learnt by the Responders (that can be used in the Service Policies):

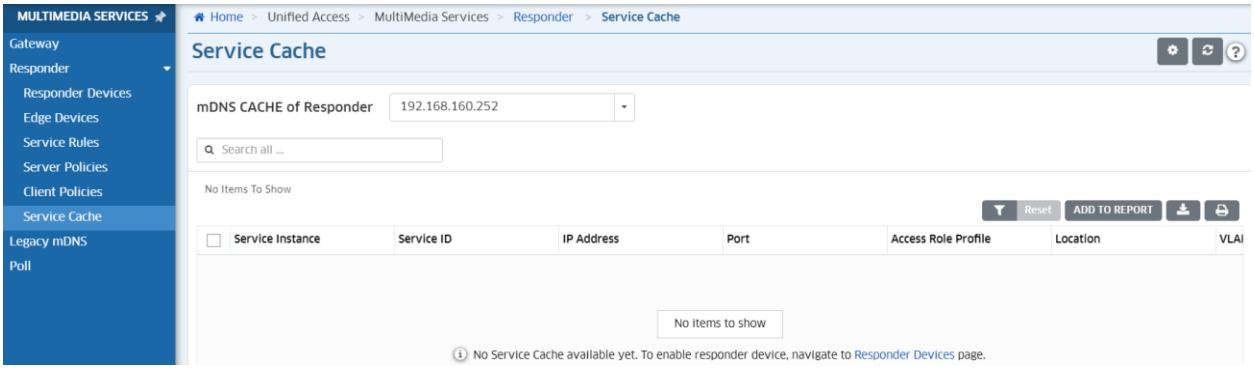


Figure 101: OmniVista Zeroconf Responders Services cache – Omnivista 2500 (Service Cache)

Edge devices, OmniSwitch and Stellar AP configuration:

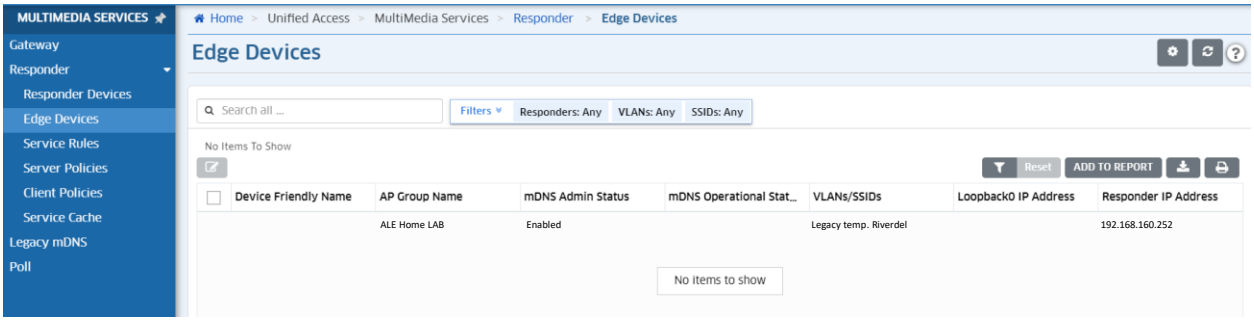


Figure 102: OmniVista Zeroconf Edge devices configuration – Omnivista 2500 (Edge Devices)

Service Rules will enable the Responder to forward mDNS/SSCP messages between the allowed devices:

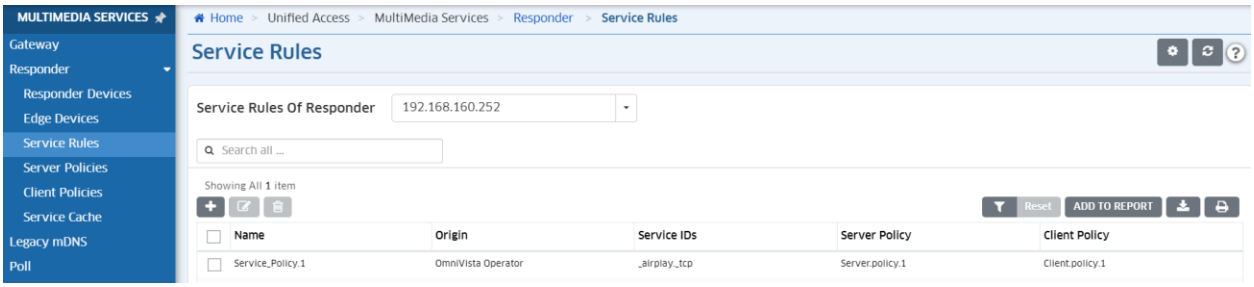


Figure 103: OmniVista Zeroconf Service policies – Omnivista 2500 (Service Rules)

Service Policies specify what services are allowed in the network, and relations between clients and servers serving the specified services. In this case, devices in VLAN 100 and 110 will be allowed to exchange information about 9 services:

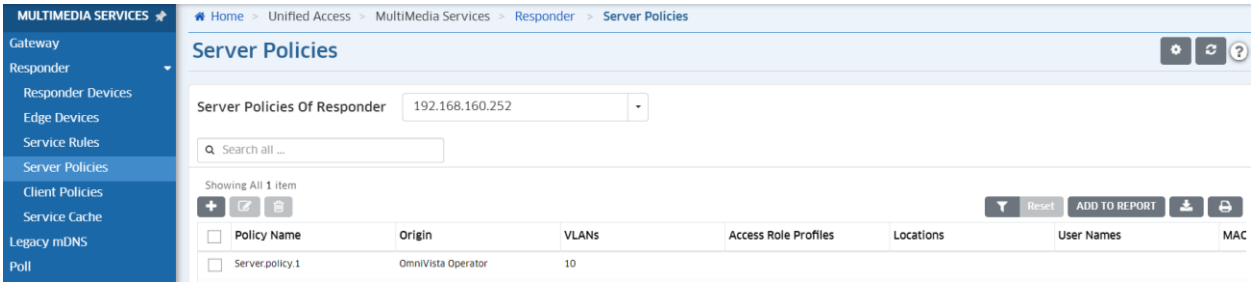


Figure 104: OmniVista Zeroconf Server policies – Omnivista 2500 (Server Policies)

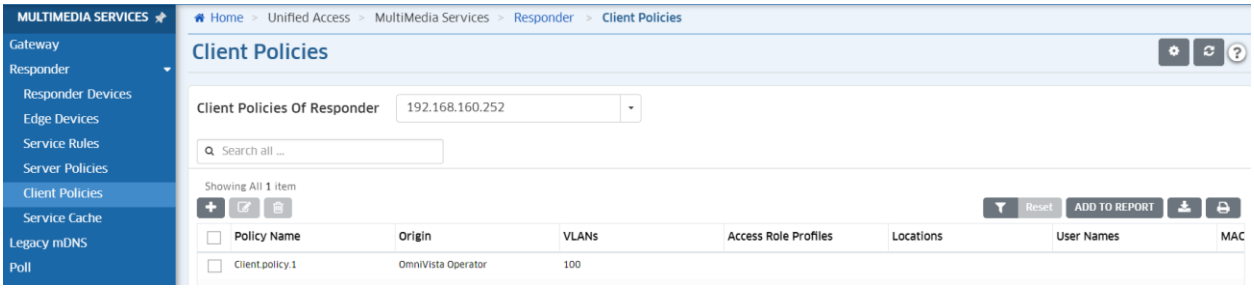


Figure 105: OmniVista Zeroconf Client policies – Omnivista 2500 (Client Policies)

3.7. IoT Servers & Advanced servers

123.	At least for a “Large deployment” scenario as described previously [4], wireless WLAN solution shall support advanced location-based services provided by Cloud services included in the solution and using Bluetooth LE wireless with dedicated Asset Tracking applications. This without of third-party component for location-based services.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*, and when combined with Omnivista Cirrus Asset Manager solution for the asset tracking & contact tracing application. High-Performance AP1201, AP1220, AP1230, AP1251 series, AP1201BG BLE gateway, High-Efficient Premium AP1311, AP1320, AP1331, AP1351, Wi-Fi 6E high-efficient AP1451, AP1411, AP1431 series and Wi-Fi 7 extremely high throughput AP1511, AP1521 are IoT-enabled APs and support Bluetooth LE radio with Omnivista 2500, enabling Stellar Asset Tracking related services for OmniAccess Stellar WLAN as Wi-Fi at the same place.

OmniAccess Stellar Asset Tracking solution uses Bluetooth Low Energy (BLE) to enable the location and tracking of assets and people, BLE is a near-field technology and provides up to 3-meter location accuracy without additional and expensive Wi-Fi overlay solution. BLE technology is a continuously evolving standard and targets sub-meter accuracy in future. The Stellar Asset Tracking & Contact Tracing solution does not interfere with WLAN infrastructure and is not limited to a proprietary technology as could be used by competitors.

Stellar Asset Tracking & Contact tracing solution architecture is based on Stellar APs as BLE gateways, OmniAccess Stellar APs uses their BLE radio to receive signals from BLE calibration and asset mobile tags to provide tags informations to the WLAN infrastructure through APs Wi-Fi/LAN interfaces. AP1201BG is single BLE gateway model for BLE deployment without WLAN, and AP1201BG WLAN can be activated via license if required.

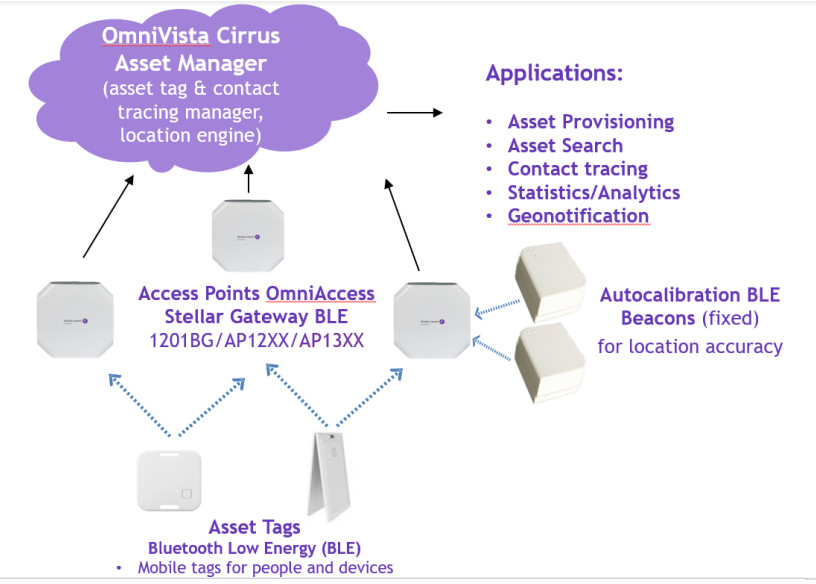


Figure 106: OV Cirrus Stellar Asset Tracking Manager

Stellar Asset Tracking profile with Stellar Asset tracking engine is created via OmniVista 2500 for APs with BLE radios. Asset Tracking profile is selected and BLE advertising/scanning enabled for APs to perform BLE iBeacon scanning for Stellar location-based services.

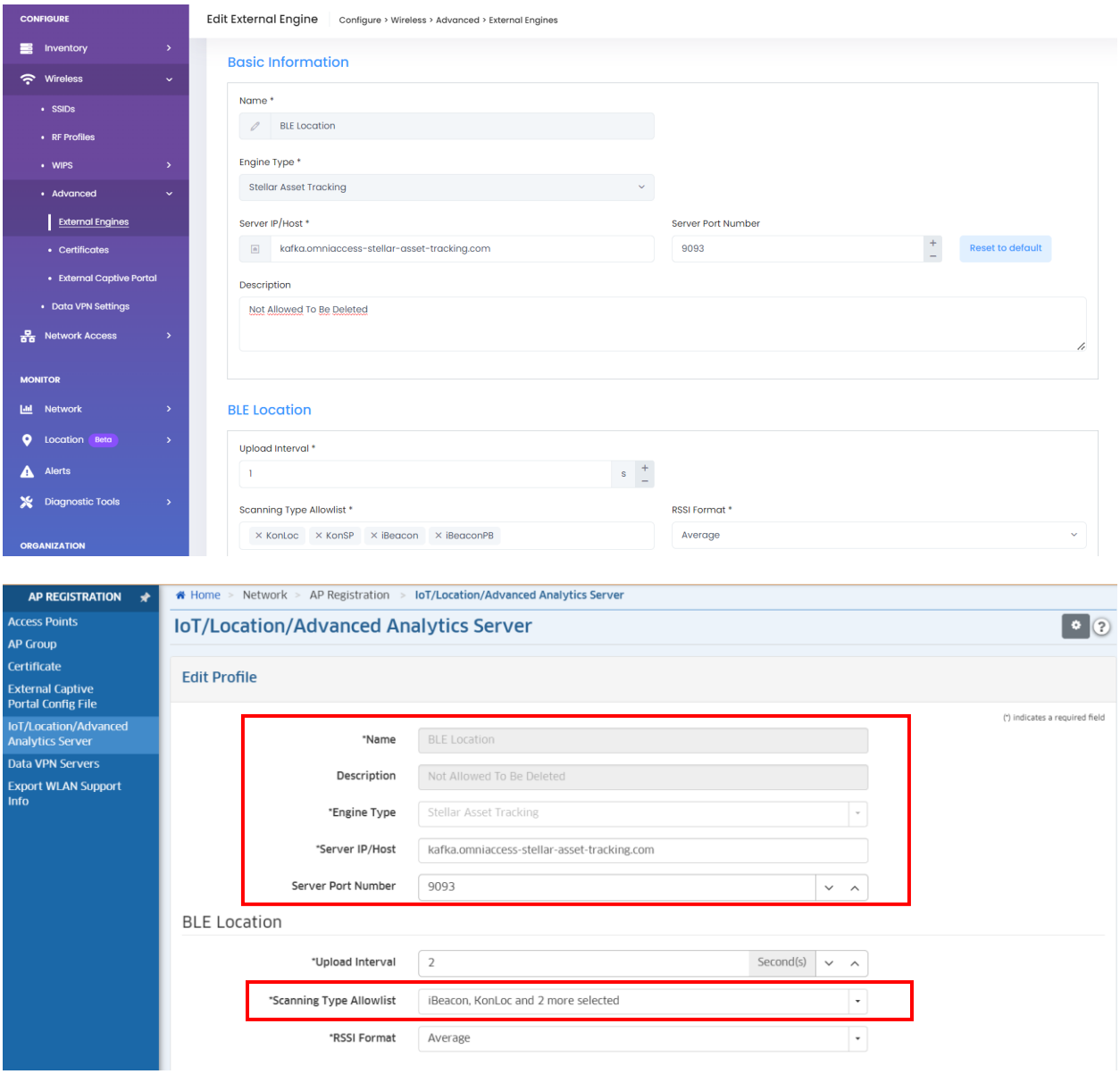


Figure 107: Stellar Asset Tracking profile – Omnivista 2500 (IoT/Location/Advanced analytics Server)

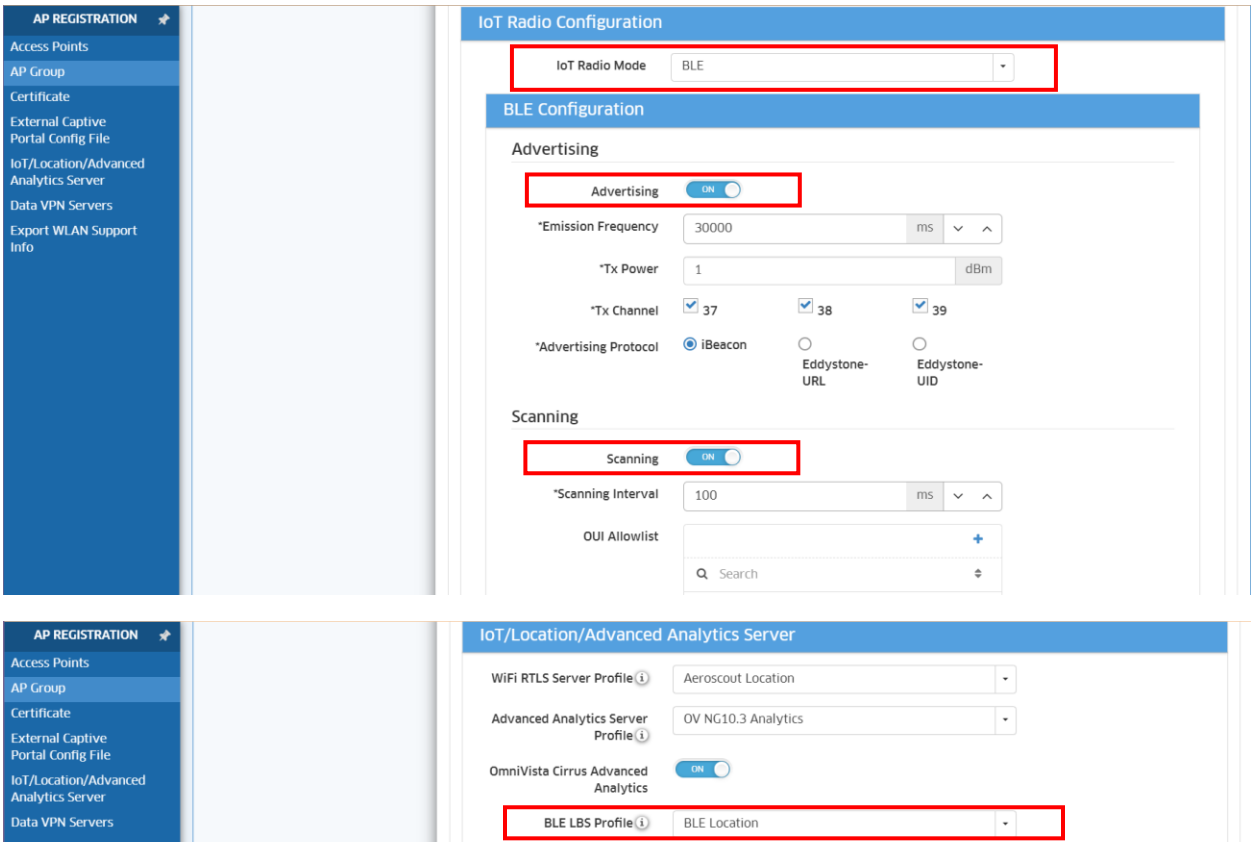


Figure 108 : BLE radio & Stellar Asset Tracking configuration – Omnivista 2500 (AP Group)

124.	At least for a "Large" scenario deployment as described previously [4], wireless WLAN solution shall support IoT devices using ZigBee access network technology, with ZigBee applications included in WLAN solution	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement on premises with Omnivista 2500 server.
High-Performance AP1201, AP1220, AP1230, AP1251, High-Efficient Premium AP1311, AP1320, AP1331, AP1351 series, high-efficient AP1451, AP1411, AP1431 and extremely high throughput AP1511, AP1521 are IoT-enabled APs and support Zigbee radio with OmniVista 2500, enabling Zigbee Control Service (ZCS) for OmniAccess Stellar WLAN as Wi-Fi at the same place.

Zigbee is a personal access network (WPAN) technology based on IEEE 802.15.4 standard. Unlike Bluetooth or wireless USB devices, ZigBee devices have the ability to form a mesh network between nodes. Meshing technique allows the short range of an individual node to be expanded and multiplied, covering a much larger area. The source information is generated by a keypad and is encrypted and is sent to destination through Zigbee modules. ZigBee receiving system decrypt/check the data and displays the data.

Stellar APs equipped with BLE/Zigbee radio plays the role of ZigBee agent for 802.15.4 devices. They are connecting to the ZigBee devices and provide ZigBee Control Service (ZCS) managed with Omnivista 2500 through Stellar WMA protocol.

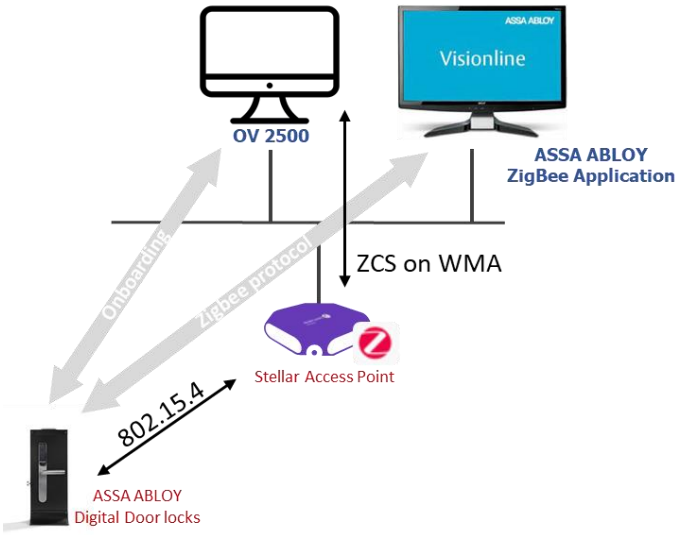


Figure 109: Stellar Zigbee agent for third-party applications

A ZigBee profile with ASSA ABLOY engine type must be created for APs in OmniVista 2500. Omnivista 2500 manages ASSA ABLOY Third-Party Zigbee application for ASSA ABLOY Guestrooms Digital Door Locks in hospitality.

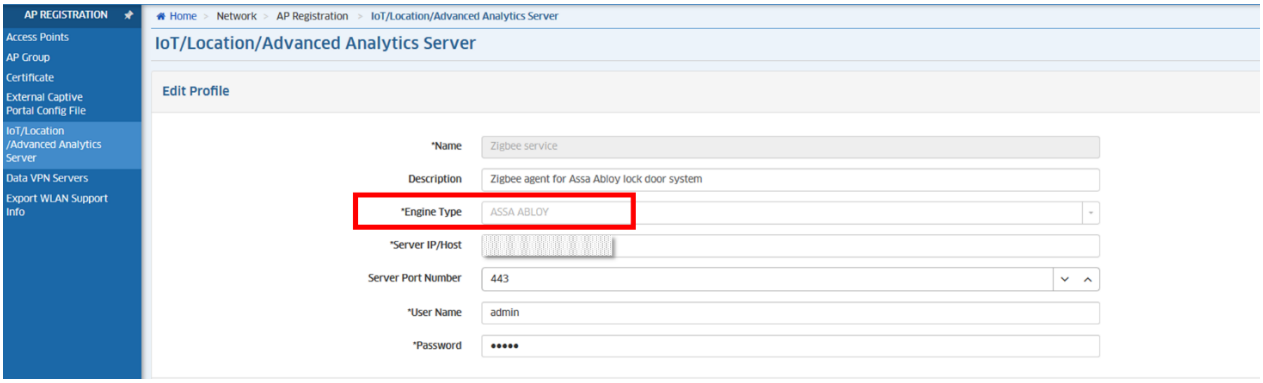


Figure 110: Zigbee agent profile – Omnivista 2500 (IoT/Location/Adv. analytics Server)

ZigBee profile must be activated and ZigBee Device Discovery enabled for the onboarding of ASSA ABLOY Guestrooms Digital Door Locks devices (vendor OUI 00:17:72) and for the management of the devices through ASSA ABLOY Digital Door Locks application.

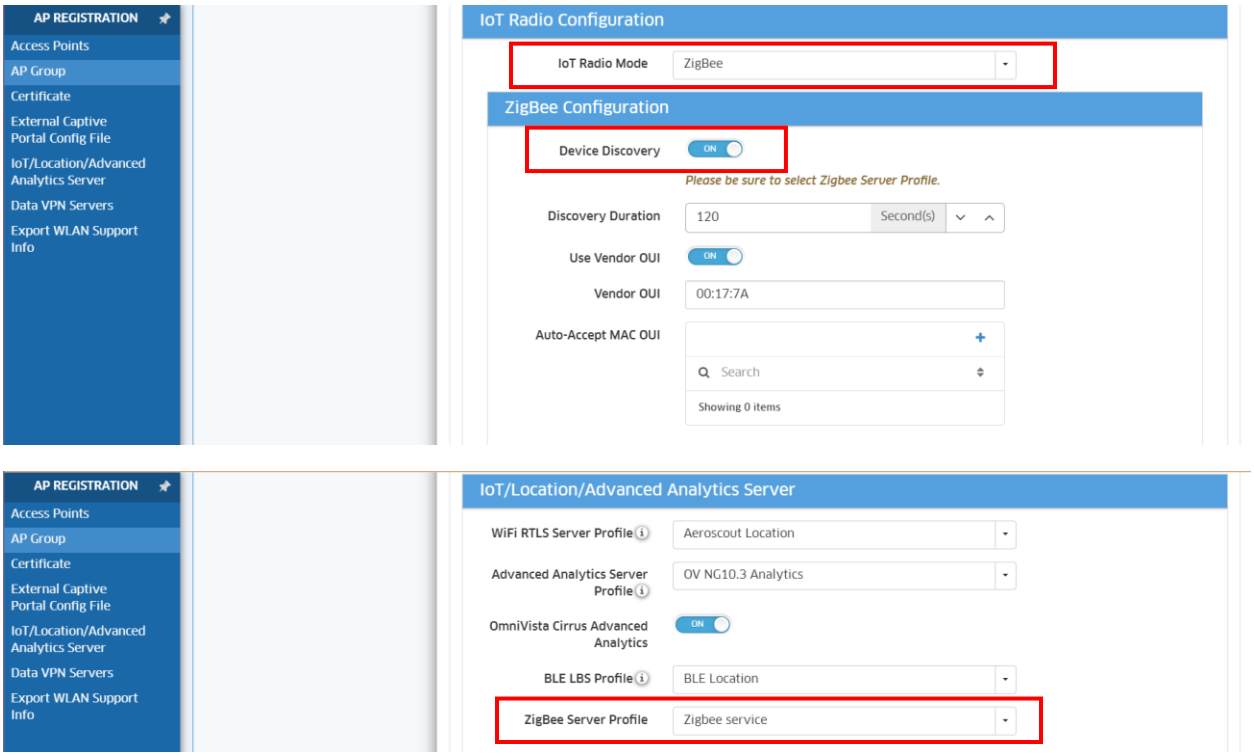


Figure 111: Zigbee radio agent & Zigbee server configuration – Omnivista 2500 (AP Group)

125.	At least for a "Large deployment" scenario as described previously [4], wireless WLAN solution shall support RTLS service provided by RTLS application if existing in the network, or by RTLS Cloud service included in the solution, using WLAN radio only for location-based service.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*.
High-Performance AP12xx, high-efficient AP13xx series (Wi-Fi 6), high-efficient AP14xx (Wi-Fi 6E) and extremely high throughput AP15xx (Wi-Fi 7) support Real-Time Location Service (RTLS) and provide data to RTLS location-based engines with WLAN radio measurements only (on the basis of received WLAN RSSIs from devices).

The OV Cirrus Wi-Fi RTLS instance offers customer the ability to manage RTLS location-based service in the Cloud on the basis of received WLAN RSSIs from APs. The Aeroscout RTLS application type offers customer the ability to manage RTLS location-based service on premises, with existing RTLS application (Ekahau engine for example) on the basis of received WLAN RSSIs from devices.

The management of RTLS service in OmniVista 2500 is identical to ones already discussed for IoT servers above [123] [124]. RTLS profile must be created in OmniVista 2500 for APs that are supporting RTLS, with Aeroscout engine or Wi-Fi RTLS engine. The RTLS profile must be applied to AP-Groups that perform RTLS reports to RTLS engine.

126.	At least for a “Large scenario deployment” as described previously [4], wireless WLAN solution shall offer IoT device secure onboarding that is as simple as possible and without requiring additional third-party components.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode*.
High-Performance AP12xx, high-efficient AP13xx series (Wi-Fi 6), high-efficient AP14xx (Wi-Fi 6E) and extremely high throughput AP15xx (Wi-Fi 7) can provide scan on IoT devices (Devices Discovery) and OmniVista 2500, as centralized management, manages the enforcement of IoT devices discovered by APs in the network, to secure the onboarding of devices.

This completes the following actions for onboarding and inventory of IoT devices in OmniVista 2500:

- Device enforcement per category and per authentication.
- Device classification can be established and different categories can be defined, with assignation to specific category and automatic enforcement to Access Role Profile (ARP).
- Manage exception list per SSID, per MAC endpoints or per AP Groups attributes (sites)

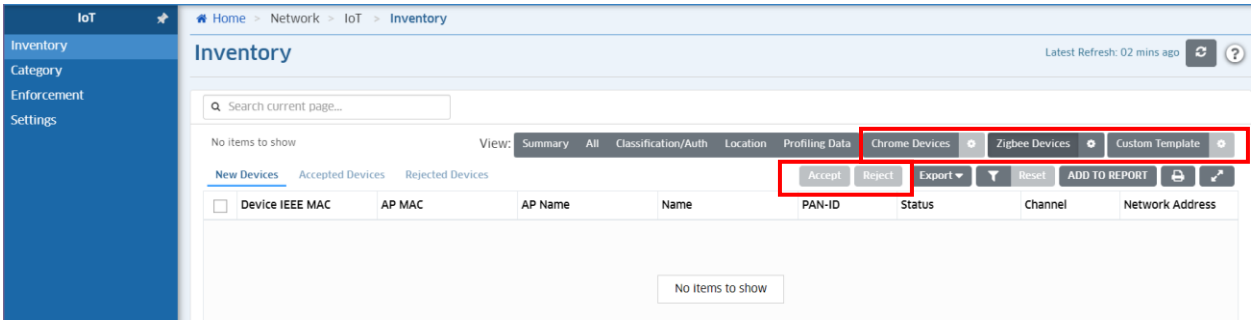


Figure 112: IoT secure Onboarding – Omnivista 2500 (IoT Inventory)

127.	At least for a “Large deployment” scenario as described previously [4], wireless WLAN solution shall support advanced analytics services provided by Cloud services included in the solution, services dedicated to statistical and analytical tasks for large deployments. This without of third-party component for analytics.	C/PC/NC

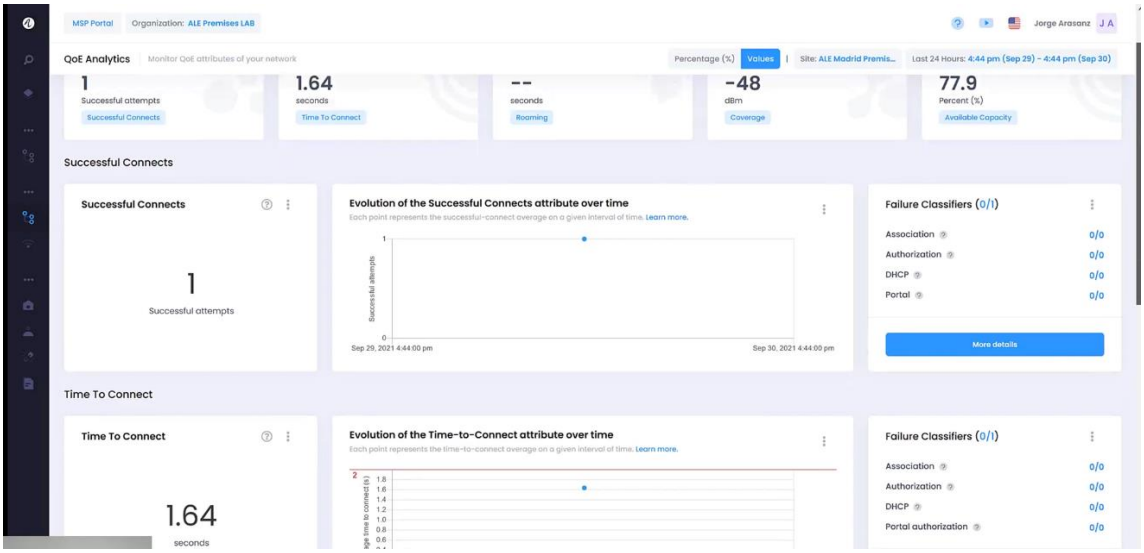
The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Enterprise mode* for large deployments, and when combined with Omnivista Cirrus 10 instance for statistical & analytical tasks.

High-Performance AP12xx (except AP1101/AP1201H), Wi-Fi 6 AP13xx series, Wi-Fi 6E AP14xx series and Wi-Fi 7 AP15xx support advanced analytics, reporting and recording and can send their data to OmniVista Cirrus 10 Cloud instance for advanced statistical and analytical services, for any large Stellar WLAN network, when managed with Omnivista 2500.

Omnivista Cirrus 10 Cloud instance offers the ability to provide and manage dashboards to customer for analytics tasks for example Quality of Experience (QoE) for the whole Stellar WLAN networks, through a single platform and in various forms of charts or graphs.

- Management of Multi-Tenants with support of Quality of Experience (QoE) on Stellar WLAN
- Dashboards to display WLAN statistics in various forms of charts or graphs

The picture below shows Time on connections (with reasons of failure) and users Mobility (roaming and coverage) QoE analytics, analytics that can be enriched with statistics on mode of connections, users connections accross SSIDs, device types or OS types, users distribution accross APs/channels or users accesses on domains/web URLs etc.



Quality of Experience (QoE) analytics with Omnivista Cirrus 10

Analytics on Stellar WLAN itself can be realized with statistics on access points, Health of access points, access points capacity and channels utilization (channels distribution/use accross the APs and throughputs accross channels or APs) etc.

Omnivista 2500 for management, combined with OV Cirrus 10 for analytics, enables elastic architecture for a deep analysis of Stellar WLAN from the Cloud. The only prerequisite for Stellar access points is to have internet access to access to OV Cirrus 10 instance.

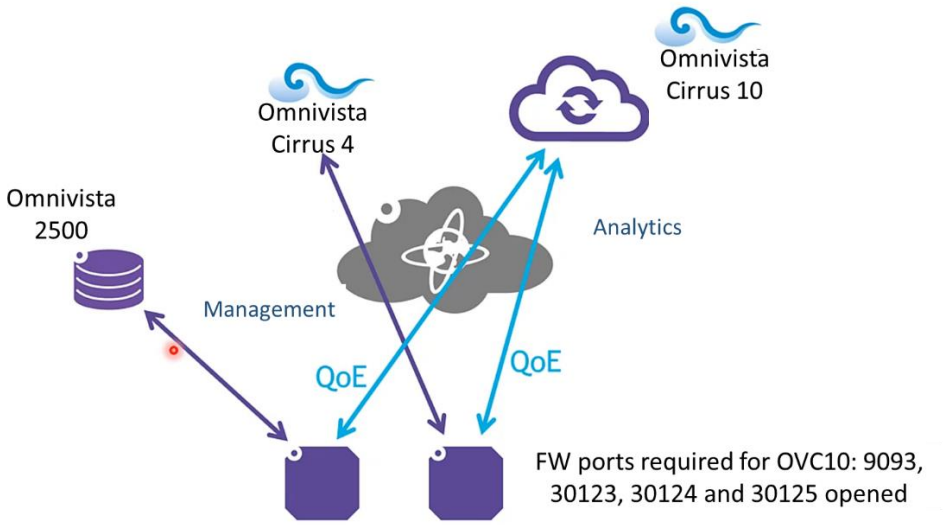
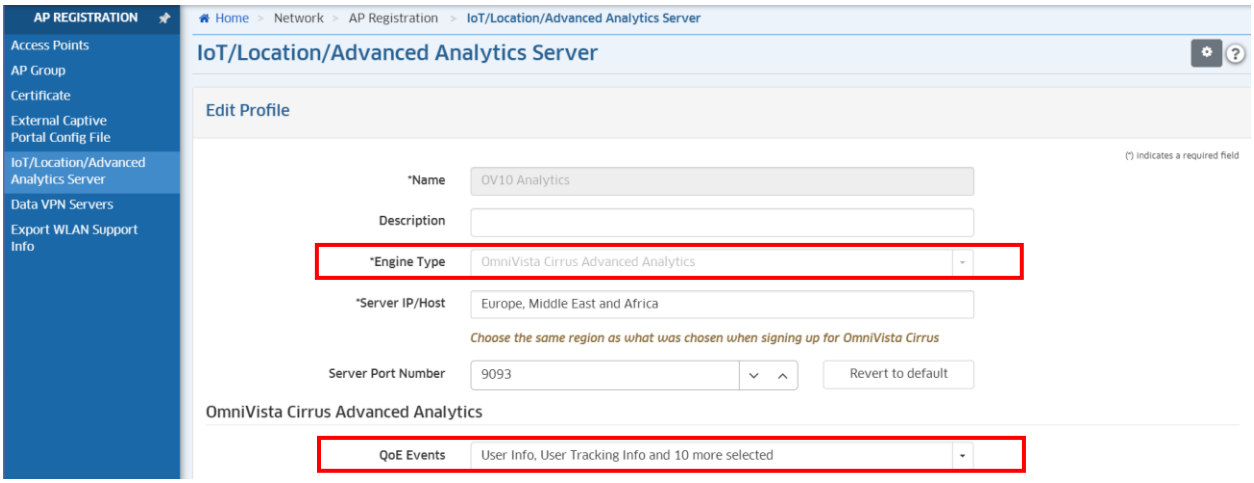


Figure 113: Omnivista Cirrus 10 connectivity in Enterprise mode

OV Cirrus 10 profile must be created in OmniVista 2500 for APs with OmniVista Cirrus Advanced Analytics engine. The default analytics profile applies only for events collection (simple-Event-Collection) to perform advanced troubleshooting on Stellar WLAN. Analytics profile must apply and analytics engine enabled to provide data to Omnivista Cirrus 10.



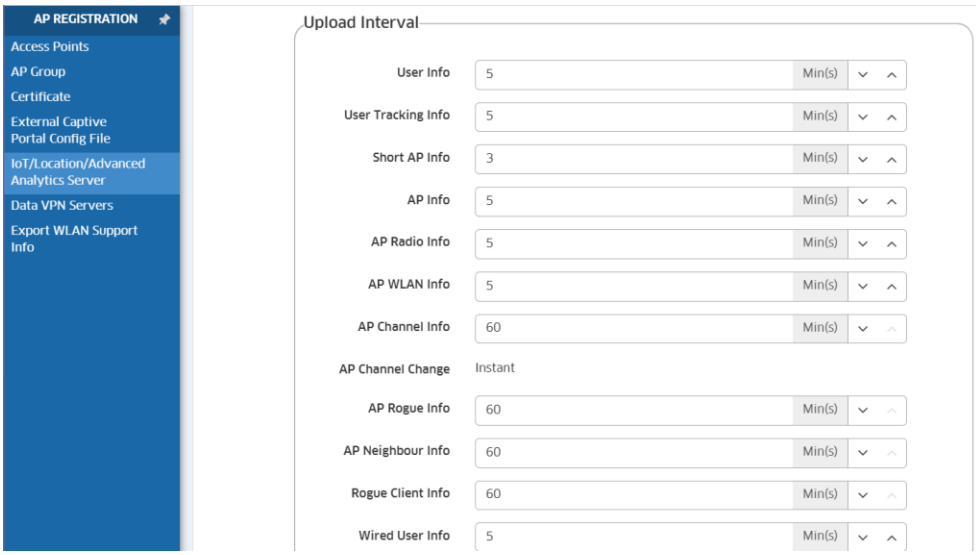


Figure 114: OV Cirrus 10 Advanced Analytics profile – Omnivista 2500 (IoT/Location/Adv. Analytics Server)

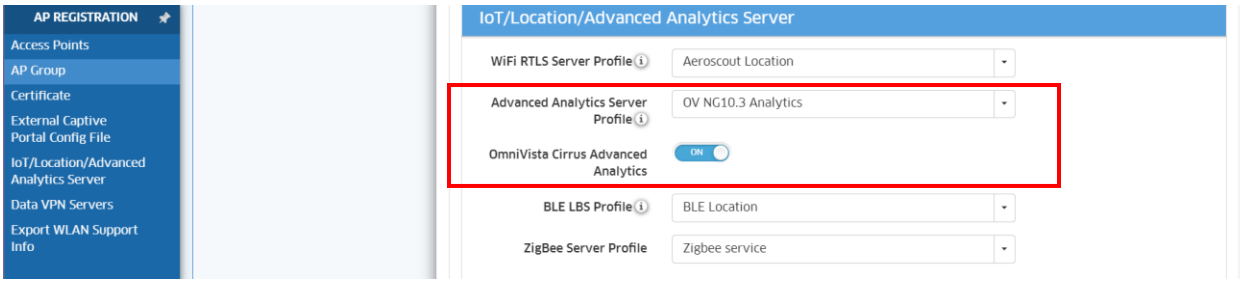


Figure 115: Advanced Analytics configuration – Omnivista 2500 (AP Group)

3.8. Omnivista 2500 specific requirements

128.	If the centralized management function requires the deployment of a dedicated application in the framework of a "Large deployment" scenario as described previously [4], this one shall be in the form of a Virtual Appliance that can be installed on top of any of following hypervisors: VMware ESXi, Microsoft HyperV and Oracle VirtualBox.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement with Omnivista 2500. Indeed, the OmniVista 2500 NMS that is part of the OmniAccess Stellar WLAN solution in *Wi-Fi Enterprise mode* is available as a Virtual Appliance (e.g., OVF file) that may be installed on top of a VMware ESXi, Oracle VirtualBox, or Microsoft HyperV hypervisor.
OmniVista 2500 virtual appliance can now also be installed on Microsoft HyperV 2022 and Linux KVM on Ubuntu 20.04 (Omnivista 2500 release 4.7).

129.	If the centralized management function requires the deployment of a dedicated application for "Large deployment" scenario as described previously [4], this one	C/PC/NC

	shall run in high avaibility mode to allow uninterrupted access to the network management, even in case of virtual appliance failure during operation.	

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement with Omnivista 2500. Indeed, the OmniVista 2500 NMS that is part of the OmniAccess Stellar WLAN solution in *Wi-Fi Enterprise mode* can operate in High-Avaibility (HA) mode and two OV2500 applications can manage an active-passive mode in the event a virtual appliance fails. This mode allows two OV2500 appliances to operate as a single NMS unit and allows uninterrupted access to the network management, with virtual appliances physically hosted in different places, in the *Stellar Wi-Fi Enterprise mode*.
Alcatel-Lucent Enterprise licensing model foresees an additional single license for High-Avaibility of OV2500.

130.	At least for a “Large deployment” scenario as described previously [4], the WLAN solution shall be able to automatically discover new APs added to the network.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500.

In *Wi-Fi Enterprise mode*, the APs contact the OmniVista 2500 server according to the Option 138 inserted in the DHCP lease they have received (please refer to requirement [15]). They can then “register”. By default, for security reasons, new APs are not automatically registered and require a "Trust" action in the registration tool. An untrusted AP will have the radios turned off. But the OmniVista 2500 NMS offers the possibility to configure “automatic registration” for new APs:

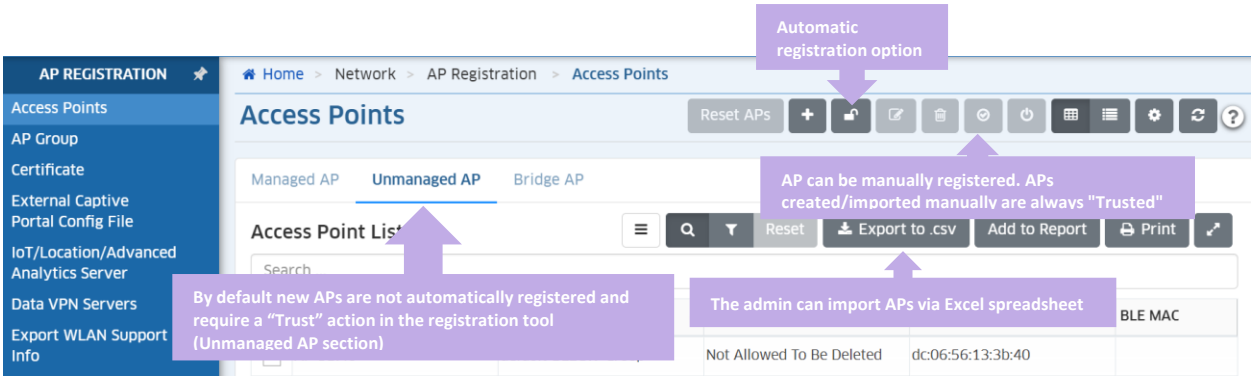


Figure 116: APs Automatic discovery – Omnivista 2500 (Access Points)

131.	At least for a “Large” scenario as described previously [4], the centralized management function shall allow to display the physical topology of the network, including wireless links between APs.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. The OmniVista 2500 NMS, as a unified management platform (wired

& wireless), automatically builds a topology of the network, displaying the wireless Access Points and the switches that connect them. The links between devices are displayed:

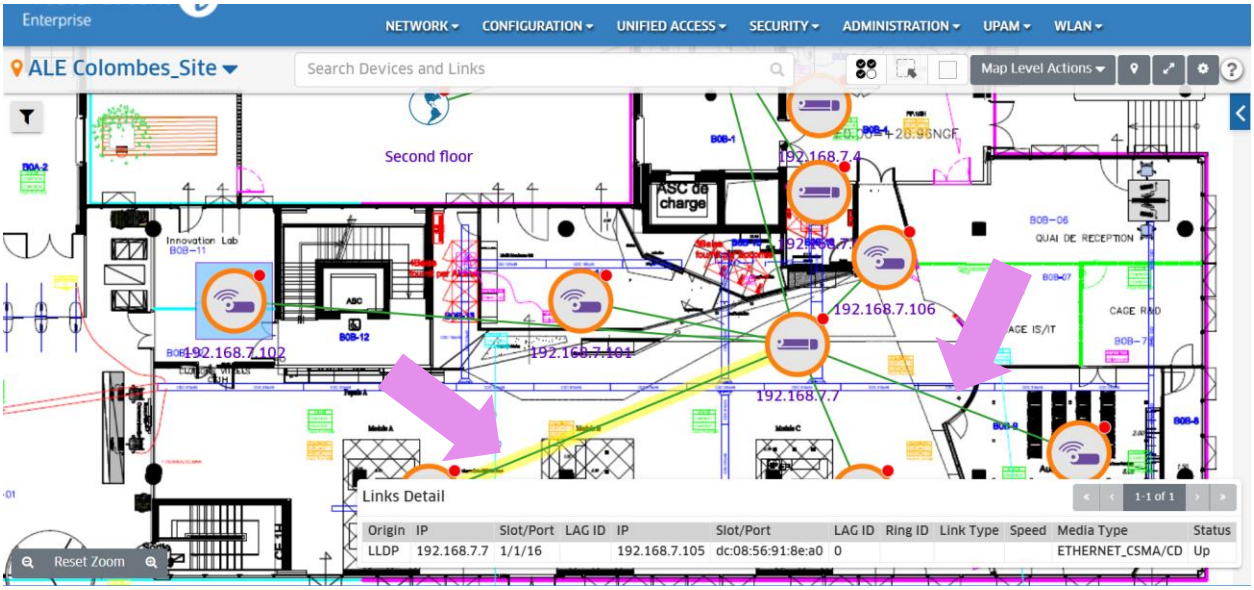


Figure 117: Network topology – Omnivista 2500 (Topology)

Mesh (or Bridge) networks can be also displayed on the Topology map. APs involved in Mesh or Bridge networks will be displayed with an additional Wi-Fi icon and a network symbol is added next to the Root AP of a Mesh network.

The network administrator can easily display only the wireless devices and clicking on a device allows the administrator to see more detailed information about any device.

132.	At least for a "Large deployment" scenario as described previously [4], the centralized management function shall allow per equipment configuration and software backup and restore, and bulk backup and restore.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500 in *Wi-Fi Enterprise mode* as depicted in following picture. Omnivista 2500 Resource Manager provides a backup method by device, maps or AP groups. As well as a bulk upgrade method that can be scheduled to handle site-specific outage periods.

