



Pulse Policy Secure

SNMP Enforcement using 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.

SNMP Enforcement using 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."

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 and printers often do not have a supplicant or Pulse client. VoIP phones which support 802.1x can be configured to use 802.1x based authentication.

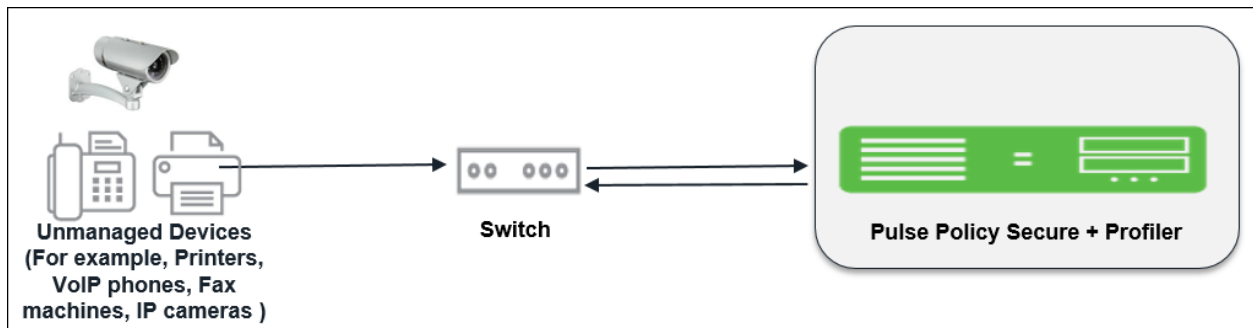
To allow such devices on the network, the PPS admin can configure MAC Address Authentication using SNMP and Profiler profiles these devices to ensure that only devices of a certain “profile” can access the network.

This document explains a use case of a typical host, such as a VoIP phone, that is not 802.1x enabled to be permitted on the network using SNMP enforcement and the native Profiler.

Note:

SNMP enforcement is supported only with Cisco and HP switches. The Switch must be configured for linkup, MAC Address Notification or Port Security traps.

Figure 1: Overview



Pulse Policy Secure Configuration

The following configurations are required to permit the VoIP phone to access the LAN network:

- Create 2 roles, one for hosts that don't have a 802.1x supplicant (For example, VoIP Phones) and another for putting all the other devices onto a remediation role.
- Create a MAC Address Authentication Server and MAC Address Authentication Realm.
- Create a Local Profiler authorization server and assign them to a MAC Address Authentication Realm.
- In the MAC Address Authentication Realm, create role mapping rules to assign roles to devices.
- Create a location group and map the location group to MAC Address Authentication Realm.
- Configure an SNMP client.
- Configure the SNMP enforcement policies for final VLAN assignment.

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

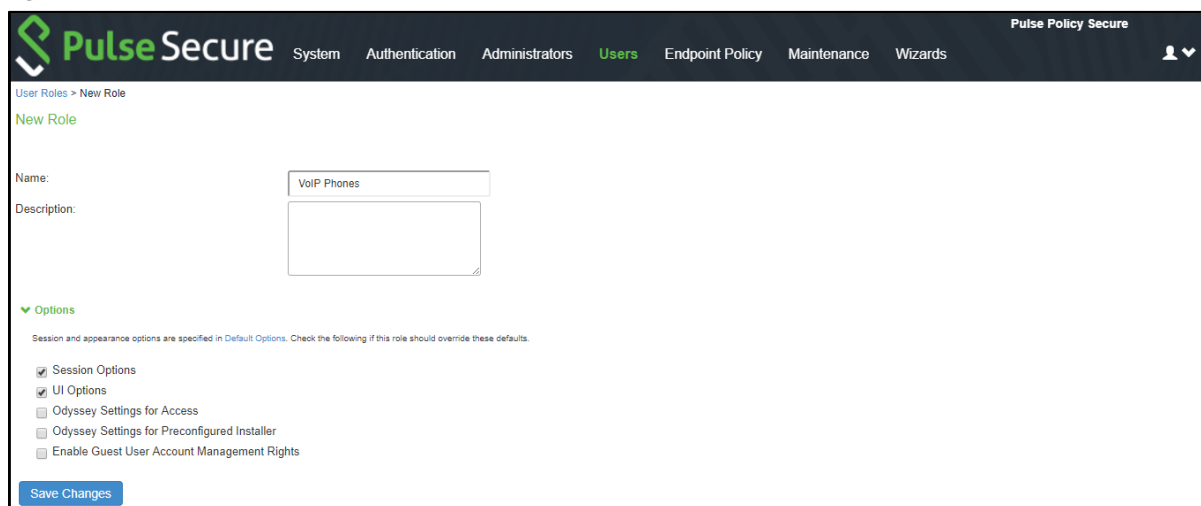
Pre-Requisite

You must ensure that the Switch is configured with the linkup, MAC Address notification or port security trap. You must procure Profiler license for profiler functionality. For sample configuration, See [Profiler Deployment Guide](#).

