



Pulse Policy Secure

MAC Address Authentication with Profiler

Configuration Guide

Document

2.0

Published

December 2018



Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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

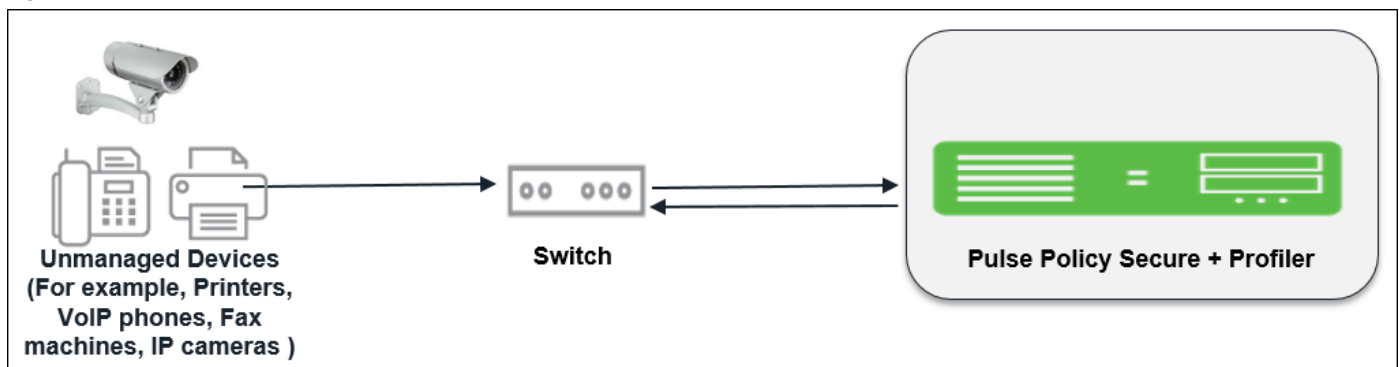
Devices that have a native 802.1x supplicant or Pulse Client can authenticate themselves using the appropriate credentials (username/password, certificate, token-based, etc) and access the network.

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

Pulse Secure System Authentication Administrators **Users** Endpoint Policy Maintenance Wizards

User Roles > New Role

New Role

Name: VoIP Phones

Description:

▼ Options

Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.

- ☒ Session Options
- ☒ UI Options
- ☐ Odyssey Settings for Access
- ☐ Odyssey Settings for Preconfigured Installer
- ☐ Enable Guest User Account Management Rights

Save Changes

Uncheck **Install Agent for this Role**. Do not configure any role restrictions.

Figure 3: User Role- Agent

Pulse Secure System Authentication Administrators **Users** Endpoint Policy Maintenance Wizards

User Roles > VoIP Phones > Agent > General

General Agent Agentless

General Pulse Secure Client Settings

Options

☐ Install Agent for this role

☐ Enable Host Enforcer

Note: (Odyssey Access Client only) By default, if you enable Host Enforcer on a role, all traffic is blocked for users mapped to this role. Make sure you create Host Enforcer policies on the "Resource Policies-Host Enforcer" page to allow particular traffic for this role.

Host Enforcer policies that apply to this role:

- Access control

Session scripts

Windows: Session start script
This script is executed after the session has started.
Script Location:

Windows: Session end script
This script is executed after the session has ended.
Script Location:

Save Changes

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

Pulse Secure System **Authentication** Administrators Users Endpoint Policy Maintenance Wizards

Settings Users

Name: Label to reference this authentication.

MAC Addresses

Maximum 500 addresses

Delete **Up** **Down**

MAC Address	Action	Attributes	
<input type="text"/>	Allow	<input type="text"/>	Add
*****	Allow	deviceName=Unknown	

