OmniVista UPAM and Palo Alto Networks User-ID Integration Guide

Application Note
OmniVista UPAM and Palo Alto Networks User-ID Integration Guide

Alcatel·Lucent Enterprise

Table of Contents

1. About this Integration Guide

The purpose of this integration guide is to help ALE Business Partners and customers integrate Alcatel-Lucent OmniVista® Unified Policy Authentication Management (UPAM) with Palo Alto Networks' (PAN) next-generation firewall's User-ID feature. Through this integration, users or devices authenticated to the LAN and/or WLAN networks can also be simultaneously and seamlessly authenticated to the PAN firewall. OmniVista UPAM can share user or device connection status as well as identity or role information with the firewall for enhanced visibility, finer policy control and improved logging, reporting and forensic analysis.

2. The Zero-Trust Paradigm

In a legacy firewall, the "trust" boundary is based on the point of connection: "Inside" users are implicitly trusted and "outside" users are not. In an airport analogy, this would be equivalent to allowing land-side passengers to go through security unchecked. With trends such as mobility and Internet of Things (IoT), that notion of "trust" is completely outdated. Some examples: A BYOD device may bring malware into the organization; an IoT device may be intrinsically vulnerable and become an attack vector; and even corporate users could be malicious.

The paradigm today is "Zero Trust". No matter where the user or device is connected, *never* trust and *always* verify. Establishing identity is at the core of the Zero-Trust Paradigm. Going back to the airport analogy, the first thing an immigration officer will do is check the passport. Other checks such as a visa check, database checks and so on, are done after identity is established with a passport, a matching fingerprint, etc. And since establishing identity is such a fundamental check at the core of the Zero-Trust Paradigm, next-generation firewalls have multiple mechanisms of determining identity.

3. About Palo Alto Networks User-ID

User-ID is a standard feature on Palo Alto Networks (PAN) firewalls that enables the firewall to identify users by leveraging various information repositories and techniques. Knowing users' identities and/or roles, rather than just their IP address, brings several benefits including: Improved visibility into usage patterns, finer policy control by only allowing application and/or resource access to those users/roles with a legitimate need for it (principle of least privilege) and enhanced logging, reporting and forensics by referencing user identity or role rather than just an IP address. Please refer to Palo Alto Networks documentation for further information on the User-ID feature.

