Alcatel-Lucent Enterprise OmniVista® Cirrus 10.5 GOLDEN RFP

Release Version	Date	Comments
10.4.3	December 2024	
10.5.1	July 2025	

Table of Contents

Table of figures

Introduction

Alcatel-Lucent OmniVista® Cirrus release 10, a new cloud SaaS Network Management solution offers advanced centralized Wireless visibility and configuration for Alcatel-Lucent Stellar Enterprise Access Points, is a scalable, resilient, secure, native, cloud-based network management system for unified access, offered as a subscription service. Relying on state-of-the-art microservices architecture and developed with the latest DevOps methodologies and tools, OmniVista® Cirrus Release 10 facilitates your digital transformation. It allows you to respond to business needs such as real-time analytics, monitoring the Quality of Experience (QoE) for wireless Wireless User, zero trust access policies, micro-segmentation, and Internet of Things (IoT) total enablement, including identification of network-connected devices.

OmniVista® Cirrus provides an easy-to-deploy, effective way to manage and monitor Alcatel Lucent OmniAccess® Stellar Access Point infrastructure. It offers advanced analytics for proactive service assurance and Unified Policies Access Manager (UPAM), a Network Access Control (NAC) module that includes enterprise authentication, role management, policy capabilities for guest access, and BYOD. OmniVista® Cirrus is designed to improve wireless user insights by providing detailed user QoE and behaviour analytics.

OmniVista® Cirrus is a subscription-based service that facilitates alignment with your new business imperatives. Ease of purchasing, provisioning and ongoing daily operations are at the core of OmniVista® Cirrus. Shifting to a cloud-based network management solution with OmniVista® Cirrus simplifies digital transformation by reducing cost and administrative IT burden.

OmniVista® Cirrus sets a new IT experience standard for simple yet powerful capabilities. It can scale and adapt to your business requirements. It offers advanced visibility and control over users and applications. By focusing on core IT operations, the comprehensive management OmniVista® Cirrus solution makes it easy to improve application performance and troubleshoot issues in deployments with distributed locations and limited IT staff. OmniVista® Cirrus protects your network infrastructure investment by adapting to changing business needs without the expense of “rip and replace”.

OmniVista® Cirrus, as a native cloud-based network management platform backed with a microservices architecture, delivers valuable outcomes such as continuous improvement without downtime, always up-to-date management platform, scalability and security. The automatic software update, including critical security patches, improves security and compliance.

Datasheet

https://www.al-enterprise.com/-/media/assets/internet/documents/omnivista-cirrus-network-management-as-a-service-datasheet-en.pdf

Scope

This document covers the features and improvements which are relatively new to this release and specific to OmniVista® Cirrus 10.5 and will not cover Stellar WLAN features. Please refer to the Stellar WLAN Enterprise Golden RFP for Wireless LAN specific features.

Golden RFP – Minimum Supported Features

1. Ordering and Activation

1.	The cloud-based NMS shall support a seamless Quote-to-Cash process, enabling self-service to simplify the ordering and customization processes for the administrator	C/PC/NC

NMS Cloud is based on the Quote-to-Cash (QTC) offering model. The model provides ease of use and transparency throughout the process of ordering and registration of OmniVista® Cirrus 10 as SaaS Cloud solution.

Ebuy page for OmniVista® Cirrus is accessible on myPortail in self-service

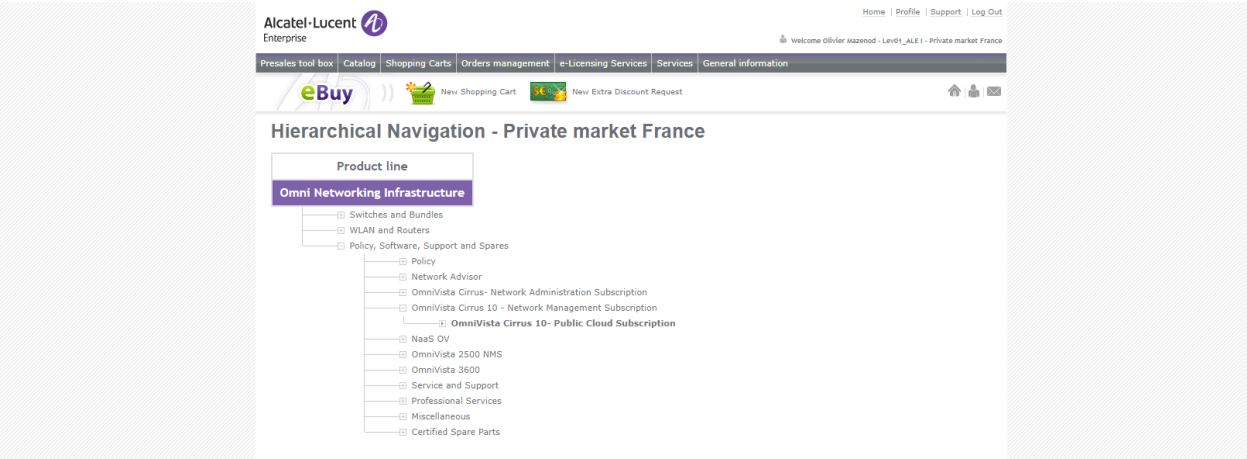


Figure 1: License Ordering for Omnivista Cirrus 10 – ebuy.businesspartner.al-enterprise.com

Local ALE pre-sales teams are available to guide through the quotation process for complex configurations for OmniVista® Cirrus 10. ALE offer details the services and features offered by NMS Cloud, the different levels service level (SLA) and price.

- Configuration of the offer can be personalized according to specific needs such as storage options, computing power or even security.

Flexible and transparent facturation for OmniVista® Cirrus 10

- Based only on use of the services consumed

Provides full cost visibility and proactive management of IT budget for the administrator.

2.	The cloud-based NMS shall follow a flexible SaaS subscription model	C/PC/NC

NMS SaaS is based on two Cloud subscription models with licensing for 8 categories of LAN/WLAN device.

- FlexPay is the initial full OPEX model and managed via MyPortal/MyShopping tool
- Capex (version 10.4) which is the CAPEX model including BUSINESS and PREMIUM services bundles and managed via Ebuy & OVC-SM subscription manager

With different subscription durations and services bundles:

- 1Y, 3Y and 5Y subscription durations with access to all NMS functionnalities
- BASE service, BUSINESS service bundle (Partner Plus), PREMIUM bundle (End Customer Plus)
- Flexible free trial mode for up to 360 days with access to all NMS functionnalities

The NMS SaaS Cloud subscriptions are designed to adapt to demand, consequently the licensing model is likely to evolve in future releases.

3.	The cloud-based NMS shall support its own management interface allowing a flexible management of subscription life cycles, purchased licenses and adapted support for the different offers proposed	C/PC/NC

NMS Cloud (version 10.4) has its own subscription and licenses manager (OVC-SM) allowing a common approach for the management of subscriptions for OmniVista® Cirrus 10 and also OmniVista® Cirrus 4. Each OmniVista® Cirrus solution has its management page:

- Creation/extension and renewal of subscriptions from the subscription manager
- Transfer of licenses to support a Value-Added distributor to Indirect Reseller model
- View of purchased licenses
- Update from BASE bundle to BUSINESS/PREMIUM bundles
- History of operations by subscriptions

The figures show the Capex subscriptions and the licenses purchased for a VAD and its various users.

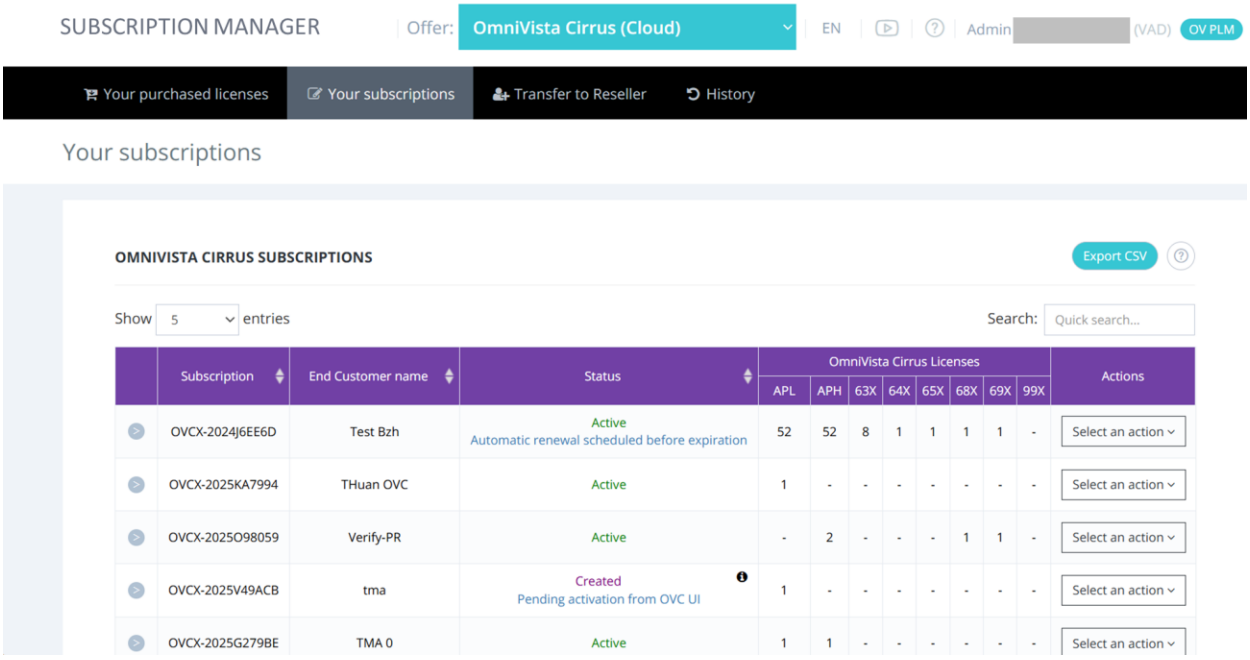


Figure 2: View of subscriptions (OVC-SM VAD) – licensemanager.al-enterprise.com

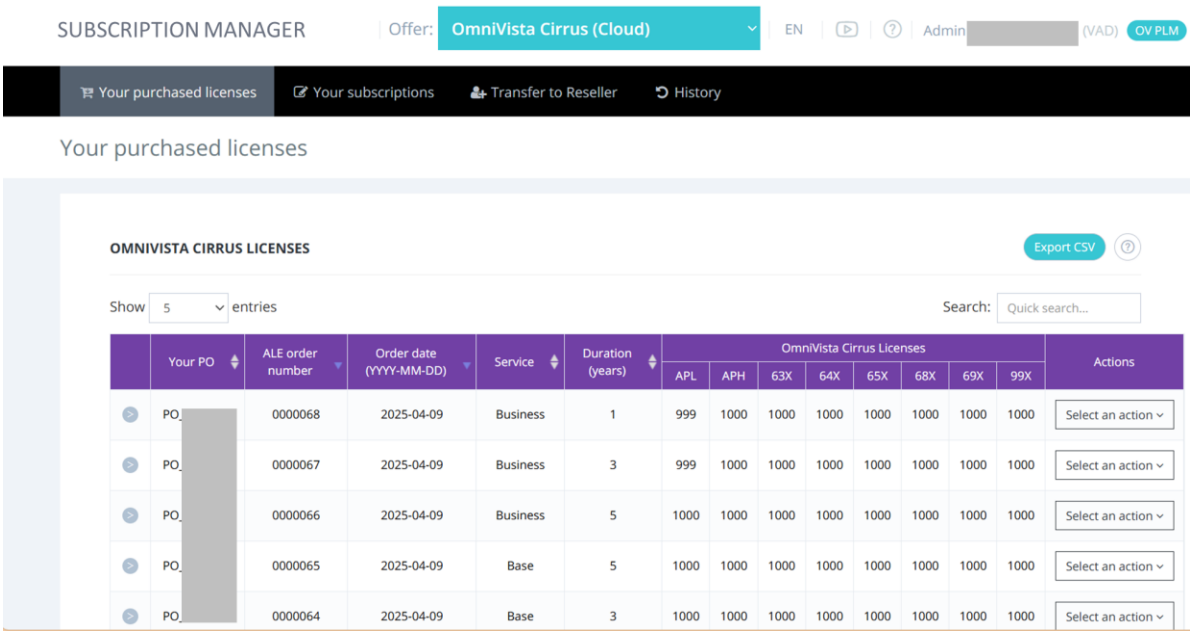


Figure 3: View of purchased licenses (OVC-SM VAD) – licensemanager.al-enterprise.com

4.	The cloud-based NMS licensing and pricing shall be based on devices categories	C/PC/NC

NMS Cloud offers a license paid model for 8 categories of LAN/WLAN device. Licenses are purchased from Ebuy and all license families are available for devices at a progressive price:

- APL - Stellar AP Low End (AP1x0x i.e. 1201, 1301,1401), AP1x1x (i.e. 1211, 1311, 1411) and AP1x2x (i.e. 1221, 1321, 1421) Stellar access points)
- APH – Stellar AP High End (all other models)
- 63X - license for OS63xx switches
- 64X - license for OS64xx switches
- 65X - license for OS65xx switches
- 68X - license for OS68xx switches
- 69X - license for OS69xx switches
- 99X - license for OS99xx switches

One license is consumed per device and license activates all features on device (AOS 8.9R4 recommended). There are no licenses for Guest or BYOD users. The importation of licenses in OVNG10 is based on the subscription IDs, order IDs, and activation codes received by email at the time of purchase, according to the Capex/Flexpay subscription model chosen for a client.

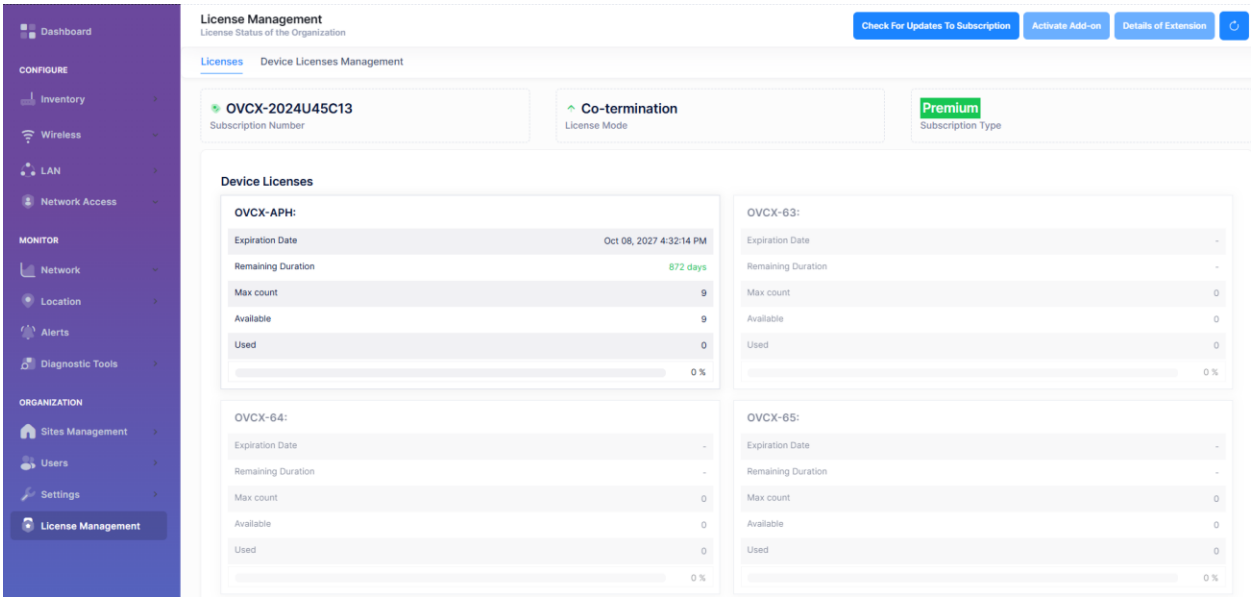


Figure 4: License dashboard - License Management [ORGA]

2. Architecture and Solution Overview

5.	The cloud-based NMS shall be hosted in SOC1 and SOC2 compliant and energy-efficient data centers	C/PC/NC

Cloud-based NMS 10.5 is an application hosted in the following OVH data centers:

- DC in Frankfurt, serving the EU and APAC/ANZ regions
- DC in West Virginia (USA), serving the North America and South America regions

NMS benefits then from the features provided by the OVH platform:

- Global cloud infrastructure: allows the deployment of the NMS application close to customers
- Data maintenance, data localization, and compliance with local regulations: EU, US, or rest of the world

OVH platform complies with SOC 1 (Service Organization Control 1) requirements. This certification confirms that the internal controls implemented by OVH as a cloud operator, concerning financial information, are adequately designed and operate effectively to protect the sensitive business data handled by the cloud NMS.

OVH platform also complies with SOC 2 (Service Organization Control 2), which focuses on five trust principles: security, availability, processing integrity, confidentiality, and privacy. SOC 2 compliance demonstrates that OVH's services adhere to strict data management standards for cloud NMS, ensuring their protection against cyber threats and guaranteeing their confidentiality and integrity.

In a continuous effort to improve the energy consumption of its data centres, OVH holds the ISO 50001 certification, which attests that OVH follows rigorous practices to enhance the energy performance of its data centres. OVH also holds the ISO 14001 certification, which attests to its commitment to minimizing the environmental impact of its data centres.

6.	The cloud-based NMS shall be based on a micro-services architecture for high-availability and resiliency	C/PC/NC

The micro-services architecture chosen for the NMS application meets the requirements for availability and scalability. OVH cloud uses Kubernetes to orchestrate containers, enabling efficient deployment, management, and scaling of microservices. OVH Containerization distributes workloads across multiple nodes, ensuring high availability and horizontal scalability. OVH auto-scaling and service mesh ensure efficient traffic distribution and enhanced resilience, capable of handling thousands of requests per second to manage over 12,000 LAN & WLAN devices.

OVH cloud global presence (Point of Presence) ensures fast and reliable connectivity, facilitating global workload distribution.

In terms of storage, OVH cloud offers distributed storage solution (like Ceph) and managed databases, capable of handling massive data volumes while ensuring rapid response times.

To maximize resilience, NMS application is deployed across multiple regions and availability zones, ensuring seamless failover in case of datacenter failure and thus guaranteeing service continuity.

7.	The cloud-based NMS shall be designed with scalability in mind to allow large number of devices without requiring new equipment or deployment design change.	C/PC/NC

From few to a thousand devices NMS is designed to be scalable up to a total of 12,000 devices per instance. This includes up to 10,000 Stellar access points (any models) and up to 2,000 OmniSwitches (refer to models supported) without requiring changes in deployment or addition of third-party components to support XL/multi-tenant LAN & WLAN networks.

This is not a limit in term of architecture and limits are expected to evolve in future releases.

8.	The cloud-based NMS shall comply with data privacy, security and regulatory frameworks in US, EU, and abroad	C/PC/NC

The cloud-based NMS complies with international regulations such as ISO 27001 for information security management. Specifically for Europe, NMS adheres to GDPR for personal data protection. In the United States, NMS meets local regulations including HIPAA for healthcare data protection, FIPS 140-2, and NIST standards. This ensures that the application meets compliance requirements across different regions worldwide.

9.	The cloud-based NMS shall be hosted in a public cloud environment based on regional DCs	C/PC/NC

NMS can be hosted in a public cloud environment based on regional data centers, leveraging well-known solutions such as Azure (Microsoft Azure), Google Cloud, or AWS (Amazon Web Services). These cloud providers have data centers in various countries, allowing NMS to store data locally to comply with local regulations. This approach ensures that NMS benefits from shared cloud services while maintaining the security and confidentiality of its data.

10.	The cloud-based NMS shall support any XL/Multi-tenant deployment (single/Multi-tenant, single/Multi-site) and offer advanced management functionalities, this without third party additional component	C/PC/NC

NMS Cloud provides advanced features for LAN & WLAN and a single pan of glass for the entire network management via a single platform.

The deployment mode is called *Enterprise mode* from the Cloud and ALE OmniVista® Cirrus 10 Network Management System (NMS) is deployed on Omniswitch equipment (refer to supported models) and Stellar access points (any model) to carry out management, the configuration and monitoring of all equipment for maximum scalability.

Figure 5: Omnivista Cirrus 10

The general idea for designing a enterprise network and managing devices as logical entities for any XL/Multi-site and Multi-tenant/Multi-organisations configurations:

- Centralize LAN & WLAN visibility and management from the Cloud
- Deliver SaaS NMS solution with multi-tenant/multi-organization support Provide a scalable, resilient, secure and cloud-based solution.
- Provide advanced analytics services
- Control the Quality of the Experience (QoE)
- Enable the Internet of Things (IoT)
- Manage all ALE equipment in a unified way, introducing OmniSwitch management (version 10.4)
- Manage Stellar Access Points in a unified manner by introducing Remote Access Points (RAP) management (version 10.5)

- Ensure network assistance and preventive maintenance (with the use of AI-based tools in future releases)

OmniVista® Cirrus 10 supports a new communication model with managed equipment and particular for LAN and OmniSwitches (AOS 8.9R4 AMS application, AOS 8.9R1 also possible)

- The operating mode between OVNG10 and OmniSwitches is automatically downloaded, installed and launched once OmniSwitch is added to the inventory and interact in Push-report model, on demand
- MQTT based light weight asynchronous configurations
- LAN monitoring is based on AOS8 AMS event reporting, on demand

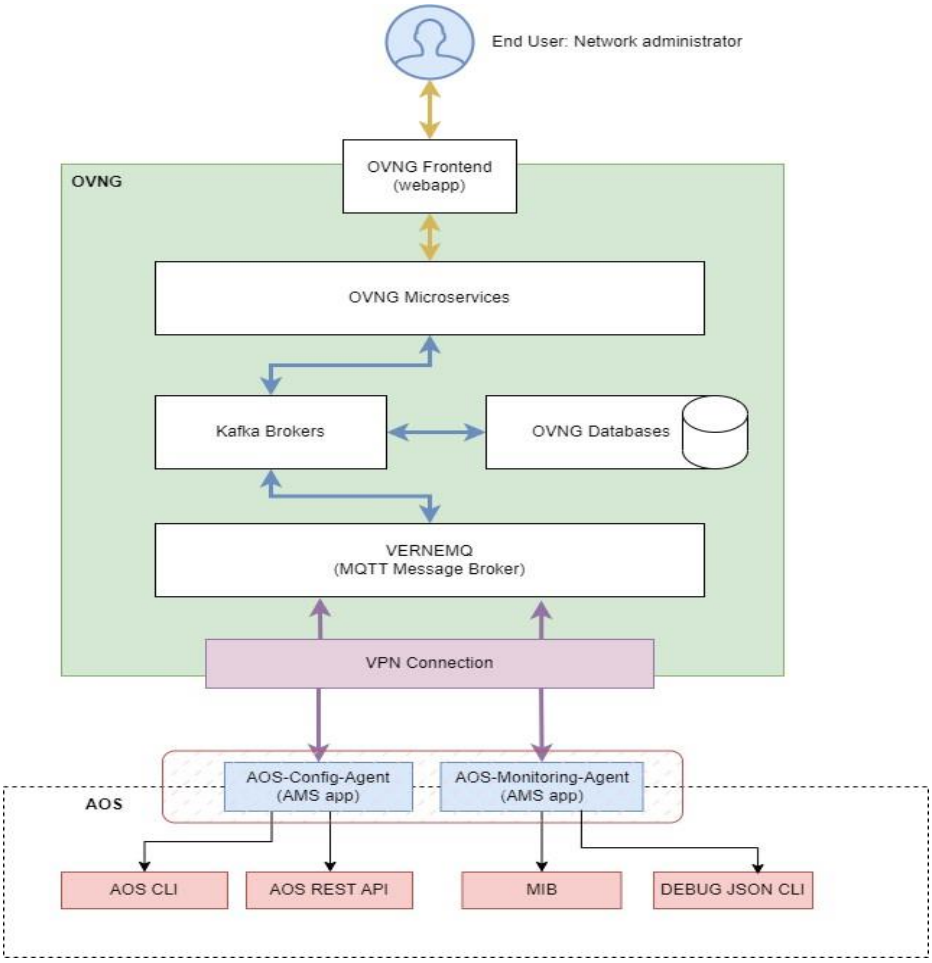


Figure 6: Omnivista Cirrus 10 LAN communication model

OmniVista® Cirrus 10 (version 10.4) introduces the LAN management:

- Unified management with focus on onboarding, LAN inventory and template configuration
- Unified monitoring including topology, OmniSwitch details with analytics
- Unified assurance (alerts & events)
- Support for OmniSwitches with AOS 8.9.R4 minimum (AOS 8.9R4 recommended)

OmniVista® Cirrus10 (version 10.5) introduces the management of WLAN Stellar Access Points in RAP mode:

- An organization defines specifically the onboard of APs in RAP mode (see also item 30 in Multi-tenancy and Multi-site services).
- Management of each Stellar RAP remains centralized at the NMS OmniVista® 10 level like for other APs.
- In the RAP architecture VPN VA server is exclusively installed in the On-Premise Data Center.
- VPN data server dedicated to the RAP organization is defined at the time of creation (server IP addresses and VPN clients data pools).

11.	The cloud-based NMS shall propose an centralized management function based on embedded and secure Web GUI	C/PC/NC

NMS Cloud meets this demand, the Enterprise mode from the Cloud and management on OmniVista® Cirrus 10 NMS offers a secure Web interface (HTTPS) to the end user.

NMS Cloud supports multi-factor authentication to access accounts through the Web, thus strengthening security. NMS Cloud also carries out security updates (CVE) to correct vulnerabilities as well as framework maintenance upgrades
for Web components (Metronix, Quarkus, MongoDB)

12.	The cloud-based NMS shall be able to manage both wired equipment (LAN) and wireless equipment (WLAN) in a “unified management” approach.	C/PC/NC

OmniVista® Cirrus 10 NMS as a part of OmniVista® solution for Enterprise mode provides an unified management approach of the whole ALE network. This unified LAN/WLAN management is detailed in Network Access Control chapter. NMS Cloud management specifically for Stellar is not developed in this document.

13.	The cloud-based NMS shall ensure the integrity of the LAN /WLAN network by supporting optimal monitoring, management and security features on the network.	C/PC/NC

Cloud-based NMS fully complies, NMS Cloud monitors the network and manages OmniSwitch and Stellar access points using Single Network Management Protocol (SNMP). Monitoring is now secured with SNMP version 3 for all equipment to collect, organize equipment information (based on MIB structure) and verify activity of device registered in Ominivista Cirrus 10 NMS.
SNMPv3 is also advantageously use for monitoring LAN/WLAN network with 3th-party network hypervisor. Legacy SNMPv2 and standard SNMP versions stay supported.

OmniVista® NMS Cloud optimizes the security of registered devices with several features. OmniVista® allows to provide additional information on the attachment of devices using dynamic IP configuration by inserting specific data into the DHCP option 82. In particular DHCP relay supports the Circuit ID information to identify the device attachment point.

For Stellar access points OmniVista® NMS also frees the WLAN network from any impersonation of Stellar APs (known as rogue APs) by fully managing a switch port-based 802.1x identification for APs and applying an access role (port-based ARP) in OmniVista® Cirrus 10.
The administrator can then either use built-in PKI and certificates or import customer's PKI and certificate(s) into OmniVista® Cirrus 10 for a totally private site configuration for devices identification.

3. Deployment

14.	The cloud-based NMS shall have a simplified deployment process with plug-and-play features	C/PC/NC

Cloud-based NMS offers a streamlined deployment process characterized by following integrated features:

NMS Managed Service Provider (MSP) supports a multi-administrator environment and enables each organization defined in NMS to assign one or multiple administrators to manage the system.

The process of declaring equipment or performing mass provisioning, particularly during migrations, is easily done. Cloud-based NMS facilitates the inventory and equipment catalog management, ensuring all devices are accounted for all organisations and sites managed by NMS.
Provisioning profiles further complete the deployment process by providing detailed configurations for each OmniSwitch and Stellar access point.

Furthermore NMS site management is facilitated through detailed maps that include buildings and floors configurations, along with topologies, to provide a clear visual representation of all deployed geographic locations within each organization.