Optional LDAP Servers

Available LDAP Servers: (none) **Add ->** **Remove**

Selected LDAP Servers: LDAP_Authz_Server **Up** **Down**

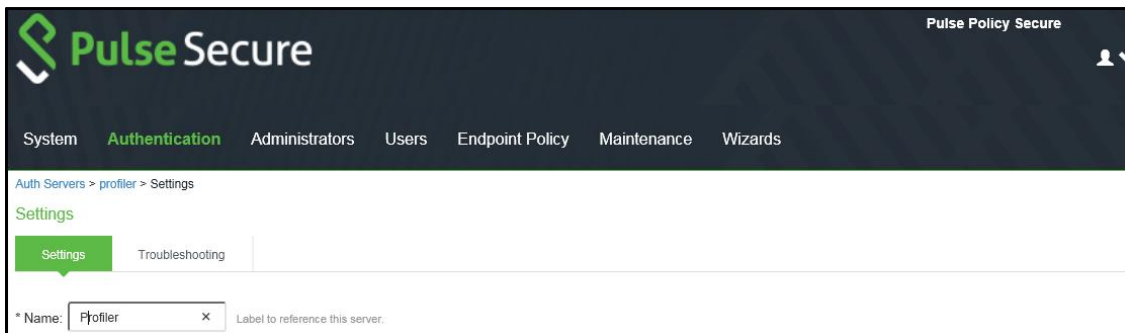
Example MAC Address:
00:11:85:bb:8c06
00:ff:****

Example Attribute:
attribute1=value1;attribute2=value2;
(for attribute: alphanumeric or '_' or '-' characters only)
The Allow & Attributes action accepts the defined MAC Address expression and looks it up in the optional LDAP Server(s) below for authorization attributes.

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



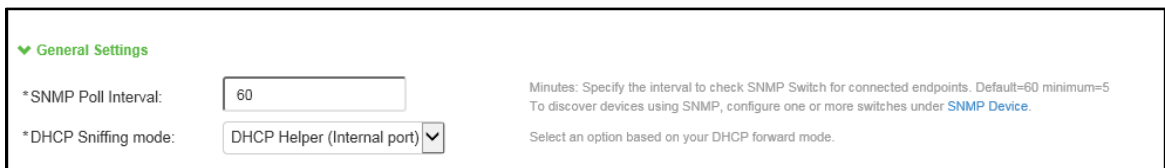
b. Click **Browse** and upload the device fingerprints package.

Figure 6: Uploading Device Fingerprints Package



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

Figure 7: SNMP Poll Interval



- d. For Profiling devices using SNMP, you can configure the switch under **Endpoint Policy > Network Access > SNMP Device Configuration**.

Figure 8: SNMP Device Configuration

The screenshot shows the Pulse Secure web interface. The top navigation bar includes links for System, Authentication, Administrators, Users, Endpoint Policy (highlighted), Maintenance, and Wizards. The breadcrumb trail is Network Access > SNMP Device Configuration > JuniperSW. The main form is titled JuniperSW and contains the following fields:

- *SNMP Version: Radio buttons for v1/v2c (selected) and v3.
- *Name: Text input field containing JuniperSW. A tooltip indicates: Label to reference this SNMP Device.
- Description: Text input field.
- *IP Address: Text input field containing 10.10.10.10. A tooltip indicates: IP Address of this SNMP Device.
- *Vendor: Dropdown menu showing JUNIPER. A tooltip indicates: Device Vendor.
- SNMP Settings (expanded):
 - Same credentials for Trap user: Checked checkbox.
 - *Read Community String: Text input field containing public.
- Save Changes button.

- 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

The screenshot shows the Pulse Secure web interface for configuring endpoints to scan using NMAP/WMI. The page title is Endpoints to scan using NMAP/WMI. Below the title, there is a description: "Once devices are discovered using DHCP, SNMP or other mechanisms, more granular profiling is done only for those devices using NMAP or WMI active scan. Use the following subnet configuration to either allow, or disallow, such scans. Maximum 100 subnets." Below this description are three buttons: Delete, Up arrow, and Down arrow. The main configuration area is a table with the following columns: Subnet, Include/Exclude, Collector, and an Add button. The table is currently empty. To the right of the table, there is a note: "Subnets should be in valid CIDR format or individual IP or IP Range. Example Subnets: Valid CIDR Format: 192.168.1.0/24 10.200.0.0/16 IP or IP-Range: 10.10.10.10 10.10.10.10-100 10.10.1.1-10.10.5.200".

Subnet	Include/Exclude	Collector	
	<input checked="" type="radio"/> Include <input type="radio"/> Exclude	<input checked="" type="checkbox"/> Nmap <input type="checkbox"/> Wmi	Add

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

The screenshot shows the Pulse Secure web interface for configuring a MAC Address Authentication Realm. The breadcrumb trail is "MAC Address Realms > MAC_Auth_Realm > General". The "General" tab is selected, with sub-tabs for "General", "Authentication Policy", and "Role Mapping".

