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

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.

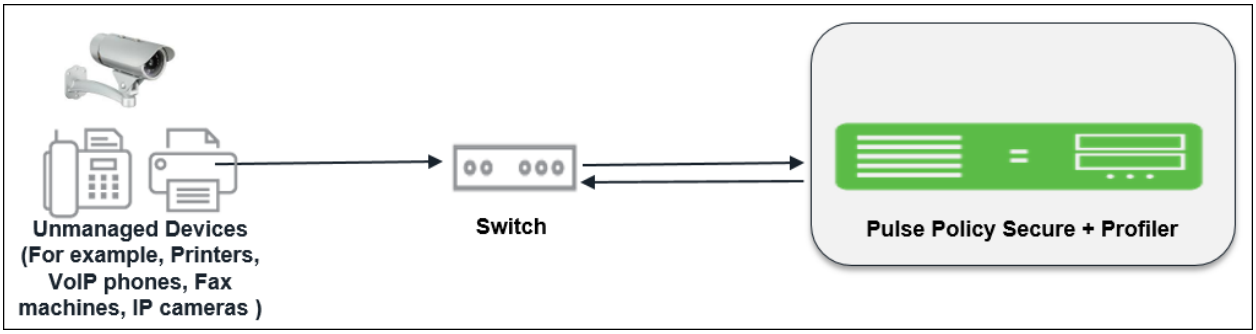
To allow such devices on the network, the PPS admin can configure MAC Address Authentication using SNMP and Profiler profiles these devices to ensure that only devices of a certain "profile" can access the network.

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.

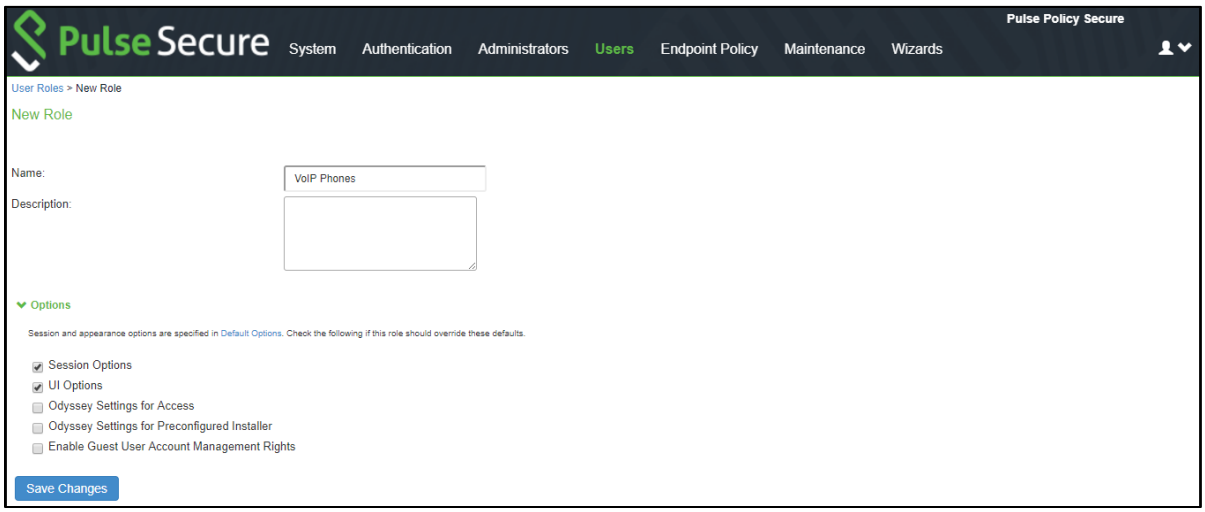
Pre-Requisite

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

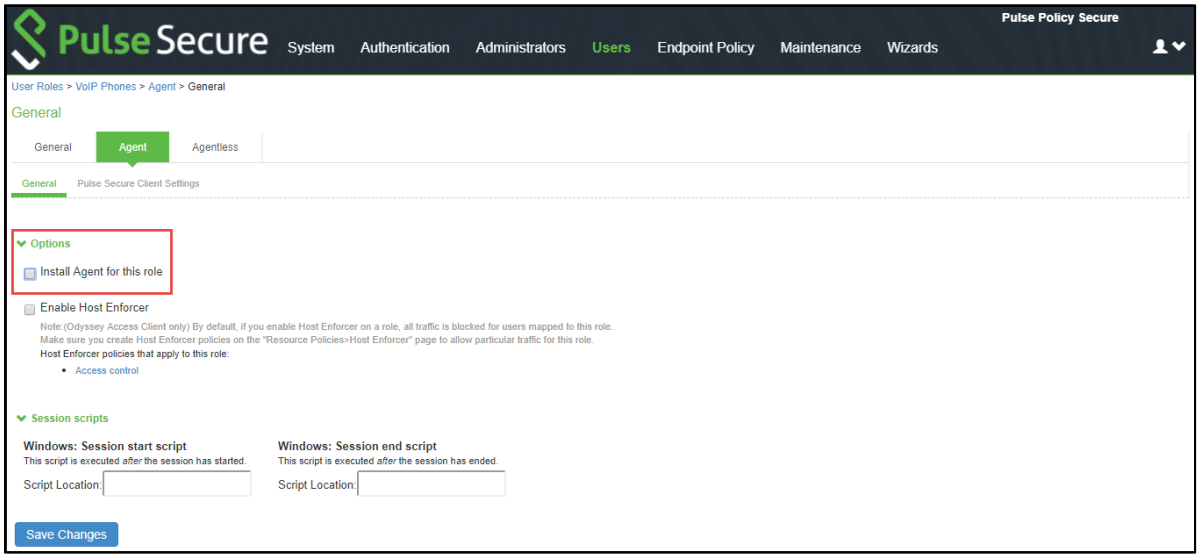
1. Create a new user role, select **Users > User Roles > New User Role**. Enter a name. For example, VoIP Phones.