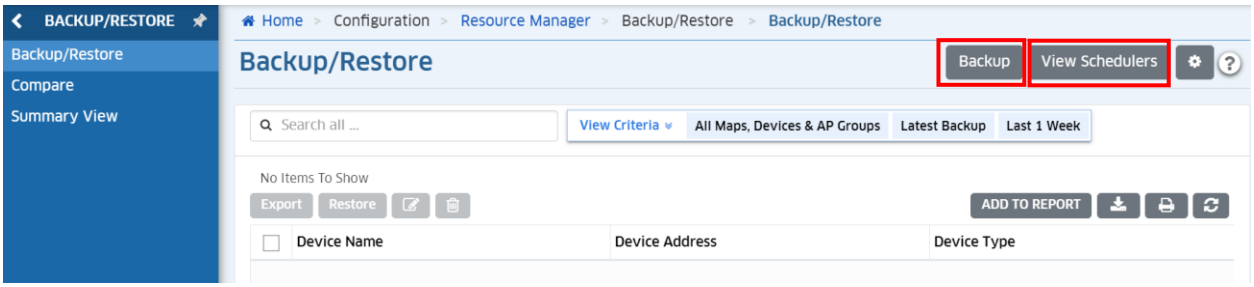


Figure 118: Resource Manager – Omnivista 2500 (Backup/Restore)

133.	At least for a "Large deployment" scenario as described previously [4], the centralized management function shall allow to display the Wi-Fi coverage quality within a given area ("Heatmap").	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, the OmniVista 2500 NMS allow to use the "***Heat Map***" application which is a design, verification, troubleshooting tool for installed Stellar Wi-Fi networks. The application provides a way to create and organize Heat Maps from multiple locations, from Campus level to Building level and Floor level to give a comprehensive view of Wi-Fi coverage:

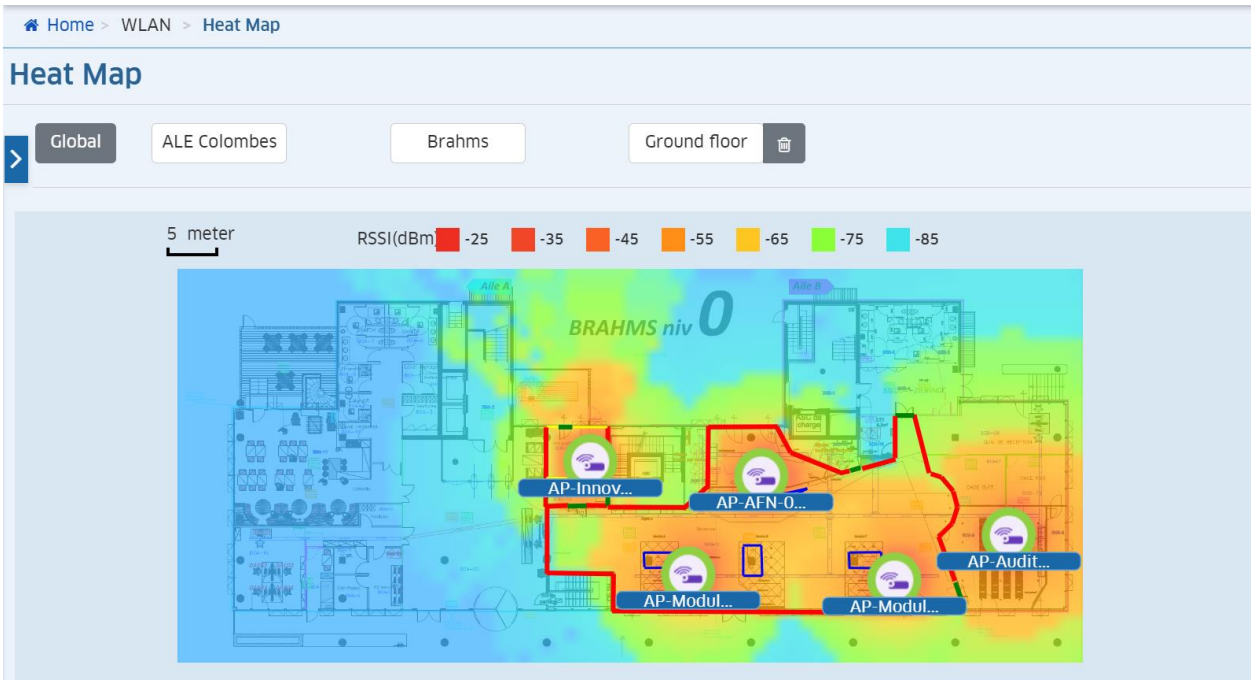


Figure 119: WLAN Heat Map – Omnivista 2500 (Heat Map)

After creating a Heat Map, the map displays the Wi-Fi coverage quality. Wi-Fi coverage areas are displayed by color depending on the quality of the coverage.

134.	At least for a "Large deployment" scenario as described previously [4], the centralized management function shall allow, before deployment, to determine optimal placement of Access Points (APs) in a location (RF Planning).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista 2500. Indeed, the OmniVista 2500 NMS allow to use the "***Floor Plan***" application which is a design, verification, troubleshooting tool for Stellar Wi-Fi networks. Floor Plan can be used to determine optimal placement of APs in a location. The application can also automatically determine AP placement and configurations for optimal set-up.
The application enables to create a floor plan for a location and manually place Stellar APs on the floor plan to view the effective Wi-Fi coverage within the floor plan. An expected coverage area on the floor plan can also be set up and the application will automatically identify the optimal number and location of APs within the floor plan to use as a guide when installing APs on site.

4. Omnivista Cirrus 4 requirements

4.1. Access Control, Authentication and Encryption

135.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support MAC based authentication provided by a NMS cloud solution included in WLAN solution, for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. MAC-based authentication is fully supported when Stellar WLAN solution is managed by Omnivista NMS, and is further described in [26] for Omnivista 2500 NMS server.

136.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support 802.1x based authentication provided by a NMS cloud solution included in WLAN solution, for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. 802.1x based authentication is fully supported when Stellar WLAN solution is managed by Omnivista NMS, and is further described in [27] for Omnivista 2500 NMS server.

137.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication, provided by a NMS cloud solution included in WLAN solution, for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments by offering an embedded Radius server in *Wi-Fi Enterprise mode* for 802.1x and MAC authentication. *Unified Policy Access Manager* (UPAM) is fully supported when Stellar WLAN solution is managed by Omnivista NMS, and is essentially described in [28] for Omnivista 2500 NMS server.

138.	At least for a "Cloud scenario" as described previously [4], built-in RADIUS server as described [28] shall be able to interface with an external authentication server (Radius, LDAP, Active Directory, Microsoft Azure AD): FreeRadius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP etc. when managed by a NMS cloud solution included in WLAN solution, for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments by offering connection to external authentication sources. This feature is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [29] for Omnivista 2500 NMS server.

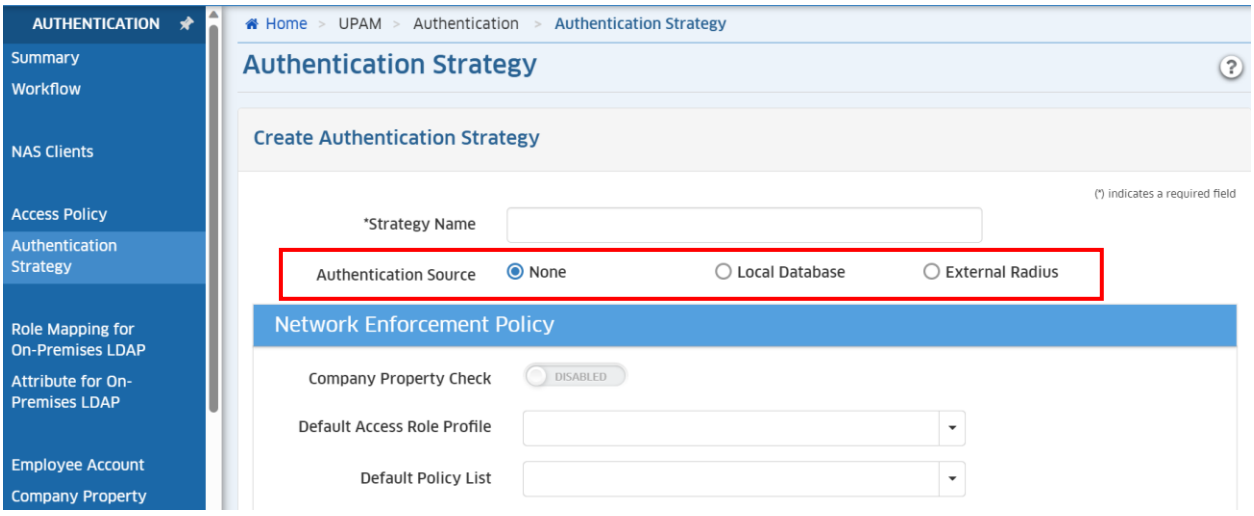


Figure 120: UPAM-NAC Access Policies – Omnivista Cirrus 4 (Authentication strategy)

139.	At least for a "Cloud scenario" as described previously [4], built-in RADIUS server as described previously [28] shall support following EAP types: EAP-MD5, EAP-	C/PC/NC

	TLS, EAP-AKA, EAP-PEAP, EAP-FAST, EAP-SIM, EAP-TTLS, EAP-GTC. when managed by a NMS cloud solution included in WLAN solution, for multi-tenant site deployments. This does not require a third-party component for NMS management.	

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Various EAP types are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution.

140.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall have the ability to utilize RADIUS attributes to assign each authenticated user/device to a specific ROLE. A role defines a VLAN and enforces security and QoS through the use of role-based ACLs and QoS policies that can be directly integrated with the roles defined within existing authentication servers. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. User role assignment from RADIUS attributes is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [31] for Omnivista 2500 NMS server.

141.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall include and handle a flexible and adaptive RADIUS attributes dictionary allowing to add an IETF or any vendor specific RADIUS attribute, when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. As depicted in following figure, the UPAM embedded RADIUS server available in *Wi-Fi Enterprise mode* with Omnivista Cirrus 4 can store multiple RADIUS attributes defined by the IETF, by *Alcatel-Lucent Enterprise*, or by any other vendor:

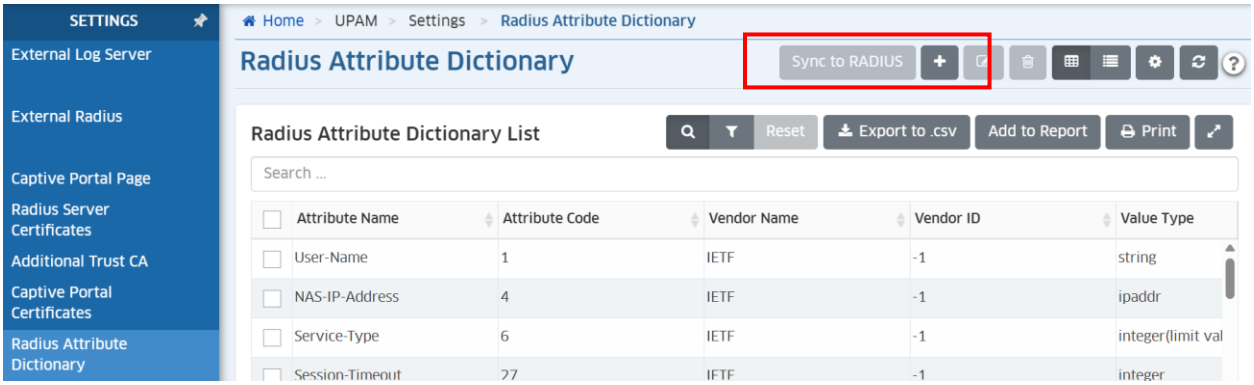


Figure 121: UPAM-NAC- Access Policies – Omnivista Cirrus 4 (RADIUS Attributes Dictionary)

The RADIUS Attribute Dictionary enables UPAM to integrate with other vendor's network infrastructure and allows UPAM to act as a RADIUS server to authenticate user requests from Third-Party devices.

142.	If the built-in RADIUS server as described [28] shall interface with an external RADIUS server, then it shall be able to interface with multiple and distinct RADIUS servers depending on specific access conditions (SSID name, Access Point IP address, identity of the connecting user…). This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Interface with multiple external RADIUS is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [33] for Omnivista 2500 NMS server.

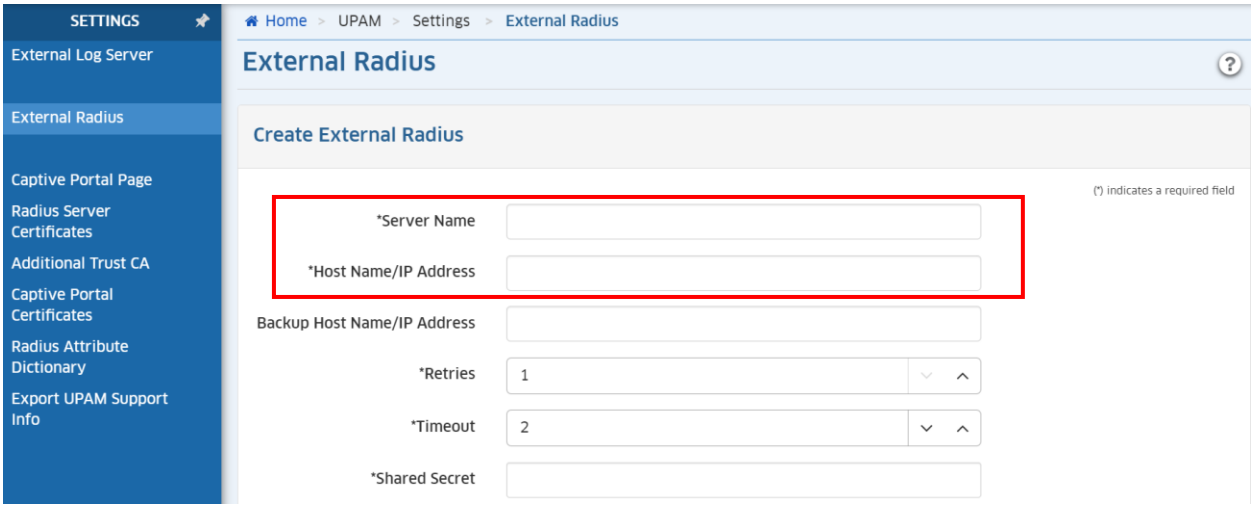


Figure 122: UPAM-NAC External RADIUS server – Omnivista Cirrus 4 (Create external RADIUS server)

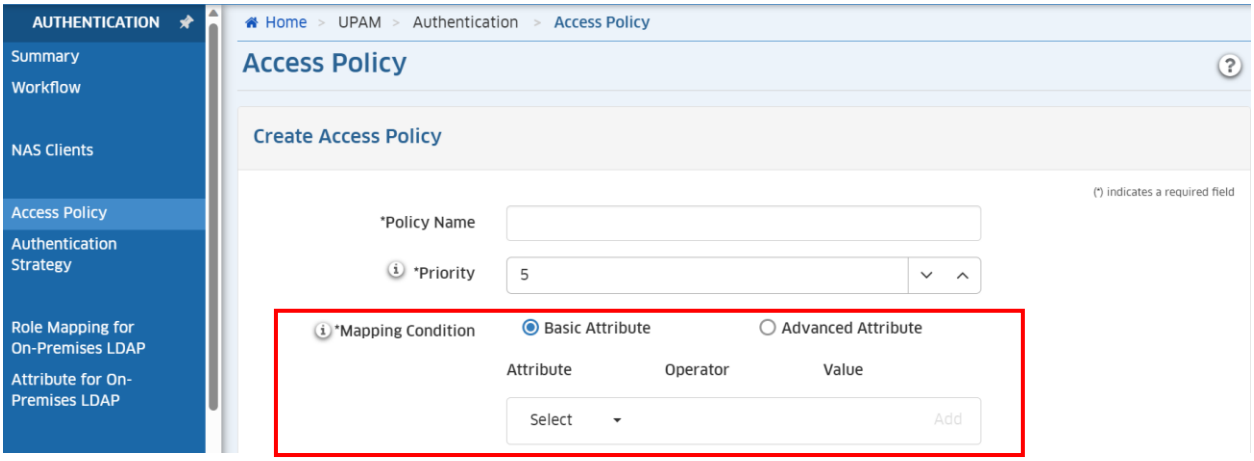


Figure 123: UPAM-NAC-Access Policy and mapping condition - Omnivista Cirrus 4 (Access Policy)

143.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support following link layer encryption standards: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP, WPA3_PSK_SAE_AES, WPA3_SAE_AES, OWE_PMF. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments, and this without third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

144.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support the latest WPA3 encryption standard. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. WPA3 encryption is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [35] for Omnivista 2500 NMS server.

145.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support OWE encryption standard with open Wi-Fi networks. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. Wi-Fi Enhanced Open security standard based on Opportunistic Wireless Encryption (OWE) is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [36] for Omnivista 2500 NMS server.

146.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support following 802.1x supplicants: Windows 7, 10 (and more), MAC OS, IOS, Android, Chromebook…. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

147.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support time-based policy access to a SSID when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Time-based policy access to a SSID is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution.

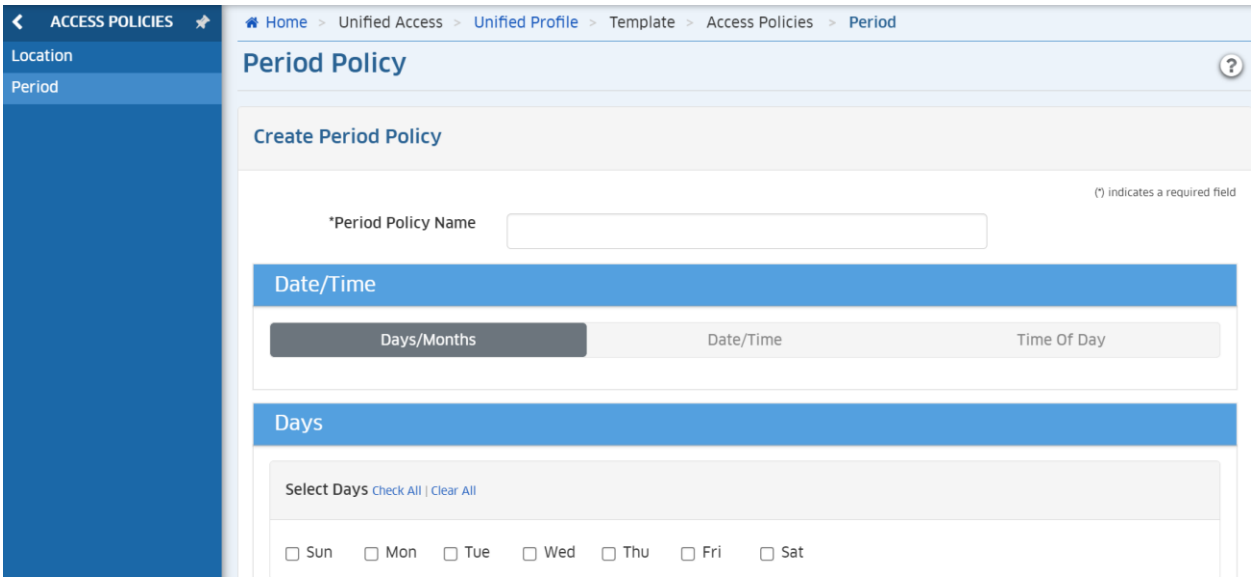


Figure 124: SSID time-based policy access - Omnivista Cirrus 4 (Period Policies)

148.	For the “Cloud” deployment model as described previously [4], the wireless LAN solution shall propose a “Guest” management solution based on an embedded and built-in Captive Portal providing web-based authentication for guests and visitors. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. Guest management is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [39] for Omnivista 2500 NMS server.
Descriptions [149] to [164] depict the Guest access management with Omnivista Cirrus 4.

149.	The Guests Captive Portal included in the wireless LAN solution shall allow a customizable look & feel.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. The Captive Portal provided by UPAM in Wi-Fi *Enterprise mode* is fully customizable.

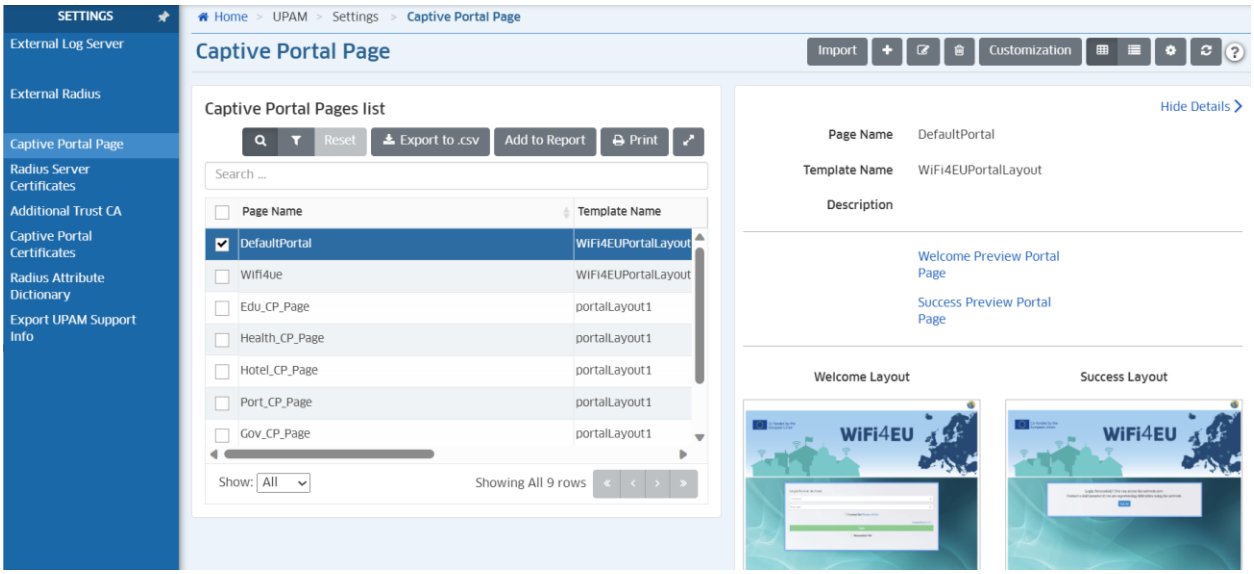


Figure 125: UPAM-NAC Captive Portal customization – Omnivista Cirrus 4 (Captive Portal Page)

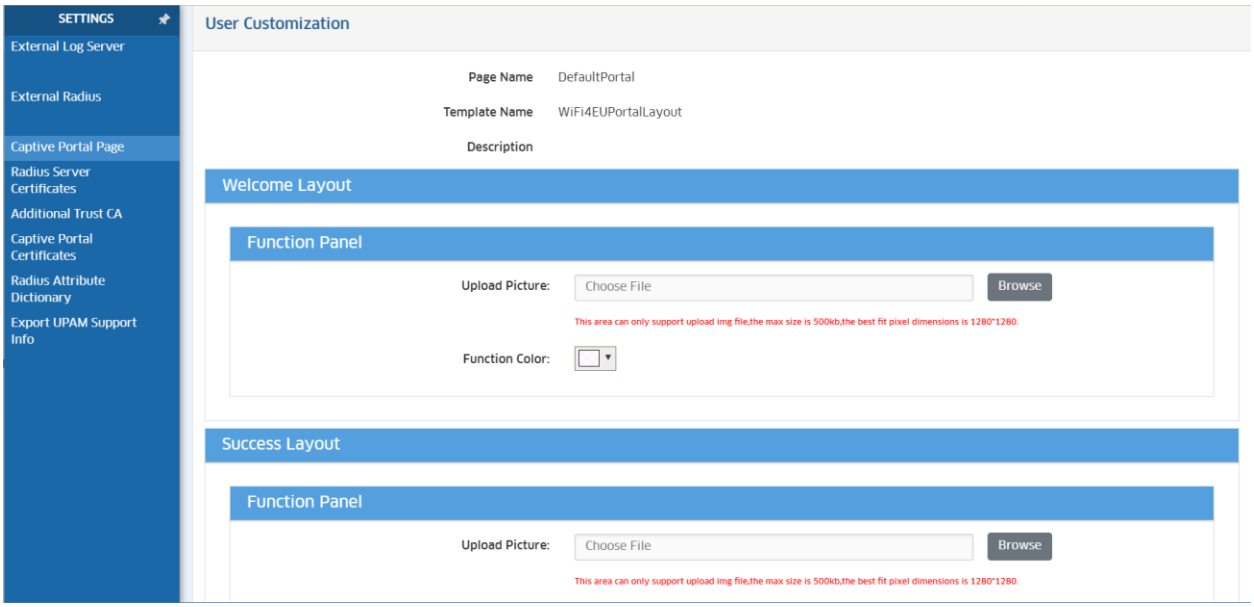


Figure 126: UPAM-NAC "success page" customization – Omnivista Cirrus 4 (Captive Portal Page)

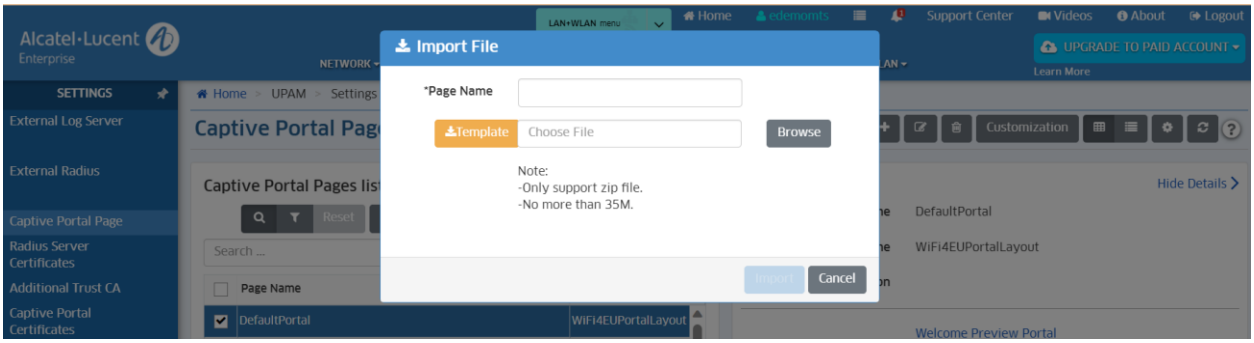


Figure 127: UPAM-NAC Captive Portal full customization – Omnivista Cirrus 4 (Captive Portal page)

150.	The Guest management solution shall allow, at least, following authentication methods: ▪ Username & Password ▪ Access Code ▪ Simple Term & Condition acceptance	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

151.	A least for a "Cloud" scenario as described previously [4], the Guest management solution shall allow guests to authenticate using their favorite social network account (supported social networks shall be listed).	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. A short description is done in [42] for Omnivista 2500 NMS server.

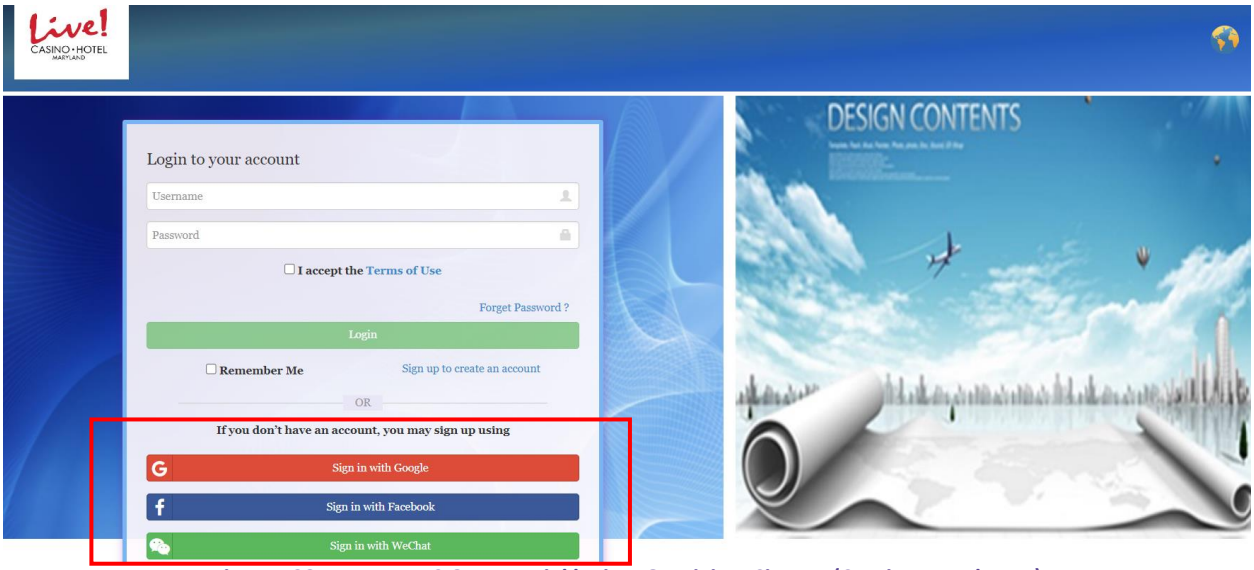


Figure 128: UPAM-NAC Guest social login – Omnivista Cirrus 4 (Captive Portal page)

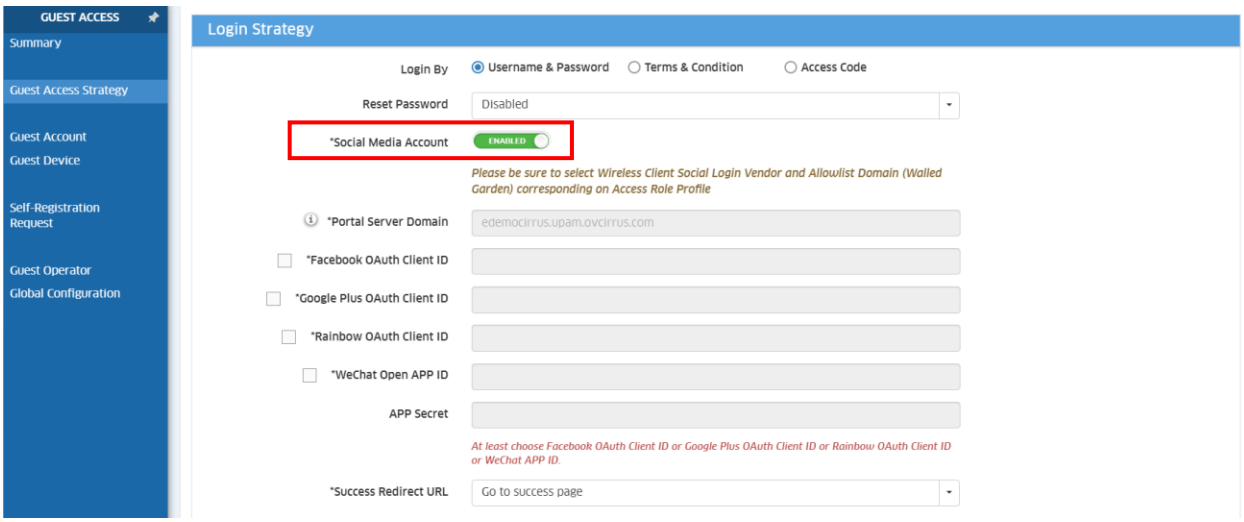


Figure 129: UPAM-NAC Guests Social Login method – Omnivista Cirrus 4 (Guest Access Strategy)

152.	For the "Cloud" deployment model as described previously [4], the wireless LAN solution shall offer the possibility to build a walled garden environment (with configured domain names) for guest users before they authenticate.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

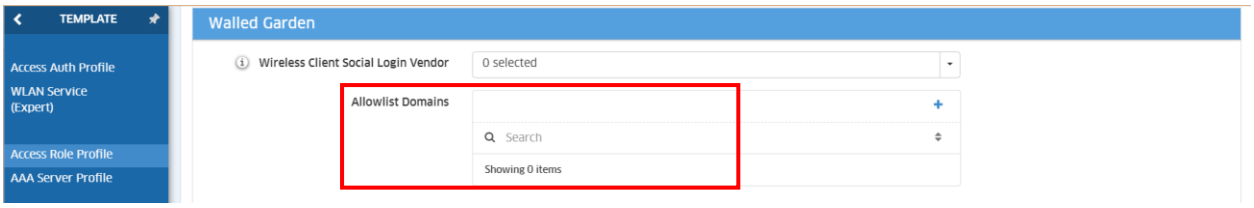


Figure 130: Walled Garden – Omnivista Cirrus 4 (Access Role Profile)

153.	The Guest management solution shall allow non-IT staff (e.g., a receptionist) to create temporary guest accounts.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

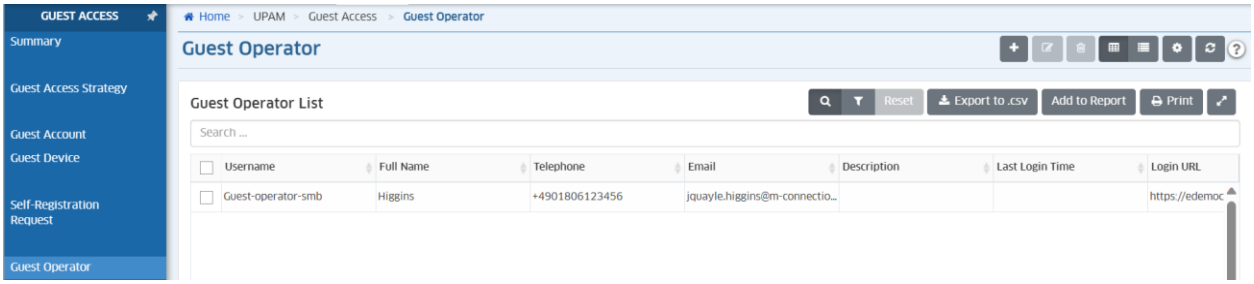


Figure 131: Guests Operator accounts creation – Omnivista Cirrus 4 (Guest Operator)

154.	A least for a "Cloud" scenario as described previously [4], the WLAN solution shall allow guest self-registration and employee sponsored access.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. A short description is done in [45] for Omnivista 2500 NMS server.

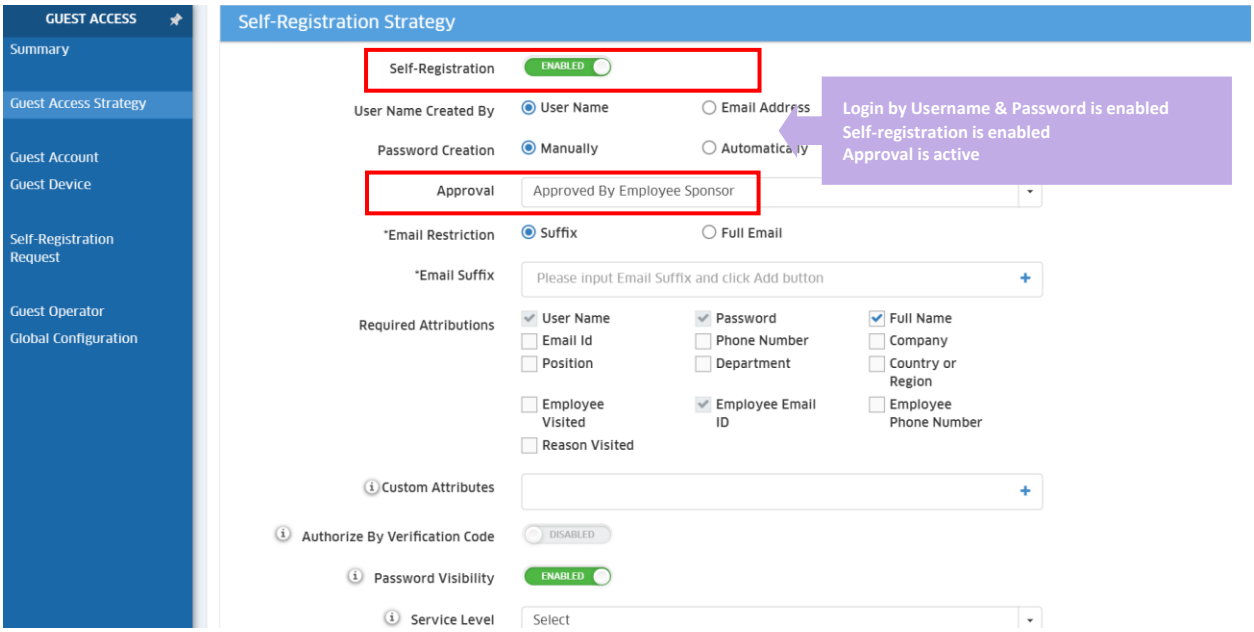


Figure 132: Guest self-registration – Omnivista Cirrus 4 (Guest Access Strategy)

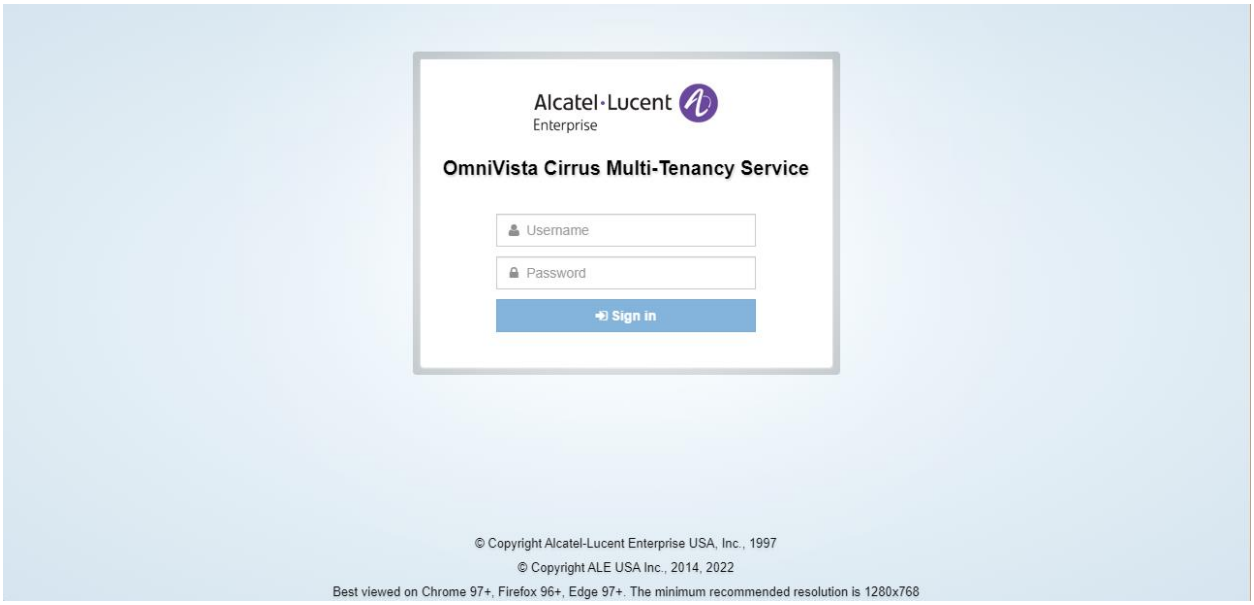


Figure 133: Guest Operator & Employee Sponsor UI – Omnivista Cirrus 4

155.	The WLAN solution shall allow guests accounts bulk provisioning by importing a file containing guest accounts information and shall propose a template import file.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

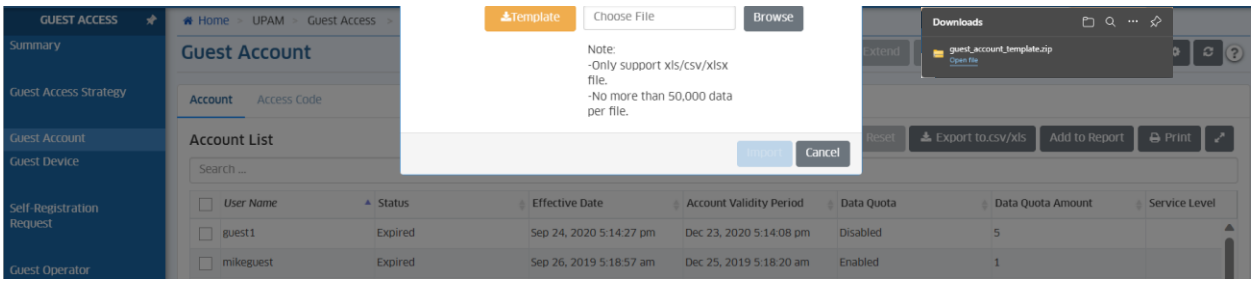


Figure 134: Guests accounts bulk import - Omnivista Cirrus 4 (Guest Account)

156.	A least for a "Cloud" scenario as described previously [4], the WLAN solution shall allow to create batch of guests accounts just by specifying a guest prefix and a number of accounts to be created.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

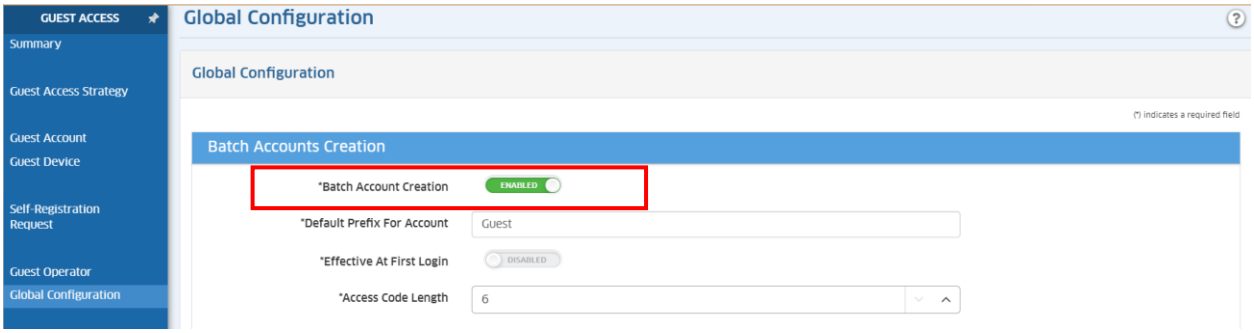


Figure 135: Guest accounts batch creation – Omnivista Cirrus 4 (Global Configuration)

157.	A least for a "Cloud" scenario as described previously [4], the WLAN solution shall allow to define networking SLAs (security, QoS…) to be applied to guest network connections.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

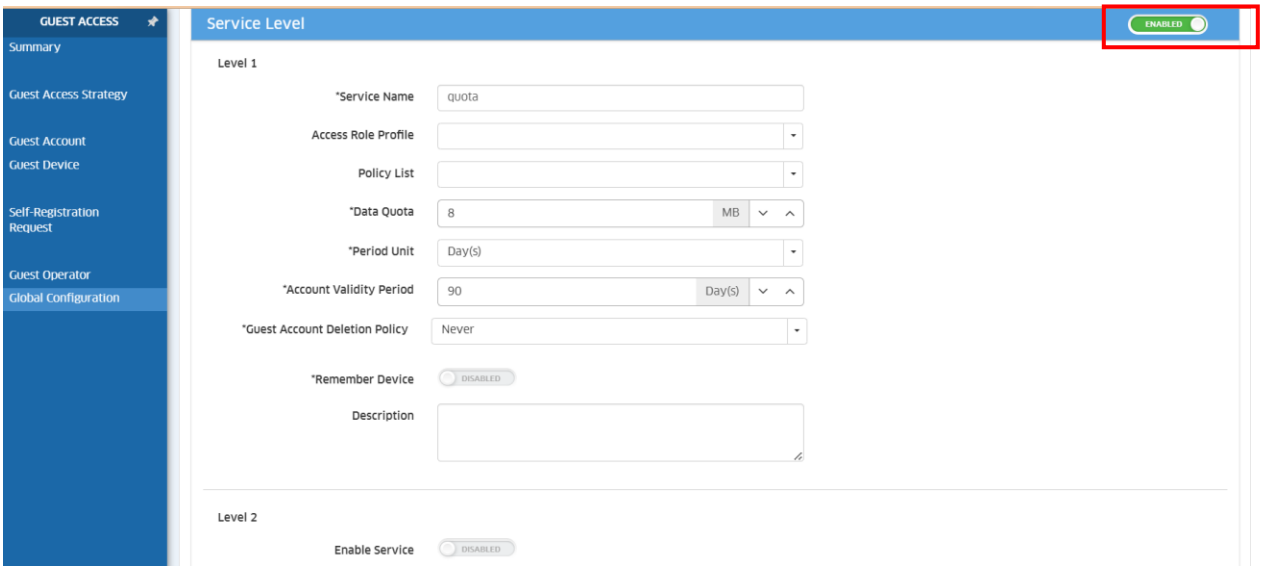


Figure 136: Service Levels - Omnivista Cirrus 4 (Global Configuration)

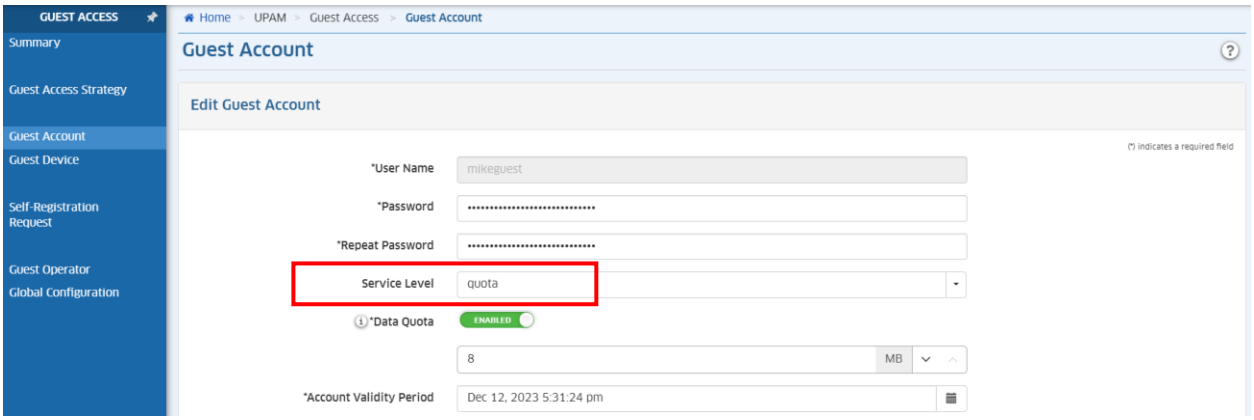


Figure 137: Service Level and Guest account - Omnivista Cirrus 4 (Guest Account)

158.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow to define and apply “data quotas” to guests to limit access based on total traffic consumed.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

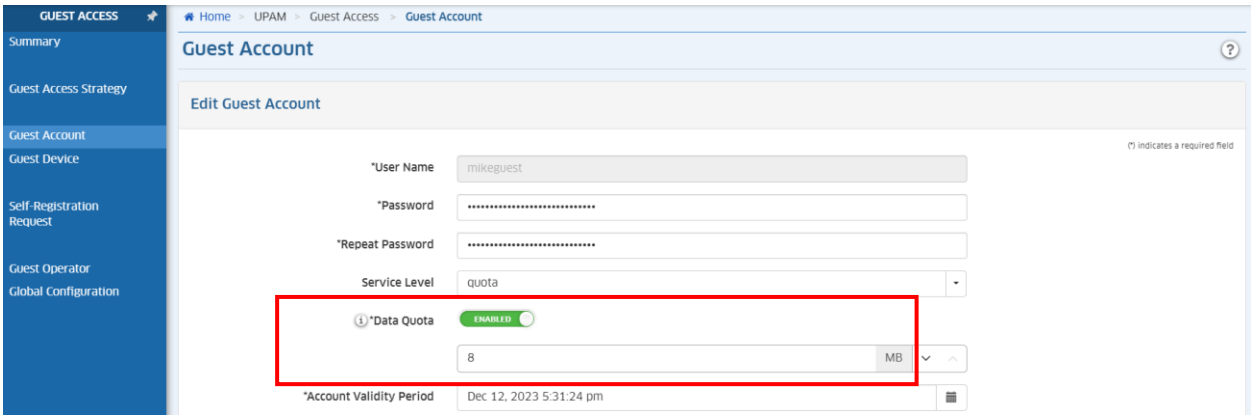


Figure 138: Guest data quota – Omnivista Cirrus 4 (Guest Account)

159.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow guests SMS notification.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

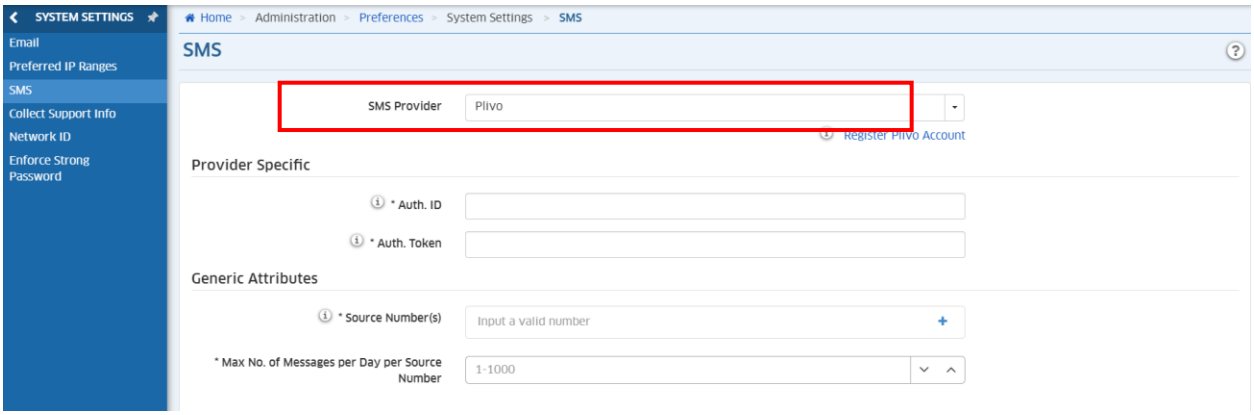


Figure 139: SMS gateway – Omnivista Cirrus 4 (System Settings)

160.	For the "Cloud" deployment model as described previously [4], the wireless LAN solution shall offer the possibility to interface with a third-party external Captive Portal for guest authentication, without necessarily forcing the traffic to through any server or appliance.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. Interface with a 3th-party external Captive Portal is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [51] for Omnivista 2500 NMS server.

161.	For a “Cloud deployment” scenario as described previously [4], the licensing model of the Guest management solution shall be based on the number of devices.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

162.	For a “Cloud deployment” scenario as described previously [4], the Guest management solution shall allow setting a validity period for an authenticated device, in order to avoid entering credentials each time a guest access the network.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

163.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall implement strict Guests traffic isolation.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*. Strict Guest traffic isolation is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [54] for Omnivista 2500 NMS server.

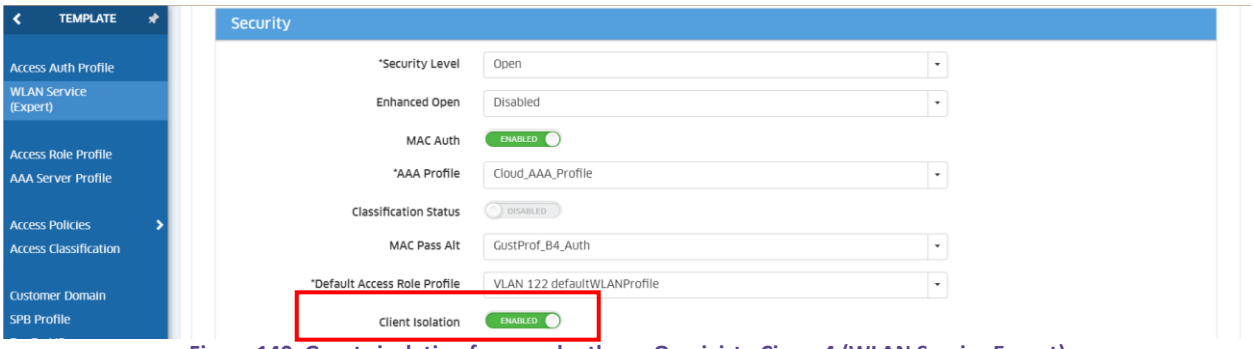


Figure 140: Guests isolation from each other – Omnivista Cirrus 4 (WLAN Service Expert)

164.	The WLAN solution shall allow data retention on user sessions when providing Guest Wi-Fi.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Wi-Fi Enterprise mode*.