Name: MAC_Auth_Realm
Description: [Empty text area]
☐ When editing, start on the Role Mapping page

Servers
Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:	MacAuthServer	Specify the server to use for authenticating users.
User Directory/Attribute:	Same as above	Specify the server to use for authorization.
Accounting:	None	Specify the server to use for Radius accounting.
Device Attributes:	Profiler	Specify the server to use for device authorization.
Device Check Interval:	60 minutes	Specify the interval to check device attributes server. disable=0, min=10, max=10000 minutes

Dynamic policy evaluation
☐ Enable dynamic policy evaluation

Other Settings
Authentication Policy: No restrictions
Role Mapping: 3 Rules

[Save Changes](#)

- 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

The screenshot shows the Pulse Secure web interface for configuring a Role Mapping Rule. The breadcrumb trail is "MAC Address Realms > MAC_Auth_Realm > Role Mapping > Role Mapping Rule". The page title is "Role Mapping Rule". The "Rule based on:" dropdown is set to "Device attribute" with an "Update" button next to it. The "Name:" field contains "ipphone". Below this, a green checkmark indicates the rule: "Rule: If device has any of the following attribute values...". The "Attribute:" dropdown is set to "category", and the "Value:" field contains "VoIP Phones/Adapters". A note states: "If more than one value for this attribute should match, enter one per line. You can use * wildcards." Below this, a green checkmark indicates the assignment: "then assign these roles". The "Available Roles:" list includes "Guest Sponsor", "Guest Wired Restricted", "ipphone", "Unknown_Device", and "Users". The "Selected Roles:" list contains "VoIP Phones". There are "Add ->" and "Remove" buttons between the lists. A checkbox labeled "Stop processing rules when this rule matches" is checked. At the bottom, there are "Save Changes" and "Save + New" buttons. A small note at the bottom left says "*Indicates required field".

- 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

The screenshot shows the Pulse Secure web interface for configuring a Role Mapping Rule. The breadcrumb trail is "MAC Address Realms > MAC_Auth_Realm > Role Mapping > Role Mapping Rule". The page title is "Role Mapping Rule". The "Rule based on:" dropdown is set to "User attribute" with an "Update" button next to it. The "Name:" field contains "Unknown_Device". Below this, a green checkmark indicates the rule: "Rule: If user has any of the following attribute values...". The "Attribute:" dropdown is set to "(Select an attribute)", and the "Value:" field is empty. A note states: "If more than one value for this attribute should match, enter one per line. You can use * wildcards." Below this, a green checkmark indicates the assignment: "then assign these roles". The "Available Roles:" list includes "Guest", "Guest Admin", "Guest Sponsor", "Guest Wired Restricted", and "ipphone". The "Selected Roles:" list is empty, showing "(none)". There are "Add ->" and "Remove" buttons between the lists. A checkbox labeled "Stop processing rules when this rule matches" is checked. At the bottom, there are "Save Changes" and "Save + New" buttons. A small note at the bottom left says "*Indicates required field".

Overlaid on the right side of the screenshot is a browser window titled "MacAuthServer Server Catalog - Google Chrome". The address bar shows "https://10.204.88.184/dana-admin/auth/serverDict.cgi". The page content is "Server Catalog for MacAuthServer". There are tabs for "Attributes", "Expressions", and "Variables". The "Attributes" tab is active, showing a list of attributes: "department", "departmentNumber", "employeeNumber", "employeeType", "homeDirectory", "homeDrive", and "memberOfGroup". The "Attribute:" field contains "deviceName". There is an "Add Attribute" button. At the bottom of the browser window are "OK", "New...", and "Delete" buttons.

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**.

MAC Address Realms > MAC_Auth_Realm > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: User attribute Update

* Name: Unknown_Device

▼ Rule: if user has any of the following attribute values...

Attribute: deviceName Attributes...

is Unknown

If more than one value for this attribute should match, enter one per line. You can use * wildcards.

▼ then assign these roles

Available Roles: Guest Sponsor, Guest Wired Restricted, ipphone, Users, VoIP Phones

Selected Roles: Unknown_Device

☒ Stop processing rules when this rule matches

To manage roles, see the Roles configuration page.