Figure 2: User Role



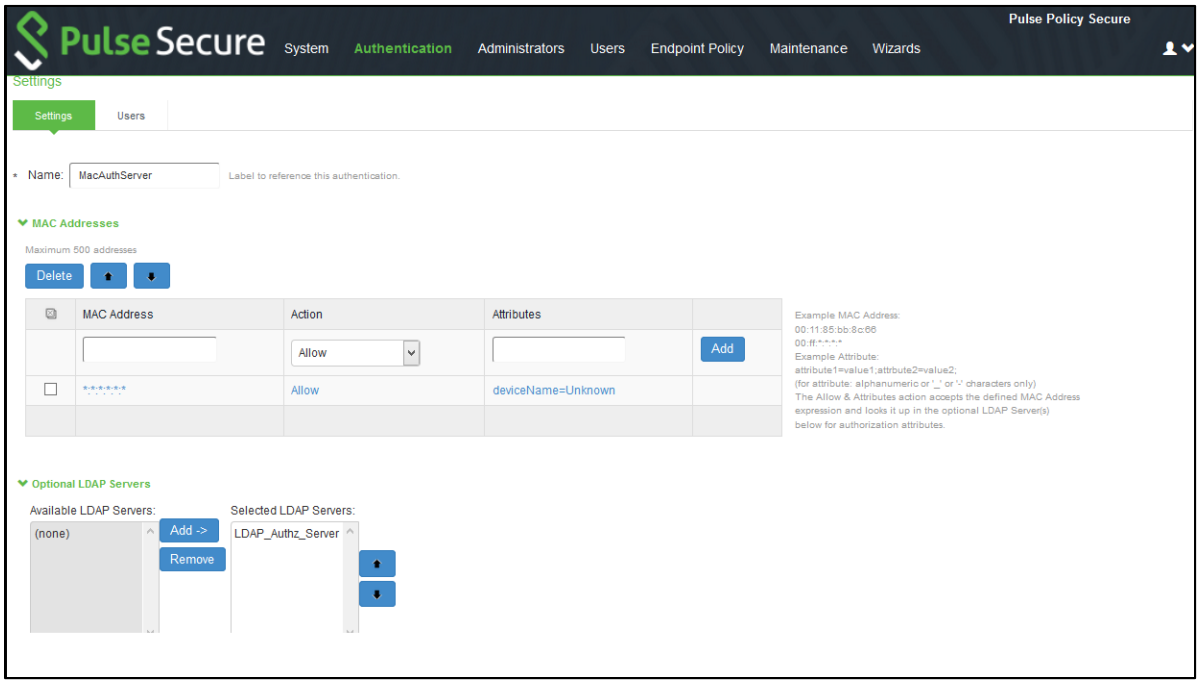
Uncheck **Install Agent for this Role**. Do not configure any role restrictions.

Figure 3: User Role- Agent



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.

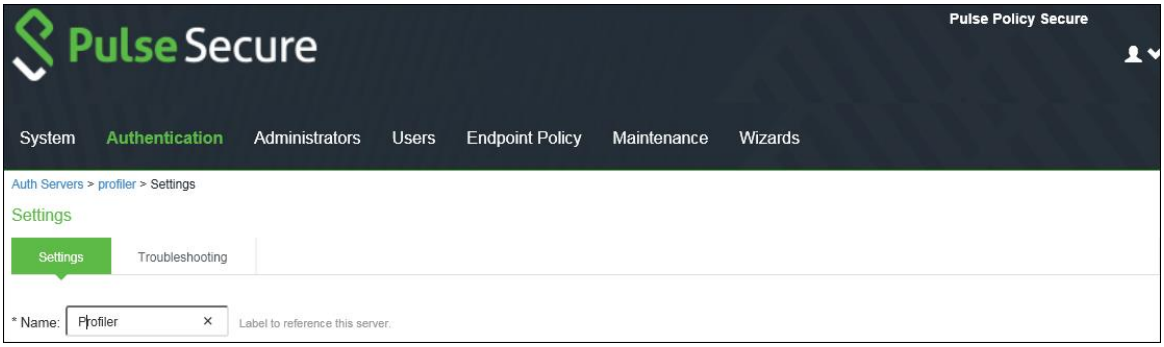
Figure 4: MAC Authentication Server



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

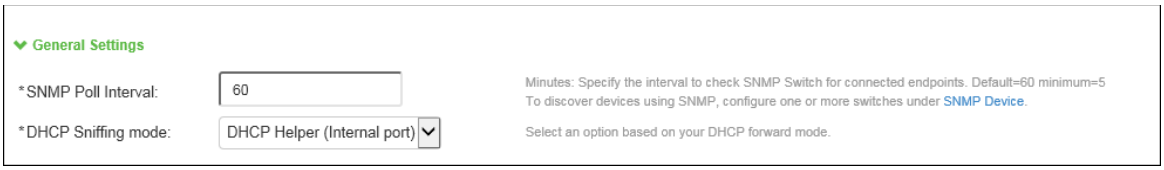


b. Click **Browse** and upload the device fingerprints package from the [software download site](#).

Figure 6: Uploading Device Fingerprints Package

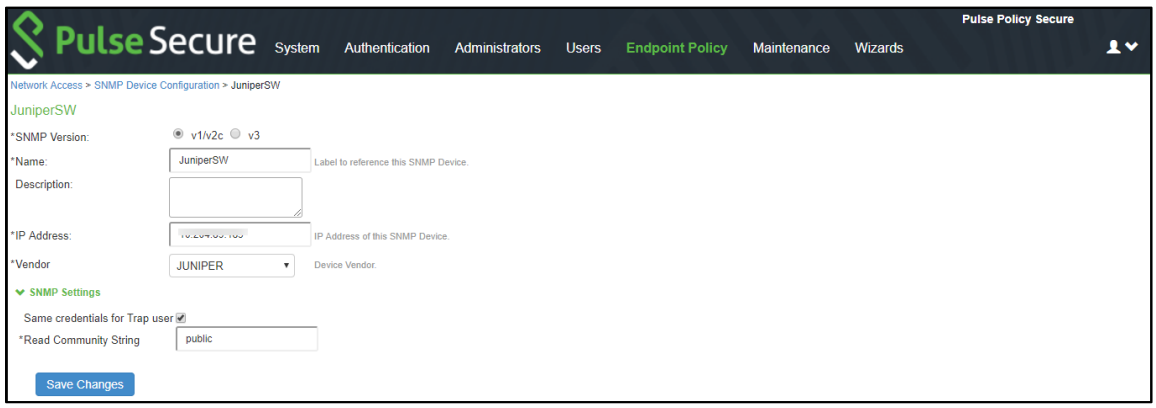
c. Configure SNMP Poll interval and DHCP sniffing mode interface. The SNMP poll interval must be set depending on your deployment. For example, if it is set to 60, the connected SNMP Switches are checked for every 60 minutes.