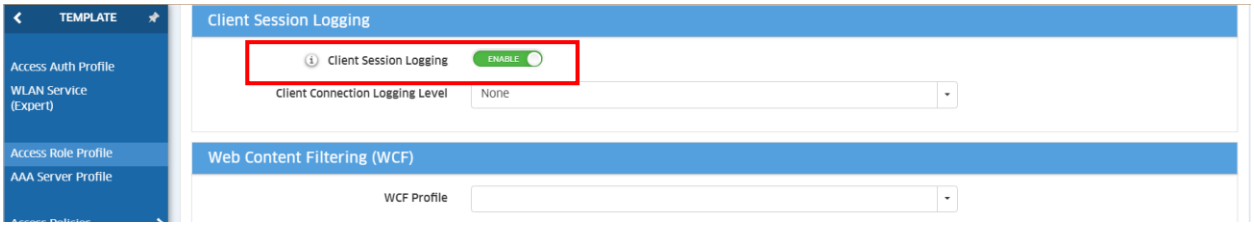


Figure 141: Client Behavior Tracking – Omnivista Cirrus 4 (Access Role Profile)

165.	In the framework of a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support BYOD and be able to provide device on-boarding that is as simple as possible. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. BYOD application included in UPAM module is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [56] for Omnivista 2500 NMS server.

166.	At least for a "Cloud deployment" scenario as described previously [4], the on-boarding process of employee devices shall be based on employee corporate accounts. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. The feature is included in BYOD application and is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution. A description is done in [57] for Omnivista 2500 NMS server.

167.	The BYOD application shall allow setting the validity period for the device, and the maximum number of devices per account. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments.

168.	The licensing model of the BYOD application shall be based on the number of on-boarded devices.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments.

169.	The WLAN solution shall support DSPSK to allow the use of different Pre-Shared Keys (PSK) for WPA2 encryption standard in the same SSID at the same time. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. DSPSK (Device-Specific PSK) is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [60] for Omnivista 2500 NMS server.

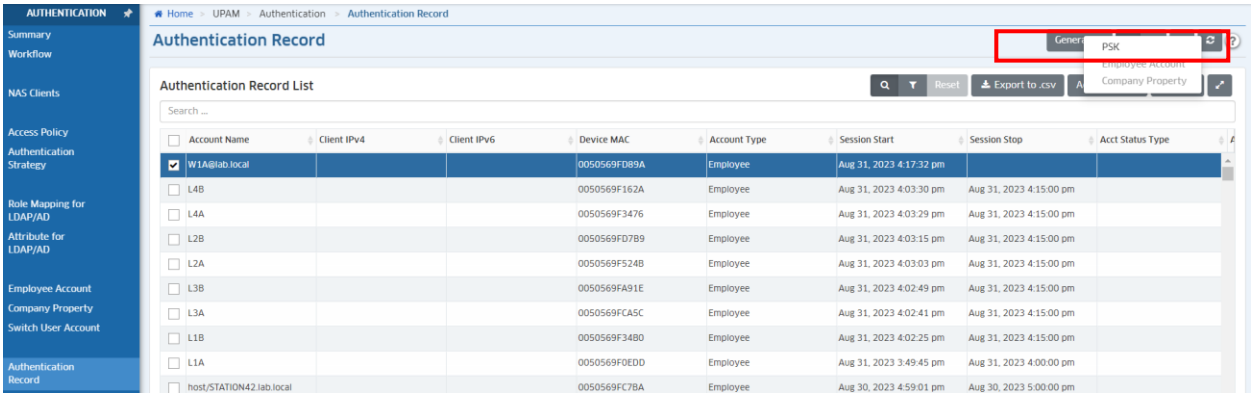


Figure 142: UPAM-NAC DSPSK generation with device MAC – Omnivista Cirrus 4 (Authentication Record)

170.	A least for a "Large" scenario as described previously [4], the WLAN solution shall support the WIFI4EU initiative from the EU. That includes support for Hotspot 2.0 (Passpoint® release 3Wi-Fi Alliance certification program)	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. WIFI4EU is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution. A description is done in [61] for Omnivista 2500 NMS server.

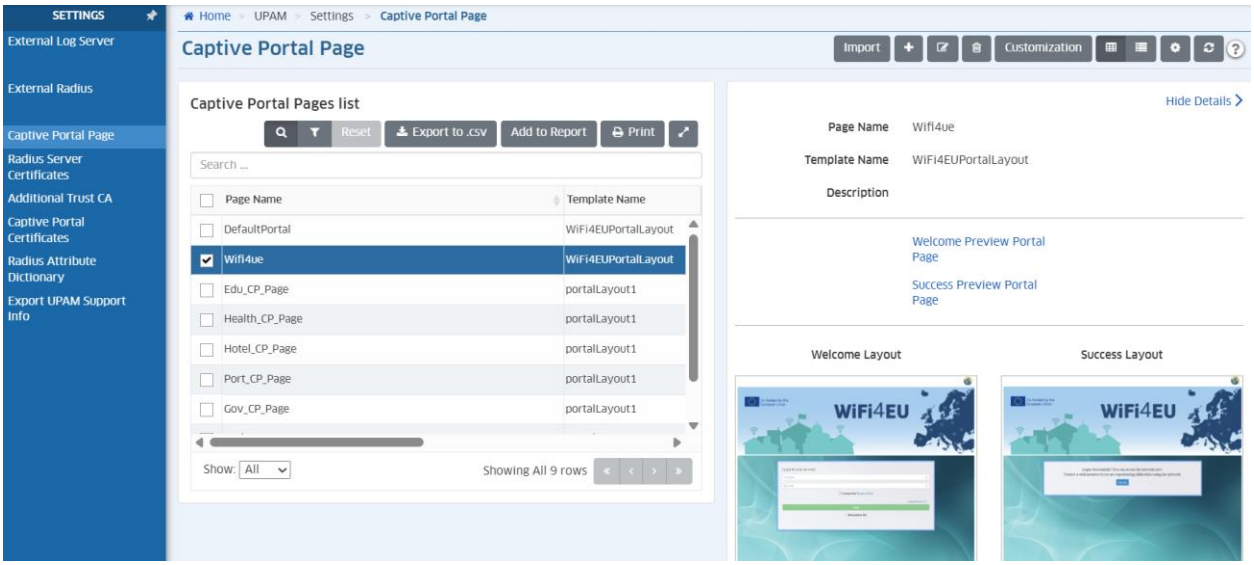


Figure 143: UPAM-NAC WIFI4EU Captive Portal template – Omnivista Cirrus 4 (Captive Portal page)

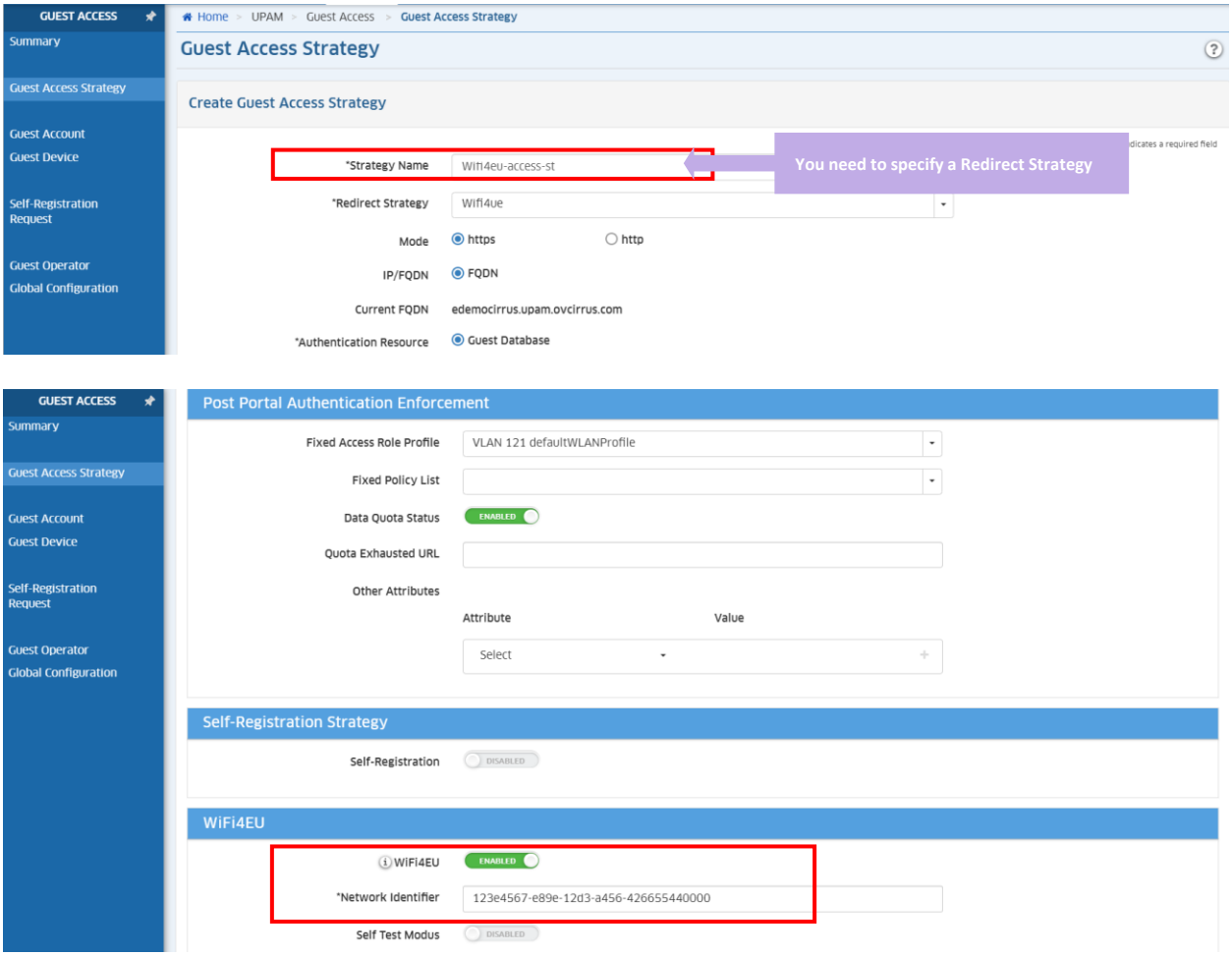


Figure 144: UPAM-NAC WIFI4UE Captive Portal snippet configuration – Omnvista Cirrus 4 (Guest Access Strategy)

171.	At least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall support the EDUROAM authentication hierarchy for Universities and Research Centers. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista Cirrus 4 are fully compliant with this requirement for Stellar multi-tenant deployments. The EDUROAM Authentication Hierarchy is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [62] for Omnivista 2500 NMS server.

172.	At least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall support Web content filtering for users that connect to the Internet. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista Cirrus 4 are fully compliant with this requirement for Stellar multi-tenant deployments. Web content access control in *Enterprise mode* is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [63] for Omnivista 2500 NMS server.

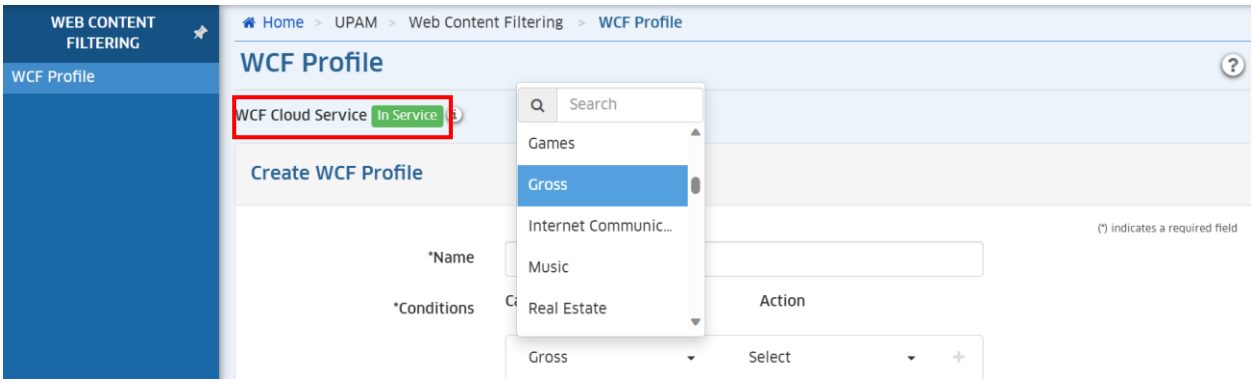


Figure 145: UPAM-NAC Web content filtering configuration – Omnivista Cirrus 4 (WCF Profile)

4.2. RF Management

173.	In the framework of a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow automatic and/or manual RF management (channel and power). This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista Cirrus 4 are fully compliant with this requirement for Stellar multi-tenant deployments. *Radio Dynamic Adjustment™* (RDA) technology is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [64] for Omnivista 2500 NMS server.

Figure 146: DRM with Channel List with tri-radio AP – Omnivista Cirrus 4 (RF Profile)

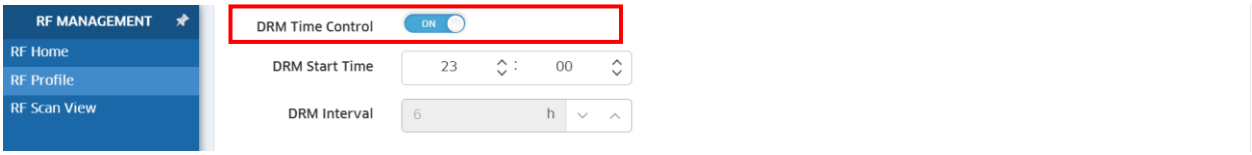


Figure 147: DRM Time Control – Omnivista Cirrus 4 (RF Profile)

174.	The WLAN solution shall support IEEE 802.11d standard in order to adapt channel and power levels to specific regulations of the geographical regions and countries to cover. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista Cirrus 4 are fully compliant with this requirement for Stellar multi-tenant deployments. Stellar Access Points support country information, to identify the regulatory domain where the access point is installed, along with other radio parameters such Frequency Hopping (FH). Stellar HW models exist to specifically support regulations for regions such as US HW model (US, Japan), ME HW model (Egypt, Israel) or RW HW model for any other country worldwide.

175.	The WLAN solution shall support IEEE 802.11h standard in order to adapt to regulatory constraints related to the use of the 5GHz frequency band. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4. Stellar Access Points implement IEEE 802.11h standard when Stellar

WLAN solution is managed by Omnivista NMS as a global solution, and description is done in [66] for Omnivista 2500 NMS server.

176.	The WLAN solution shall comply with different WLAN coverage classes defined for next-generation services deployed in the 6GHz frequency band when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4. Stellar Wi-Fi 7 Access Points manage transmit power and power range per band in the 6GHz when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and description is done in [67] for Omnivista 2500 NMS server.

177.	The WLAN solution shall support large width for sparse AP deployment when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Sparse AP deployment is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and description is done in [68] for Omnivista 2500 NMS server.

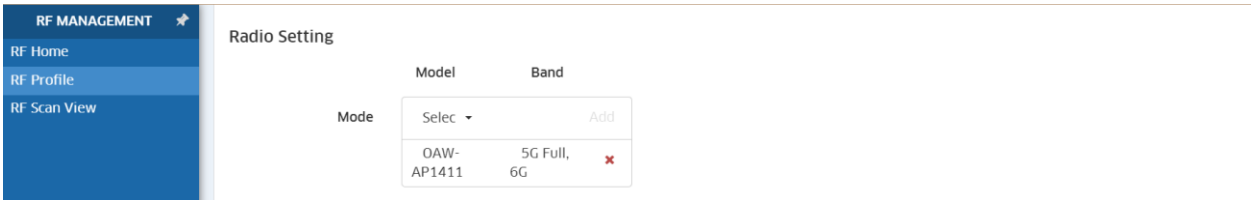


Figure 148: Sparse AP deployment on dual radio – Omnivista Cirrus 4 (RF Profile)

178.	The WLAN solution shall support preamble puncturing for better use of wideband channels in the presence of interference within the band when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Preamble puncturing is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and description is done in [69] for Omnivista 2500 NMS server.

179.	The WLAN solution shall support most recent modulations for latest dual-band and tri-band clients when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Most recent modulations are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution.

180.	The WLAN solution shall support power saving functions for battery consuming clients or for clients with specific data transmission. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Power saving functions are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [71] for Omnivista 2500 NMS server.

181.	The WLAN solution shall minimize the airtime consumption in extremely dense environments where cell overlap is significant. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Basic Service Set coloring (BSS coloring) for 802.11ax OFDMA-based communications is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [72] for Omnivista 2500 NMS server.

182.	The WLAN solution must be compatible with previous 802.11ax (Wi-Fi 6/6E), 802.11ac (Wi-Fi 5) and 802.11b/g/n (Wi-Fi 4) standards and remains compatible in case of clients do not support fully the latest standards. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Compatibility with previous Wi-Fi standards is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [73] for Omnivista 2500 NMS server.

Figure 149: 802.11be, 802.11ax and MU-MIMO operation – Omnivista Cirrus 4 (RF Profile)

183.	The WLAN solution shall support Short Guard Interval when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Short Guard Interval is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [74] for Omnivista 2500 NMS server.

184.	The WLAN solution shall support Long Guard Interval and Long symbol duration when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This without requiring third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Long Guard Interval and Long symbol duration are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [75] for Omnivista 2500 NMS server.

185.	The WLAN solution shall be smart enough to guide a new client to the optimal band/channel (2.4GHz/5GHz and 6GHz) considering, at a given time, both the number of associated clients on each band, and the medium utilization. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Guiding a new client to the optimal 2.4GHz/5GHz and 6GHz band/channel is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [76] for Omnivista 2500 NMS server.

186.	If no channel (2.4GHz/5GHz/6GHz) is overloaded (high medium utilization) or crowded (high client count), an AP shall by default guide a new client to the 5GHz/6GHz band. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4.

187.	Even if the 5GHz/6GHz band is not overloaded but is crowded (high client count), an AP shall guide a new client to the 2.4GHz band. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4.

188.	If a channel (2.4GHz/5GHz/6GHz) is overloaded (high medium utilization) and even if it is not crowded, an AP shall guide a new client to the less loaded band/channel. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4.

189.	If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilization) and no band/channel is crowded, an AP shall guide a new client to the 5GHz/6GHz band. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4.

190.	If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilization) and the 5GHz is crowded, an AP shall guide a new client to the 2.4GHz band. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4.

191.	The WLAN solution must be able to guide a new client to the appropriate channel (5GHz/6GHz) when connecting to access points supporting the 6GHz band separately (Wi-Fi 6E), considering the capability of client to connect to this frequency band. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Prioritize connection on 6GHz band is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [82] for Omnivista 2500 NMS server.

192.	The WLAN solution must be able to guide a new tri-band client to the appropriate resources and channels (2.4GHz/5GHz/6GHz) when connecting to access points	C/PC/NC

	that support aggregation of these bands (Wi-Fi 7 access points), considering the capability of client to connect to these aggregated resources. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Support Multi-Link operations on 2.4GHz/5GHz/6GHz bands is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [83] for Omnivista 2500 NMS server.

Figure 150: MLO operation with tri-band radio AP – Omnivista Cirrus 4 (WLAN Service Expert)

193.	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omni vista Cirrus 4 for Stellar multi-tenant deployments. Smart/dynamic load balancing is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [84] for Omnivista 2500 NMS server.

194.	The WLAN solution shall force clients to the 5GHz (or 6GHz) only when they are dual band capable. The WLAN solution shall force clients to the 5GHz only or shall force clients to the 6GHz only (Wi-Fi 6E capable) when they are dual band capable. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4, in *Wi-Fi Enterprise mode* as depicted in following figures:

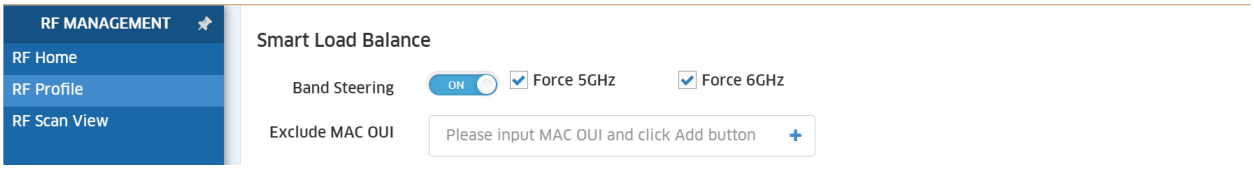


Figure 151: 5GHz and 6GHz forcing for dual band clients – Omnivista Cirrus 4 (RF Profile)

195.	The WLAN solution shall deny connection to an AP when the signal of the client becomes too weak and disconnect a client to force it to roam when the signal becomes too weak. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Indeed, the OmniAccess Stellar WLAN solution allows to set RSSI (*Received Signal Strength Indication*) thresholds in decibels in order to optimize connectivity by forbidding client access to the network when the signal is too weak or by disconnecting a client (forcing it to roam) when the signal becomes too weak.

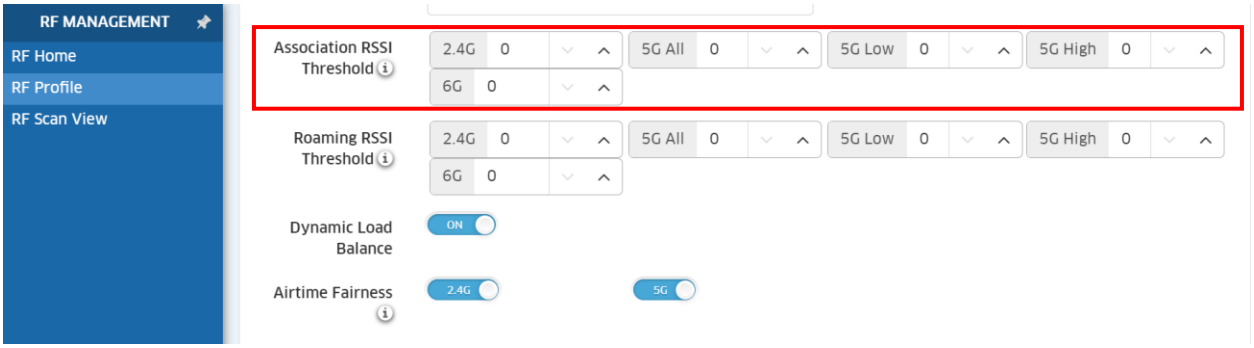


Figure 152: Per-band Association and Roaming RSSI Thresholds – Omnivista Cirrus 4 (RF Profile)

196.	The WLAN solution shall support the IEEE 802.11v and 802.11k standards to facilitate network guided roaming. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. 802.11v and 802.11k are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [87] for Omnivista 2500 NMS server.

Both standards are supported in Omnivista Cirrus 4 as depicted in the following figures:

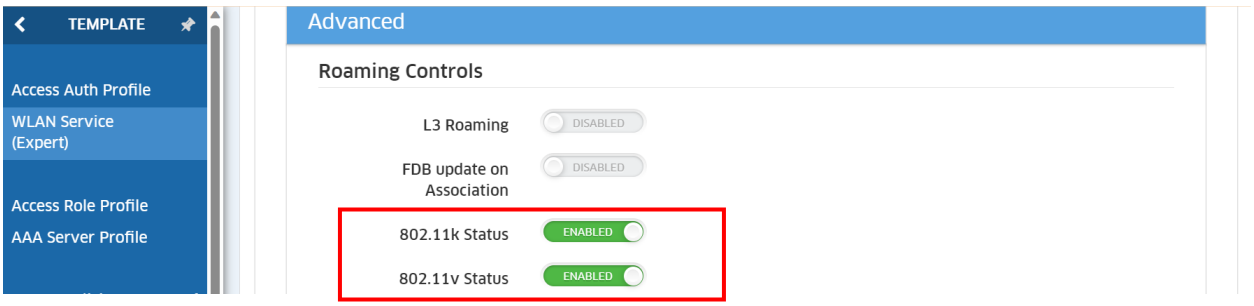


Figure 153: IEEE 801.11k & 802.11v support – Omnivista Cirrus 4 (WLAN Service Expert)

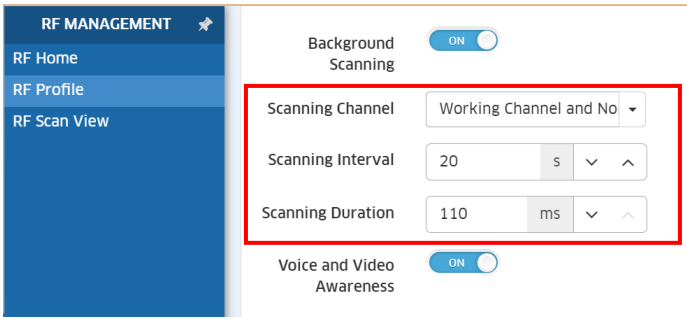


Figure 154: Background scanning for 802.11k/v support – Omnivista Cirrus 4 (RF Profiles)

197.	The WLAN solution shall support data rate control to encourage clients to roam at higher rates. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Data rate control is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [88] for Omnivista 2500 NMS server.

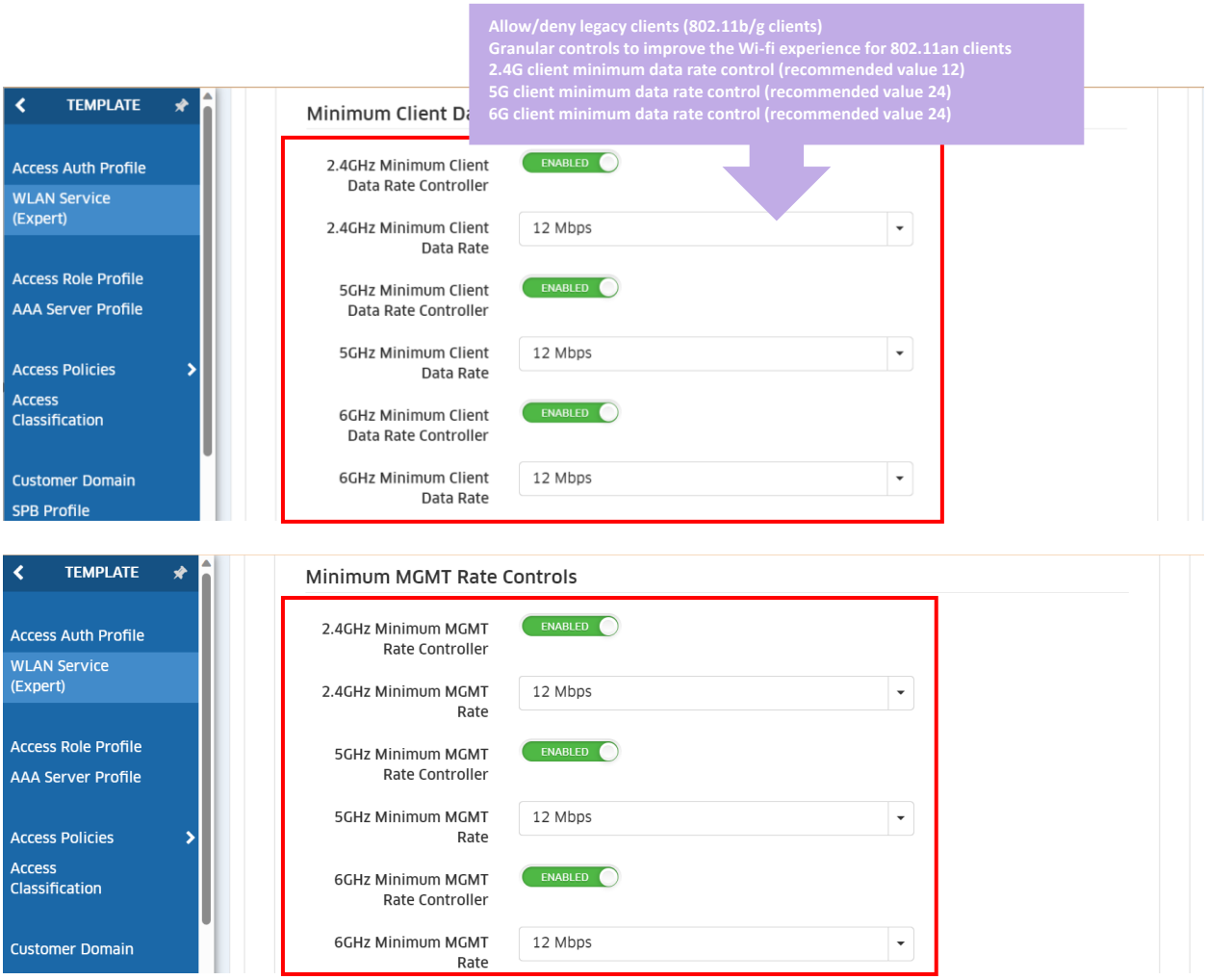


Figure 155: Minimum Data Rates Control - Omnivista Cirrus 4 (WLAN Service Expert)

198.	The WLAN solution shall propose APs that have the ability to scan the air in order to provide interfering/rogue APs and wireless attacks detection and shall not rely on external scanning equipment. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Background scanning is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [89] for Omnivista 2500 NMS server.

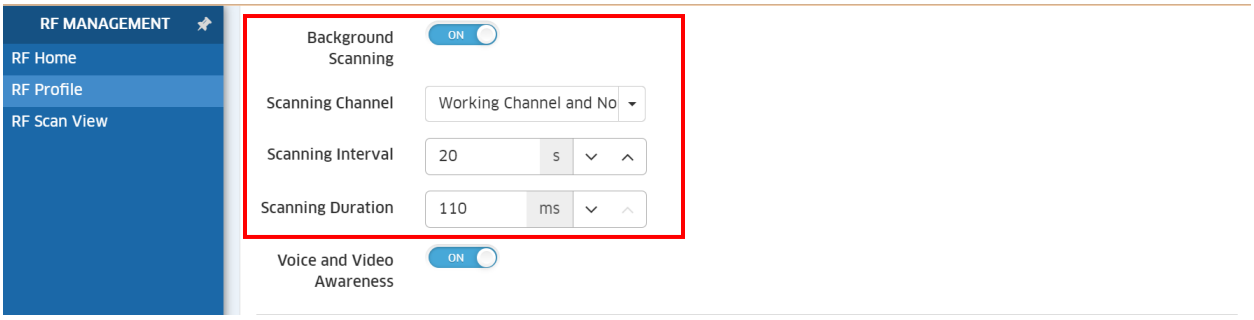


Figure 156: Background Scanning support – Omnivista Cirrus 4 (RF Profile)

199.	The scanning function of the APs shall not impact active voice or video calls (SIP and H.323). The scanning function of the APs shall not impact active voice or audio/video calls (SIP, H.323 or proprietary). This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Voice and video awareness is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [90] for Omnivista 2500 NMS server.

200.	At least for the 5GHz/6GHz band, the WLAN solution shall allow to define the list of channels which can participate in dynamic configuration. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments.

The list of authorized channels can be defined in *Wi-Fi Enterprise mode* through *RF profiles* which can then be applied to OmniAccess Stellar Access Points directly or via AP-Groups:

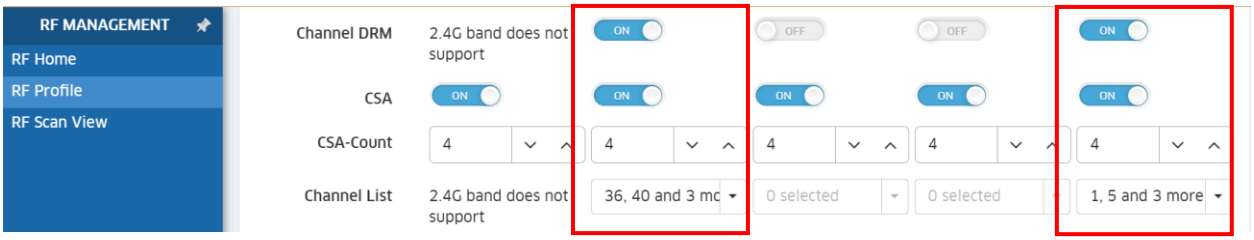


Figure 157: Authorized Channel List definition – Omnivista Cirrus 4 (RF Profile)

201.	The WLAN solution shall allow to define a range of transmit power per band (min & max) even if power settings are configured for automatic and dynamic assignments. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. All *Enterprise modes*, with power settings set as "automatic", allow to configure a range of transmit power per band (min & max). The auto power selection algorithm then selects the transmit power of the AP within the minimum and maximum specified.

The range of transmit power per band can be defined in *Wi-Fi Enterprise mode* through *RF profiles* which can then be applied to OmniAccess Stellar Access Points directly or via AP-Groups:

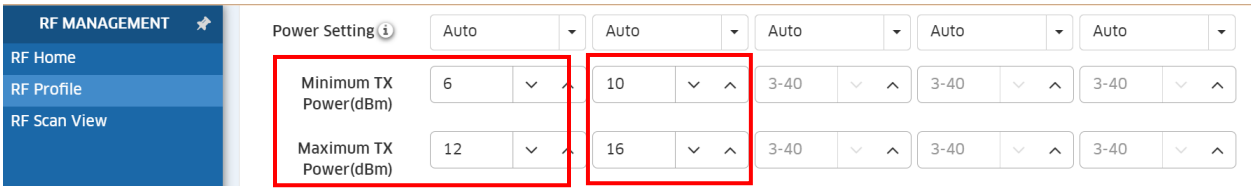


Figure 158: Min & max automatic transmit power – Omnivista Cirrus 4 (RF Profile)

OmniAccess Stellar transmit power management feature is also known as DFS/TPC feature for the control of transmitted power for outdoor using the UNII-2 5GHz DFS sub-band.

202.	The WLAN solution shall propose Access Points which can all be configured and deployed in a dedicated scanning mode. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. In *Wi-Fi Enterprise mode*, OmniAccess Stellar AP15xxs, AP14xxs, AP13xxs and AP12xxs can be set to examine the radio frequency environment in which the Wi-Fi network is operating by analyzing all channels, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel. In *Wi-Fi Enterprise mode*, scanning mode can be enabled permanently or for a one-shot scan.

The picture below show an AP managed by Omnivista Cirrus 4, with dedicated scanning enabled

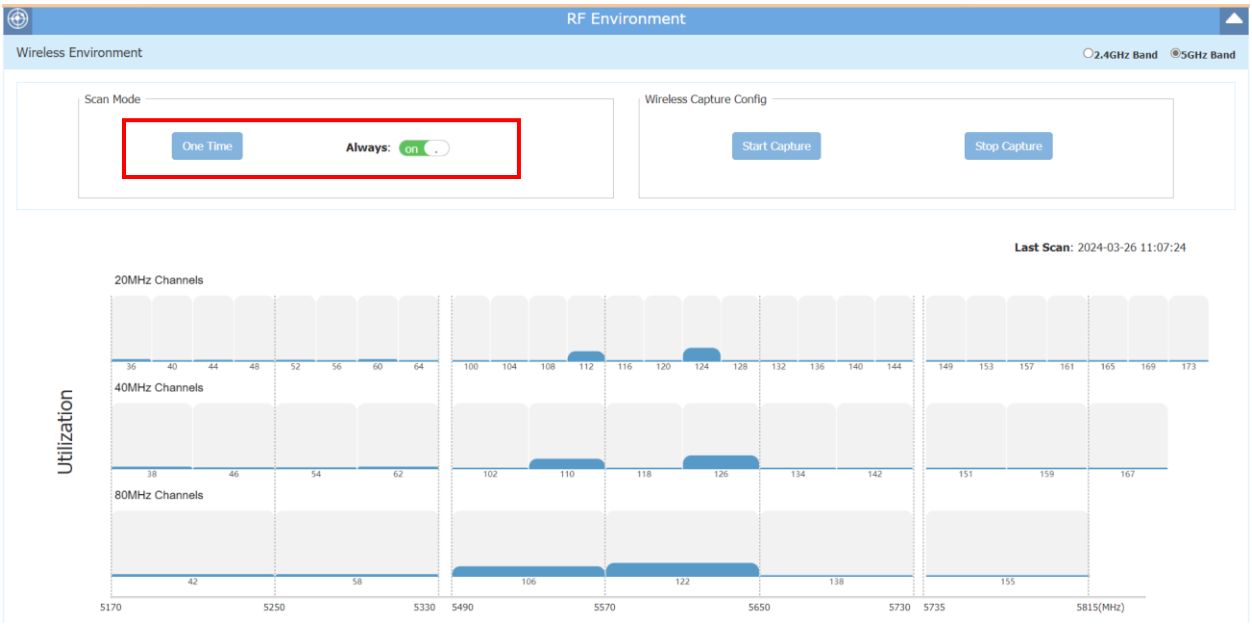


Figure 159: AP dedicated Scanning Mode activation – AP Web (RF environment)

203.	The WLAN solution shall propose Access Points with wireless packet capture capabilities. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Wireless packet capture is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [94] for Omnivista 2500 NMS server.

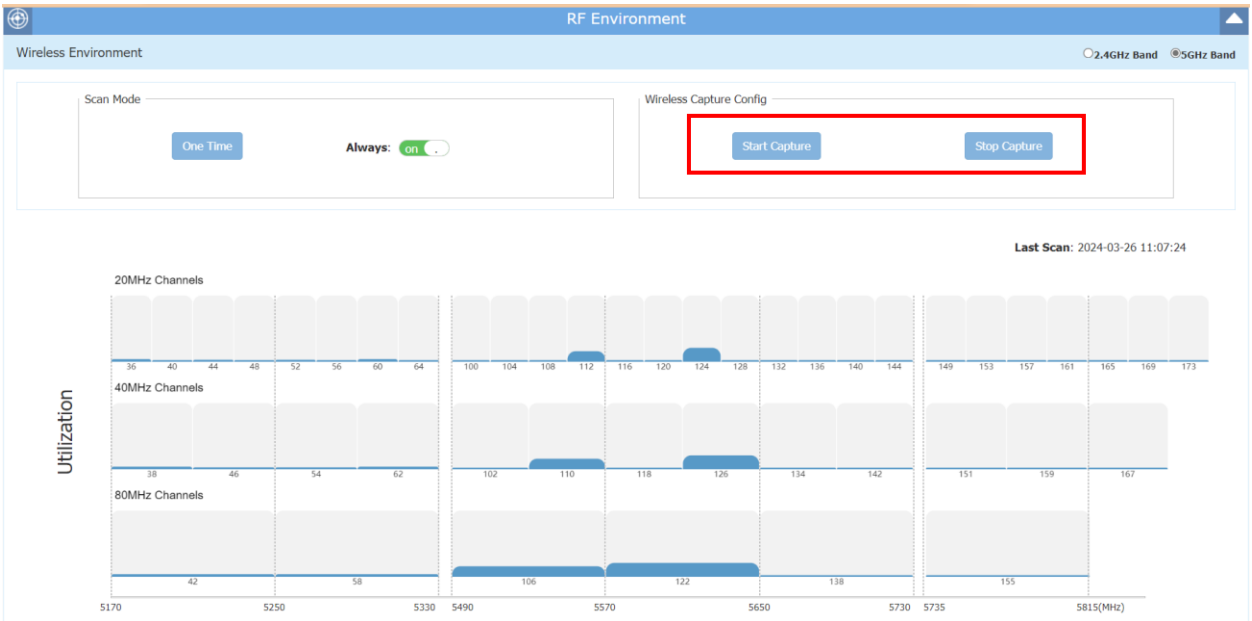


Figure 160: AP dedicated Wireless Capture – AP Web (RF environment)

204.	The WLAN solution shall make it simple to review the roaming history for a given client device. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments, by allowing to easily trace clients roaming behavior and Quality of Experience (QoE) for devices connectivity. As shown in following figure with Omnivista 2500, the *Wi-Fi Enterprise mode* provides the time of roaming and RSSI historical information over a completely customized time range. For each roaming occurrence, Roaming AP, Association Time, Band and RSSI are recorded. With more resources in the Cloud *Wi-Fi Enterprise mode* offers Up to 30 days of roaming & RSSI history:

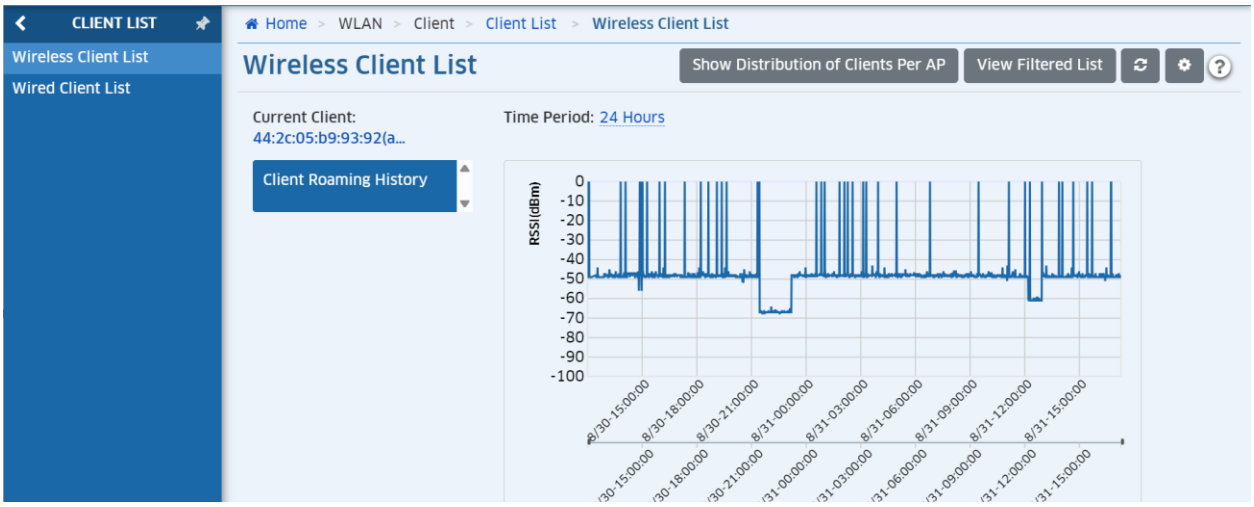


Figure 161: Network Analytics – Omnivista Cirrus 4 (Wireless Client List)

205.	The WLAN solution shall allow long interval background scanning, when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Long interval background scanning is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [96] for Omnivista 2500 NMS server.

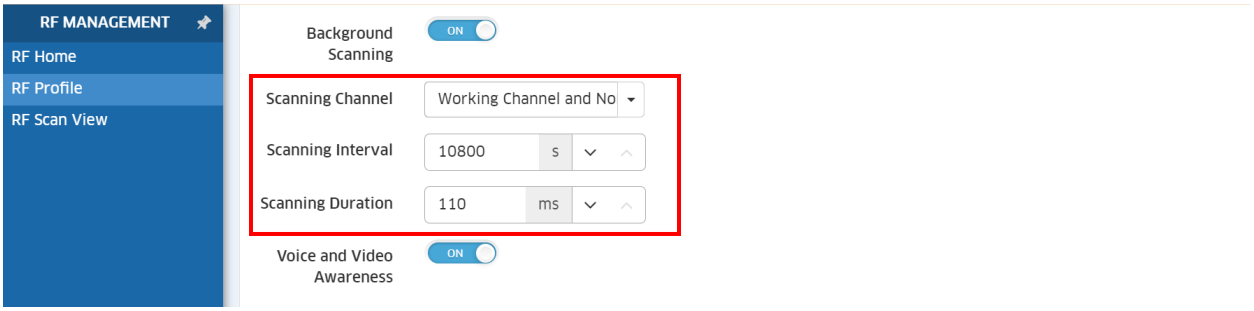


Figure 162: Long Interval Background Scanning – Omnivista Cirrus 4 (RF Profile)

4.3. Intrusion Detection and Prevention

206.	At least for a "Cloud scenario deployment" as described previously [4], the WLAN solution have wIDS/wIPS capabilities with no additional and dedicated equipment nor additional license. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Indeed, OmniAccess Stellar Access Points integrate *wireless Intrusion Detection and Prevention* (wIDS/wIPS) capabilities and reduce deployment and management costs by using Access Points to simultaneously serve clients and contain wireless threats.
With OmniAccess Stellar, there is no need for a costly overlay IDS with dedicated sensors. Automatic threat mitigation protects the network from unauthorized clients or APs and attacks. Integrated wIDS/wIPS capabilities allow to protect the WLAN better than an overlay deployment by virtue of being able to analyze and correlate 802.11 frames inline. It is possible to monitor the wireless radio spectrum for the presence of unsafe Access Points or unsafe clients, and countermeasures can be taken to mitigate the impact of foreign intrusions.

Last but not least, in *Wi-Fi Enterprise mode*, the OmniAccess Stellar APs embedded wIDS/wIPS capabilities do not require any additional license to protect the wireless network.

207.	The WLAN solution shall be able to identify Interfering APs, when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Identify Interfering APs is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [98] for Omnivista 2500 NMS server.

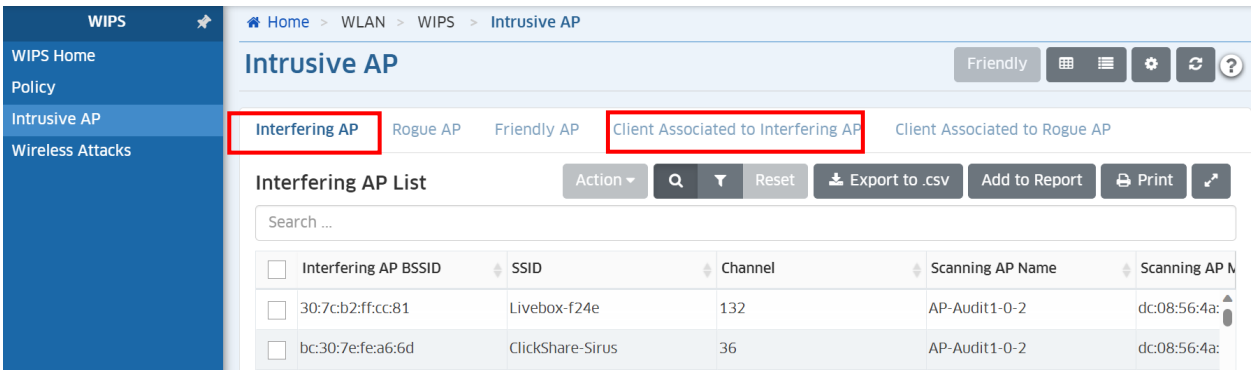


Figure 163: wIDS/wIPS – Omnivista Cirrus 4 (Intrusive Access Points)

208.	The WLAN solution shall be able to identify and contain Rogue APs, when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Beyond potential RF interference it can cause, a **rogue AP** is considered as a security threat to the WLAN network. This is typically the case of an unauthorized AP plugged into the wired side of the network (in that case, the MAC address of the scanned interfering AP is identified in the Forwarding Database of the scanning AP) or a foreign interfering AP broadcasting a SSID that is configured and set in the WLAN network.

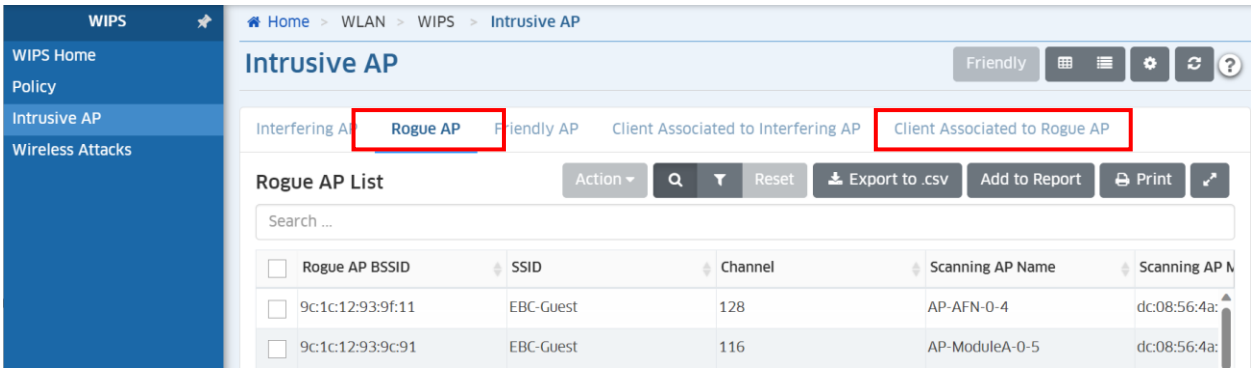


Figure 164: Rogue APs containment – Omnivista Cirrus 4 (Intrusive Access Points)

When an AP is classified as a rogue AP and when containment is enabled (disabled by default), the detecting AP (the one that detected the rogue AP) will send DEAUTH frames to clients that have associated to the rogue AP, keeping the clients away from the unsafe wireless network.

209.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible policies to classify an AP as a Rogue AP. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Define flexible policies to classify Rogue AP is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [100] for Omnivista 2500 NMS server.