This comprehensive geographic visualization supports multi-organization and multi-site deployments, enhancing the management and oversight of networks infrastructures to ensure all equipment is clearly seen placed and easily accessible for their monitoring and maintenance by administrators.

15.	The cloud-based NMS shall support Zero-touch Provisioning	C/PC/NC

The cloud-based NMS (version 10.4) introduces the Zero-touch Provisioning (ZTP) on OmniSwitch with a feature that facilitates the automated onboarding for each switch. This includes CLI Push configuration on switch based on configuration templates, ensuring

simplified configuration and finalize provisioning for OmniSwitch (AOS8) without manual intervention.

ZTP Push configuration maps the main LAN variables defined for the site (variables are handled in same menu)

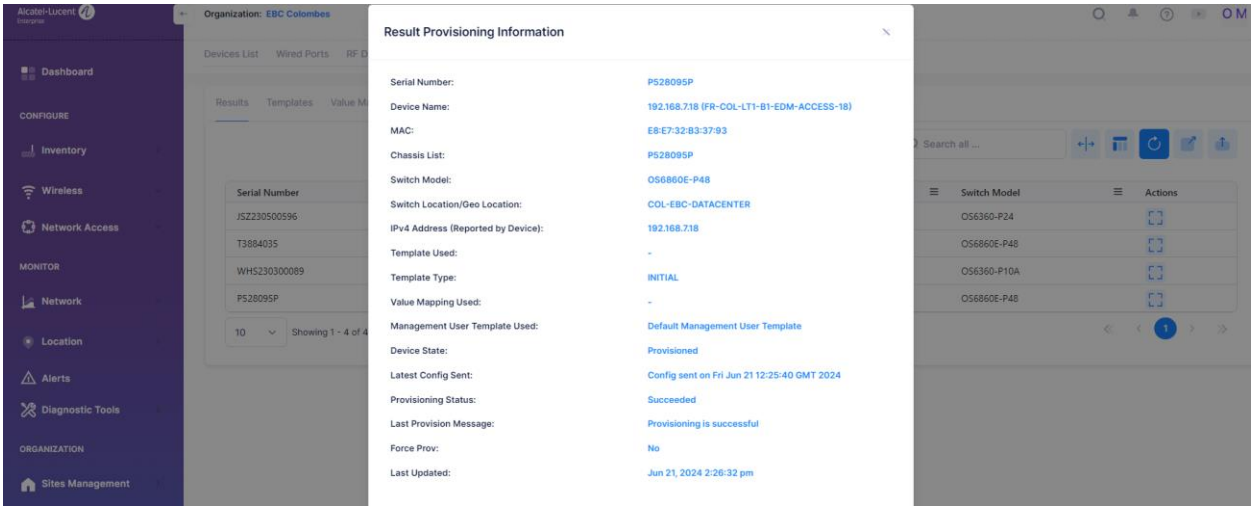


Figure 7: Initial template result for OS6860E - Device Catalog [CONF] CLI Based Provisioning

16.	The cloud-based NMS shall support device objects grouping for easier provisioning of equipment for a given organization or site	C/PC/NC

NMS cloud (version 10.4) introduces the grouping of objects such as Stellar access points, OmniSwitches, or even others (ports) by applying a labelling for each one for a better provisioning of equipment for the site. Thus some configurations can be facilitated by working only on common labels for equipment.

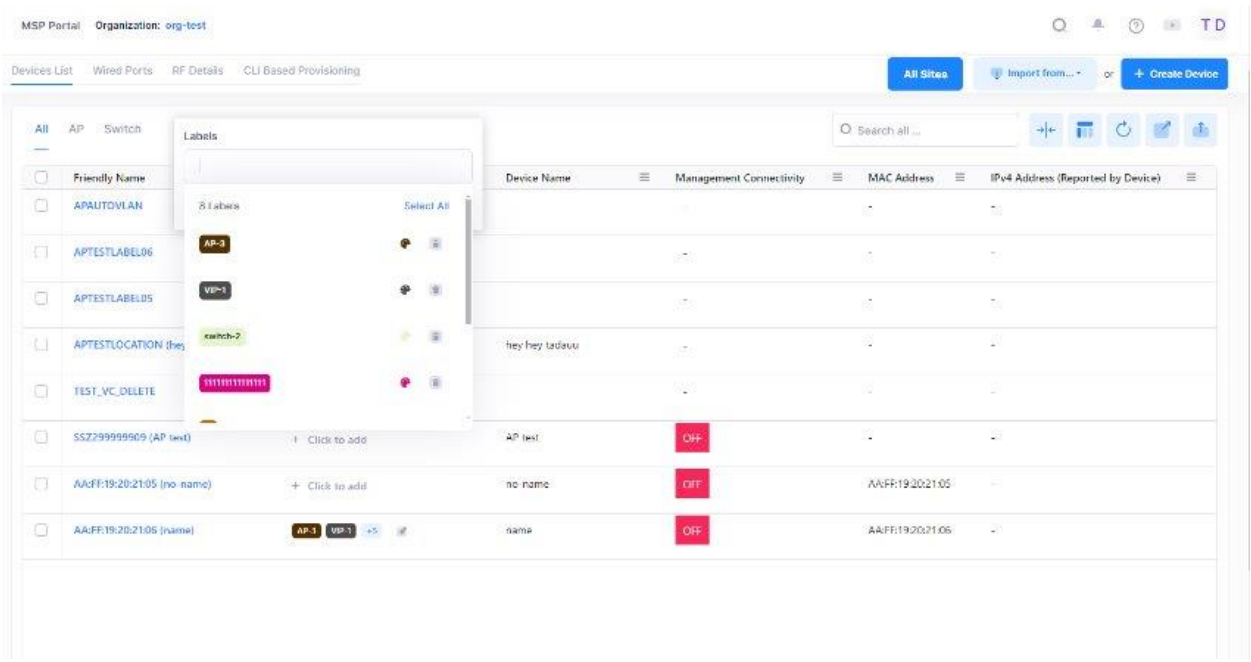


Figure 8: Create and Manage equipment labels - Device Catalog [CONF]

17.	The cloud-based NMS shall provide a simple migration process from an on-premises deployment to the cloud	C/PC/NC

The OmniSwitch network is designed with future evolutions in mind. The migration of Stellar access points from Express/OV2500 modes to the Cloud is already detailed in the Golden RFP Stellar document.

The OmniSwitch management modes Webview2.0/CLI, 2500, OV Terra 10, OV Cirrus 4 or 10 are generally exclusive. The migration from an on-premise management mode to OmniVista® Cirrus 10 mode happens naturally as soon as the switch has Internet access. The operating mode at the boot of an AOS8 switch is as follows:

- The switch obtains its IP configuration either from a DHCP server (by default) or statically.
- Once the Internet configuration is established, the switch's Cloud agent contacts OmniVista® Cirrus 10. If the switch is already registered (serial number and MAC address) in an OVNG10 instance, the switch's operational mode permanently shifts to Cloud mode.

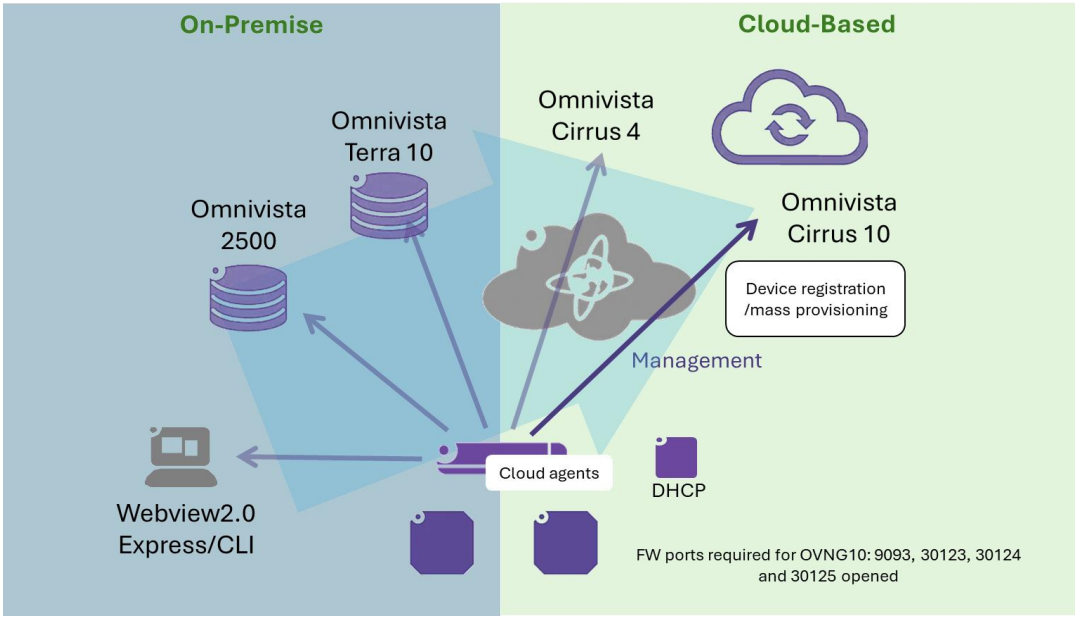


Figure 9: Migration to Omnivista Cirrus 10

For a switch already operating in OV2500, OmniVista® Terra 10 or OmniVista® Cirrus 4 mode, it is sufficient to restart the Cloud agent, ensuring beforehand that the switch and Stellar access points registration migrated to an OmniVista® 10 inventory. In case of mass provisioning:

- From Webview2.0/CLI modes: A simple registration of the equipment in NMS is sufficient.
- From Ominivista 2500, OmniVista® Terra 10 or OmniVista® Cirrus 4 modes: The mass provisioning is done by importing OmniVista® 2500, OmniVista® Terra or OmniVista® Cirrus 4 inventory files for an organisation.

Full management mode is set by default in the case of a complete device migration to OmniVista® Cirrus 10, analytics mode only is possible for device remaining managed in Webwiew2.0/Express/CLI or OV2500/OV Terra 10 /OV Cirrus 4 modes.

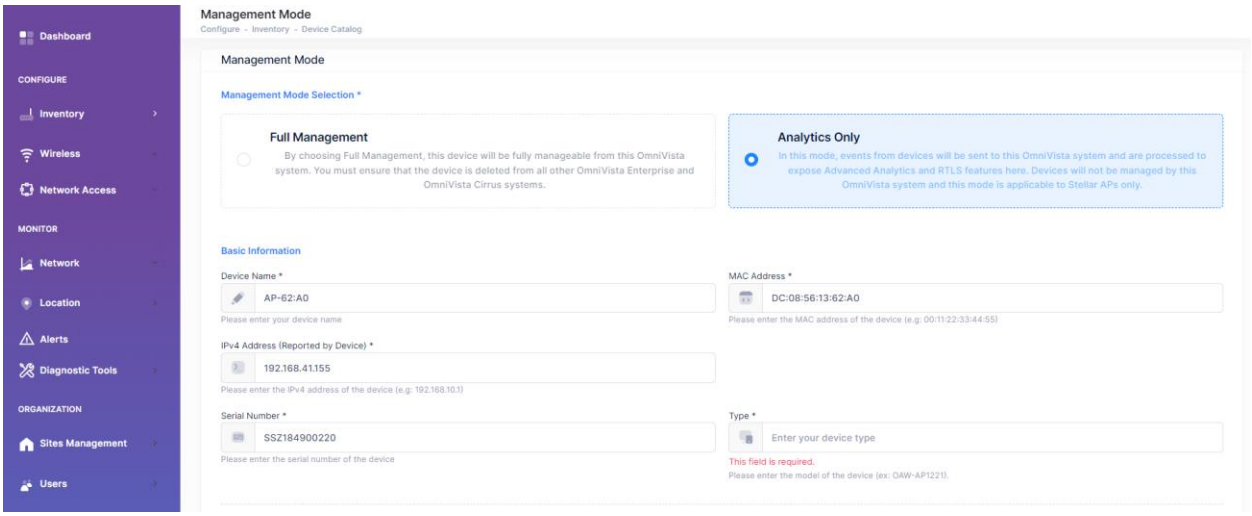


Figure 10: Management mode - Device Catalog [CONF]

4. Multi-tenancy and multi-site services

18.	The cloud-based NMS shall allow multi-tenancy services for MSP including inventory management, user management control, and alerting capabilities from a single supervisor account and dashboard	C/PC/NC

There are 2 levels of administration for NMS users: Managed Service Provider (MSP) level and multi-tenant level. This 2-level model enables the creation of multiple organizations and rules access to organizations:

- MSP level access and manage all organizations
- Organization or tenant level access specifically to organizations. with a well-defined role.

19.	MSP level shall display organisations, tenants accounts, their roles and manage different tenants accounts	C/PC/NC

All organizations are displayed at MSP level and a MSP level can:

- Add a user in organizations and assign a specific role
- Access an organization and completely manage this organization
- Audit/supervise all organizations
- View lists of devices
- View users activity across organizations

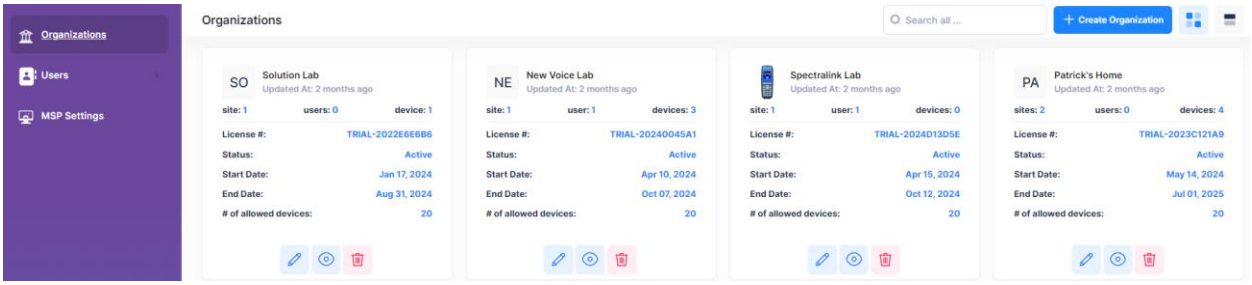


Figure 11: Displaying organizations as MSP - Organizations [MSP portal]

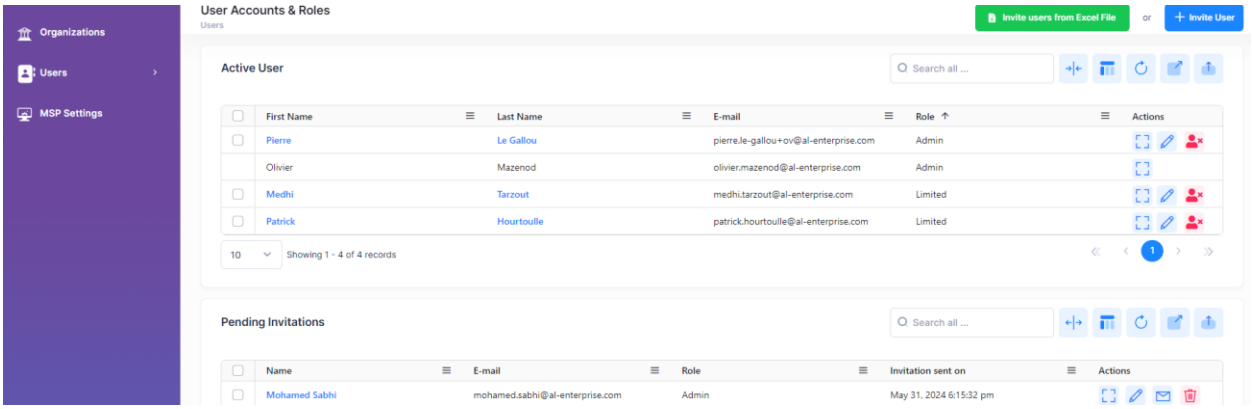


Figure 12: Displaying users accounts & roles as MSP - User Accounts & Roles [MSP Portal]

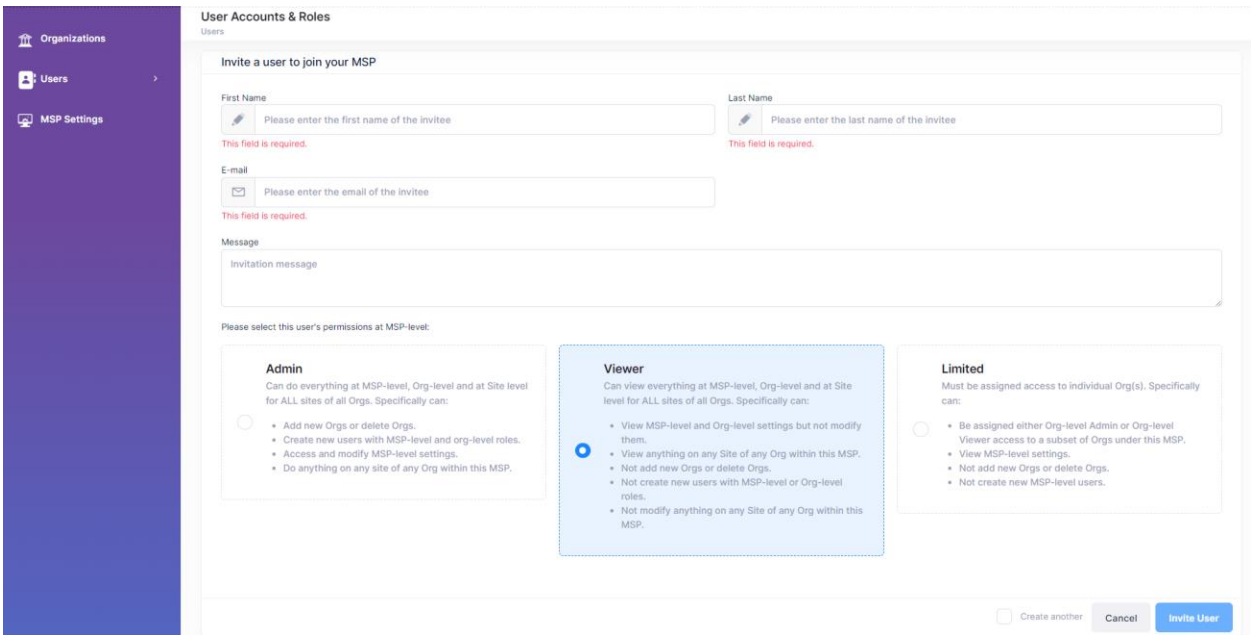


Figure 13: Invite a user as MSP - User Accounts & Roles [MSP Portal]

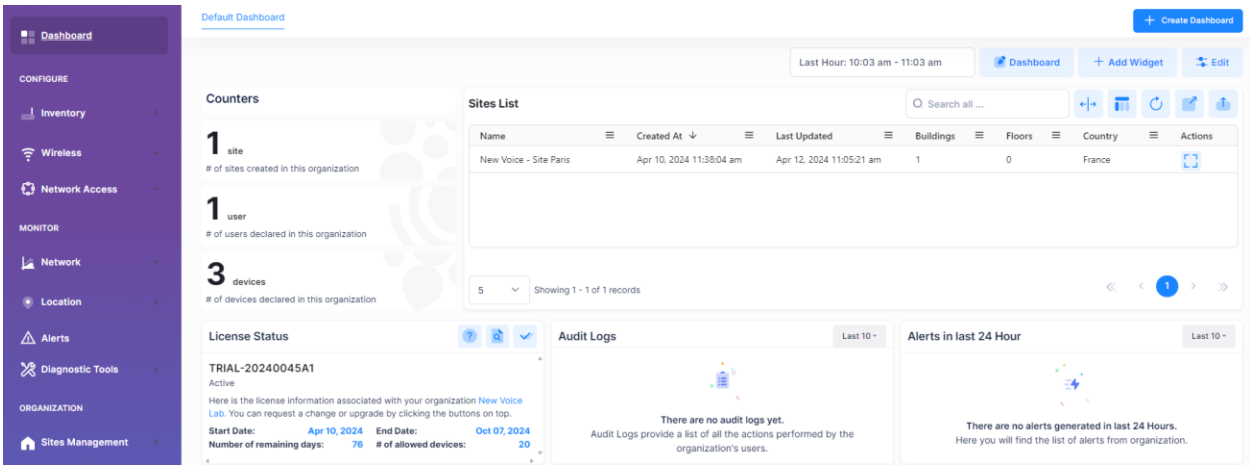


Figure 14: Access organization & organization overview as MSP - Organizations [MSP Portal]

20.	Tenant level shall display organisation and manages its organisations upon the role defined	C/PC/NC

All organizations under responsibility of a tenant are displayed and user can:

- View details of the organizations
- Access and manage organizations using various NMS Cloud tools according to the role (e.g sites, LAN/WLAN equipment, topology, configuration, monitoring etc.)
- Audit/supervise organizations under its responsibility

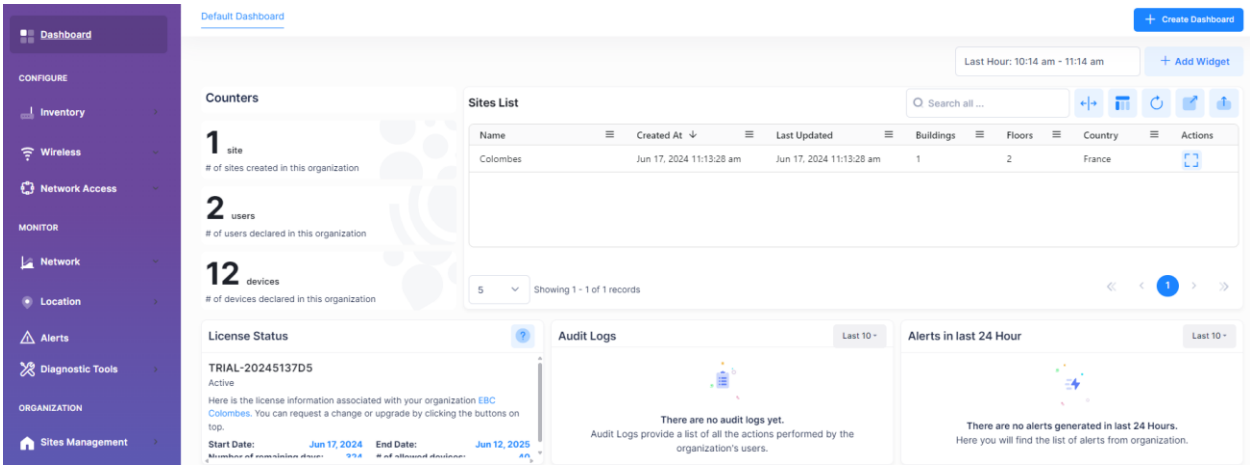


Figure 15: View organization dashboard as Tenant - [ORGA]

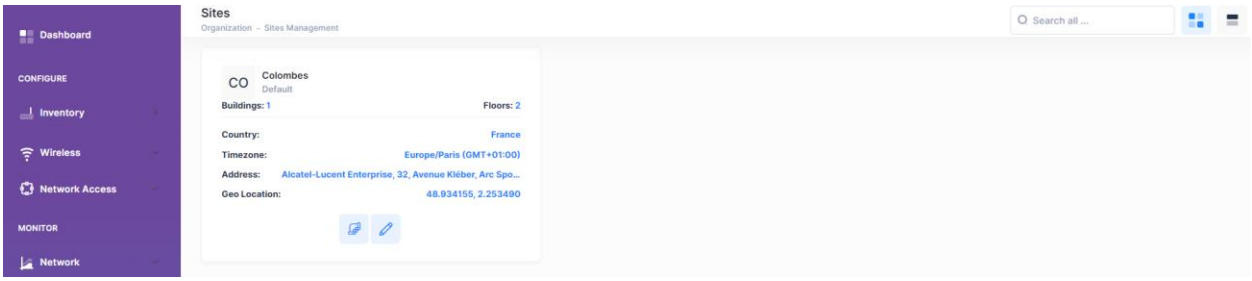


Figure 16: Access sites management as Tenant - Sites [ORGA]

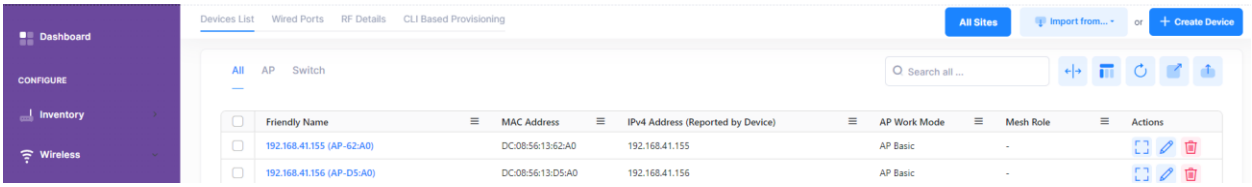


Figure 17: Create a device as Tenant - Device Catalog [CONF]

The tenant can manage an organization in order to specifically provision Stellar APs in Remote AP (RAP) mode. The provisioning of RAP access points involves defining the data VPN server for this organization and data VPN client pools.

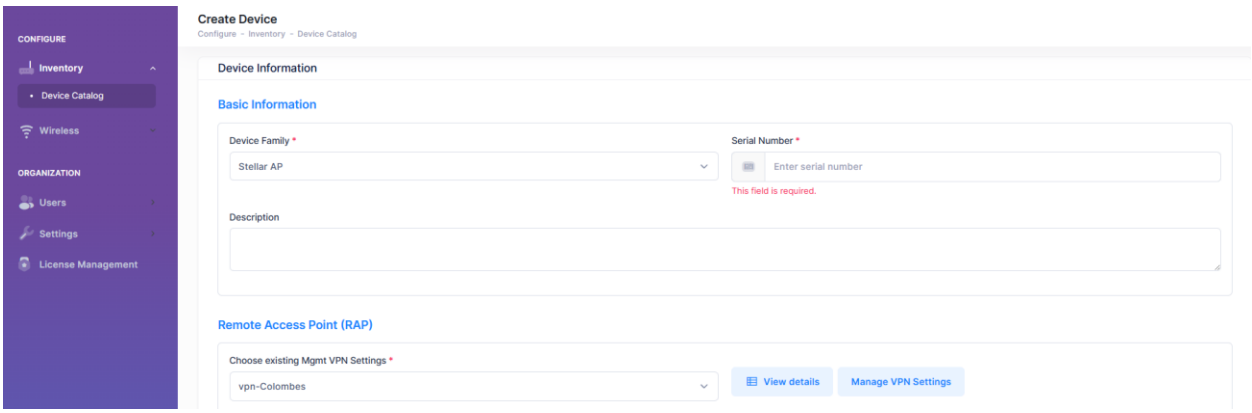


Figure 18: Create Stellar Remote AP device as Tenant - Device Catalog [CONF]

21.	The cloud-based NMS shall support Role-Based Access Control (RBAC) of administrators per tenant with external authentication	C/PC/NC

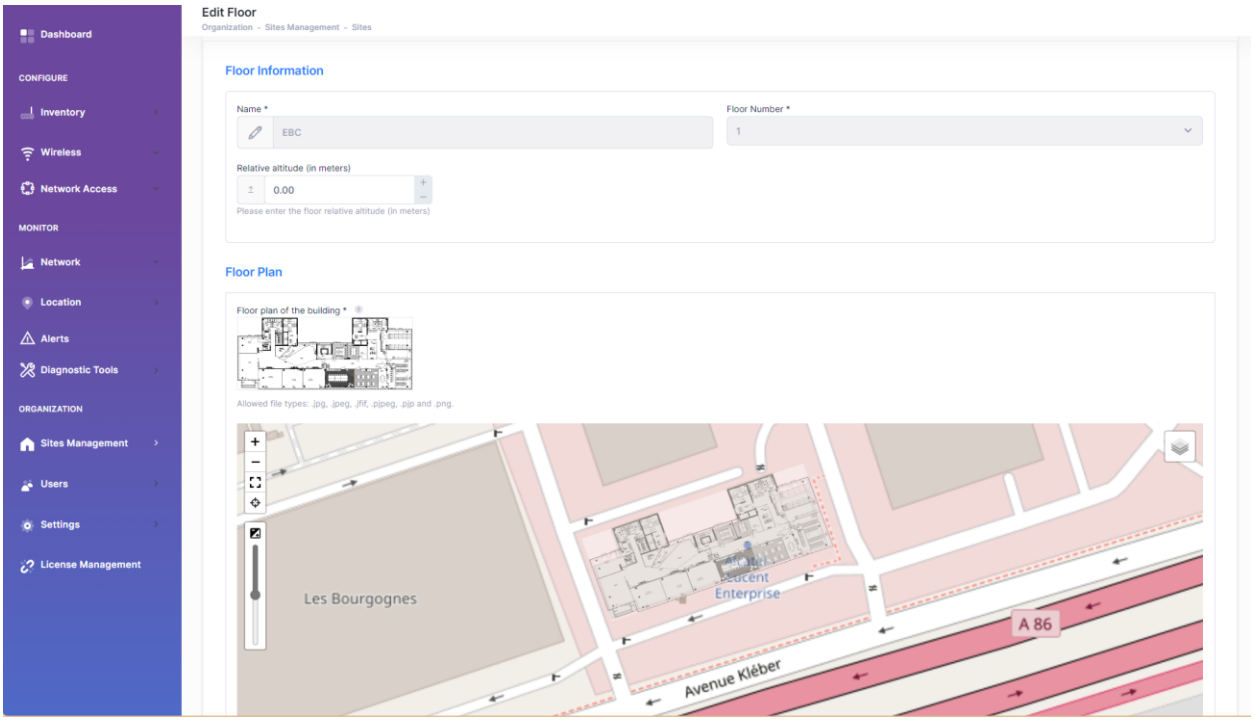
Cloud-based NMS supports Multi-Form Authentication (MFA) for the authentication of its users and with use of external resources for NMS user authentication.

