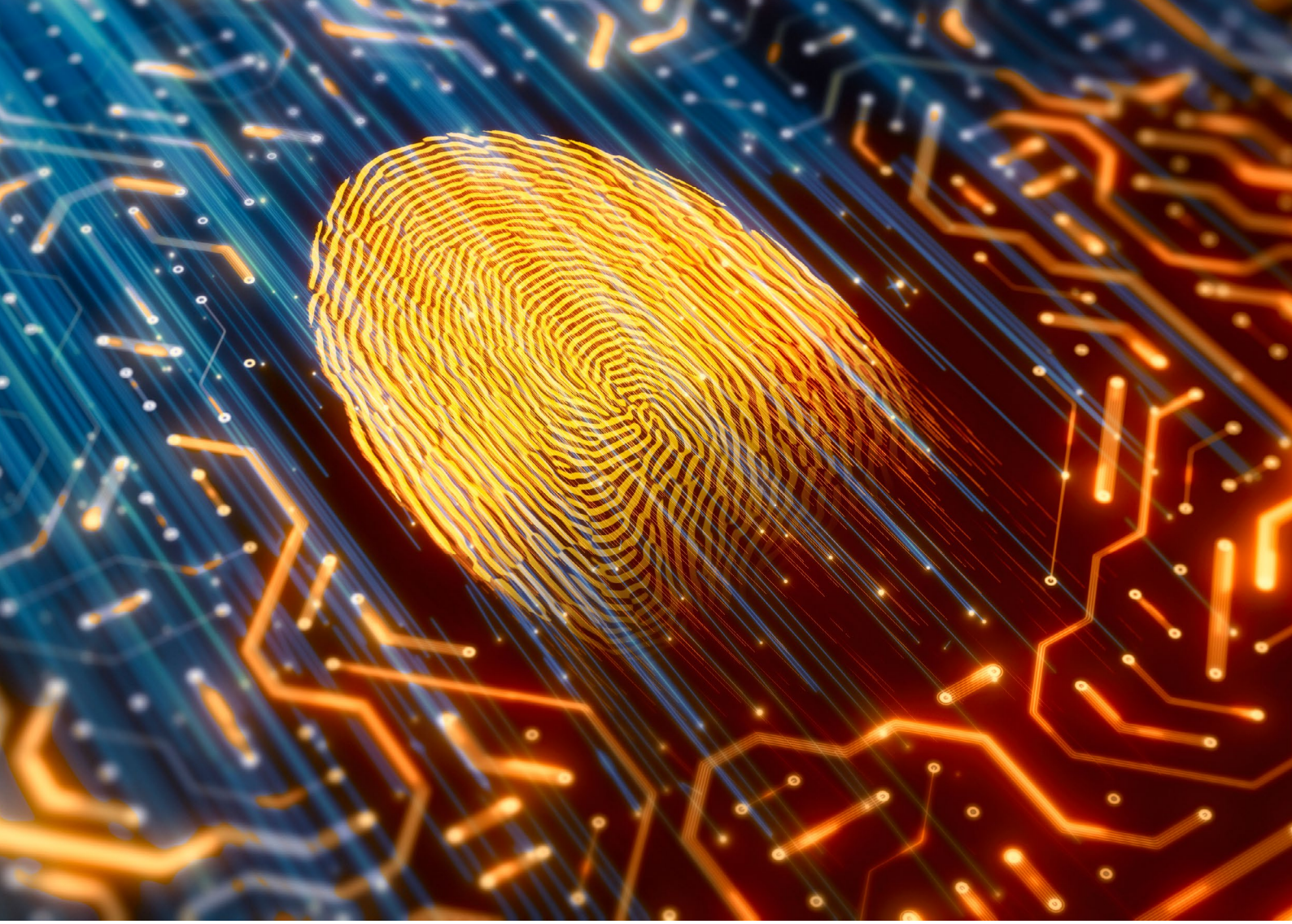


Augmented intelligence and device fingerprinting enabled networks

Effective network security and secure device mobility requires a Service Defined Network architecture

July 2020

Alcatel·Lucent Enterprise

Table of contents

Introduction and technical background

Digital age technologies that help improve efficiency are being adopted by the business world at an increasing rate. To achieve a competitive advantage, enterprises need to integrate the latest mobility, data analytics, cloud and Internet of Things (IoT) digital innovations into their operations, processes and computing systems.

