Pulse Policy Secure Profiler: Deployment Guide

Published April 2020

Document Version 1.5

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2020 by Pulse Secure, LLC. All rights reserved.

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.

Pulse Policy Secure Profiler: Deployment 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 http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

INTRODUCTION 1

DOWNLOAD AND INSTALL PROFILER LICENSE 3

SWITCH CONFIGURATION 5
- FORWARDING DHCP REQUESTS TO PPS 5
- SWITCH CONFIGURATION FOR CDP/LLDP 5
- SWITCH CONFIGURATION FOR SNMP TRAPS 5
- CONFIGURING THE PROFILER TO WORK WITH RSPAN CONFIGURATION 5

WIRELESS LAN CONTROLLER (WLC) CONFIGURATION 7
- FORWARDING HTTP USER AGENT TO PPS 7

PPS CONFIGURATION (LOCAL PROFILER) 9
- CONFIGURING SNMP DEVICES 9
- CONFIGURING THE LOCAL PROFILER AUTHENTICATION SERVER 10
- VIEW DISCOVERED DEVICES 15
  - DASHBOARD VIEW 15
  - DEVICE DISCOVERY REPORT VIEW 16
- CONFIGURING PROFILE GROUPS 17
- CONFIGURING ROLE-MAPPING RULES FOR PROFILED DEVICES 18

PPS/PCS CONFIGURATION (REMOTE PROFILER) 21
- ALLOWING ACCESS TO THE PROFILER 21
- CONFIGURING REMOTE PROFILER AUTHENTICATION SERVER 22
- CONFIGURING ROLE-MAPPING RULES FOR PROFILED DEVICES 23

ADDITIONAL INFORMATION 25
- PROFILER LICENSE 25
- DEVICE DISCOVERY REPORT 25
- DEVICE SPONSORING 26
- EXPORT/IMPORT 28
- DETECTING SPOOF 28

TROUBLESHOOTING 29
- DHCP TEST EXAMPLE 30
- SWITCH DIAGNOSTICS EXAMPLE 30
- NMAP SCAN TEST EXAMPLE 31

© 2020 Pulse Secure, LLC.

Trap Test Example....31
SMTP Test....32

PROFILER LOGS....33

APPENDIX: CONFIGURING CISCO SWITCHES....35
Configure DHCP Forwarding....35
Configure CDP/LLDP....35
Configure SNMP Traps....35
Configure RSPAN....36
Forward HTTP User Agent Data....37

APPENDIX: CONFIGURING JUNIPER SWITCHES....39
Configure DHCP Forwarding....39
Configure LLDP....39
Configure SNMP Traps....39
Configure RSPAN....40

APPENDIX: CONFIGURING HP (PROCURVE) SWITCHES....43
Configure DHCP Forwarding....43
Configure LLDP....43
Configure SNMP Traps....43
Configure RSPAN....43

APPENDIX: CONFIGURING VIPTELA SWITCHES....45
Configure SNMP on Viptela Switch....45
Sample Configuration....45

APPENDIX: PORTS USED FOR PROFILING....47

© 2020 Pulse Secure, LLC.

Introduction

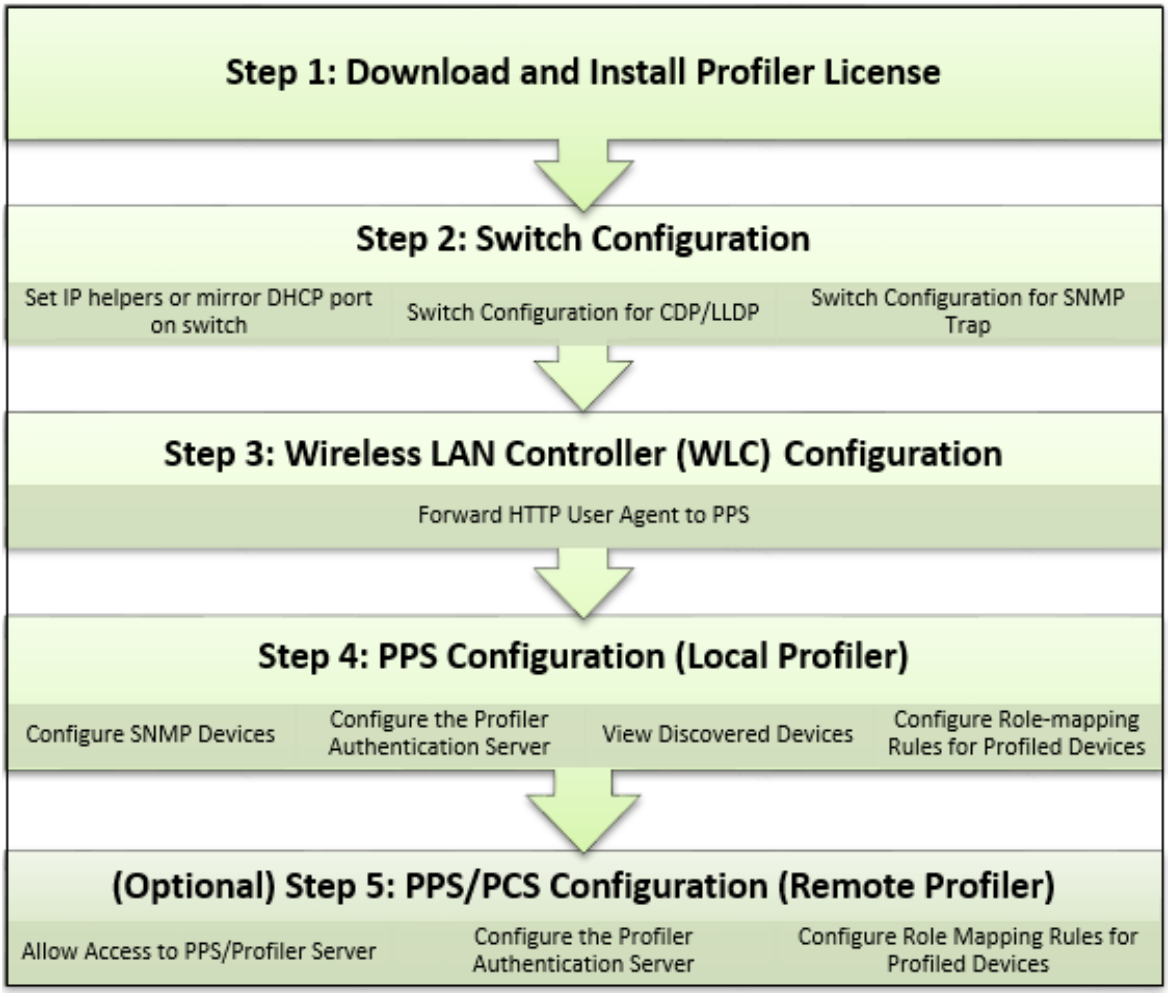
The Profiler dynamically identifies and classifies both managed and unmanaged endpoint devices, enabling control of access to networks and resources based on the type of the device.

Pulse Policy Secure (PPS), an industry recognized network access control (NAC) solution, authenticates users, ensures that endpoints meet security policies, and then dynamically provisions access through an enforcement point (such as a firewall or switch) based on the resulting user session information - including user identity, device type, IP address, and role.

Pulse Policy Secure integrates with the Profiler to provide visibility and control of endpoint devices. This document focuses on how to deploy the Profiler in a network with an existing Policy Secure deployment already configured with the basic elements required to provide network access, including authentication servers, sign-in policies, roles, realms, and SNMP-based enforcement or RADIUS attributes policies for enforcement based on 802.1X / MAC authentication. Please refer to the *PPS Administration Guide* for details.

A high-level overview of the configuration steps needed to set up and run the Profiler is shown in Figure 1. Click each step to directly jump to the related instructions.

Figure 1 Profiler Deployment Process



© 2020 Pulse Secure, LLC.

Glossary

Term	Description
CDP	Cisco Discovery Protocol is a device discovery protocol that runs over Layer 2 (Data link). It allows network management applications to automatically discover and learn about other Cisco devices connected to the network.
Concurrent Users	Total number of users connected to Pulse Connect Secure or Pulse Policy Secure simultaneously.
LLDP	Link Layer Discovery Protocol is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network
Managed Devices	Managed devices can be detected by the MDM or a Pulse Client session is established on the device.
MDM	Mobile device management (MDM) manages the mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices.
Profile	A profile is the combination of the MAC OUI, Category and OS for a device.
Profile Change	A profile change occurs when a device changes its OS or category.
WMI	Windows Management Instrumentation

© 2020 Pulse Secure, LLC.