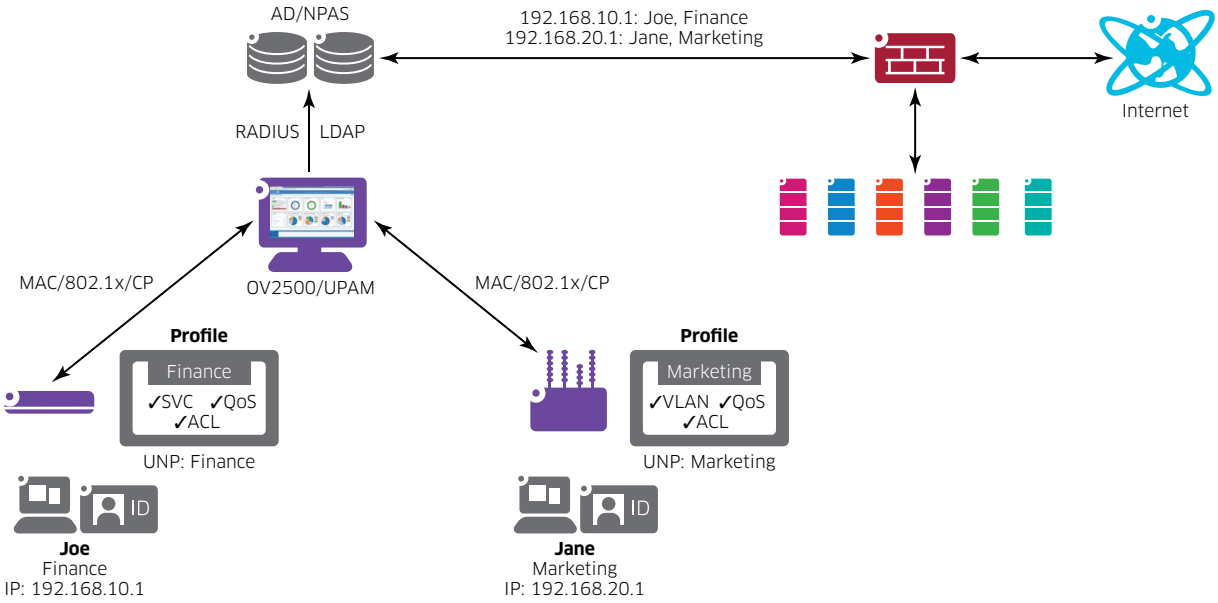
4. About Alcatel-Lucent OmniVista UPAM

OmniVista's Unified Policy Authentication Management module is a unified access management platform for both Alcatel-Lucent OmniSwitch® Ethernet switches and Alcatel-Lucent OmniAccess® Stellar access points. UPAM includes both a captive portal and a RADIUS server and can implement multiple authentication methods such as MAC authentication, 802.1x authentication and captive portal authentication. Users can authenticate against UPAM's local database or against external databases including Microsoft Active Directory, LDAP and external RADIUS. UPAM's customizable captive portal can implement flexible authentication strategies for guest and BYOD users with integrated credential management through email, SMS and social login (Facebook, Google, WeChat and Rainbow).

5. Use case

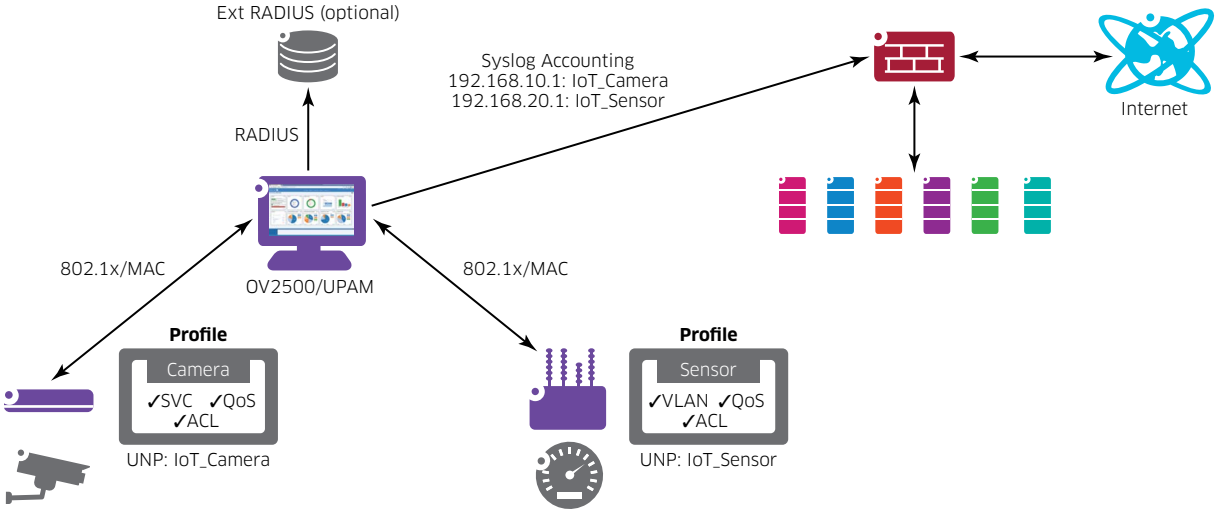
There are two main use cases when it comes to wired and wireless users: Corporate (AD) devices and BYOD or IoT devices. For corporate devices, such as a corporate user on a corporate laptop, OmniVista UPAM can proxy authentication to AD and the preferred point of integration is directly on AD, not on UPAM. This guide will not elaborate on this use case. Please refer to Palo Alto Networks documentation for further details on the AD-based integration.

Figure 1. AD-based integration



In this guide, we focus on the other use case in which a BYOD or IoT device is authenticated directly against the UPAM database or proxied to an external RADIUS database (other than Microsoft's Network Policy and Access Services or NPAS) because these devices may not be associated with an AD account. This use case is shown in the figure below with IoT as an example. This document focuses on this use case because the point of integration is directly on OmniVista UPAM.