The latest evolutions in mobility, IoT and data analytics are directly impacting network infrastructures and driving enterprises to reconsider their network technology choices. Legacy infrastructures are often unable to securely and efficiently support new use cases and business scenarios based on cloud native applications and the massive number of IoT devices in use. Adoption of applications and IoT-based digital processes is happening at an unprecedented scale and speed. Manual and static network configurations can no longer address the demand to make configuration changes to keep the network secure and performing at high efficiency.

The inherent problem in handling these new IoT devices is that they can be vulnerable; may not support certificates or just not be configured to use them; and they can become attack vectors. Network managers are faced with addressing these problems: Do they block the devices and become the 'bad guys' leading to in-fighting in the organization; or do they enable the IoT devices as securely as possible with fingerprinting and containers? This paper will discuss the latter in the context of using the Alcatel-Lucent OmniVista® 2500 Network Management System (NMS) device fingerprinting/profiling application tools as an enabler to the containment solution.

These device fingerprinting and profiling features fall under the Service Defined Network architecture and help administrators automatically provision network services to securely handle the wired or wireless IoT device proliferation in today's networks.

Augmented intelligence: With OmniVista NMS device fingerprinting and profiling verified using a cloud-based database

OmniVista NMS has easy to follow configuration workflows to help simplify the IoT device on-boarding. This helps to provide secure access into the LAN and Wi-Fi network for all types of categorized IP-enabled devices. OmniVista NMS embedded application tools leverage the device classification using a cloud-based device profiling/fingerprinting populated inventory list. This functionality works with the Unified Access (UA) architecture umbrella to enable Access Guardian-based policies that are part of the Universal Network Profiles (UNPs). A UNP profile defines network access or in this case, it's manually or dynamically enabled through the enforcement of the Access Role Profile for the categorized devices.

As mentioned above, the inventory list is populated through communication with an external cloud-based database used for device profiling. Once it is populated, enforcement of the Access Role Profile can be used to implement the organization's network micro-segmentation strategy to provision a new VLAN or a set of ACLs to help keep the network secure within the organization's defined network containers. The creation of custom categories that need to be enforced, such as Access Role Profiles, are discussed later in this paper.

This new feature set helps network administrators use OmniVista NMS to address the access issues associated with unplanned/unapproved IoT devices being connected to the network. Once an IoT device is profiled (added to the inventory list) via the IoT Inventory application and authenticated (using the Unified Access policies), enforcement policies can be applied to the physical infrastructure to make sure each device connected to the network receives the right UNP (for example, quality of service (QoS) and bandwidth and security policies) to securely assign those devices to the organization's defined network containers.