22.	The cloud-based NMS shall support Multi-site and Multi-level configurations with support for geo-location services	C/PC/NC

NMS is a multi-site and multi-level based-map solution for the different organizations that are attached to MSP. Administrators can manage topologies for each site with support for multiple ground plans. Coverage areas are defined per floor or different floors and certain number of boundaries inside such as walls.

NMS supports geo-location and a time zone for each site, as well as elevation for each floor. NMS also supports Wi-Fi heatmap for each area with the possibility of filtering by type of equipment, by zone or by radio resource for the WLAN.

The NMS geo-location tools will be enriched in the future with a client density tool (beta) evaluating in real-time the number of clients connected in certain very specific areas.



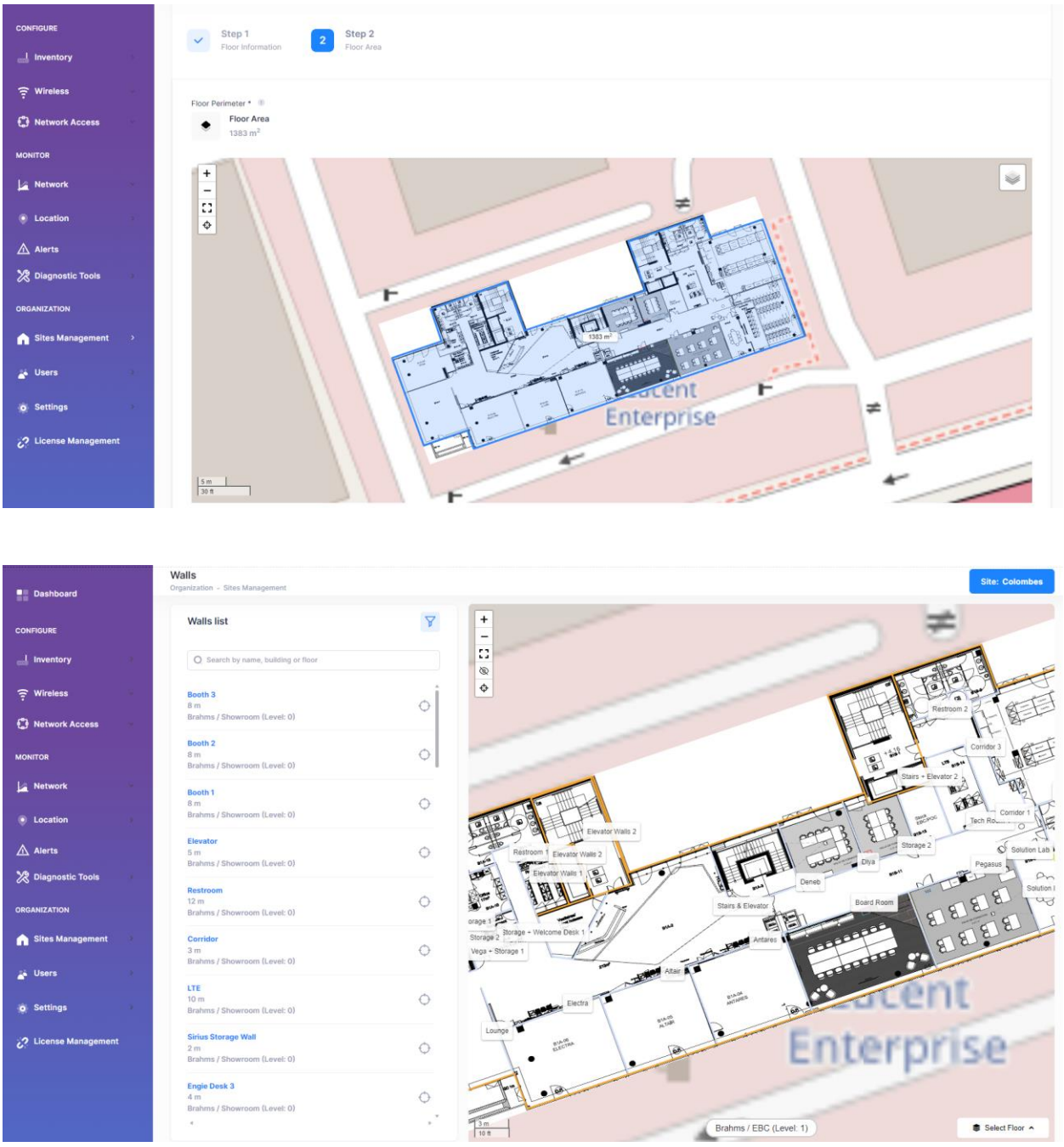


Figure 19: Configure buildings & floors - Sites [ORGA]

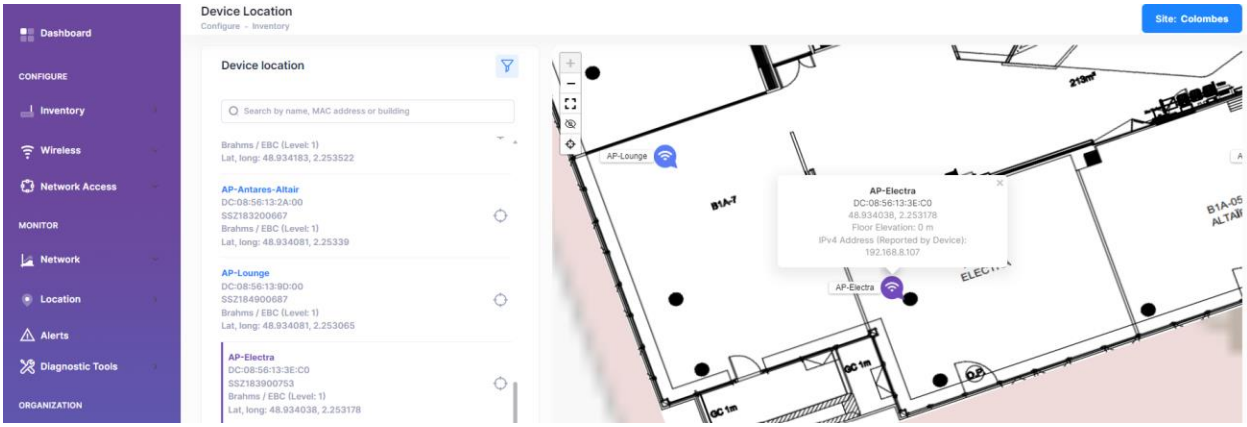


Figure 20: Manage device location - Device location [CONF]

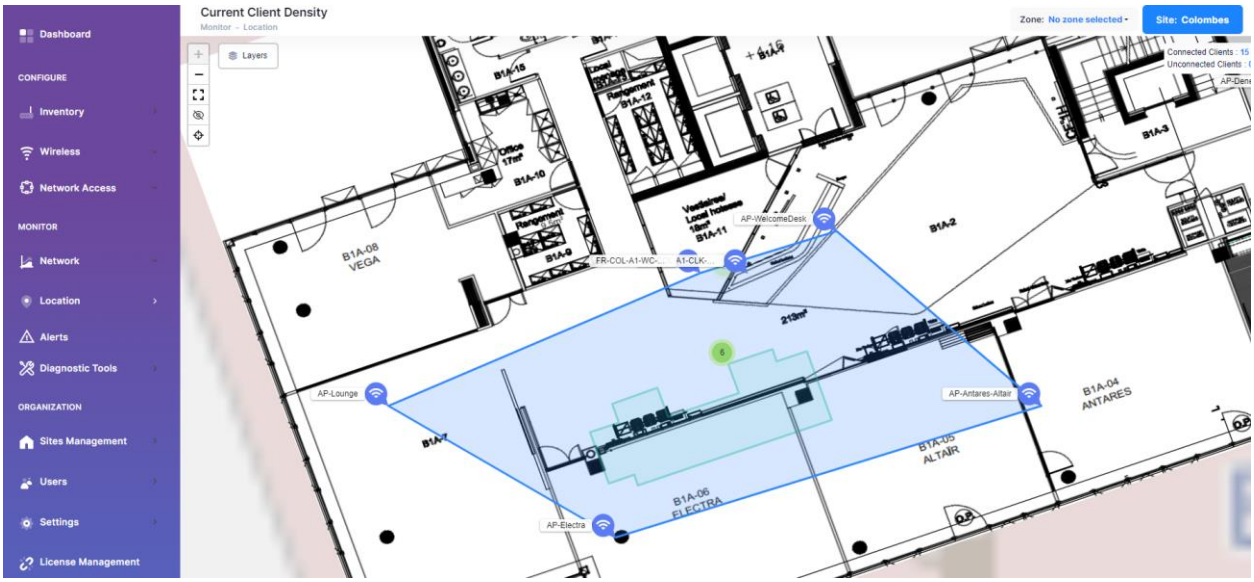


Figure 21: Current client density (beta) - Location [MON]

5. LAN management

24.	The cloud-based NMS shall provide GRE tunneling feature on LAN layer 2 that offers GRE terminations for any type of device or clients when traversing the LAN on switches for an organization or a given site	C/PC/NC

Cloud-based NMS supports the establishment of GRE tunnel links on the LAN layer 2, identifiable by tunnel IDs in the LAN, for any type of OmniSwitch or OmniAccess® Stellar

terminations (use case for Guest WLAN clients, for example). GRE tunnels are fully managed by the User Network Profile (ARP) (version 10.5).

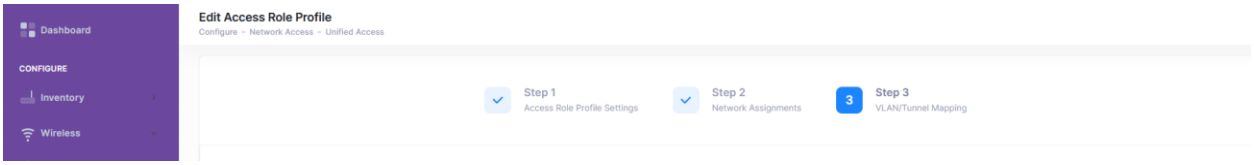


Figure 22: Map Device to a GRE tunnel – Access Rôle Profile [CONF]

25.	The cloud-based NMS shall provide a VLAN manager for easy management of VLANs on the switches for an organization or a given site	C/PC/NC

Cloud-based NMS allows the management of VLAN domains for complete LAN layer 2 management for a given device and site and this with easy provisioning of VLANs by OmniSwitch device. Creating a VLAN allows defining a type of VLAN (default or Q-tagged) on a type of resource (port, lag, spb, etc.) on each OmniSwith.

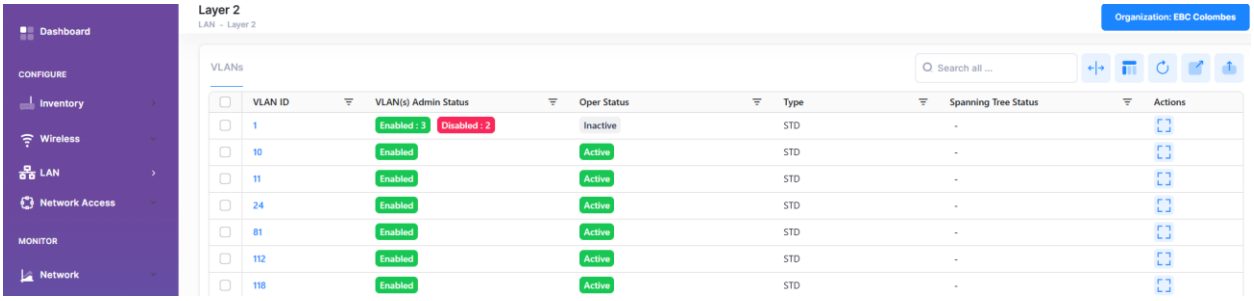


Figure 23: Create and Manage VLAN domains - Layer 2 [CONF]

The Cloud-based NMS provides the operational mode and the details of each VLAN managed on the site and the devices. The details can be provided:

- by devices (IPv4/IPv6 addresses, MAC addresses and STP status reported),
- by ports (tagged or untagged with ports reported)
- by link aggregates (tagged or untagged with link IDs reported)

Following figures show the configuration details for a VLAN domain 112.

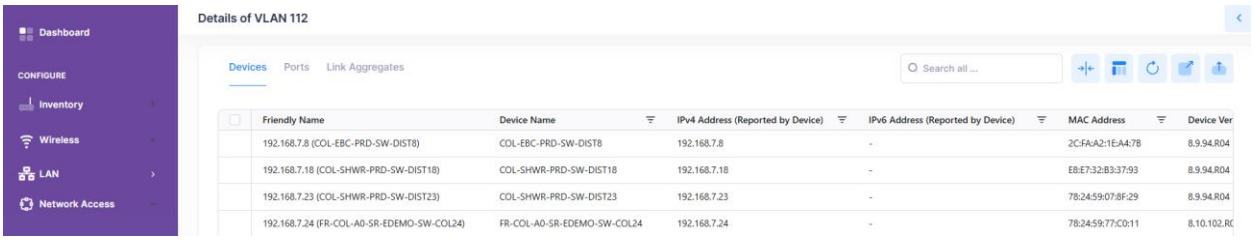


Figure 24: VLAN Details per device for data VLAN 112 – Layer 2 [CONF]

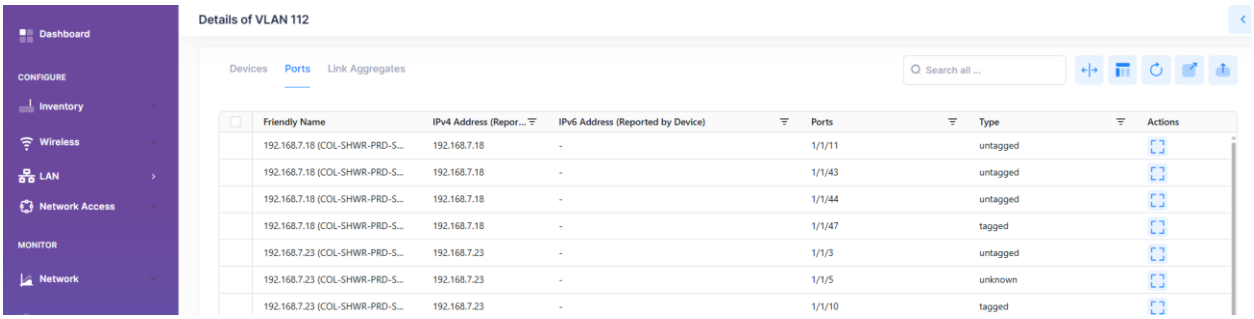


Figure 25: VLAN Details per port for data VLAN 112 – Layer 2 [CONF]

Figure 26: VLAN Details per lag for data VLAN 112 – Layer 2 [CONF]

26.	The cloud-based NMS shall provide a IP manager for easy management of IP Interfaces on the switches for an organization or a given site	C/PC/NC

Cloud-based NMS allows the management of different types of interfaces for each OmniSwitch for a complete management of the L3 LAN and their attachment to a type of domain/device.

The NMS allows defining an IPv4/IPv6 address and configuring the following range of interfaces on OmniSwitch®:

- VLAN interface – assign an IP address to a VLAN to enable Layer 3 services (e.g. routing) for devices within the VLAN
- Loopback interface – logical interface used as a stable endpoint in OmniSwitch®
- GRE tunnel interface – termination for GRE tunnel over an IP network
- VPN interface – traffic and service isolation within the OmniSwitch®
- IPIP interface – simpler tunneling method for IP-over-IP transport
- EMP interface – out-of-band management interface dedicated to a physical port on OmniSwitch®

Each interface on OmniSwitch® belongs to a VRF (Virtual Routing and Forwarding) instance to support separate routing tables and forwarding or proxy options as required. Interfaces are assigned to a specific OmniSwitch®.

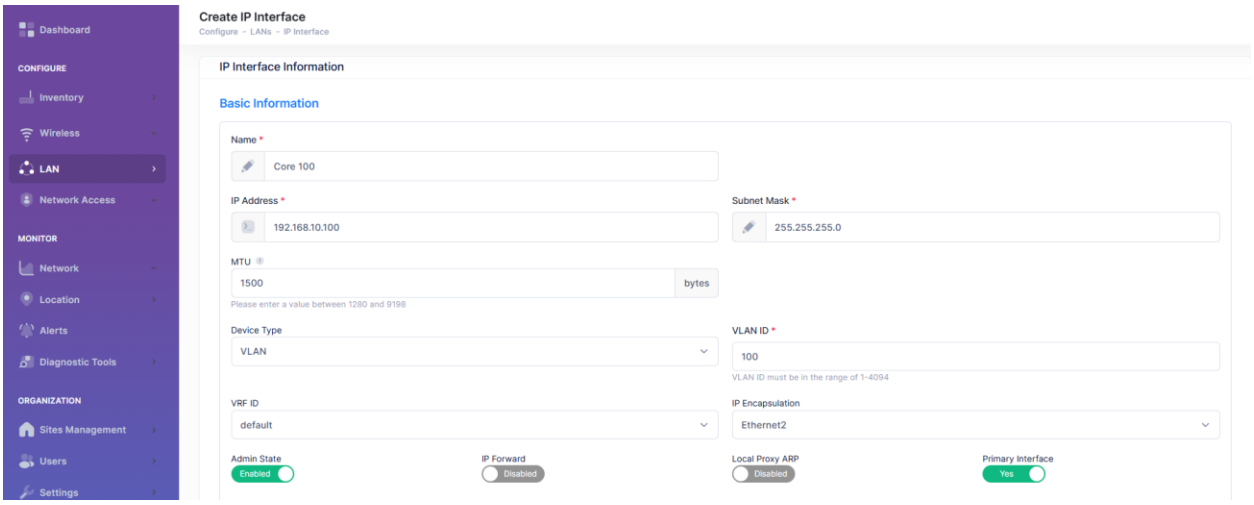
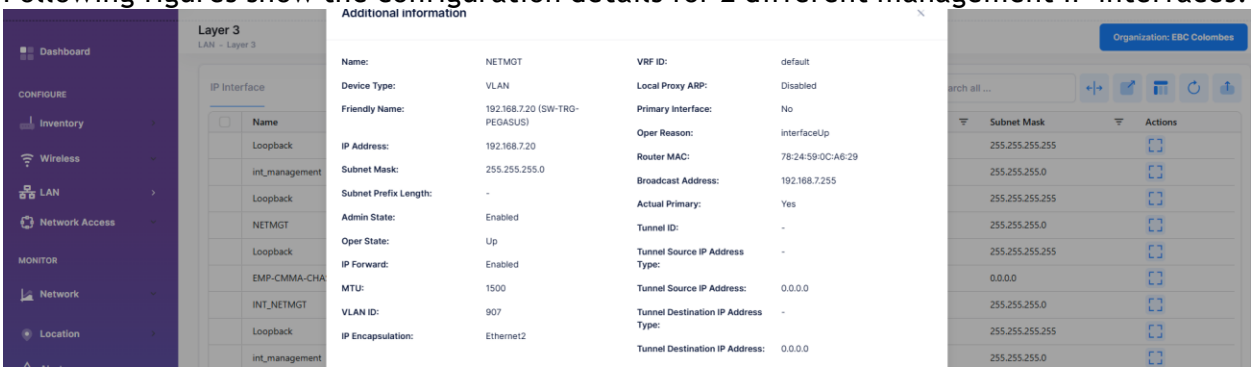


Figure 27: Create and Manage IP Interface - Layer 3 [CONF]

Cloud-based NMS provides the operating mode and details of each managed IP interface on the site and the devices. It includes for example the assignment to an OmniSwitch device, the IPv4/IPv6 address with mask, the VLAN ID, the router MAC address and the inter-VLAN transfer option.

Following figures show the configuration details for 2 different management IP interfaces.



28Figure 29: Details of IP Interface for a local management VLAN 907 - Layer 3 [CONF]

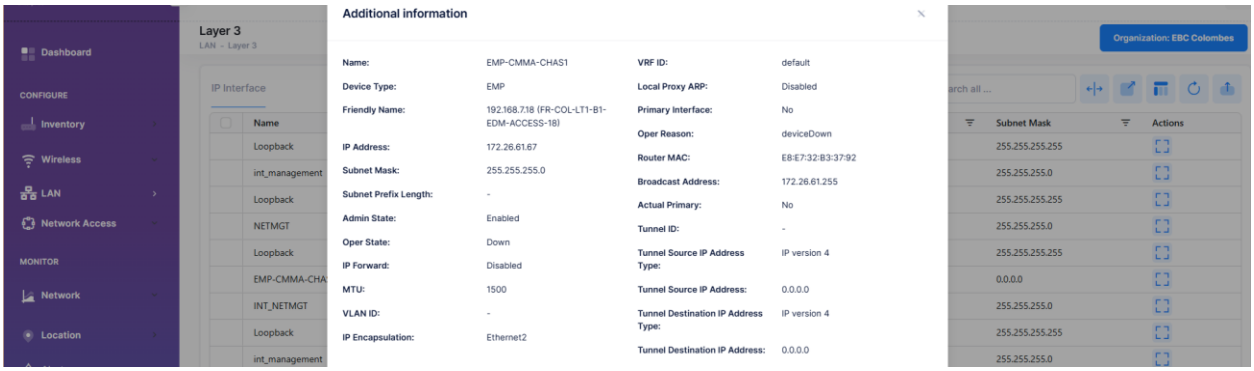


Figure 30: Details of IP Interface for an out-of-band EMP management - Layer 3 [CONF]

27.	The Cloud-based NMS must provide full support for the IPv6 protocol in managing the LAN infrastructure of a given site or organization.	C/PC/NC

OmniVista® Cirrus 10 delivers complete, transparent, and integrated IPv6 support, like for IPv4, for the local LAN. IPv6 support covers both Layer 2 and Layer 3 of the network, enabling user to seamlessly manage dual-stack IPv4/IPv6 and native IPv6 environments.

Support on LAN & WLAN

Cloud-based NMS provides native IPv6 address management through the IP Interfaces Manager across the entire OmniSwitch range. It supports automatic IPv6 address assignment via DHCPv6, as well as ICMPv6 support, required for the proper operation of key network protocols such as ND (Neighbor Discovery), RA (Router Advertisement), and RS (Router Solicitation).

IPv6 inter-switch communication is fully supported, enabling seamless multi-site deployments. IPv6 forwarding modes include Layer 3 unicast routing, Layer 2 bridging, and tunneling over IPv4 using IPv6 GRE L2 tunnels.

On the WLAN side, Stellar access points support IPv6 management addresses and transparent inter-AP communication over IPv6. Both Layer 2 and Layer 3 roaming are

supported for IPv6 or dual-stack wireless clients. Stellar RAP mode also support IPv6 VPN connections, including IPv6 addressing for the data VPN server and for data VPN client address pool.

Monitoring & client visibility
OmniVista® Cirrus offers comprehensive visibility into IPv6 traffic. IPv6 addresses of LAN / WLAN clients are displayed through different NMS interfaces (inventory, unified access, IoT) and available through APIs. The platform supports detailed client behavior tracking for IPv6 and provides bandwidth and Quality of Service (QoS) analytics for IPv6 traffic.
OS fingerprint of IPv4/IPv6 dual-stack client or IPv6 only client

For IPv6 traffic crossing Layer 2 domains or accessing the Internet, a dual-stack (IPv4/IPv6) gateway is always required to ensure proper translation or routing to external services.

Network Access Control (NAC)
OmniVista® Cirrus 10 also provides full IPv6 support across all NAC-related features, including UPAM-NAC, Captive Portal features, unified policies and DPI capabilities, as detailed further in the Network Access Control section.

28.	The cloud-based NMS shall support flexible and automated LAN management and updating using switch configurations after their onboarding	C/PC/NC

OmniVista® Cirrus 10 (version 10.5) supports incremental CLI-based Provisioning templates, which complement the initial templates used during Zero-Touch Provisioning (item 15).

This enhancement gives user the ability to update LAN configurations at any time in a controlled and efficient manner.
As with initial provisioning, Provisioning updates are pushed to the switches via CLI/FTP user-defined templates. Incremental templates can be applied to one or several OmniSwitch devices already managed by the NMS. Before any configuration change is deployed, user can audit the site *Golden configurations* to validate and secure the LAN update process.

Figure 31: Create and Manage Incremental Provisioning Template - CLI-based Provisioning [CONF]

6. Programmability

29.	The cloud-based NMS shall provide a secure RESTful programming interface	C/PC/NC

The NMS API allows programming third-party applications with support for many types of programming languages. NMS API is an open platform based on REST applications specially developed for business applications, development projects or testing.
OmniVista® Cirrus 10 NMS web application uses the same API platform for its own functionalities.

30.	The cloud-based NMS shall support 3th-party integration via its programming interface	C/PC/NC

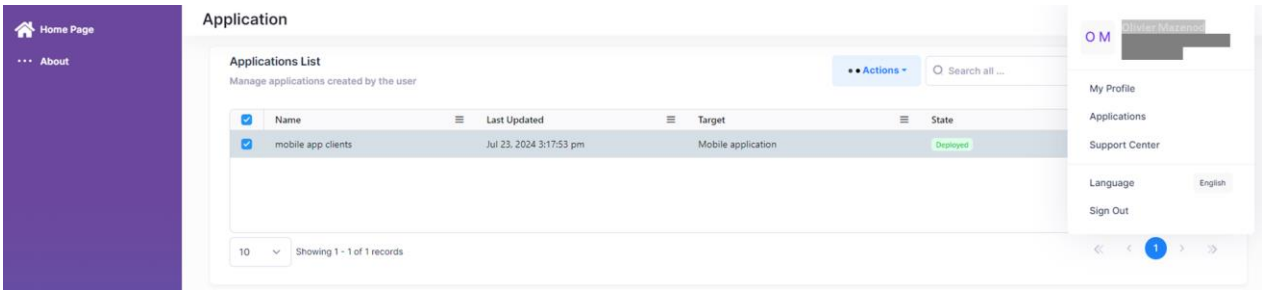
OmniVista® Cirrus 10 NMS Web application meets the most NMS demands for a Cloud managed Enterprise network but partners can always develop their own applications and NMS API the open solution that can interface with specific requests and integrate to third-party systems.

Integration with 3th-party systems is a growing demand and is subject of a constant update of the NMS API version on OmniVista® Cirrus 10 site.

31.	The NMS API shall be protected by authentication and method to access API described	C/PC/NC

NMS API answers fully to this demand, an administrator activates his NMS application option from his account and email, administrator password, key and secret code provided are required to authenticate to NMS API.

Once the token is retrieved for his application, all subsequent API end point is protected by token and its data protected.