Save Changes Save + New

*Indicates required field

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

Figure 13: Completed Role Mapping Rules

MAC Address Realms > MAC_Auth_Realm > Role Mapping

Role Mapping

General Authentication Policy **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete ↑ ↓ Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
1.	device attribute "category" is "VoIP Phones/Adapters"	→ VoIP Phones	ipphone	✓
2.	attribute "deviceName" is "Unknown"	→ Unknown_Device	Unknown_Device	✓

When more than one role is assigned to a user the settings for all assigned roles will be merged.
Note: Users that do not meet any of the above rules will not be able to sign into this realm.

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

Pulse Secure System Authentication Administrators Users **Endpoint Policy** Maintenance Wizards

Network Access > Location Group > mac

mac

Location Group

* Name: mac Label to reference this Location Group.

Description:

* Sign-in Policy: */ To manage policies, see the Sign-In Policies

MAC Authentication Realm: MAC_Auth_Realm To manage realm, see the MAC Address Realms

Save Changes

* indicates required field

- 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

Pulse Secure System Authentication Administrators Users **Endpoint Policy** Maintenance Wizards

Network Access > RADIUS Client > RadiusClient

RadiusClient

RADIUS Client

* Name: RadiusClient Label to reference this RADIUS Client.

Description:

* IP Address: 10.204.0.100 IP Address of this RADIUS Client.

* IP Address Range: 1 Number of IP Addresses for this RADIUS Client

* Shared Secret: ***** RADIUS shared secret

* Make/Model: Juniper Networks Inc (JUNOS) To manage make/model, see the RADIUS Vendor

* Location Group: mac To manage groups, see the Location Group

Dynamic Authorization Support

Support Disconnect Messages ☒ Disconnect Message Support

Support CoA Messages ☐ Change of Authorization Message Support

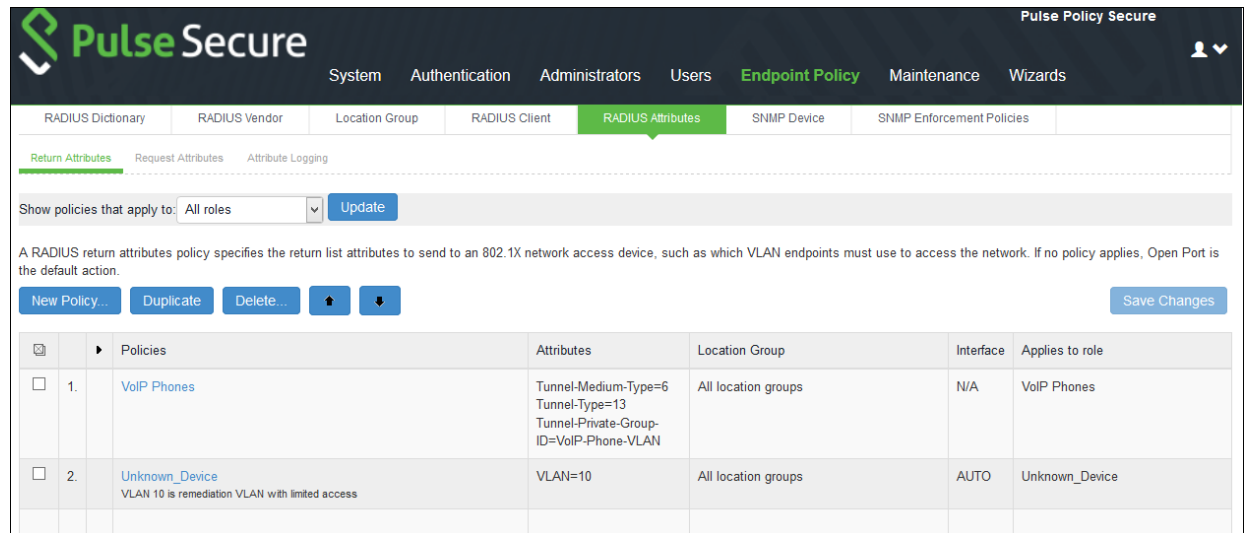
* Dynamic Authorization Port: 3799 Dynamic Authorization Extensions Port

Save Changes

- c. Set RADIUS return attributes. Select **Endpoint Policy > Network Access > RADIUS Return Attribute Policies**. Click **New Policy**.