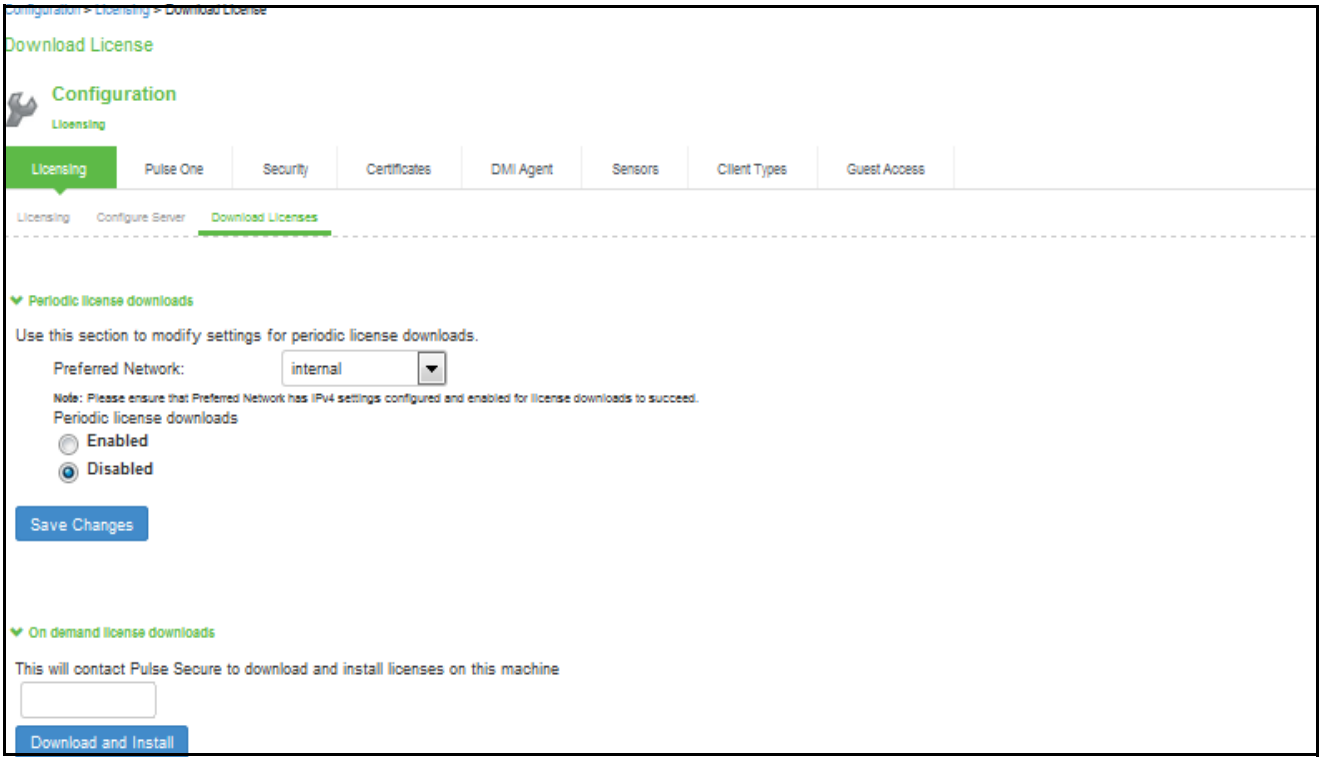
Download and Install Profiler License

From Profiler v1.3 onwards, new license SKUs are available for customers on Pulse Secure license portal, for example, PSPROFILERLG SKU. The Profiler SKUs are device count based licenses. For more information, see "Profiler License" on page 25

To obtain and install the Profiler license:

1. Select **System > Configuration > Licensing > Download Licenses**.
2. Under **On demand license downloads**, enter the authentication code in the text box.
3. Click on **Download and Install**.

   Figure 2 Download and Install License



4. Select the **Licensing** tab to view a list of licenses installed.

   Note: The licensing server does not allow leasing of the Profiler licenses.

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.

Switch Configuration

- Forwarding DHCP Requests to PPS 5
- Switch Configuration for CDP/LLDP 5
- Switch Configuration for SNMP Traps 5
- Configuring the Profiler to Work with RSPAN Configuration 5

The profiler interacts with switches from various vendors. The switch configuration varies for each switch type.

See the following sections for general switch configuration procedures for widely used switches.

- "Appendix: Configuring Cisco Switches" on page 35
- "Appendix: Configuring Juniper Switches" on page 39
- "Appendix: Configuring HP (Procurve) Switches" on page 43

Forwarding DHCP Requests to PPS

To enable DHCP fingerprinting for endpoint classification, one or more edge devices (switches or wireless access points / wireless LAN controllers) need to be configured to forward all DHCP packets for each VLAN to the internal interface of the PPS appliance. This enables the on-box Profiler to profile endpoints by parsing the DHCP packets arriving at the PPS appliance.

In some environments, it might be easier to forward DHCP traffic to the Profiler using the SPAN/RSPAN configuration.

Switch Configuration for CDP/LLDP

Profiler can also use CDP/LLDP broadcast messages to profile a device more accurately. CDP/LLDP must be enabled at the switches for this to take place

Switch Configuration for SNMP Traps

The Profiler uses the Link Up/Down and MAC notification traps to:

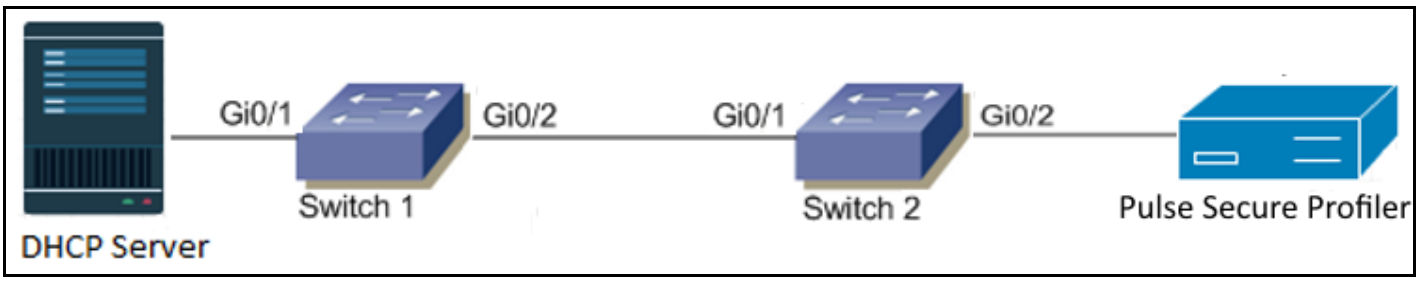
- Profile the device
- Detect if the device is connected to the network

Configuring the Profiler to Work with RSPAN Configuration

Switched Port Analyzer (SPAN) allows you to send a copy of traffic passing through ports to another port on the switch. SPAN is important to mirror the traffic received or transmitted (or both) on one or more source ports to a destination port for analysis, such as to the Profiler. When Profiler receives the traffic, it filters out the DHCP packets and uses them for profiling devices. While SPAN mirrors ports in the same switch, RSPAN (Remote SPAN) mirrors ports on one switch to a port on different switch.

© 2020 Pulse Secure, LLC.

Figure 3 RSPAN Sample Configuration



The incoming traffic passing through port Gi0/1 on Switch 1 will be mirrored to port Gi0/2 on Switch 2 and captured by the Profiler on PPS connected to port Gi0/2.

© 2020 Pulse Secure, LLC.

Wireless LAN Controller (WLC) Configuration

Forwarding HTTP User Agent to PPS

The Profiler can also profile devices using HTTP User Agent data. This is especially helpful for classifying mobile devices since the HTTP User Agent received from such devices contains granular information about the operating systems / OS versions running on the devices.

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.

PPS Configuration (Local Profiler)

- Configuring SNMP Devices 9
- Configuring the Local Profiler Authentication Server 10
- View Discovered Devices 15
- Configuring Profile Groups 17
- Configuring Role-Mapping Rules for Profiled Devices 18

Configuring SNMP Devices

While DHCP fingerprinting is useful for endpoints with a DHCP-assigned IP address, it cannot detect devices that have been assigned static IP addresses. The Profiler can detect statically addressed endpoints by fetching the ARP/CAM table from switches using SNMP. Endpoints detected through SNMP may be profiled using Nmap.

Steps to configure SNMP polling of switches are shown below.