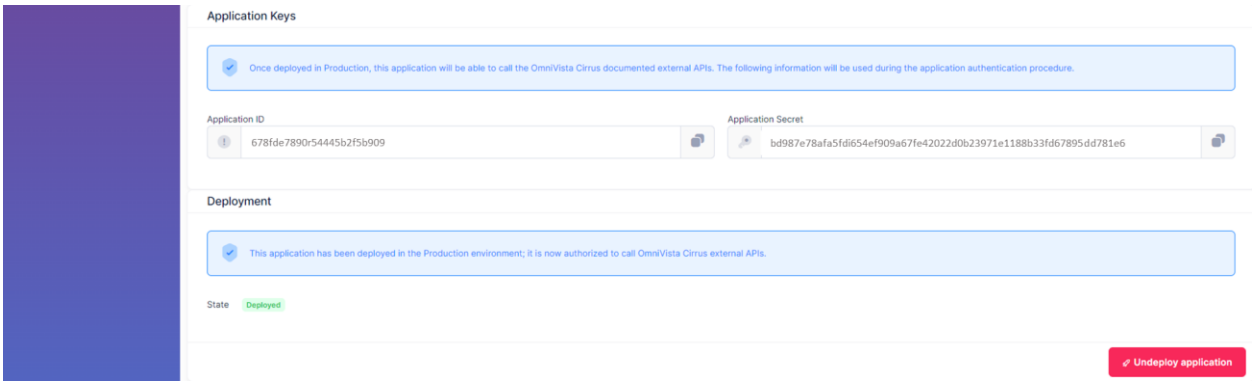


Figure 32: User API application option - Home page [USER]

32.	The cloud-based NMS shall contain OpenAPI documentation with use cases	C/PC/NC

The complete 10.5 reference API documentation is accessible from OmniVista® Cirrus 10 site for developer community (and also from ALE Networks Development Center on Spacewalkers):

- Reference guide for the entire API including the latest updates per release and use cases integration: OmniVista Cirrus API Reference (ovcirrus.com)
- OpenAPI specifications downloadable on same page
- Technical forum with Q&A for experts and user tips

The NMS API services are regularly updated by version and integrations done with this version are noted.

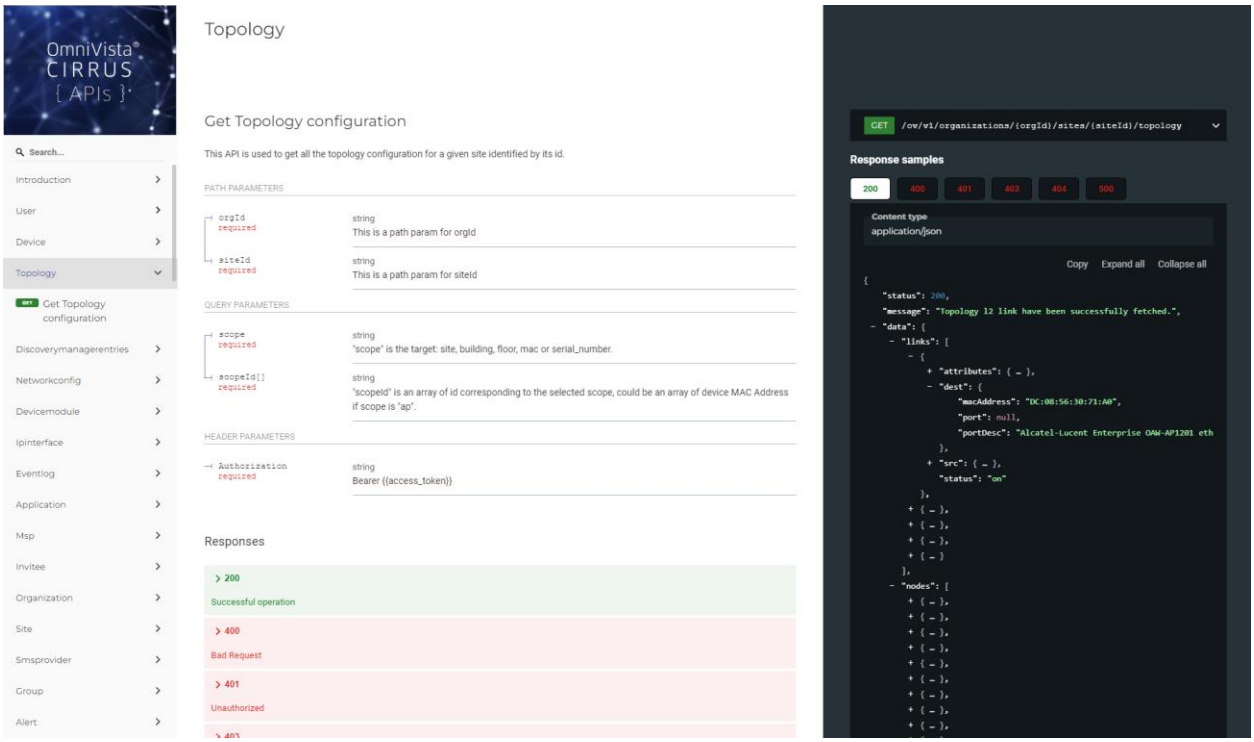


Figure 33: Developer API reference 10.5.1 - ovcirrus.com/apidoc

7. Security and data privacy

33.	The cloud-based NMS shall encrypt management traffic of managed network devices to the cloud	C/PC/NC

NMS manages management traffic over the Internet with devices in a fully encrypted manner. Traffic is fully tunneled between the Cloud and each device via a secure VPN and each Stellar and OmniSwitch device acts as a Cloud agent for NMS, with asynchronous management messages sent via UDP/MQTT.

As discussed in architecture overview, the NMS Cloud uses a new communication model for the LAN, as well as for the configuration and monitoring of switches. Cloud activation for each Stellar and OmniSwitch device is also securely performed to the NMS Cloud activation server, with the tunnel establishment initiated by Stellar access point or the AOS8 switch cloud agent.

34.	The cloud-based NMS shall support certificate-based authentication and encryption	C/PC/NC

Cloud-based NMS provides certificate management tool for its operation with devices and users authentication.

35.	The cloud-based NMS shall support RADsec client for user and device authentication	C/PC/NC

For an effective security in today's Cloud solutions RADsec support is crucial for managing any Enterprise authentication in a Cloud-based server ecosystem. NMS Cloud supports RADsec and ensures a secure and reliable communication between Enterprise devices and Cloud servers. RADsec support is more detailed in Network Access Control chapter and UPAM-NAC.

36.	The cloud-based NMS shall support two-factor authentication for administrator access	C/PC/NC

NMS cloud supports two-factor authentication (MFA) for administrator, further enhancing security to access the NMS. The two-factor authentication is enabled at the creation of users account.

37.	The cloud-based NMS shall support enforcing a strong password policy	C/PC/NC

A robust password policy is essential for security in Enterprise. NMS Cloud, as a Cloud solution for enterprises, enforces a strong password policy ofr administrators and users.

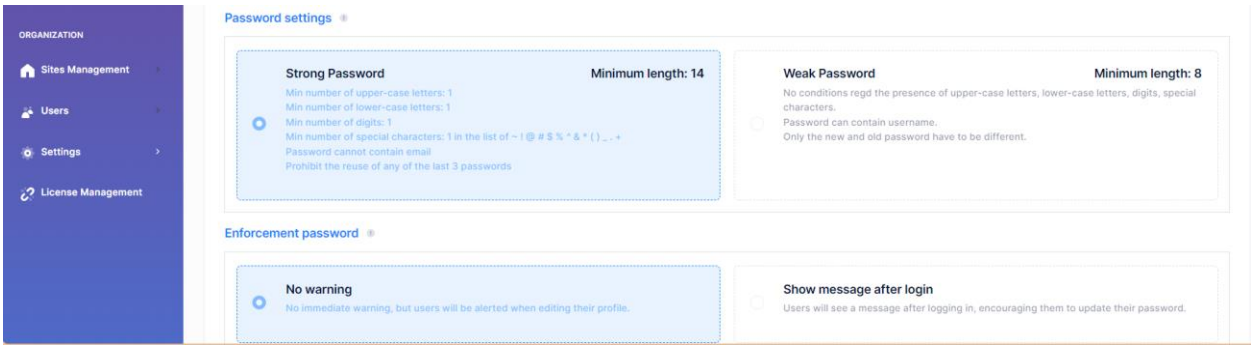


Figure 34: Password settings and enforcement - Basic Settings [ORGA]

8. Maintenance and operation

38.	The cloud-based NMS should allow automated and scheduled firmware updates for managed devices with latest releases reducing IT involvement and maintenance windows	C/PC/NC

Cloud-based NMS supports automated and scheduled maintenance for managed devices and based on profiles, allowing the scheduling of firmware updates, configuration backups, and generation of some maintenance history (such as backup history). This leverages the capabilities of Cloud management for facilitated IT maintenance operations.

NMS (version 10.4) introduces automated updates of Stellar access points in the inventories of each site, according to well-defined schedules and during off-peak hours. NMS Cloud naturally provides the latest Stellar firmware versions for the maintenance tool. The maintenance tool continues to evolve, notably with the support of OmniSwitch.

NMS (version 10.5) supports option to upload private builts or patches for devices when it is required.

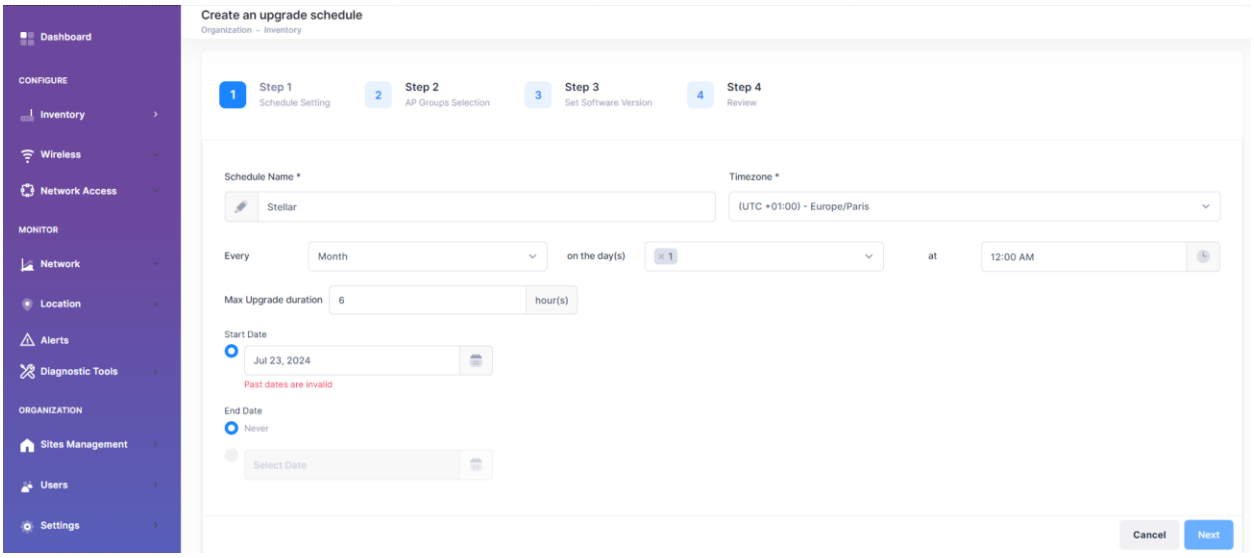


Figure 35: Create an upgrade schedule for WLAN - Scheduled Upgrades [CONF]

39.	The cloud-based NMS shall support a unified LAN and WLAN topology providing complete visibility of each installation on the sites, and actions on an equipment if required	C/PC/NC

NMS Cloud supports an advanced LAN and WLAN topology tool, allowing an overview of the physical connectivity between each component and obtaining details for each component:

- View of the physical topology
- View of the status of each link
- Actions on a selected device: Several actions are possible; obtaining details and information about the equipment or performing specific maintenance actions such as console access, cloud agent diagnostics, running/certified configuration management, trap management, etc.

All specific actions for an access point, for example, in OmniVista® 2500 NMS, are now integrated into the NMS cloud topology tool: Immediate AP updates, console access, reboot, WebUI access, Bridge/mesh management, LED mode change, etc.

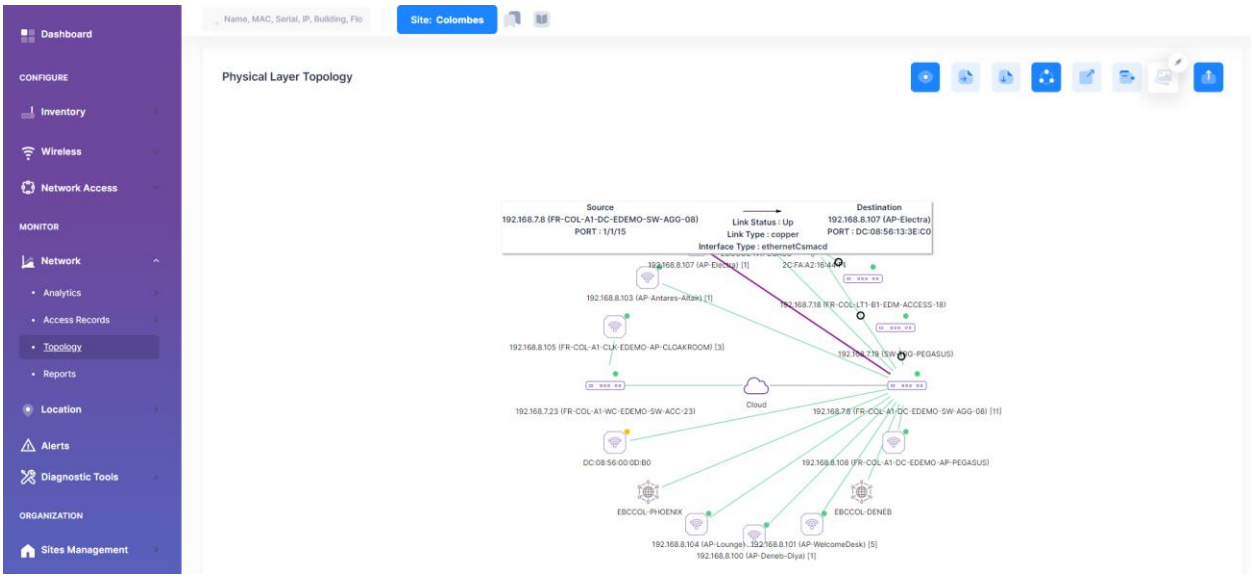


Figure 36: Physical layer topology overview - Topology [MON]

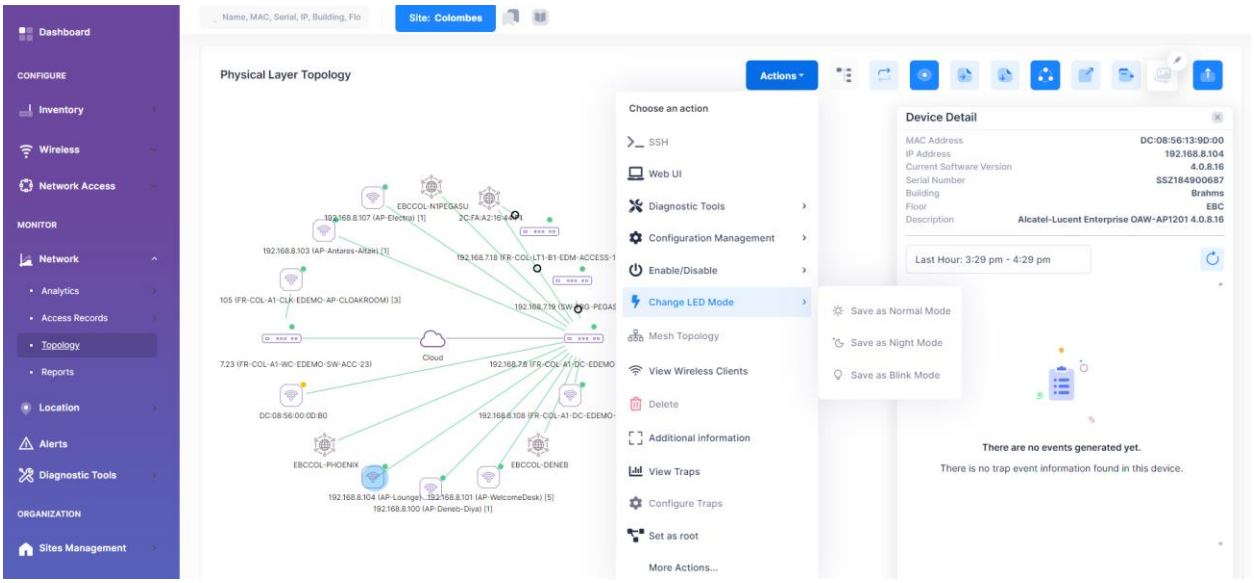


Figure 37: Display details and actions on AP - Topology [MON]

A specific audit action for a switch, for example, with the possibility to audit the running configuration on the OmniSwitch. The user has the possibility to download the configuration and mark OmniSwitch configuration as *"Golden Configuration"* for his site. NMS allows the user to automatically detect any configuration drift from the *"Golden Configuration"* and to restore validated reference configuration if needed (version 10.5).

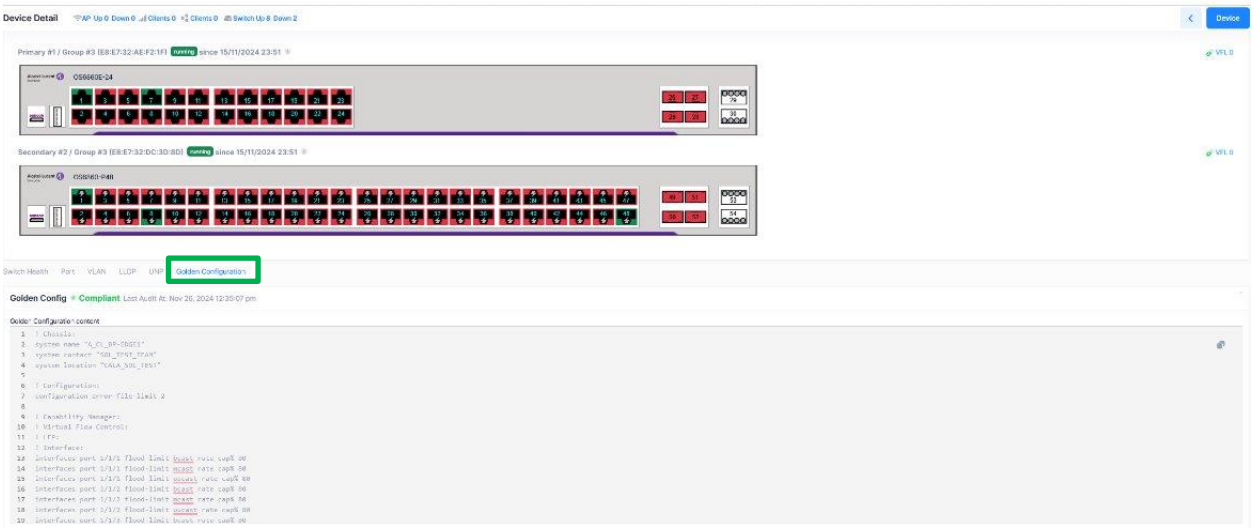
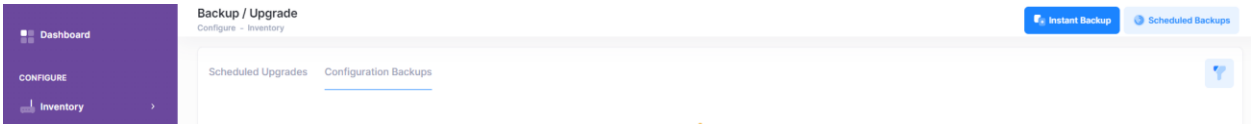


Figure 38: Audit running configuration on Switch - Topology [MON]

40.	The cloud-based NMS should allow automated and instant configuration backups for managed devices, including all common and security configurations of the device	C/PC/NC

NMS Cloud supports instant and automated backup of OmniSwitch to fully manage a switch history for a given site/topology. This leverages the capabilities of Cloud management for facilitated IT maintenance operations.

NMS introduces backup of current switch configurations (version 10.4) from */flash/working*, */flash/certified*, */flash/switch*, */flash/network* and */flash/switch/captive_portal*. Security files from */flash/system/*, ssh keys, etc. are also backed up.



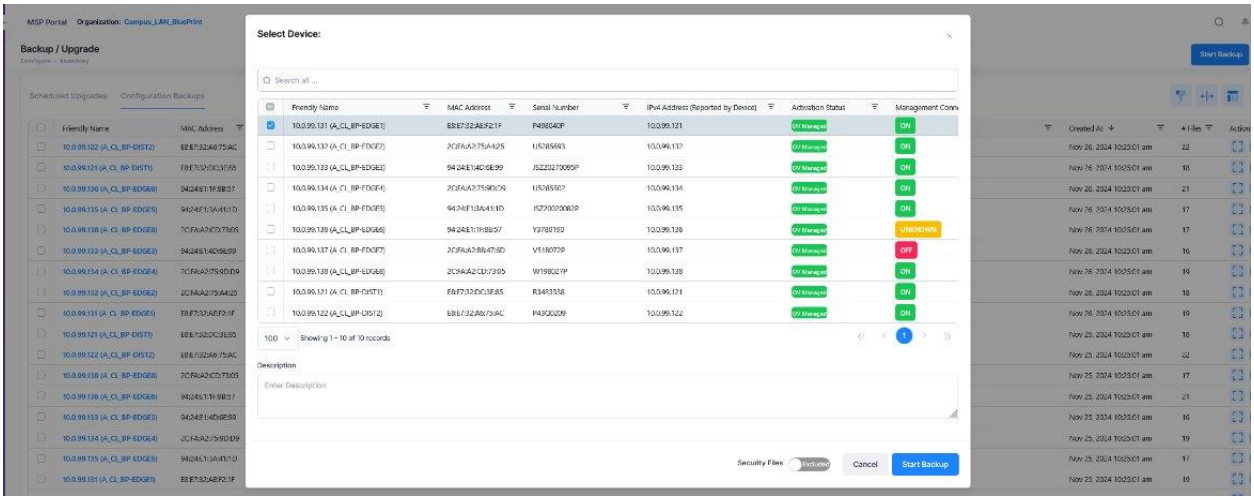


Figure 39: Start Instant Backup on Switch – Backup/Upgrade [CONF]

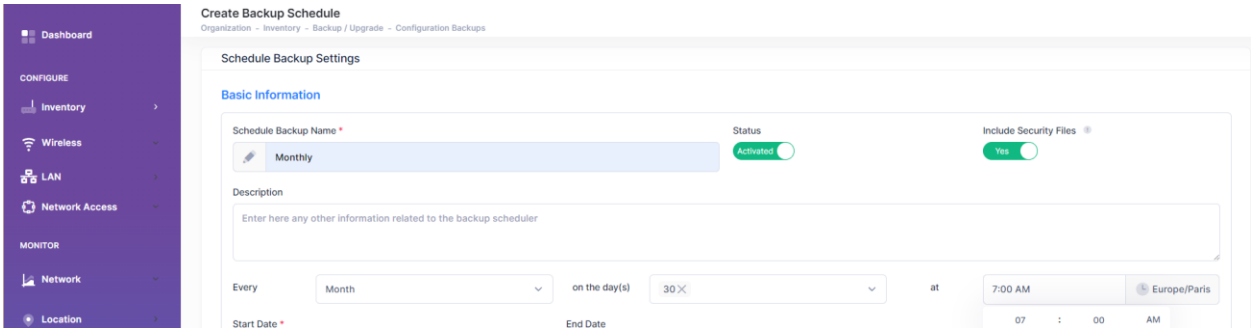


Figure 40: Create Backup Schedule on Switch – Backup/Upgrade [CONF]

9. Monitoring - Analytics and Reporting

41.	The cloud-based NMS shall support real-time monitoring of network performance and KPIs through customizable dashboard with visual widgets	C/PC/NC

NMS cloud fully enables real-time monitoring of LAN and WLAN networks and provides analytical KPIs through customized dashboards. Stellar access points and AOS8 Omniswitch support advanced analytics and report their data to NMS Cloud for advanced statistical and analytical services on the network:

- Quality of Experience (QoE) for LAN and WLAN, in form of tables and graphs displaying various metrics
- Network capacity and WLAN health, including WIPS policy monitoring
- Numerous statistics on clients
- Numerous statistics on applications (version 10.5)

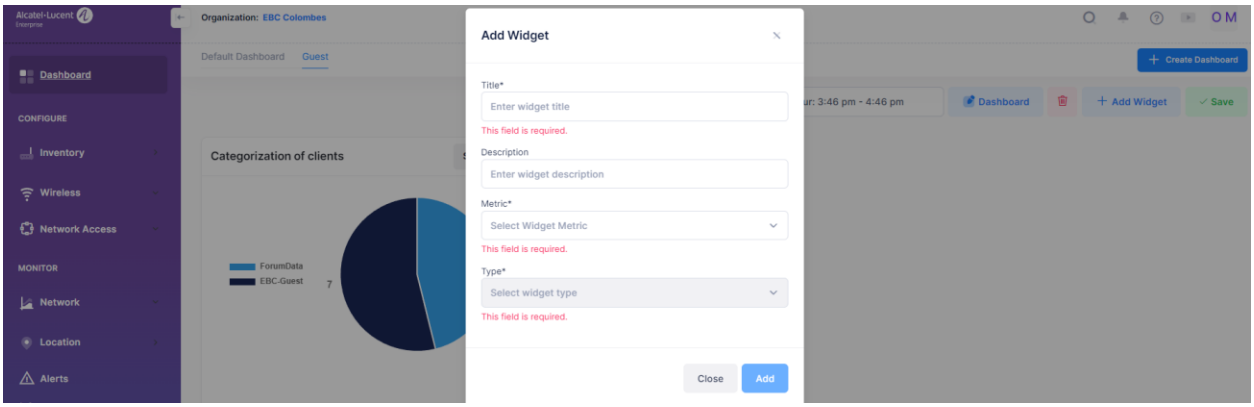
All available NMS analytics metrics can be grouped into visual widgets within fully customized dashboards, this allowing different aspects of the network to be monitored and for specific areas of the site. Different dashboards can be created, displayed directly from the organization and used with configurable analysis time windows.

OmniVista® Cirrus 10 already generates a range of interesting statistics particularly on the APs and RF for Stellar WLAN (under the "network analytics" menu), including AP hardware metrics, client distribution across channels or statistics on connection modes (connection time, connection success, roaming, and WLAN coverage). With customized dashboards, Stellar statistics can evolve into application statistics: user access to domains/URLs, user connections to SSIDs, user access through captive portals, connection times for visitors, or number of devices per user.

In the case of a Guest area covered by WLAN for a building with a Welcome center, all statistics can be grouped into a single dashboard entirely customized for Guest usage in this area. Tools and metrics grouped for the area include:

- Top clients for the Guest area
- Client categorization per SSID
- Number of successful connections
- Average coverage in the area
- Channel distribution
- Channel utilization
- List of APs in Guest area with CPU and memory usage
- Network events historic and alerts in the area

An example of possible dashboard customization is described below. All Guest clients metrics here come with a configurable analysis time window.