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

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: MacAuthServer Label to reference this authentication.

MAC Addresses

Maximum 500 addresses

Delete Add Remove

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

Add

Optional LDAP Servers

Available LDAP Servers: (none) Add -> Remove

Selected LDAP Servers: LDAP_Authz_Server

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

The screenshot shows the Pulse Secure web interface. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Endpoint Policy', 'Maintenance', and 'Wizards'. The 'Authentication' tab is selected. Below the navigation bar, the breadcrumb trail reads 'Auth Servers > profiler > Settings'. The 'Settings' tab is active, and the 'Troubleshooting' tab is also visible. The main content area shows the 'Name' field set to 'Profiler' and a 'Label to reference this server:' field.

- b. Click **Browse** and upload the device fingerprints package from the [software download site](#).

Figure 6: Uploading Device Fingerprints Package

The screenshot shows the 'Fingerprint Database file' section of the Pulse Secure web interface. It includes a 'No file chosen' status, a 'Browse' button, and an 'Upload and Save' button. Below the buttons, it states 'Last uploaded version: 23 | Last imported on: Thu Aug 3 02:00:03 2017'.

- c. Configure SNMP Poll interval and DHCP sniffing mode interface. The SNMP poll interval must be set depending on your deployment. For example, if it is set to 60, the connected SNMP Switches are checked for every 60 minutes.

Figure 7: SNMP Poll Interval

The screenshot shows the 'General Settings' section of the Pulse Secure web interface. It includes the 'SNMP Poll Interval' field set to '60' and the 'DHCP Sniffing mode' dropdown menu set to 'DHCP Helper (Internal port)'. A note on the right states: 'Minutes: Specify the interval to check SNMP Switch for connected endpoints. Default=60 minimum=5. To discover devices using SNMP, configure one or more switches under [SNMP Device](#). Select an option based on your DHCP forward mode.'

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

Figure 8: SNMP Device Configuration

The screenshot shows the 'SNMP Device Configuration' page for 'JuniperSW' in the Pulse Secure web interface. The 'SNMP Version' is set to 'v1/v2c'. The 'Name' field is 'JuniperSW'. The 'IP Address' field is '192.168.1.100'. The 'Vendor' dropdown is set to 'JUNIPER'. The 'SNMP Settings' section includes a checkbox for 'Same credentials for Trap user' (checked) and a 'Read Community String' field set to 'public'. A 'Save Changes' button is at the bottom.

- 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

♥ Endpoints to scan using NMAP/WMI

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.

Delete ↑ ↓

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

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

4. Create a new MAC Address Authentication Realm and assign the MAC Address Authentication Server and Profiler server to it, select **Endpoint Policy > MAC Address Realms > MAC Authentication Realm**.

Figure 10: MAC Address Authentication Realm

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

MAC Address Realms > MAC_Auth_Realm > General

General Authentication Policy Role Mapping

Name: Label to reference this realm

Description:

☐ 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: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: Specify the server to use for device authorization.

Device Check Interval: minutes Specify the interval to check device attributes server. disable=0, min=10, max=10080 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.

Figure 11: Role Mapping Rule1

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".

Rule based on: Device attribute [Update]

* Name: ipphone

Rule: If device has any of the following attribute values...

Attribute: category [Attributes...]

is VoIP Phones/Adapters

then assign these roles

Available Roles: Guest Sponsor, Guest Wired Restricted, ipphone, Unknown_Device, Users

Selected Roles: VoIP Phones

☒ Stop processing rules when this rule matches

To manage roles, see the Roles configuration page.

[Save Changes] [Save + New]

*Indicates required field

Create another rule, to assign all other devices to the role called “Guest wired restricted”.

Figure 12: Role Mapping Rule2

The screenshot shows the Pulse Secure web interface for configuring a Role Mapping Rule. The breadcrumb trail is: MAC Address Realms > macauth > Role Mapping > Role Mapping Rule. The page title is "Role Mapping Rule".