Figure 7: SNMP Poll Interval



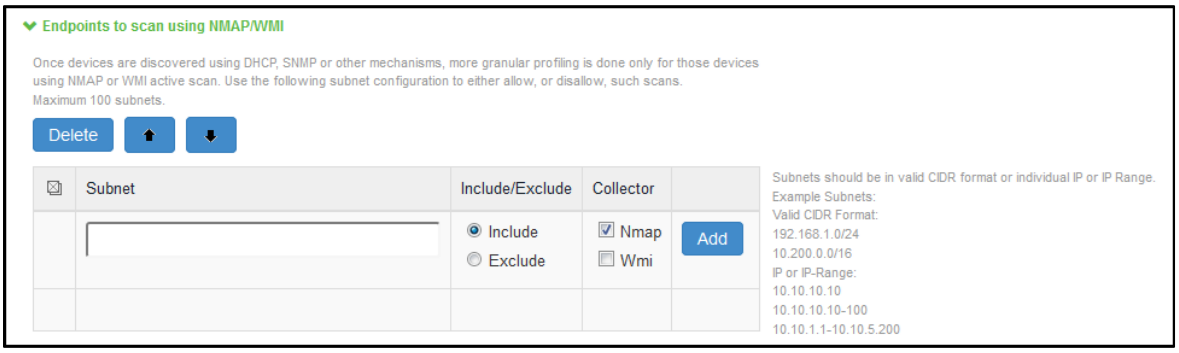
d. For Profiling devices using SNMP, configure the switch under **Endpoint Policy > Network Access > SNMP Device Configuration**.

Figure 8: SNMP Device Configuration



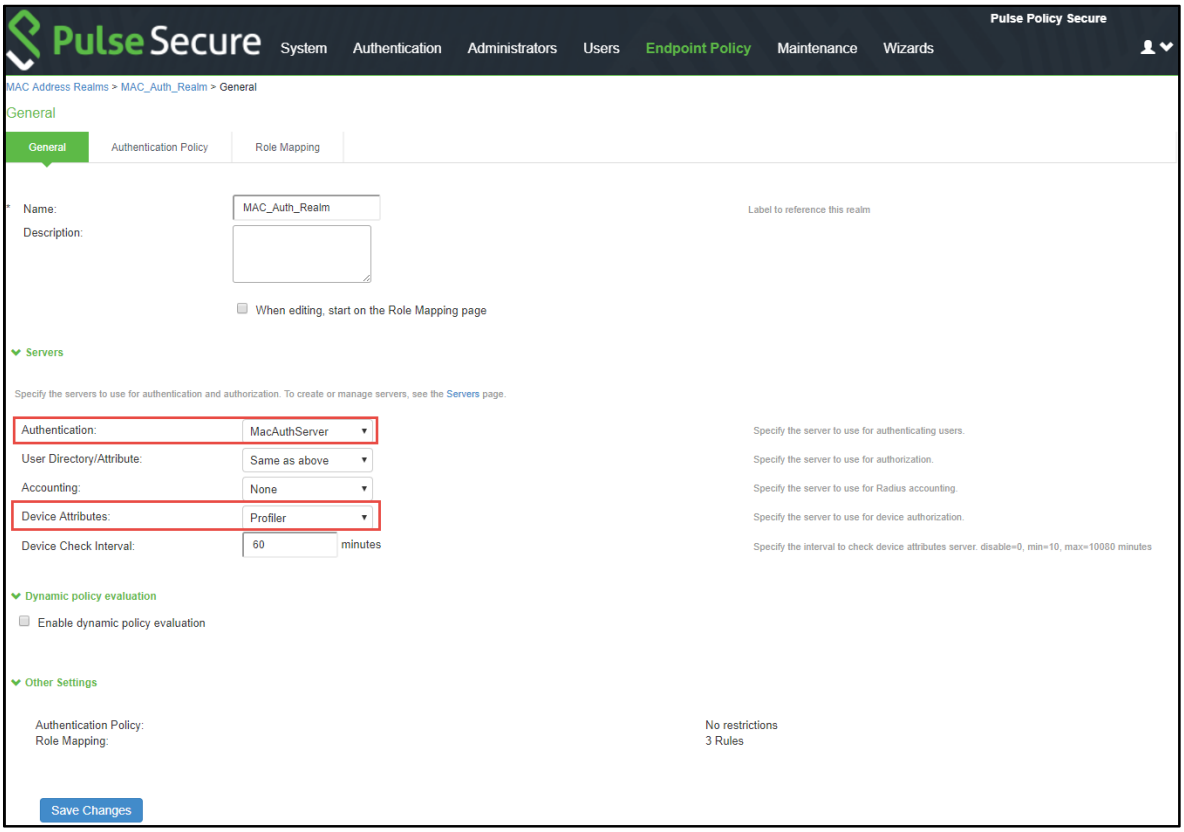
e. (Optional) Add one or more subnets that can be included or excluded for fingerprinting unmanaged devices using Nmap target scans. Note that an Nmap target scan is only performed on valid IP addresses in the subnet.