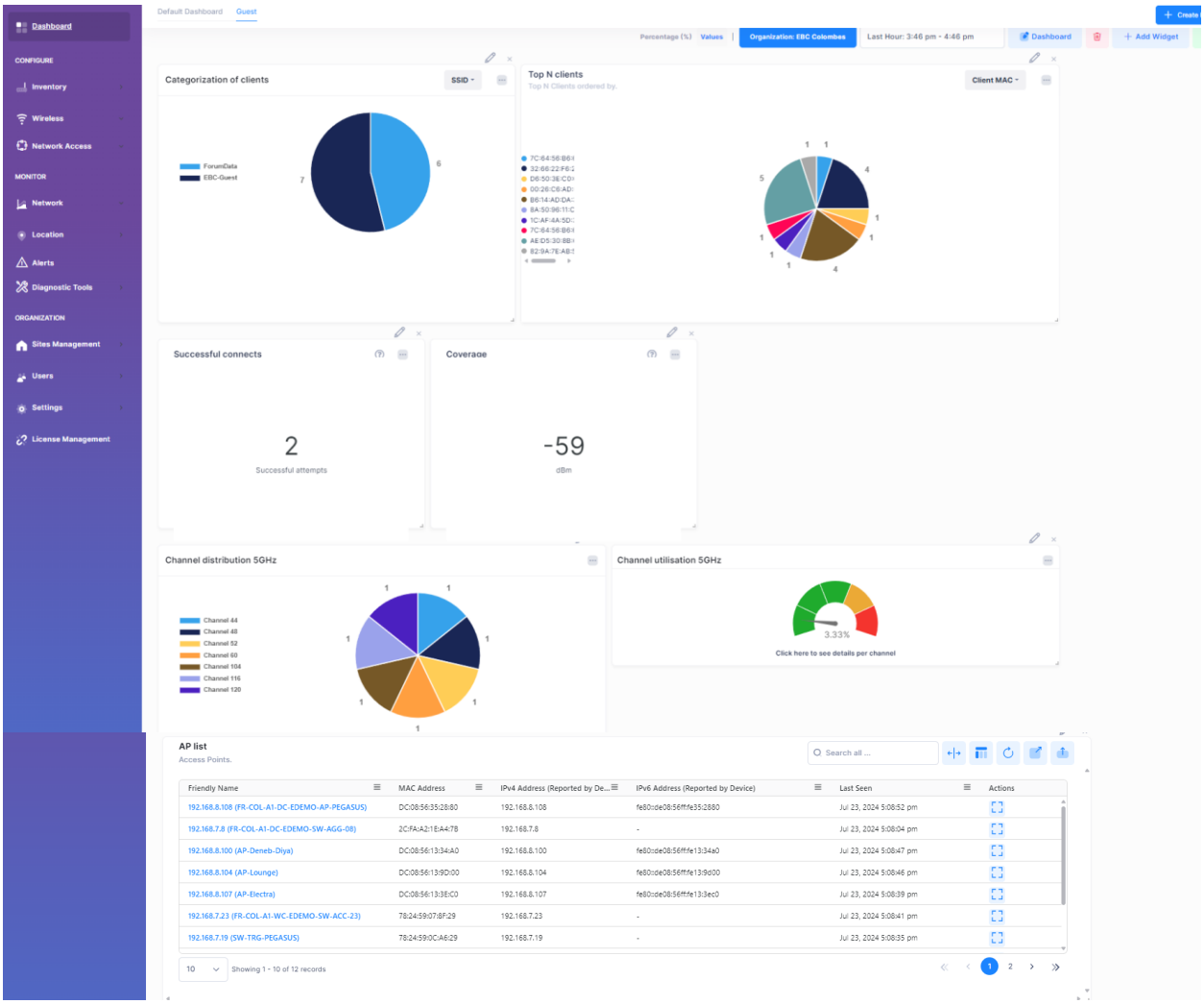


Figure 41: Dashboard customization - Dashboard [ORGA]

42.	The cloud-based NMS solution main dashboard shall support generating user QoE metrics and Network KPIs for WLAN clients	C/PC/NC

The NMS Cloud solution supports Quality of Experience (QoE) and provides comprehensive network monitoring tools for tenants at WLAN clients point of view, all accessible from a single menu: network > monitoring > QoE. These tools are available by default on the main dashboard. The QoE analysis tool for Stellar WLAN displays numerous metrics, including:

- Successful connections: Showing WLAN network reliability.
- Time to connect: Measuring connection speed.
- Roaming: Tracking device performance across access points.
- Coverage: Detailing network reach and signal strength.
- Capacity of WLAN: Monitoring avaibility of APs.
- Uptime of AP: Tracking access point operation

All WLAN clients metrics come with a configurable analysis time window.

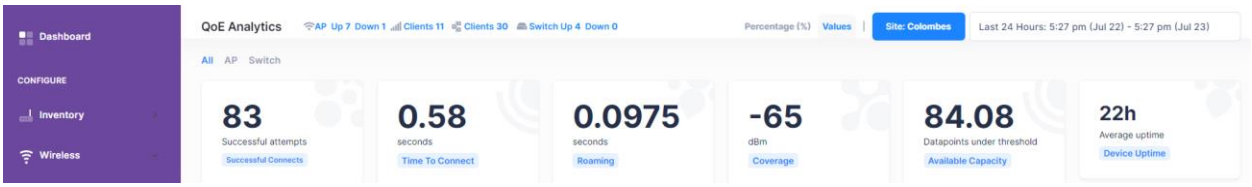


Figure 42: QoE attributes summary section (QoE [MON])

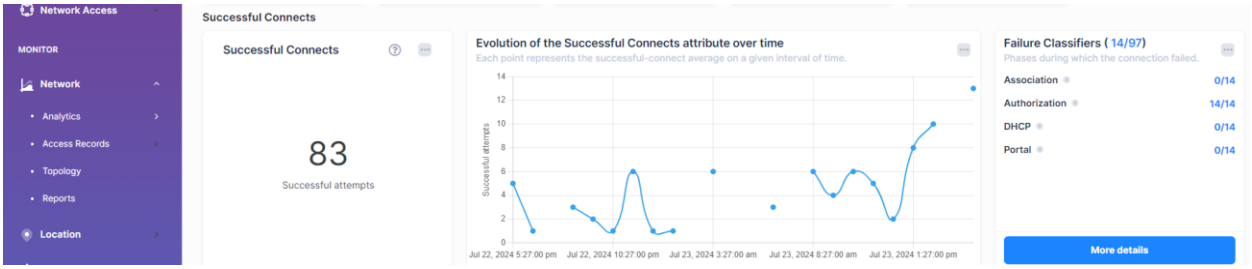


Figure 43: Successful connection section - QoE [MON]

43.	The cloud-based NMS solution main dashboard should provide quick QoE analytics to find root causes of connectivity issues for WLAN clients	C/PC/NC

NMS supports in addition a QoE problem analysis tool, where each failure reported in a metric is classified for advanced analysis and troubleshooting:

- Failures linked to an association, an authorization, a DHCP failure, or portal issues
- Excessive time related to associations, authorization, DHCP or portal processes
- WLAN roaming failures counted
- WLAN coverage problems related to weak signal, asymmetry of coverage, or other issues
- WLAN capacity problem that are evaluated on several criteria

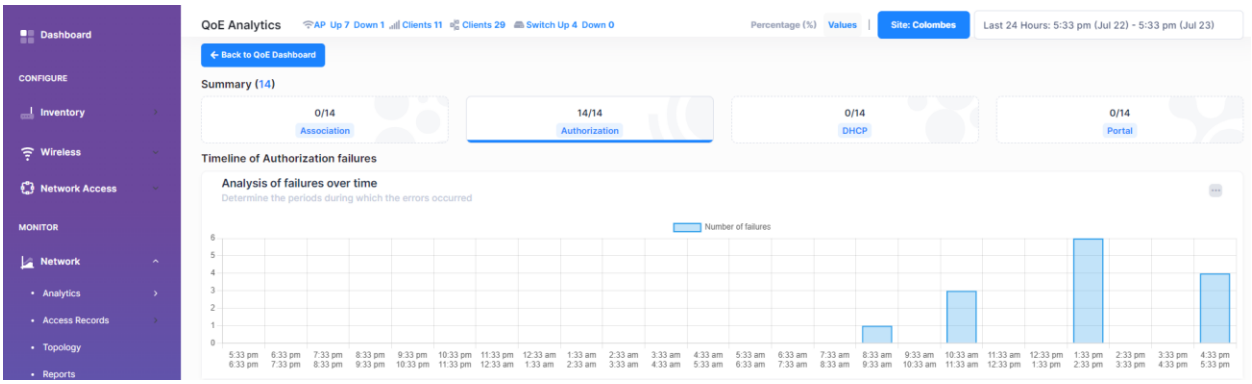


Figure 44: QoE Failure classifiers on connection issues - QoE [MON]

QoE problem analysis tool provides simultaneously an analysis of problems over time and a table that lists impacted customers by issues, with possibility to display network alerts and network events associated. The WLAN issues analyse is done with statistics on access points, health and capacity etc.

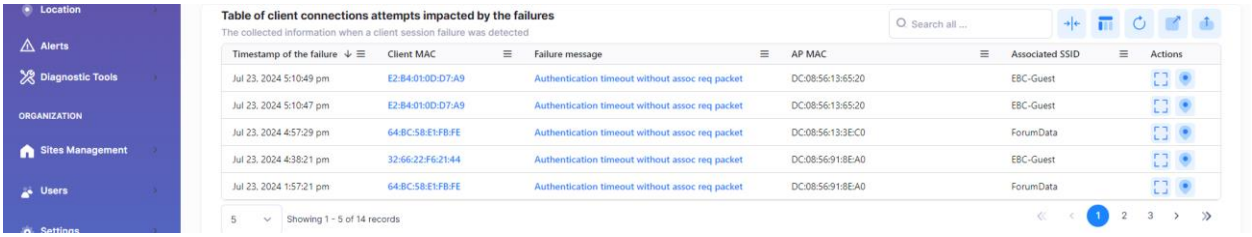


Figure 45: QoE list of impacted clients by connection issues - QoE [MON]

NMS cloud is a single architecture for in-depth LAN/WLAN connectivity issues analysis from the cloud.

44.	The cloud-based NMS shall support live and historical client analytics for at least 30 days	C/PC/NC

NMS supports a default client analytics history of 30 days, QoE data for 15 days, and a similar duration for network analytics, UPAM records, events, and alerts loggings. There is always the option to extend data storage and persistency for longer durations.

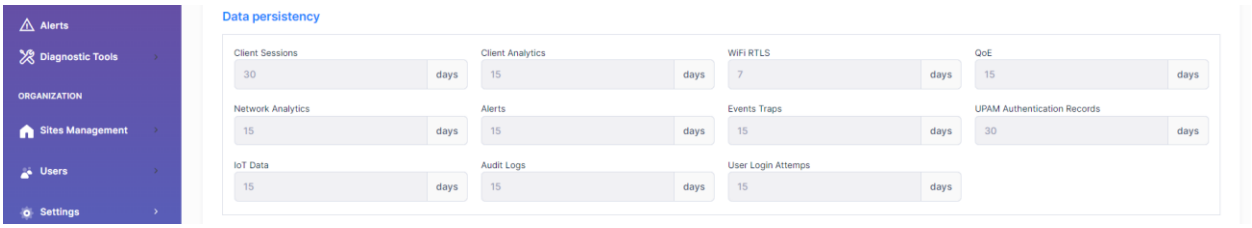


Figure 46: Data persistency for organization - Basic Settings [ORGA]

45.	The cloud-based NMS solution shall support generating client distribution reports per channel and per frequency band for WLAN	C/PC/NC

Cloud-based NMS fully complies with integrated support for WLAN reports with distribution of clients by channel or by frequency band. NMS supports predefined templates with integrated widgets like client distribution by channel or by frequency band.

NMS Cloud supports a client analytics tool for WLAN, displaying the distribution of clients across various WLAN resources for advanced analysis of user WLAN utilization. WLAN client analytics tool is accessible from the main dashboard and includes:

- Clients connected over time
- Distribution of clients across frequency bands
- Distribution of clients across SSIDs
- Distribution of clients across access points
- Client datarates consumption
- Client connection durations
- Devices per Guest user, etc.

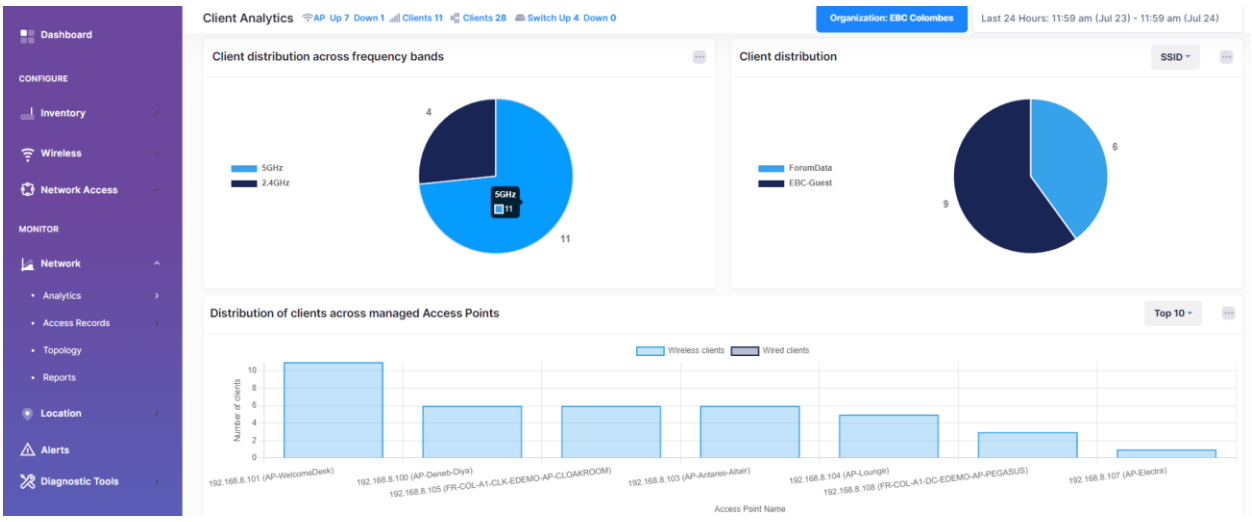


Figure 47: Distribution across frequency bands, SSIDs and managed APs - Client Analytics [MON]

Figure 48: Connected Clients over Time - Client Analytics [MON]

Additionally, certain widgets allow the display of client distributions based on various connection information. NMS Cloud provides a single architecture for in-depth client analysis of WLAN from the cloud.

46.	The cloud-based NMS solution shall support generating user application analytics to monitor usages on LAN/WLAN and manage reporting on clients usages for an organization or a given site	C/PC/NC

Cloud-based NMS fully complies with integrated support for analytics for user application traffic traversing the LAN/WLAN when managed by OmniVista® Cirrus 10 (WLAN clients in version 10.5). The latest OmniSwitch and OmniAccess® Stellar devices support an advanced real-time Packet Inspection (DPI) function that allows for in-depth analysis of application traffic on the LAN/WLAN, and NMS offers several widgets for full visibility of applications traversing the network. The application analytics tool is accessible from the main dashboard and includes following analytics:

- Categories
- Applications
- Top Users per Applications
- Top Applications per User
- Bandwidth Utilization per Application

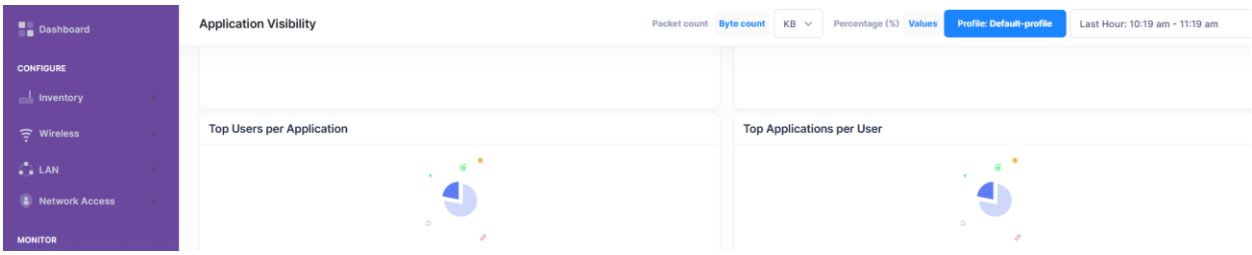


Figure 49: Top users per Application – Application Visibility [MON]

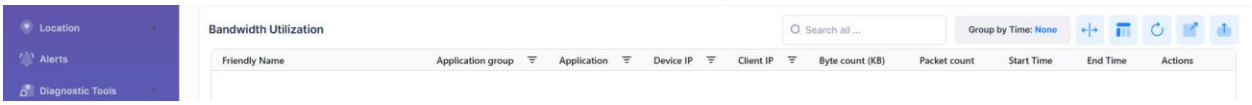


Figure 50: Bandwidth Utilization per Application – Application Visibility [MON]

47.	The cloud-based NMS shall support generating managed devices live and historical health reports and metrics	C/PC/NC

NMS fully supports different types of reports, which are emailed to administrators. The built-in template report is generated based on predefined templates and offer a wide selection of client health data from a list of widgets seen previously.

The scope of a report can be refined to a site, a building, or an organization, and it can be generated either instantly or on a scheduled basis.

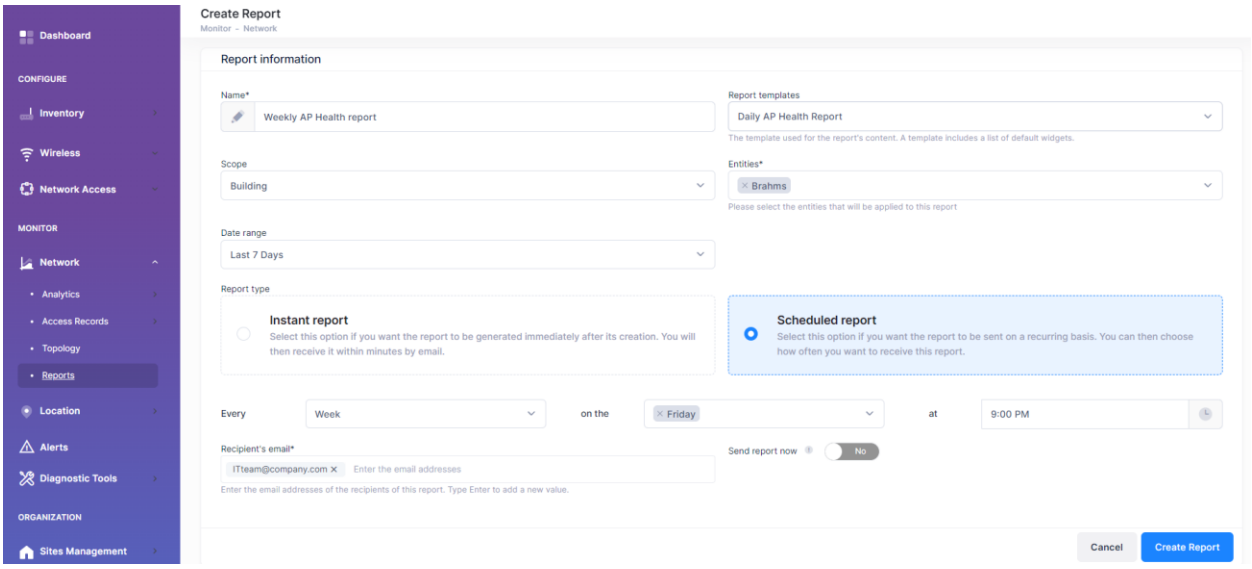


Figure 51: Scheduled AP Health report using built-in templates - Reports [MON]

48.	The cloud-based NMS shall support analytics data reports with report scheduling option	C/PC/NC

NMS cloud supports integrated analytics network reports based on numerous network analytics metrics, which are emailed to administrators. Analytics data reports are instant or scheduled reports, in csv excel or pdf formats over a period of time.

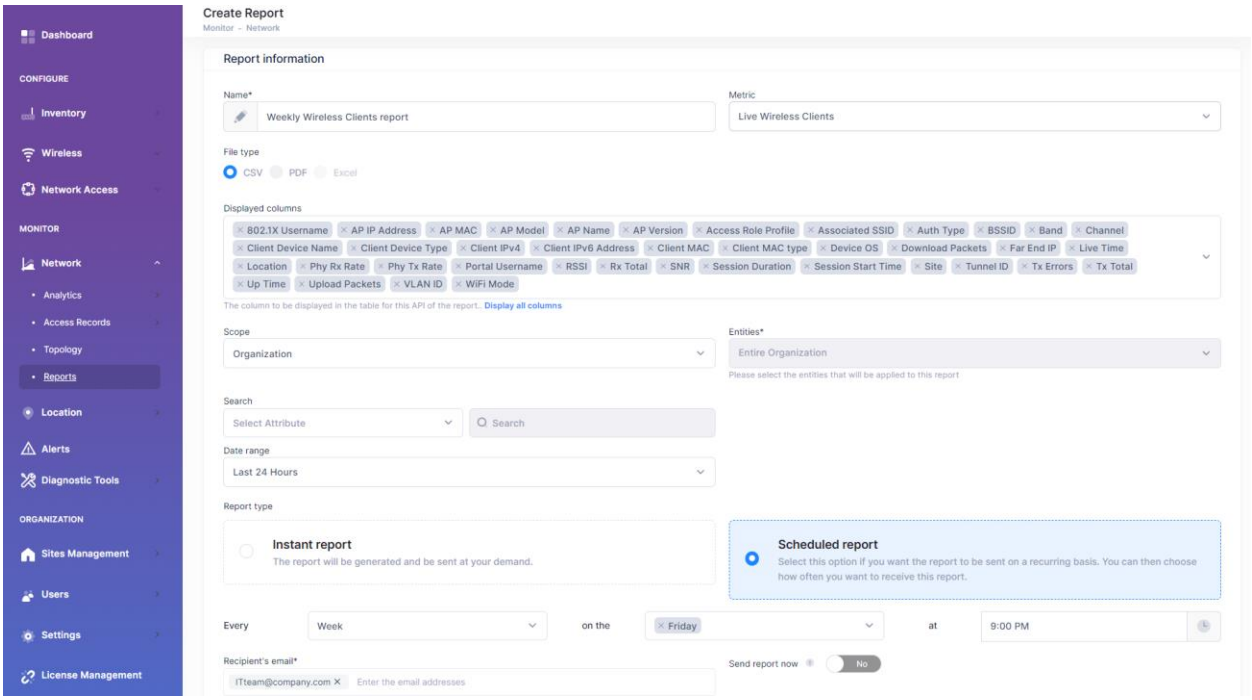


Figure 52: Scheduled Analytics Data report for wireless clients - Reports [MON]

49.	The cloud-based NMS shall support configurable term data persistency and durations	C/PC/NC

NMS supports a default client analytics history of 30 days, QoE data for 15 days, and a similar duration for network analytics, UPAM records, events, and alerts loggings. There is always the option to extend data storage and persistency for longer durations.

50.	The cloud-based NMS shall support configuring at least four remote syslog servers	C/PC/NC

NMS integratedly supports remote system logging to Internet or private servers up to 4 syslog servers. The level of log alerts can be managed according to the desired maintenance.
NMS supports the dump of LAN/WLAN devices state when encountering an error or crash, with machine dumps stored on a local TFTP server.

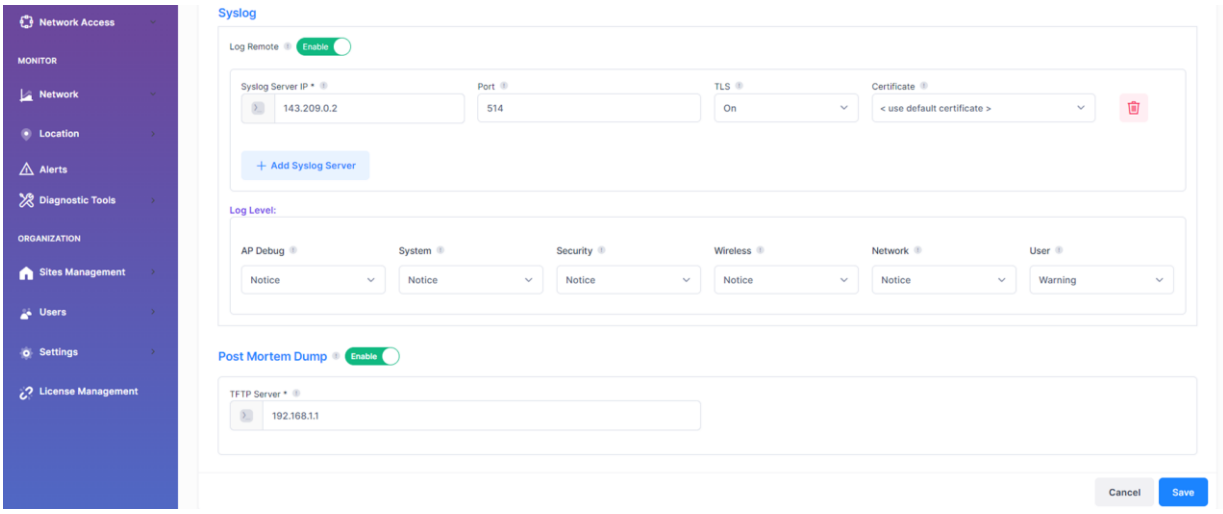


Figure 53: Manage syslog servers and PMD - Provisioning Configuration [CONF]

10. IoT Enablement

IoT features specific to Stellar WLAN (BLE location, Zigbee radio or RTLS location servers) are not described in this document.

51.	The cloud-based NMS shall provide IoT devices inventory management with identification features of contextual information	C/PC/NC

NMS provides a fully unified LAN/WLAN IoT inventory based on IoT categorization (IoT fingeprinting). Features include:

- Classification of IoT devices into predefined categories or customized by the customer with hierarchical enforcement
- Direct MAC identification with enforcement
- Exception lists to accurately define the IOT scope from rest of network (by MAC endpoints, devices, SSID, APs group etc.)

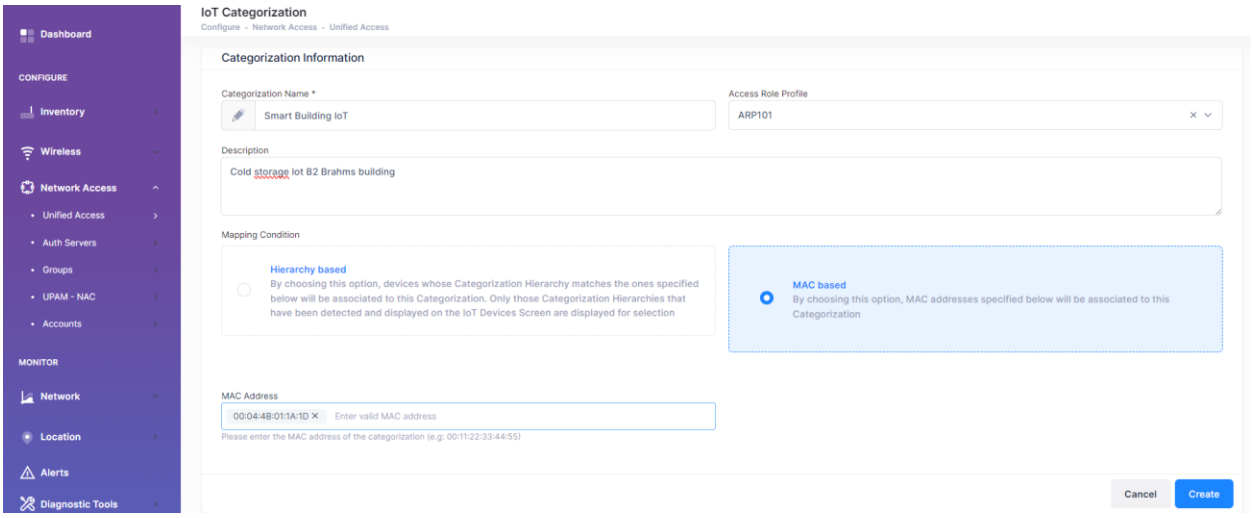


Figure 54: Direct MAC identification with enforcement - IoT Categorization [CONF]

52.	The cloud-based NMS shall provide IoT devices policy enforcement and control	C/PC/NC

NMS Cloud supports automatic IoT device policy enforcement when the onboarding of an IoT. This includes:

- Activation of automatic device enforcement
- Automatic application of an Access Role Profile (ARP)

The access role profile specifically managed for IoT devices complements the access profiles managed for the entire network, thanks to the Network unified access of NMS.