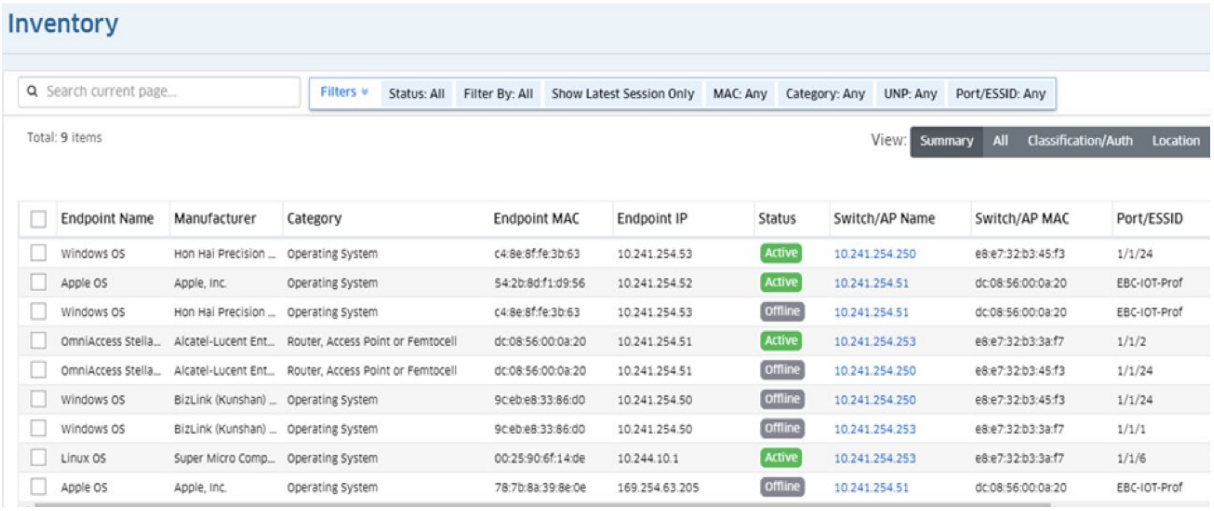
The network leverages OmniVista NMS user, device, and application profiling capabilities to automatically create and assign UNPs to each IoT and/or a group of IoT devices. The enforcement capabilities of this feature are supported starting with OmniVista NMS release 4.5R01 through the Unified Access and IoT Inventory applications; AOS 8.7.x in the Alcatel-Lucent OmniSwitch® family of multi-layer switches; and release 3.0.7 or later in the Alcatel-Lucent OmniAccess® Stellar Wireless Access Points. Together they enable automatic network micro-segmentation to build secure and controlled network containers. Refer to the "Dynamic UNP Enforcement: How is category-based device UNP enforcement possible?" section below for more details on the IoT inventory list and enforcement of UNPs using the Access Role Profile workflow tool.

Another benefit to on-boarding and keeping IoT devices in controlled containers is for security purposes; when the device is in a container you can try to enable certificate-based authentication or device-specific PSK. It is also important to educate device owners to keep them security-patched with strong passwords while setting guidelines for software updates of existing devices or for future devices that will show up in the network.

Inventory summary list and field definition

The new device profiling and fingerprinting feature builds an inventory list (see Figure 1) of devices profiled by an external cloud-based database of industry recognized device signatures. That information can be leveraged to provision UNPs that can be enforced at the access layer to further protect an OmniSwitch and Stellar wireless network.

Figure 1. Inventory list



In Figure 1, the inventory Summary provides an administrator with useful information that can be used to provision UNPs. For example, the Summary view displays the following:

- **Endpoint MAC**: The device MAC Address
- **Endpoint IP**: The device IP Address
- **Status**: The operational status of the device on the network
  - ***Active***: The device was active on the network when it was last known by the OmniVista NMS. Note that if a switch/Access Point (AP) is deleted from the OmniVista NMS or IoT is disabled on a switch/AP, the OmniVista NMS will indicate Offline for all devices connected to that switch/AP regardless of the device's actual status. This is because the OmniVista NMS does not receive updates regarding these devices in these scenarios. If a switch/AP goes down, the OmniVista NMS will not automatically change the status of the devices connected to it.
  - ***Offline***: The device is not currently active on the network; the switch/AP to which the device is connected was deleted from the OmniVista NMS, or IoT was disabled on the switch/AP to which the device is connected
  - ***Error***: The device was unable to connect to the network (for example, MAC authentication fails)