Figure 9: Adding One or More Subnets



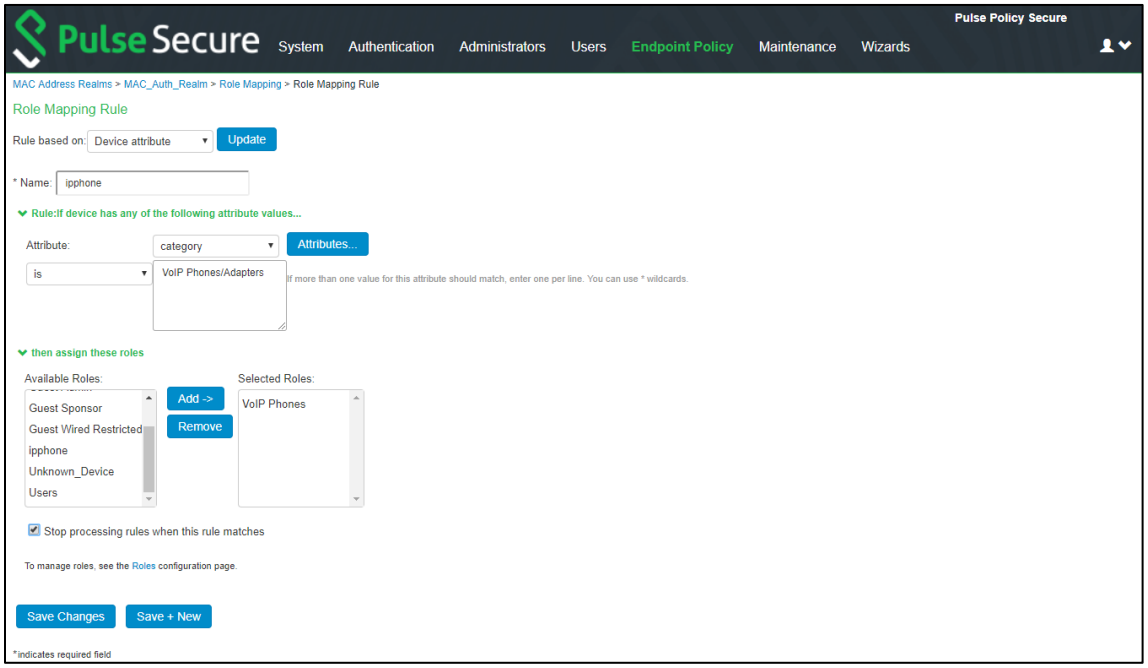
4. Create a new MAC Address Authentication Realm and assign the MAC Address Authentication Server and Profiler server to it, select **Endpoint Policy > MAC Address Realms > MAC Authentication Realm**.

Figure 10: MAC Address Authentication Realm



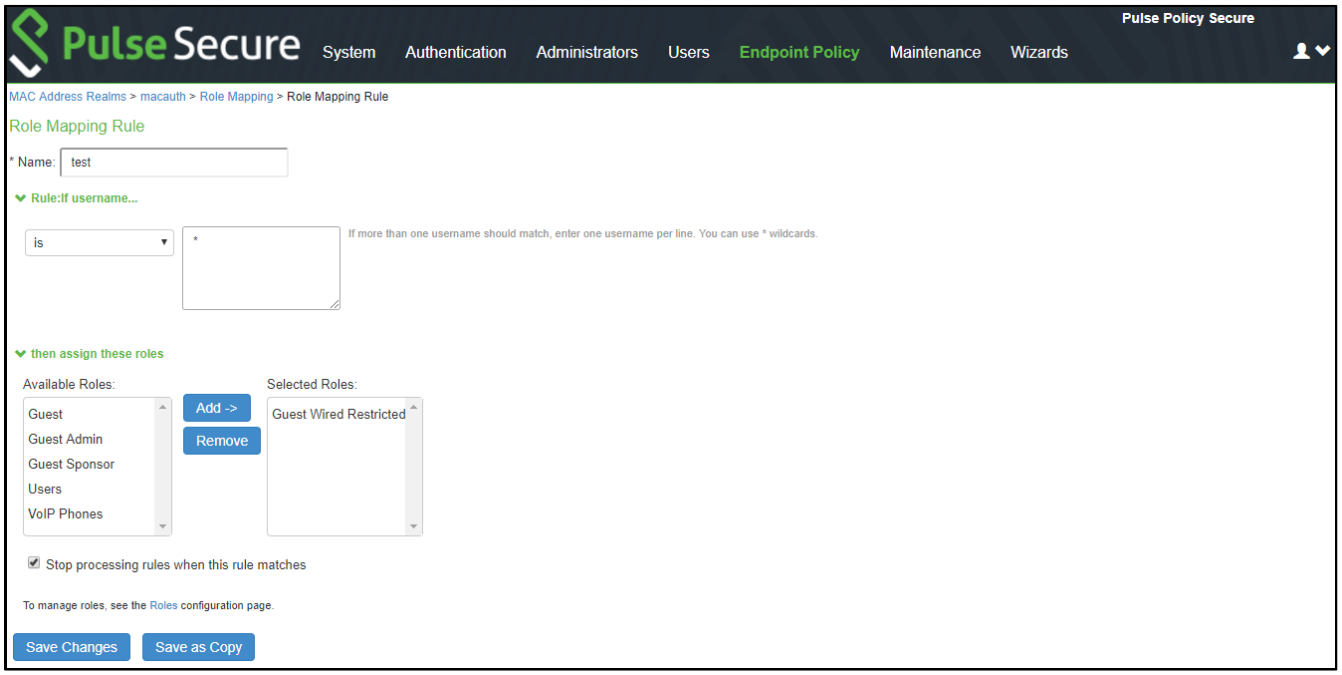
5. Set Role Mapping rules. Select Rule based on Device attribute and click **Update**. Enter the rule name and under Rule, select **Category** as Attribute and values as "VoIP Phone/Adapters" and then assign all devices of category to the role called "VoIP Phone" as shown below.

Figure 11: Role Mapping Rule1



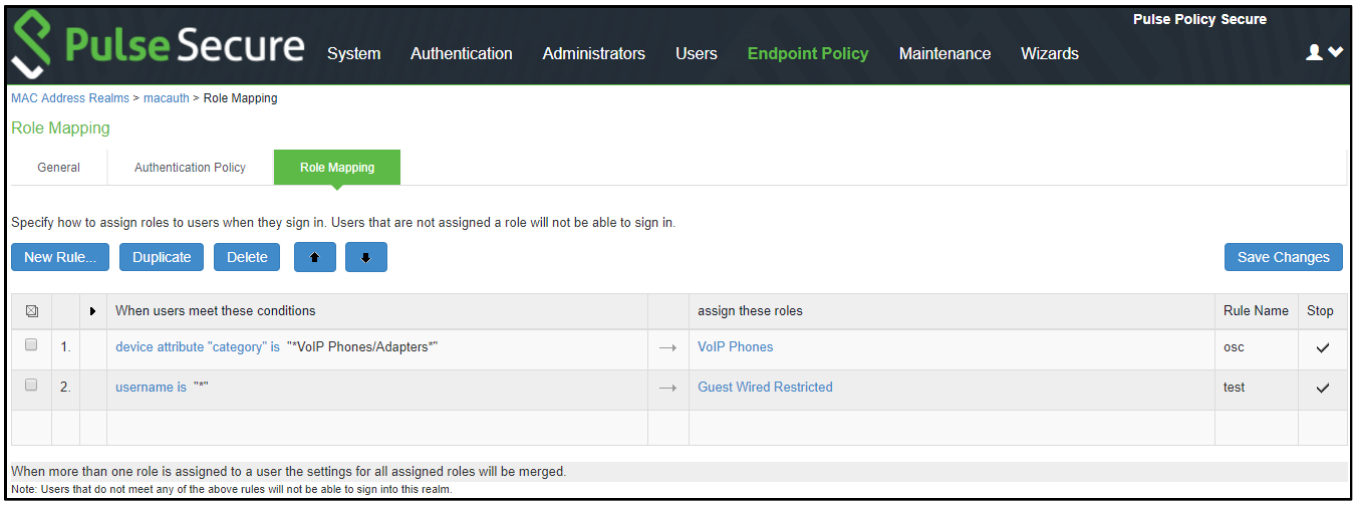
Create another rule, to assign all other devices to the role called "Guest wired restricted".