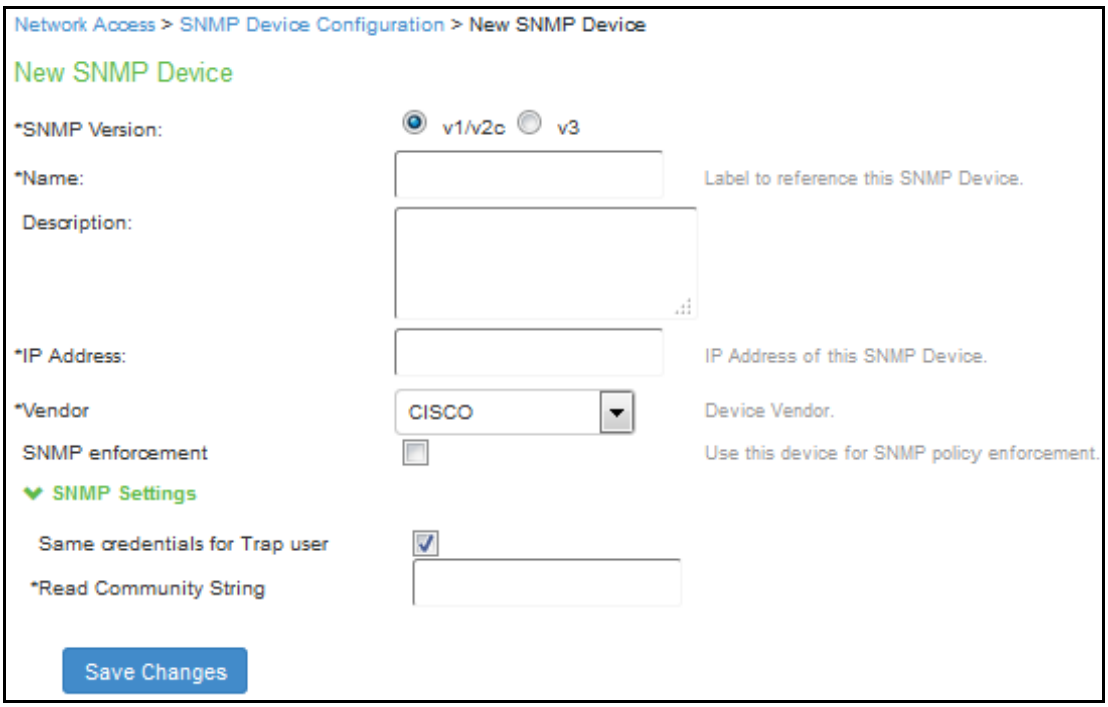
1. Select **Endpoint Policy > Network Access > SNMP Device > Configuration > New SNMP Device** and add one or more switches.
   If you wish to use the switch from HP or Cisco for profiling endpoints only, do not select the **SNMP Enforcement** check box. Leave it checked if you wish to also use the switch to enforce policy.

   Note: If you wish to use SNMP enforcement, configure Location Group to add an SNMP device. For Location Group configuration instructions, refer PPS Administration Guide.

   Note: Standard Switch in the Vendor list allows the Profiler administrator to add any switch that is not listed under the **Switch Vendors** drop down list. This will provide visibility into the devices connected to the switch, but SNMP enforcement cannot be carried out on that switch.

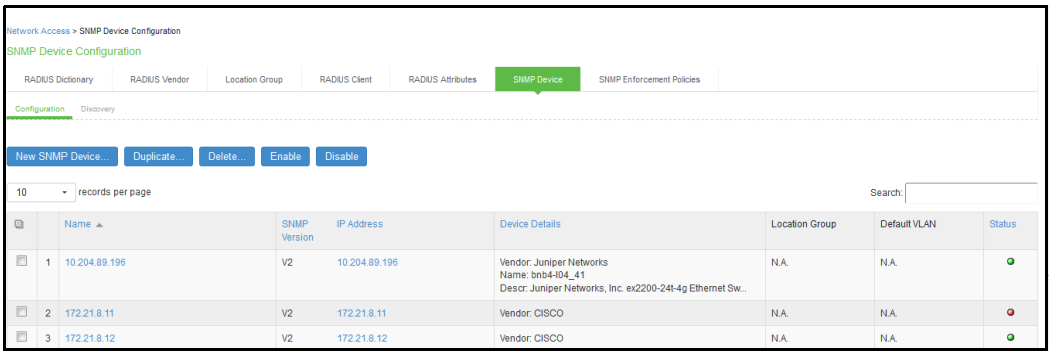
© 2020 Pulse Secure, LLC.

Figure 4 Configuring New SNMP Device



2. Save the changes. The SNMP Device Configuration table is updated.

Figure 5 SNMP Device Configuration Table



You can also discover an SNMP device and add to SNMP Device Configuration table from the **Discovery** tab. See the PPS Policy Enforcement Using SNMP Deployment Guide for additional SNMP switch configuration details.

Configuring the Local Profiler Authentication Server

Ensure the following tasks are performed before proceeding with the Profiler Authentication server configuration.

- If you wish to use DHCP fingerprinting, you have configured the switch(es) to forward DHCP packets to the PPS.
- If you wish to use SNMP/SSH-based profiling from Network Infrastructure Devices, you have configured one or more switches in the Network Infrastructure Device page of the PPS Administrator User.

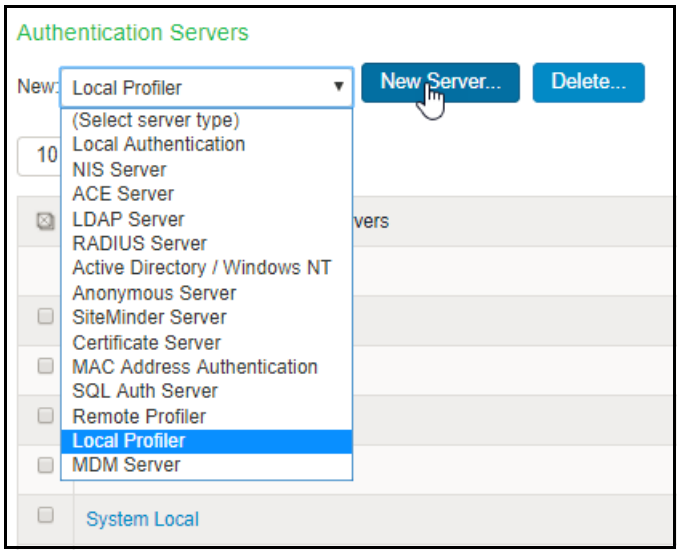
© 2020 Pulse Secure, LLC.

- You have downloaded the latest device fingerprints package from the support portal.

To create a new Local Profiler Authentication Server:

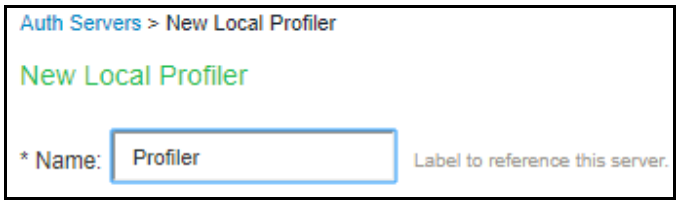
1. Select **Authentication > Auth.Servers**.
2. Select **Local Profiler** from the server type drop-down list and click **New Server**.

   Figure 6 Creating a Local Profiler Authentication Server



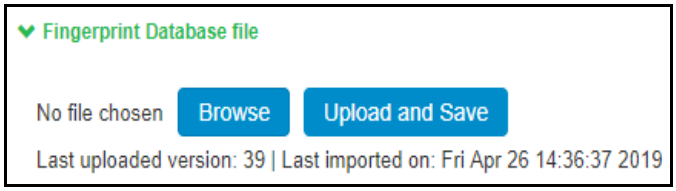
3. Enter a name for the Authentication server.

   Figure 7 Naming a Local Profiler Authentication Server



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

   Figure 8 Uploading Device Fingerprints Package



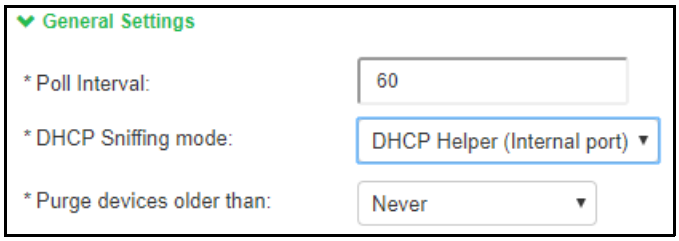
5. (Optional) The SNMP/SSH scan for Network Infrastructure Devices would trigger and look for connected endpoints after a predefined Poll interval.

- Set SNMP Poll interval, if any Network Infrastructure Devices are configured. By default, the poll interval is set as 60 minutes.
- Select the DHCP forward mode. RSPAN for external ports and DHCP Helper for internal ports.

© 2020 Pulse Secure, LLC.

- Select the interval to purge older devices from the database periodically. By default, the interval is set to Never.