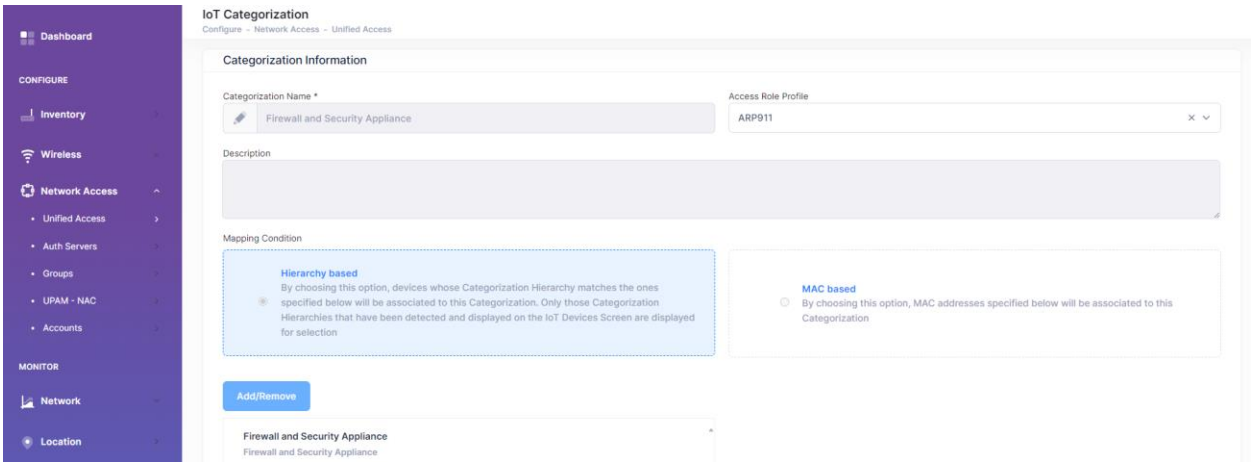


Figure 55: Hierarchy Based Categorization with access role profile - IoT Categorization [CONF]

53.	The cloud-based NMS solution shall offer IoT device secure onboarding that is as simple as possible for managed WLAN and without requiring additional third-party component.	C/PC/NC

NMS supports secure IoT device onboarding for Stellar WLAN and Stellar APs can search for IoT devices. NMS manages inventory and policies on IoT devices discovered by the APs and IoT inventory is completely unified LAN/WLAN. This fully includes:

- Classification of IoT devices on WLAN to a specific category
- Automatic enforcement and application to access profile (ARP)
- Exception list management by SSID, AP/APs group

NMS integrates a small dialogue tool for WLAN to select the APs covering the specific IoT devices.

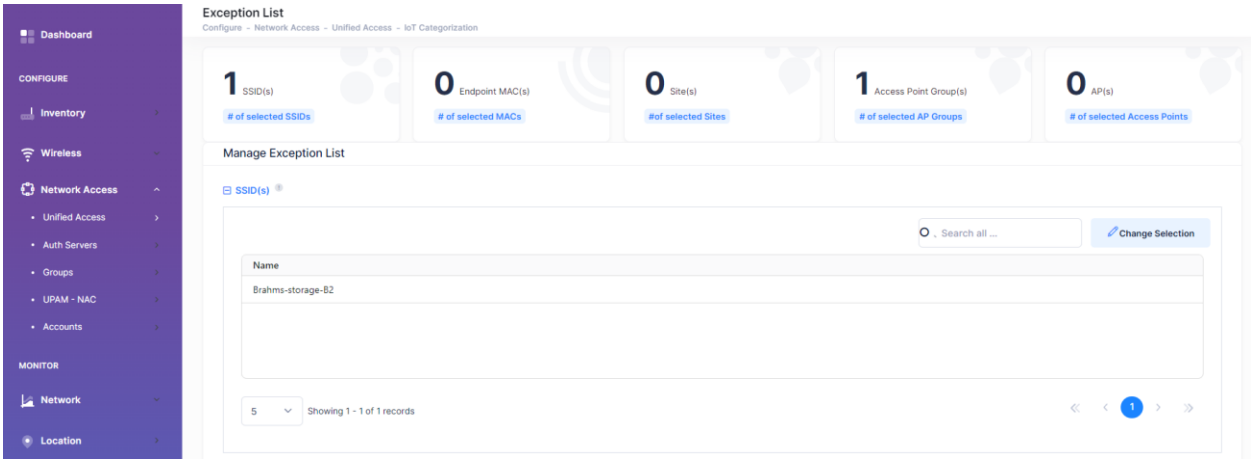


Figure 56: Manage exception list with device selection tool for WLAN - IoT categorization [CONF]

11. Network Access Control

Stellar Guest access is not developed in this document. Stellar Guest access provides a comprehensive captive portal solution with extensive customization capabilities and various access methods (sponsored guests, self-registration, social media login, WIFI4EU, etc.). Please refer to the Golden RFP Stellar for more details on the CP solution designed for Stellar.

54.	The cloud-based NMS shall support an integrated Network Access Control (NAC) with various authentication capabilities, including 802.1x, MAC, and certificate-based authentication.	C/PC/NC

The cloud-based NMS supports a fully integrated Network Access Control (NAC) for any device connected to the LAN/WLAN network. It provides MAC-based and 802.1x certificate-based authentication methods managed by NMS.

MAC-based authentication offers a simple layer of security and 802.1x authentication involves the requesting device, authenticator, and an authentication server. The supplicant can be a computer, smartphone, phone or any WLAN/LAN equipment.

The authentication server supports RADIUS and EAP protocols for the network and is fully integrated in NMS (the UPAM-NAC is described in next point). UPAM-NAC provides comprehensive certificate management for 802.1x authentication of corporate network with integrated RADIUS from NMS:

- CA certificates (public authorities) with support for various formats
- Server certificates with support for various formats
- Private keys according to the desired EAP protocol
- Additional certification authorities depending on the network in different organizations

55.	The cloud-based NMS shall support built-in RADIUS server and Captive Portal capabilities. RADIUS must not be proposed as separated feature	C/PC/NC

Cloud-based NMS offers an embedded Radius server for 802.1x and MAC authentication. called UPAM-NAC in the form of a software module integrated into the NMS.
UPAM-NAC is a comprehensive access policy manager:

- Application for WLAN visitor access to the network
- Application for BYOD access for integration of WLAN employee devices

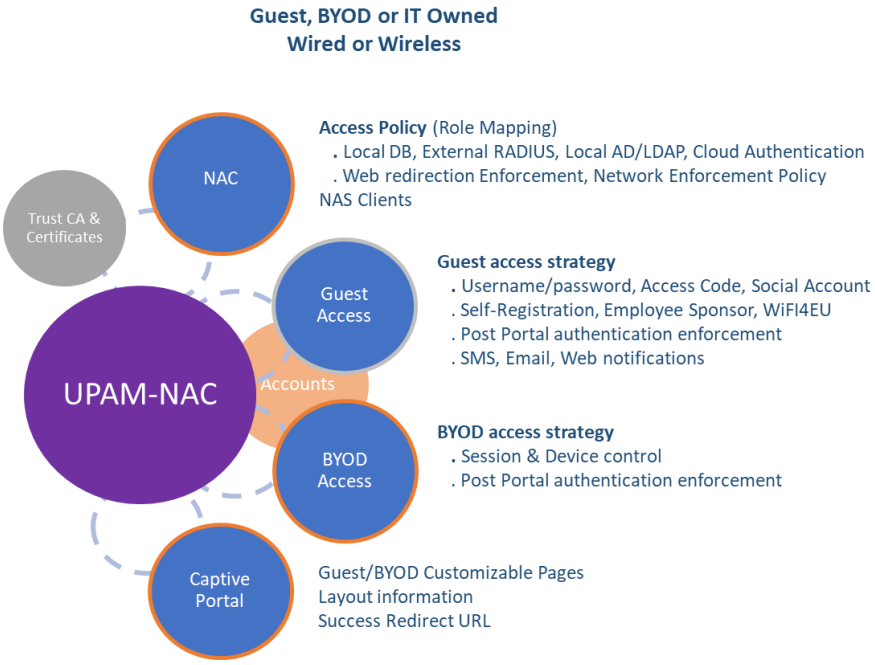


Figure 57: Unified Policy Access Manager

- A very flexible service model:
  - RADIUS requests are checked against access policies by matching to parameters configured in access policies.
  - Access policies route to "authentication strategy" to adopt, the authentication EAP, the authentication source, access policy (ARP) and web redirection strategy
  - Authentication can be done with the local NMS database or by external AAA or LDAP/AD and/or internal or external CP solution

UPAM-NAC supports main EAP authentication methods.

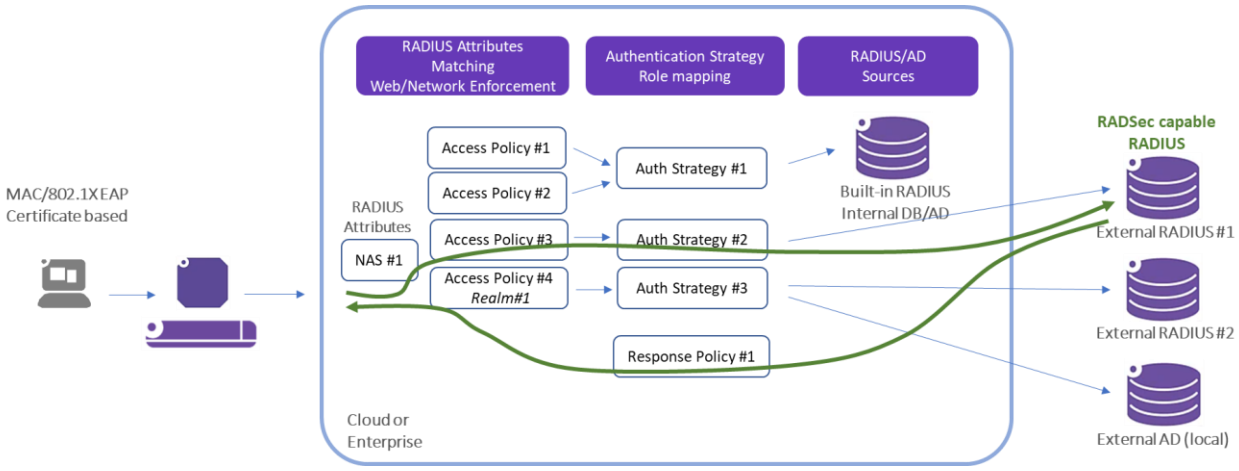


Figure 58: operation in UPAM-NAC for 802.1X EAP client

UPAM-NAC (version 10.4) can handle up to 1000 authentications and 500 captive portal accesses per minute in high-density Wi-Fi environments. It also supports up to 400,000 active devices simultaneously, making it very competitive with dedicated cloud-based Captive Portal solutions from the competition. The advanced Captive Portal embedded solution for Stellar in Enterprise mode is also managed by the UPAM-NAC module and is not detailed in this document.

UPAM-NAC supports authentication based on 802.1X, MAC, Captive Portal, and RADIUS for IPv6 clients (version 10.5).

56.	The cloud-based NMS shall support minimum of one built-in RADIUS instance and one built-in LDAP	C/PC/NC

NMS supports at least one integrated RADIUS instance (UPAMRadiusServer). It can also declare one integrated LDAP instance, allowing organizations to deploy a complete NMS UPAM-NAC with internal LDAP user database, without additional costs.

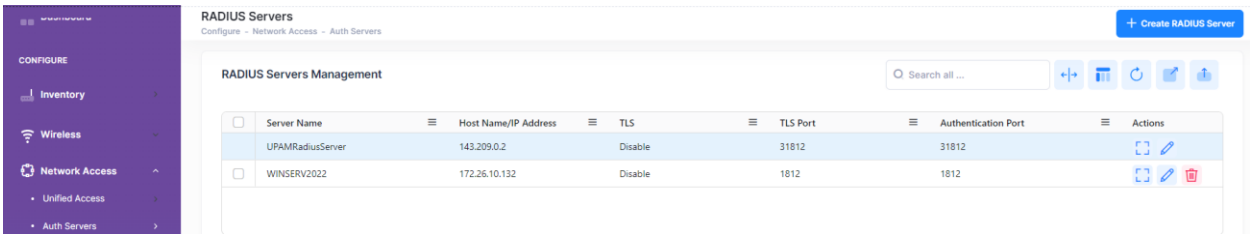


Figure 59: Built-in RADIUS server - Auth Servers [CONF]

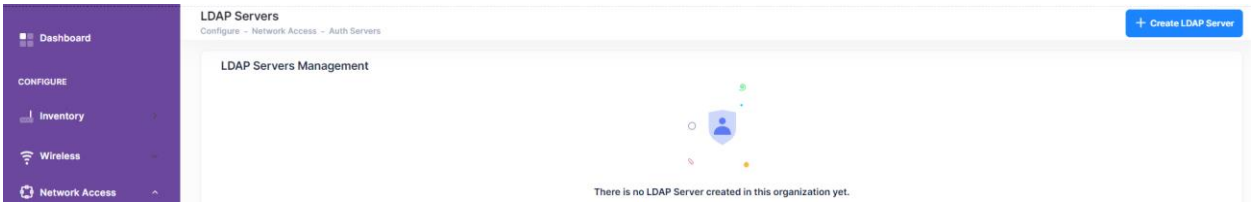


Figure 60: Create LDAP server - Auth Servers [CONF]

57.	The cloud-based NMS shall support external RADIUS and LDAP servers with role-mapping capabilities	C/PC/NC

UPAM-NAC can interface with external Radius servers or external LDAP servers. It can interface with most external authentication servers like Radius, LDAP, Active Directory and Microsoft Azure AD) FreeRadius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP

It securely manages UPAM-NAC credentials with RADSec option for communication with external RADIUS instances in the Cloud, can interface with multiple RADIUS according to speciic access conditions defined in access policy (SSID, IP, Aps group or RADIUS attribute)
and can integrate multiple NAS clients based on RADIUS attributes:

- Connection to various external authentication sources
- Centralized user management
- Possibility of assign unified access profiles to users based on AD/LDAP attributes.

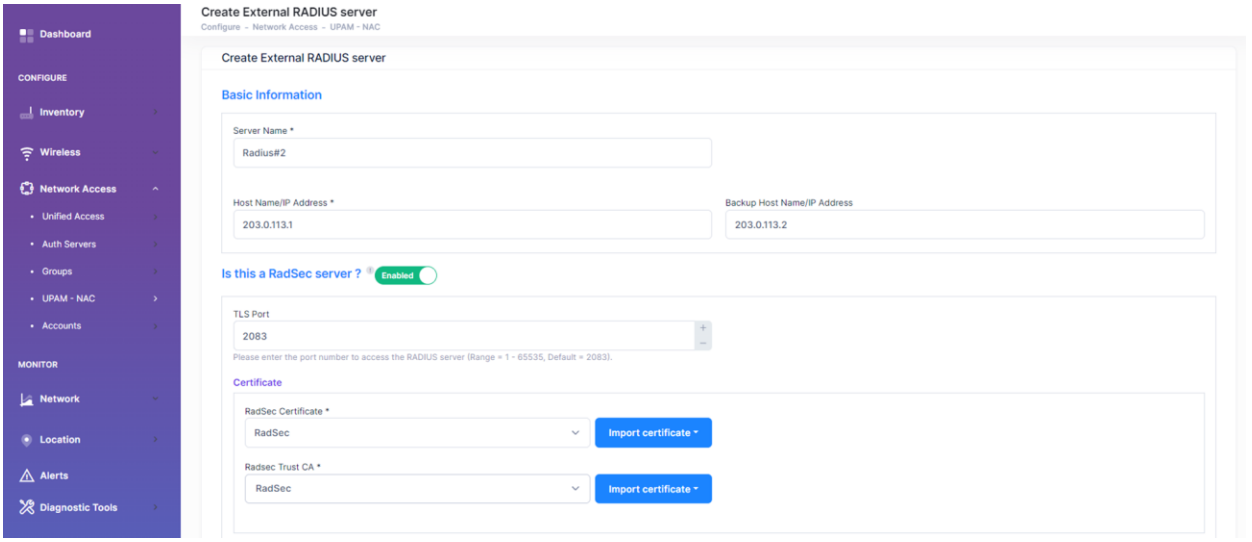


Figure 61: Manage External RADIUS server - External Source [CONF]

58.	The cloud-based NMS shall support grouping of attributes such as MAC and IP addresses, ports, or services into lists or profiles for easy policy configuration	C/PC/NC

Cloud-based NMS includes and manages a flexible and adaptive RADIUS attribute dictionary. This dictionary allows UPAM-NAC to integrate third-party network infrastructure and act as a RADIUS server to authenticate users from third-party devices.

UPAM-NAC uses RADIUS attributes to assign authenticated users/devices to a specific unified access role, simplifying the management of access policies in OmniVista® Cirrus 10 NMS. The attribute grouping feature ensures that multiple RADIUS attributes can be handled together, managing then efficient policy enforcement for users/devices.

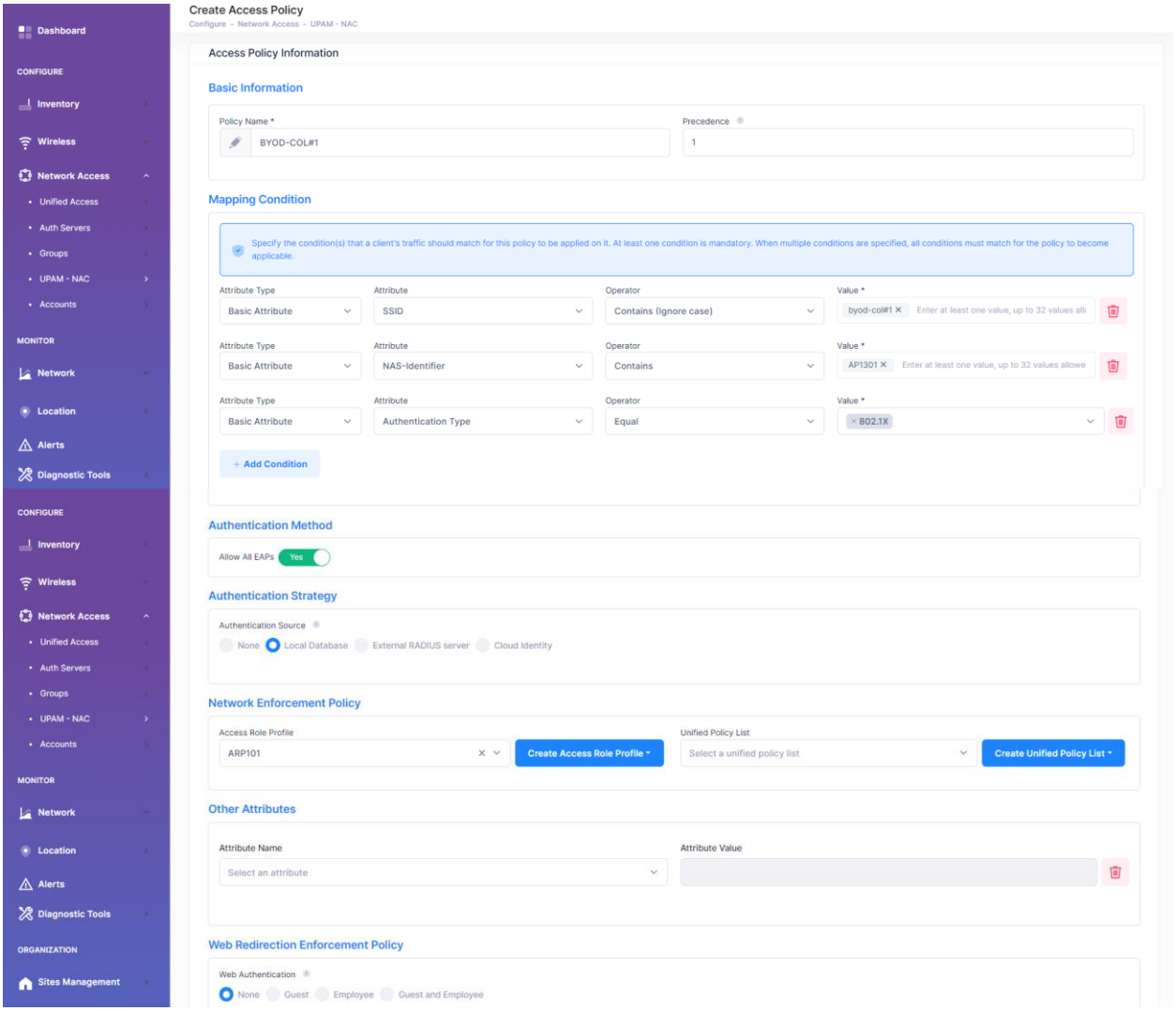


Figure 62: Map condition based on RADIUS attributes - Access Policies [CONF]

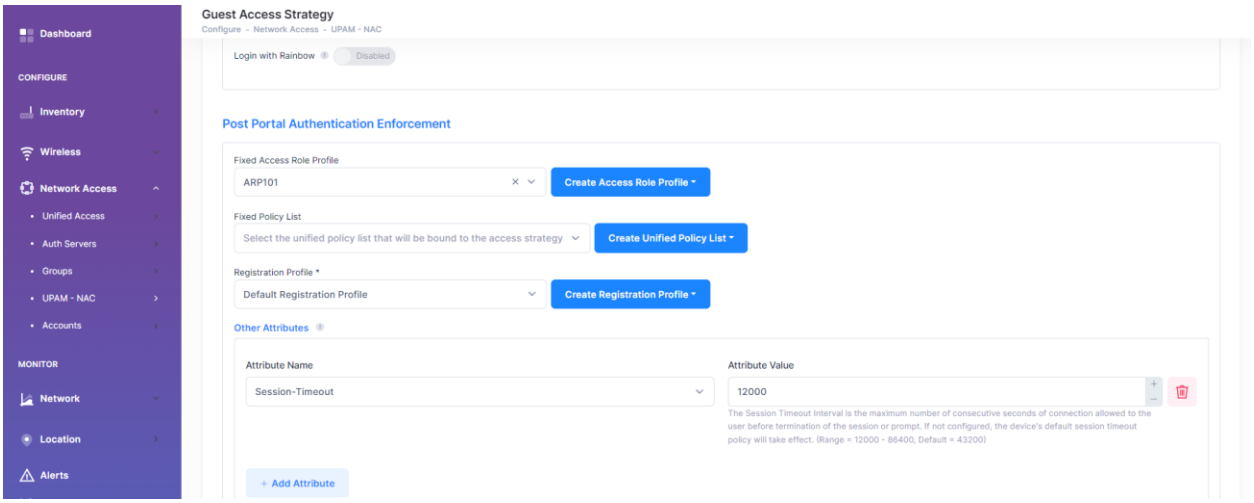


Figure 63: Post Portal enforcement for Guest with session timeout - Guest Access Strategy [CONF]

59.	The built-in RADIUS of NMS shall support dynamically filter ids such as VLANs and Private Groups to respond to extended WLAN user connections usage with dedicated specific groups	C/PC/NC

For some use cases like education, hospitality or government that require large number of connections, UPAM-NAC supports dynamic VLAN and allows to scale up to 4K VLANs instead of 255 ARPs provided in Stellar APs. UPAM-NAC sends ARP in VLAN ID and/or attributes without pre-configured ARP for any 802.1x/MAC authentication.
Similarely UPAM-NAC supports PSK type Private Groups that allows a same SSID to connect different private groups with each its own PSK.

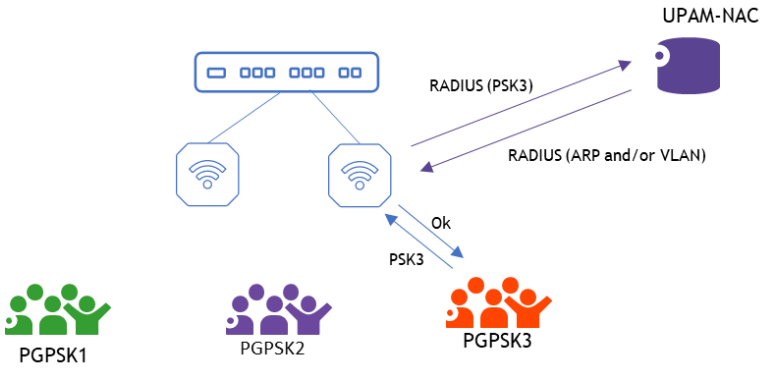


Figure 64: Dynamic VLAN and Dynamic Private Group SSID with UPAM-NAC

60.	The cloud-based NMS shall support the configuration of unified LAN/WLAN access with policy-based control, for connected and authenticated users and equipment	C/PC/NC

NMS Cloud supports the management of different types of roles and policies, for devices and users, for a complete unified management of mobility in the LAN/WLAN network. Key features include:

- Access Classification: Classifies equipment based on MAC/SSID/LLDP attributes and applies User network profile directly to a set of equipment/ports.

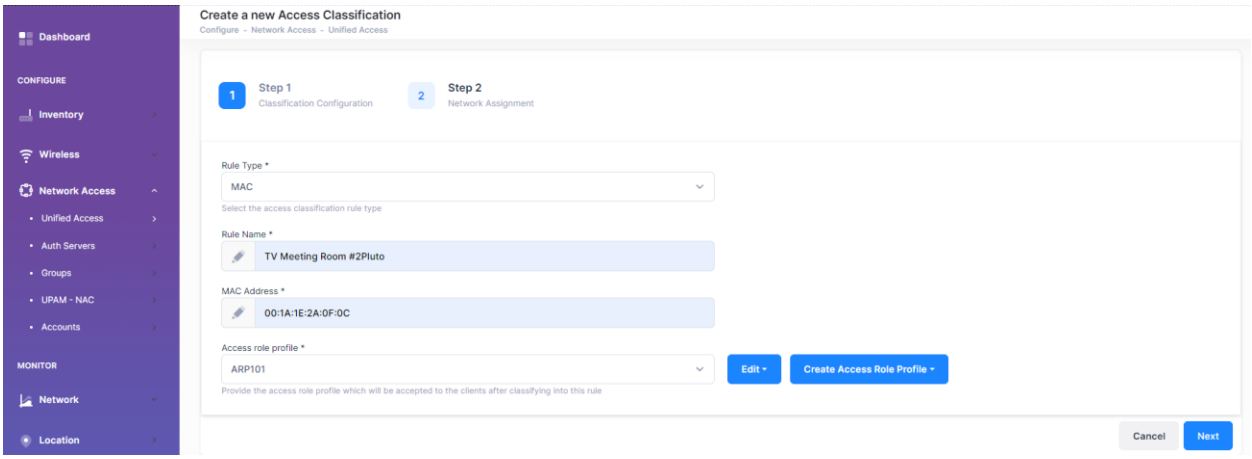
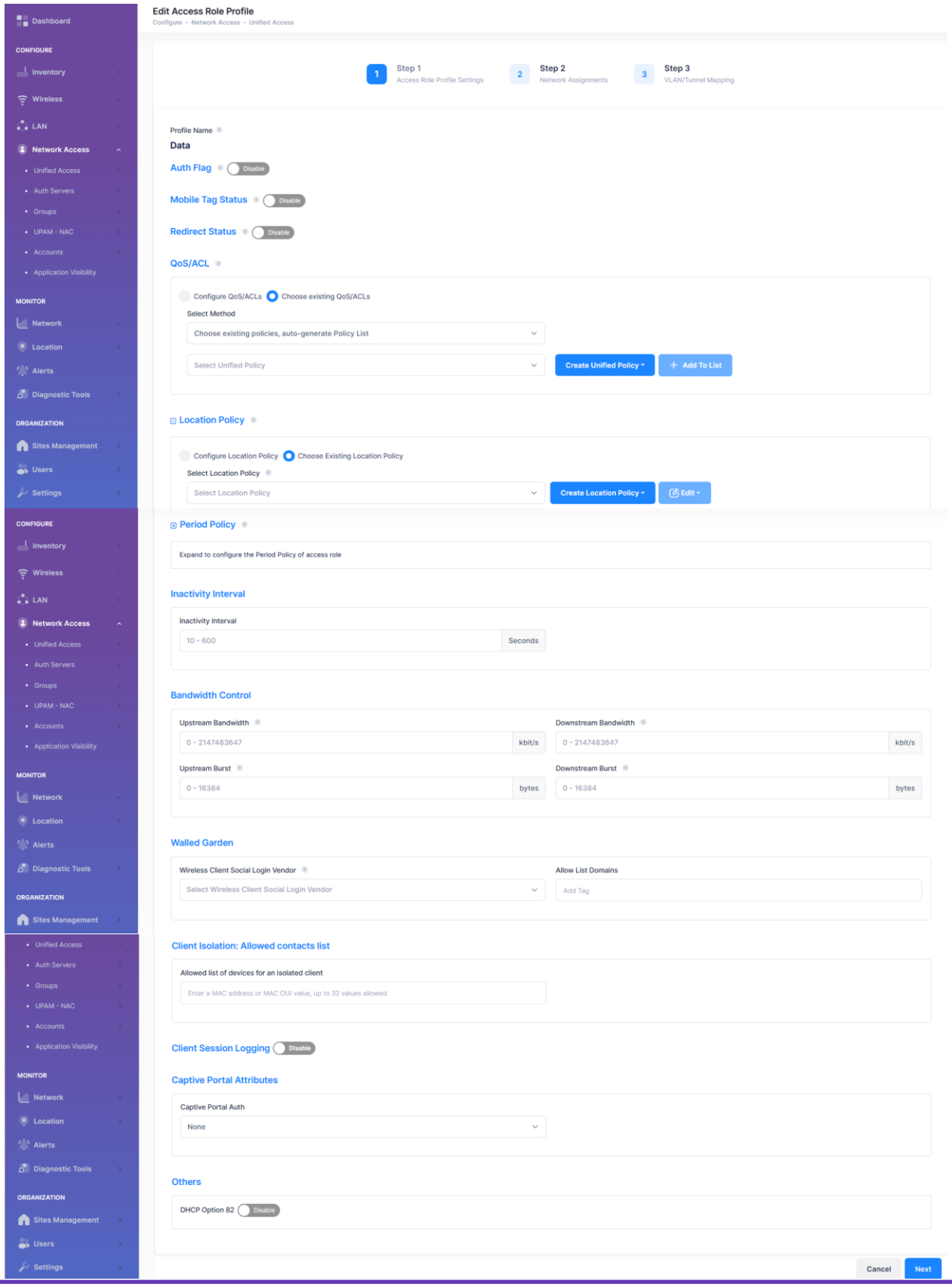


Figure 65: User Network Profile on MAC address - Access classification [CONF]

- Access Authentication policy: Manages MAC/802.1x authentication directly to equipment/ports or specifies actions to be done if authentication fails on resources (access classification or VLANs actions).