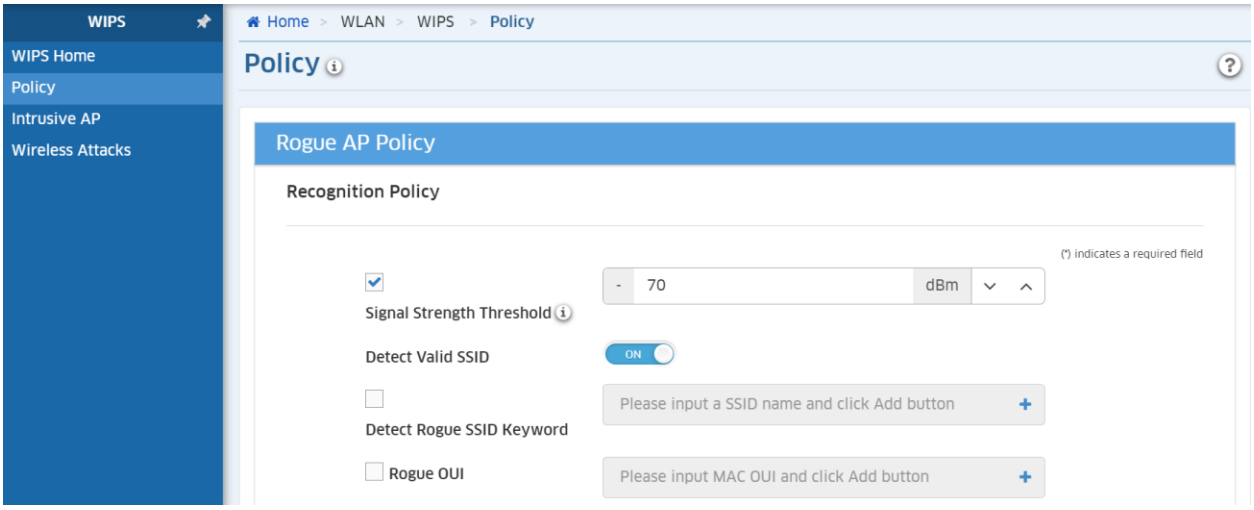


Figure 165: Rogue APs policy – Omnivista Cirrus 4 (WIPS Policy)

210.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible AP attacks detection policies. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Define flexible AP attacks detection policies is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [101] for Omnivista 2500 NMS server.

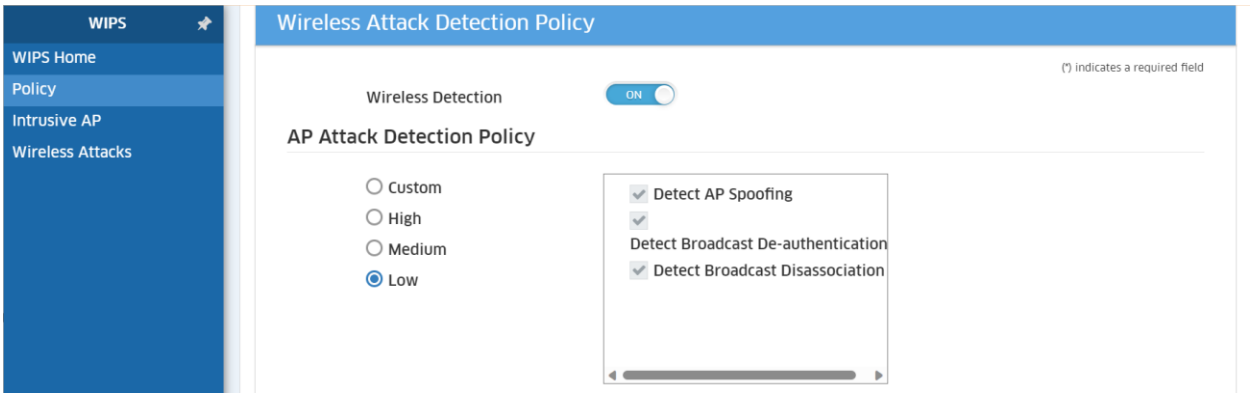


Figure 166: AP attack detection policy – Omnivista Cirrus 4 (WIPS Policy)

211.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow the definition of flexible client attacks detection policies. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Define flexible client attacks detection policies is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [102] for Omnivista 2500 NMS server.

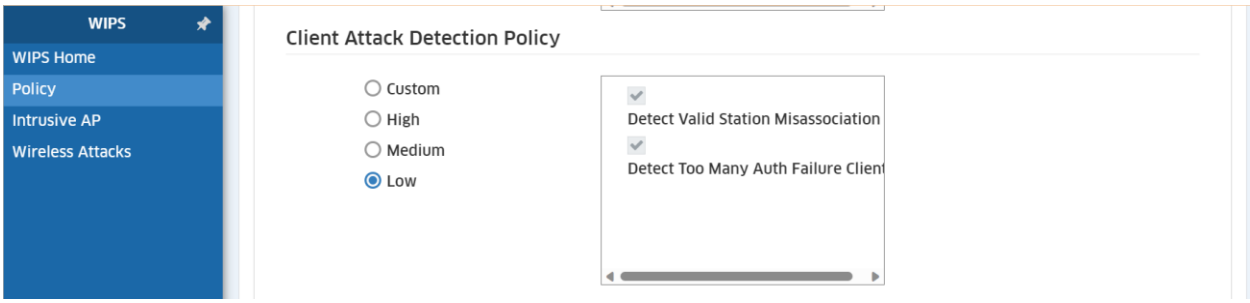


Figure 167: Client attack detection policy – Omnivista Cirrus 4 (WIPS Policy)

212.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. In *Wi-Fi Enterprise mode*, the

OmniAccess Stellar solution allows to blacklist a client manually or automatically. If a wireless attack has been detected the intruder identified (MAC address) by the wIDS/wIPS application is prevented from associating with the network.

213.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow to configure a blacklist duration.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments.

214.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow to configure an authentication failure times threshold.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 in *Wi-Fi Enterprise mode*. A description is done in [105] for Omnivista 2500 NMS server.

Picture below summarizes the policies on client blocklist for Omnivista Cirrus 4.

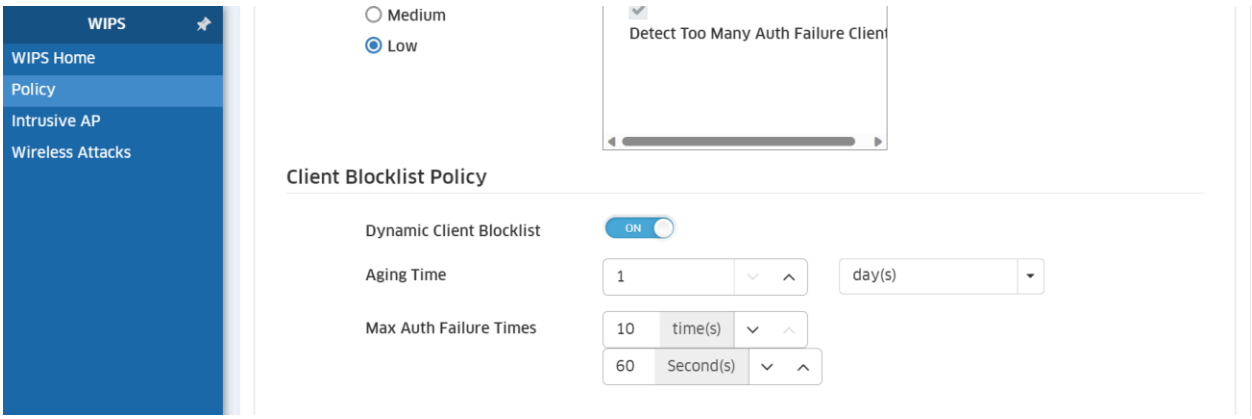


Figure 168: Client Blocklist policy – Omnivista Cirrus 4 (Policy)

4.4. Quality of Service

215.	At least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall offer WLAN Access Points that shall support fine-tuned Quality of Service (QoS) allowing following actions based on the identity of the connecting user: - ACL based (source/destination IP address and TCP/UDP ports) permit/deny decision	C/PC/NC

	- QoS priority marking and queuing This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 in *Wi-Fi Enterprise mode*. A description is done in [106] for Omnivista 2500 NMS server.

216.	At least for a "Cloud deployment" scenario as described previously [4], the wireless LAN solution shall comply with the 802.11e WMM standard and shall allow for custom QoS tag (802.1p/DSCP) to WMM queue mapping. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 in *Wi-Fi Enterprise mode*. A description is done in [107] for Omnivista 2500 NMS server.

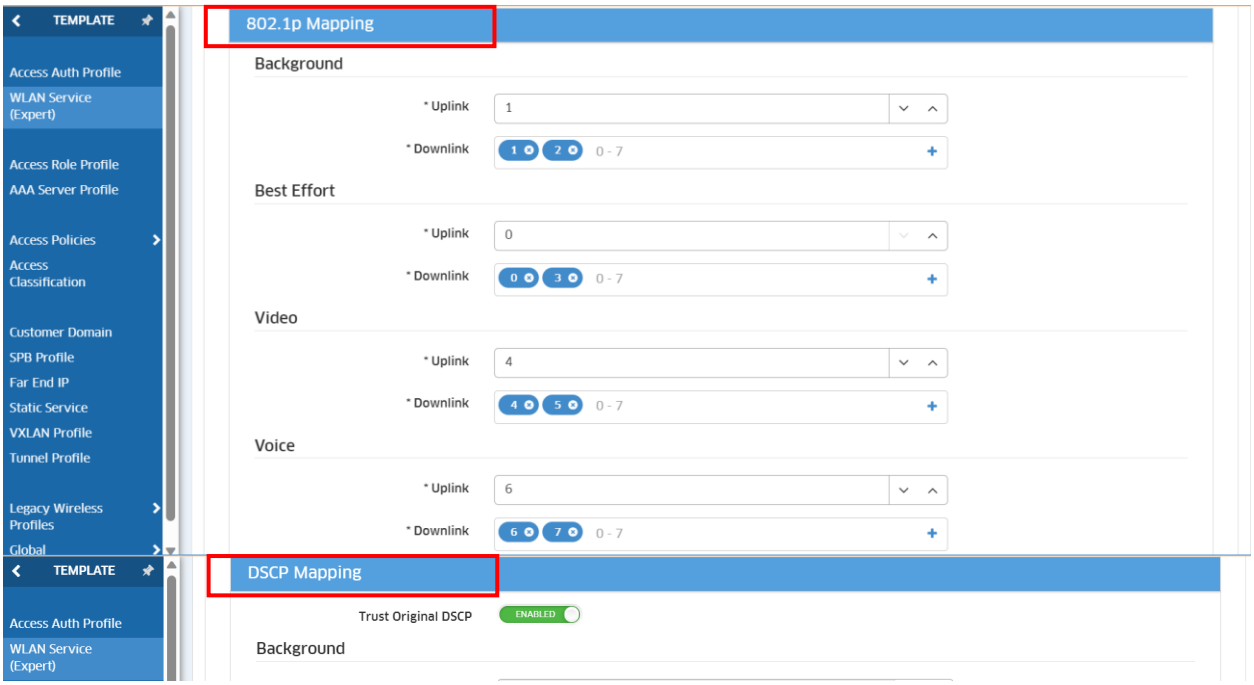


Figure 169: WMM/802.1p-DSCP mapping - Omnivista Cirrus 4 (WLAN Service Expert)

217.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall have traffic L7 Application fingerprinting (aka *Deep Packet Inspection* (DPI) capabilities allowing an administrator to take control of applications (even if they all run on top of the HTTP or HTTPs protocols), including not only blocking applications, but also allowing to prioritize and rate-limit applications. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Built-in DPI technology is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [108] for Omnivista 2500 NMS server.

218.	At least for a "Cloud deployment" scenario as described previously [4], the wireless LAN solution shall be able to define and guarantee bandwidth on basis of a SSID. It shall also be able to define and guarantee bandwidth based on a user/device role. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. A "bandwidth contract" definition is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [109] for Omnivista 2500 NMS server.

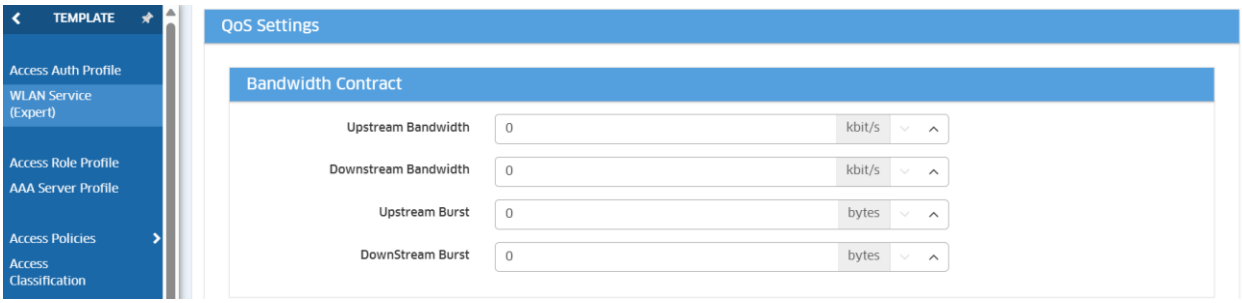


Figure 170: SSID Bandwidth Contract – Omnivista Cirrus 4 (WLAN Service Expert)

219.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow to set the maximum number of clients per band/radio and per AP for a specific SSID. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments.

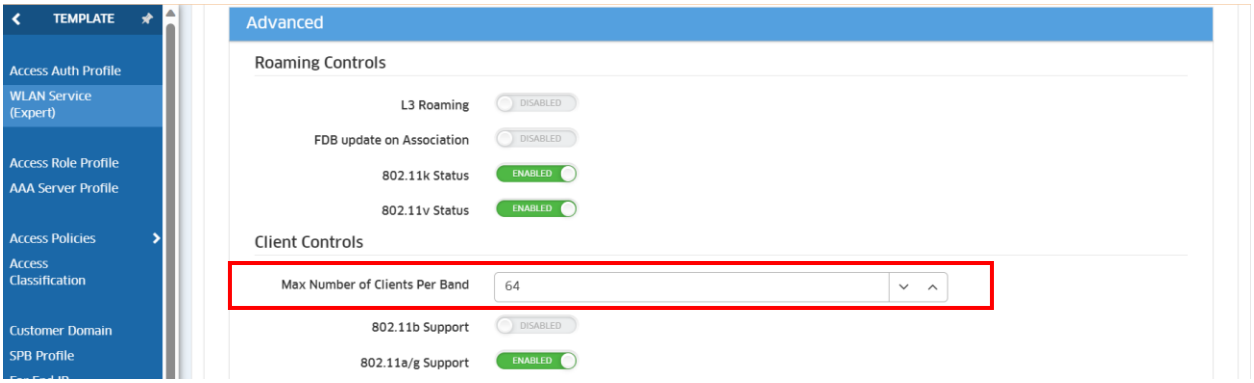


Figure 171: Maximum number of clients per band per SSID – Omnivista Cirrus 4 (WLAN Service Expert)

220.	At least for a "Cloud deployment" scenario as described previously [4], the wireless LAN solution shall propose broadcast traffic optimization mechanisms (including Broadcast filtering and Broadcast/Multicast Key rotation). This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Broadcast traffic optimization mechanisms are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [111] for Omnivista 2500 NMS server.

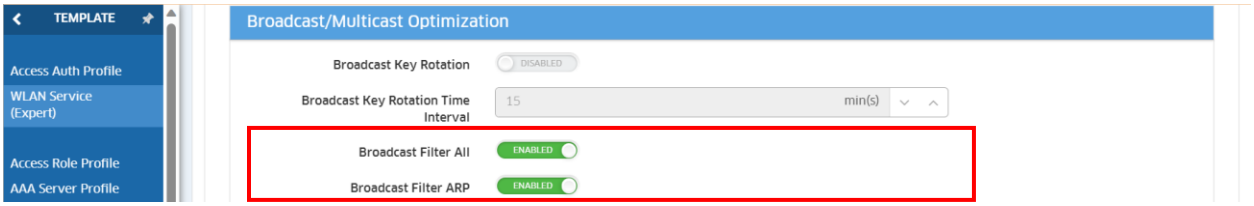


Figure 172: Broadcast traffic Optimization – Omnivista Cirrus 4 (WLAN Service Expert)

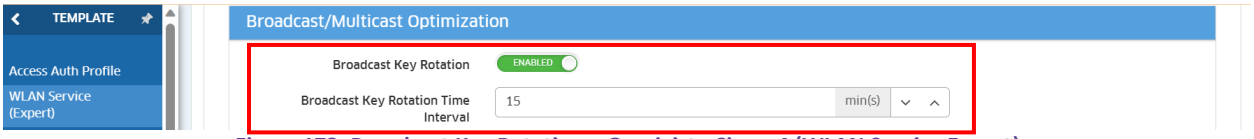


Figure 173: Broadcast Key Rotation – Omnivista Cirrus 4 (WLAN Service Expert)

221.	At least for a "Cloud deployment" scenario as described previously [4], the wireless LAN solution shall be able to optimize multicast traffic by converting multicast traffic to unicast traffic, leveraging its IGMP snooping capabilities. This	C/PC/NC

	when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Multicast traffic optimization is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [112] for Omnivista 2500 NMS server.

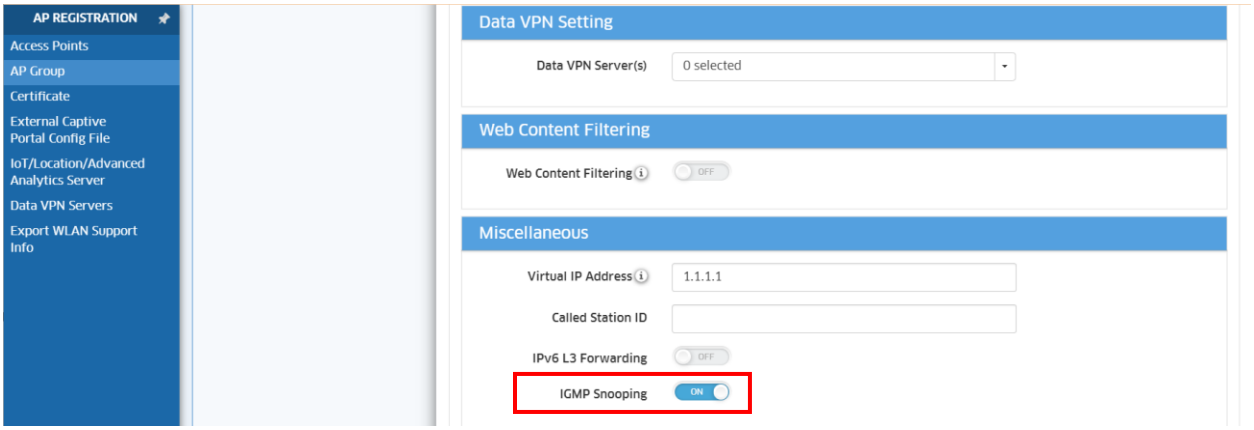


Figure 174: IGMP snooping – Omnivista Cirrus 4 (AP Group)

222.	At least for a "Cloud deployment" scenario as described previously [4], Multicast optimization shall stop on high load. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This without requiring third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Multicast based channel utilization is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a short description is done in [113] for Omnivista 2500 NMS server.

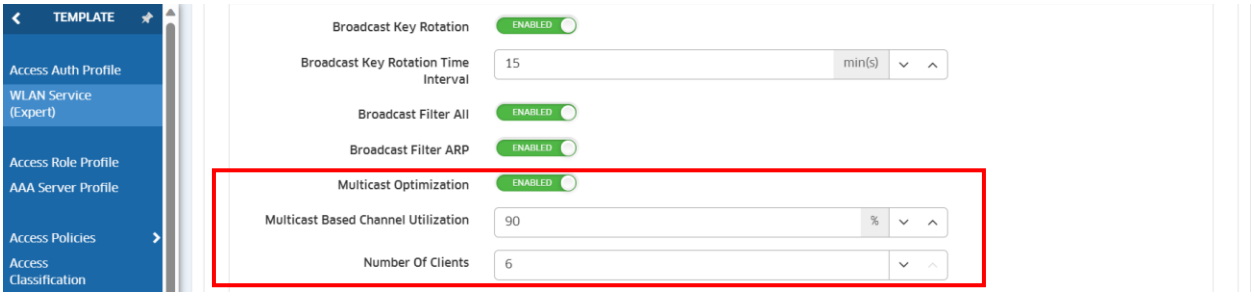


Figure 175: Multicast optimization - Omnivista Cirrus 4 (WLAN Service Expert)

223.	The wireless LAN solution shall propose the WMM *Automatic Power Save delivery* (APSD) feature to allow clients conserve battery life. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. WMM APSD is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [114] for Omnivista 2500 NMS server.

224.	The wireless LAN solution shall by default identify Voice and Audio/Video calls and provide appropriate treatment. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. It is indeed Voice and Video over IP aware and can dynamically classify real-time traffic in appropriate Class of Service. In addition, this level of voice awareness enables OmniAccess Stellar APs to know that a voice/audio/video call is taking place and not to scan channels for RF management or intrusion detection purposes until the call is terminated.

4.5. Mobility

225.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support Layer 2 roaming capabilities across APs with no special client-side software required. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Layer 2 roaming is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [116] for Omnivista 2500 NMS server.

226.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support Layer 3 roaming across APs with no special client-side software required. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. Layer 3 roaming is fully

supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [117] for Omnivista 2500 NMS server.

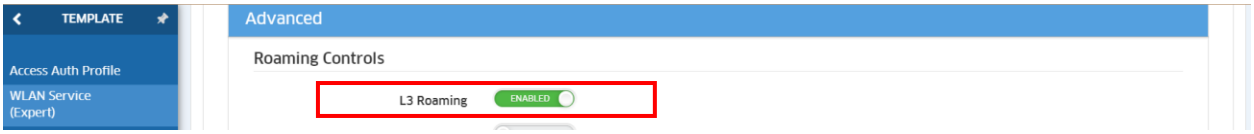


Figure 176: L3 roaming activation – Omnivista Cirrus 4 (WLAN Service Expert)

227.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support 802.11r Fast Roaming and OKC - *Opportunistic Key Caching*. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This without requiring third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. 802.11r Fast Roaming and OKC are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [118] for Omnivista 2500 NMS server.

228.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall comply with the 802.11k Radio Resource Management standard. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. 802.11k standard is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [119] for Omnivista 2500 NMS server.

229.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall comply with the 802.11v BSS Transition Management standard. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. 802.11v standard is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [120] for Omnivista 2500 NMS server.

230.	At least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall inform the wired side of the network about roaming across APs. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. *Forward Data Base Update* (FDB Update) *on association* is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and with a description in [121] for Omnivista 2500 NMS server.

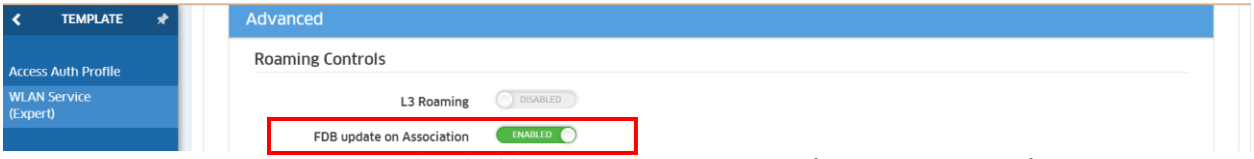


Figure 177: FDB Update disable option – Omnivista Cirrus 4 (WLAN Service Expert)

4.6. Wireless LAN Services

231.	In the framework of a “Cloud deployment” scenario as described previously [4], the solution shall provide BYOD Zeroconf services for mDNS. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments. BYOD Zeroconf services for mDNS are fully supported in *AOS-Responder mode* when Stellar WLAN solution is managed by Omnivista NMS as a global solution. A description is done in [122] for Omnivista 2500 NMS server.

Configuring the *AOS-Responder mode* is done using following menus in Omnivista Cirrus 4:

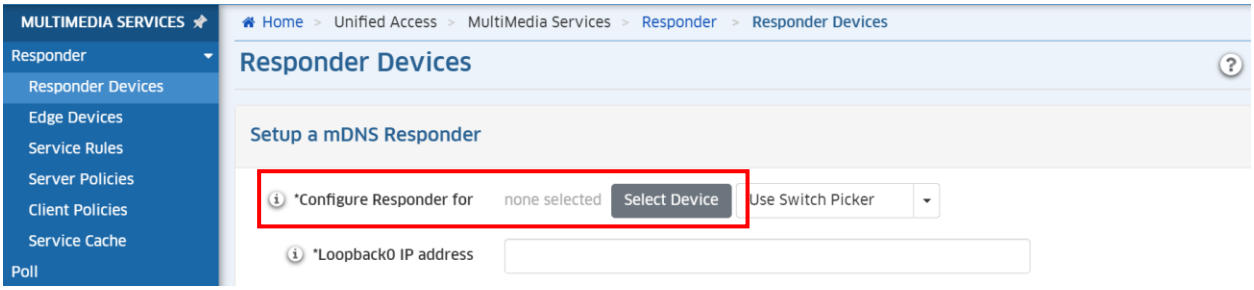


Figure 178: OmniVista Zeroconf configuration – Omnivista Cirrus 4 (Responder Devices)

In Responder mode, there is an overview in Omnivista Cirrus 4 about the current status of the Zeroconf network:

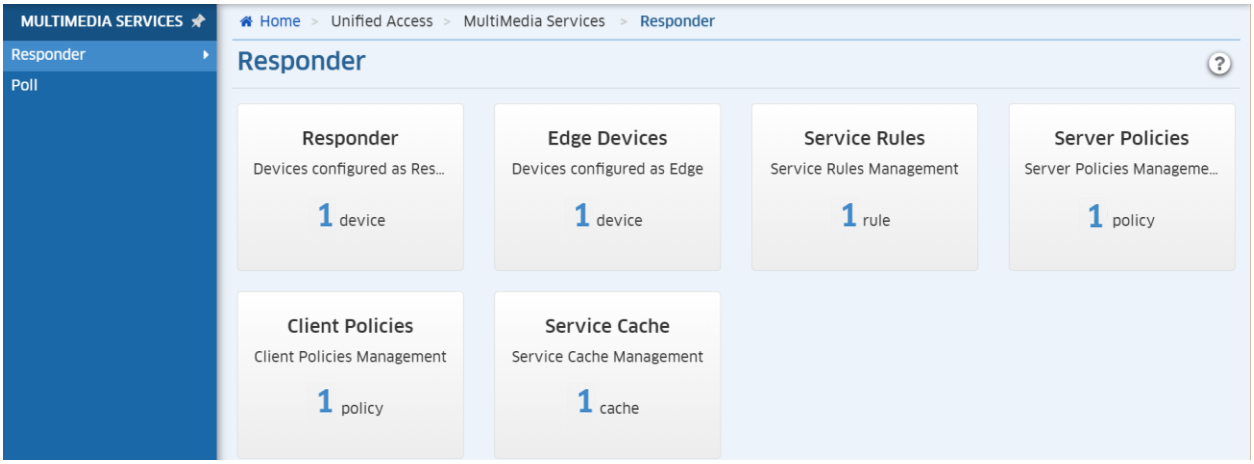


Figure 179: OmniVista Zeroconf Responder overview – Omnivista Cirrus 4 (Responder)

Responder devices configuration:

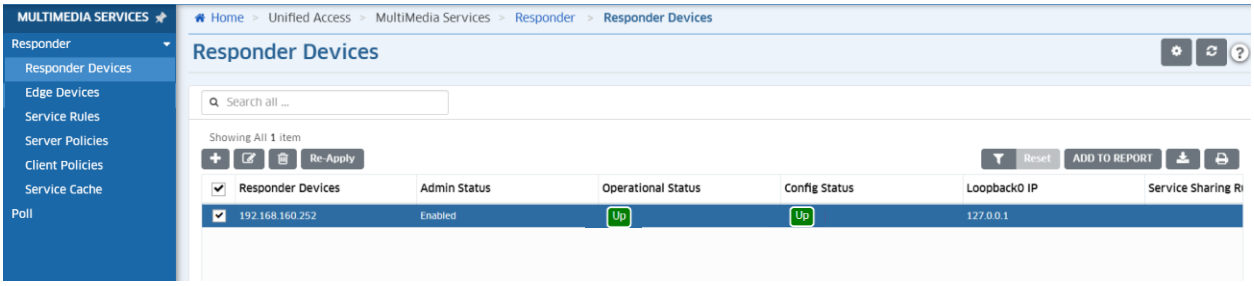


Figure 180: OmniVista Zeroconf Responder Configuration – Omnivista Cirrus 4 (Responder Devices)

Services learnt by the Responders (that can be used in the Service Policies):

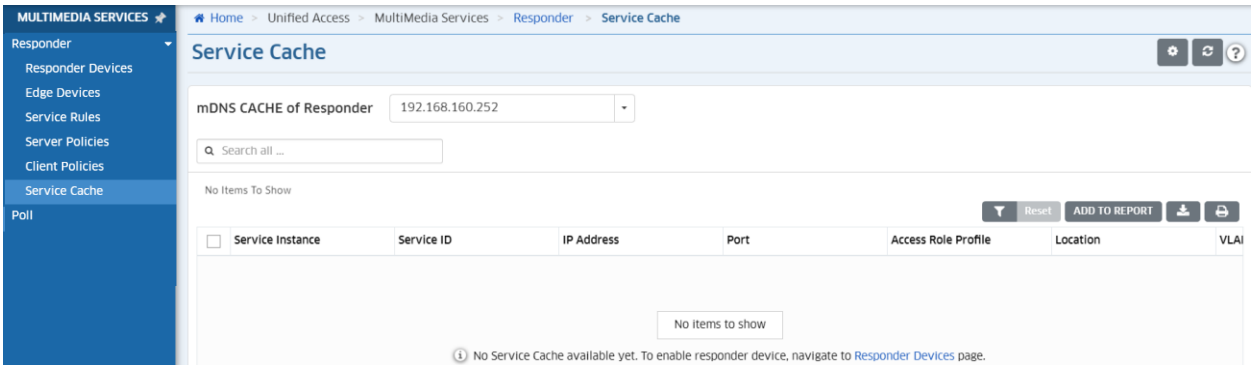


Figure 181: OmniVista Zeroconf Responders Services cache – Omnivista Cirrus 4 (Service Cache)

Edge devices, OmniSwitch and Stellar AP configuration:

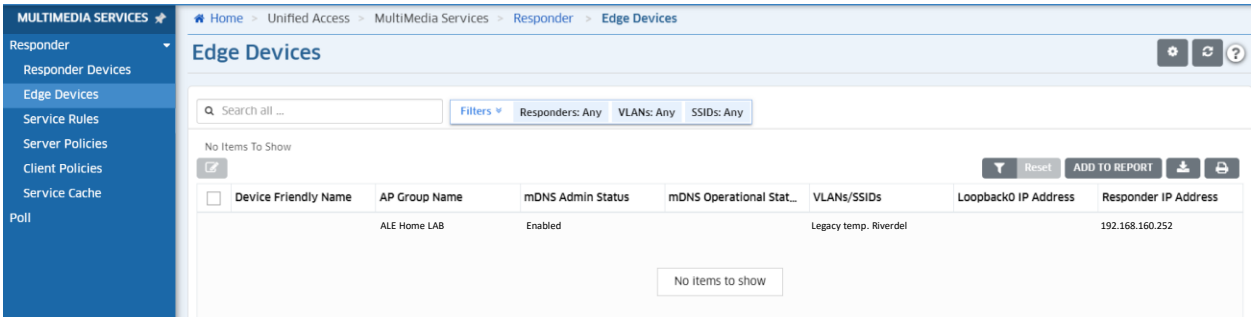


Figure 182: OmniVista Zeroconf Edge devices configuration – Omnivista Cirrus 4 (Edge Devices)

Service Rules will enable the Responder to forward mDNS/SSCP messages between the allowed devices:

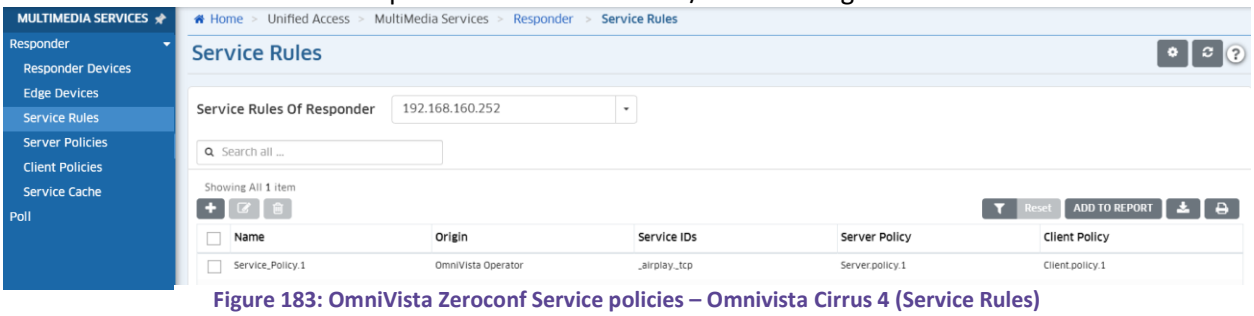


Figure 183: OmniVista Zeroconf Service policies – Omnivista Cirrus 4 (Service Rules)

Service Policies specify what services are allowed in the network, and relations between clients and servers serving the specified services. In this case, devices in VLAN 100 and 110 will be allowed to exchange information about 9 services:

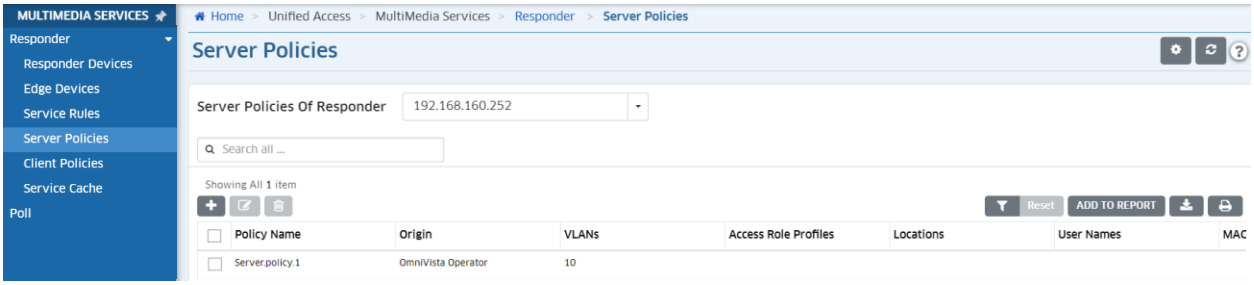


Figure 184: OmniVista Zeroconf Server policies – Omnivista Cirrus 4 (Server Policies)

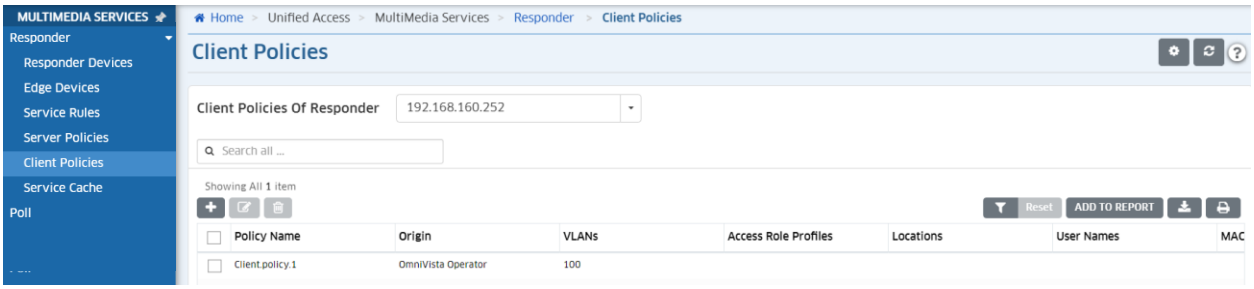


Figure 185: OmniVista Zeroconf Client policies – Omnivista Cirrus 4 (Client Policies)

4.7. IoT Servers & Advanced servers

232.	At least for a "Cloud deployment" scenario as described previously [4], wireless WLAN solution shall support advanced location-based services provided by Cloud services included in the solution and using Bluetooth LE wireless with dedicated Asset Tracking applications. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Enterprise mode*, and when combined with Omnivista Cirrus Asset Manager solution for the asset tracking & contact tracing application. A description of Omnivista Cirrus Asset Manager is given in [123] for Omnivista 2500 NMS server.

Stellar Asset Tracking profile with Stellar Asset tracking engine is created via OmniVista Cirrus 4 for APs with BLE radios.

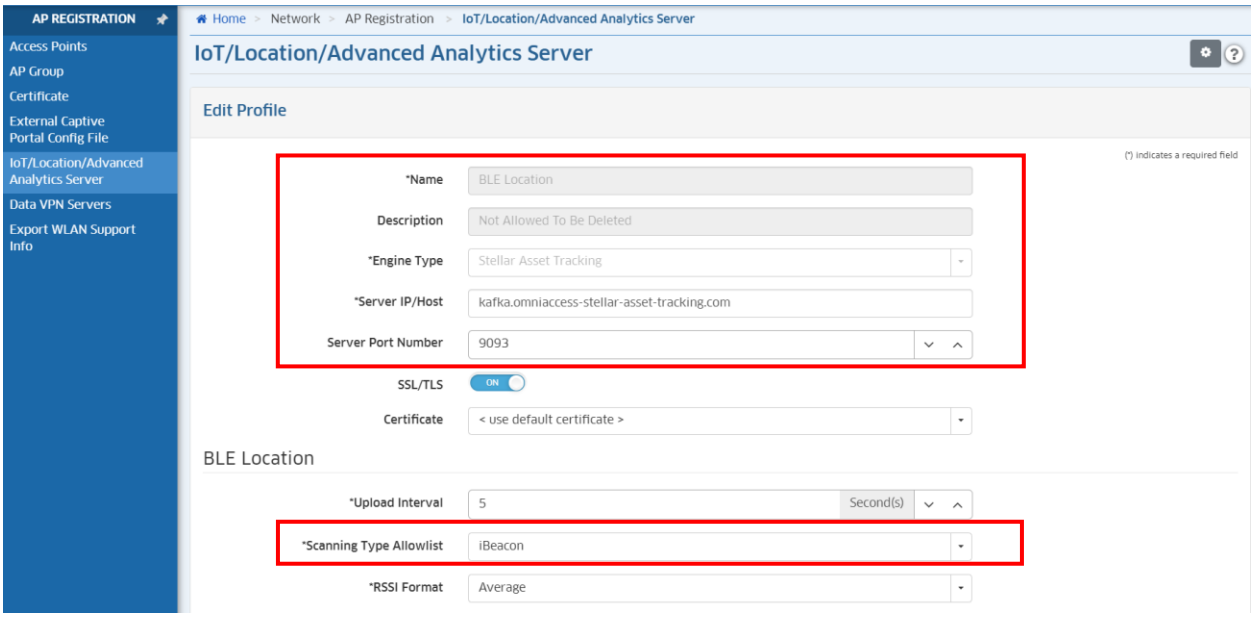


Figure 186: Stellar Asset Tracking profile – Omnivista Cirrus 4 (IoT/Location/Advanced analytics Server)

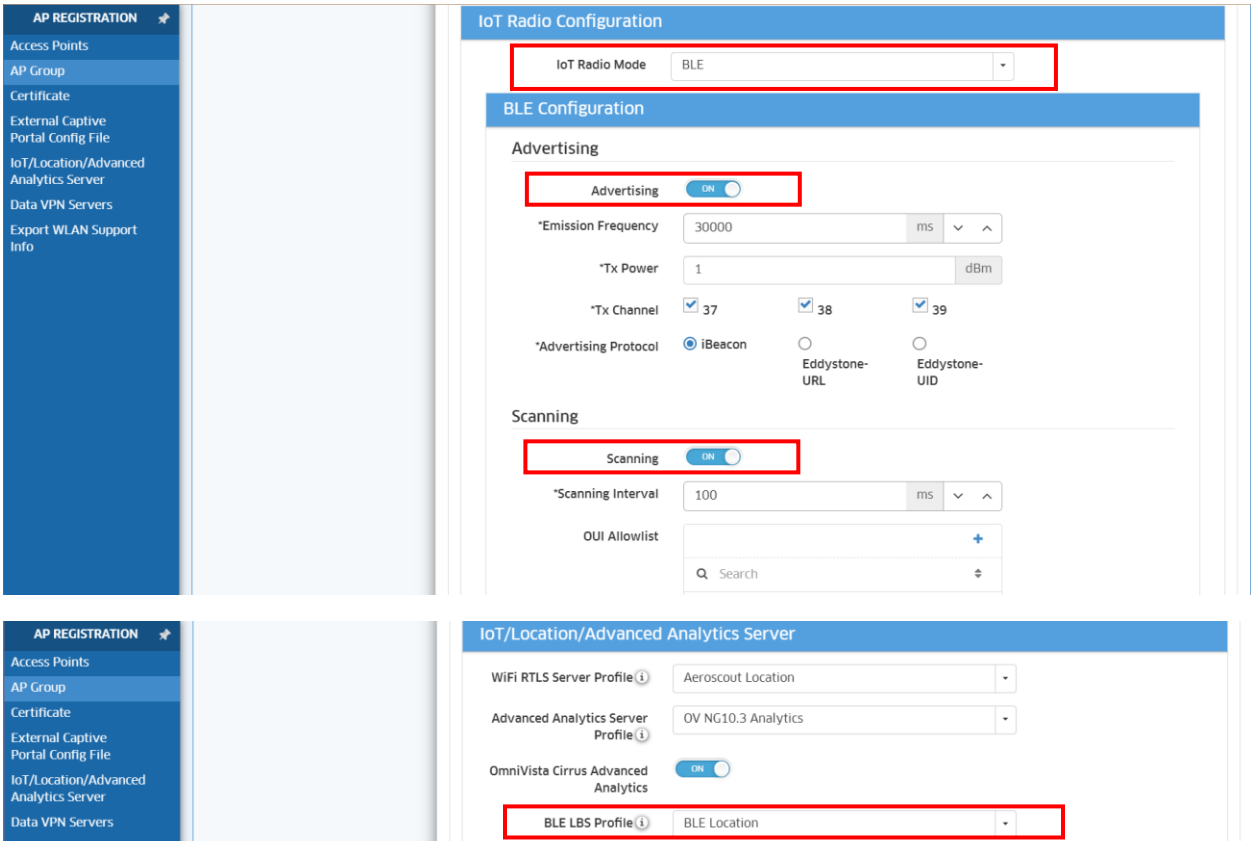


Figure 187 : BLE radio & Stellar Asset Tracking configuration – Omnivista Cirrus 4 (AP Group)

233.	At least for a “Cloud deployment” scenario as described previously [4], wireless WLAN solution shall support RTLS service provided by RTLS application if existing in the network, or by RTLS Cloud service included in the solution, using WLAN radio only for location-based service. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 for Stellar multi-tenant deployments in *Enterprise mode*.
High-Performance AP12xx, high-efficient AP13xx series (Wi-Fi 6), high-efficient AP14xx (Wi-Fi 6E) and extremely high throughput AP15xx (Wi-Fi 7) support Real-Time Location Service (RTLS) and provide data to RTLS location-based engines with WLAN radio measurements only (on the basis of received WLAN RSSIs from devices).

Omnivista Cirrus 4 offers customer the ability to manage RTLS location-based service in the Cloud on basis of received WLAN RSSIs from APs. Aeroscout RTLS application type offers customer the ability to manage RTLS location-based service on premises with existing RTLS application (Ekahau engine for example).

The management of RTLS service in OmniVista Cirrus 4 is identical to ones already discussed for IoT servers above [231]. RTLS profile must be created in OmniVista Cirrus 4 for APs that are supporting RTLS, with Aeroscout engine or any other Wi-Fi RTLS engine. The RTLS profile must be applied to AP-Groups that perform RTLS reports to RTLS engine.

234.	At least for a “Cloud scenario deployment” as described previously [4], wireless WLAN solution shall offer IoT device secure onboarding that is as simple as possible and without requiring additional third-party components. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 in *Enterprise mode*. A short description is done in [126] for Omnivista 2500 NMS server.

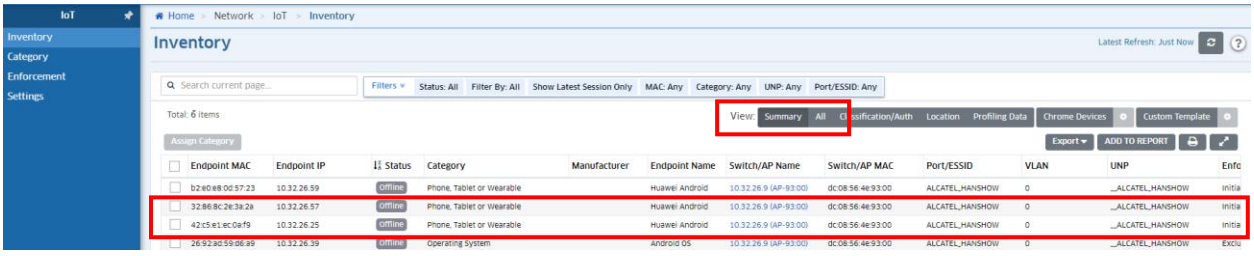


Figure 188: IoT Secure Onboarding – Omnivista Cirrus 4 (IoT Inventory)

235.	At least for a “Cloud deployment” scenario as described previously [4], wireless WLAN solution shall support advanced analytics services provided by Cloud	C/PC/NC

	services included in the solution, services dedicated to statistical and analytical tasks for large deployments. This without of third-party component for analytics. This when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments.	

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 4 in *Enterprise mode* for Stellar multi-tenant deployments, and when combined with Omnivista Cirrus 10 instance for statistical & analytical tasks. A description is done in [127] for Omnivista 2500 NMS server.

Stellar advanced analytics support via OmniVista Cirrus 4 is done through the following menus.

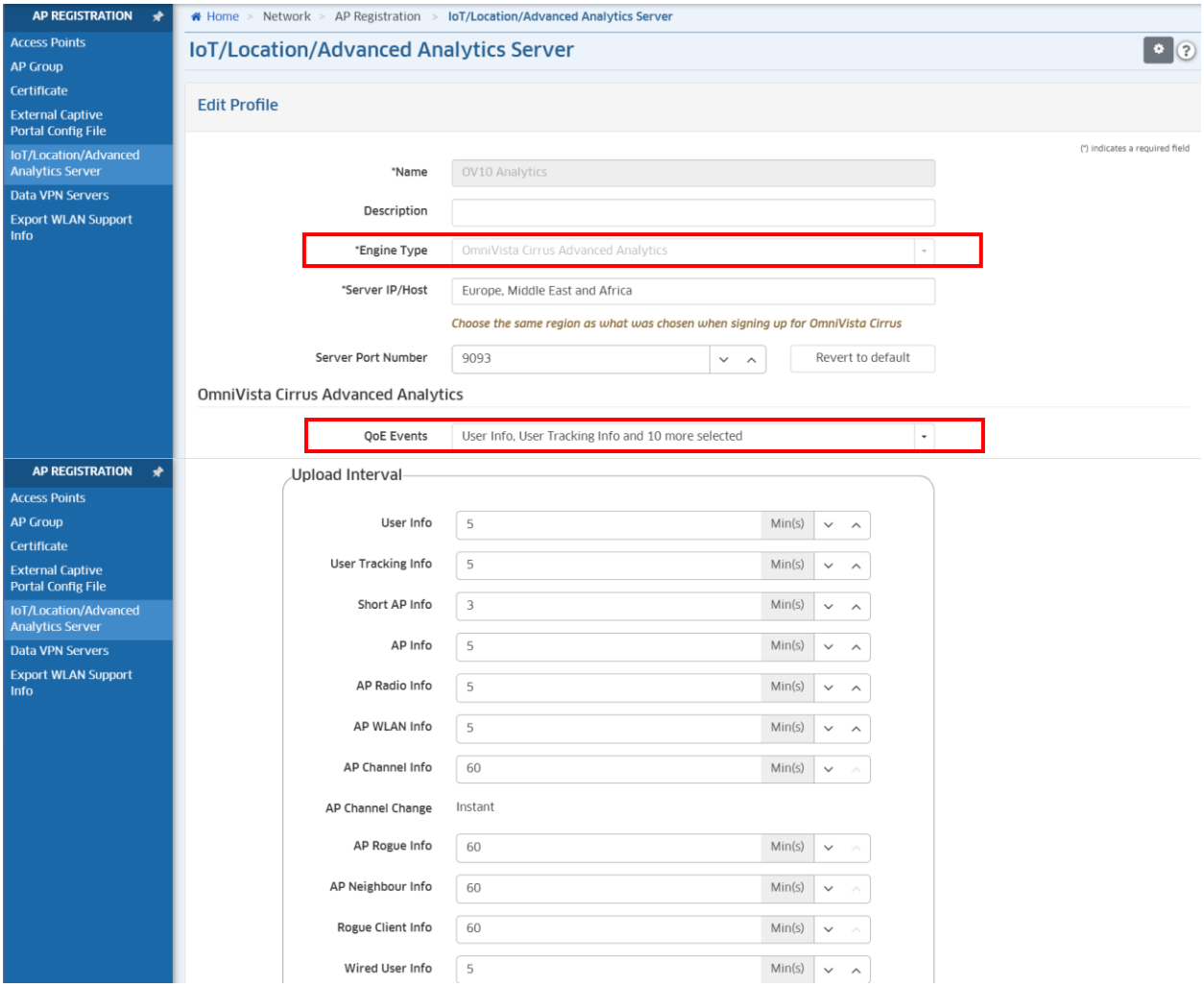


Figure 189: OV Cirrus 10 Advanced Analytics profile – Omnivista Cirrus 4 (IoT/Location/Adv. Analytics Server)

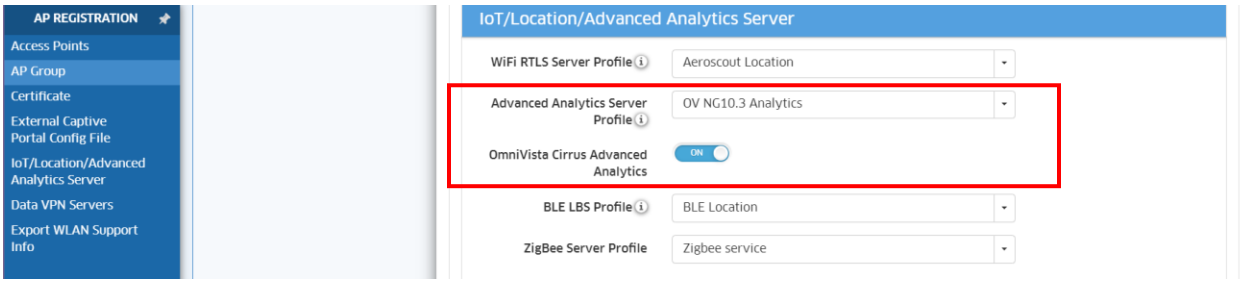


Figure 190: Advanced Analytics configuration – Omnivista Cirrus 4 (AP Group)

5. Omnivista Cirrus 10 requirements

5.1. Access Control, Authentication and Encryption

236.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support MAC based authentication provided by a SaaS NMS cloud solution included in WLAN solution, for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. MAC-based authentication is fully supported when Stellar WLAN solution is managed by Omnivista NMS, and is further described in [26] for Omnivista 2500 NMS server.