Figure 9 General Settings

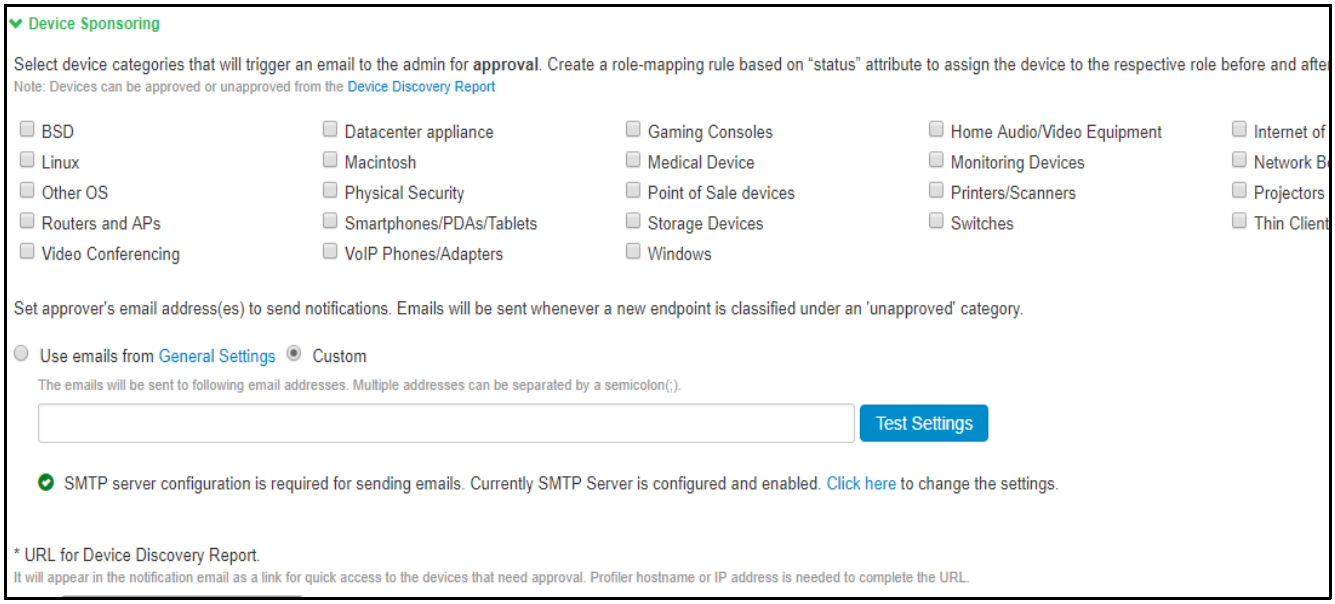


6. (Optional) Select device categories which trigger e-mail(s) to the administrator for approval. Also create a role-mapping rule based on **status** attribute to assign the device to the respective role before and after approval. For more information see, "Device Sponsoring" on page 25.

   Select **Use emails from General Settings** to send e-mails to address specified in General Settings or select **Custom** and enter the e-mail addresses separated by semicolon.

   Enter the Profiler hostname or IP address to fill the URL. This link in the e-mail notification allows to quickly to access the Device Discovery Report and take appropriate action for devices that require approval.

Figure 10 Device Sponsoring

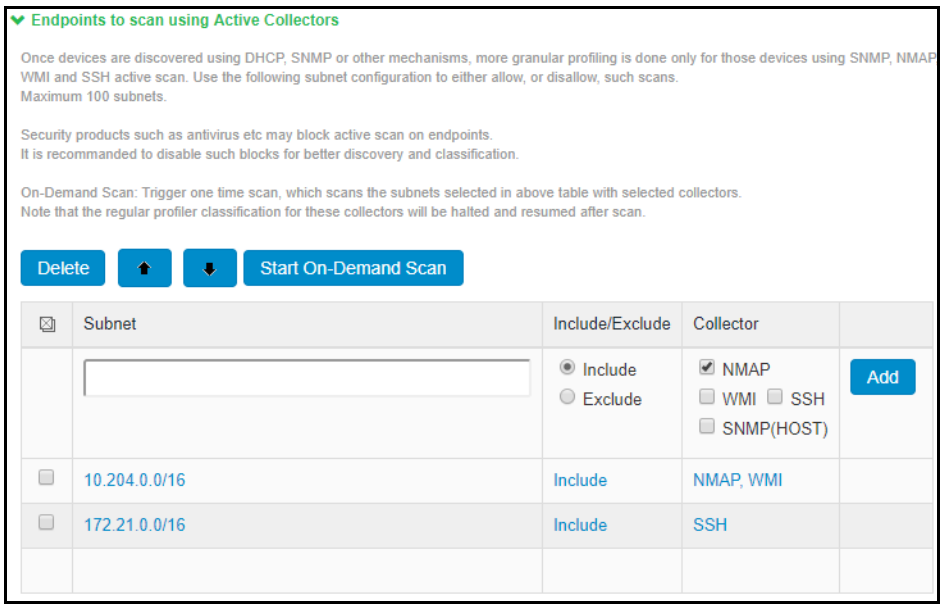


7. (Optional) Upon device discovery, using DHCP, SNMP or other mechanisms, granular profiling is performed on devices using various active collectors. Add one or more subnets which are included or excluded for collectors like SSH, WMI, SNMP (HOST), and NMAP. Maximum 100 subnets configuration are supported.

   On-Demand Scan can be triggered anytime on the subnets for selected collectors.

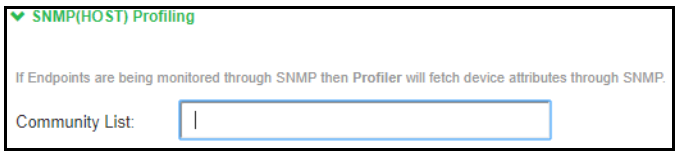
© 2020 Pulse Secure, LLC.

Figure 11 Adding One or More Subnets



8. (Optional) In the SNMP (HOST) Profiling section, enter the possible names, separated by commas, for the community list for the endpoints monitored through SNMP.

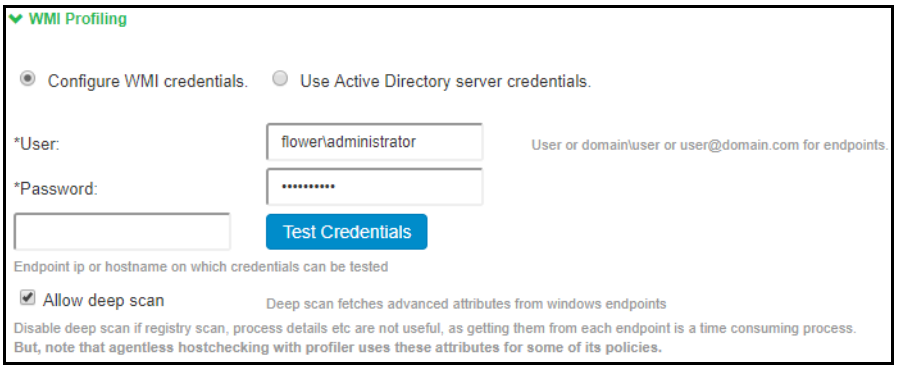
Figure 12 Community List



9. (Optional) In the WMI profiling section, select **Configure WMI credentials** and specify the domain administrator or user with administrator credentials to fetch accurate endpoint information from remote desktops running Microsoft Windows. Select **Use Active Directory server credentials** to use existing Active Directory server credentials.

   Select **Allow deep scan** to control the level of information to fetch from the Endpoint remotely through WMI. Deep Scan includes information on ports, process, and security product details such as product version, signature version, signature date attributes. This option is required if Agentless Host checker with Profiler policies are configured for endpoint posture assessment.

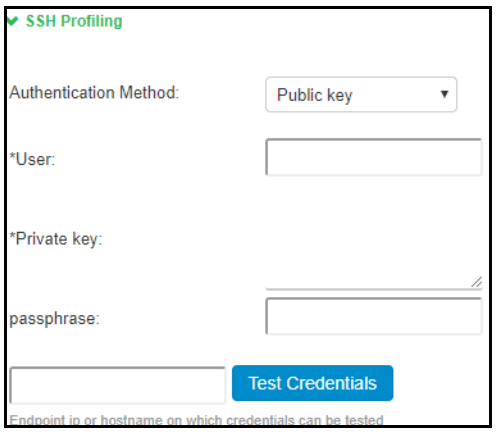
Figure 13 WMI Profiling



© 2020 Pulse Secure, LLC.

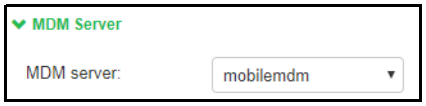
10. (Optional) In the SSH Profiling section, select the **Authentication Method** and enter credentials as applicable. Enter the Endpoint IP or hostname to test the credentials.

    Figure 14 SSH Profiling



11. (Optional) Specify the existing MDM authentication server for accurate profiling of mobile devices which are registered through MDM providers.