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

Figure 16: RADIUS return Attributes



The screenshot shows the Pulse Secure web interface. The top navigation bar includes links for System, Authentication, Administrators, Users, **Endpoint Policy**, Maintenance, and Wizards. The sub-navigation bar includes links for RADIUS Dictionary, RADIUS Vendor, Location Group, RADIUS Client, **RADIUS Attributes**, SNMP Device, and SNMP Enforcement Policies. The main content area is titled "Return Attributes" and includes a "Show policies that apply to:" dropdown set to "All roles" and an "Update" button. Below this is a descriptive text: "A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action." There are buttons for "New Policy...", "Duplicate", "Delete...", and "Save Changes". A table of policies is displayed below:

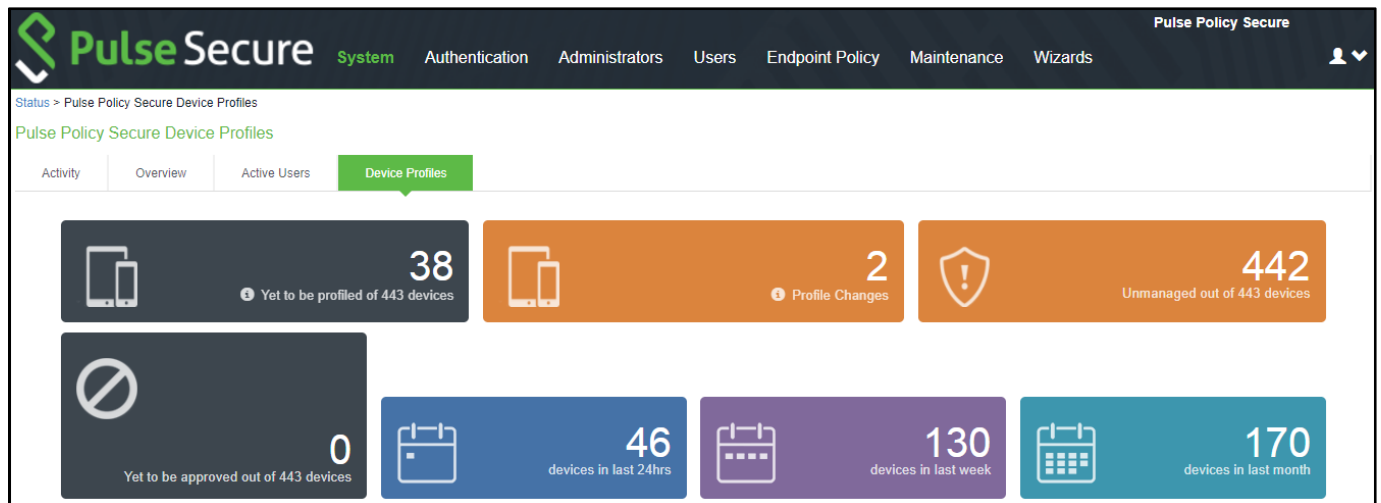
		Policies	Attributes	Location Group	Interface	Applies to role
<input type="checkbox"/>	1.	VoIP Phones	Tunnel-Medium-Type=6 Tunnel-Type=13 Tunnel-Private-Group-ID=VoIP-Phone-VLAN	All location groups	N/A	VoIP Phones
<input type="checkbox"/>	2.	Unknown_Device VLAN 10 is remediation VLAN with limited access	VLAN=10	All location groups	AUTO	Unknown_Device

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.