237.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support 802.1x based authentication provided by a SaaS NMS cloud solution included in WLAN solution, for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. 802.1x based authentication is fully supported when Stellar WLAN solution is managed by Omnivista NMS, and is further described in [27] for Omnivista 2500 NMS server.

238.	At least for a “Cloud scenario” as described previously [4], the wireless LAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication, provided by a SaaS NMS cloud solution included in WLAN solution, for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments by offering an embedded Radius server in *Wi-Fi Enterprise mode* for 802.1x and MAC authentication. *Unified Policy Access Manager* (UPAM-NAC) is fully supported when Stellar WLAN solution is managed by Omnivista NMS, and is essentially described in [28] for Omnivista 2500 NMS server.

Omnivista Cirrus 10 brings numerous benefits by leveraging the latest cloud technologies to securely manage UPAM-NAC authentication information. ALE NAS server and built-in RADIUS are integrated in Omnivista Cirrus 10. By enabling the RADSec option the communication between the ALE NAS server and external RADIUS servers is encapsulated within secure TLS or DTLS connections. This implementation ensures the confidentiality and integrity of credentials for the UPAM-NAC service, which covers all users and ALE equipment in the Cloud. Utilization of secure connections reduces the risks of unauthorized manipulation or interception of data during UPAM-NAC requests.

239.	At least for a “Cloud scenario” as described previously [4], built-in RADIUS server as described [28] shall be able to interface with an external authentication server (Radius, LDAP, Active Directory, Microsoft Azure AD): FreeRadius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP etc. when managed by a SaaS NMS cloud solution included in WLAN solution, for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments by offering connection to external authentication sources. This feature is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [29] for Omnivista 2500 NMS server.

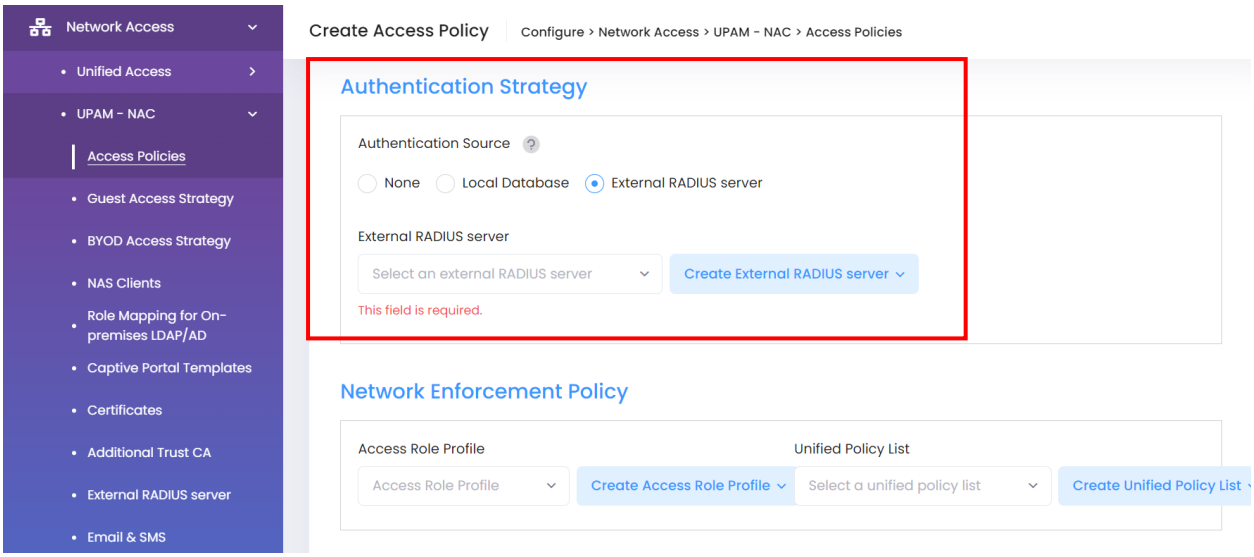


Figure 191: UPAM-NAC Access Policies – Omnivista Cirrus 10 (Authentication strategy)

Omnivista Cirrus 10 fully support backup to on premise AD server of customer and can manage preemption to this server if required.

240.	At least for a "Cloud scenario" as described previously [4], built-in RADIUS server as described previously [28] shall support following EAP types: EAP-MD5, EAP-TLS, EAP-AKA, EAP-PEAP, EAP-FAST, EAP-SIM, EAP-TTLS, EAP-GTC. When managed by a SaaS NMS cloud solution included in WLAN solution, for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Various EAP types are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution.

241.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall have the ability to utilize RADIUS attributes to assign each authenticated user/device to a specific ROLE. A role defines a VLAN and enforces security and QoS through the use of role-based ACLs and QoS policies that can be directly integrated with the roles defined within existing authentication servers. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. User role assignment from RADIUS attributes is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [31] for Omnivista 2500 NMS server.

242.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall include and handle a flexible and adaptive RADIUS attributes dictionary allowing to add an IETF or any vendor specific RADIUS attribute, when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. As depicted in following figure, the UPAM-NAC embedded RADIUS server available in *Wi-Fi Enterprise mode* with Omnivista Cirrus 10 can store multiple RADIUS attributes defined by the IETF, by *Alcatel-Lucent Enterprise*, or by any other vendor:

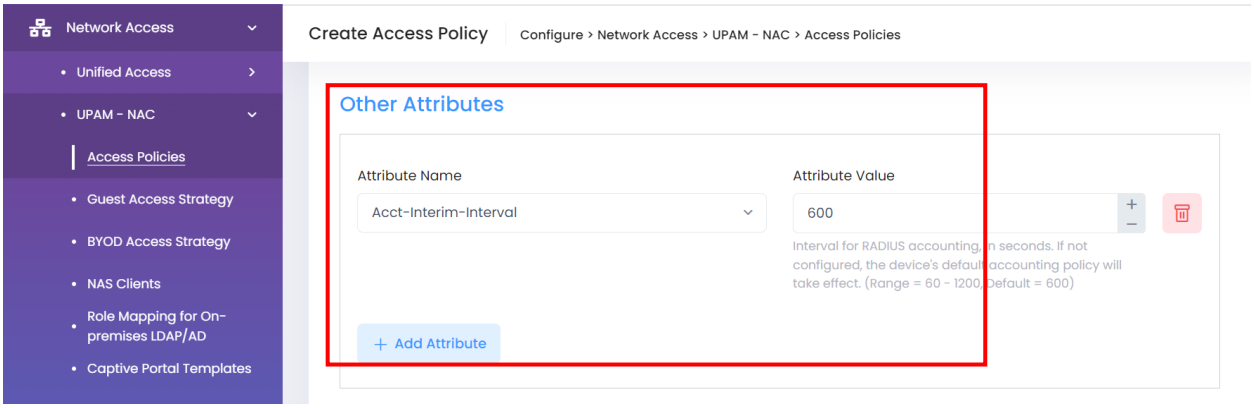


Figure 192: UPAM-NAC- Access Policies – Omnivista Cirrus 10 (RADIUS Attributes)

The RADIUS Attribute Dictionary enables UPAM to integrate with other vendor's network infrastructure and allows UPAM-NAC to act as a RADIUS server to authenticate user requests from Third-Party devices.

243.	If the built-in RADIUS server as described [28] shall interface with an external RADIUS server, then it shall be able to interface with multiple and distinct RADIUS servers depending on specific access conditions (SSID name, Access Point IP address, identity of the connecting user…). This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Interface with multiple external RADIUS is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [33] for Omnivista 2500 NMS server.

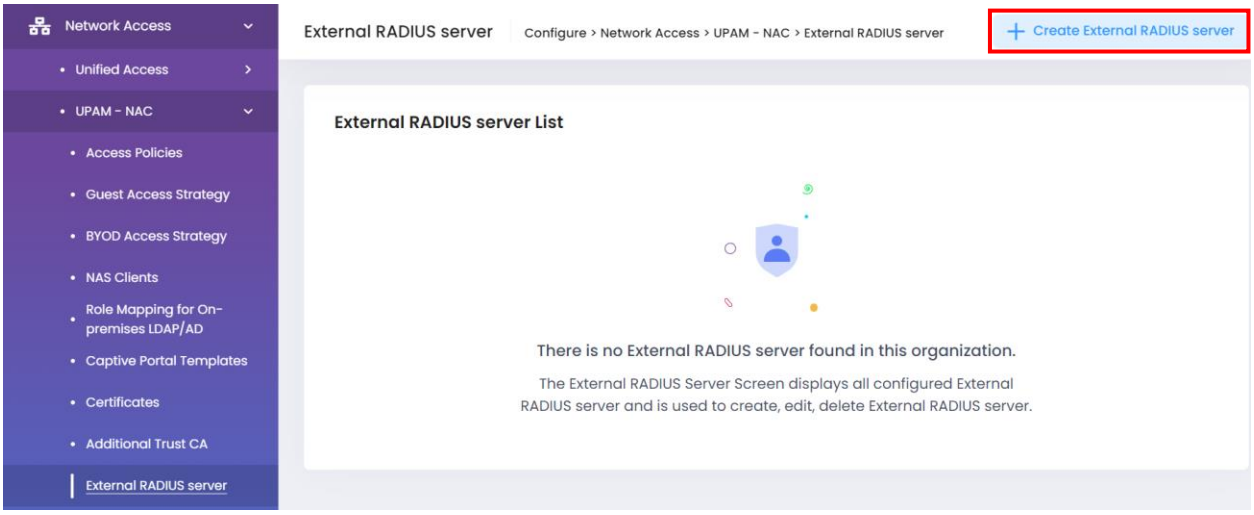


Figure 193: UPAM-NAC External RADIUS server – Omnivista Cirrus 10 (Create external RADIUS server)

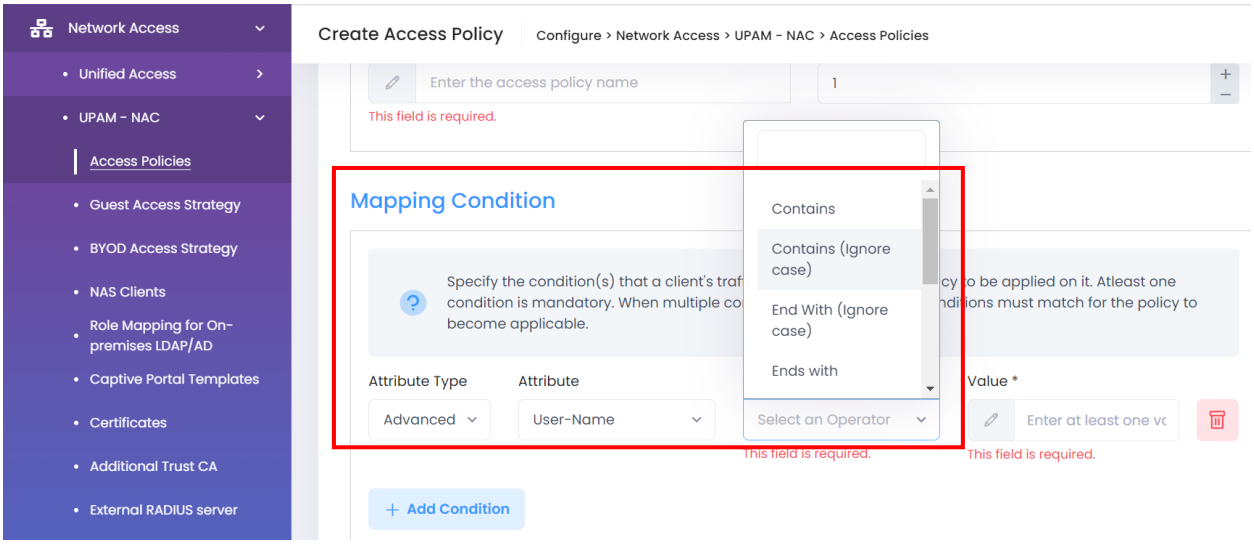


Figure 194: UPAM-NAC-Access Policy and mapping condition - Omnivista Cirrus 10 (mapping conditions)

244.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support following link layer encryption standards: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP, WPA3_PSK_SAE_AES, WPA3_SAE_AES. This when managed by a SaaS NMS cloud	C/PC/NC

	solution included in WLAN solution for XL/Multi-tenant site deployments, and this without third-party component for NMS management.	

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

245.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support the latest WPA3 encryption standard. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. WPA3 encryption is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [35] for Omnivista 2500 NMS server.

246.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support OWE encryption standard with open Wi-Fi networks. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. Wi-Fi Enhanced Open security standard based on Opportunistic Wireless Encryption (OWE) is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [36] for Omnivista 2500 NMS server.

247.	At least for a "Cloud scenario" as described previously [4], the wireless LAN solution shall support following 802.1x supplicants: Windows 7, 10 (and more), MAC OS, IOS, Android, Chromebook…. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

248.	At least for a “Cloud scenario” as described previously [4], the wireless LAN solution shall support time-based policy access to a SSID when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Time-based policy access to a SSID is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution.

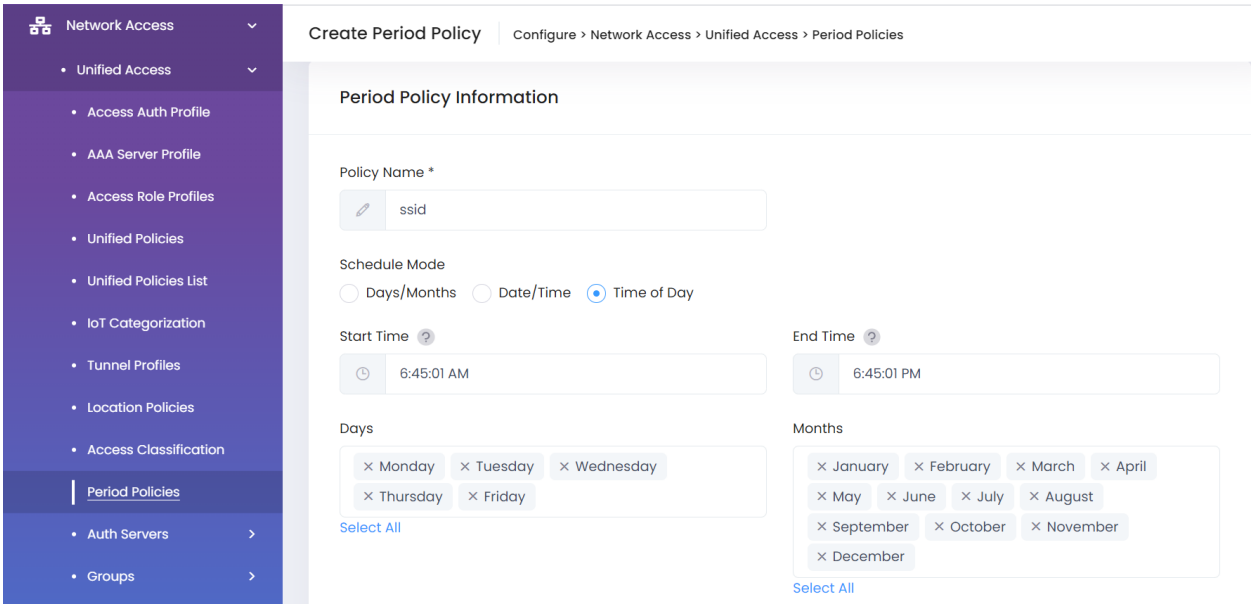


Figure 195: SSID time-based policy access - Omnivista Cirrus 10 (Period Policies)

249.	For the “Cloud” deployment model as described previously [4], the wireless LAN solution shall propose a “Guest” management solution based on an embedded and built-in Captive Portal providing web-based authentication for guests and visitors. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Guest management is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [39] for Omnivista 2500 NMS server.
Descriptions [250] to [265] depict the Guest access management with Omnivista Cirrus 10.

250.	The Guests Captive Portal included in the wireless LAN solution shall allow a customizable look & feel.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. The Captive Portal provided by UPAM-NAC in Wi-Fi *Enterprise mode* is fully customizable.

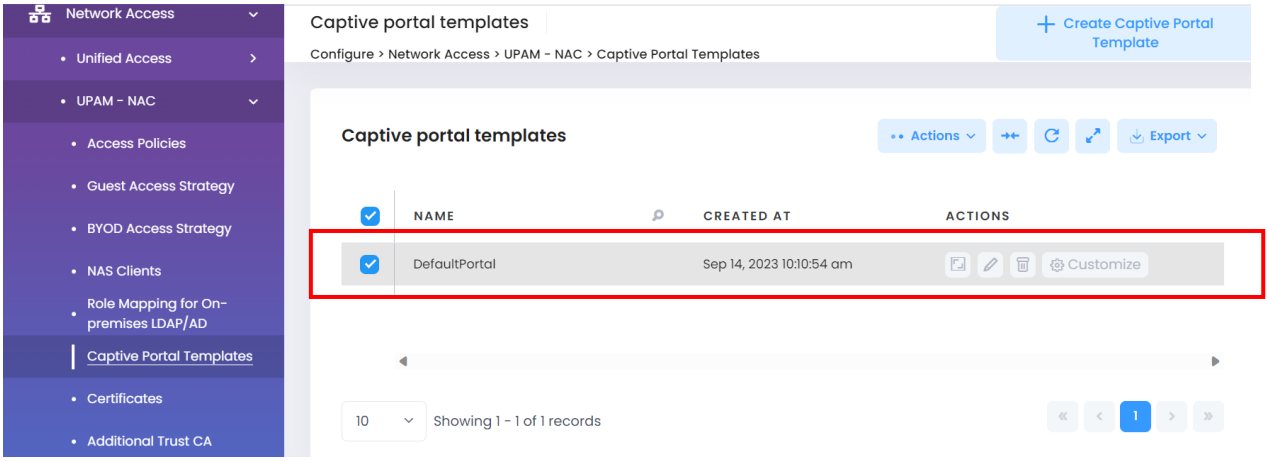


Figure 196: UPAM-NAC Captive Portal customization – Omnivista Cirrus 10 (Captive Portal Templates)

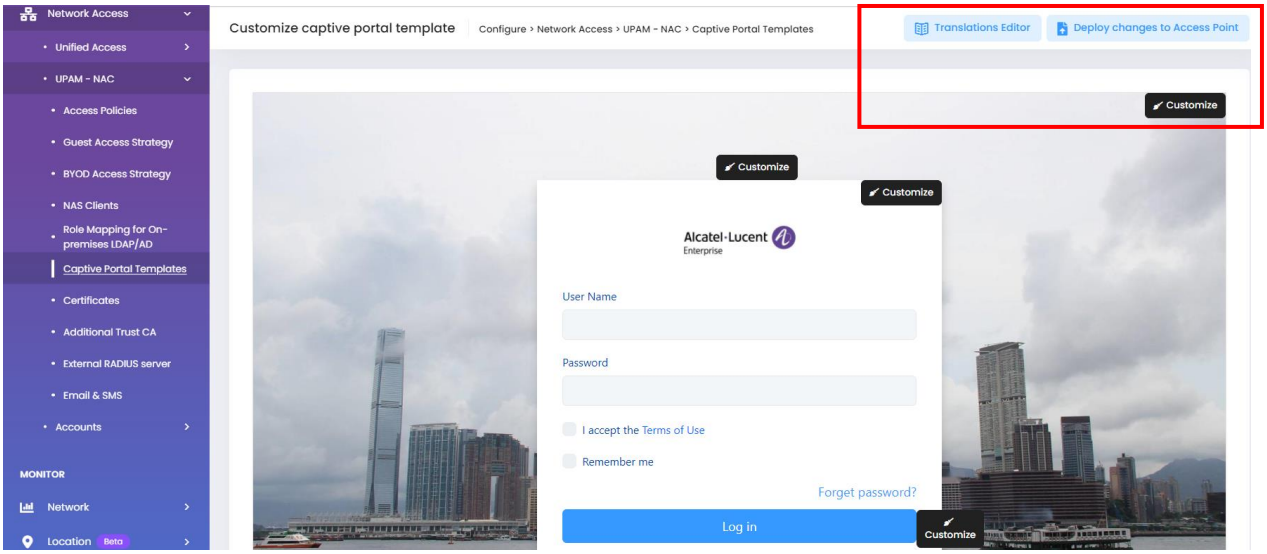


Figure 197: UPAM-NAC "Welcome page" customization – Omnivista Cirrus 10 (Captive Portal Templates)

251.	The Guest management solution shall allow, at least, following authentication methods: ▪ Username & Password ▪ Access Code ▪ Simple Term & Condition acceptance	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

252.	A least for a “Cloud” scenario as described previously [4], the Guest management solution shall allow guests to authenticate using their favorite social network account (supported social networks shall be listed).	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. A short description is done in [42] for Omnivista 2500 NMS server.

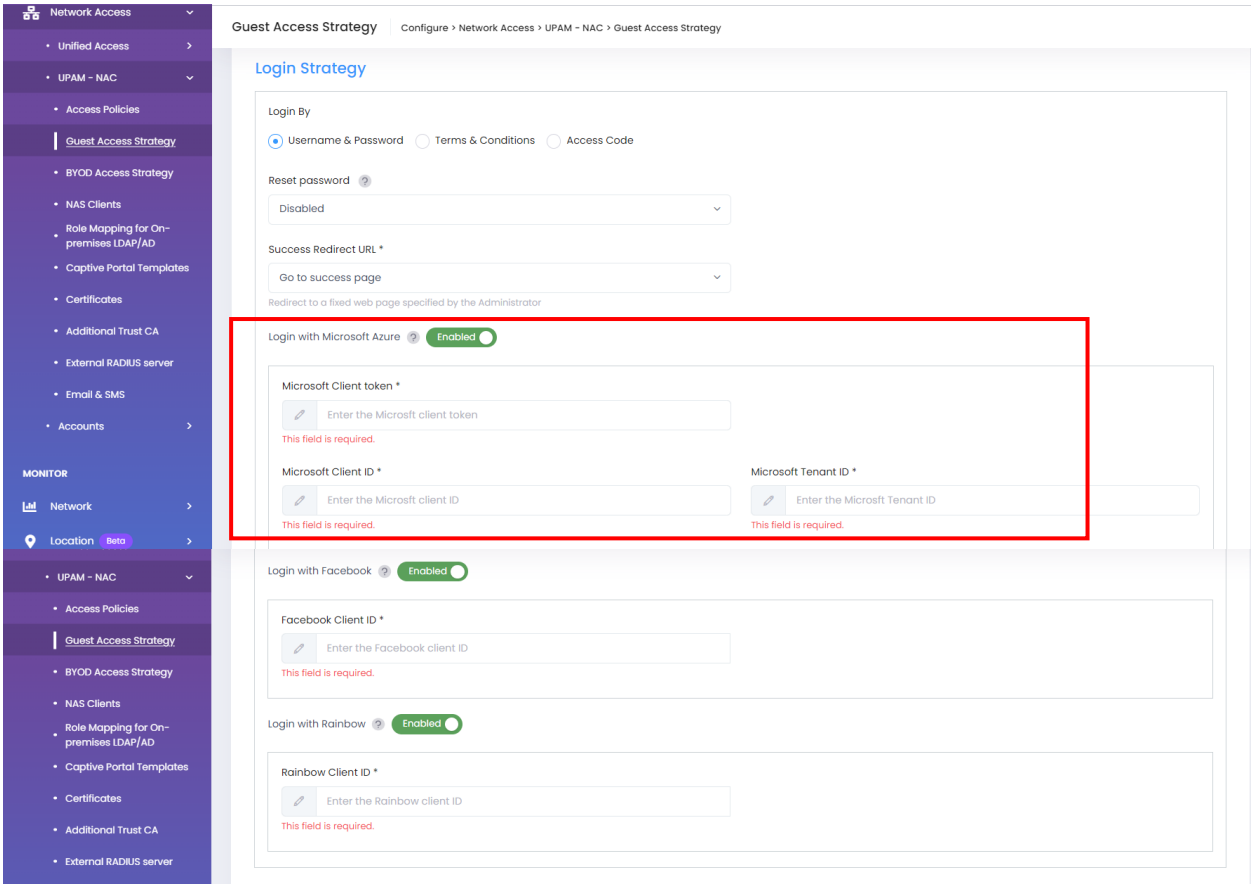


Figure 198 : Guests Social Login method – Omnivista Cirrus 10 (Guest Access Strategy)

253.	For the “Cloud” deployment model as described previously [4], the wireless LAN solution shall offer the possibility to build a walled garden environment (with configured domain names) for guest users before they authenticate.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

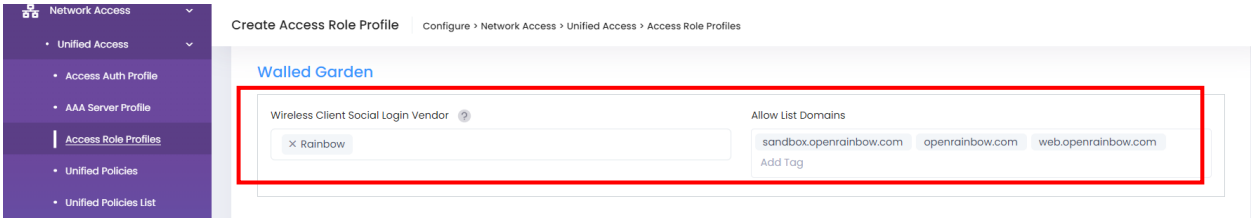


Figure 199: Walled Garden – Omnivista Cirrus 10 (Access Role Profile)

254.	The Guest management solution shall allow non-IT staff (e.g., a receptionist) to create temporary guest accounts.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

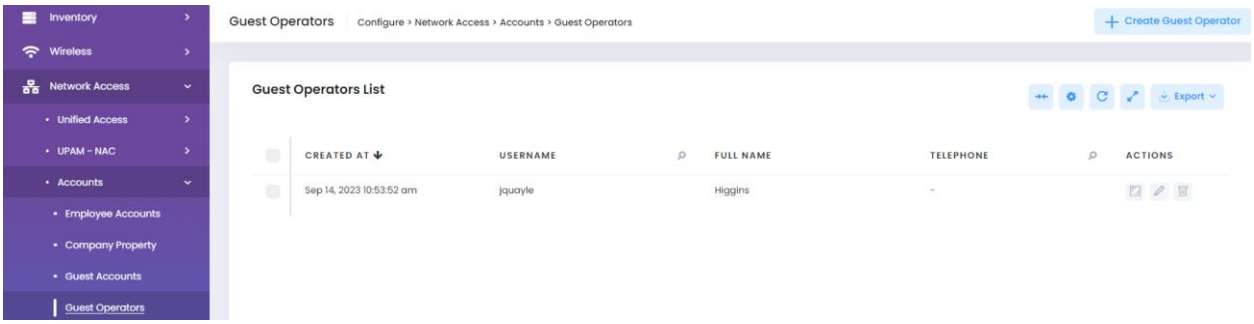


Figure 200: Guests Operator accounts creation – Omnivista Cirrus 10 (Guest Operators)

255.	A least for a “Cloud” scenario as described previously [4], the WLAN solution shall allow guest self-registration and employee sponsored access.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. A short description is done in [45] for Omnivista 2500 NMS server.

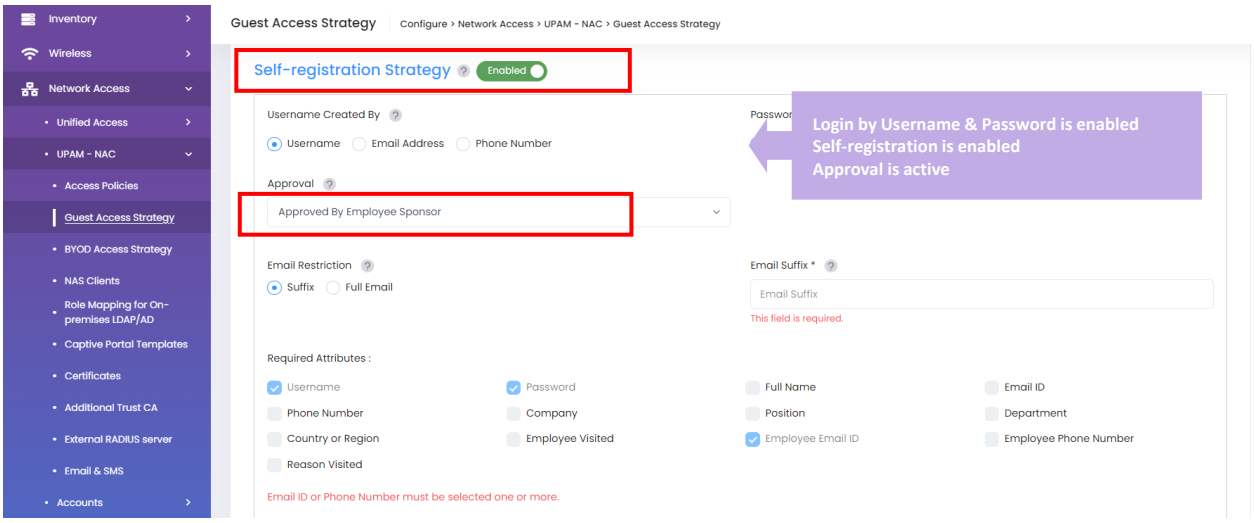


Figure 201: Guest self-registration – Omnivista Cirrus 10 (Guest Access Strategy)

256.	The WLAN solution shall allow guests accounts bulk provisioning by importing a file containing guest accounts information and shall propose a template import file.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

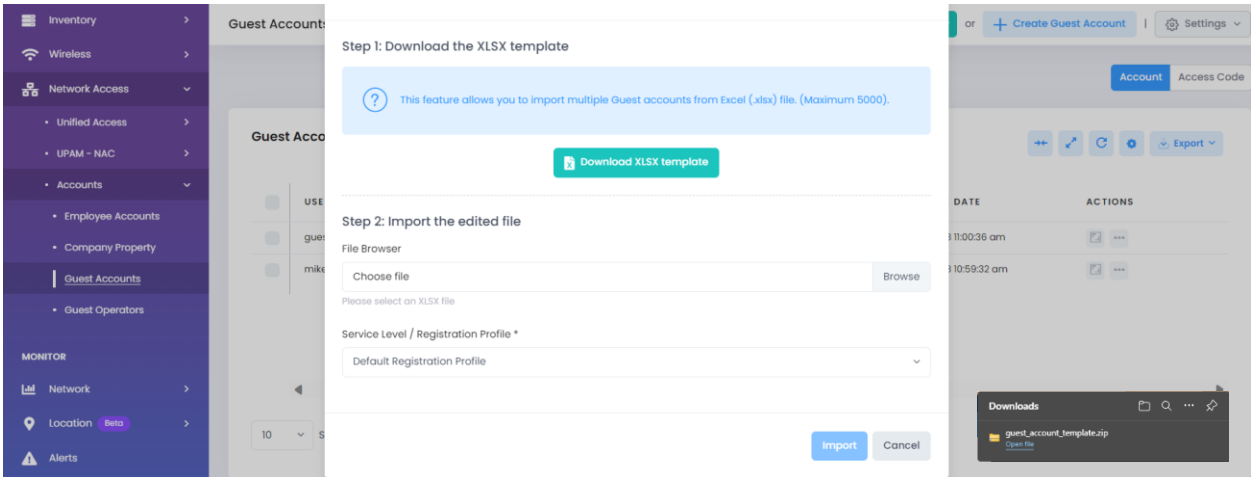


Figure 202: Guests accounts bulk import – Omnivista Cirrus 10 (Guest Accounts)

257.	A least for a "Cloud" scenario as described previously [4], the WLAN solution shall allow to create batch of guests accounts just by specifying a guest prefix and a number of accounts to be created.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

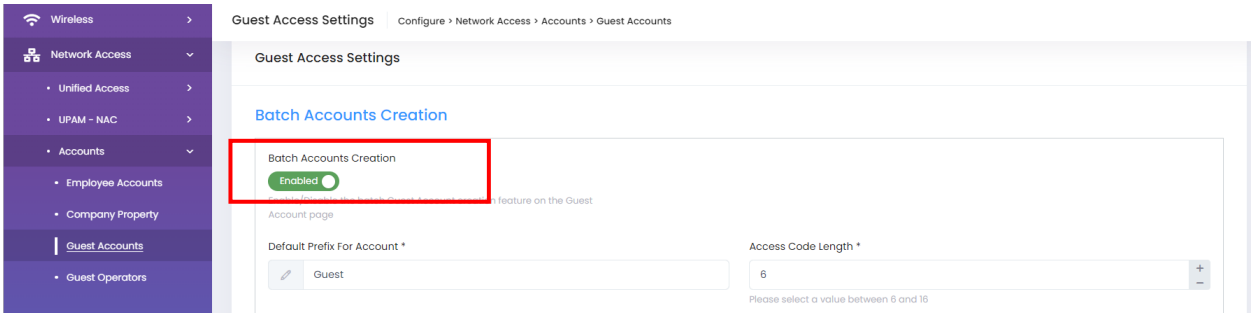


Figure 203: Guest accounts batch creation – Omnivista Cirrus 10 (Guest Accounts > Global Guest Access Settings)

258.	A least for a "Cloud" scenario as described previously [4], the WLAN solution shall allow to define networking SLAs (security, QoS…) to be applied to guest network connections.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

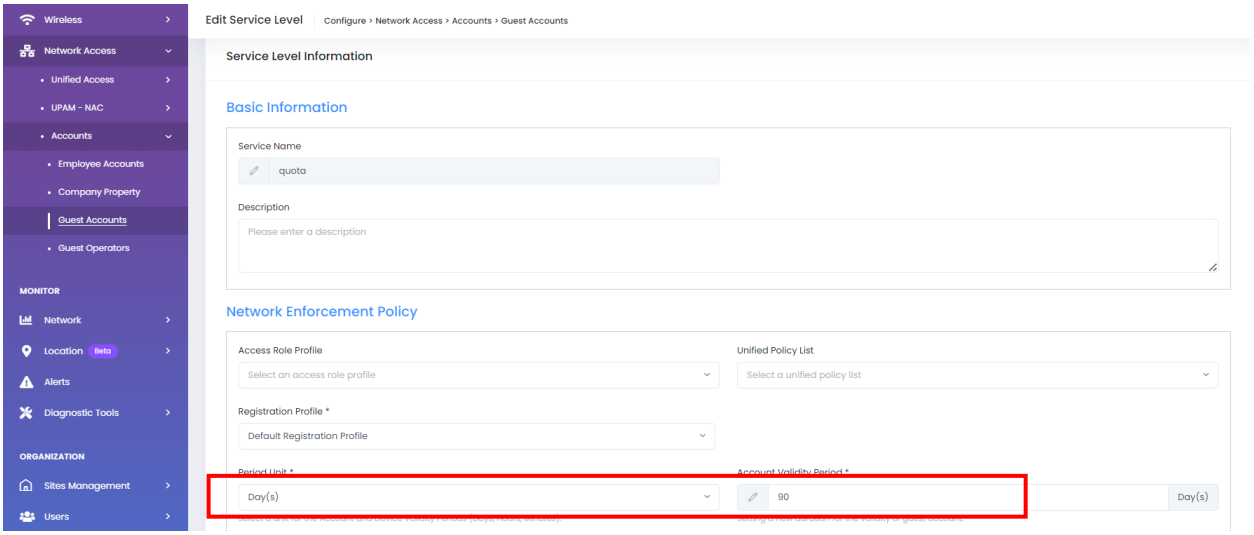


Figure 204 : Service Levels – Omnivista Cirrus 10 (Guest Accounts > Service Levels)

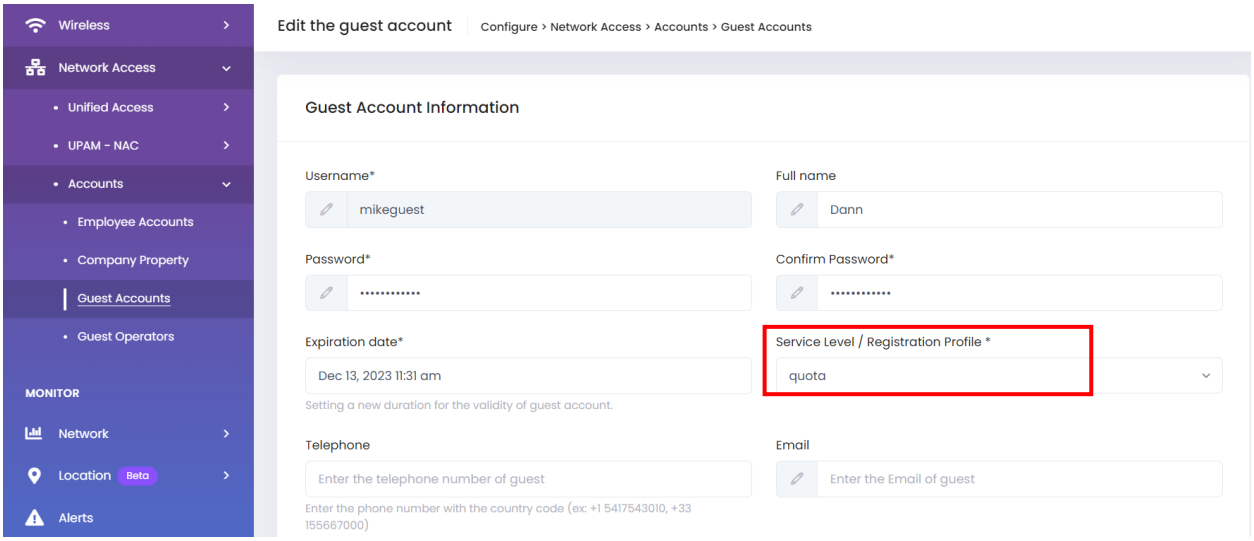


Figure 205: Service Level and Guest account – Omnivista Cirrus 10 (Guest Accounts)

259.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow to define and apply "data quotas" to guests to limit access based on total traffic consumed.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

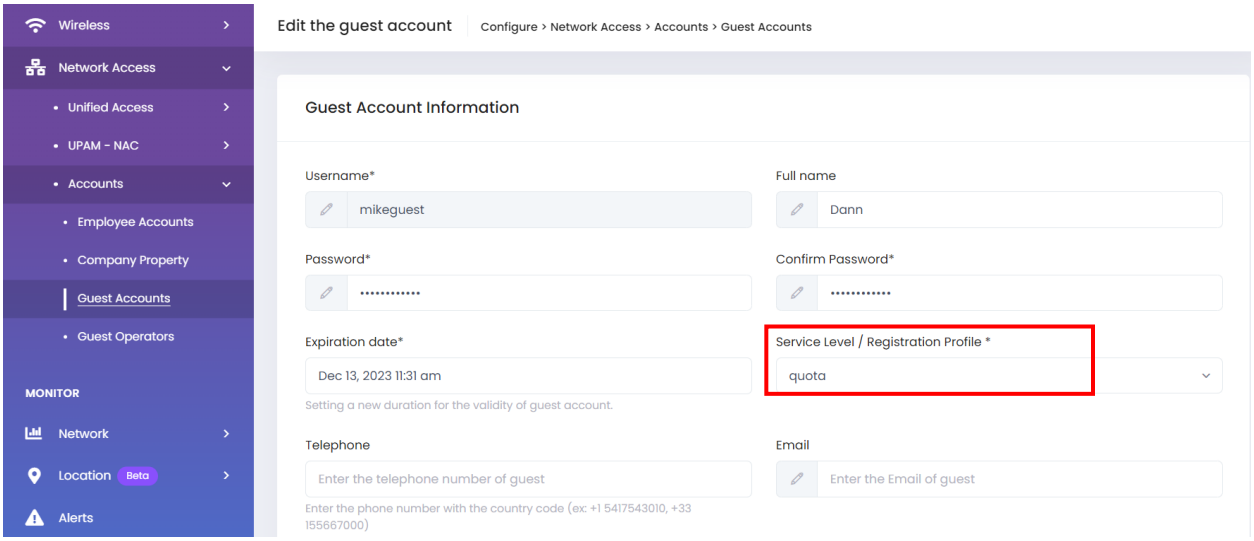


Figure 206: Guest data quota – Omnivista Cirrus 10 (Guest Accounts)

260.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow guests SMS notification.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

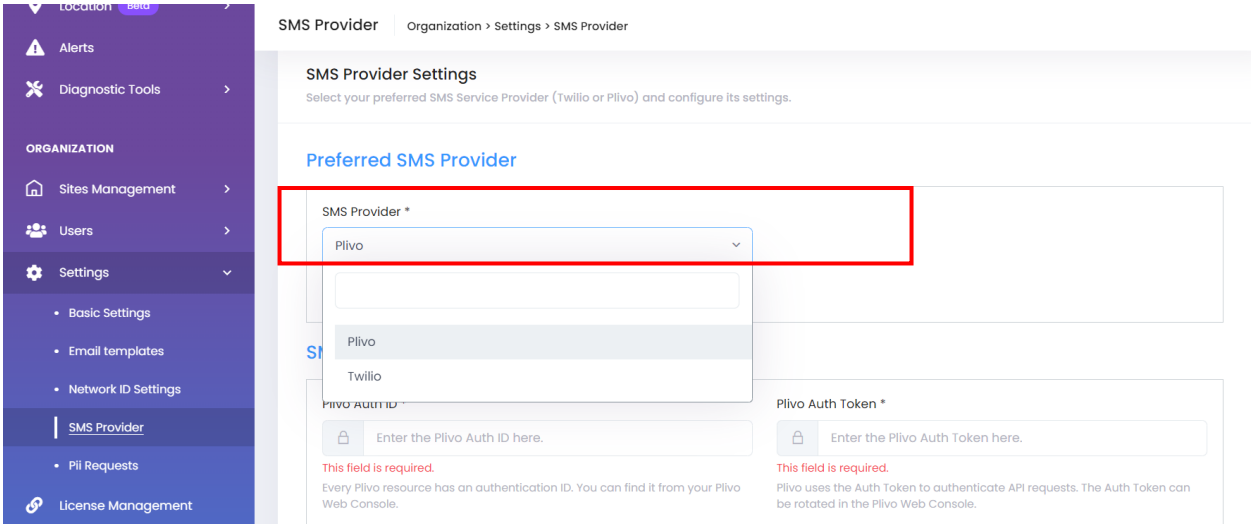


Figure 207: SMS Provider – Omnivista Cirrus 10 (SMS Provider)

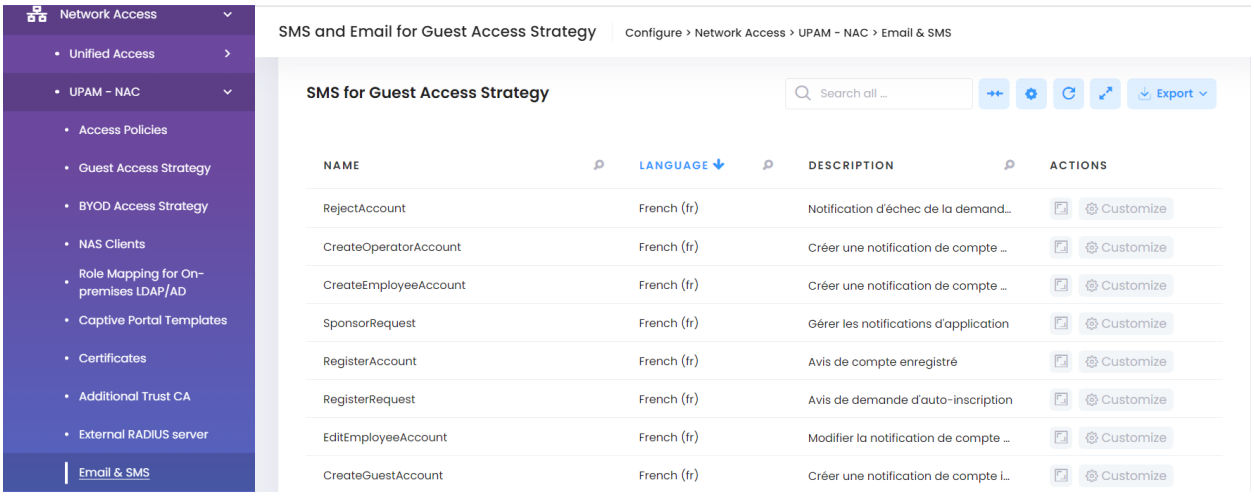


Figure 208: SMS for Guest Access – Omnivista Cirrus 10 (Email & SMS)

261.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow guests Email notification.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

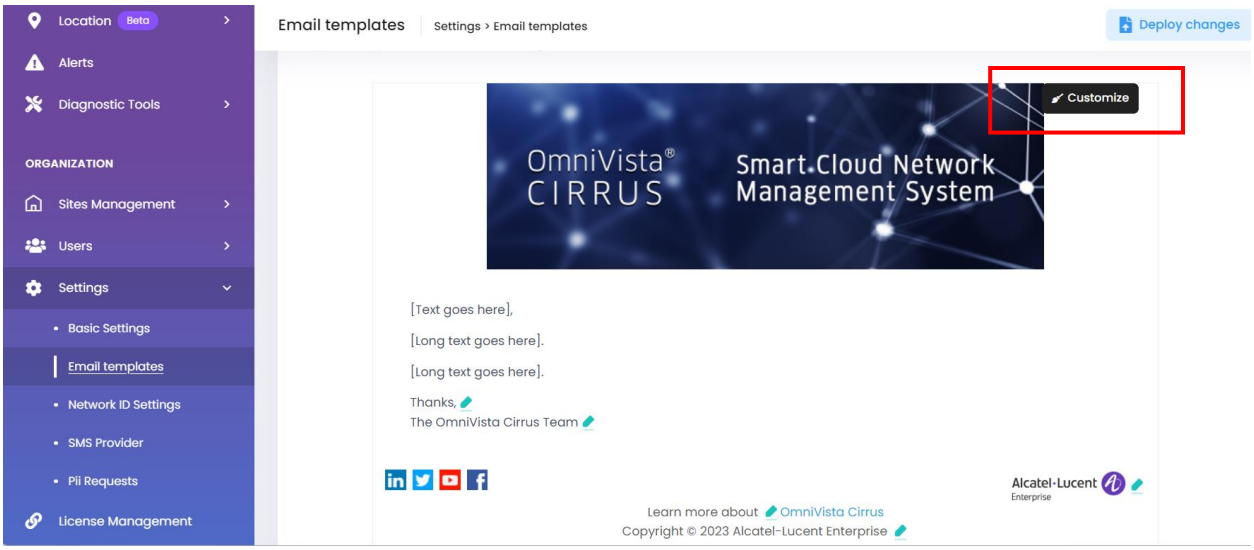


Figure 209 : Email templates – Omnivista Cirrus 10 (Email templates)

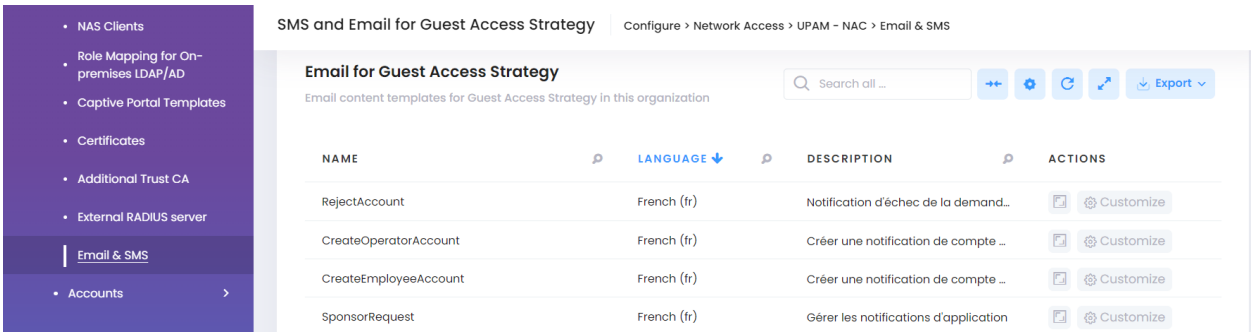


Figure 210: Email for Guest Access – Omnivista Cirrus 10 (Email & SMS)

262.	For the "Cloud" deployment model as described previously [4], the wireless LAN solution shall offer the possibility to interface with a third-party external Captive Portal for guest authentication, without necessarily forcing the traffic to through any server or appliance.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. Interface with a 3th-party external Captive Portal is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [51] for Omnivista 2500 NMS server.

263.	For a "Cloud deployment" scenario as described previously [4], the licensing model of the Guest management solution shall be based on the number of devices.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

264.	For a "Cloud deployment" scenario as described previously [4], the Guest management solution shall allow setting a validity period for an authenticated device, in order to avoid entering credentials each time a guest access the network.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

265.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall implement strict Guests traffic isolation.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*. Strict Guest traffic isolation is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [54] for Omnivista 2500 NMS server.