    Figure 15 MDM Server

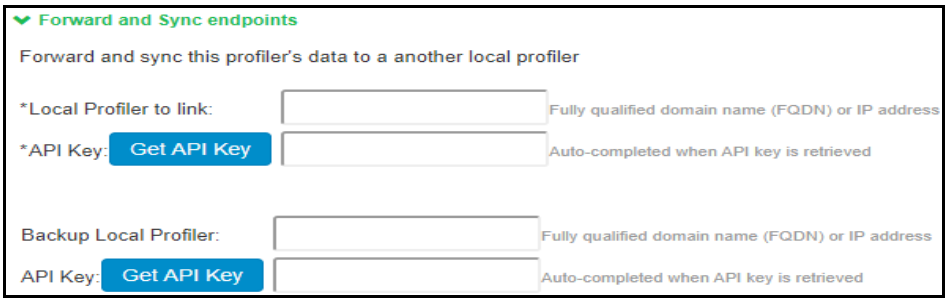


12. (Optional) Select one of the configured LDAP servers where device information is stored.

    Figure 16 LDAP Server

13. (Optional) In the Forward and Sync endpoints section, enter the FQDN or the IP address of the linking local profiler and the backup profiler. Enter the API key, or click **Get API Key** and enter the administrator credentials of the remote profiler to retrieve and auto fill the API Key.

    Figure 17 Forward and Sync endpoints



14. Click **Save Changes** to save the configuration settings.

Devices that are discovered are profiled and updated in the Device Discovery Table and an overall summary is shown in the "Dashboard View" on page 15

The devices can be grouped based on group name and rules using device attributes. For more information see, "Configuring Profile Groups" on page 17

© 2020 Pulse Secure, LLC.

View Discovered Devices

Dashboard View

Once the Profiler is configured by following the steps mentioned above, profiling starts in the background. Devices that are discovered are profiled and updated in the Device Discovery Table and an overall summary is shown in the Device Profiles Dashboard.

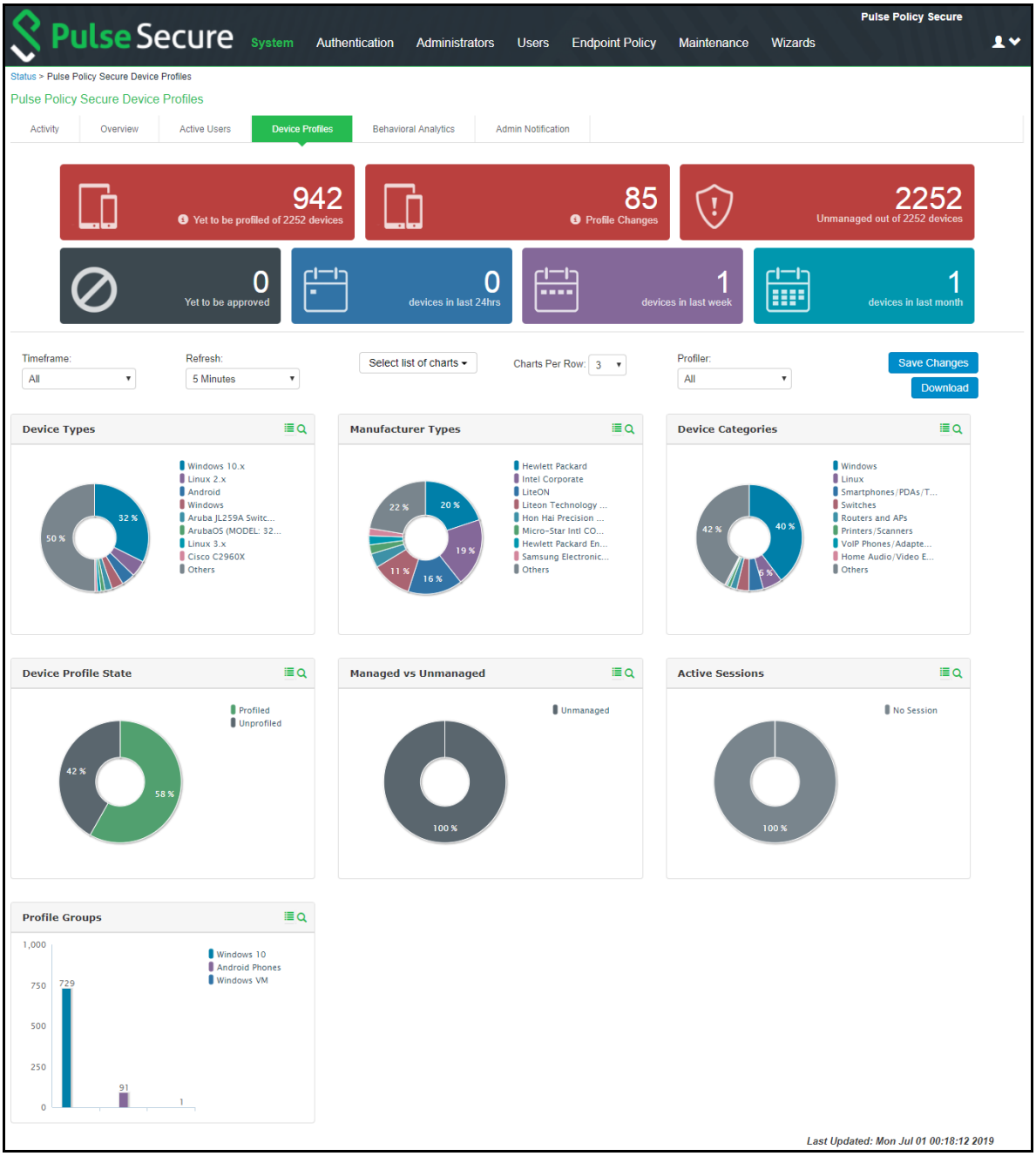
To view discovered devices through the Pulse Policy Secure dashboard:

1. Select **System > Status > Activity > Device Profiles.**
1. Set the desired timeframe. Choose 24 hours, 7 days or 30 days.
1. See the following charts:

- Device Profile State
- Manufacturer Types
- Device Categories
- Device Types
- Managed vs Unmanaged
- Active Sessions
- Profile Groups

© 2020 Pulse Secure, LLC.

Figure 18 Dashboard View



Device Discovery Report View

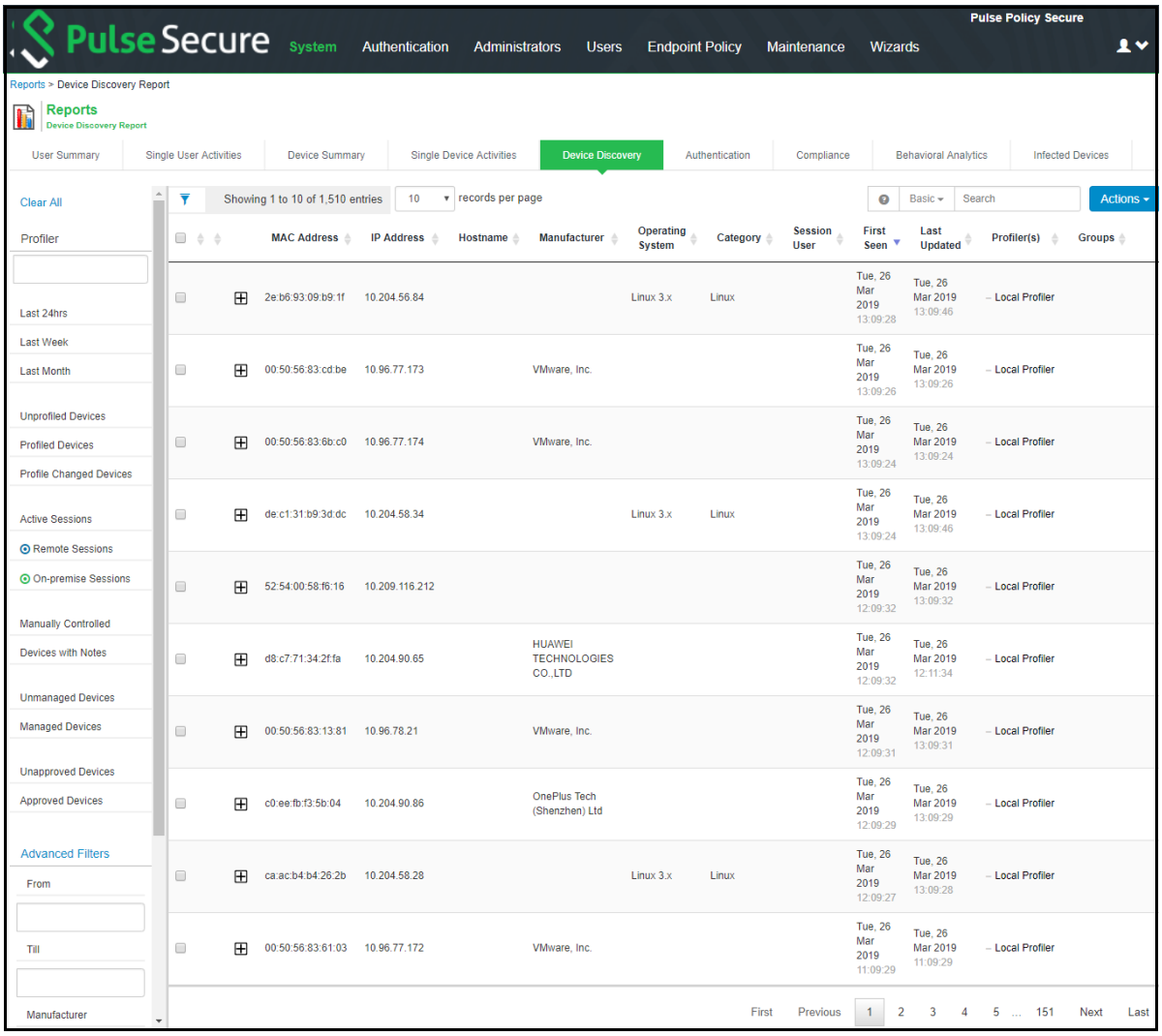
The Device Discovery Report Table contains the list of devices that are discovered in the network.