Figure 2. Syslog-based integration



6. Mechanism

Once onboarded, wired or wireless devices authenticate against the UPAM RADIUS through MAC or 802.1x authentication. UPAM logs authentication and accounting events to the PAN built-in syslog receiver. A parse filter is defined on the PAN firewall to extract the role or username from these messages. Please refer to the snippet below for some sample syslog messages generated by UPAM.

Figure 3. Sample UPAM syslog logging

<14>Mar 30 18:26:27 localhost
{"APMAC":"E8E732A48A23","acctSessionId":"E8E732A48A230003E6A6FB74","authType":"MAC",
"changeType":"Access","deviceIP":"","deviceMac":"0003E6A6FB74","filterId":
"IOT_STB","time":"2020-03-30 18:26:27","username":"0003E6A6FB74"}

<14>Mar 30 18:26:27 localhost
{"APMAC":"E8E732A48A23","acctSessionId":"192.168.114.22_03/30/2020
18:26:27_0003e6a6fb74","authType":"MAC","changeType":"Accounting","deviceIP":
"10.211.5.51","deviceMac":"0003E6A6FB74","filterId":"IOT_STB","time":"2020-03-30
18:26:27","username":"0003E6A6FB74"}

<14>Mar 30 18:26:13 localhost
{"APMAC":"E8E732A48A23","acctSessionId":"192.168.114.22_03/30/2020
18:19:10_0003e6a6fb74","authType":"MAC","changeType":"Disconnect","deviceIP":
"10.211.5.51","deviceMac":"0003E6A6FB74","filterId":"IOT_STB","time":"2020-03-30
18:26:12","username":"0003E6A6FB74"}

Let's examine some of the relevant fields in these messages:

APMAC: The RADIUS NAS (the switch or access point) MAC address.

authType: This field specifies the authentication mechanism (for example, MAC or 802.1x).

changeType: This can be "Access", which indicates successful authentication, "Accounting", for periodic RADIUS accounting messages or "Disconnect" for logout/disconnect events.

deviceIP: This is the end device's IP address.

filterID: The filterID represents the uNP (User Network Profile) or ARP (Access Role Profile) or in other words, the role assigned to the device.

username: As the name suggests, this is the username. When using MAC authentication, the username is simply the end device's MAC address.

We want to bring attention to the following aspects:

- The device's IP address, which the firewall needs for policy enforcement, is contained in "Accounting" and "Disconnect" messages, but usually not in "Access" messages. This is because obtaining an IP address through DHCP can take some time and can only occur after authentication.
- Therefore, RADIUS interim accounting needs to be enabled in addition to authentication.
- Only a single syslog parsing profile can be applied to any given syslog source on the firewall. We will create a filter for "Accounting" messages as this is the message type containing all the necessary information: deviceIP, username and/or filterID. We will not be able to configure a filter for "Disconnect" messages. As a result, users will not be immediately logged out from the firewall when they disconnect. Users will be logged out if no "Accounting" updates are received before expiration of the User Identification Timeout, which is 45 minutes by default.
- For this reason, the RADIUS interim accounting interval should be set lower than the User Identification Timeout.

7. Procedure overview

Here's a summary of the different steps required on both OmniVista/UPAM and the PAN firewall.

OmniVista UPAM

1. Configuring AAA profile for 802.1x/MAC authentication AND accounting against UPAM
2. Configuring UPAM Access Policy and Authentication Strategy
3. Configuring UPAM for external syslog logging to PAN firewall
4. Creating Access Auth profile for MAC/802.1x authentication against UPAM

PAN firewall

1. Enabling User-ID on required FW zones
2. Enabling UDP syslog listener on interface's management profile
3. Creating syslog parse profile for UPAM logs
4. Configuring syslog server monitoring
5. Enabling User-ID firewall policies
6. Verifying User-ID mappings
7. Verifying User-ID policies

8. OmniVista: Configuring the AAA profile

On OmniVista, go to Unified Access->Template->AAA Server Profile and click "+".