* Name: test

Rule: If username...

is *

then assign these roles

Available Roles: Guest, Guest Admin, Guest Sponsor, Users, VoIP Phones

Selected Roles: Guest Wired Restricted

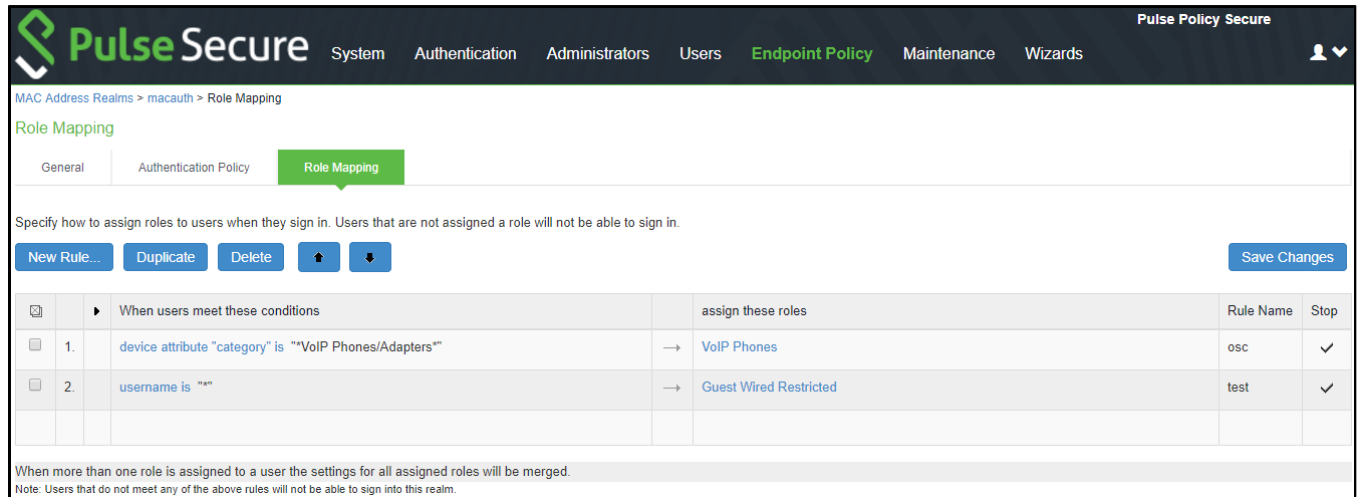
☒ Stop processing rules when this rule matches

To manage roles, see the Roles configuration page.

[Save Changes] [Save as Copy]

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

Figure 13: Role Mapping Rule



MAC Address Realms > macauth > 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.

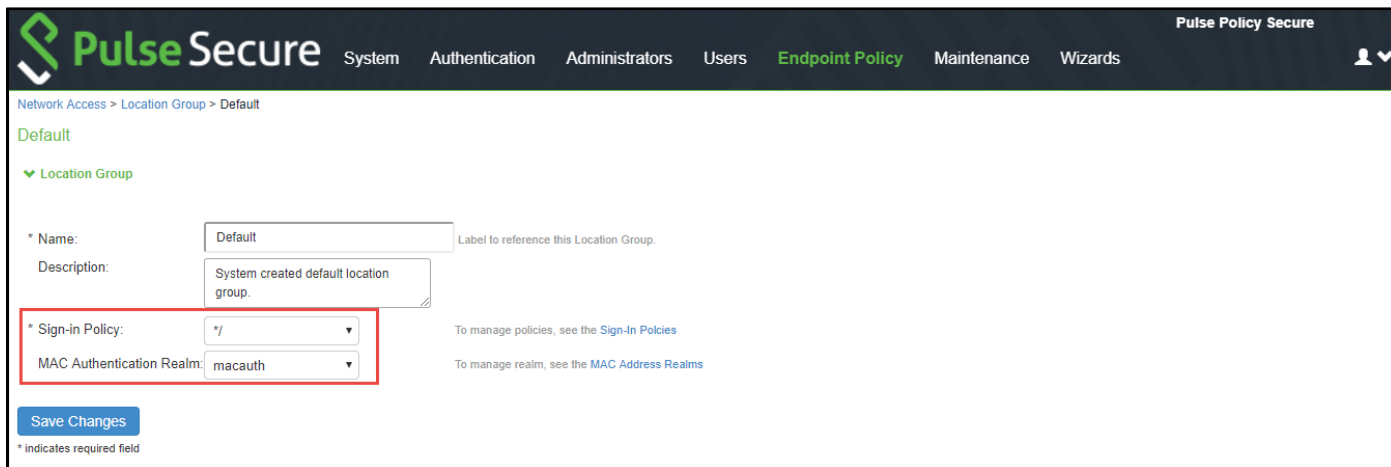
New Rule... Duplicate Delete Up Down Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
1.	device attribute "category" is "VoIP Phones/Adapters"	→ VoIP Phones	osc	✓
2.	username is "*"	→ Guest Wired Restricted	test	✓

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.