This report allows to add, modify and delete the endpoints. For more information, see “Device Discovery Report” on page 25

© 2020 Pulse Secure, LLC.

1. Select **System > Reports > Device Discovery** to bring up the table.

Figure 19 Device Discovery Report Table



Configuring Profile Groups

The devices can be grouped based on group name and rules for easy access and identification. Group names can be used in role mapping rules, resource policies, filtering etc.

1. Select the Profiler server under **Authentication à Auth. Servers.**
2. Select **Profile Groups** tab, select the **New Profile Group** and enter the Group Name and Rule.: The rules can be written with device attributes and suggested operators can be chosen from the list. As an optional step, emails also can be configured which results in notifications for any group related changes.
   To create rules for all values including null, use the format: rule: category ="*" or category ="".
3. Click **Save**.

© 2020 Pulse Secure, LLC.

Note: Updating the profile groups for existing devices may take time if a rule covers more devices. Navigating away from the page cancels the update for the existing devices. But, the group names are updated when the device receive updates during regular profiling.

Configuring Role-Mapping Rules for Profiled Devices

After creating the Local Profiler Authorization Server, you can use device attributes from the Profiler in the role mapping rules for both MAC Authorization and 802.1X realms for policy enforcement.

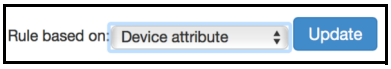
To configure role-mapping rules:

1. Select **Endpoint Policy > MAC Address Realms** (for MAC Authorization realms) or **Users > User Realms** (for 802.1X realms)
2. Select the realm name.
3. Select the Local Profiler Authentication Server as Device Attributes Server.

   Figure 20 Device Attributes

4. Click the **Role Mapping** tab.
5. Click **New Rule**.
6. Set **Rule based on** to "Device Attribute" and click **Update**.

   Figure 21 Rule based on attribute



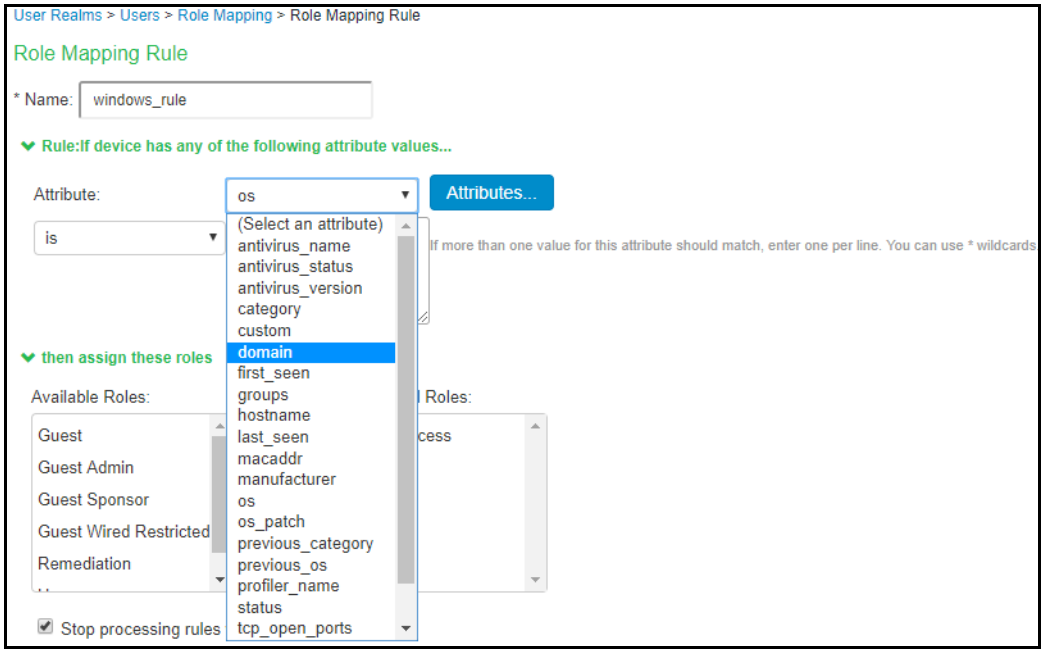
   Note: If a rule exists, then the Rule based on drop-down will not appear.

7. Enter a name for the rule (if creating a new one).
8. Create the new role mapping rules.

© 2020 Pulse Secure, LLC.

a. Select the attributes based on the new device attributes that are now available in the attributes drop-down field. When setting the attribute value, make sure the value you enter is an exact match for the value displayed in the Device Discovery Report table. Wildcards (* and ?) can be used in the attribute value.

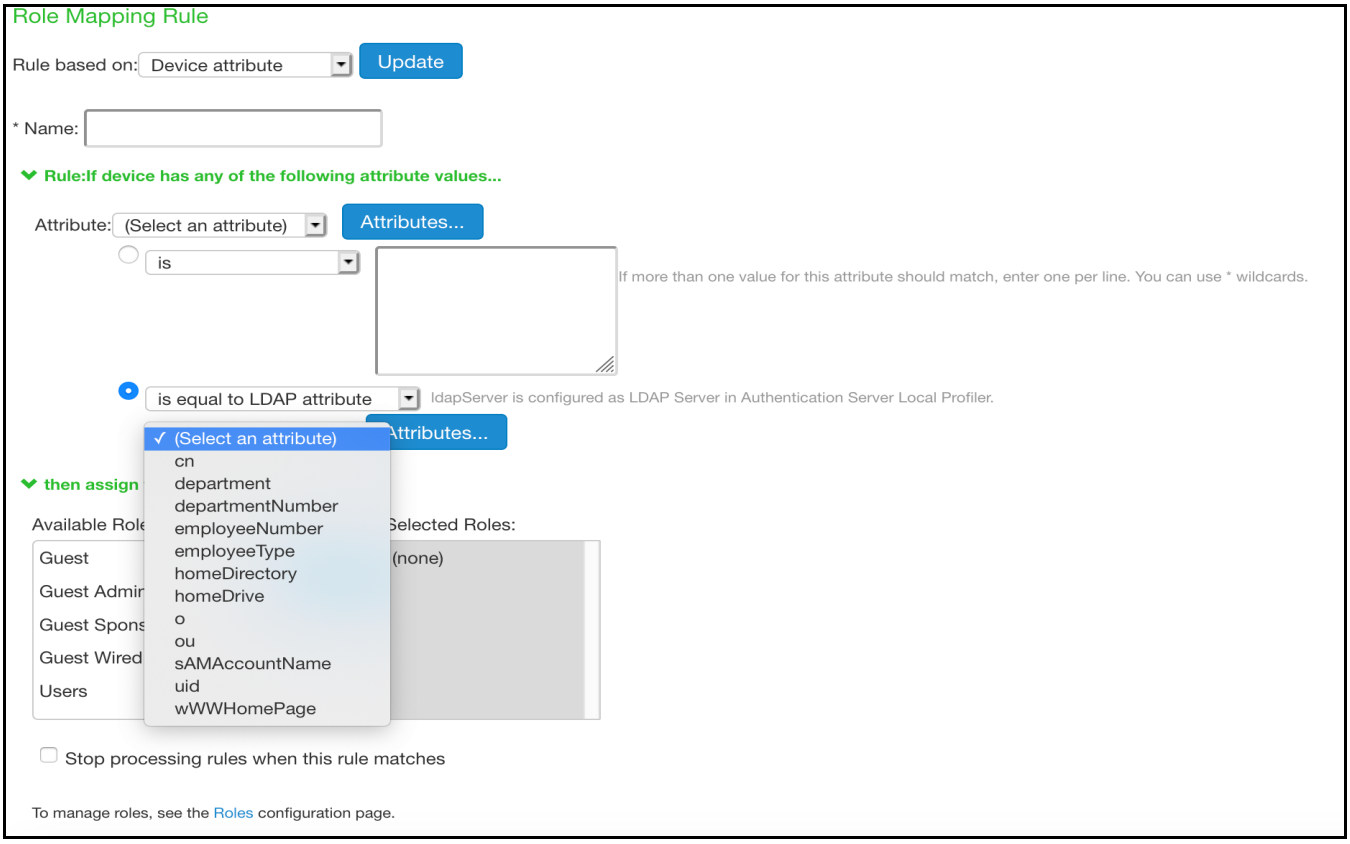
Figure 22 Creating New Role Mapping Rule



b. If LADAP server is configured in profiler, select the LDAP attribute from the list or click **Attributes to** create new LDAP attributes.