Create a new AAA server profile pointing to the UPAMRadiusServer for both authentication and accounting. You will do this for the required authentication methods: 802.1x, MAC or Captive Portal. In the example below, only 802.1x and MAC are shown as IoT devices do not normally use Captive Portal authentication.

Figure 4. AAA Server Profile - Authentication

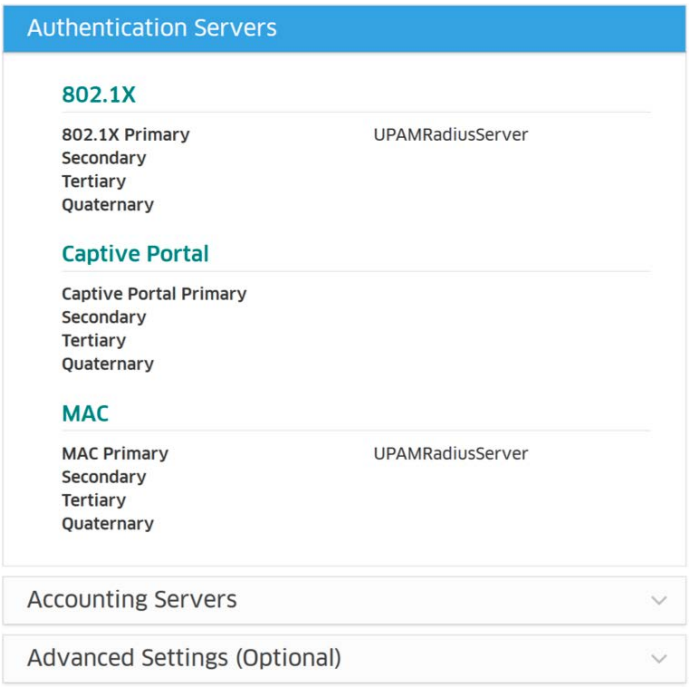
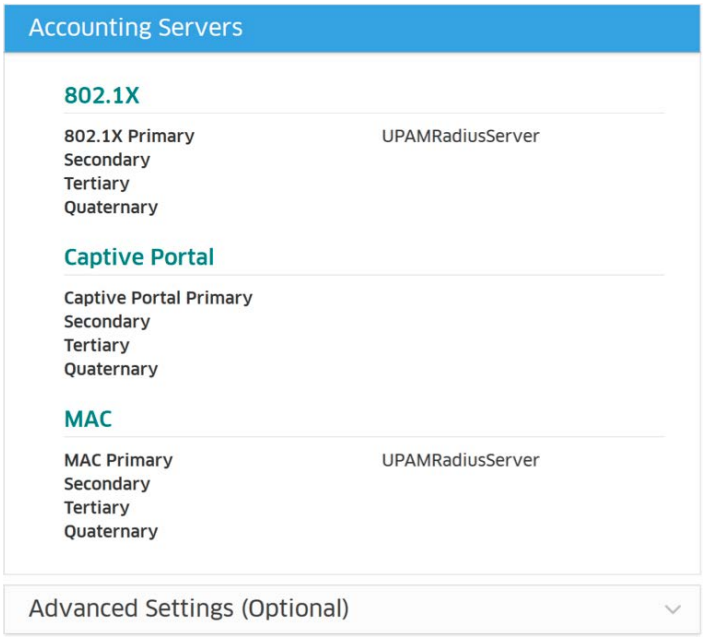


Figure 5. AAA Server Profile - Accounting



You may also specify the Accounting Interim Interval (600 seconds by default) or, alternatively, trust the accounting interim interval set by the RADIUS server (UPAM or external) in which case, the accounting interim interval must be configured on the RADIUS server. In most cases, the first accounting message sent shortly after successful authentication will contain the device's IP address and allow the firewall to identify the user. In other cases, however, the device's IP address will only be present in the second and later accounting messages. In such case, setting a lower interim interval will result in this information being updated quicker on the firewall.

Regardless of whether the accounting interim interval is trusted from the RADIUS server or set on the AAA Server Profile, it must be lower than the User Authentication Timeout set on the firewall, which is 45 minutes by default. The 600 second default setting meets this requirement.

Figure 6. MAC - Accounting Interim Interval