6. Configure the SNMP client (i.e 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



Network Access > Location Group > Default

Default

Location Group

* Name: Default Label to reference this Location Group.

Description: System created default location group.

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

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

Save Changes

* indicates required field

- b. Create a new SNMP client. Select **Endpoint Policy > Network Access > SNMP Device Configuration**. Enable **SNMP Enforcement** and select the location group.
- You can also choose to add the SNMP client through **Endpoint Policy > Network Access > SNMP Device Discovery**.

Figure 15: SNMP client

The screenshot displays the Pulse Secure web interface for configuring an SNMP device. The breadcrumb trail is **Network Access > SNMP Device Configuration > HP-2920-24G-PoEP**. The page title is **HP-2920-24G-PoEP**. The configuration fields are as follows:

- *SNMP Version:** Radio buttons for v1/v2c and v3. v3 is selected.
- *Name:** Text field containing "HP-2920-24G-PoEP".
- Description:** Empty text area.
- *IP Address:** Text field containing "10.20.1.200".
- *Vendor:** Dropdown menu showing "HP".
- *SNMP enforcement:** Checkmark is selected and highlighted with a red box.
- *Location Group:** Dropdown menu showing "Default".
- *Default VLAN:** Text field containing "1".

Below these fields is the **SNMP Settings** section, which includes:

- Same credentials for Trap user:** Checkmark is selected.
- *Read Username:** Text field containing "profiler".
- *Read Security Level:** Dropdown menu showing "Auth, Priv".
- *Auth Protocol:** Dropdown menu showing "SHA".
- *Auth Password:** Text field with masked characters "*****".
- *Priv Protocol:** Dropdown menu showing "CBC-DES".
- *Priv Password:** Text field with masked characters "*****".

A **Save Changes** button is located at the bottom left of the configuration area.

- c. Define the SNMP enforcement policy. Select Endpoint Policy > **Network Access** > **SNMP Enforcement Policies**. Click **New Policy**.
- For example, Define an SNMP enforcement policy for moving VoIP Phones to the appropriate VLAN.

Figure 16: SNMP Enforcement Policy1

The screenshot displays the Pulse Secure web interface for configuring a new SNMP Enforcement Policy. The breadcrumb trail at the top reads: **Network Access > SNMP Enforcement Policies > VOIP rule**. The page title is **VOIP rule**. Under the **SNMP Policy** section, the following fields are visible:

- *Policy Name:** (Label to reference this SNMP Policy.)
- Description:**
- *VLAN:**
- Location Group:** (To manage groups, see the [Location Group](#))

Under the **Roles** section, three radio buttons are present:

- ☐ Policy applies to ALL roles
- ☒ Policy applies to SELECTED roles
- ☐ Policy applies to all roles OTHER THAN those selected below

Below the radio buttons, there are two lists of roles:

- Available roles:** Guest, Guest Admin, Guest Sponsor, Guest Wired Restrict, Users
- Selected roles:** VoIP Phones

Buttons for **Add ->** and **Remove** are located between the two lists. A **Save Changes** button is at the bottom left.

Define an SNMP enforcement policy for moving other devices to the appropriate VLAN.

Figure 17: SNMP Enforcement Policy2

The screenshot displays the Pulse Secure web interface for configuring an SNMP Enforcement Policy. The breadcrumb trail at the top reads: Network Access > SNMP Enforcement Policies > Remid Rule. The page title is "Remid Rule".

SNMP Policy Section:

- *Policy Name:** A text field containing "Remid Rule". A tooltip indicates: "Label to reference this SNMP Policy."
- Description:** An empty text area.
- *VLAN:** A text field containing "74".
- Location Group:** A dropdown menu set to "Default". A tooltip indicates: "To manage groups, see the [Location Group](#)".

Roles Section:

- Three radio buttons for role application:
 - ☐ Policy applies to ALL roles
 - ☒ Policy applies to SELECTED roles
 - ☐ Policy applies to all roles OTHER THAN those selected below
- Available roles:** A list box containing: Guest, Guest Admin, Guest Sponsor, Users, and VoIP Phones.
- Selected roles:** A list box containing: Guest Wired Restrict.
- Buttons: "Add ->" and "Remove".