Figure 12: Role Mapping Rule2



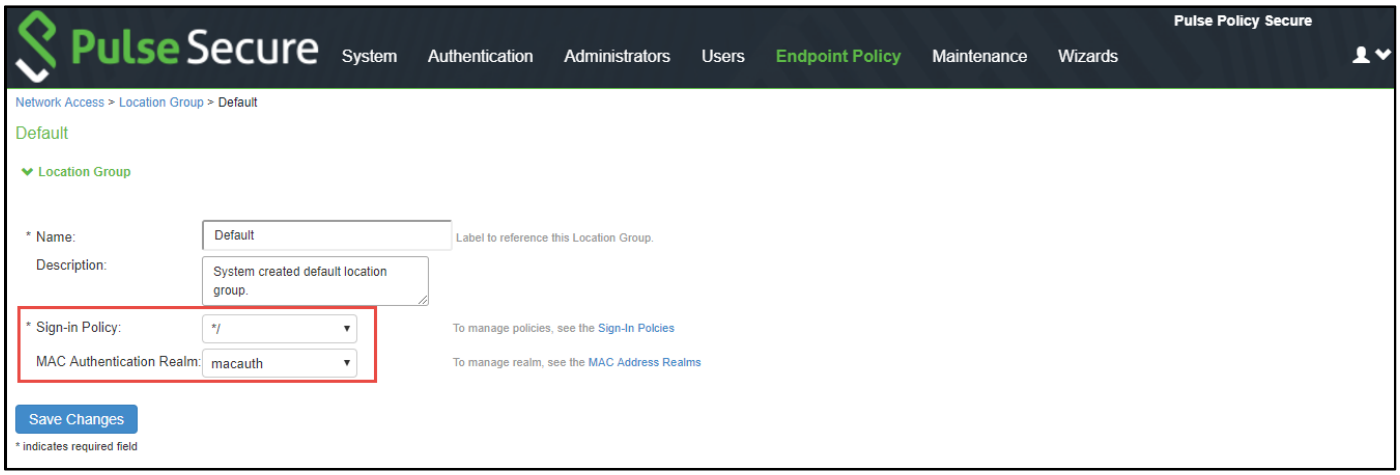
Once the role mapping roles are configured the following screen is displayed.

Figure 13: Role Mapping Rule



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).

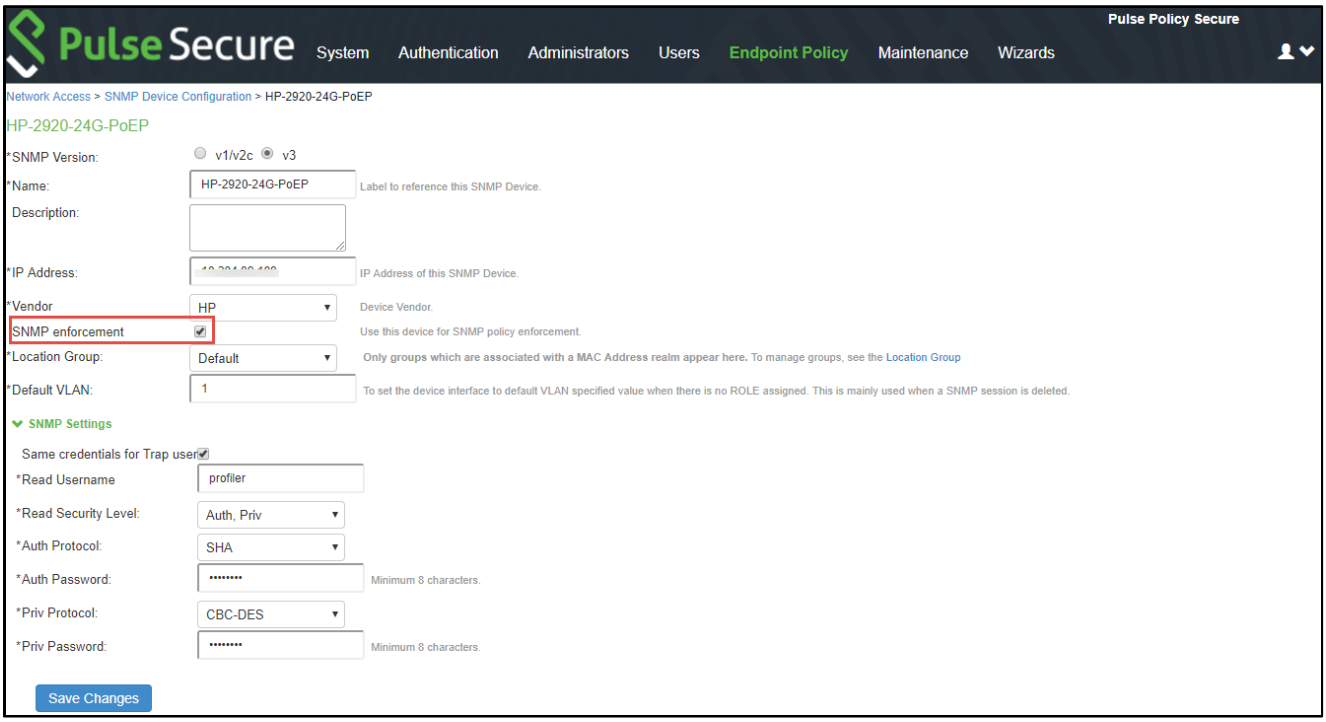
Figure 14: Location Group



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**.