- User Network profile (or ARP): Applies when the authentication process was successful for this user or did not return a role. This profile assign the user to QoS, security ACL or BW policies, and ensures isolation from other users in the network.

The user role enables the assignement of the appropriate VLAN(s) and/or L2GRE tunnels to the user or equipment, OmniSwitch® or AP Group (version 10.5)


Edit Access Role Profile
Configure → Network Access → Unified Access
Step 1
Access Role Profile Settings
Step 2
Network Assignments
Step 3
VLAN/Tunnel Mapping
Profile Name
Data
Auth Flag
Disable
Mobile Tag Status
Disable
Redirect Status
Disable
QoS/ACL
Configure QoS/ACLs
Choose existing QoS/ACLs
Select Method
Choose existing policies, auto-generate Policy List
Select Unified Policy
Create Unified Policy
Add To List
Location Policy
Configure Location Policy
Choose Existing Location Policy
Select Location Policy
Select Location Policy
Create Location Policy
Edit
Period Policy
Expand to configure the Period Policy of access role
Inactivity Interval
Inactivity Interval
10 - 600
Seconds
Bandwidth Control
Upstream Bandwidth
0 - 2147483647
kbit/s
Downstream Bandwidth
0 - 2147483647
kbit/s
Upstream Burst
0 - 16384
bytes
Downstream Burst
0 - 16384
bytes
Walled Garden
Wireless Client Social Login Vendor
Select Wireless Client Social Login Vendor
Allow List Domains
Add Tag
Client Isolation: Allowed contacts list
Allowed list of devices for an isolated client
Enter a MAC address or MAC OUI value, up to 32 values allowed
Client Session Logging
Disable
Captive Portal Attributes
Captive Portal Auth
None
Others
DHCP Option 82
Disable
Cancel
Next
Dashboard
CONFIGURE
Inventory
Wireless
LAN
Network Access
Unified Access
Auth Servers
Groups
UPAM - NAC
Accounts
Application Visibility
MONITOR
Network
Location
Alerts
Diagnostic Tools
ORGANIZATION
Sites Management
Users
Settings

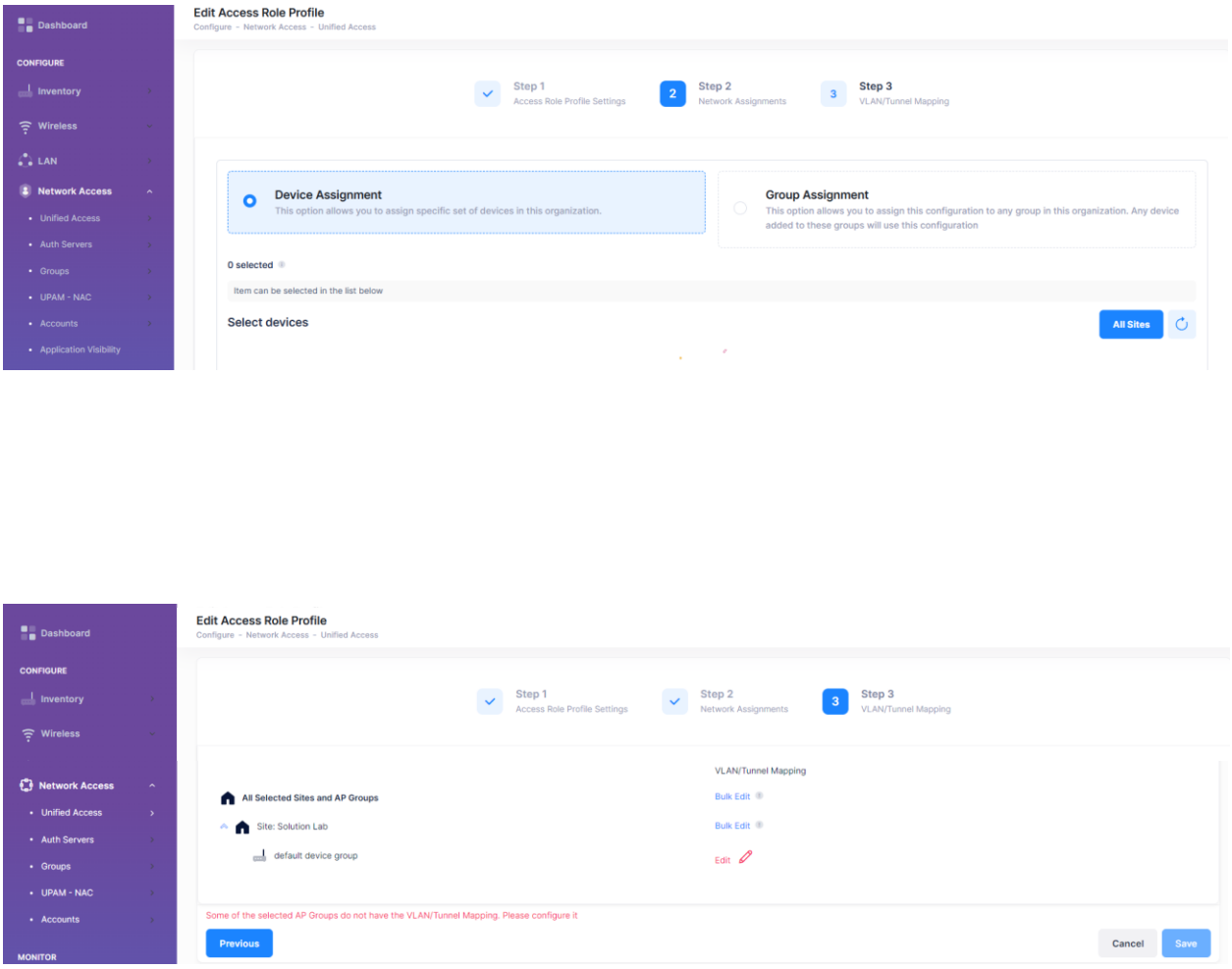
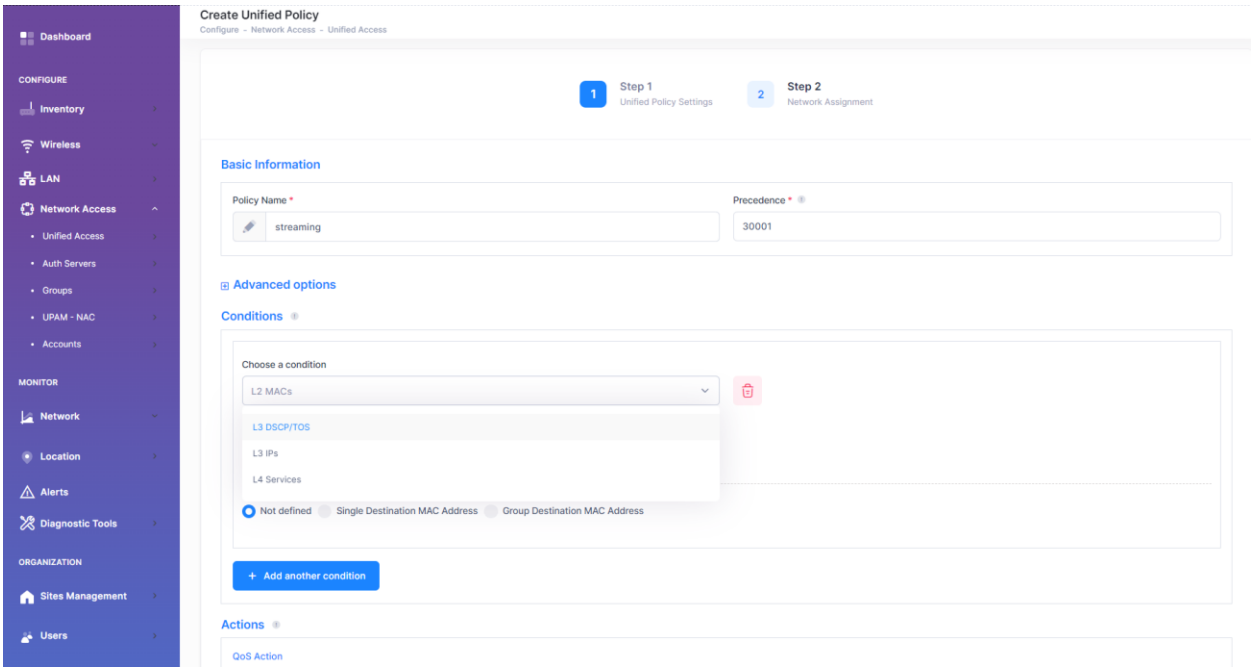


Figure 66: Manage User Network Profile - Access Role Profiles [CONF]

- Support of Unified security ACL, QoS, BW, time periods policies for any user or equipment: These additional policies, or list of policies, can be directly assigned to network device, group or directly to User Network profiles.
  NMS supports IPv6 based ACL for client traffic, with IPv6 Security, QoS, Firewall, IPv6 Policies management (version 10.5)



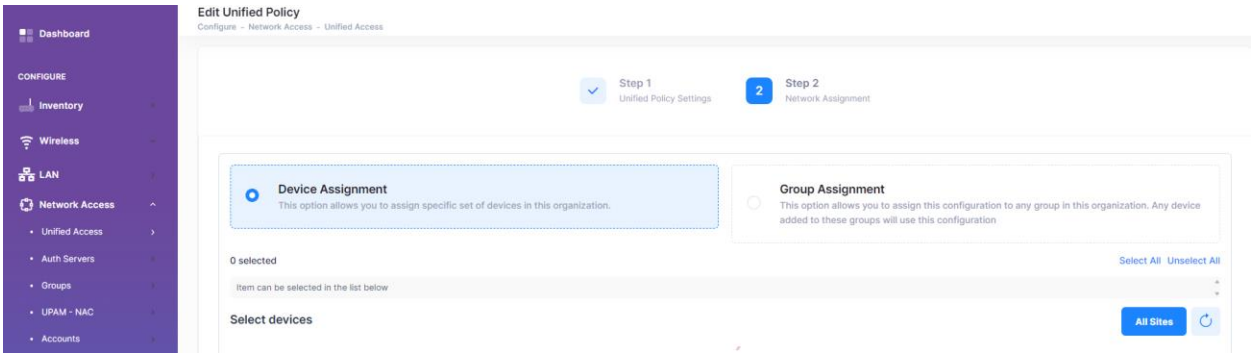


Figure 67: Manage and assign Unified Policy – Unified Policies [CONF]

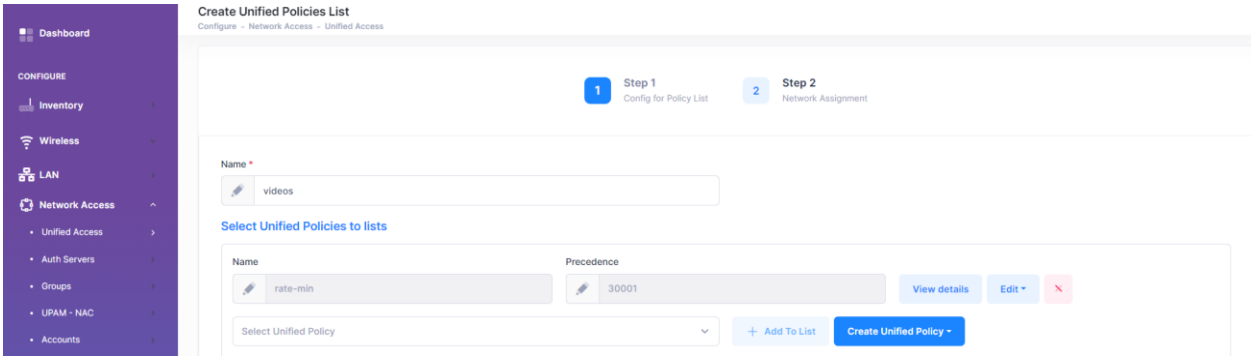


Figure 68: Manage and assign list of Policies – Unified Policies list [CONF]

- Tunnel profile: Support for tunnel IDs and L2GRE server IP terminations, as well as their IP backups (version 10.5)

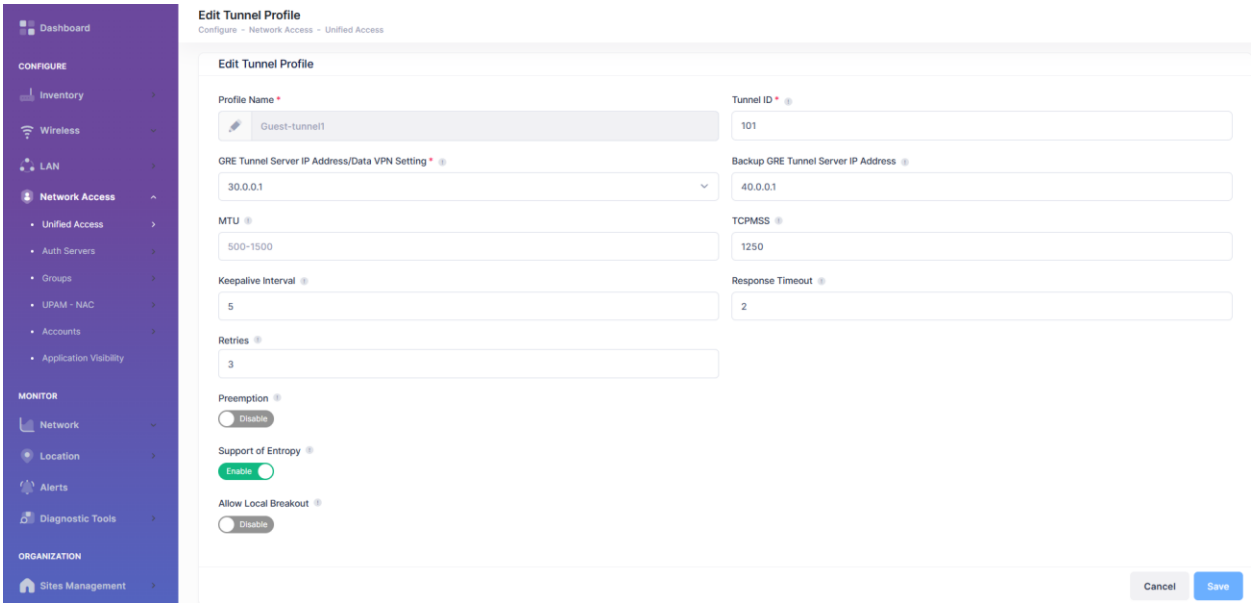


Figure 69: Manage L2GRE Tunnel - Tunnel Profiles [CONF]

- Unified location-based policies and periods-based policies: These are highlighted hereinafter

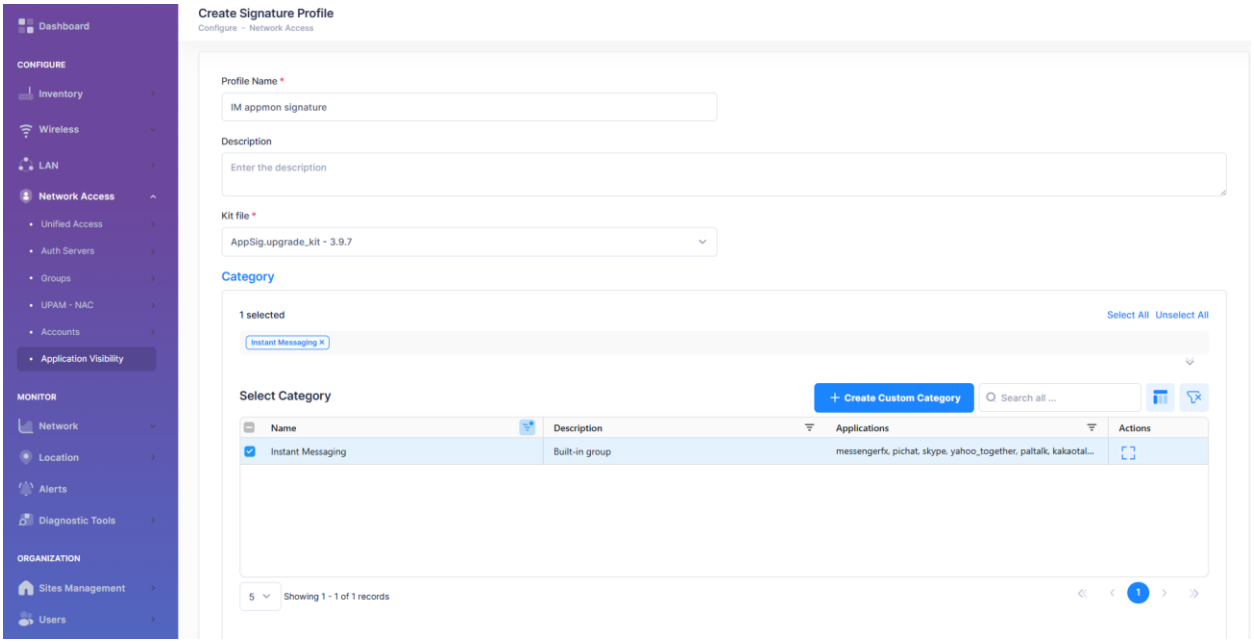
61.	The cloud-based NMS shall support Deep Packet Inspection (DPI) capabilities for application-level recognition up to Layer 7 (L7). This feature should enable advanced control over applications running on the LAN/WLAN, including those using secure HTTPS protocols. The administrator must be able to monitor application traffic and apply application-level QoS policies (such as bandwidth management or blocking).	C/PC/NC

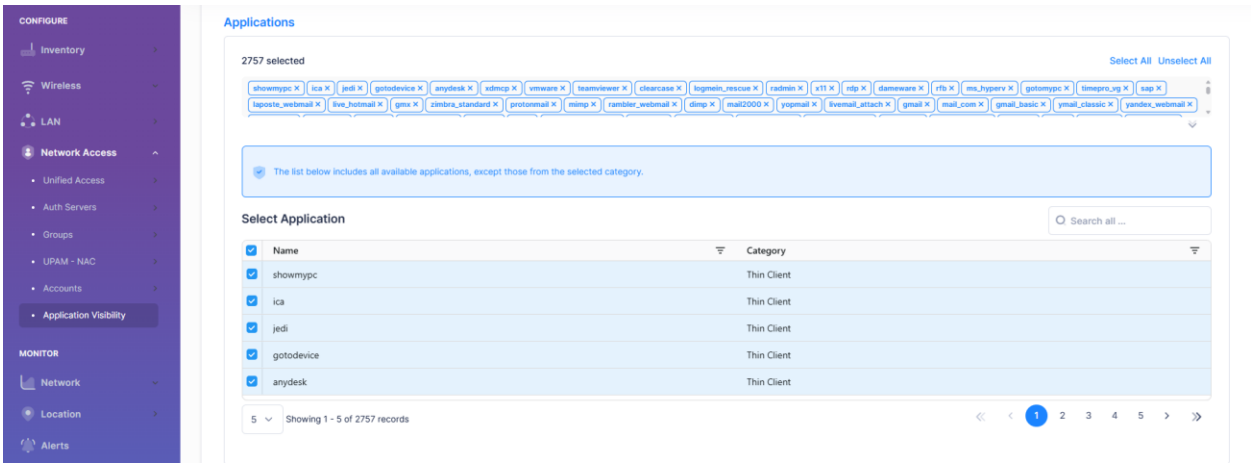
OmniVista® Cirrus 10 fully meets this requirement. The latest Stellar Access Points (see datasheets for list of compatible APs) embed DPI technology, enabling real-time application classification by category and role-based User Network control (ARP).

This provides the user with complete *visibility of LAN/WLAN application traffic* (WLAN only version 10.5) with the ability to enforce QoS policies, bandwidth management, and ACL filtering to ensure optimal performance for business-critical applications. The system can also block harmful or non-compliant applications when needed.

This functionality, known as **DPI / Application Visibility & Application Monitoring**, is natively integrated into the NMS. It addresses the increasing standarization of application traffic over HTTP/HTTPS, including critical enterprise applications. Through a regularly updated application signature file (e.g. kit version 3.9.7 in OmniVista® Cirrus 10.5), the solution inspects traffic at higher layers (up to L7) even when traffic is encrypted.

For instance, by applying the *"Instant Messaging" category*, the user can evaluate use of WhatsApp, Gmail Chat, or Discord as business-related, compared to more personal services such as Facebook Messenger, Jabber, or Telegram. Similarly, the *"Audio/Video" category* can be used to restrict voice traffic to SIP or UAUDP telephony applications only. In the example below, the *"Instant Messaging" version 3.9.7 signature* is applied to a group of Stellar APs with embedded DPI, to monitor and control application traffic across the WLAN.





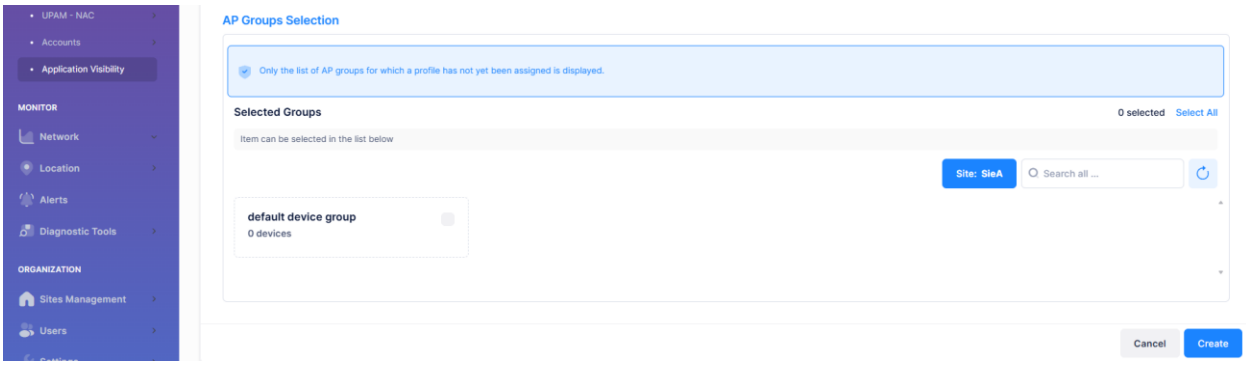


Figure 70: Create and Manage IM Signature Profile – Application Visibility [CONF]

62.	The cloud-based NMS shall support a built-in local database for company property and user accounts for employees and guests	C/PC/NC

Cloud-based NMS supports local and comprehensive database for employee, guest as well as specific company property database for devices.

The Employee Account tool enables bulk provisioning of employee accounts by importing a file. It supports employee network enforcement policies with an access role profile and allows to define employee account strategy, including company's password policy.

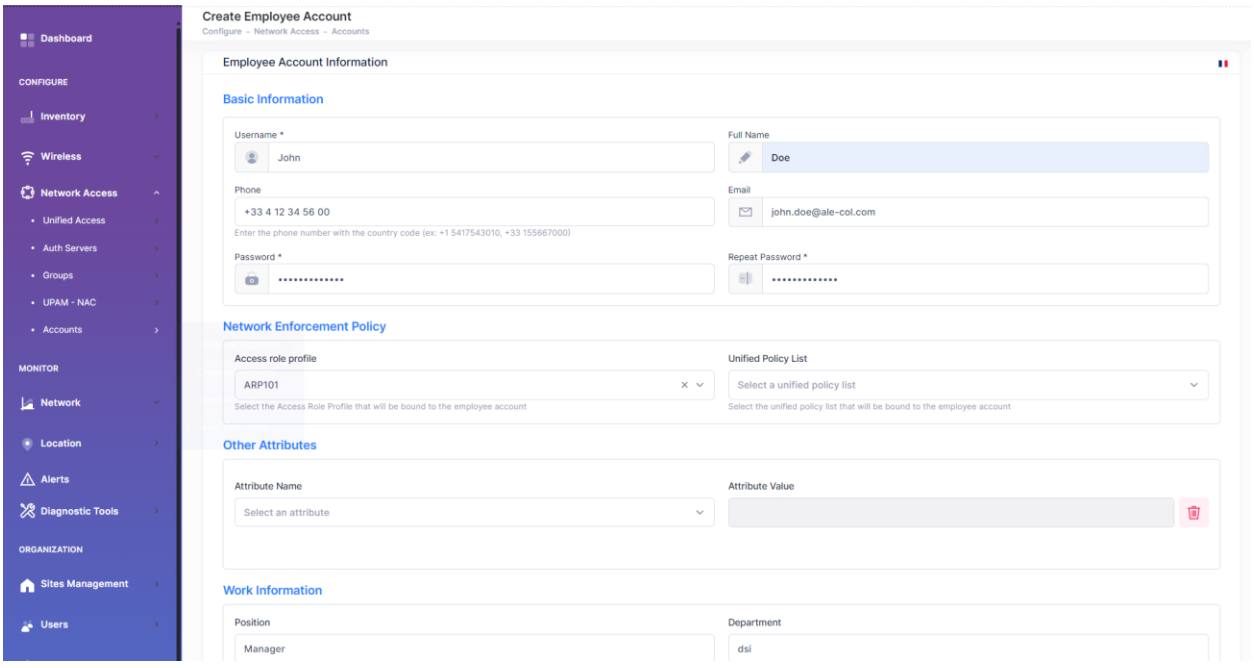


Figure 71: Create Employee Account - Employees Accounts [CONF]

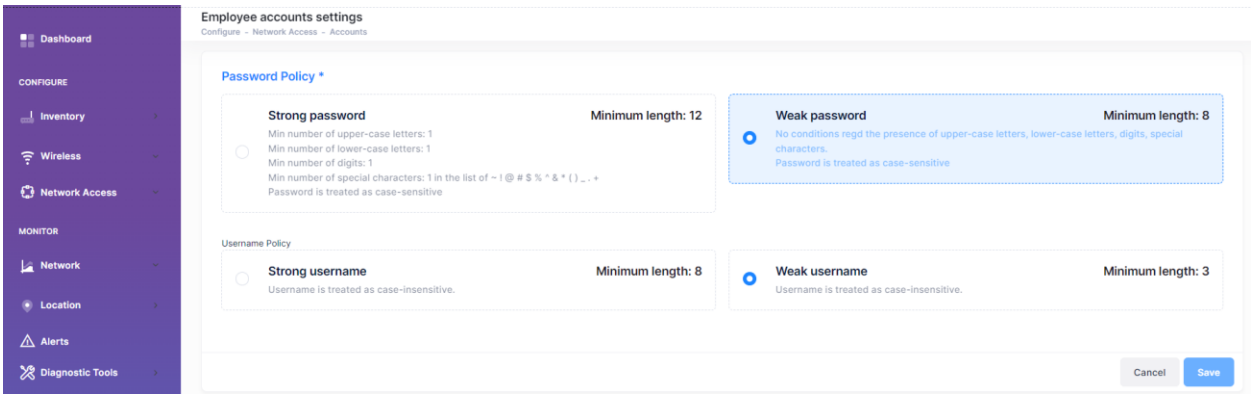


Figure 72: Employee Password Policy - Employees Accounts settings [CONF]

The Guest Account tool of NMS enables bulk provisioning of guest accounts by importing a file and allows batch creation of guest accounts. Guest account tools allows to define a guest account strategy, in particular for validity period of the accounts, for registration in hotspots Wifi (WIFI4EU Europe) for guest service levels or managing a voucher for guests. Guest account tool in version 10.4 can handle up to 5000 accounts.

