Pulse Policy Secure

MAC Address Authentication with Profiler

Configuration Guide
MAC Address Authentication with Profiler Configuration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Palo Alto Networks, the Palo Alto Networks Logo, Palo Alto Networks Firewall, PAN-OS, User-ID, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. For additional information on Palo Alto Networks products, visit www.paloaltonetworks.com
Introduction

Devices that have a native 802.1x supplicant or Pulse Client can authenticate themselves using the appropriate credentials (username/password, certificate, token-based, etc) and access the network.

However, devices such as VoIP phones, printers, IP cameras often do not have a supplicant or Pulse client. VoIP phones which support 802.1x can be configured to use 802.1x based authentication.

To allow such devices on the network, the PPS admin can configure MAC Address Authentication server using RADIUS and profile them using Profiler to ensure that only devices of a certain “profile” can access the network.

This document explains how to configure a typical host, such as a VoIP phone, that is not 802.1x enabled to be permitted on the network using MAC address authentication and the native Profiler.

Figure 1: Overview
Pulse Policy Secure Configuration

The goal is to configure the following to permit the VoIP phone to access the LAN network:

- Create a role for hosts that don't have a 802.1x supplicant. For example, VoIP Phones.
- Create MAC Address Authentication Server and MAC Address Authentication Realm.
- Create Local Profiler Authorization Server and assign it to a MAC Address Authentication Realm.
- In the MAC Address Authentication Realm, create role mapping rules to assign roles to devices based on their device "profile".
- Create a location group and map the location group to MAC Address Authentication Realm.
- Configure a RADIUS client.
- Create RADIUS return attributes for final VLAN assignment and assign it to Roles.

*Note:* This use case configuration applies to profiled devices using either DHCP, or SNMP/NMAP mechanisms. For more information, see [Profiler Deployment Guide](#).

**Pre-Requisite**

You must ensure that the Switch port is configured to allow MAC Address Authentication. See PPS Admin Guide for sample configurations.

**Procedure**

1. Create a new user role, select **Users > User Roles > New User Role**. Enter a name. For example, VoIP Phones.

*Figure 2: User Role*
Uncheck **Install Agent for this Role**. Do not configure any role restrictions.

*Figure 3: User Role - Agent*

2. Create a new MAC address Authentication server, select **Authentication > Auth.Servers > MAC Address Authentication**. Click **New Server**. To allow all MAC addresses, configure * as a wild character and assign the device attribute of “deviceName=unknown” as shown in the below screenshot.

*Figure 4: MAC Authentication Server*

3. Create a new Local Profiler authorization server.
   
a. Select **Authentication > Auth.Servers**. Select **Local Profiler** from the server type drop-
down list and click **New Server**.

*Figure 5: Local Profiler*

![Figure 5: Local Profiler](image)

b. Click **Browse** and upload the device fingerprints package.

*Figure 6: Uploading Device Fingerprints Package*

![Figure 6: Uploading Device Fingerprints Package](image)

c. Configure SNMP Poll interval and DHCP sniffing mode interface.

*Figure 7: SNMP Poll Interval*

![Figure 7: SNMP Poll Interval](image)
d. For Profiling devices using SNMP, you can configure the switch under **Endpoint Policy > Network Access > SNMP Device Configuration.**

![Figure 8: SNMP Device Configuration](image)

Figure 8: SNMP Device Configuration

e. (Optional) Add one or more subnets that can be included or excluded for fingerprinting unmanaged devices using Nmap target scans. Note that an Nmap target scan is only performed on valid IP addresses in the subnet.

![Figure 9: Adding One or More Subnets](image)

Figure 9: Adding One or More Subnets
4. Create a new MAC Address Authentication realm and assign it to MAC Address Authentication and profiler server, select Endpoint Policy > MAC Address Realms > MAC Authentication Realm.

*Figure 10: MAC Address Authentication Realm*
5. Set Role Mapping rules. Select Rule based on Device attribute and click **Update**. Enter the rule name and under Rule, select **Category** as Attribute and values as “VoIP Phone/Adapters” and then assign all devices of category to the role called “VoIP Phone” as shown below.

Select Stop processing rules when the rule matches and click **Save Changes**.

*Figure 11: Role Mapping Rule 1*

6. Similarly Create another rule, to assign other unknown devices to “Unknown_Device” Role. Select Rule based on User attribute and click **Update**. Enter the rule name and under Rule, click **Attributes** to add the custom attribute as shown in the screenshot. Provide a custom attribute name, which matches with the attribute name configured previously in the Mac Auth Server by clicking **Add Attribute** and then click **OK**.

*Figure 12: Role Mapping Rule 2*
Select Attribute as **deviceName** from the list and value as “Unknown” and then assign all devices of category to the role called “Unknown_Device” as shown below. Select **Stop processing rules when the rule matches** and click **Save Changes**.

![Role Mapping Rule](image)

Once the role mapping roles are configured the following screen is displayed.

**Figure 13: Completed Role Mapping Rules**

![Completed Role Mapping Rules](image)

7. Configure the RADIUS client (Add the switch in the PPS admin UI).
   a. Create a location group. Select **Endpoint Policy > Network Access > Location Group** (and assign the **default** Signing In policy and MAC Address Authentication Realm).

**Figure 14: Location Group**
b. Create new RADIUS client. Select **Endpoint Policy > Network Access > RADIUS Client**. Enable **Support Disconnect Messages**.

**Note:** RADIUS Disconnect is used for session termination.

Change of Authorization (CoA) is used to change the ACLs and several other attributes for the endpoint instantly based on roles without the need of re-authentication through Switch/WLC.

**Figure 15: RADIUS client**

For example, define a “VoIP Phones” policy for moving endpoint to the appropriate VLAN.

*Figure 16: RADIUS return Attributes*
Conclusion

You should now be able to properly authenticate devices based on their profile even if they do not have a 802.1x supplicant. For example, in the above scenario, all VoIP phones will automatically be assigned to the appropriate VLAN when they attempt to access the network.

You can view the high-level device statistics from the Device dashboard page at System > Status > Device Profiles.

Figure 17: Device Profiles

You can view the device reports at System > Reports > Device Discovery.

Figure 18: Device Discovery Report
You can verify the active users table to view the session details of the user.

**Figure 19: Active Users**

![Active Users Table](image)

For troubleshooting you can verify the user access logs.

**Figure 20: User Access Logs**

![User Access Logs](image)