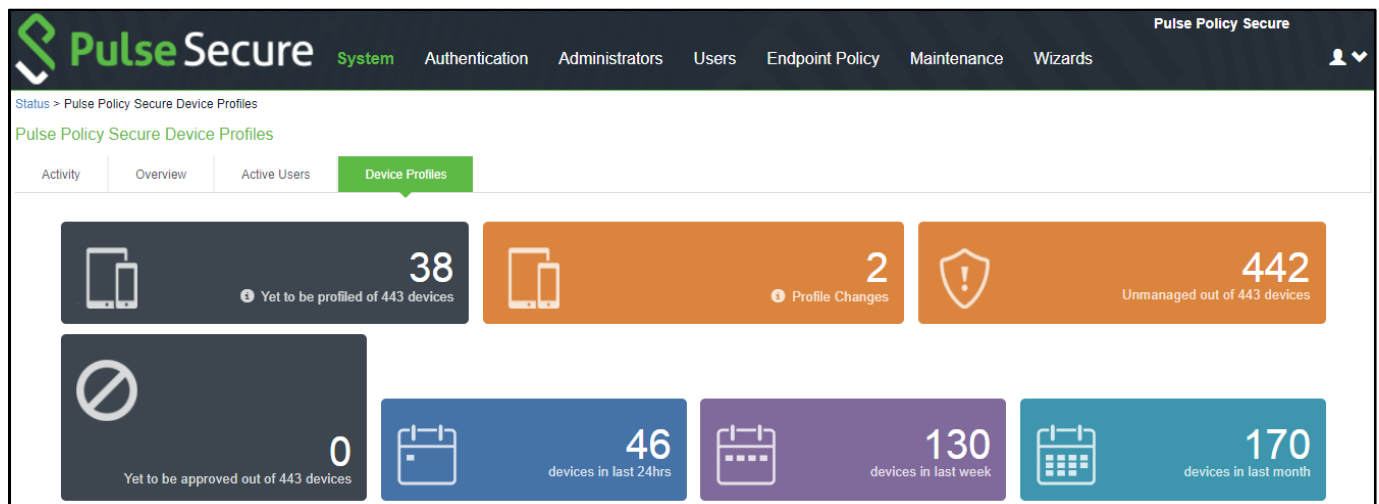
A "Save Changes" button is located at the bottom left of the configuration area.

Conclusion

You should now be able to properly authenticate devices based on their profile. For example, in the above scenario, all VoIP phones will be assigned with VoIP role and will be put under VLAN 65 when they attempt to access the network. The other devices will be assigned with a remediation role and will be put under VLAN 74.

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

Figure 18: Device Profiles



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

Figure 19: Device Discovery Report

The screenshot shows the Pulse Secure Device Discovery Report table. The table has the following columns: MAC Address, IP Address, Hostname, Manufacturer, Operating System, Category, First Seen, and Last Seen. The table displays three rows of device data.

MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	First Seen	Last Seen
0c:c4:7a:c7:0c:83			Super Micro Computer, Inc.	Linux	Linux	Tue, 13 Jun 2017 08:53:41	Fri, 18 Aug 2017 00:54:41
00:21:86:f4:a7:80	10.200.122.3	server01-ws3	Universal Global Scientific Industrial Co., Ltd	Windows	Windows	Wed, 01 Mar 2017 04:03:42	Fri, 18 Aug 2017 00:54:39
00:50:56:bf:32:c2	10.200.122.206	admin-PC	VMware, Inc.	Windows	Windows	Wed, 01 Mar 2017 04:01:18	Fri, 18 Aug 2017 00:54:28

Figure 20: SNMP Enforcement Policies

Network Access > SNMP Enforcement Policies

SNMP Enforcement Policies

RADIUS Dictionary RADIUS Vendor Location Group RADIUS Client RADIUS Attributes SNMP Device **SNMP Enforcement Policies**

New SNMP Enforcement Policy... Duplicate... Delete... Home Refresh Save Changes

	Name	Location Group	VLAN	Roles
<input type="checkbox"/>	1 VOIP rule	Default	65	VoIP Phones
<input type="checkbox"/>	2 Remid Rule	Default	74	Guest Wired Restricted

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

Figure 21: Active Users

Status > Active Users

Active Users

Activity Overview **Active Users** Device Profiles

Show users named: * Show 200 users Update

Delete Session... Delete All Sessions... Refresh Roles Disable All Users...