NMS guest management allows non-IT staff to create temporary guest accounts using their guest operator account.

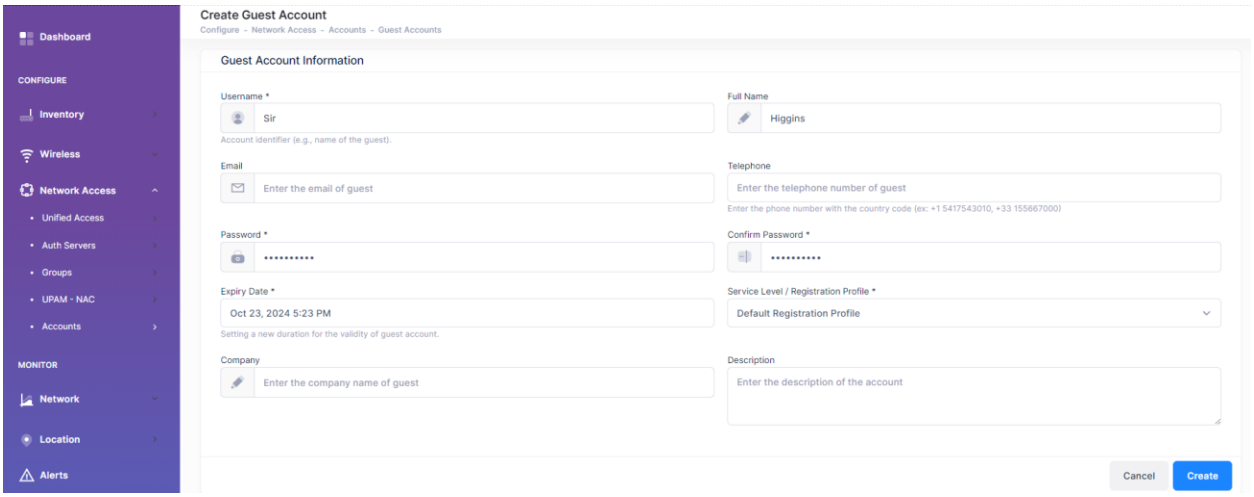


Figure 73: Create Guest Account - Guest Accounts [CONF]

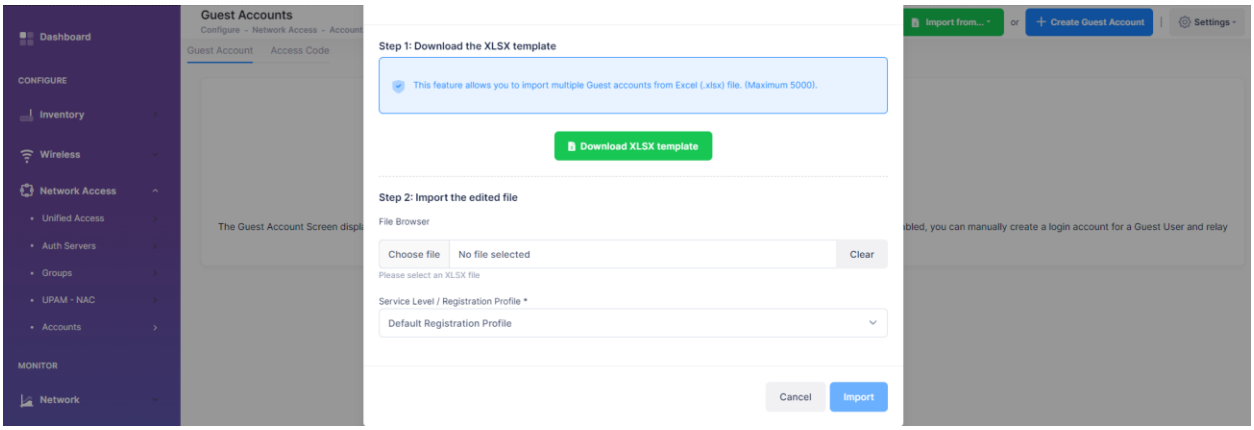


Figure 74: Bulk Guest Provisioning - Guest Accounts [CONF]

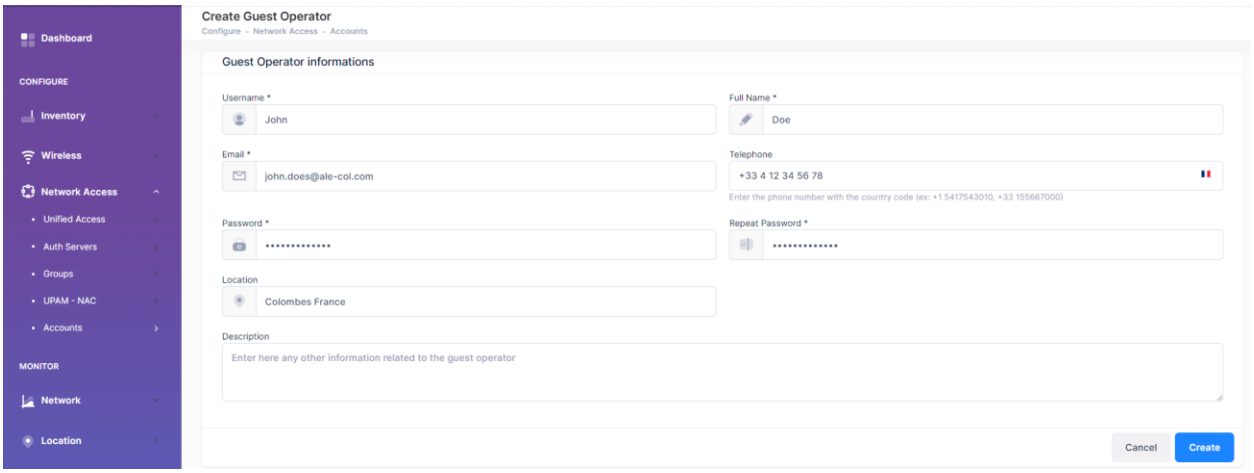


Figure 75: Guest operator account creation - Guest Operators [CONF]

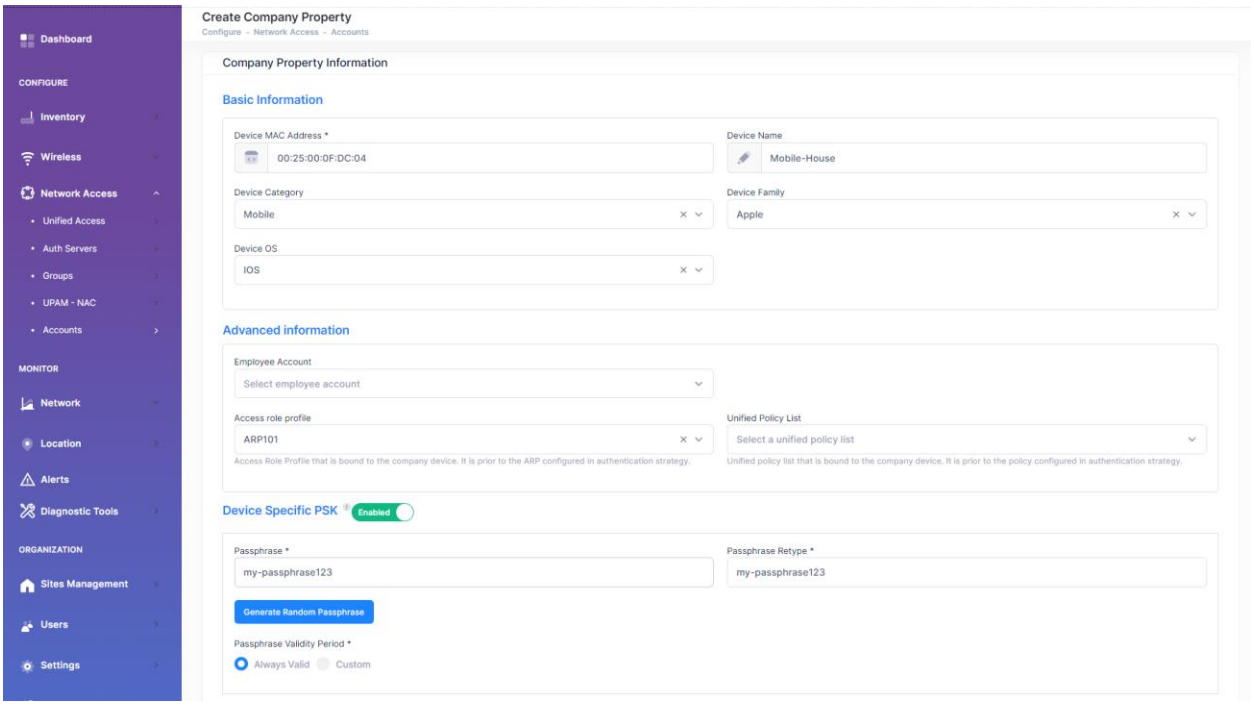


Figure 76: Device specific settings - Company Property [CONF]

63.	The cloud-based NMS shall support GRE tunneling features such as isolation for WLAN Guest	C/PC/NC

Cloud-based NMS manages strict isolation of guest user traffic. A dedicated OS6860 or OS6900 serves as the GRE tunnel gateway, terminating guest GRE tunnels established by APs. Firewall rules are enforced for strict traffic control, ensuring that traffic between guests is blocked even if they are in the same VLAN.

NMS fully supports GRE tunnel profiles identifiable in LAN by tunnel IDs. Tunnel termination is mapped to any unified access role and the two GRE terminations are managed by LAN. OS6860 support up to 750 GRE, while OS6900 supports up to 1000 GRE tunnels. NMS fully supports Stellar <> OmniSwitch® and OmniSwitch® <> OmniSwitch® tunnels on the LAN and supports IPv6 forwarding over IPv4 GRE Tunnels (version 10.5).

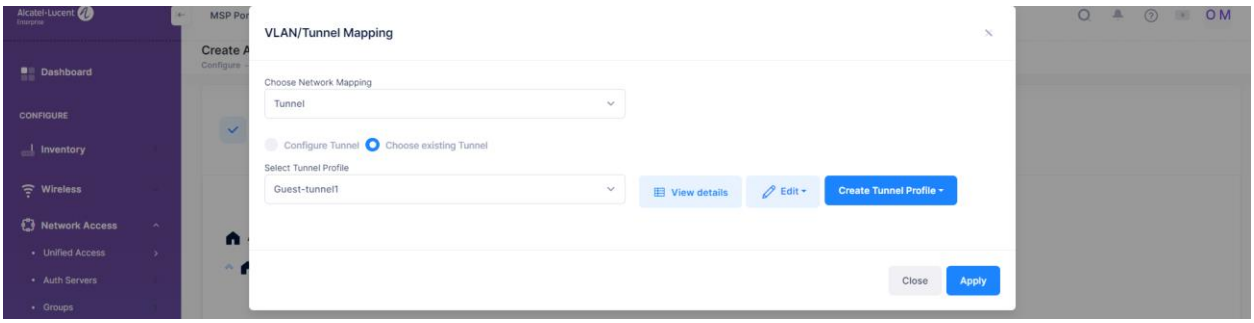


Figure 77: Map Stellar Guest User Network Profile to Tunnel - Access Role Profiles [CONF]

The client isolation in Stellar solution can be done without use of dedicated GRE gateway. It can be configured directly at the SSID level with a list of authorized MAC addresses and with ACLs. However in this mode network is not isolated from guest traffic.

64.	The cloud-based NMS shall support unified location and period-based policy configuration	C/PC/NC

Cloud-based NMS supports the management of location policies and period-based policies in a completely unified way. Different location systems can be declared under NMS, and different time-period policies can be created according to a precise schedule or specific time zone.

These policies are applicable in any Unified Access Role (ARP), providing a fully structured approach to the scheduling and location policies for a site or an organisation.

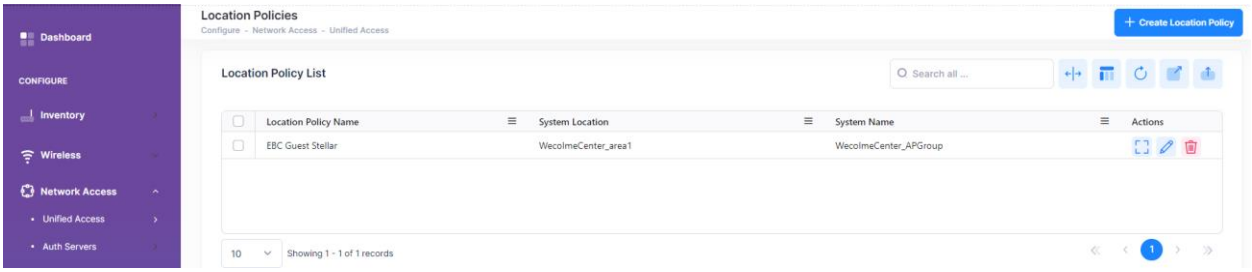


Figure 78: Manage Location Policy - Location Policies [CONF]

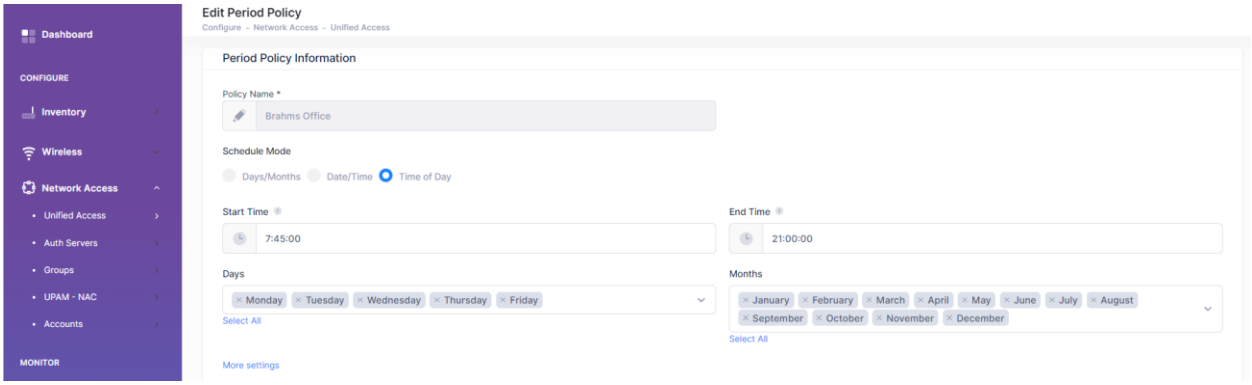


Figure 79: Manage Time of Day policy - Period Policies [CONF]

65.	The cloud-based NMS shall support configuring different guest service levels	C/PC/NC

Cloud-based NMS allows you to define service level agreements for guest connections, ensuring security or even QoS enforcement. These service levels can include bandwidth limits, access time restrictions, and specific usage policies.

For public networks such as WIFI4EU, service levels can be configured into a recording profile to comply with WIFI4EU requirements. Additionally, guest service levels can be customized based on user type (such as VIP, standard Guest or event-specific access) providing a flexible and secure guest Wi-Fi experience.

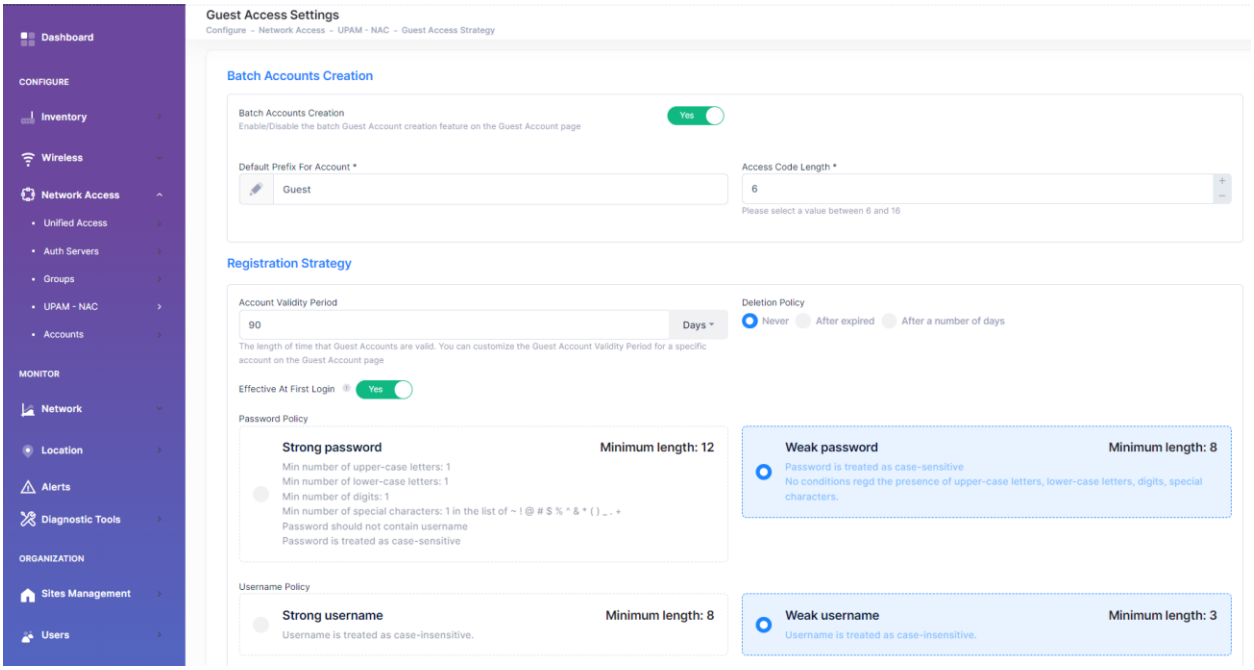


Figure 80: Global configuration for standard Guest - Global Guest Access Settings [CONF]

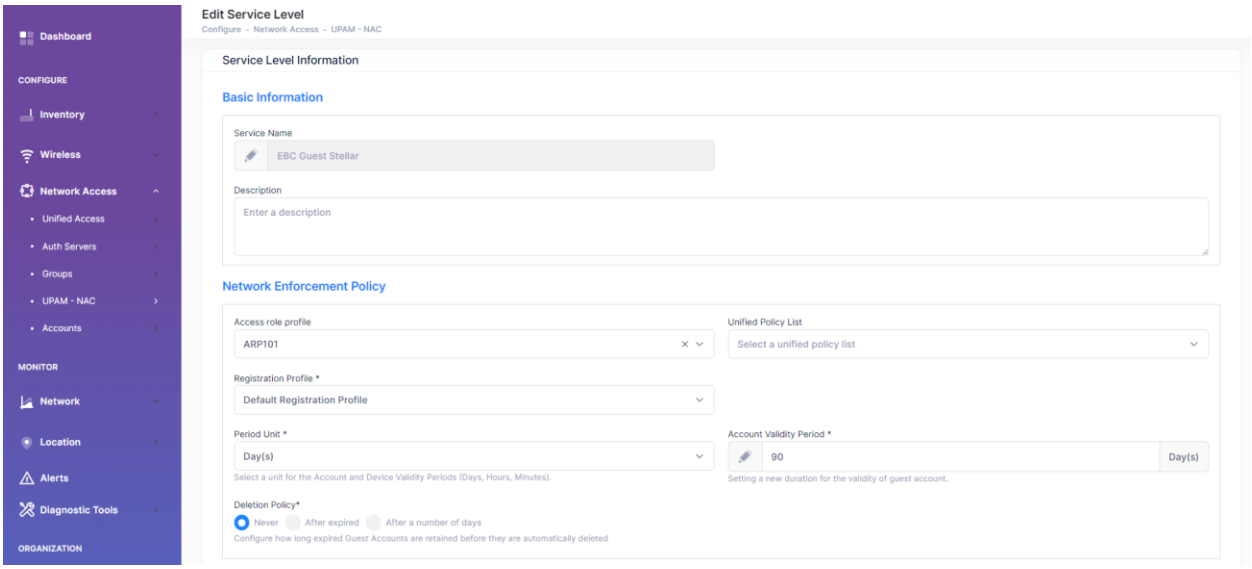


Figure 81: Manage Network enforcement - Service levels [CONF]

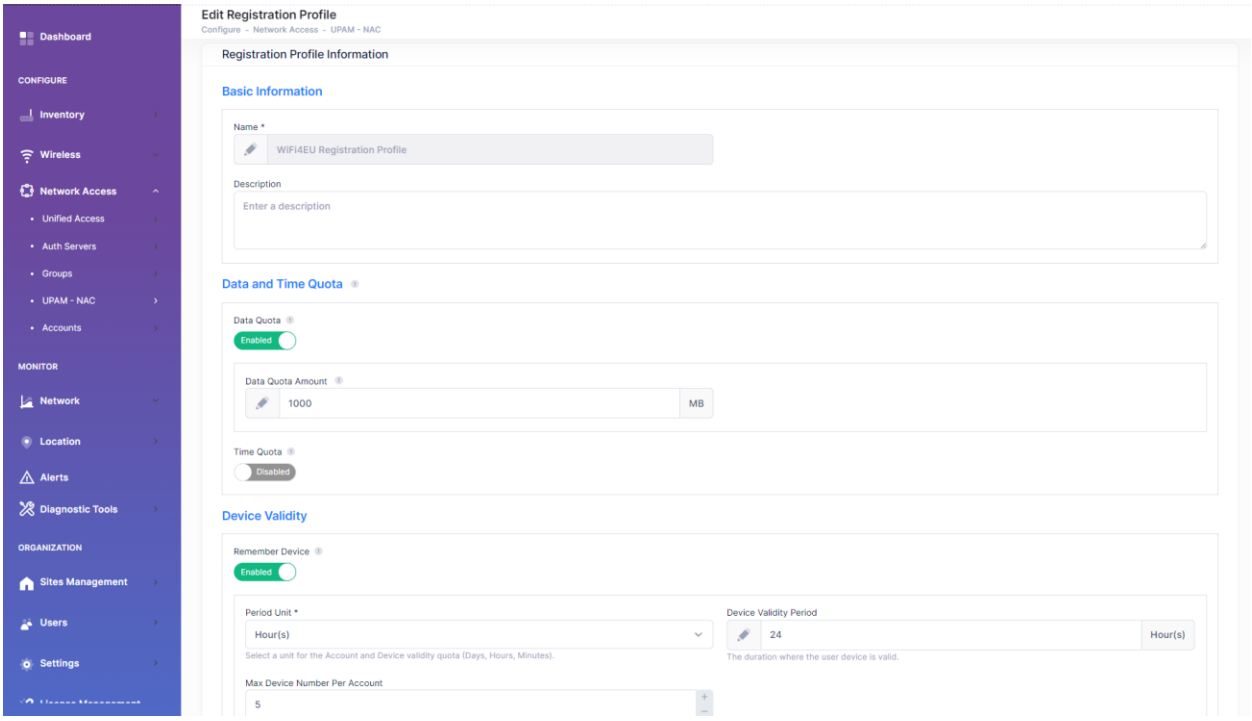


Figure 82: WiFi4EU Registration Profile - Registration Profiles [CONF]

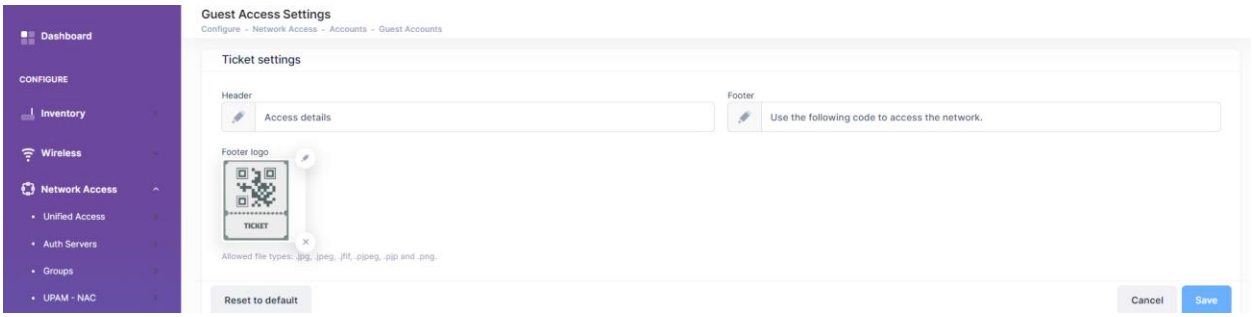


Figure 83: Manage Ticket - Ticket Settings [CONF]

66.	The cloud-based NMS shall support configuring guest time and data quotas	C/PC/NC

Cloud-based NMS fully supports Guest time and data quotas that can be configured into a registration profile.

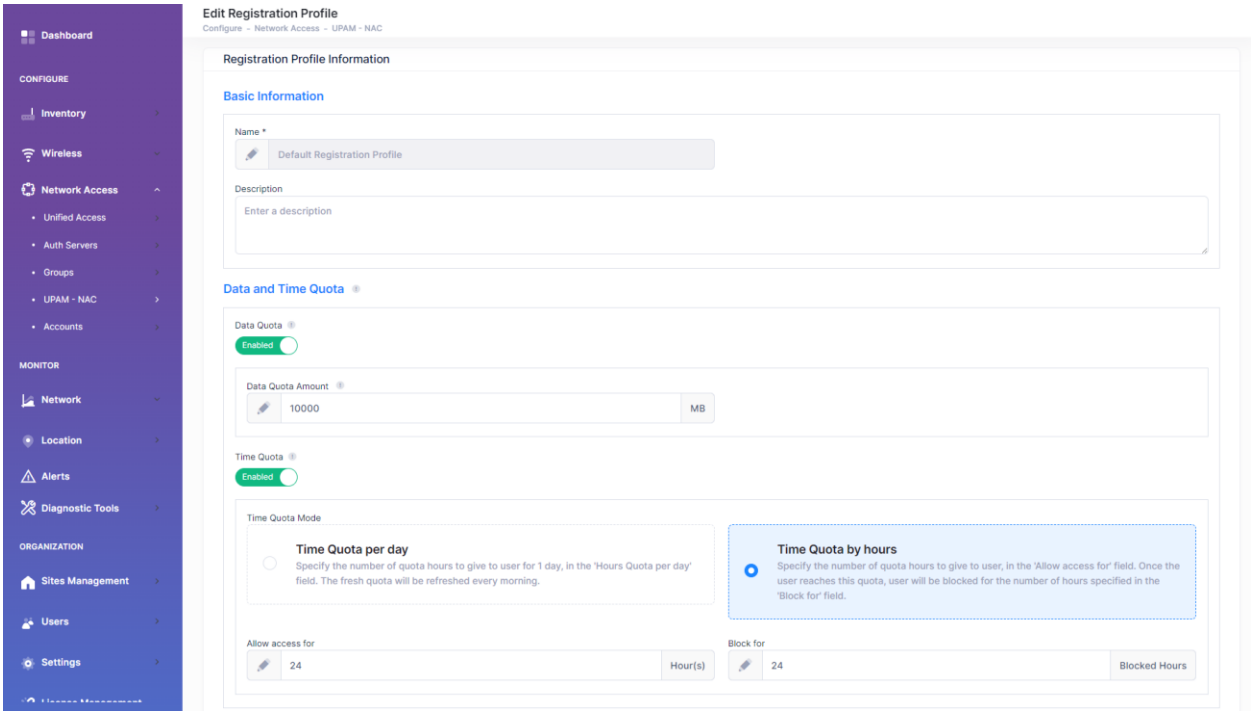


Figure 84: Manage Data and Time Quota - Registration Profiles [CONF]