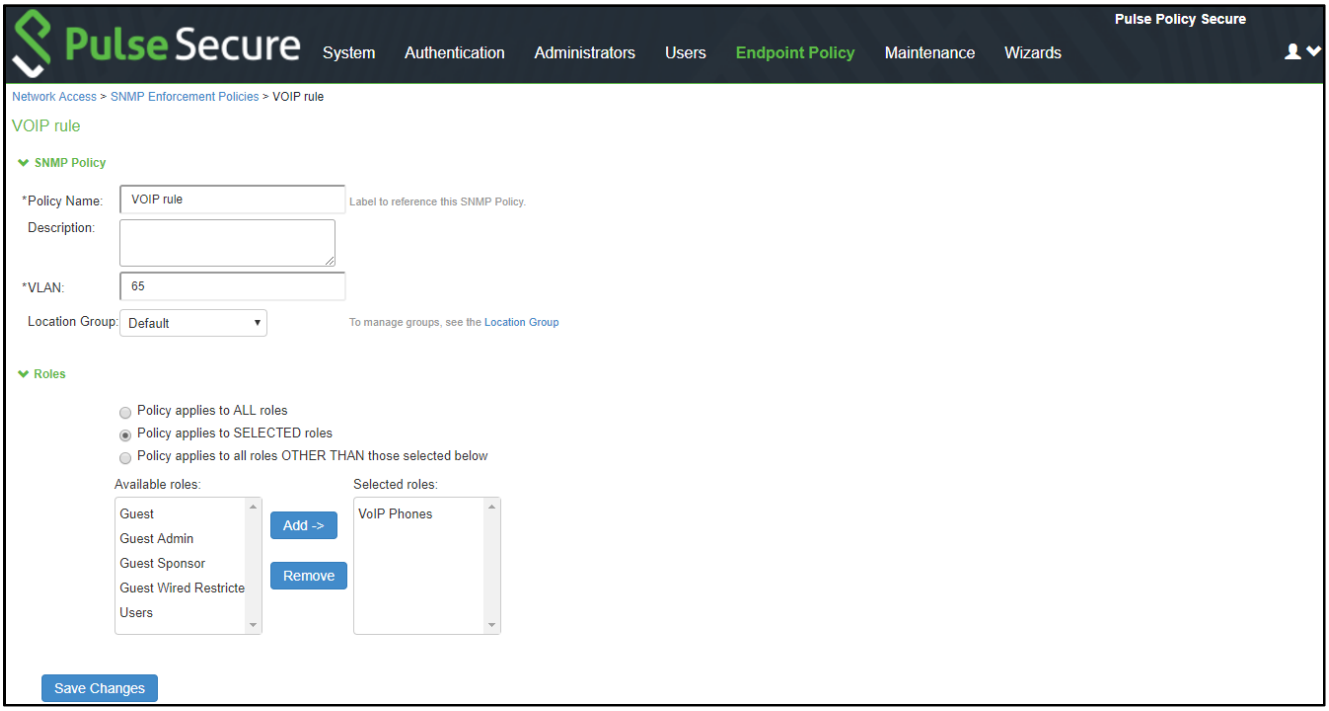
Figure 15: SNMP client



c. Define the SNMP enforcement policy. Select Endpoint Policy **> Network Access > SNMP Enforcement Policies**. Click **New Policy**.

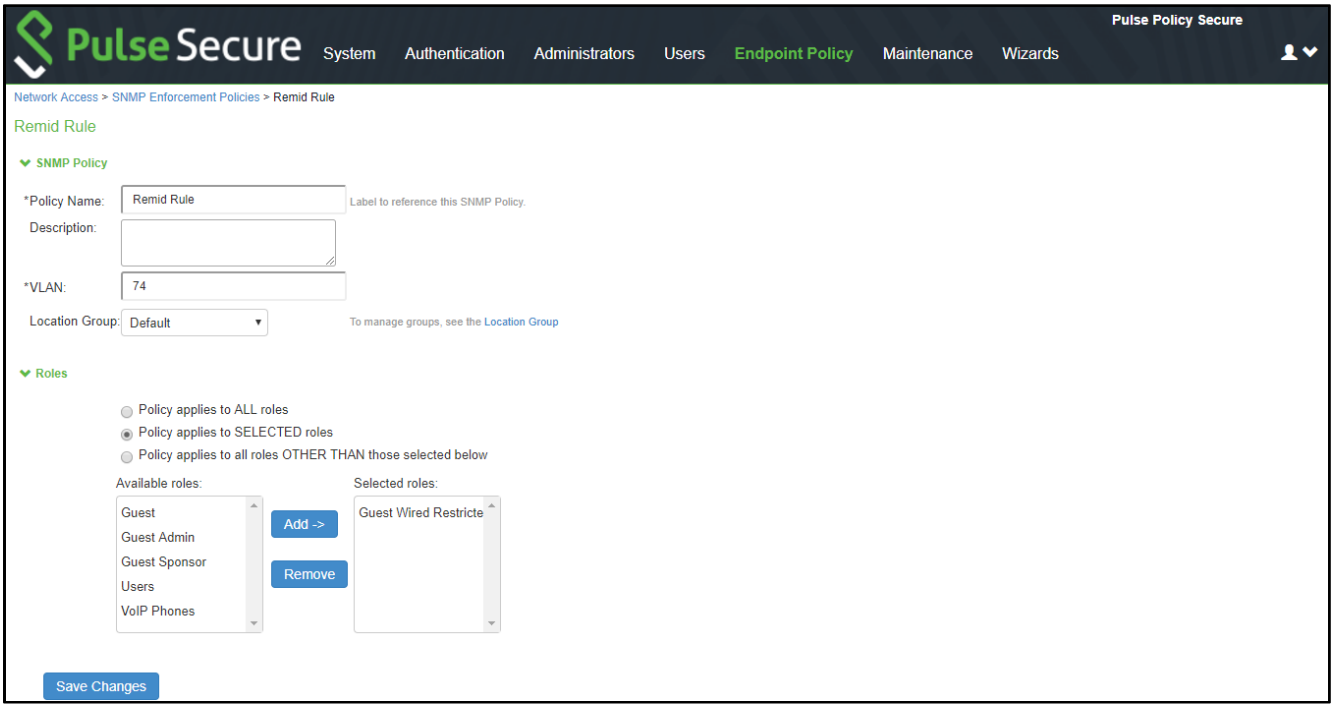
For example, Define an SNMP enforcement policy for moving VoIP Phones to the appropriate VLAN.