Number of Users: 2

	User	Realm	Roles	Signed in	Signed in IP	MAC Address	Device Details	Agent Type	Agent Version	Endpoint Security Status
<input type="checkbox"/>	admin	Admin Users	Administrators	2017/8/16 03:02:09	172.21.16.203			Windows 10 MSIE		Not Applicable
<input type="checkbox"/>	f0-b2-e5-8e-69-31	macauth	VoIP Phones	2017/8/16 03:13:35		f0-b2-e5-8e-69-31				Not Applicable

Device Details

first_seen	2017-08-16
last_seen	2017-08-16
manufacturer_fingerprint_source	1
macaddr	f0-b2-e5-8e-69-31
manufacturer	Cisco Systems, Inc
status	approved
previous_os	
os	Cisco CP-8841 IP Phone
previous_category	
category	VoIP Phones/Adapters
hostname	SEPF0B2E58E6931

For troubleshooting you can verify the user access logs.

Figure 22: User Access Logs

The screenshot shows the Pulse Secure System interface with the 'User Access' tab selected under the 'Logs' section. The page displays a list of log entries with columns for Severity, ID, and Message. The logs show various system events related to port bounces, VLAN settings, and user authentication.

Severity	ID	Message
Info	EAM24460	2017-08-16 03:13:52 - ic - [127.0.0.1] System[] - port bounce for 10.204.89.188 succeeded
Info	EAM24460	2017-08-16 03:13:52 - ic - [127.0.0.1] System[] - setting VLAN 65 for switch 10.204.89.188 succeeded.
Info	EAM24460	2017-08-16 03:13:51 - ic - [127.0.0.1] System[] - VLAN setting sent to switch 10.204.89.188 VLAN = 65
Info	AUT23524	2017-08-16 03:13:51 - ic - [0.0.0.0] f0:b2:e5:8e:69:31(macauth)[VoIP Phones] - Roles for user f0:b2:e5:8e:69:31 on host 0.0.0.0 changed from <Guest Wired Restricted> to <VoIP Phones> during policy reevaluation.
Info	EAM24460	2017-08-16 03:13:35 - ic - [127.0.0.1] System[] - port bounce for 10.204.89.188 succeeded
Info	EAM24460	2017-08-16 03:13:35 - ic - [127.0.0.1] System[] - setting VLAN 74 for switch 10.204.89.188 succeeded.
Info	AUT24562	2017-08-16 03:13:35 - ic - [127.0.0.1] System[] - MAC address login succeeded for f0:b2:e5:8e:69:31/macauth from f0:b2:e5:8e:69:31.
Info	AUT24326	2017-08-16 03:13:35 - ic - [0.0.0.0] f0:b2:e5:8e:69:31(macauth)[] - Primary authentication successful for f0:b2:e5:8e:69:31/macauth from f0:b2:e5:8e:69:31

You can also verify the event logs.

Figure 23: Event Logs

The screenshot shows the Pulse Secure System interface with the 'Events' tab selected under the 'Logs' section. The page displays a list of log entries with columns for Severity, ID, and Message. The logs show various system events related to device attributes, user status, and local profiler retrieval.

Severity	ID	Message
Info	PRO31459	2017-08-16 03:13:51 - ic - [0.0.0.0] f0:b2:e5:8e:69:31(macauth)[Users] - Device f0:b2:e5:8e:69:31's attributes got updated from (first_seen = (2017-08-16) last_seen = (2017-08-16) manufacturer_fingerprint_source = [1] macaddr = (f0:b2:e5:8e:69:31) manufacturer = (Cisco Systems, Inc)) to (first_seen = (2017-08-16) last_seen = (2017-08-16) manufacturer_fingerprint_source = [1] macaddr = (f0:b2:e5:8e:69:31) manufacturer = (Cisco Systems, Inc) status = [approved] previous_os = [] os = (Cisco CP-8841 IP Phone) previous_category = [] category = (VoIP Phones/Adapters) hostname = (SEPF0B2E58E6931)).
Info	PRO31368	2017-08-16 03:13:51 - ic - [127.0.0.1] System[] - Device (f0:b2:e5:8e:69:31) is classified as Cisco IP Phone CP-8841.
Info	PRO31457	2017-08-16 03:13:35 - ic - [0.0.0.0] f0:b2:e5:8e:69:31(macauth)[] - Device(f0:b2:e5:8e:69:31)'s attributes are retrieved from local profiler .