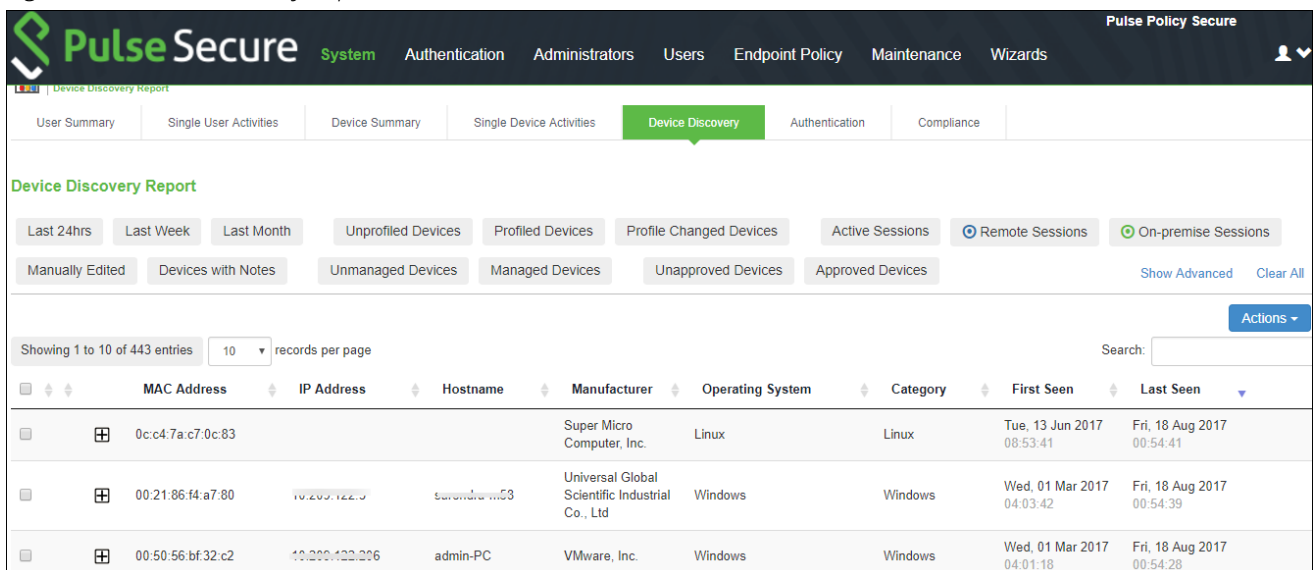
You can view the high-level device statistics from the Device dashboard page at **System > Status > Device Profiles**.

Figure 17: Device Profiles



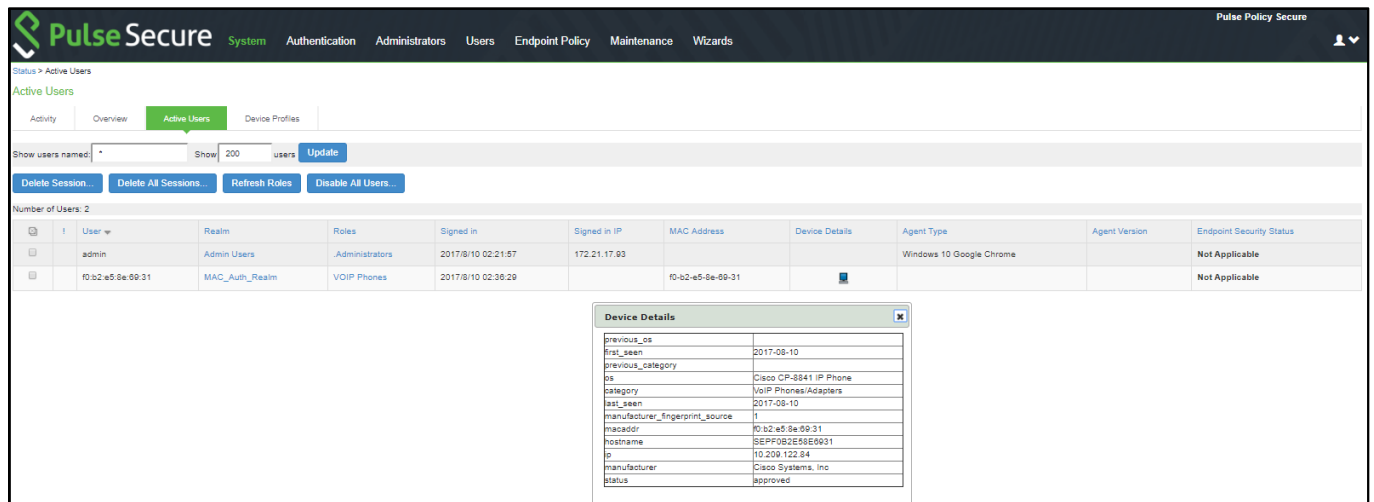
You can view the device reports at **System > Reports > Device Discovery**.