Figure 16: SNMP Enforcement Policy1



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

Figure 17: SNMP Enforcement Policy2

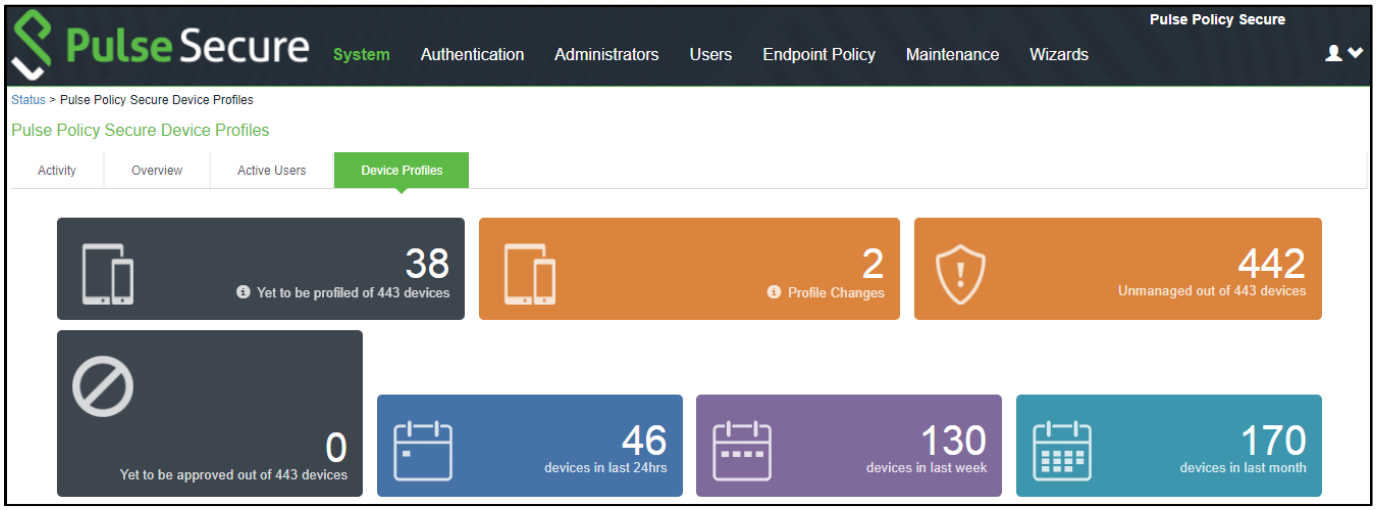


Conclusion

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

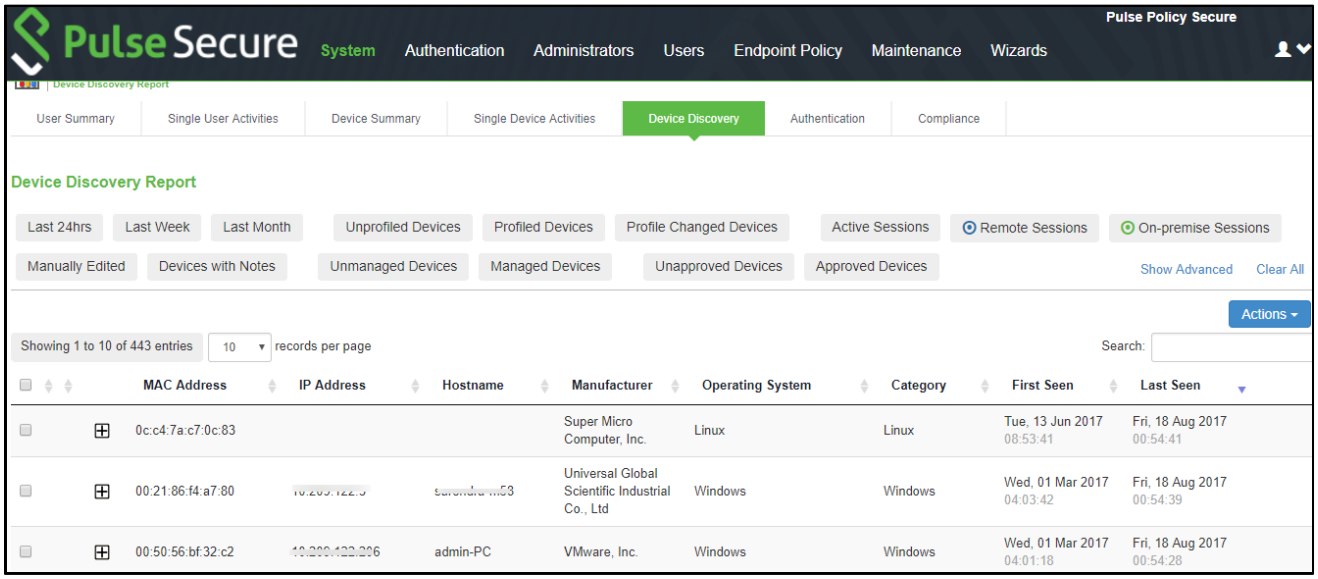
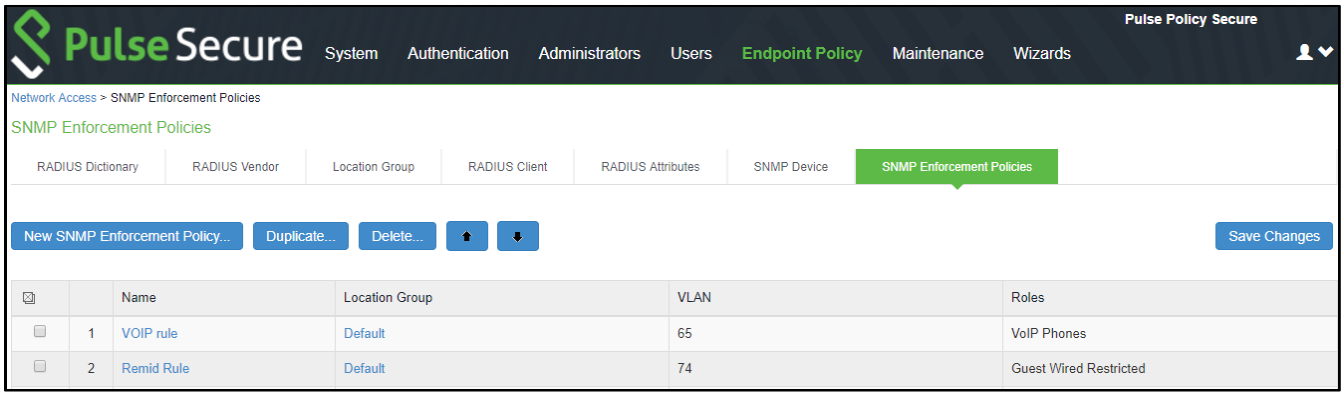
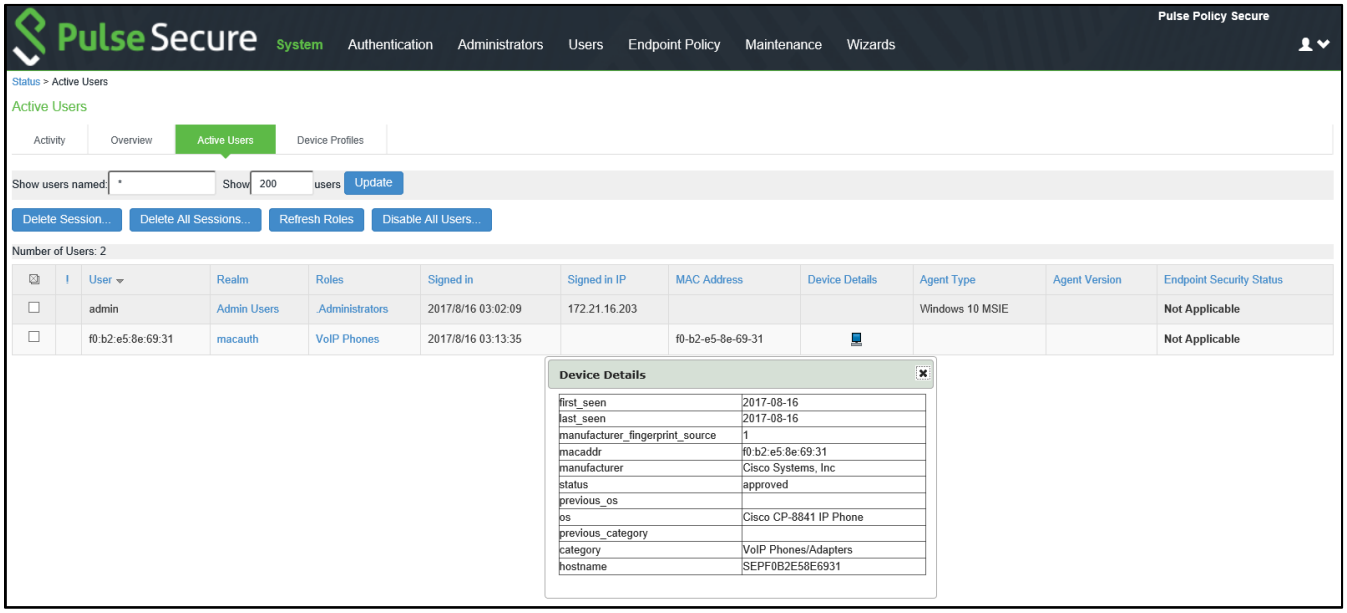