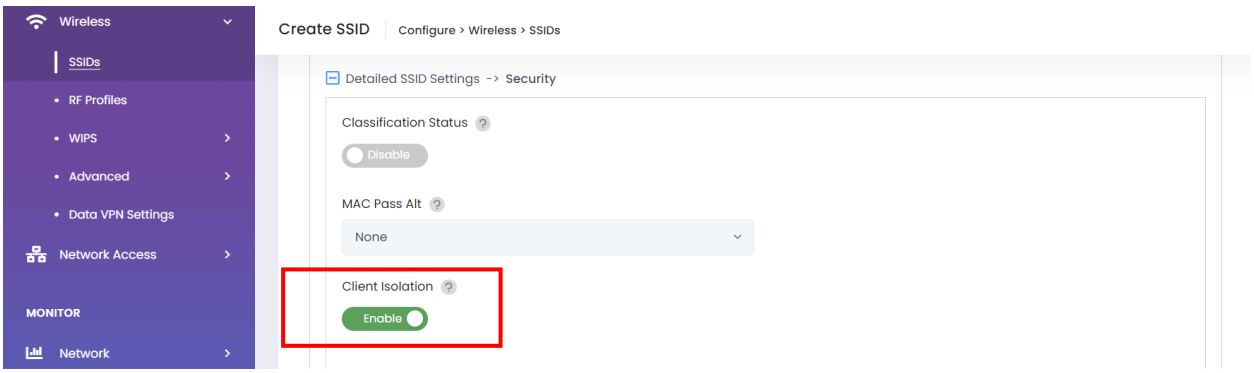


Figure 211: Guests isolation from each other – Omnivista Cirrus 10 (SSIDs)

266.	The WLAN solution shall allow data retention on user sessions when providing Guest Wi-Fi.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Wi-Fi Enterprise mode*.

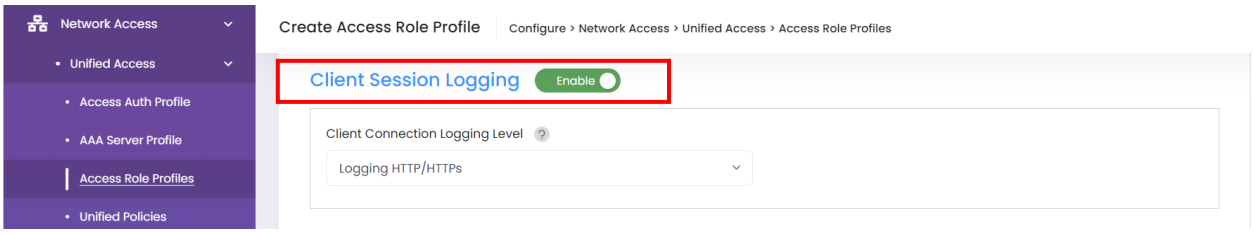


Figure 212: Client Behavior Tracking – Omnivista Cirrus 10 (Access Role Profile)

267.	In the framework of a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support BYOD and be able to provide device on-boarding that is as simple as possible. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. BYOD application included in UPAM-NAC module is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [56] for Omnivista 2500 NMS server.

268.	At least for a "Cloud deployment" scenario as described previously [4], the on-boarding process of employee devices shall be based on employee corporate accounts. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. The feature is included in BYOD application and is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution. A description is done in [57] for Omnivista 2500 NMS server.

269.	The BYOD application shall allow setting the validity period for the device, and the maximum number of devices per account. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

270.	The licensing model of the BYOD application shall be based on the number of on-boarded devices.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

271.	The WLAN solution shall support DSPSK to allow the use of different Pre-Shared Keys (PSK) for WPA2 encryption standard in the same SSID at the same time. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. DSPSK (Device-Specific PSK) is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [60] for Omnivista 2500 NMS server.

Ominivista Cirrus 10 introduces separate account management from UPAM-NAC, for the authentication of any employee, guest or operator. Administrator can choose either assisted key generation or manually specify a DSPSK key for the device and for the account managing the properties of the account.

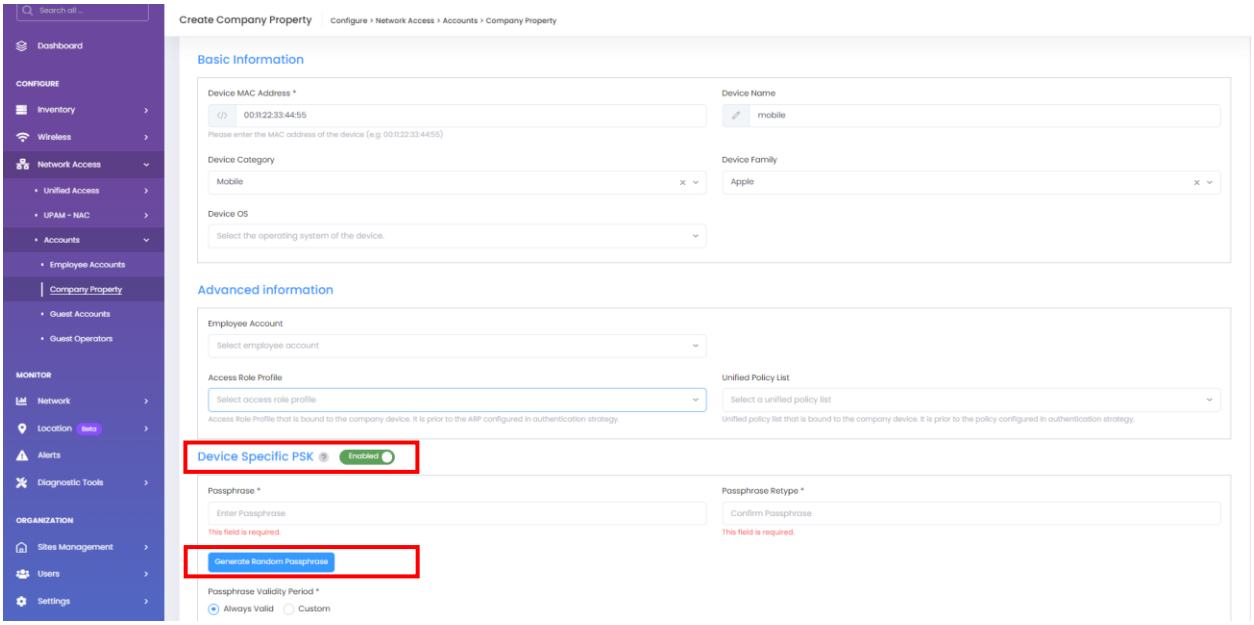


Figure 213: DSPSK generation with device MAC – Omnivista Cirrus 10 (Company Property)

272.	A least for a "Cloud" scenario as described previously [4], the WLAN solution shall support the WIFI4EU initiative from the EU. That includes support for Hotspot 2.0 (Passpoint® release 3Wi-Fi Alliance certification program). This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. WIFI4EU is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution. A description is done in [61] for Omnivista 2500 NMS server.

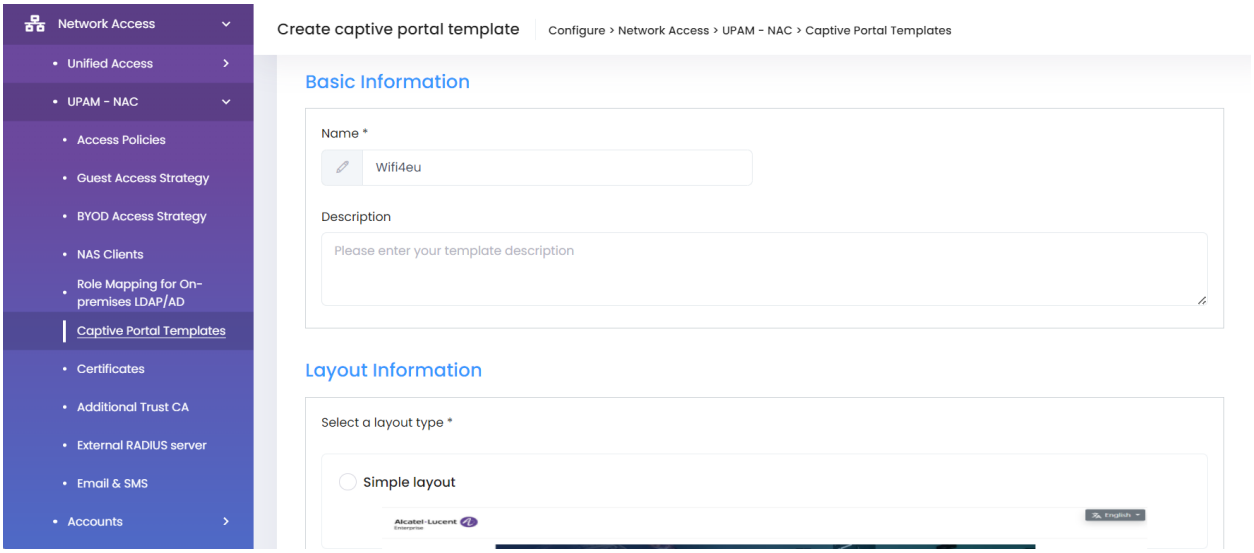
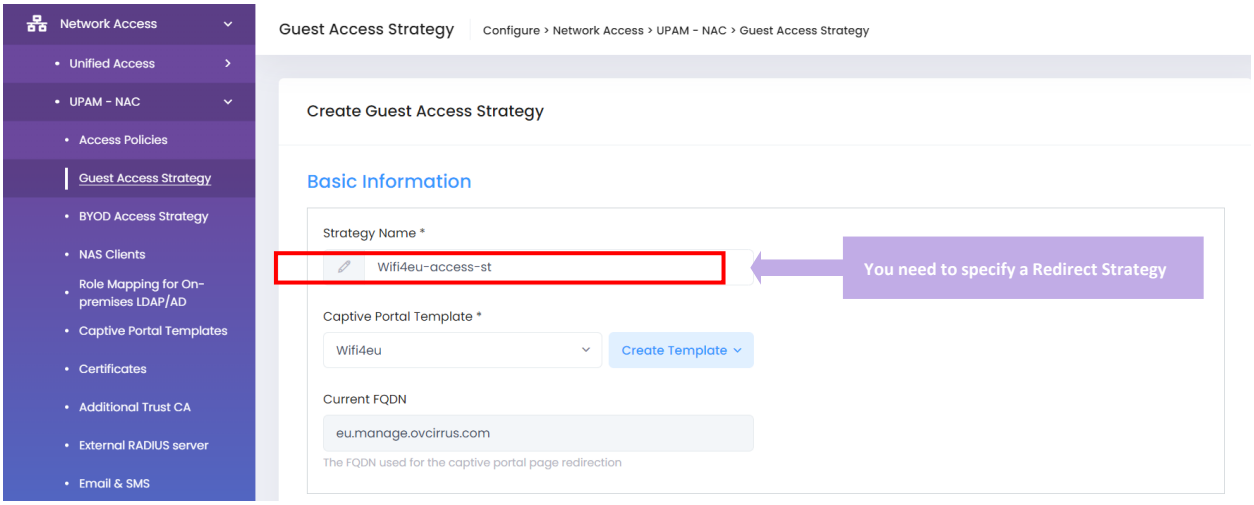


Figure 214: WIFI4EU Captive Portal template – Omnivista Cirrus 10 (Captive Portal Templates)



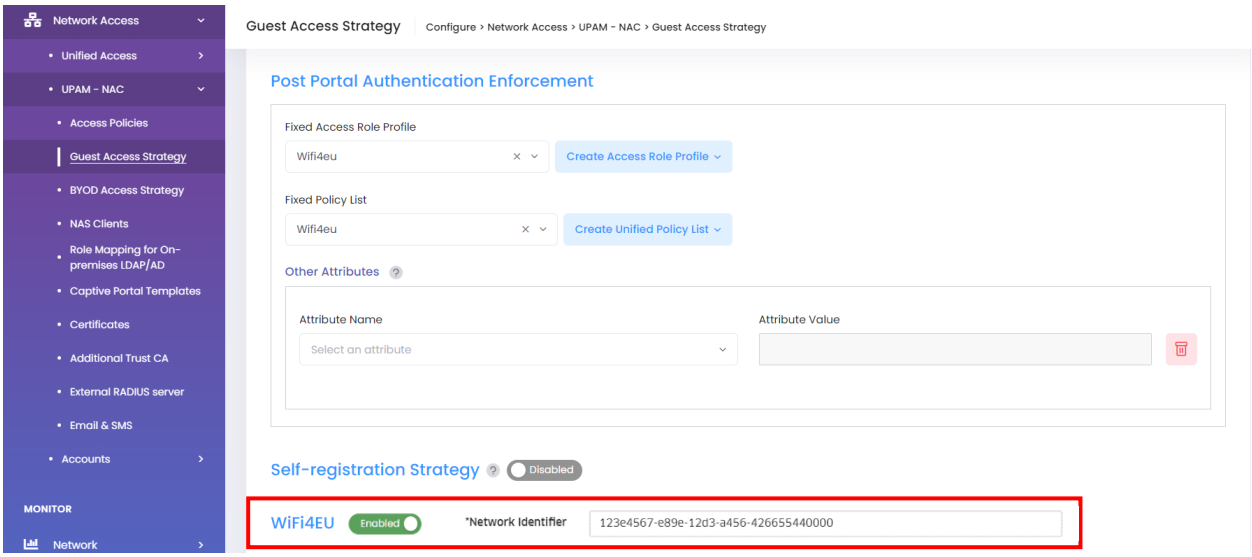


Figure 215: WIFI4UE Captive Portal snippet configuration – Omnvista Cirrus 10 (Guest Access Strategy)

273.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support the EDUROAM authentication hierarchy for Universities and Research Centers. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista Cirrus 10 are fully compliant with this requirement for Stellar XL/Multi-tenant deployments. The EDUROAM Authentication Hierarchy is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [62] for Omnivista 2500 NMS server.

5.2. RF Management

274.	In the framework of a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow automatic and/or manual RF management (channel and power). This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista Cirrus 10 are fully compliant with this requirement for Stellar XL/Multi-tenant deployments. *Radio Dynamic Adjustment™* (RDA) technology is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and is described in [64] for Omnivista 2500 NMS server.

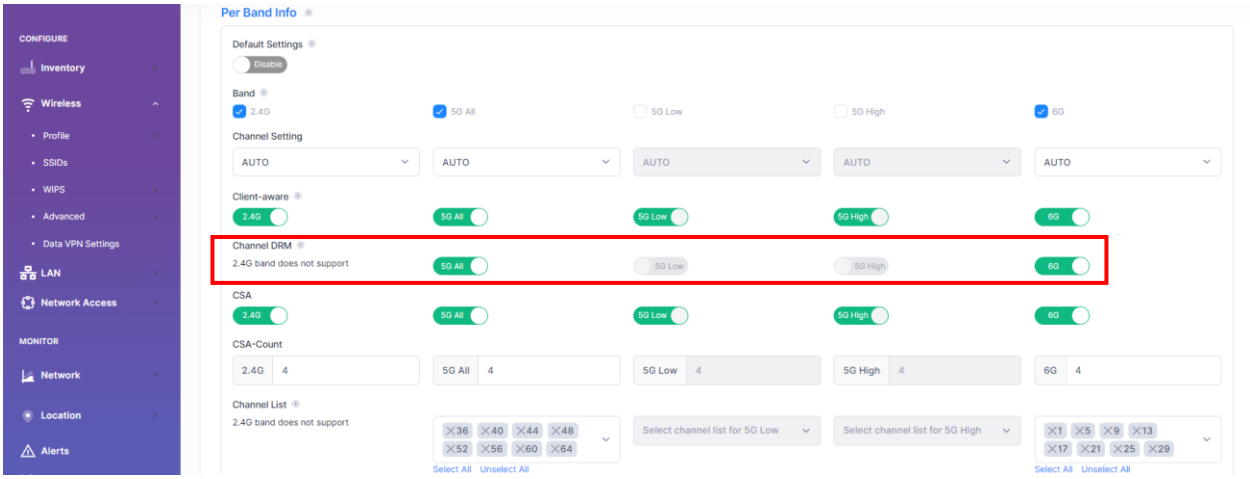


Figure 216: DRM with Channel List with tri-radio AP – Omnivista Cirrus 10 (RF Profiles)

Figure 217: DRM Time Control – Omnivista Cirrus 10 (RF Profiles)

275.	The WLAN solution shall support IEEE 802.11d standard in order to adapt channel and power levels to specific regulations of the geographical regions and countries to cover. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

Alcatel-Lucent OmniAccess Stellar WLAN and OmniVista Cirrus 10 are fully compliant with this requirement for Stellar XL/Multi-tenant deployments. Stellar Access Points support country information, to identify the regulatory domain where the access point is installed, along with other radio parameters such Frequency Hopping (FH). Stellar HW models exist to specifically support regulations for regions such as US HW model (US, Japan), ME HW model (Egypt, Israel) or RW HW model for any other country worldwide.

276.	The WLAN solution shall support IEEE 802.11h standard in order to adapt to regulatory constraints related to the use of the 5GHz frequency band. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10. Stellar Access Points implement IEEE 802.11h standard when

Stellar WLAN solution is managed by Omnivista NMS as a global solution, and description is done in [66] for Omnivista 2500 NMS server.

277.	The WLAN solution shall comply with different WLAN coverage classes defined for next-generation services deployed in the 6GHz frequency band when managed by a NMS cloud solution included in WLAN solution for multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10. Stellar Wi-Fi 7 Access Points manage transmit power and power range per band in the 6GHz when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and description is done in [67] for Omnivista 2500 NMS server.

278.	The WLAN solution shall support large width for sparse AP deployment when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Sparse AP deployment is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution, and description is done in [68] for Omnivista 2500 NMS server.

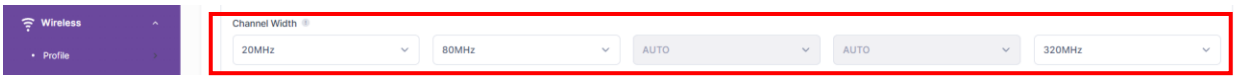


Figure 218: Ultra-Wide Channel selection with tri-radio AP – Omnivista Cirrus 10 (RF Profiles)

279.	The WLAN solution shall support most recent modulations for latest Dual-band clients when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Most recent modulations are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution.

280.	The WLAN solution shall support power saving functions for battery consuming clients or for clients with specific data transmission. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Power saving functions are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [71] for Omnivista 2500 NMS server.

281.	The WLAN solution shall minimize the airtime consumption in extremely dense environments where cell overlap is significant. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Basic Service Set coloring (BSS coloring) for 802.11ax OFDMA-based communications is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [72] for Omnivista 2500 NMS server.

282.	The WLAN solution must be compatible with previous 802.11ax (Wi-Fi 6/6E), 802.11ac (Wi-Fi 5) and 802.11b/g/n (Wi-Fi 4) standards and remains compatible in case of clients do not support fully the latest standards. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Compatibility with previous Wi-Fi standards is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [73] for Omnivista 2500 NMS server.

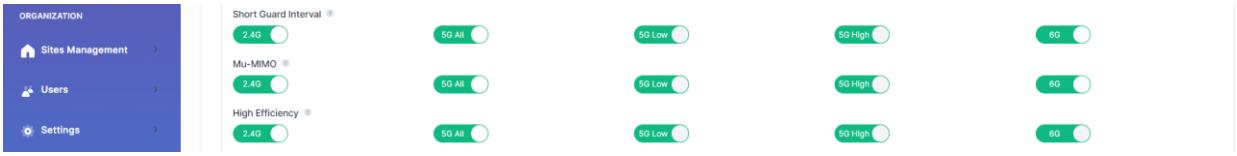


Figure 219: 802.11be, 802.11ax and MU-MIMO operation – Omnivista Cirrus 10 (RF Profiles)

283.	The WLAN solution shall support Short Guard Interval when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Short Guard Interval is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [74] for Omnivista 2500 NMS server.

284.	The WLAN solution shall support Long Guard Interval and Long symbol duration when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This without requiring third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Long Guard Interval and Long symbol duration are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [75] for Omnivista 2500 NMS server.

285.	The WLAN solution shall be smart enough to guide a new client to the optimal band/channel (2.4GHz/5GHz and 6GHz) considering, at a given time, both the number of associated clients on each band, and the medium utilization. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Guiding a new client to the optimal 2.4GHz/5GHz and 6GHz band/channel is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [76] for Omnivista 2500 NMS server.

286.	If no channel (2.4GHz/5GHz/6GHz) is overloaded (high medium utilization) or crowded (high client count), an AP shall by default guide a new client to the 5GHz/6GHz band. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10.

287.	Even if the 5GHz/6GHz band is not overloaded but is crowded (high client count), an AP shall guide a new client to the 2.4GHz band. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10.

288.	If a channel (2.4GHz/5GHz/6GHz) is overloaded (high medium utilization) and even if it is not crowded, an AP shall guide a new client to the less loaded band/channel. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10.

289.	If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilization) and no band/channel is crowded, an AP shall guide a new client to the 5GHz/6GHz band. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10.

290.	If all channels (2.4GHz/5GHz/6GHz) are overloaded (high medium utilization) and the 5GHz is crowded, an AP shall guide a new client to the 2.4GHz band. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10.

291.	The WLAN solution must be able to guide a new client to the appropriate channel (5GHz/6GHz) when connecting to access points supporting the 6GHz band separately (Wi-Fi 6E), considering the capability of client to connect to this frequency band. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Prioritize connection on 6GHz band is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [82] for Omnivista 2500 NMS server.

292.	The WLAN solution must be able to guide a new tri-band client to the appropriate resources and channels (2.4GHz/5GHz/6GHz) when connecting to access points that support aggregation of these bands (Wi-Fi 7 access points), considering the capability of client to connect to these aggregated resources. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Multi-Link operations on 2.4GHz/5GHz/6GHz bands are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [83] for Omnivista 2500 NMS server.

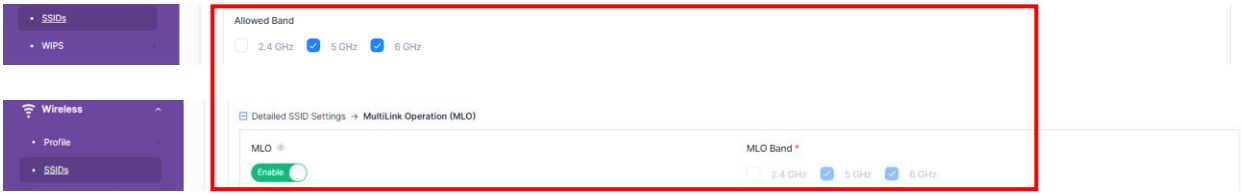


Figure 220: MLO operation with tri-band radio AP – Omnivista Cirrus 10 (SSIDs)

293.	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Smart/dynamic load balancing is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [84] for Omnivista 2500 NMS server.

294.	The WLAN solution shall force clients to the 5GHz (or 6GHz) only when there are dual band capable. The WLAN solution shall force clients to the 5GHz only when they are dual band capable and shall force clients to the 6GHz only when they are Wi-Fi 6E capable. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10, in *Wi-Fi Enterprise mode* as depicted in following figures:

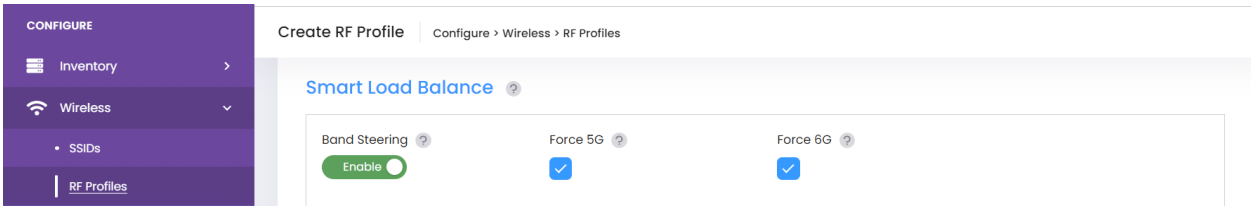


Figure 221: 5GHz and 6GHz forcing for dual band clients – Omnivista Cirrus 10 (RF Profiles)

295.	The WLAN solution shall deny connection to an AP when the signal of the client becomes too weak and disconnect a client to force it to roam when the signal becomes too weak. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Indeed, the OmniAccess Stellar WLAN solution allows to set RSSI (*Received Signal Strength Indication*) thresholds in decibels in order to optimize connectivity by forbidding client access to the network when the signal is too weak or by disconnecting a client (forcing it to roam) when the signal becomes too weak.

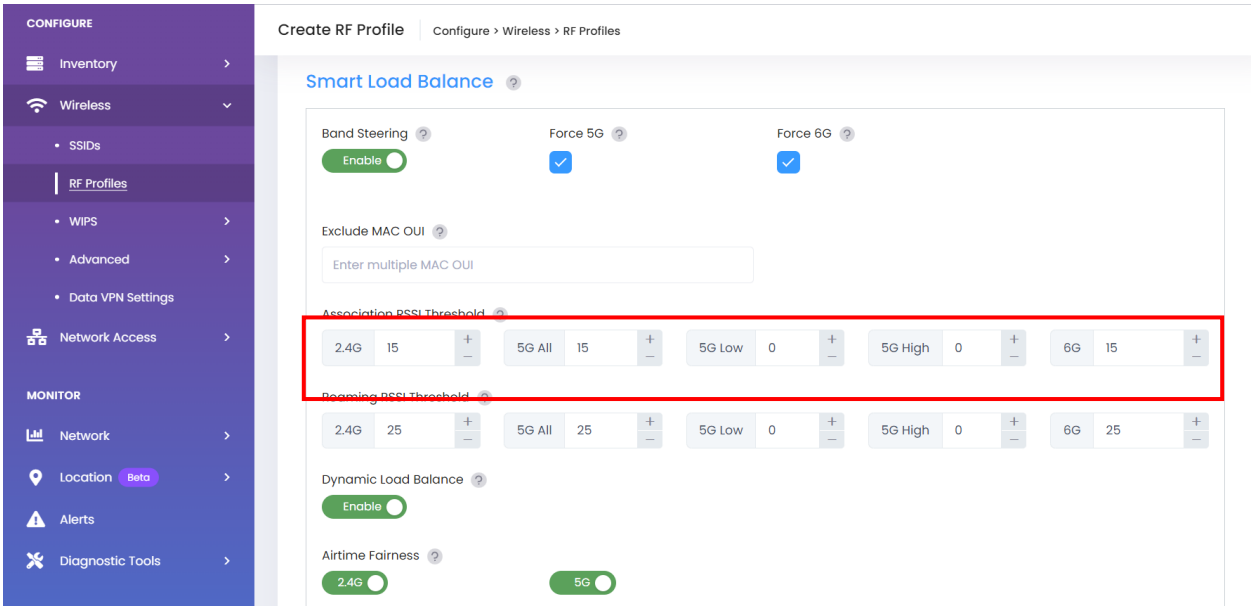


Figure 222: Per-band Association and Roaming RSSI Thresholds – Omnivista Cirrus 10 (RF Profiles)

296.	The WLAN solution shall support the IEEE 802.11v and 802.11k standards to facilitate network guided roaming. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. 802.11v and 802.11k are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [87] for Omnivista 2500 NMS server.

Both standards are supported in Omnivista Cirrus 10 as depicted in the following figures:

Figure 223: IEEE 801.11k & 802.11v support – Omnivista Cirrus 10 (SSIDs)

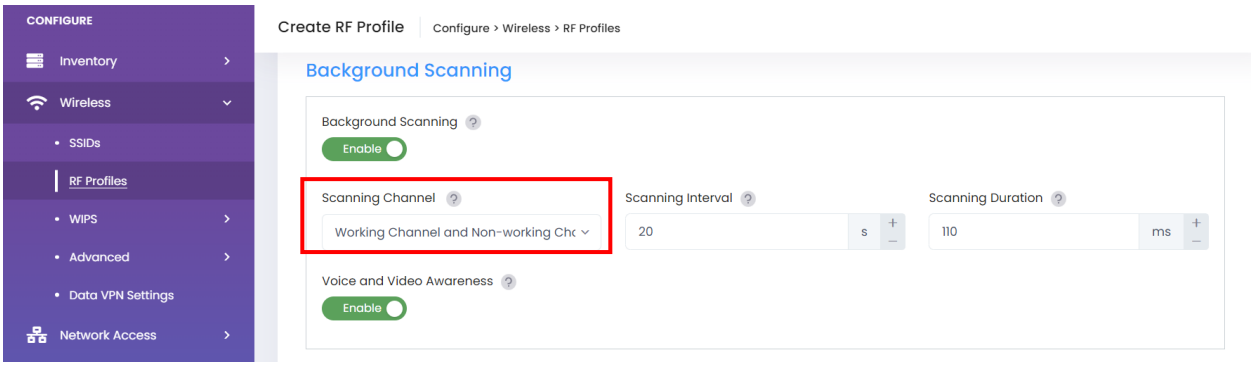
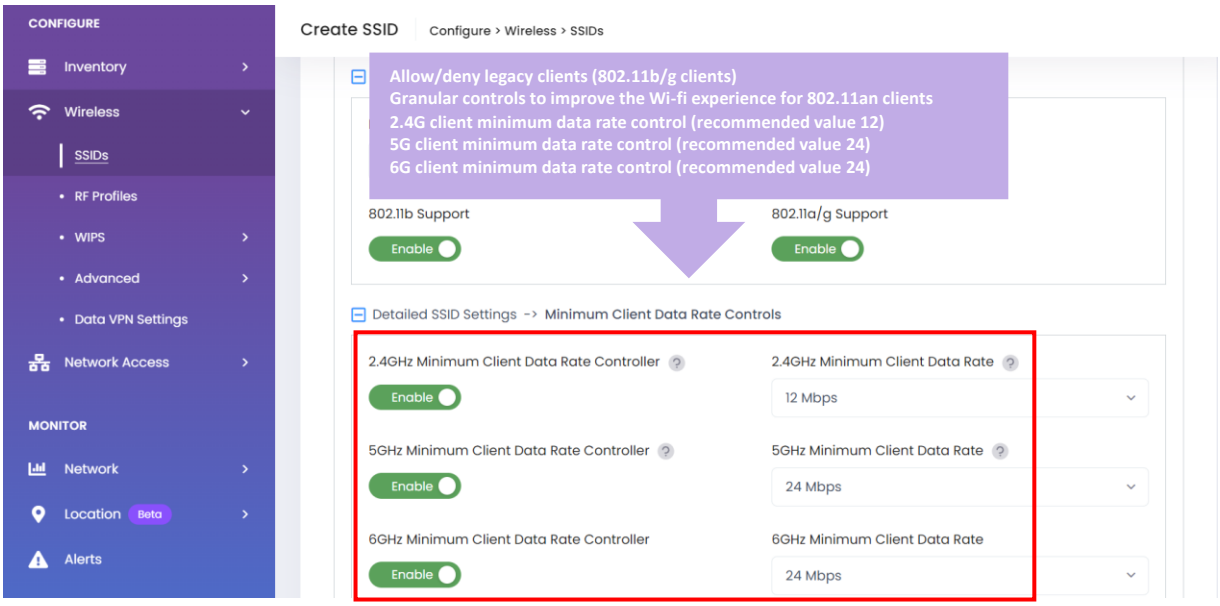


Figure 224: Background scanning for 802.11k/v support – Omnivista Cirrus 10 (RF Profiles)

297.	The WLAN solution shall support data rate control to encourage clients to roam at higher rates. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Data rate control is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [88] for Omnivista 2500 NMS server.



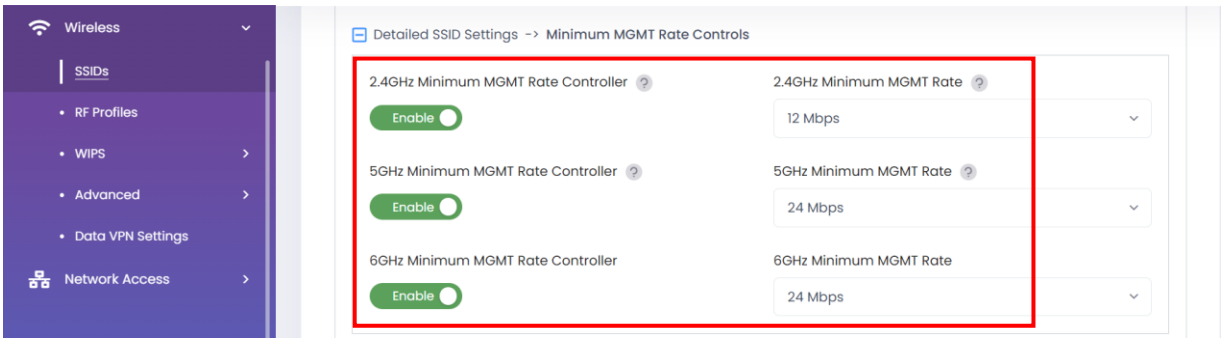


Figure 225: Minimum Data Rates Control - Omnivista Cirrus 10 (SSIDs)

298.	The WLAN solution shall propose APs that have the ability to scan the air in order to provide interfering/rogue APs and wireless attacks detection and shall not rely on external scanning equipment. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Background scanning is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [89] for Omnivista 2500 NMS server.

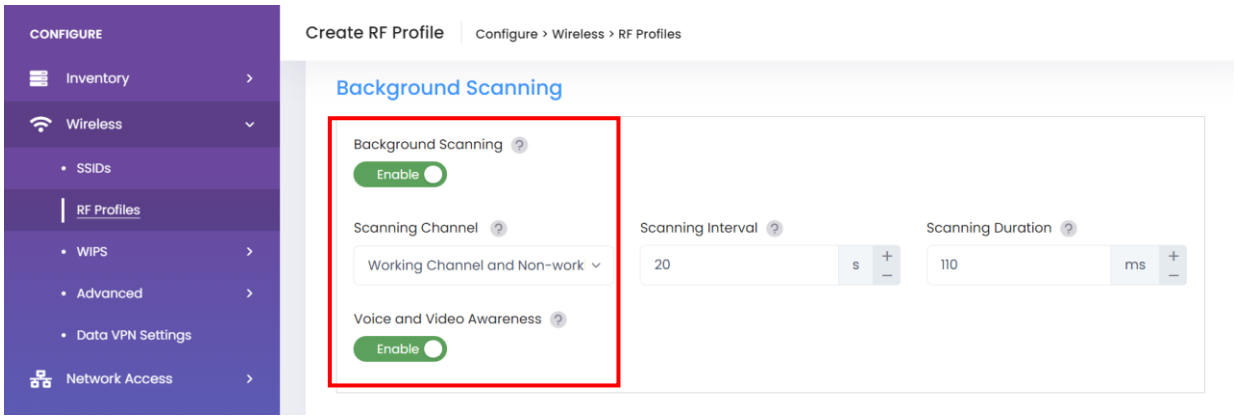


Figure 226: Background Scanning support – Omnivista Cirrus 10 (RF Profiles)

299.	The scanning function of the APs shall not impact active voice or video calls (SIP and H.323). The scanning function of the APs shall not impact active voice or audio/video calls (SIP, H.323 or proprietary). This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Voice and video

awareness is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [90] for Omnivista 2500 NMS server.

300.	At least for the 5GHz/6GHz band, the WLAN solution shall allow to define the list of channels which can participate in dynamic configuration. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

The list of authorized channels can be defined in *Wi-Fi Enterprise mode* through *RF profiles* which can then be applied to OmniAccess Stellar Access Points directly or via AP-Groups:

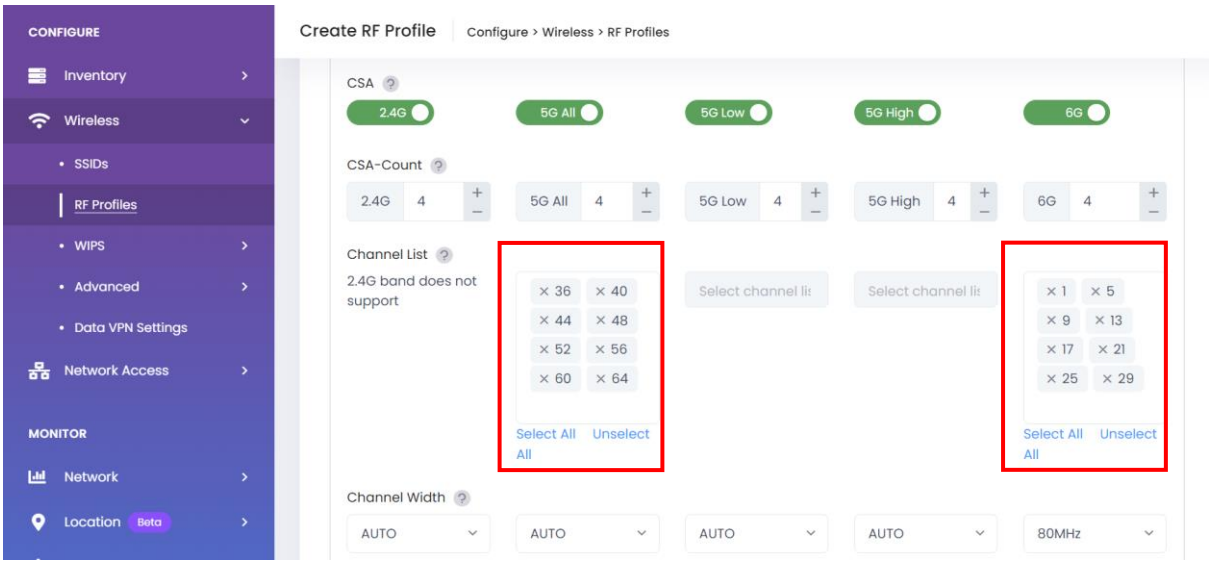


Figure 227: Authorized Channel List definition – Omnivista Cirrus 10 (RF Profiles)

301.	The WLAN solution shall allow to define a range of transmit power per band (min & max) even if power settings are configured for automatic and dynamic assignments. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. All *Enterprise modes*, with power settings set as “automatic”, allow to configure a range of transmit power per band (min & max). The auto power selection algorithm then selects the transmit power of the AP within the minimum and maximum specified.

The range of transmit power per band can be defined in *Wi-Fi Enterprise mode* through *RF profiles* which can then be applied to OmniAccess Stellar Access Points directly or via AP-Groups:

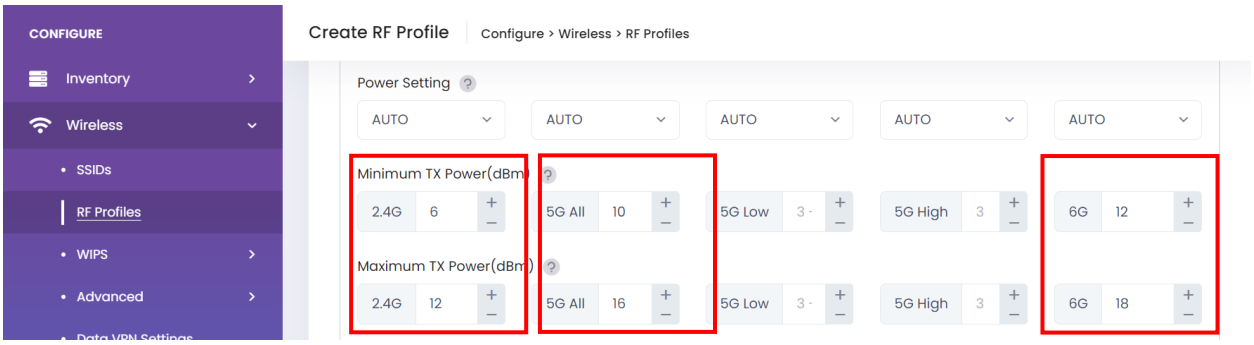


Figure 228: Min & max automatic transmit power – Omnivista Cirrus 10 (RF Profiles)

OmniAccess Stellar transmit power management feature is also known as DFS/TPC feature for the control of transmitted power for outdoor using the UNII-2 5GHz DFS sub-band.

302.	The WLAN solution shall propose Access Points which can all be configured and deployed in a dedicated scanning mode. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. In *Wi-Fi Enterprise mode*, OmniAccess Stellar AP15xxs, AP14xxs, AP13xxs and AP12xxs can be set to examine the radio frequency environment in which the Wi-Fi network is operating by analyzing all channels, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel. In *Wi-Fi Enterprise mode*, scanning mode can be enabled permanently or for a one-shot scan.

The picture below show an AP managed by Omnivista Cirrus 10, with dedicated scanning enabled

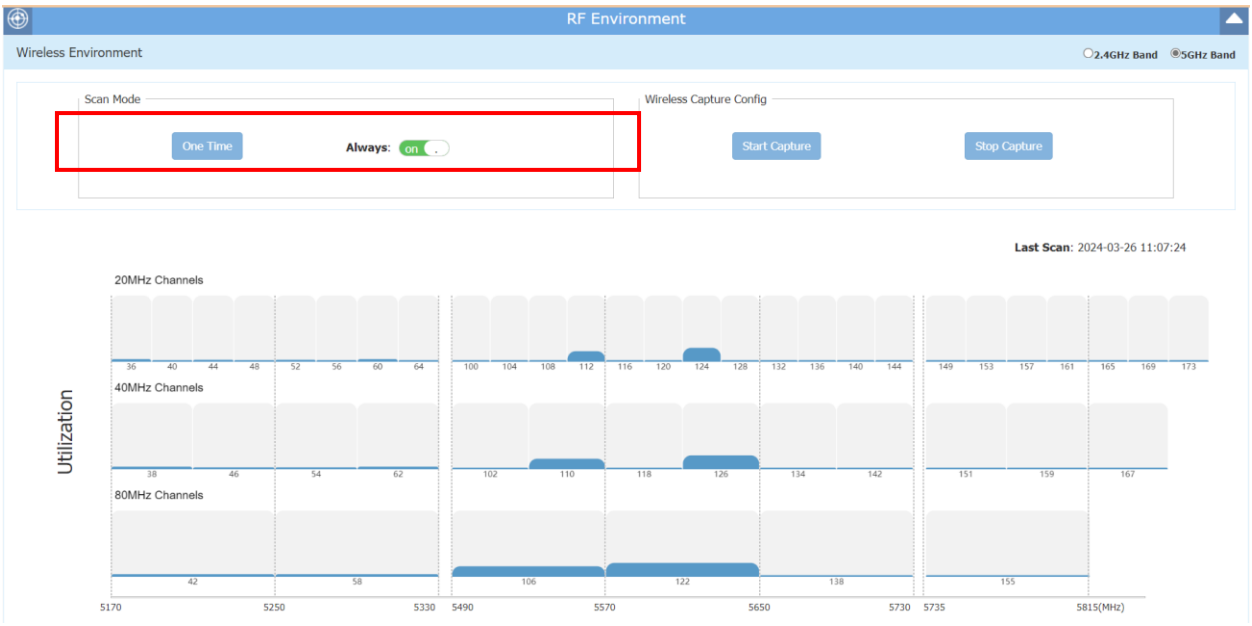


Figure 229: AP dedicated Scanning Mode activation – AP Web (RF environment)

303.	The WLAN solution shall propose Access Points with wireless packet capture capabilities. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Wireless packet capture is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [94] for Omnivista 2500 NMS server.

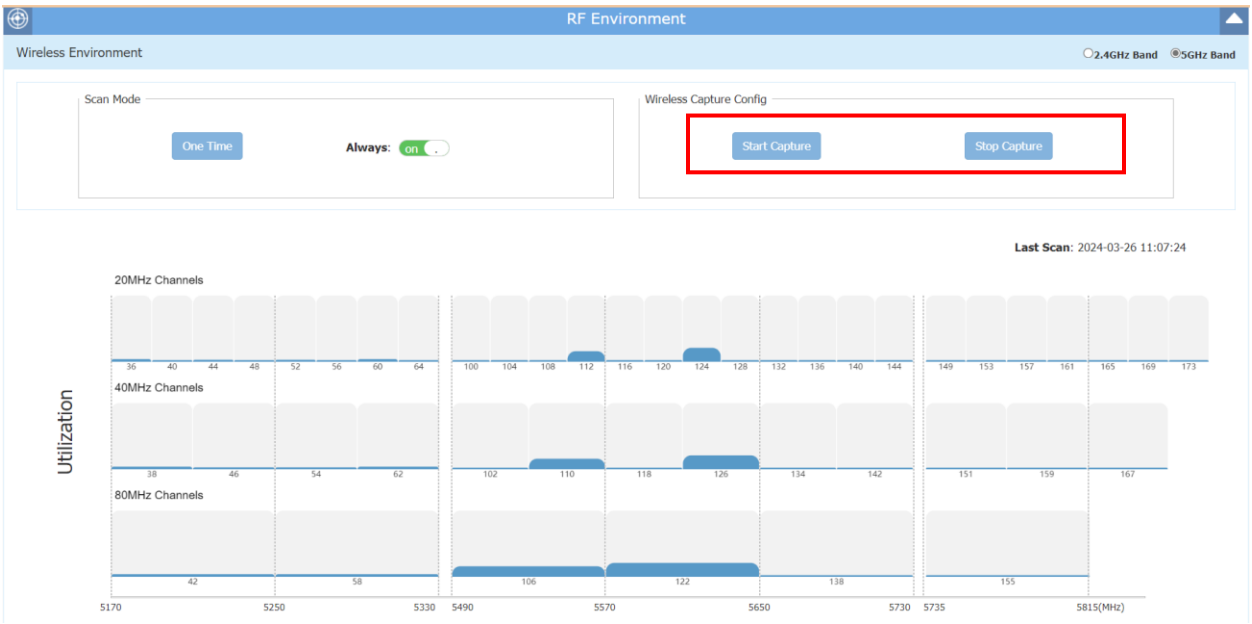


Figure 230: AP dedicated Wireless Capture – AP Web (RF environment)

304.	The WLAN solution shall make it simple to review the roaming history for a given client device. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments, by allowing to easily trace clients roaming behavior and Quality of Experience (QoE) for devices connectivity. As shown in following figure with Omnivista 2500, the *Wi-Fi Enterprise mode* provides the time of roaming and RSSI historical information over a completely customized time range. For each roaming occurrence, Roaming AP, Association Time, Band and RSSI are recorded. With more resources in the Cloud *Wi-Fi Enterprise mode* offers Up to 30 days of roaming & RSSI history:

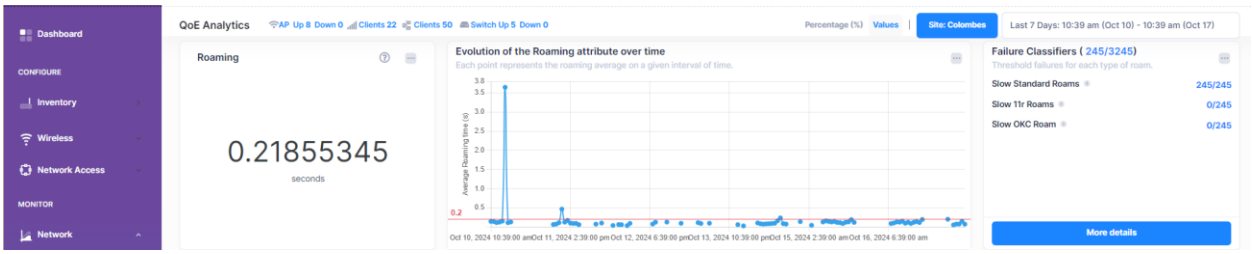


Figure 231: Evolution of roaming over time and client RSSI History (QoE and client analytics)

305.	The WLAN solution shall allow long interval background scanning, when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Long interval background scanning is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [96] for Omnivista 2500 NMS server.

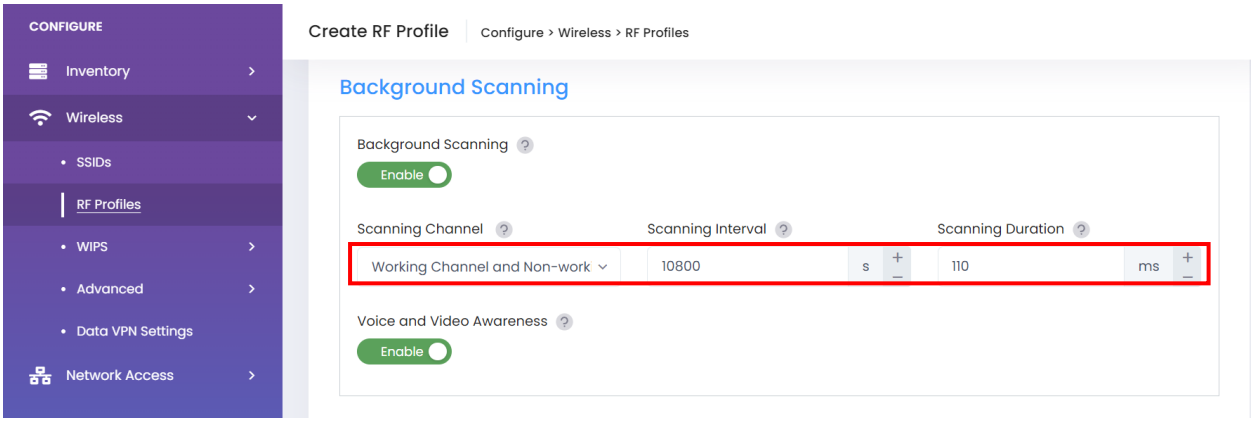


Figure 232: Long Interval Background Scanning – Omnivista Cirrus 10 (RF Profiles)

5.3. Intrusion Detection and Prevention

306.	At least for a "Cloud scenario deployment" as described previously [4], the WLAN solution have wIDS/wIPS capabilities with no additional and dedicated equipment nor additional license. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Indeed, OmniAccess Stellar Access Points integrate *wireless Intrusion Detection and Prevention* (wIDS/wIPS) capabilities and reduce deployment and management costs by using Access Points to simultaneously serve clients and contain wireless threats.
With OmniAccess Stellar, there is no need for a costly overlay IDS with dedicated sensors. Automatic threat mitigation protects the network from unauthorized clients or APs and attacks. Integrated wIDS/wIPS capabilities allow to protect the WLAN better than an overlay deployment by virtue of being able to analyze and correlate 802.11 frames inline. It is possible to monitor the wireless radio spectrum for the presence of unsafe Access Points or unsafe clients, and countermeasures can be taken to mitigate the impact of foreign intrusions.