- **Category**: The device category, such as Data Center appliance, phone/tablet/wearable device. Note that the initial category value is not likely to be very specific. As more activity happens on the endpoint device, switches/APs send additional details about the endpoint, and the category description will be more specific. Also, note that for some devices this field may be empty. This generally happens when insufficient fingerprint information about the device is available (for example, switch/AP receives only the MAC address of the endpoint and the MAC is unknown or unpopular).
- **Manufacturer**: The device manufacturer
- **Endpoint name**: The name of the endpoint device as determined by the Device Fingerprinting Service
- **Endpoint version**: The endpoint device OS version
- **Category hierarchy**: The category, manufacturer, and endpoint name used to categorize the device
- **Switch/AP name**: The IP address of the switch/AP through which the device is connected to the network
- **Switch/AP MAC**: The MAC address of the switch/AP through which the device is connected to the network
- **Port/ESSID**: The switch port or ESSID through which the device is connected to the network
- **Port type**: The port type through which the device is connected to the network (wireless/wired/UNP)
- **Port description**: A description of the port through which the device is connected to the network, as received from the device
- **VLAN**: The VLAN through which the device is connected to the network
  - ***AOS devices***: The untagged VLAN, or the tagged VLAN if traffic is tagged
  - ***Stellar APs***: The VLAN mapped to the AR Profile
- **Far end IP**: The IP address of the far end tunnel termination (displayed for wireless clients only)
- **VPN ID**: The tunnel ID that identifies a GRE tunnel VPN (displayed for wireless clients only)
- **UNP**: The AR profile assigned to the device, if applicable
- **UNP type**: The UNP type, if applicable
- **Policy list**: The policy list applied to the device, if applicable
- **Authentication type**: The type of authentication used for the device (for example, MAC, 802.1X)
- **Authentication status**: The status of device authentication, if applicable (for example, pass, fail). Following is a sample screen shot with information for the configuration referenced throughout this document. Note the Authentication Type as 802.1x with a status of Passed for the wireless devices that joined the ESSID EBC-IOT-Prof and the UNP type coming from RADIUS.

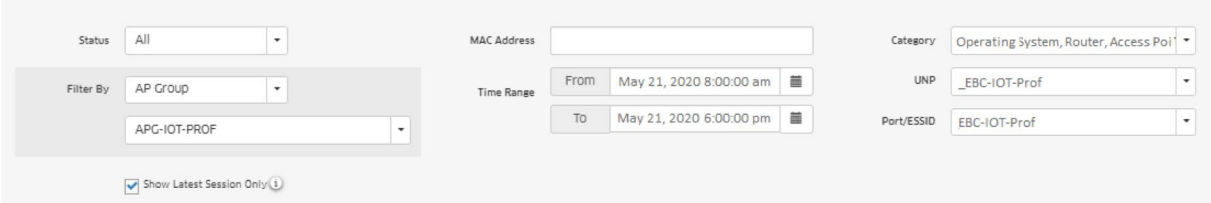
Endpoint MAC	Endpoint IP	Category	Manufacturer	Switch/AP Name	Switch/AP MAC	Port/ESSID	VLAN	UNP	UNP Type	Policy List	Authentication Type	Authentication Status
00:25:90:6f:14:de	10.244.10.1	Operating System	Super Micro Comp...	10.241.254.253	e8:e7:32:b3:3a:f7	1/1/6	244					
54:2b:8d:f1:d9:56	10.241.254.52	Operating System	Apple, Inc.	10.241.254.51	dc:08:56:00:0a:20	EBC-IOT-Prof	0	_EBC-IOT-Prof	UNP from RADIUS	PL-Access	802.1X	Passed
78:7b:8a:39:8e:0e	169.254.63.205	Operating System	Apple, Inc.	10.241.254.51	dc:08:56:00:0a:20	EBC-IOT-Prof	2	defaultWLANPr...	UNP from RADIUS		802.1X	Passed
9c:eb:e8:33:86:d0	10.241.254.50	Operating System	BizLink (Kunshan) ...	10.241.254.250	e8:e7:32:b3:45:f3	1/1/24	241					
9c:eb:e8:33:86:d0	10.241.254.50	Operating System	BizLink (Kunshan) ...	10.241.254.253	e8:e7:32:b3:3a:f7	1/1/1	241					
c4:8e:8f:fe:3b:63	10.241.254.53	Operating System	Hon Hai Precision ...	10.241.254.250	e8:e7:32:b3:45:f3	1/1/24	241					
c4:8e:8f:fe:3b:63	10.241.254.53	Operating System	Hon Hai Precision ...	10.241.254.51	dc:08:56:00:0a:20	EBC-IOT-Prof	0	_EBC-IOT-Prof	UNP from RADIUS	PL-Access	802.1X	Passed