© 2020 Pulse Secure, LLC.

Figure 23 Creating New Role Mapping Rule with LDAP Attributes



9. Assign the roles and click **Save Changes**.

Note: Role mapping rules in the MAC authorization realm apply to both MAC-RADIUS enforcements in an 802.1X environment and SNMP-based enforcement.

© 2020 Pulse Secure, LLC.

PPS/PCS Configuration (Remote Profiler)

This configuration procedure is optional.

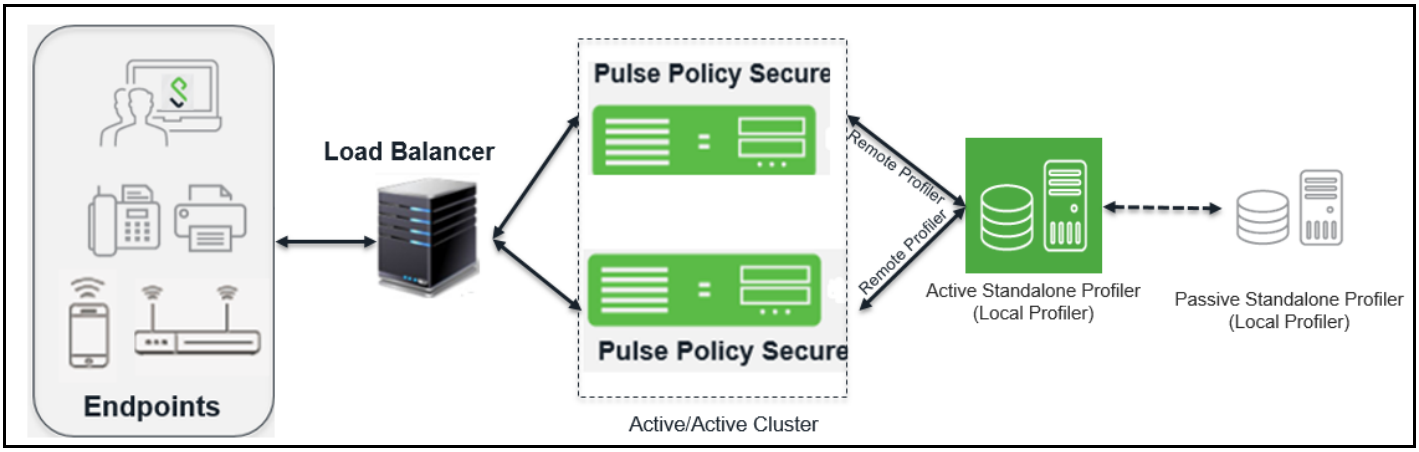
A Remote Profiler can be useful in the following cases:

You want to profile devices that are outside the enterprise network and connected via PCS.

You have an active/active cluster (or multiple un-clustered set) of PPS appliances.

Note: The Profiler can be deployed in Active/Passive clusters or without clustering.

Figure 24 Example of a Standalone Profiler deployed in a typical Active/Active cluster



When user connects to a remote PCS or PPS and starts a session:

- Information such as hostname and IP address, device IP address and MAC address, session identifier, user-agent are retrieved by the session and sent to the Remote Profiler.
- The Remote Profiler returns Device OS, Device Manufacturer, Device Category and Session Identifier to PPS/PCS.
- The Remote Profiler updates the PCS/PPS session with the device attributes and triggers role re-evaluation.

The following sections describe the steps to configure a Remote Profiler.

Allowing Access to the Profiler

The first step is to allow PCS or PPS to connect to the Remote Profiler:

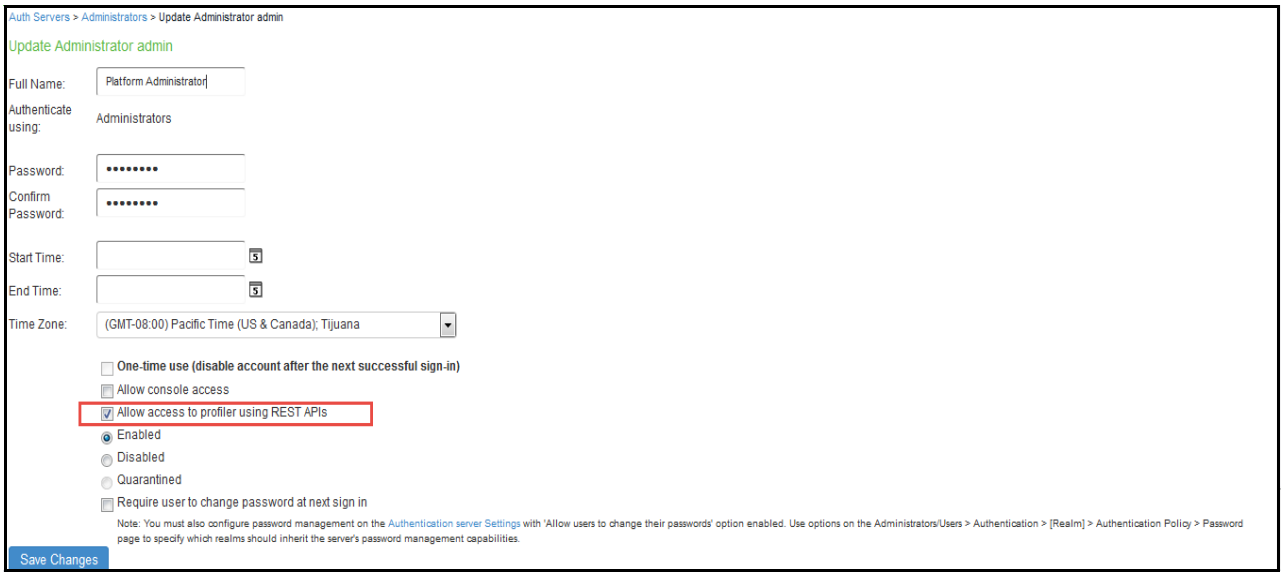
1. Log in to the PPS/PCS
2. Select **Authentication > Auth. Servers**.
3. Click on the **Administrator** link.
4. Select the **Users** tab.

© 2020 Pulse Secure, LLC.

5. Select the corresponding administrator user link, then select **Allow access to the Profiler using REST APIs** and Save Changes.

   Note: REST API access to the Profiler can be enabled only for local administrators.

   Figure 25 Allow Access to the Profiler



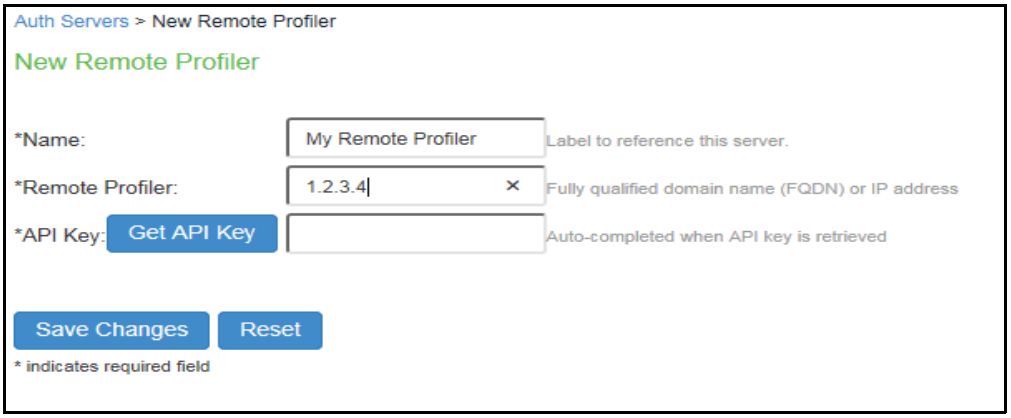
Configuring Remote Profiler Authentication Server

To configure Remote Profiler Authentication Server, follow the procedure "Configuring the Local Profiler Authentication Server" on page 10

1. Select **Authentication > Auth. Servers**.
2. Select **Remote Profiler** from the server type drop-down list and click **New Server**.
3. Enter a name for the Authentication server.
4. Enter the FQDN name or IP address of the PPS appliance where Standalone or Local Profiler is running.

   Note: Do not include http:// or https:// before the IP address.