Figure 20: SNMP Enforcement Policies



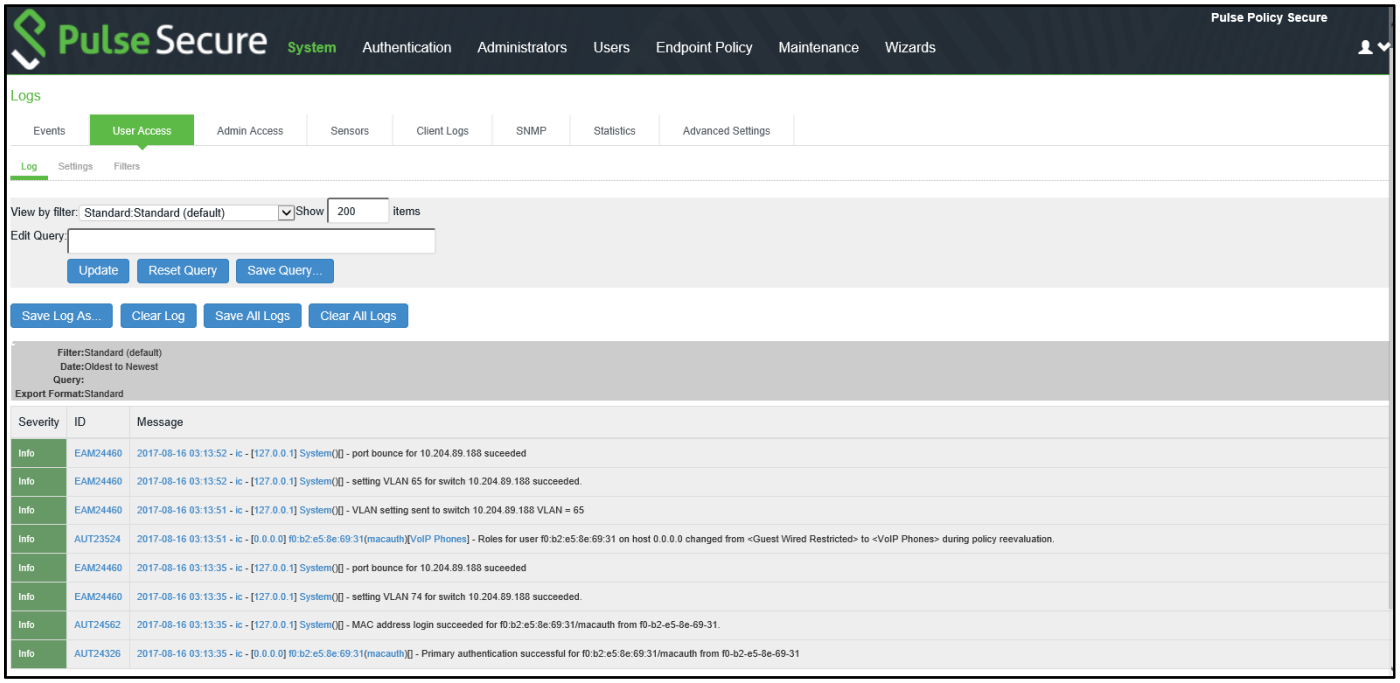
You can verify the active users table to view the session details of the user.

Figure 21: Active Users



For troubleshooting you can verify the user access logs.

Figure 22: User Access Logs



You can also verify the event logs.

Figure 23: Event Logs