Last but not least, in *Wi-Fi Enterprise mode*, the OmniAccess Stellar APs embedded wIDS/wIPS capabilities do not require any additional license to protect the wireless network.

307.	The WLAN solution shall be able to identify Interfering APs, when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Identify Interfering APs is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [98] for Omnivista 2500 NMS server.

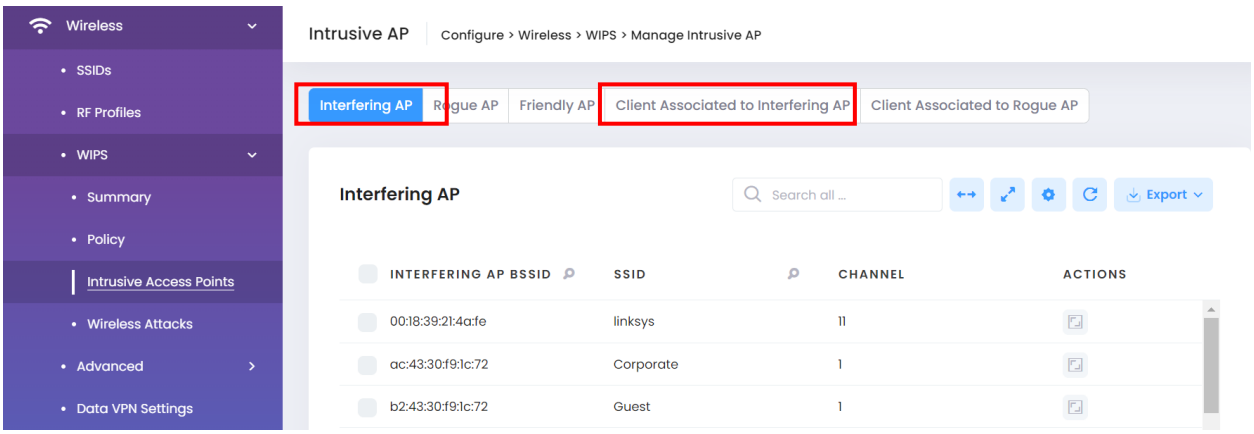


Figure 233: wIDS/wIPS – Omnivista Cirrus 10 (Intrusive Access Points)

308.	The WLAN solution shall be able to identify and contain Rogue APs, when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Beyond potential RF interference it can cause, a **rogue AP** is considered as a security threat to the WLAN network. This is typically the case of an unauthorized AP plugged into the wired side of the network (in that case, the MAC address of the scanned interfering AP is identified in the Forwarding Database of the scanning AP) or a foreign interfering AP broadcasting a SSID that is configured and set in the WLAN network.

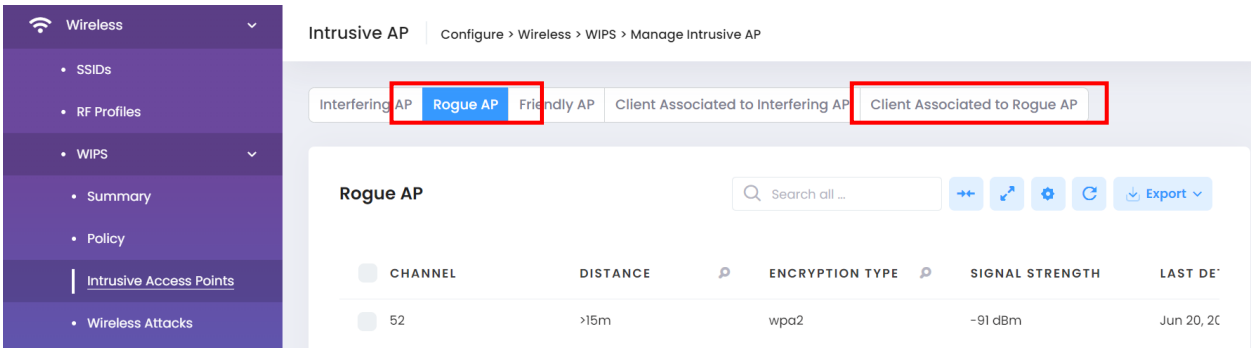


Figure 234: Rogue APs containment – Omnivista Cirrus 10 (Intrusive Access Points)

When an AP is classified as a rogue AP and when containment is enabled (disabled by default), the detecting AP (the one that detected the rogue AP) will send DEAUTH frames to clients that have associated to the rogue AP, keeping the clients away from the unsafe wireless network.

309.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible policies to classify an AP as a Rogue AP. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Define flexible policies to classify Rogue AP is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [100] for Omnivista 2500 NMS server.

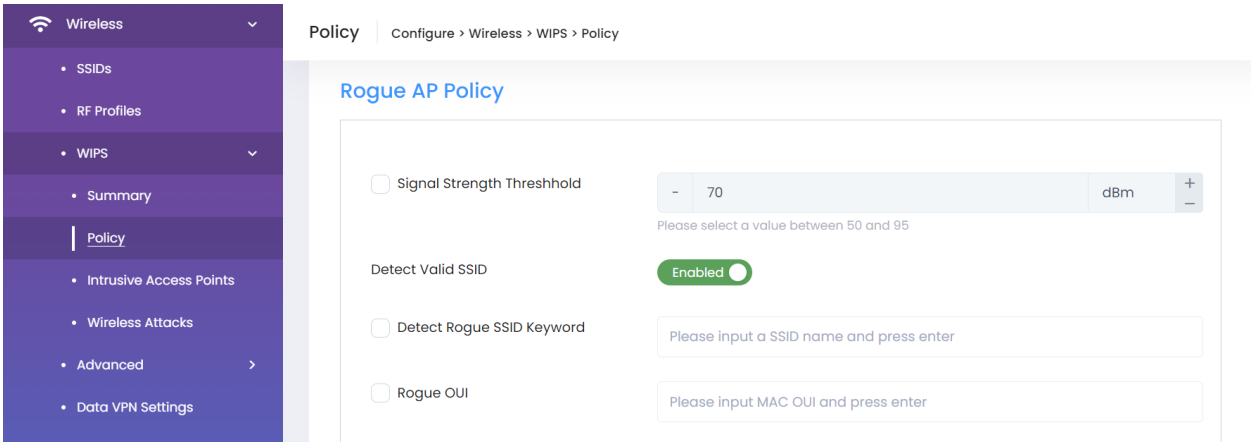


Figure 235: Rogue APs policy – Omnivista Cirrus 10 (Policy)

310.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible AP attacks detection policies. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Define flexible AP attacks detection policies is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [101] for Omnivista 2500 NMS server.

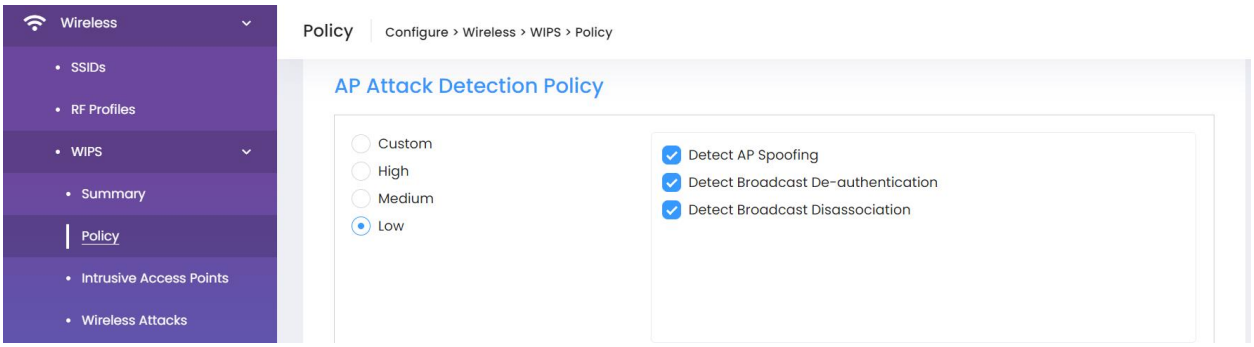


Figure 236: AP attack detection policy – Omnivista Cirrus 10 (Policy)

311.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall allow the definition of flexible client attacks detection policies. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Define flexible client attacks detection policies is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [102] for Omnivista 2500 NMS server.

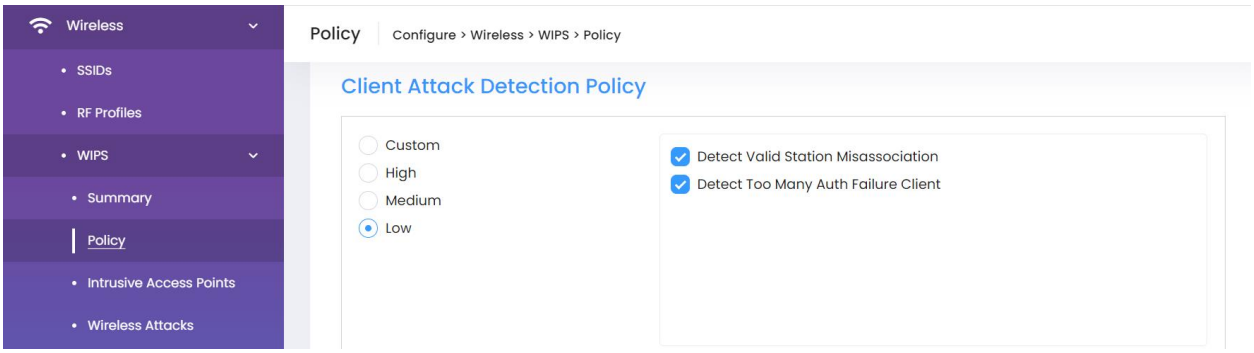


Figure 237: Client attack detection policy – Omnivista Cirrus 10 (Policy)

312.	A least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. In *Wi-Fi Enterprise mode*, the OmniAccess Stellar solution allows to blacklist a client manually or automatically. If a wireless attack

has been detected the intruder identified (MAC address) by the wIDS/wIPS application is prevented from associating with the network.

313.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow to configure a blacklist duration.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

314.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow to configure an authentication failure times threshold.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 in *Wi-Fi Enterprise mode*. A description is done in [105] for Omnivista 2500 NMS server.

Picture below summarizes the policies on client blocklist for Omnivista Cirrus 10.

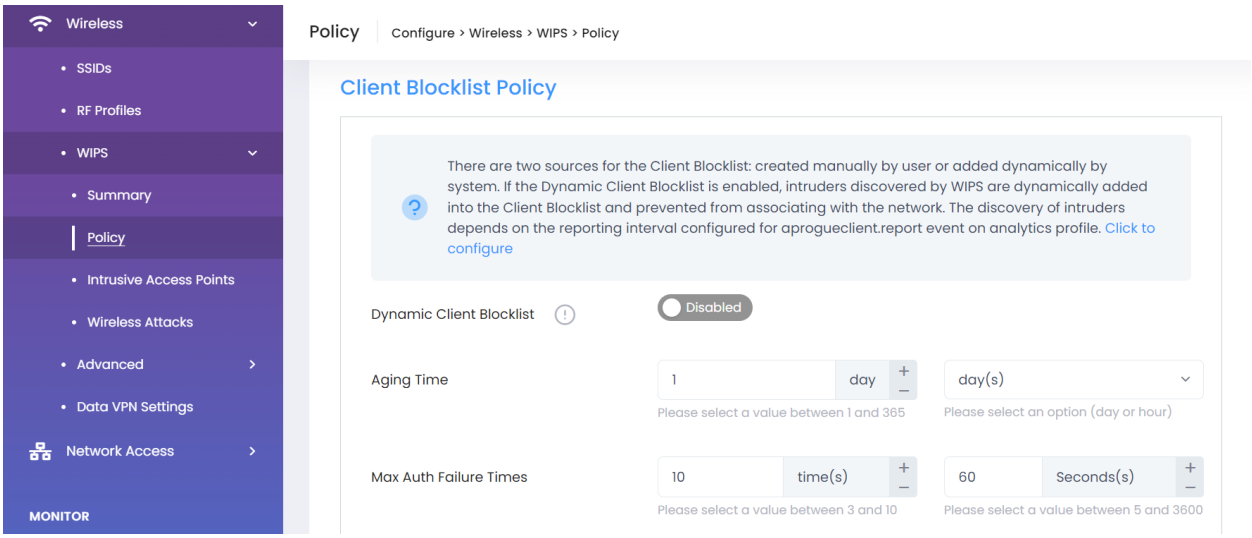


Figure 238: Client Blocklist policy – Omnivista Cirrus 10 (Policy)

5.4. Quality of Service

315.	At least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall offer WLAN Access Points that shall support fine-tuned Quality of Service (QoS) allowing following actions based on the identity of the connecting user:	C/PC/NC

	- ACL based (source/destination IP address and TCP/UDP ports) permit/deny decision - QoS priority marking and queuing This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 in *Wi-Fi Enterprise mode*. A description is done in [106] for Omnivista 2500 NMS server.

316.	At least for a "Cloud deployment" scenario as described previously [4], the wireless LAN solution shall comply with the 802.11e WMM standard and shall allow for custom QoS tag (802.1p/DSCP) to WMM queue mapping. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 in *Wi-Fi Enterprise mode*. A description is done in [107] for Omnivista 2500 NMS server.

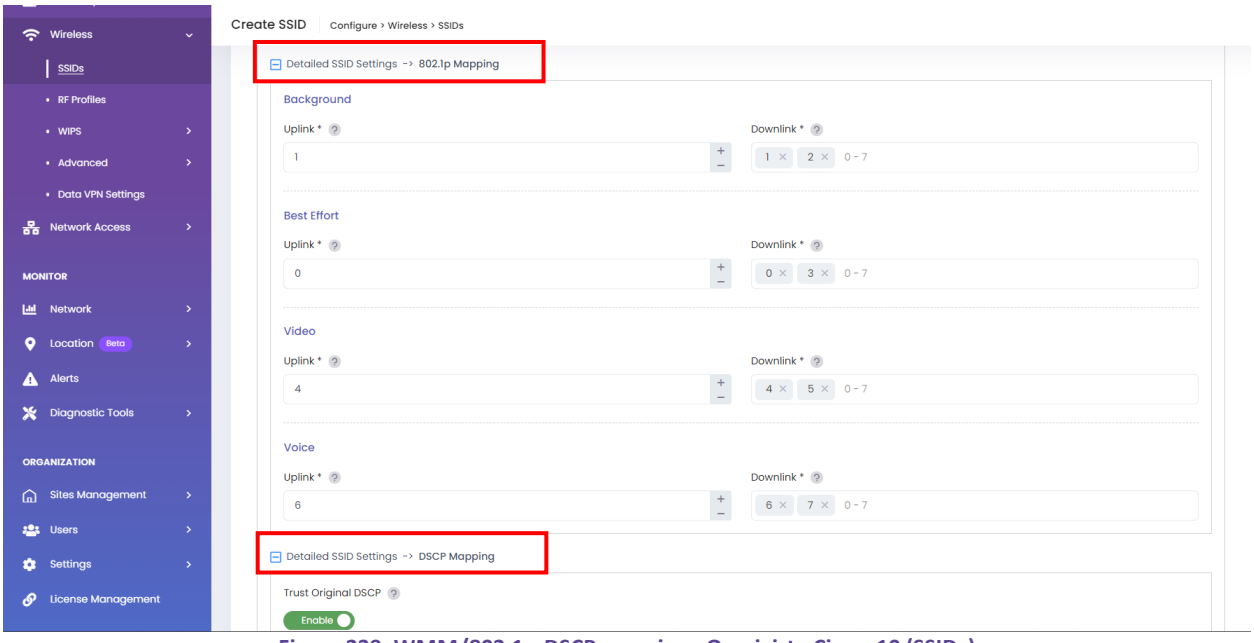


Figure 239: WMM/802.1p-DSCP mapping - Omnivista Cirrus 10 (SSIDs)

317.	A least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall have traffic L7 Application fingerprinting (aka *Deep Packet Inspection* (DPI) capabilities allowing an administrator to take control of applications (even if they all run on top of the HTTP or HTTPs protocols), including not only blocking applications, but also allowing to prioritize and rate-limit applications. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Built-in DPI technology is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and will be implemented in further Omnivista Cirrus 10.X versions. A description is done in [108] for Omnivista 2500 NMS server.

318.	At least for a “Cloud deployment” scenario as described previously [4], the wireless LAN solution shall be able to define and guarantee bandwidth on basis of a SSID. It shall also be able to define and guarantee bandwidth based on a user/device role. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. A “bandwidth contract” definition is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [109] for Omnivista 2500 NMS server.

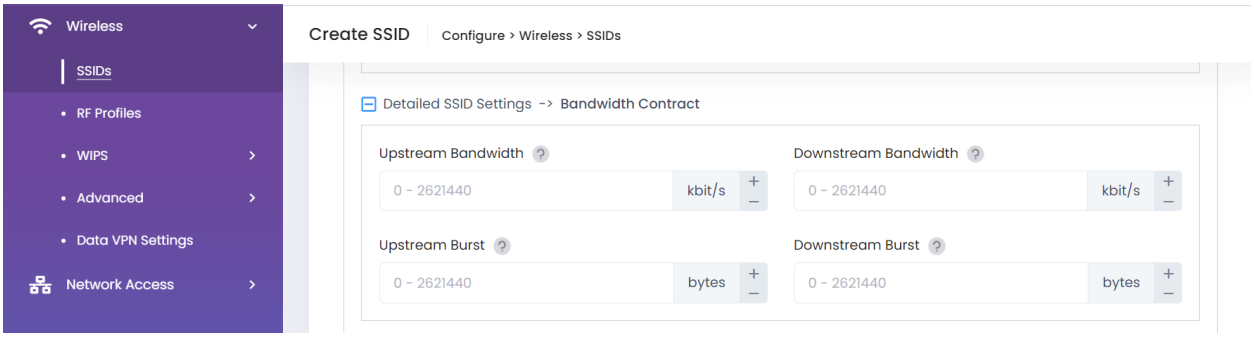


Figure 240: SSID Bandwidth Contract – Omnivista Cirrus 10 (SSIDs)

319.	At least for a “Cloud deployment” scenario as described previously [4], the WLAN solution shall allow to set the maximum number of clients per band/radio and per AP for a specific SSID. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments.

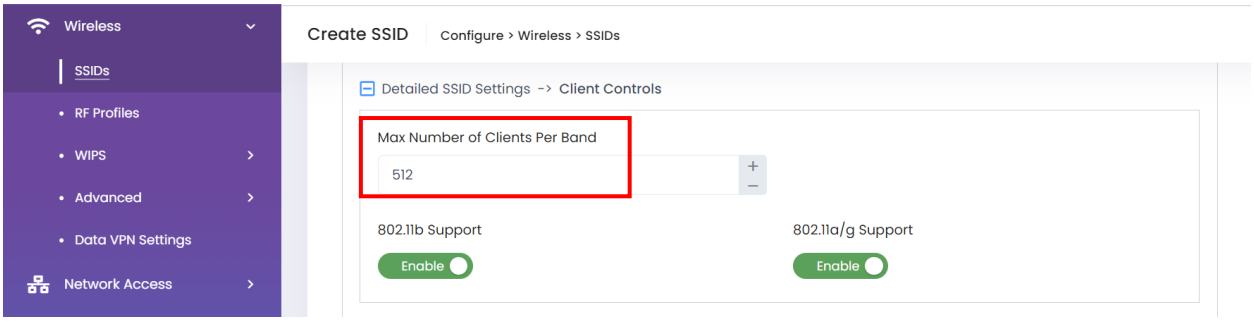


Figure 241: Maximum number of clients per band per SSID – Omnivista Cirrus 10 (SSIDs)

320.	At least for a "Cloud deployment" scenario as described previously [4], the wireless LAN solution shall propose broadcast traffic optimization mechanisms (including Broadcast filtering and Broadcast/Multicast Key rotation). This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Broadcast traffic optimization mechanisms are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [111] for Omnivista 2500 NMS server.

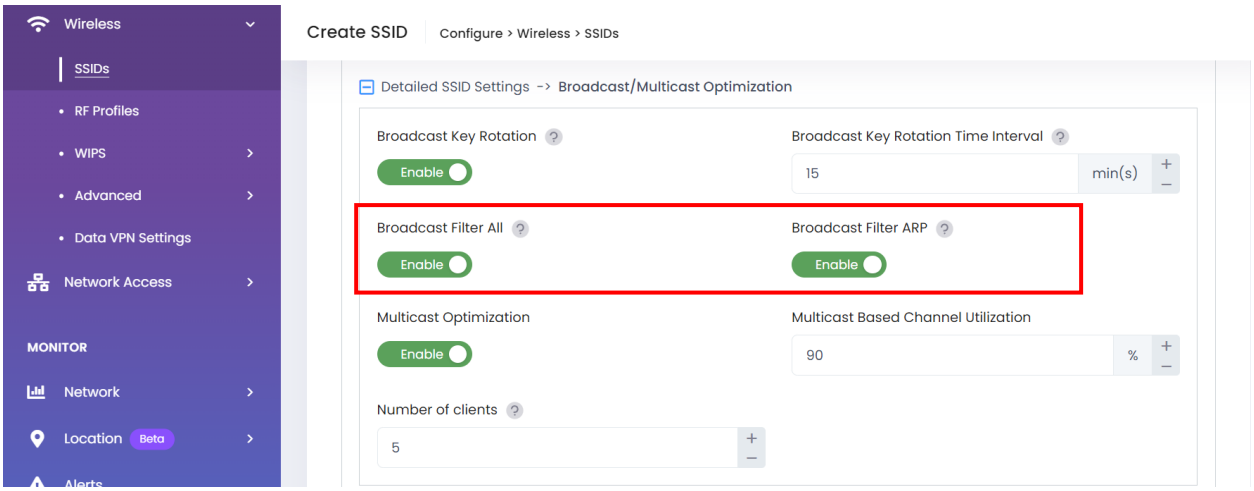


Figure 242: Broadcast traffic Optimization – Omnivista Cirrus 10 (SSIDs)

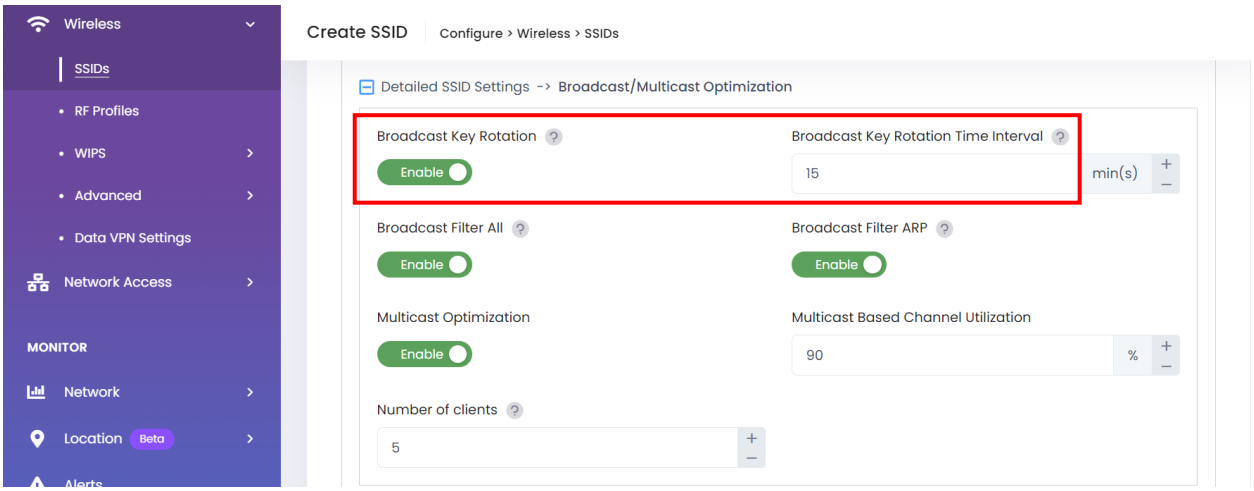


Figure 243: Broadcast Key Rotation – Omnivista Cirrus 10 (SSIDs)

321.	At least for a "Cloud deployment" scenario as described previously [4], the wireless LAN solution shall be able to optimize multicast traffic by converting multicast traffic to unicast traffic, leveraging its IGMP snooping capabilities. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Multicast traffic optimization is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [112] for Omnivista 2500 NMS server.

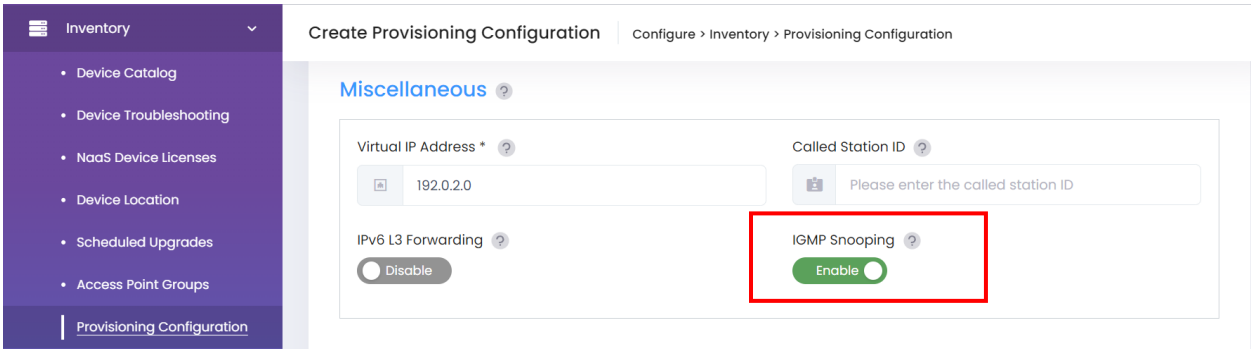


Figure 244: IGMP snooping – Omnivista Cirrus 10 (Provisioning Configuration)

322.	At least for a "Cloud deployment" scenario as described previously [4], Multicast optimization shall stop on high load. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This without requiring third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Multicast based channel utilization is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a short description is done in [113] for Omnivista 2500 NMS server.

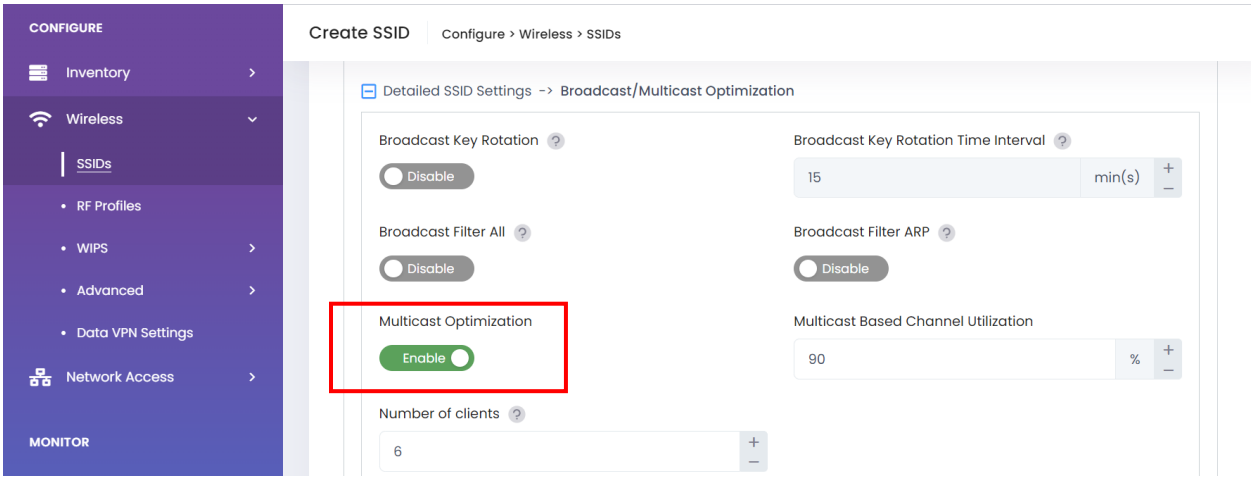


Figure 245: Multicast optimization - Enterprise mode – Omnivista Cirrus 10 (SSIDs)

323.	The wireless LAN solution shall propose the WMM *Automatic Power Save delivery* (APSD) feature to allow clients conserve battery life. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. WMM APSD is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [114] for Omnivista 2500 NMS server.

324.	The wireless LAN solution shall by default identify Voice and Audio/Video calls and provide appropriate treatment. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. It is indeed Voice and Video over IP aware and can dynamically classify real-time traffic in appropriate Class of Service. In addition, this level of voice awareness enables OmniAccess Stellar APs to know that a voice/audio/video call is taking place and not to scan channels for RF management or intrusion detection purposes until the call is terminated.

5.5. Mobility

325.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support Layer 2 roaming capabilities across APs with no special client-side software required. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Layer 2 roaming is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [116] for Omnivista 2500 NMS server.

326.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support Layer 3 roaming across APs with no special client-side software required. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. Layer 3 roaming is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [117] for Omnivista 2500 NMS server.

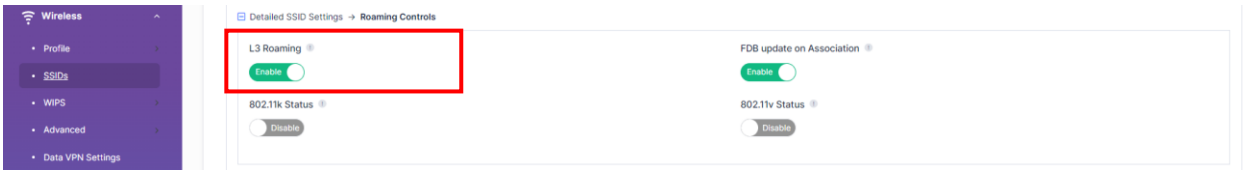


Figure 246: L3 roaming activation – Omnivista Cirrus 10 (SSIDs)

327.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall support 802.11r Fast Roaming and OKC - *Opportunistic Key Caching*. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This without requiring third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. 802.11r Fast Roaming and OKC are fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [118] for Omnivista 2500 NMS server.

328.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall comply with the 802.11k Radio Resource Management standard. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. 802.11k standard is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [119] for Omnivista 2500 NMS server.

329.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall comply with the 802.11v BSS Transition Management standard. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. 802.11v standard is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and a description is done in [120] for Omnivista 2500 NMS server.

330.	At least for a "Cloud deployment" scenario as described previously [4], the WLAN solution shall inform the wired side of the network about roaming across APs. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments. *Forward Data Base Update* (FDB Update) *on association* is fully supported when Stellar WLAN solution is managed by Omnivista NMS as a global solution and with a description in [121] for Omnivista 2500 NMS server.

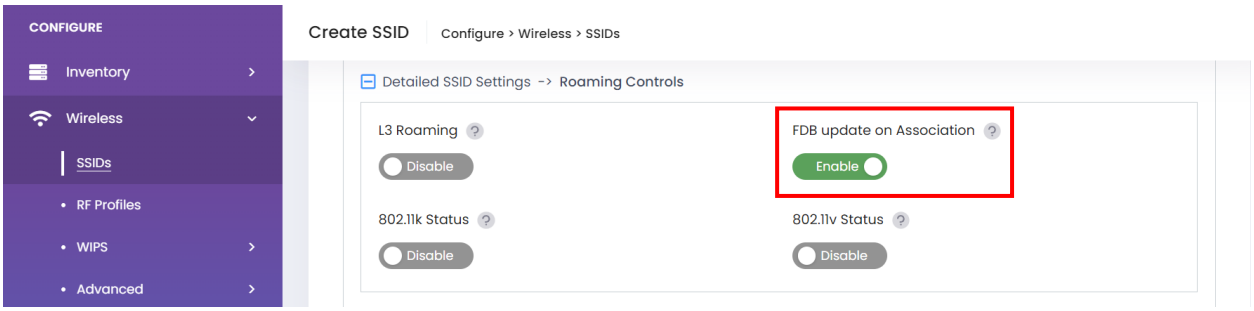


Figure 247: FDB Update disable option – Omnivista Cirrus 10 (SSID)

5.6. IoT Servers & Advanced servers

331.	At least for a "Cloud deployment" scenario as described previously [4], wireless WLAN solution shall support advanced location-based services provided by Cloud services included in the solution and using Bluetooth LE wireless with dedicated Asset Tracking applications. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Enterprise mode*, and when combined with Omnivista Cirrus Asset Manager solution for the asset tracking & contact tracing application. A description of Omnivista Cirrus Asset Manager is given in [123] for Omnivista 2500 NMS server.

Stellar Asset Tracking profile with Stellar Asset tracking engine is created via OmniVista Cirrus 10 for APs with BLE radios.

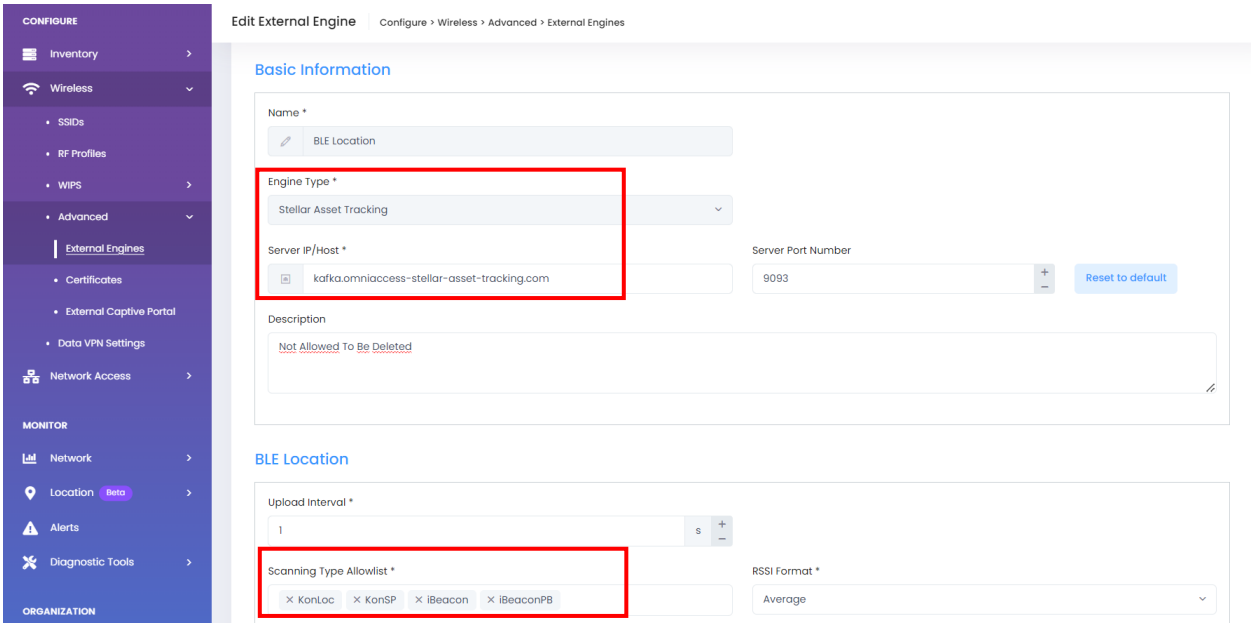


Figure 248: Stellar Asset Tracking profile – Omnivista Cirrus 10 (External Engines)

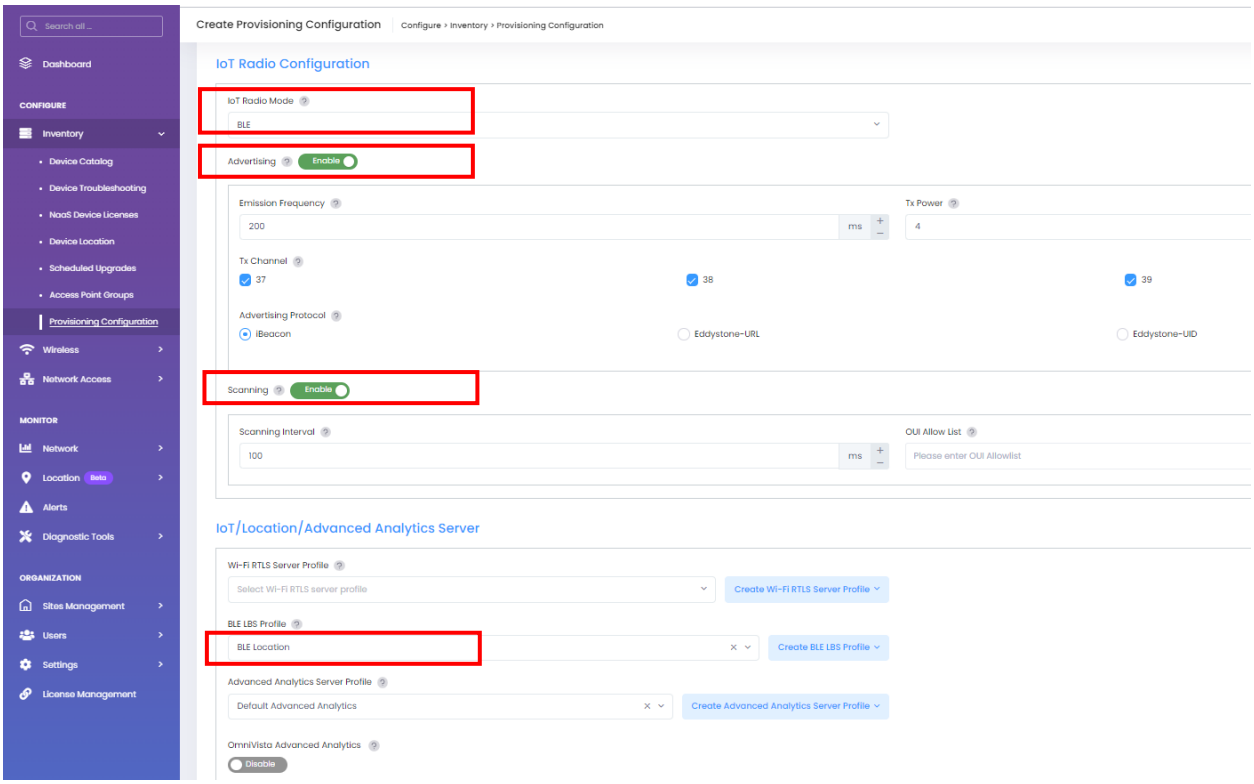


Figure 249 : BLE radio & Stellar Asset Tracking configuration – Omnivista Cirrus 10 (Provisioning Configuration)

332.	At least for a “Cloud deployment” scenario as described previously [4], wireless WLAN solution shall support RTLS service provided by RTLS application if existing in the network, or by RTLS Cloud service included in the solution, using WLAN radio only for location-based service. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Enterprise mode*.
High-Performance AP12xx, high-efficient AP13XX series (Wi-Fi 6), high-efficient AP14xx (Wi-Fi 6E) and extremely high throughput AP15xx (Wi-Fi 7) support Real-Time Location Service (RTLS) and provide data to RTLS location-based engines with WLAN radio measurements only (on the basis of received WLAN RSSIs from devices).

Omnivista Cirrus 10 offers customer the ability to manage RTLS location-based service in the Cloud on basis of received WLAN RSSIs from APs. Aeroscout RTLS application type offers customer the ability to manage RTLS location-based service on premises with existing RTLS application (Ekahau engine for example).

The management of RTLS service in OmniVista Cirrus 10 is identical to ones already discussed for IoT servers above [483]. RTLS profile must be created in OmniVista Cirrus 10 for APs that are supporting RTLS, with Aeroscout engine or any other Wi-Fi RTLS engine. The RTLS profile must be applied to AP-Groups that perform RTLS reports to RTLS engine.

333.	At least for a “Cloud scenario deployment” as described previously [4], wireless WLAN solution shall offer IoT device secure onboarding that is as simple as possible and without requiring additional third-party components. This when managed by a SaaS NMS cloud solution included in WLAN solution for XL/Multi-tenant site deployments.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Enterprise mode*.
High-Performance AP12xx, high-efficient AP13xx series (Wi-Fi 6), high-efficient AP14xx (Wi-Fi 6E) and extremely high throughput AP15xx (Wi-Fi 7) can provide scan on IoT devices (Devices Discovery) and OmniVista Cirrus 10, as centralized management, manages the enforcement of IoT devices discovered by APs in the network, to secure the onboarding of devices.

This completes the following actions for onboarding and inventory of IoT devices in OmniVista Cirrus 10:

- Device enforcement per category and per authentication.
- Device classification can be established and different categories can be defined, with assignation to specific category and automatic enforcement to Access Role Profile (ARP).
- Manage exception list per SSID, per MAC endpoints or per AP Groups attributes (sites)

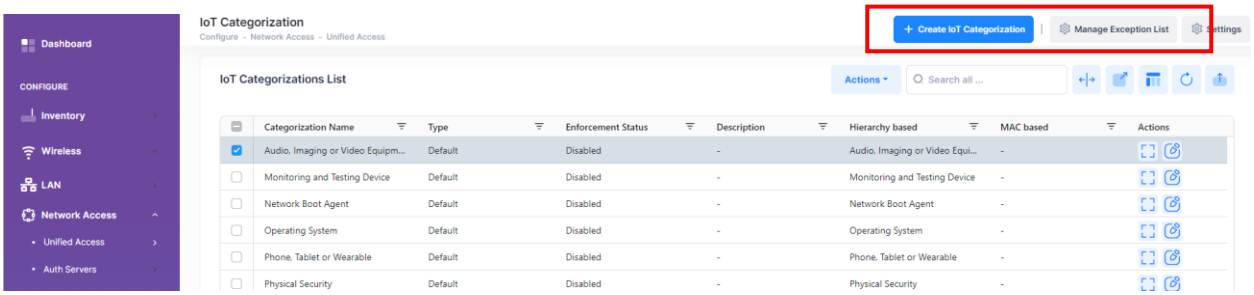


Figure 250: IoT secure Onboarding – Omnivista Cirrus 10 (IoT Categorization)

334.	At least for a "Cloud deployment" scenario as described previously [4], wireless WLAN solution shall support advanced analytics services provided by SaaS NMS cloud solution included in WLAN solution, services dedicated to statistical and analytical tasks for different XL/Multi-tenant deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement when managed by Omnivista Cirrus 10 for Stellar XL/Multi-tenant deployments in *Enterprise mode*. High-Performance AP12xx (except AP1101/AP1201H), Wi-Fi 6 AP13xx, series Wi-Fi 6E AP14xx series and Wi-Fi 7 AP15xx support advanced analytics, reporting and recording and can send their data to OmniVista Cirrus 10 Cloud instance for advanced statistical and analytical services, for different XL/Multi-tenant Stellar WLAN networks, when managed with Omnivista Cirrus 10.

Omnivista Cirrus 10 Cloud instance offers the ability to provide and manage, through integrated menus, dashboards to customer for analytics tasks for example Quality of Experience (QoE) for the whole Stellar WLAN networks, through a single platform and in various forms of charts or graphs.

- Management of Multi-Tenants with support of Quality of Experience (QoE) on Stellar WLAN
- Dashboards to display WLAN statistics in various forms of charts or graphs

The picture below shows Time on connections (with reasons of failure) and users Mobility (roaming and coverage) QoE analytics, analytics that can be enriched with statistics on mode of connections, users connections accross SSIDs, device types or OS types, users distribution accross APs/channels or users accesses on domains/web URLs etc.

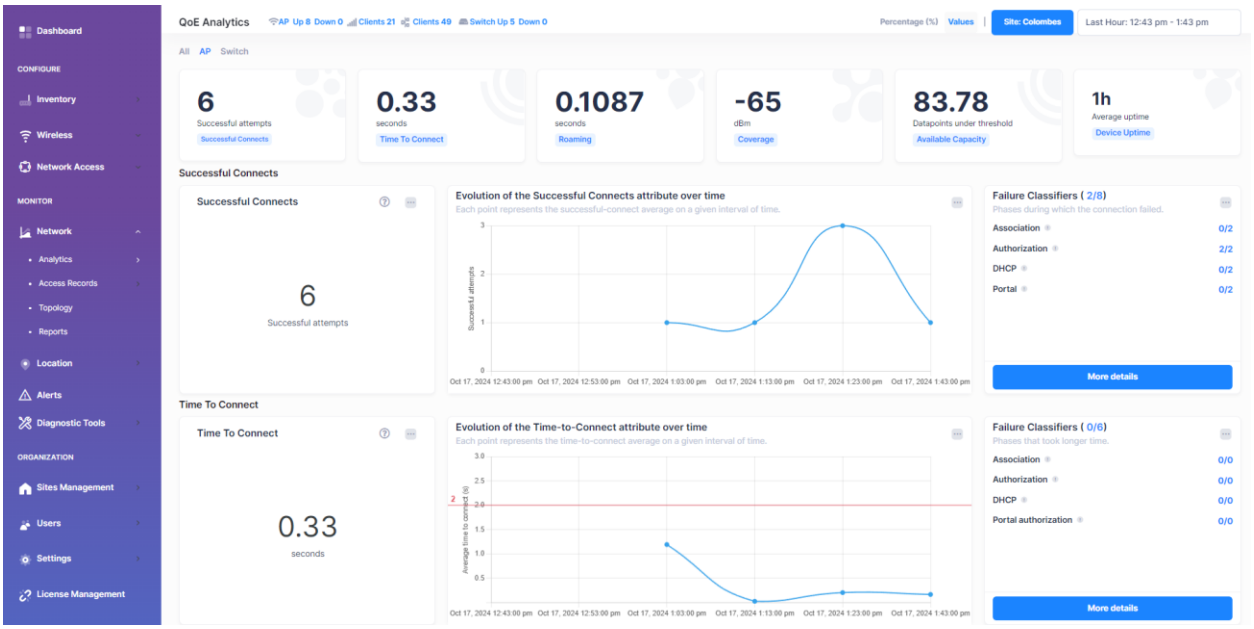


Figure 251: Quality of Experience (QoE) analytics – Omnivista Cirrus 10 (QoE)

Analytics on Stellar WLAN itself can be realized with statistics on access points, Health of access points, access points capacity and channels utilization (channels distribution/use accross the APs and throughputs accross channels or APs) etc.

Omnivista Cirrus 10 for advanced management and analytics, enables a single architecture for a deep analysis of Stellar WLAN from the Cloud. The only prerequisite for Stellar access points is to have internet access to access to Omnivista Cirrus 10 instance.

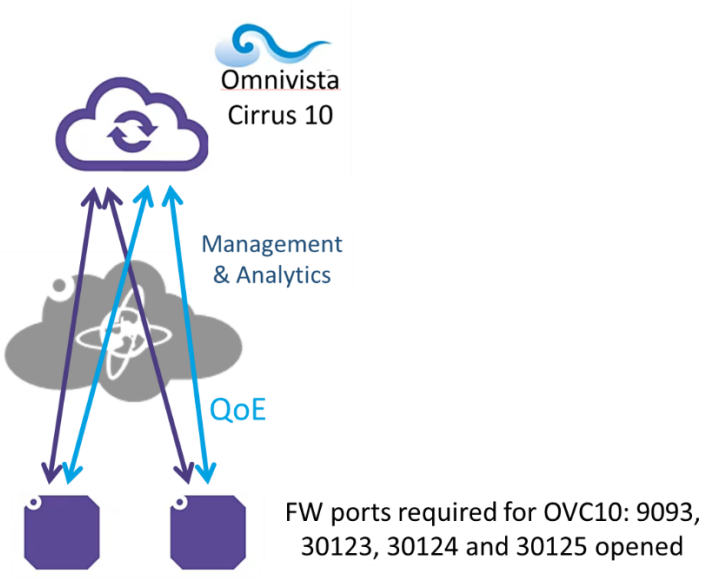


Figure 252: Advanced analytics with OV Cirrus 10 in Enterprise mode

335.	At least for a “Cloud deployment” scenario as described previously [4], wireless WLAN solution shall support advanced management services provided by SaaS NMS cloud solution included in the solution, services dedicated to different sites, dedicated to the management of WLAN devices for each site and dedicated to the management of wireless itself for XL deployments. This does not require a third-party component for NMS management.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement in *Enterprise mode* when managed by Omnivista Cirrus 10 for XL/Multi-Tenant deployments. The high-performance AP12xx (except AP1101/AP1201H), Wi-Fi 6 AP13xx series, Wi-Fi 6E AP14xx series and Wi-fi 7 AP15xx series (supported from Omnivista Cirrus 10.4.3 with AWOS 5.0.1) support advanced, centralized WLAN management with AP groups control from Omnivista Cirrus 10 instance for turnkey WLAN network management and analytics for different customers and sites.

The initial versions of Omnivista Cirrus 10 integrate WLAN inventory for given sites; Stellar equipment management and provisioning, license management, localization service and devices troubleshooting. Stellar management integrates Omnivista updated wireless management functionalities; SSIDs, RF, WIPS, external servers, data VPNs etc., as well as a revised Omnivista network access management; Unified Access, UPAM-NAC (Network Access Controller) and dedicated menus (for example new menu for accounting).

In addition to revised menus for Omnivista, what is new with Omnivista Cirrus 10 is complete WLAN management for different organizations in size, with multi-tenants, as already discussed for example for RAP in [24] in the document. The integration of a complete and unified WLAN and LAN management for the Enterprise will continue in subsequent versions of the Omnivista Cirrus 10 SaaS management solution. Omnivista Cirrus 10 is now the subject of a fully-fledged Golden RFP document: *ALE Omnivista Cirrus 10.x Golden RFP*. For any proposal preparation and questions concerning the complete Omnivista Cirrus 10 solution and its subsequent developments for WLAN and LAN, please refer systematically to this new RFP document dedicated to fully cloud-managed mode for Enterprise.

Referring to the *Figure 245: Omnivista Cirrus 10 connectivity in Enterprise mode* depicting Omnivista Cirrus 10 for advanced management and analytics, the tunnels for Stellar devices management now end to the Omnivista Cirrus 10 instance attached to the related site when Stellar devices are set to be fully managed by Omnivista Cirrus 10.