Figure 18: Device Discovery Report



You can verify the active users table to view the session details of the user.

Figure 19: Active Users

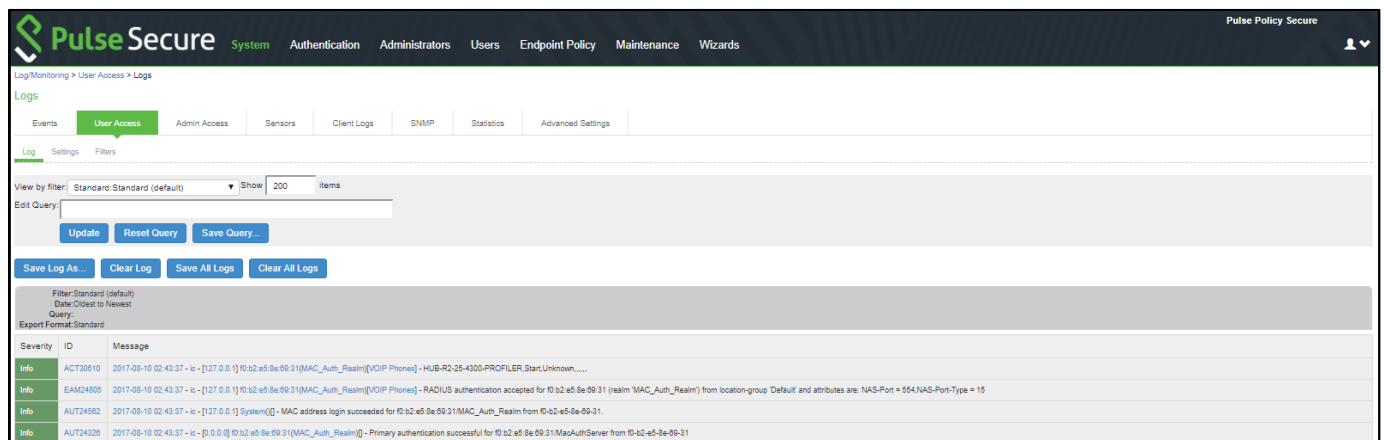


The screenshot displays the 'Active Users' section of the Pulse Secure management console. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Endpoint Policy', 'Maintenance', and 'Wizards'. The 'Active Users' tab is selected, showing a table of active users. A 'Device Details' pop-up window is open, displaying the following information:

Device Details	
previous_os	
first_seen	2017-08-10
previous_category	
os	Cisco CP-8841 IP Phone
category	VoIP Phones/Adapters
last_seen	2017-08-10
manufacturer_fingerprint_source	1
macaddr	02:00:00:00:00:00
hostname	SEP082158E00031
ip	10.209.122.84
manufacturer	Cisco Systems, Inc
status	approved

For troubleshooting you can verify the user access logs.

Figure 20: User Access Logs



The screenshot displays the 'User Access Logs' section of the Pulse Secure management console. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Endpoint Policy', 'Maintenance', and 'Wizards'. The 'User Access' tab is selected, showing a table of user access logs. The 'Log' sub-tab is active, displaying the following log entries:

Severity	ID	Message
Info	ACT30910	2017-08-10 02:43:37 - [127.0.0.1] 02:00:00:00:00:00 [MAC_Auth_Realm] - HUB-R2-25-0200-PROFILER_StartUnknown...
Info	EA024805	2017-08-10 02:43:37 - [127.0.0.1] 02:00:00:00:00:00 [MAC_Auth_Realm] - RADIUS authentication accepted for 02:00:00:00:00:00 (realm 'MAC_Auth_Realm') from location-group 'Default' and attributes are: NAS-Port = 554/NAS-Port-Type = 15
Info	AUT24592	2017-08-10 02:43:37 - [127.0.0.1] System[] - MAC address login succeeded for 02:00:00:00:00:00 [MAC_Auth_Realm] from 02:00:00:00:00:00
Info	AUT24328	2017-08-10 02:43:37 - [127.0.0.1] 02:00:00:00:00:00 [MAC_Auth_Realm] - Primary authentication successful for 02:00:00:00:00:00 [MAC_Auth_Realm] from 02:00:00:00:00:00