- **Connection error**: The connection error if the device was unable to connect to the network, if applicable
- **Start time**: The time the device first accessed the network
- **End time**: The time the device disconnected from the network
- **Last updated**: The last time the OmniVista NMS received a message from the device and the message was successfully processed

Applying filters to the inventory list

Filters can be applied to the inventory list to make the information more relevant for reporting and administration purposes. For instance, if a university's network administrator wants to view a real-time list of active wireless devices that are attached to SSID EBC-IOT-Prof during the daytime class sessions on May 21st, the administrator would create the following filter.

Figure 2. Inventory list filters



Following is a sample capture of Active and Offline device information to illustrate what's active or offline based on the communication with the OmniVista NMS service for that device.

Figure 3. Fingerprinted device status list

Endpoint Name	Manufacturer	Category	Endpoint MAC	Endpoint IP	Status	Switch/AP Name	Switch/AP MAC	Port/ESSID
Apple OS	Apple, Inc.	Operating System	54:2b:8d:f1:d9:56	10.241.254.52	Active	10.241.254.253	e8:e7:32:b3:3a:f7	1/1/2
Apple OS	Apple, Inc.	Operating System	54:2b:8d:f1:d9:56	10.241.254.52	Active	10.241.254.250	e8:e7:32:b3:45:f3	1/1/24
Apple OS	Apple, Inc.	Operating System	54:2b:8d:f1:d9:56	10.241.254.52	Active	10.241.254.51	dc:08:56:00:0a:20	EBC-IOT-Prof
Apple OS	Apple, Inc.	Operating System	78:7b:8a:39:8e:0e	10.241.254.54	Offline	10.241.254.253	e8:e7:32:b3:3a:f7	1/1/2
Apple OS	Apple, Inc.	Operating System	78:7b:8a:39:8e:0e	10.241.254.54	Offline	10.241.254.250	e8:e7:32:b3:45:f3	1/1/24
Apple OS	Apple, Inc.	Operating System	78:7b:8a:39:8e:0e	10.241.254.54	Offline	10.241.254.51	dc:08:56:00:0a:20	EBC-IOT-Prof
OmniAccess Stella...	Alcatel-Lucent Ent...	Router, Access Point or Femtocell	dc:08:56:00:0a:20	10.241.254.51	Active	10.241.254.253	e8:e7:32:b3:3a:f7	1/1/2

There are many applications for the device fingerprinting feature depending on the enterprise vertical industry where this functionality is deployed; for instance, the example of the inventory filter illustrated in Figure 2 is for a higher education network application. In this scenario, the feature can be applied to wireless IoT devices that students bring into the university. Once those devices are profiled (fingerprinted) they can be dynamically assigned to specific network profiles which will dictate their network access, type of security, and bandwidth parameters. In a video streaming and gaming scenario, if the university wishes to keep their network bandwidth available for educational purposes during prime class session hours, the network administrators can provision UNPs for both wired and wireless through the OmniVista NMS to restrict devices (or simply limit the bandwidth of those devices) on the university's wireless network during class sessions. The first phase of this feature set provided device listing as per the sample table shown above. Through the release of phase two, dynamic enforcement capabilities are possible with the OmniVista NMS for provisioning and enforcement to automatically enable UNPs for the network micro-segmentation that makes business sense for your organization.