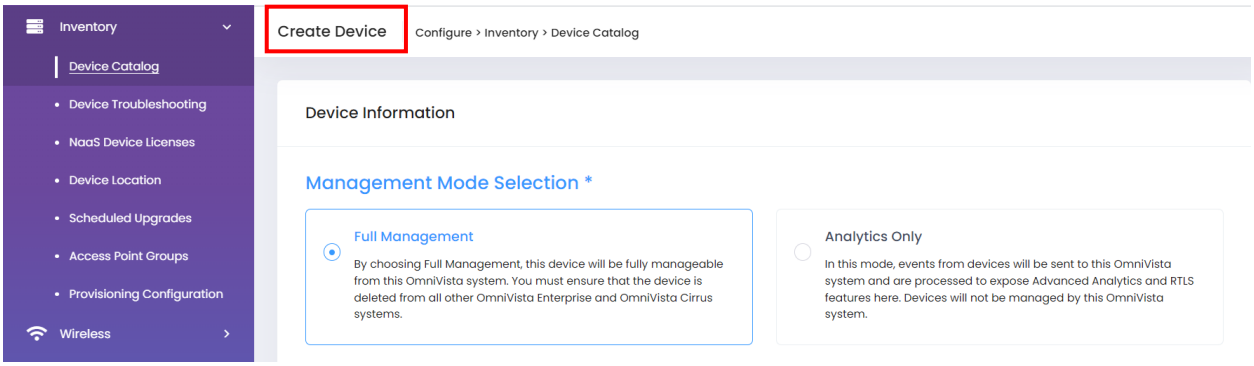


Figure 253: Full management mode selection – Omnivista Cirrus 10 (Device Catalog)

6. Access Points Specific Requirements

Type A	AP1101
Type B	AP1201
Type C	AP1220
Type D	AP1230
Type E	AP1201H
Type F	AP1320
Type G	AP1311
Type H	AP1251
Type I	AP1360
Type J	AP1301
Type K	AP1301H
Type L	AP1331
Type M	AP1351
Type N	AP1261
Type O	AP1451
Type P	AP1411
Type Q	AP1431
Type R	AP1511
Type S	AP1521

Table 12: OmniAccess Stellar AP list

6.1. Indoor Access Point – Type A

336.	The WLAN solution shall propose a 802.11ac wave1 indoor dual-radio AP (2GHz, 5GHz) Access Point: “Type A”.	C/PC/NC

With the OmniAccess Stellar AP1101 wave1 and dual-radio AP, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 254: OmniAccess Stellar AP1101 Access Point

337.	The “Type A” Access Point shall have integrated omnidirectional antennas.	C/PC/NC
338.	The “Type A” Access Point shall support up to 16 SSIDs (8 per radio).	C/PC/NC
339.	The “Type A” Access Point shall offer up to 867Mbps throughput on the 5Ghz band and up to 300Mbps throughput on the 2.4GHz band.	C/PC/NC
340.	The “Type A” Access Point shall support up to 128 clients.	C/PC/NC
341.	The “Type A” Access Point shall have one 1Gb Ethernet port.	C/PC/NC
342.	The “Type A” Access Point shall support 802.3af/at PoE with 10W maximum consumption.	C/PC/NC
343.	The MTBF for the “Type A” Access Point shall be at least 525600h (60 Years).	C/PC/NC
344.	The “Type A” Access Point shall propose a Factory reset button.	C/PC/NC
345.	The “Type A” Access Point shall propose a console port.	C/PC/NC

6.2. Indoor Access Point – Type AB

346.	The WLAN solution shall propose a 802.11ac wave2 indoor dual-radio AP (2GHz, 5GHz) Access Point: "Type B".	C/PC/NC

With the OmniAccess Stellar AP1201 wave2 and dual-radio AP, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 255: OmniAccess Stellar AP1201 Access Point

347.	The "Type B" Access Point shall have integrated omnidirectional antennas.	C/PC/NC
348.	The "Type B" Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC
349.	The "Type B" Access Point shall offer up to 867Mbps throughput on the 5Ghz band and up to 400Mbps throughput on the 2.4GHz band.	C/PC/NC
350.	The "Type B" Access Point shall support up to 512 clients.	C/PC/NC
351.	The "Type B" Access Point shall have one 1Gb Ethernet port.	C/PC/NC
352.	The "Type B" Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1201 Access Point fully comply to this requirement. Please refer to requirement [108].

353.	The "Type B" Access Point shall support 802.3af/at PoE with 11W maximum consumption.	C/PC/NC
354.	The MTBF for the "Type B" Access Point shall be at least 1143213h (130.5 years).	C/PC/NC
355.	The "Type B" Access Point shall propose a Factory reset button.	C/PC/NC

356.	The "Type B" Access Point shall propose a console port.	C/PC/NC

6.3. Indoor Access Point – Type AC

357.	The WLAN solution shall propose a 802.11ac wave2 MU-MIMO indoor dual-radio AP Access Point with integrated omni-directional antennas or that may be equipped with external antennas: "Type C".	C/PC/NC

With the OmniAccess Stellar AP1220 series wave2 and dual-radio APs, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 256: OmniAccess Stellar AP1220 Series

As depicted on previous figure, the Stellar AP1220 series includes the AP1221 Access Point with omni-directional antennas and the AP1222 Access Point with connectors to connect external antennas.

358.	The "Type C" Access Point shall offer BLE radio support and additional Ethernet support through USB port (via attached devices). Ethernet interface through USB (AWOS 5.0.1) shall be disableable.	C/PC/NC
359.	The "Type C" Access Point shall support up to 16 SSIDs (8 per radio).	C/PC/NC
360.	The "Type C" Access Point shall offer up to 1733Mbps throughput on the 5Ghz band and up to 400Mbps throughput on the 2.4GHz band.	C/PC/NC
361.	The "Type C" Access Point shall support up to 512 clients.	C/PC/NC
362.	The "Type C" Access Point shall have one 1Gb Ethernet port.	C/PC/NC
363.	The "Type C" Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1220 series Access Points fully comply to this requirement. Please refer to requirement [108].

364.	The “Type C” Access Point shall support 802.3af/at PoE with 18.5W maximum consumption.	C/PC/NC

365.	The MTBF for the “Type C” Access Point shall be at least 525600h (60 years).	C/PC/NC

366.	The “Type C” Access Point shall propose a Factory reset button.	C/PC/NC

367.	The “Type C” Access Point shall propose a console port.	C/PC/NC

6.4. Indoor Access Point - Type AD

368.	The WLAN solution shall propose a 802.11ac wave2 MU-MIMO indoor tri-radio AP Access Point (**2.4, 5G low, 5G high**): “Type D”.	C/PC/NC

With the OmniAccess Stellar AP1230 series wave2 and tri-radio APs, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 257: OmniAccess Stellar AP1230 Series

369.	The “Type D” Access Point shall have integrated omni-directional antennas or may be equipped with external antennas.	C/PC/NC

As depicted on previous figure, The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the Stellar AP1230 series includes the AP1231 Access Point with omni-directional antennas and the AP1232 Access Point with connectors to connect external antennas.

370.	The “Type D” Access Point shall offer native BLE radio support.	C/PC/NC

371.	The “Type D” Access Point shall support up to 24 SSIDs (8 per radio).	C/PC/NC

372.	The “Type D” Access Point shall offer up to 1733Mbps throughput on the 5Ghz band (low and high bands) and up to 800Mbps throughput on the 2.4GHz band.	C/PC/NC

373.	The “Type D” Access Point shall support up to 768 clients.	C/PC/NC

374.	The “Type D” Access Point shall have one 1Gb Ethernet port and one 2.5Gb Ethernet (IEEE 802.3bz Multi-rate Gigabit Ethernet) which may be aggregated as a single logical link (LACP).	C/PC/NC

375.	The “Type D” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable.	C/PC/NC

376.	The “Type D” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1230 series Access Points fully comply to this requirement. Please refer to requirement [108].

377.	The “Type D” Access Point shall support 802.3af/at PoE with 27.6W maximum consumption.	C/PC/NC

378.	The MTBF for the “Type D” Access Point shall be at least 525600h (60 years).	C/PC/NC

379.	The “Type D” Access Point shall propose a Factory reset button.	C/PC/NC

380.	The “Type D” Access Point shall propose a console port.	C/PC/NC

6.5. Indoor Access Point - Type AE

381.	The WLAN solution shall propose a 802.11ac wave2 MU-MIMO indoor dual-radio AP Access Point for in room applications: “Type E”.	C/PC/NC

With the OmniAccess Stellar AP1201H wave2 and dual-radio Access Point, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 258: OmniAccess Stellar AP1201H Access Point

The OmniAccess Stellar AP1201H Access Point is a highly versatile, and performance rich Access Point providing, indeed, operational simplicity, quality user experience and high-performance Gigabit Wi-Fi for in room applications such as hotels, classrooms, dormitories, clinics, remote/home office and more… The AP1201H Access Point is an answer to the challenge of the high ports density introduced by the various devices (IP phones, IPTVs...) connected to the network. It allows to make savings on ports and cabling, and the radio coverage in rooms is highly improved and secured. Additionally, the need for site surveys (and associated costs) is also reduced:

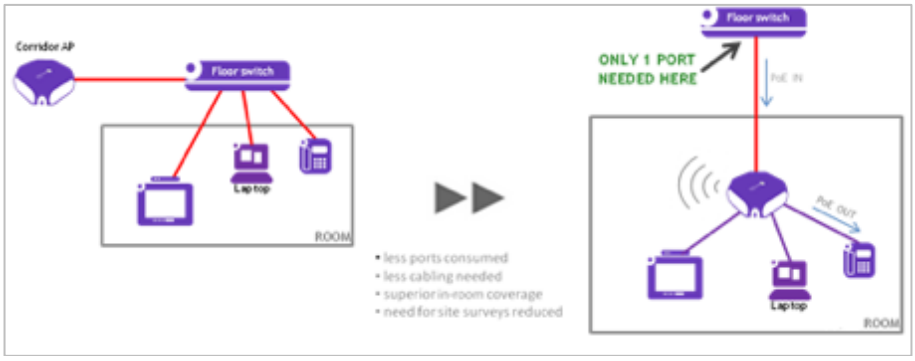


Figure 259: AP1201H deployment and benefits

382.	The “Type E” Access Point shall have integrated omnidirectional antennas.	C/PC/NC
383.	The “Type E” Access Point shall support up to 16 SSIDs (8 per radio).	C/PC/NC
384.	The “Type E” Access Point shall offer up to 867Mbps throughput on the 5Ghz band and up to 300Mbps throughput on the 2.4GHz band.	C/PC/NC
385.	The “Type E” Access Point shall support up to 256 clients.	C/PC/NC
386.	The “Type E” Access Point shall have three 1Gb Ethernet downlink ports and one of which supports 802.3af PSE to power to the attached device.	C/PC/NC
387.	The “Type E” Access Point shall have one USB 2.0 port capable of supplying up to 5V/500mA power to an attached device.	C/PC/NC

388.	The “Type E” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable.	C/PC/NC

389.	The “Type E” Access Point shall have one pair of RJ-45 passive pass through port (back and bottom).	C/PC/NC

390.	The “Type E” Access Point shall have one 1Gb Ethernet uplink port with 10W maximum consumption when USB and PSE function are disabled, or 25.5W maximum consumption when USB and PSE function are enabled.	C/PC/NC

391.	The “Type E” Access Point shall trust IEEE 802.1q marking on downlink ports.	C/PC/NC

The OmniAccess Stellar AP1201H Access Point allows reception of “tagged” traffic on downlink ports by trusting IEEE 802.1q marking of incoming traffic as depicted in following figure (*AP UI*, AP dedicated web interface, as described above [7]):

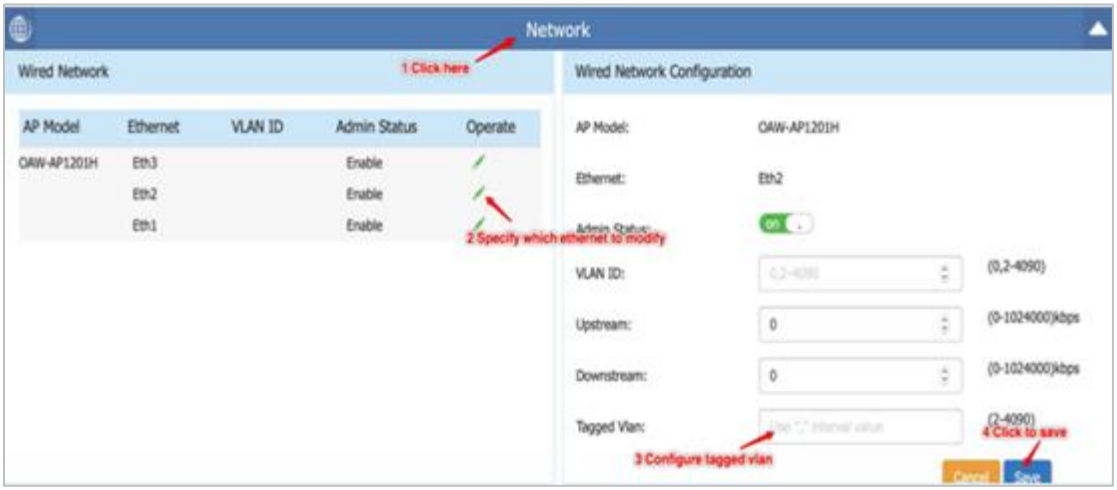


Figure 260: 802.1q Tag Support on AP1201H Downlink Ports

392.	The MTBF for the “Type E” Access Point shall be at least 1393193h (159 years).	C/PC/NC

393.	The “Type E” Access Point shall propose a Factory reset button.	C/PC/NC

6.6. Indoor Access Point - Type AF

394.	The WLAN solution shall propose an 802.11ax MU-MIMO indoor tetra-radio AP Access Point (2,4GHz, 5GHZ, Full Band Scanning dedicated Radio and Bluetooth/Zigbee): “Type F”.	C/PC/NC

With the OmniAccess Stellar AP1320 family, an 802.11ax and tetra-radio Access Point, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 261: OmniAccess Stellar AP1321 Access Point

Figure 262: OmniAccess Stellar AP1322 Access Point

395.	The “Type F” Access Point shall have integrated omnidirectional antennas or be equipped with external antennas.	C/PC/NC

As depicted in the previous figure, The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the Stellar AP1320 series includes the AP1321 Access Point with omnidirectional antennas and the AP1322 Access Point with SMA-RP connectors to connect external antennas.

396.	The “Type F” Access Point shall offer native BLE5.1/Zigbee radio support.	C/PC/NC

397.	The “Type F” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC

398.	The “Type F” Access Point shall offer up to 2,4Gbps throughput on the 5Ghz band (low and high bands) and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC

399.	The “Type F” Access Point shall support up to 1024 clients.	C/PC/NC

400.	The “Type F” Access Point shall have one 1Gb Ethernet port and one 2.5Gb Ethernet (IEEE 802.3bz Multi-rate Gigabit Ethernet), which may be aggregated as a single logical link (LACP).	C/PC/NC

401.	The “Type F” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable.	C/PC/NC

402.	The “Type F” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1320 Series Access Points fully comply with this requirement. Please refer to requirement [108].

403.	The “Type F” Access Point shall support 802.3af/at PoE with 24.8W maximum consumption.	C/PC/NC

404.	The MTBF for the “Type F” Access Point shall be at least 1,104,490 h (126.08 years).	C/PC/NC

405.	The “Type F” Access Point shall propose a Factory reset button.	C/PC/NC

406.	The “Type F” Access Point shall propose a console port.	C/PC/NC

407.	The “Type F” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHZ) for detecting security and RF anomalies.	C/PC/NC

6.7. Indoor Access Point - Type AG

408.	The WLAN solution shall propose an 802.11ax MU-MIMO indoor tetra-radio AP Access Point (2,4GHz, 5GHz, Full Band Scanning dedicated Radio and Bluetooth/Zigbee): “Type G”.	C/PC/NC

With the OmniAccess Stellar AP1311, an 802.11ax and tetra-radio Access Point, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 263: OmniAccess Stellar AP1311 Access Point

Figure 264: OmniAccess Stellar AP1311 Access Point (Rear View)

409.	The “Type G” Access Point shall have integrated omnidirectional antennas.	C/PC/NC

As depicted in the previous figure, The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The Stellar AP1311 Access Point has integrated omnidirectional antennas.

410.	The “Type G” Access Point shall offer native BLE5.1/Zigbee radio support.	C/PC/NC
411.	The “Type G” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC
412.	The “Type G” Access Point shall offer up to 1,2Gbps throughput on the 5Ghz band and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC
413.	The “Type G” Access Point shall support up to 512 clients.	C/PC/NC
414.	The “Type G” Access Point shall have two 1Gb Ethernet ports, which may be aggregated as a single logical link (LACP).	C/PC/NC

415.	The “Type G” Access Point shall have one 1Gb Ethernet port, for LAN connectivity or “downlink”.	C/PC/NC

416.	The “Type G” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable.	C/PC/NC

417.	The “Type G” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1311 Access Points fully comply with this requirement. Please refer to requirement [108].

418.	The “Type G” Access Point shall support 802.3af/at PoE with 19.1W maximum consumption.	C/PC/NC

419.	The MTBF for the “Type G” Access Point shall be at least 978,601 h (111.71 years).	C/PC/NC

420.	The “Type G” Access Point shall propose a Factory reset button.	C/PC/NC

421.	The “Type G” Access Point shall propose a console port.	C/PC/NC

422.	The “Type G” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHZ) for detecting security and RF anomalies.	C/PC/NC

6.8. Outdoor Access Point - Type AH

423.	The WLAN solution shall propose a 802.11ac wave2 MU-MIMO outdoor ruggedized dual-radio AP Access Point. “Type H”	C/PC/NC

With the OmniAccess Stellar AP1251 series wave2 and dual-radio AP, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 265: OmniAccess stellar AP1251 Access Point

424.	The “Type H” Access Point shall have integrated omni-directional antennas or may be equipped with external antennas.	C/PC/NC
425.	The “Type H” Access Point shall support up to 16 SSIDs (8 per radio).	C/PC/NC
426.	The “Type H” Access Point shall offer up to 1733Mbps throughput on the 5Ghz band and up to 400Mbps throughput on the 2.4GHz band.	C/PC/NC
427.	The “Type H” Access Point shall support up to 512 clients.	C/PC/NC
428.	The “Type H” Access Point shall have two (2) 1Gb Ethernet port.	C/PC/NC
429.	The “Type H” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1251 Access Point fully complies with this requirement. Please refer to requirement [108].

430.	The “Type H” Access Point shall be IP66/67 certified.	C/PC/NC
431.	The “Type H” Access Point shall support persistent moisture and precipitation, and high and low temperatures: -40°C to 65°C.	C/PC/NC
432.	The “Type H” Access Point shall support 802.3af/at PoE with 40W maximum consumption.	C/PC/NC
433.	The MTBF for the “Type H” Access Point shall be at least 525600h (60 Years).	C/PC/NC
434.	The “Type H” Access Point shall propose a Factory reset button.	C/PC/NC
435.	The “Type H” Access Point shall propose a console port.	C/PC/NC

6.9. Outdoor Access Point - Type AI

436.	The WLAN solution shall propose a 802.11ax MU-MIMO outdoor ruggedized tetra-radio AP Access Point (2,4GHz, 5GHZ, Full Band Scanning dedicated Radio and Bluetooth/Zigbee). “Type I”	C/PC/NC

With the OmniAccess Stellar AP1360 series 802.11ax and tetra-radio AP, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 266: OmniAccess stellar AP1360 Access Points Series

437.	The “Type I” Access Point shall have integrated omnidirectional antennas, integrated sectorial antennas, or be equipped with external antennas.	C/PC/NC
438.	The “Type I” Access Point shall offer native BLE5.1/Zigbee radio support.	C/PC/NC
439.	The “Type I” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC
440.	The “Type I” Access Point shall offer up to 2.4Gbps throughput on the 5Ghz band and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC
441.	The “Type I” Access Point shall support up to 1024 clients.	C/PC/NC
442.	The “Type I” Access Point shall have one (1) 10/100/1000/2500MBaseT Ethernet port UPLINK port, 802.3at/bt compliant.	C/PC/NC
443.	The “Type I” Access Point shall have one (1) 10/100/1000MBaseT Ethernet port DOWNLINK, 802.3at compliant, with PoE PSE output so that an end device can be directly connected and powered from the AP, for example an Outdoor CCTV camera. PoE on PSE port shall be disableable.	C/PC/NC

444.	The “Type I” Access Point shall have one (1) SFP port for connecting optical fiber transceivers or GPON SFP-ONT.	C/PC/NC

445.	The “Type I” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC

446.	The “Type I” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1360 Access Point Series fully complies with this requirement. Please refer to requirement [108].

447.	The “Type I” Access Point shall be IP66/67 certified.	C/PC/NC

448.	The “Type I” Access Point shall support persistent moisture and precipitation, and high and low temperatures: -40°C to 65°C.	C/PC/NC

449.	The “Type I” Access Point shall support 802.3af/at PoE with 64W maximum consumption, when powering a PSE device with 802.3at	C/PC/NC

450.	The MTBF for the “Type I” Access Point shall be at least 1,003,257h (114.5 Years).	C/PC/NC

451.	The “Type I” Access Point shall propose a Factory reset button.	C/PC/NC

452.	The “Type I” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHZ) for detecting security and RF anomalies.	C/PC/NC

6.10. Indoor Access Point - Type AJ

453.	The WLAN solution shall propose an entry-level 802.11ax MU-MIMO indoor tri-radio AP Access Point (2,4GHz, 5GHz, Full Band Scanning dedicated Radio): ”Type J”	C/PC/NC

With the OmniAccess Stellar AP1301, an 802.11ax and tri-radio Access Point, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 267: OmniAccess Stellar AP1301 Access Point

Figure 268: OmniAccess Stellar AP1301 Access Point (Rear View)

454.	The ”Type J”Access Point shall have integrated omnidirectional antennas.	C/PC/NC

As depicted in the previous figure, The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The Stellar AP1301 Access Point has integrated omnidirectional antennas.

455.	The ”Type J” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC
456.	The ”Type J” Access Point shall offer up to 1,2Gbps throughput on the 5GHz band and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC
457.	The ”Type J” Access Point shall support up to 512 clients.	C/PC/NC
458.	The ”Type J” Access Point shall have two 1Gb Ethernet ports, which may be aggregated as a single logical link (LACP).	C/PC/NC

459.	The “Type J” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC

460.	The ”Type J” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1301 Access Points fully comply with this requirement. Please refer to requirement [108].

461.	The ”Type J” Access Point shall support 802.3af/at PoE with 13.1W maximum consumption.	C/PC/NC

462.	The MTBF for the ”Type J” Access Point shall be at least 1,118,457 h (127,67 years).	C/PC/NC

463.	The ”Type J” Access Point shall propose a Factory reset button.	C/PC/NC

464.	The ”Type J” Access Point shall propose a console port.	C/PC/NC

465.	The ”Type J” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHz) for detecting security and RF anomalies.	C/PC/NC

6.11. Indoor Access Point - Type AK

466.	The WLAN solution shall propose a 802.11ax MU-MIMO indoor tri-radio AP Access Point (2,4GHz, 5GHz, Full Band Scanning dedicated Radio): “Type K”.	C/PC/NC

With the OmniAccess Stellar AP1301H and tri-radio Access Point, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 269: OmniAccess Stellar AP1301H Access Point

The OmniAccess Stellar AP1301H Access Point is a highly versatile, and efficient rich Access Point providing, indeed, operational simplicity, quality user experience and high-efficient Wi-Fi beyond the 1Gbps for in room applications such as hotels, classrooms, dormitories, clinics, remote/home office and more… The AP1301H Access Point is an answer to the challenge of the high ports density introduced by the various devices (IP phones, IPTVs...) connected to the network. It allows to make savings on ports and cabling, and the radio coverage in rooms is highly improved and secured. Additionally, the need for site surveys (and associated costs) is also reduced:

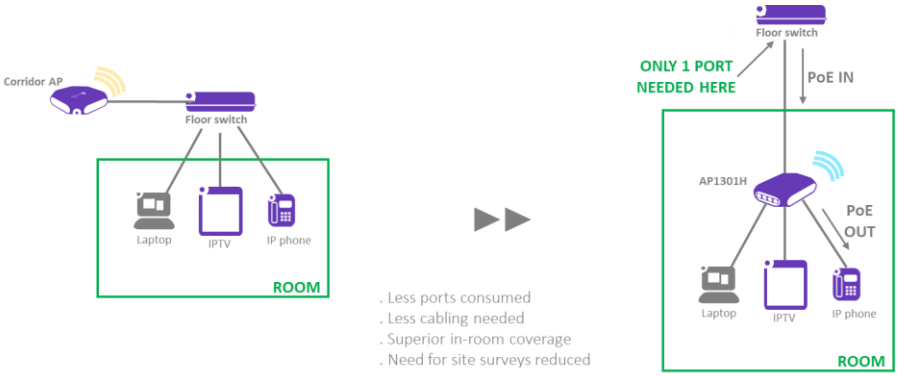


Figure 270: AP1301H deployment and benefits

467.	The “Type K” Access Point shall have integrated omnidirectional antennas.	C/PC/NC

468.	The “Type K” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC

469.	The “Type K” Access Point shall offer up to 1.2Gbps throughput on the 5GHz band and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC

470.	The “Type K” Access Point shall support up to 1024 clients.	C/PC/NC
471.	The “Type K” Access Point shall have three 1Gb Ethernet downlink ports and one of which supports 802.3af PSE to power to the attached device. PoE on PSE port shall be disableable.	C/PC/NC
472.	The “Type K” Access Point shall have one USB 2.0 port capable of supplying up to 5V/500mA power to an attached device.	C/PC/NC
473.	The “Type K” Access Point shall have one pair of RJ-45 passive pass through port (back and bottom).	C/PC/NC
474.	The “Type K” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable.	C/PC/NC
475.	The “Type K” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC
476.	The “Type K” Access Point shall have one 1Gb Ethernet uplink port with 12.7W maximum consumption when USB and PSE function are disabled, or 25W maximum consumption when USB and PSE function are enabled.	C/PC/NC
477.	The “Type K” Access Point shall trust IEEE 802.1q marking on downlink ports.	C/PC/NC

The OmniAccess Stellar AP1301H Access Point allows reception of “tagged” traffic on downlink ports by trusting IEEE 802.1q marking of incoming traffic.

478.	The MTBF for the “Type K” Access Point shall be at least 1,314,000h (150 years).	C/PC/NC
479.	The “Type K” Access Point shall propose a Factory reset button.	C/PC/NC

6.12. Indoor Access Point - Type AL

480.	The WLAN solution shall propose a premium high-end 802.11ax MU-MIMO indoor tetra-radio AP Access Point (2,4GHz, 5GHz, Full Band Scanning dedicated Radio and Bluetooth/Zigbee): “Type L”.	C/PC/NC

With the OmniAccess Stellar AP1331 family (with AWOS release 4.0.4), an 802.11ax and tetra-radio Access Point, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.
AP1331 Access Point is a highly versatile, and efficient rich Access Point providing, indeed, operational simplicity, quality user experience and accommodates the dense and high-capacity needs of next-generation mobility and IoT-enabled networks.

(OmniAccess Stellar AP1331 hardware will be supported by Stellar Wireless Operating System (AWOS) software release 4.0.4 and its description is for reference in RFP document.)

Figure 271: OmniAccess Stellar AP1331 Access Point

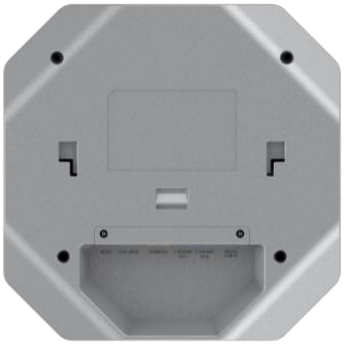


Figure 272: OmniAccess Stellar AP1331 Access Point (Rear View)

481.	The “Type L” Access Point shall have integrated omnidirectional antennas.	C/PC/NC
482.	The “Type L” Access Point shall offer native BLE5/Zigbee radio support.	C/PC/NC
483.	The “Type L” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC
484.	The “Type L” Access Point shall offer up to 2,4Gbps throughput on the 5GHz band and up to 1,15Mbps throughput on the 2.4GHz band.	C/PC/NC

485.	The “Type L” Access Point shall support 80M+80MHz large width mode for sparse AP deployment.	C/PC/NC
486.	The “Type L” Access Point shall support up to 1024 clients.	C/PC/NC
487.	The “Type L” Access Point shall have two 5Gb Ethernet port (IEEE 802.3bz Multi-rate Gigabit Ethernet), which may be aggregated as a single logical link (LACP).	C/PC/NC
488.	The “Type L” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC
489.	The “Type L” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1331 Series Access Points fully comply with this requirement. Please refer to requirement [108].

490.	The “Type L” Access Point shall support 802.3bt/at PoE with 28W maximum consumption.	C/PC/NC
491.	The MTBF for the “Type L” Access Point shall be at least 572.332 h (65.33 years).	C/PC/NC
492.	The “Type L” Access Point shall propose a Factory reset button.	C/PC/NC
493.	The “Type L” Access Point shall propose a console port.	C/PC/NC
494.	The “Type L” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHz) for detecting security and RF anomalies.	C/PC/NC

6.13. Indoor Access Point – Type AM

495.	The WLAN solution shall propose a premium high-end 802.11ax MU-MIMO indoor five built-in radio AP Access Point (**2.4, 5G low, 5G high**): “Type M”.	C/PC/NC

With the OmniAccess Stellar AP1351 series, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The 802.11ax premium high-end OmniAccess Stellar AP1351 is designed to accommodate the very dense and high capacity needs of next generation mobility and IoT-enabled networks.
These APs are powered with five built-in radios, three radios 2.4GHz/5GHz Low and 5GHz High band serving high density Wi-Fi clients, one Full Band Scanning dedicated Radio and Bluetooth/Zigbee radio for IoT.

Figure 273: OmniAccess Stellar AP1351 Series

496.	The “Type M” Access Point shall have integrated omni-directional antennas.	C/PC/NC
497.	The “Type M” Access Point shall offer native Bluetooth5/Zigbee radio support.	C/PC/NC
498.	The “Type M” Access Point shall support up to 48 SSIDs (16 per radio).	C/PC/NC
499.	The “Type M” Access Point shall offer up to 2x 4.8Gbps throughput on the 5GHz band (4.8Gbps on low and high bands) and up to 1,15Gbps throughput on the 2.4GHz band.	C/PC/NC
500.	The “Type M” Access Point shall support 160MHz large width mode for sparse AP deployment.	C/PC/NC
501.	The “Type M” Access Point shall support up to 1536 clients.	C/PC/NC
502.	The “Type M” Access Point shall have two 5Gb Ethernet port (IEEE 802.3bz Multi-rate Gigabit Ethernet) which may be aggregated as a single logical link (LACP).	C/PC/NC
503.	The “Type M” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC
504.	The “Type M” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1351 series Access Points fully comply to this requirement. Please refer to requirement [108].

505.	The “Type M” Access Point shall support 802.3bt/at PoE with 45W maximum consumption.	C/PC/NC

506.	The MTBF for the “Type M” Access Point shall be at least 572,332 h (65.33 years).	C/PC/NC
507.	The “Type M” Access Point shall propose a Factory reset button.	C/PC/NC
508.	The “Type M” Access Point shall propose a console port.	C/PC/NC

6.14. Outdoor Access Point – Type AN

509.	The WLAN solution shall propose a 802.11ac wave2 MU-MIMO low-cost outdoor ruggedized dual-radio AP Access Point. “Type N”	C/PC/NC

With the OmniAccess Stellar AP1261 wave2 and dual-radio AP in a new format for outdoor, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

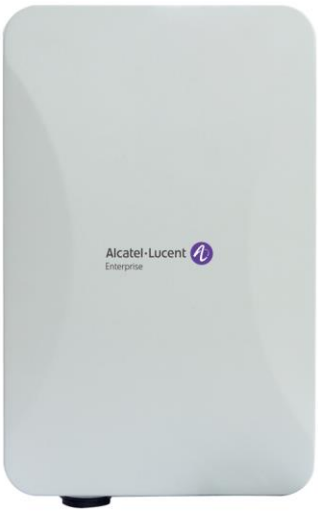


Figure 274: OmniAccess stellar AP1261 Access Point

510.	The “Type N” Access Point shall have integrated omni-directional antennas.	C/PC/NC
511.	The “Type N” Access Point shall support up to 16 SSIDs (8 per radio).	C/PC/NC
512.	The “Type N” Access Point shall offer up to 867Mbps throughput on the 5Ghz band and up to 300Mbps throughput on the 2.4GHz band.	C/PC/NC
513.	The “Type N” Access Point shall support up to 384 clients.	C/PC/NC
514.	The “Type N” Access Point shall have one 1Gb Ethernet port.	C/PC/NC

515.	The “Type N” Access Point shall be IP66/67 certified.	C/PC/NC

516.	The “Type N” Access Point shall support persistent moisture and precipitation, and high and low temperatures: -20°C to 55°C.	C/PC/NC

517.	The “Type N” Access Point shall offer wind resistance: sustained wind at 140 km/h.	C/PC/NC

518.	The “Type N” Access Point shall support 802.3af/at PoE with 20W maximum consumption.	C/PC/NC

519.	The MTBF for the “Type N” Access Point shall be at least 525600h (60 Years).	C/PC/NC

6.15. Indoor Access Point – Type AO

520.	The WLAN solution shall propose a high-end 802.11ax MU-MIMO indoor five built-in radio AP Access Point (**2.4, 5G, 6G**) with extension to the 6GHz band: “Type O”.	C/PC/NC

With the OmniAccess Stellar AP1451, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The 802.11ax high-end OmniAccess Stellar AP1451 is designed to accommodate the very dense and high capacity needs of next generation mobility and IoT-enabled networks. This AP is powered with five built-in radios, three radios 2.4GHz/5GHz and 6GHz serving high density Wi-Fi clients and Wi-Fi 6E capable clients, one Full Band Scanning dedicated Radio and Bluetooth/Zigbee radio for IoT.

Figure 275: OmniAccess Stellar AP1451 access point

521.	The “Type O” Access Point shall have integrated omni-directional antennas.	C/PC/NC

522.	The “Type O” Access Point shall offer native Bluetooth5/Zigbee radio support.	C/PC/NC

523.	The “Type O” Access Point shall support up to 24 SSIDs (8 per radio, Hardware ready for 16 SSIDs per radio)	C/PC/NC
524.	The “Type O” Access Point shall offer up to 4.8Gbps throughput on the 5GHz band, up to 4.8Gbps throughput on the 6GHz band for Wi-Fi 6E capable clients and up to 1,15Gbps throughput on the 2.4GHz band.	C/PC/NC
525.	The “Type O” Access Point shall support 160MHz large width mode for sparse AP deployment. Two 160MHz channels on the 5GHz band and up to seven 160MHz channels on the 6GHz band for Wi-Fi 6E capable clients.	C/PC/NC
526.	The “Type O” Access Point shall support up to 1536 clients.	C/PC/NC
527.	The “Type O” Access Point shall have two 10Gbps Ethernet port (IEEE 802.3bz Multi-rate Gigabit Ethernet) which may be aggregated as a single logical link (LACP).	C/PC/NC
528.	The “Type O” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC
529.	The “Type O” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1451 Access Point fully comply to this requirement. Please refer to requirement [108].

530.	The “Type O” Access Point shall support 802.3bt/at PoE with 49W maximum consumption.	C/PC/NC
531.	The MTBF for the “Type O” Access Point shall be at least 572,332 h (65.33 years).	C/PC/NC
532.	The “Type O” Access Point shall propose a Factory reset button.	C/PC/NC
533.	The “Type O” Access Point shall propose a console port.	C/PC/NC

6.16. Indoor Access Point - Type AP

534.	The WLAN solution shall propose an entry-level 802.11ax MU-MIMO indoor four built-in radio AP Access Point (**2.4, 5G, 6G**) with extension to the 6GHz band: “Type P”.	C/PC/NC

With the OmniAccess Stellar AP1411, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The OmniAccess Stellar AP1411 Access Point is a highly versatile,

and efficient rich Access Point combining, indeed, operational simplicity, quality user experience, high-efficient Wi-Fi and IoT-enabled networks.

This AP is powered with four built-in radios, dual configurable radios 2.4GHz, 5GHz and 6GHz serving high density Wi-Fi clients and Wi-Fi 6E capable clients, one Full Band Scanning dedicated Radio and Bluetooth/Zigbee radio for IoT. WLAN radios can operate in 3 configurable modes:

- 2.4GHz + 5GHz (aggregated data rate up to 1.8Gbps)
- 2.4GHz + 6GHz (aggregated data rate up to 3Gbps)
- 5GHz + 6GHz (aggregated data rate up to 3.6Gbps)

Figure 276: OmniAccess Stellar AP1411 access point

535.	The “Type P” Access Point shall have integrated omni-directional antennas.	C/PC/NC
536.	The “Type P” Access Point shall offer native Bluetooth5/Zigbee radio support.	C/PC/NC
537.	The “Type P” Access Point shall support up to 32 SSIDs (16 per radio, up to 4 for 6GHz radio)	C/PC/NC
538.	The “Type P” Access Point shall offer up to 574Mbps throughput on the 2.4GHz band, up to 1.2Gbps throughput on the 5GHz band and up to 2.4Gbps throughput on the 6GHz band for Wi-Fi 6E capable clients.	C/PC/NC
539.	The “Type P” Access Point shall support 160MHz large width mode for sparse AP deployment. Up to seven 160MHz channels on the 6GHz band for Wi-Fi 6E capable clients.	C/PC/NC
540.	The “Type P” Access Point shall support up to 1024 clients (up to 512 per radio)	C/PC/NC

541.	The “Type P” Access Point shall have one 1Gb Ethernet port and one 2.5Gb Ethernet (IEEE 802.3bz Multi-rate Gigabit Ethernet)	C/PC/NC

542.	The “Type P” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC

543.	The “Type P” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1411 Access Point fully comply to this requirement. Please refer to requirement [108].

544.	The “Type P” Access Point shall support dual 802.3at PoE with 25W maximum consumption.	C/PC/NC

545.	The MTBF for the “Type P” Access Point shall be at least 572,332 h (65.33 years).	C/PC/NC

546.	The “Type P” Access Point shall propose a Factory reset button.	C/PC/NC

547.	The “Type P” Access Point shall propose a console port.	C/PC/NC

6.17. Indoor Access Point - Type AQ

548.	The WLAN solution shall propose premium 802.11ax MU-MIMO indoor five built-in radio AP Access Point (**2.4, 5G, 6G**) with extension to the 6GHz band: “Type Q”.	C/PC/NC

With the OmniAccess Stellar AP1431, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The OmniAccess Stellar AP1431 Access Point is a highly versatile, and efficient rich Access Point delivering high-efficient Wi-Fi with more capacity for bandwidth-hungry and latency-sensitive applications, and IoT-enabled networks. This AP is powered with five built-in radios, tri radios 2.4GHz, 5GHz and 6GHz serving high density Wi-Fi clients and Wi-Fi 6E capable clients, one Full Band Scanning dedicated Radio and Bluetooth/Zigbee radio for IoT.

Figure 277: OmniAccess Stellar AP1431 access point

549.	The “Type Q” Access Point shall have integrated omni-directional antennas.	C/PC/NC
550.	The “Type Q” Access Point shall offer native Bluetooth5/Zigbee radio support.	C/PC/NC
551.	The “Type Q” Access Point shall support up to 36 SSIDs (16 per radio, up to 4 for 6GHz radio)	C/PC/NC
552.	The “Type Q” Access Point shall offer up to 574Mbps throughput on the 2.4GHz band, up to 1.2Gbps throughput on the 5GHz band and up to 2.4Gbps throughput on the 6GHz band for Wi-Fi 6E capable clients.	C/PC/NC
553.	The “Type Q” Access Point shall support 160MHz large width mode for sparse AP deployment. Up to seven 160MHz channels on the 6GHz band for Wi-Fi 6E capable clients.	C/PC/NC
554.	The “Type Q” Access Point shall support up to 1536 clients (up to 512 per radio)	C/PC/NC
555.	The “Type Q” Access Point shall have two 2.5Gb Ethernet (IEEE 802.3bz Multi-rate Gigabit Ethernet) which may be aggregated as a single logical link (LACP).	C/PC/NC
556.	The “Type Q” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable.	C/PC/NC
557.	The “Type Q” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1431 Access Point fully comply to this requirement. Please refer to requirement [108].

558.	The “Type Q” Access Point shall support dual 802.3at/bt PoE with 34W maximum consumption.	C/PC/NC

559.	The MTBF for the “Type Q” Access Point shall be at least 572,332 h (65.33 years).	C/PC/NC

560.	The “Type Q” Access Point shall propose a Factory reset button.	C/PC/NC

561.	The “Type Q” Access Point shall propose a console port.	C/PC/NC

6.18. Indoor Access Point – Type AR

562.	The WLAN solution shall propose a premium tri-radio 802.11be MU-MIMO indoor Access Point (**2.4, 5G, 6G**) with 5 integrated radios: "Type R"	C/PC/NC

With the OmniAccess Stellar AP1511 (AWOS 5.0.1), the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully meets this requirement. The OmniAccess Stellar AP1511 802.11be premium is designed to meet the high-density and high-capacity needs of next-generation mobility and IoT networks, delivering unparalleled connectivity with operational simplicity. This access point is equipped with five integrated radios: three radios for 2.4GHz/5GHz/6GHz for the latest generation of Wi-Fi clients (Wi-Fi 7), a dedicated full-band scanning radio, and a Bluetooth/Zigbee radio for IoT.

Figure 278: OmniAccess Stellar AP1511 access point

563.	The “Type R” Access Point shall have integrated omni-directional antennas.	C/PC/NC

564.	The “Type R” Access Point shall offer native Bluetooth5/Zigbee radio support.	C/PC/NC

565.	The “Type R” Access Point shall support up to 36 SSIDs (16 per radio, up to 4 in	C/PC/NC

	the 6GHz radio)	

566.	The "Type R" access point shall offer an aggregated throughput of up to 9.328 Gbps (up to 688 Mbps on the 2.4GHz band, up to 2.882 Gbps on the 5GHz band, and up to 5.76 Gbps on the 6GHz band)	C/PC/NC

567.	The “Type R” Access Point shall support 160MHz large width mode for sparse AP deployment. Up to seven 160MHz channels on the 6GHz band for Wi-Fi 6E capable clients.	C/PC/NC

568.	The “Type R” Access Point shall support the 320 MHz wideband mode for sparse AP deployment, with up to three 320 MHz channels on the full 6 GHz band (5925-7125 MHz).	C/PC/NC

569.	The “Type R” Access Point shall support up to 768 clients (up to 256 per radio)	C/PC/NC

570.	The “Type R” Access Point shall have one 5Gb Ethernet port (IEEE 802.3bz Multi-rate Gigabit Ethernet)	C/PC/NC

571.	The “Type R” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC

572.	The “Type R” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1511 Access Point fully comply to this requirement. Please refer to requirement [108].

573.	The “Type R” Access Point shall support PoE compliant with 802.3at, with 23.4W maximum consumption.	C/PC/NC

574.	The MTBF for the “Type R” Access Point shall be at least 1,075,632 h (122.79 years).	C/PC/NC

575.	The “Type R” Access Point shall propose a Factory reset button.	C/PC/NC

576.	The “Type R” Access Point shall propose a console port.	C/PC/NC

577.	The "Type R" access point shall offer a mounting kit for flat surfaces (wall/ceiling or junction) compatible with standard wall mounts and pre-drilled holes for enterprise Wi-Fi access points.	C/PC/NC

6.19. Indoor Access Point – Type AS

578.	The WLAN solution shall propose a premium tri-radio 802.11be MU-MIMO indoor Access Point (**2.4, 5G, 6G**) with 5 integrated radios: "Type S"	C/PC/NC

With the OmniAccess Stellar AP1521 (AWOS 5.0.1), the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully meets this requirement. The premium 802.11be OmniAccess Stellar AP1521 is designed to meet the high-density and capacity needs of next-generation mobility and IoT networks, providing unparalleled connectivity with operational simplicity. This access point is equipped with five integrated radios: three radios (2.4GHz, 5GHz, 6GHz) for next-generation Wi-Fi clients (Wi-Fi 7), one dedicated full-band scanning radio, and one Bluetooth/Zigbee radio for IoT.

Figure 279: OmniAccess Stellar AP1521 access point

579.	The “Type S” Access Point shall have integrated omni-directional antennas.	C/PC/NC
580.	The “Type S” Access Point shall offer native Bluetooth5/Zigbee radio support.	C/PC/NC
581.	The “Type S” Access Point shall support up to 48 SSIDs (16 per radio)	C/PC/NC
582.	The "Type S" access point shall offer an aggregated throughput of up to 12.2 Gbps (up to 688 Mbps on the 2.4GHz band, up to 5.76 Gbps on the 5GHz band, and up to 5.76 Gbps on the 6GHz band)	C/PC/NC
583.	The “Type S” Access Point shall support 160MHz large width mode for sparse AP deployment. Up to seven 160MHz channels on the 6GHz band for Wi-Fi 6E capable clients.	C/PC/NC
584.	The “Type S” Access Point shall support the 320 MHz wideband mode for sparse AP deployment, with up to three 320 MHz channels on the full 6 GHz band (5925-7125 MHz).	C/PC/NC

585.	The “Type S” Access Point shall support up to 1,280 clients (512 per radio, up to 256 on the 2.4GHz band)	C/PC/NC

586.	The "Type S" access point must have a 10 Gbps Ethernet port (IEEE 802.3bz Multi-rate Gigabit Ethernet) and a 1 Gbps Ethernet port, which can be aggregated into a single logical link (LACP).	C/PC/NC

587.	The “Type S” Access Point shall offer additional Ethernet support through USB port (via an attached device). Ethernet interface through USB (AWOS 5.0.1) shall be disableable	C/PC/NC

588.	The “Type S” Access Point shall propose *L7 Application recognition* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1521 Access Point fully comply to this requirement. Please refer to requirement [108].

589.	The "Type S" Access Point shall support PoE 802.3bt/at with a maximum power consumption of 40.2W.	C/PC/NC

590.	The MTBF for the “Type S” Access Point shall be at least 650,124 hours (74.22 years).	C/PC/NC

591.	The “Type S” Access Point shall propose a Factory reset button.	C/PC/NC

592.	The “Type S” Access Point shall propose a console port.	C/PC/NC

593.	The "Type S" access point shall offer a mounting kit for flat surfaces (wall/ceiling or junction) compatible with standard wall mounts and pre-drilled holes for enterprise Wi-Fi access points.	C/PC/NC

6.20. Certifications

594.	The WLAN solution shall be certified by recognized Wi-Fi compliance organizations and in particular by Wi-Fi Alliance, which certifies the compliance of the access points listed above against performance and interoperability requirements.	C/PC/NC

Alcatel-lucent Enterprise OmniAcces Stellar WLAN solution fully complies with this requirement. The access points are certified by the Wi-Fi Alliance and evaluated against performance and interoperability requirements, including the following certifications:

- Wi-Fi CERTIFIED 7: Stellar access points comply with the 802.11be (Wi-Fi 7) standard, supporting

ultra-wideband channels and multi-link operations to enhance capacity, bandwidth, and connection reliability for demanding applications like multimedia, cloud, and advanced applications (virtual reality, big data) in heavily loaded network environments.

- Wi-Fi CERTIFIED 6E: Stellar access points comply with the 802.11ax (WiFi 6E) standard, which supports the new 6 GHz frequencies and aims to extend the capacity, performance and benefits of Wi-Fi 6 to 6 GHz frequencies.
- Wi-Fi CERTIFIED 6: Stellar access points comply with the 802.11ax (WiFi 6) standard, offering improved performance and the ability to handle more simultaneous connections.
- Wi-Fi CERTIFIED 5: Stellar access points comply with the 802.11ac (WiFi 5) standard, offering better performance than previous generations.

595.	The WLAN solution shall be certified by recognized standards in security and in particular by Common Criteria process which realizes evaluation of access points listed above against security requirements.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Stellar Access Points are certified by Common Criteria standard and evaluated against security requirements. With the arrival of new access points ALE pursuits this type of certification on security, for more information on the tests performed with Stellar access points and on Common Criteria release EAL 2 certification please refer to CC portal: *Common Criteria : New CC Portal (commoncriteriaportal.org)*

596.	The WLAN solution shall be certified by recognized standards for the safety of installations with electronic equipment, and in particular by UL2043 which evaluates the access points listed above in terms of their ability to reduce the risk of fire.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Stellar access points are UL2043 certified and have been evaluated under specific installation conditions in suspended ceilings, or plenum spaces. Their design and manufacture are designed to withstand the specific conditions of these environments, while reducing the risk of fire and smoke propagation.

597.	The WLAN solution shall be certified by recognized standards for the safety of electro-medical equipment, and in particular by EN60601-1-1 and EN60601-1-2, which assess the access points listed above with regard to the safety of patients, medical staff or other persons, and their electrical compatibility with medical installations.	C/PC/NC

Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Stellar access points are certified to EN60601-1-1 and EN60601-1-2 standards relating to the safety of electro-medical equipment.

- EN60601-1-1 is specific to medical electrical equipment. Its main aim is to guarantee the safety of patients, medical staff and other people in contact with such equipment. It deals with the electrical risks associated with medical equipment.
- EN60601-1-2 focuses on the electromagnetic compatibility (EMC) of electro-medical equipment. Its aim is to ensure that medical equipment does not create harmful electromagnetic interference, nor is sensitive to such interference, which could disrupt the operation of other medical equipment or the Wi-Fi network used in medical facilities.