Dynamic UNP enforcement: How is category-based device UNP enforcement authentication possible?

The OmniVista NMS monitors network packets to determine the types of devices connected to the network and interfaces with the cloud-based device fingerprinting service to categorize them. The IoT enforcement feature enables the associating category with an Access Role Profile (AR Profile). Once a device accesses the network and is categorized, the assigned AR Profile is applied to the device. The network administrator can associate different Profiles with different categories, either manually or dynamically.

This IoT enforcement feature enables you to associate devices by relating them to a category with an AR Profile. Once a device accesses the network and is categorized, the assigned AR Profile is applied to the device. This functionality provides the capability to associate different Profiles with different categories; and you can enable them automatically or manually via the enforcement policies. You can also specify 'exceptions' for specific devices by SSID, MAC address, AP group, or IP address. When a device matching one of these exceptions is categorized it will not be subject to IoT enforcement that is configured for its category.

Creating a device fingerprinting category

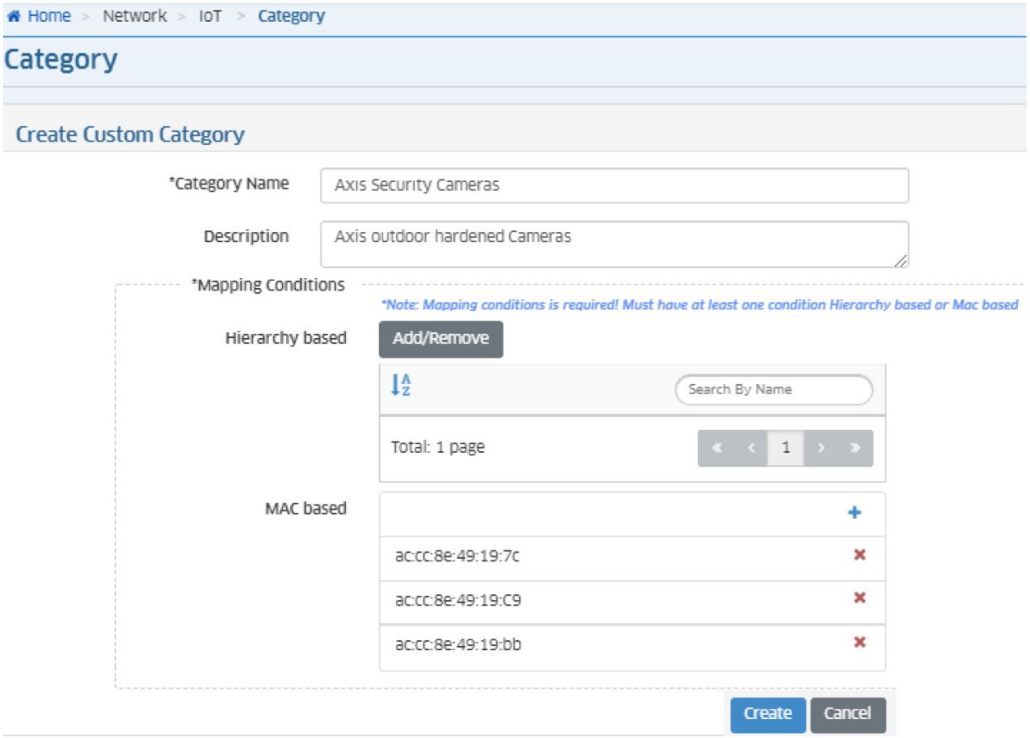
There are 24 system-defined AR profiling categories in the second phase release. An administrator can create new custom categories through the OmniVista NMS under the add (+) icon at the top of the category list. The create custom window provides the following fields to be completed when creating a custom category:

- **Category name**: A name for the custom category
- **Description**: An optional description for the category
- **Mapping conditions**: You can create a custom category based on an existing category (hierarchy-based) or create a custom category based on MAC address (MAC based)
  - ***Hierarchy-based***: Click on the Add/Remove button to access a list of categories. Only those category hierarchies that have been detected and displayed on the inventory screen are displayed for selection. Add/Remove categories to create the custom category.
  - ***MAC-based***: Enter a MAC address and click on the add (+) icon. Repeat to add additional MAC addresses. Click on the delete (x) icon to remove a MAC address from the custom category

Note: The new custom category will appear at the bottom of the category list. The custom category will be displayed for any online devices in the inventory list matching the new category.

Figure 4 is a new security camera category configuration example for enforcing UNPs as Axis cameras are connected to the wired or wireless network.

Figure 4. Creating a custom category



Assigning an Access Role Profile to a category

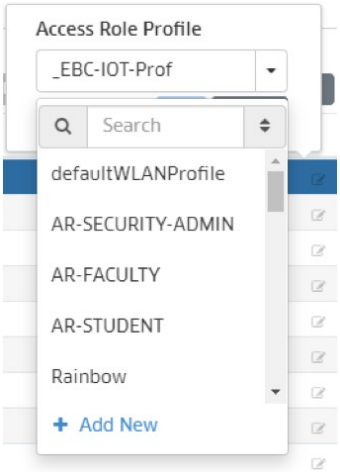
Click on the Edit (✎) icon to the right of the AR Profile column to access the AR Profile drop-down menu. Click on the drop-down menu to access a list of all configured AR Profiles; select a profile and click OK. The assigned AR Profile will be displayed in the AR Profile column next to the category.

You can also click on '+ Add New' to go to the AR Profile screen and create a new profile. Once the profile is created, return to the IoT enforcement screen and select the new profile.

Important note: The AR Profile must exist on the switches/APs connected to the endpoint devices. If you are creating a new AR Profile, you must first assign the profile to any applicable switch(es)/AP Group(s) before assigning it to a Category in the IoT application. See the AR Profile online help for more information on creating and assigning AR Profiles.

The above custom category example definition for the security camera was defined with the MAC addresses for the Axis cameras. This category can be used to enforce 'accept' or 'drop all' ACL actions for the AR Profile referenced in Figure 5. In this scenario, if the user signs in with the AR-SECURITY-ADMIN credentials to SSID UNI-NET, they will join VLAN 201 and have access to view the security camera live streaming. However, if the user signs in with the AR-STUDENT credentials to the same SSID, they will join VLAN 202 with the UNP having no access to the security camera video feed. An ACL is enforced where all traffic is dropped from any device in VLAN 202 with destination of the security camera's UNP.

Figure 5. Assigning an Access Role Profile to a category



Conclusion

To achieve a competitive advantage, enterprises need to integrate the latest mobility, data analytics, cloud and IoT digital innovations into their operations, processes and computing systems. Alcatel-Lucent Enterprise can help enable those new services through an OmniVista NMS managed OmniSwitch and Stellar wireless network. The ALE Service Defined Network architecture is further enhanced through the OmniVista NMS with device fingerprinting, classification and enforcement to help simplify IT tasks. The micro-segmentation of the network to on-board IoT devices and to keep them in their dedicated containers helps minimize security risks and this is made possible with the OmniVista NMS managing an end-to-end OmniSwitch and Stellar wireless network.

OmniVista NMS IoT device on-boarding capabilities provide an excellent solution to the IoT device proliferation problem in today's networks. The OmniVista NMS device fingerprinting/profiling application tool is an enabler to help create containers for those unsolicited, unplanned, headless IoT devices to ensure secure network access through the definition and automatic application of UNPs. With this solution all stakeholders must cooperate in keeping the IoT devices software security-patched, and use strong passwords to help maintain a clean, mobile, and secure network infrastructure.

Alcatel·Lucent Enterprise