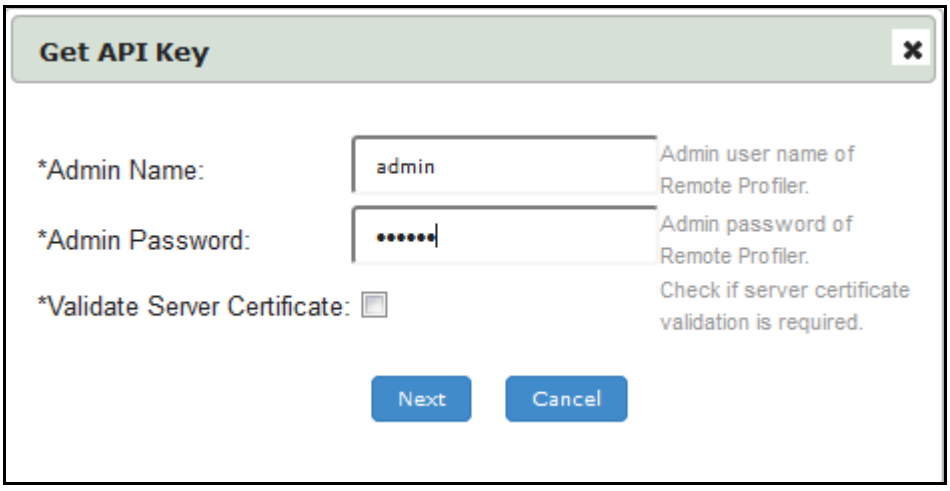
   Figure 26 New Remote Profiler



© 2020 Pulse Secure, LLC.

5. Click the **Get API Key** button to create a new key for secure communication with the Remote Profiler. In the Get API Key window, provide the credentials of valid administrator on PPS/Profiler server (see) and click **Next**. The API key will be generated and displayed in the API Key field.

   Figure 27 Get API Key



   Note:

   - If you already have the API key, you can enter it in the API Key field instead of clicking the **Get API Key** button.
   - If trusted Root CA certificate validation is required, select the **Validate Server Certificate** check box.

6. **Save** changes.

Once created, communication ensues between the PCS or PPS appliance and the Remote Profiler. Device profile data can be viewed in the Device Discovery Report table in the Remote Profiler.

Configuring Role-Mapping Rules for Profiled Devices

After creating the Remote Profiler Authentication Server, you can create role mapping rules based on endpoint profile. Follow the instructions in section "Configuring Role-Mapping Rules for Profiled Devices" on page 23

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.

Additional Information

This section describes more information related to the Profiler.

Profiler License

To enable the Profiler functionality, a new Profiler license SKU needs to be installed.

Upgrading to Profiler v1.3: For Profiler versions prior to v1.3, the profiling stops and a prompt to install the Profiler license appears in the Dashboard and Overview pages. The existing profiled devices are preserved and on installing the Profiler license v1.3, the Profiler automatically starts profiling new devices.

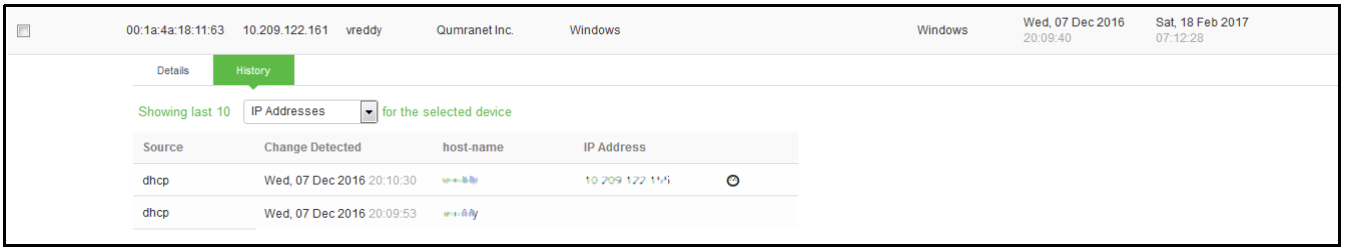
Expiry: Upon expiry of Profiler license or on reaching profiled devices limit, a warning is displayed at the top of Dashboard and Overview pages similar to existing license warnings.

Device Discovery Report

The Device Discovery Report Table Provides additional information about the devices.

- **Endpoint History:** Historical information is displayed in an expanded view based on IP address, sessions (remote, local) or profiles changes.

  Figure 28 History based on IP Address



- **Endpoint Filters:** A list of filters is available for quick analysis of discovered devices.
  - Filters based on time – Last 24 hours, Last week, Last month
  - Filters based on sessions – Active sessions, Remote sessions, On-premise sessions
  - Filters based on actions of the discovered devices – Managed devices, Unmanaged devices, Profiled devices, Approved and unapproved devices, Unprofiled devices, Profile changed devices. Manually edited devices, Devices with Notes

Note: If an endpoint is classified incorrectly, please see the Troubleshooting section to rectify the problem.

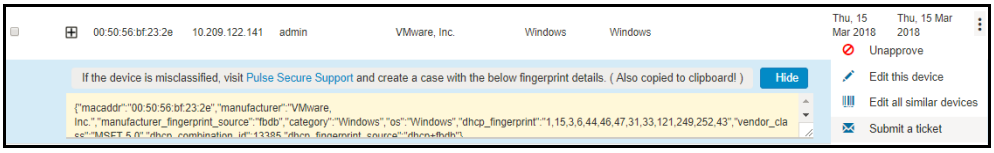
The Device Discovery Report Table allows the following operations for each of the listed devices.

- **Approve/Unapprove:** Each endpoint has an attribute called status and allows to manually approve or unappove a specific device. See Device Sponsoring for more information.

© 2020 Pulse Secure, LLC.

- **Edit**: Allows to edit Manufacturer, Category and Operating System fields. Manually Added or Edited device attributes are auto updated when the classifier updates its attributes. If you want to avoid updates from classifier, select Override any updates by the profiler and use this profile always for the device.
- Edit all similar devices: Allows to edit all similar devices which have same fingerprint. When similar devices are added, the updated fingerprint is used for profiling.
- **Submit a ticket**: The Profiler uses Fingerbank database to classify devices.
  It is possible that some devices are not correctly classified in this process. In such cases, the administrator can use the Copy Fingerprint option to copy the fringerprint and send the relevant information about the wrongly classified device to the Pulse Secure using an E-mail. This information is verified before updating the Custom Fingerprint database.

  Figure 29 Submit a ticket



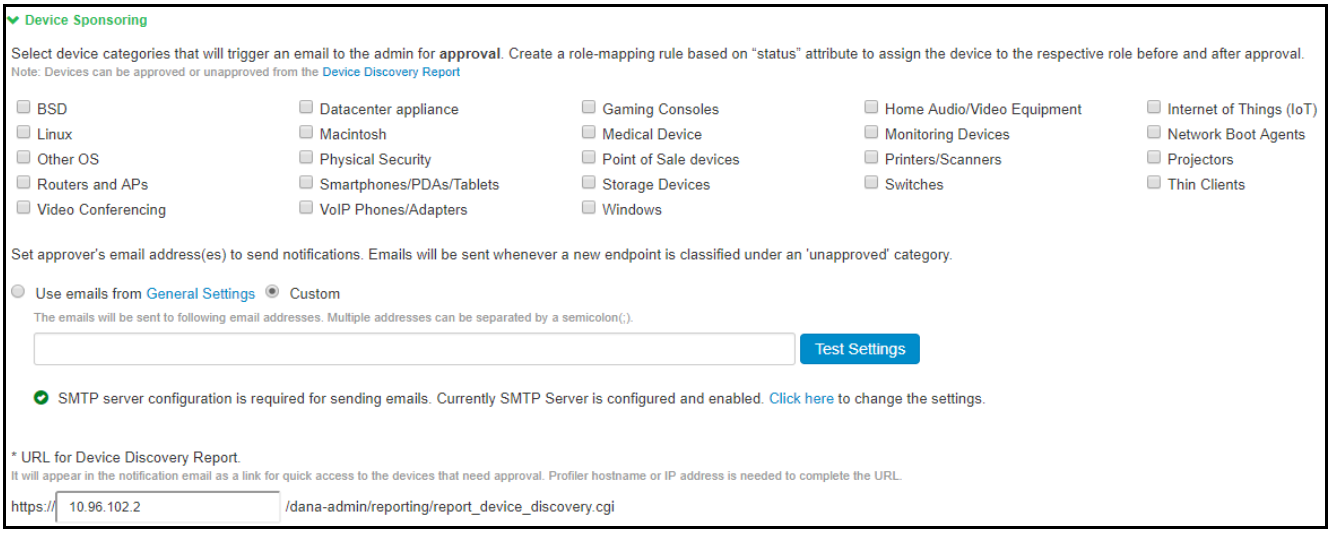
- **Delete**: Allows to delete a device. If the deleted devices are rediscovered by the Profiler, they are again included in the list.

Device Sponsoring

The administrator can sponsor devices that belong to a set of pre-defined categories using the following steps.

1. Select categories that need manual approval.
2. Provide an e-mail address to receive notifications about the changes to the devices.

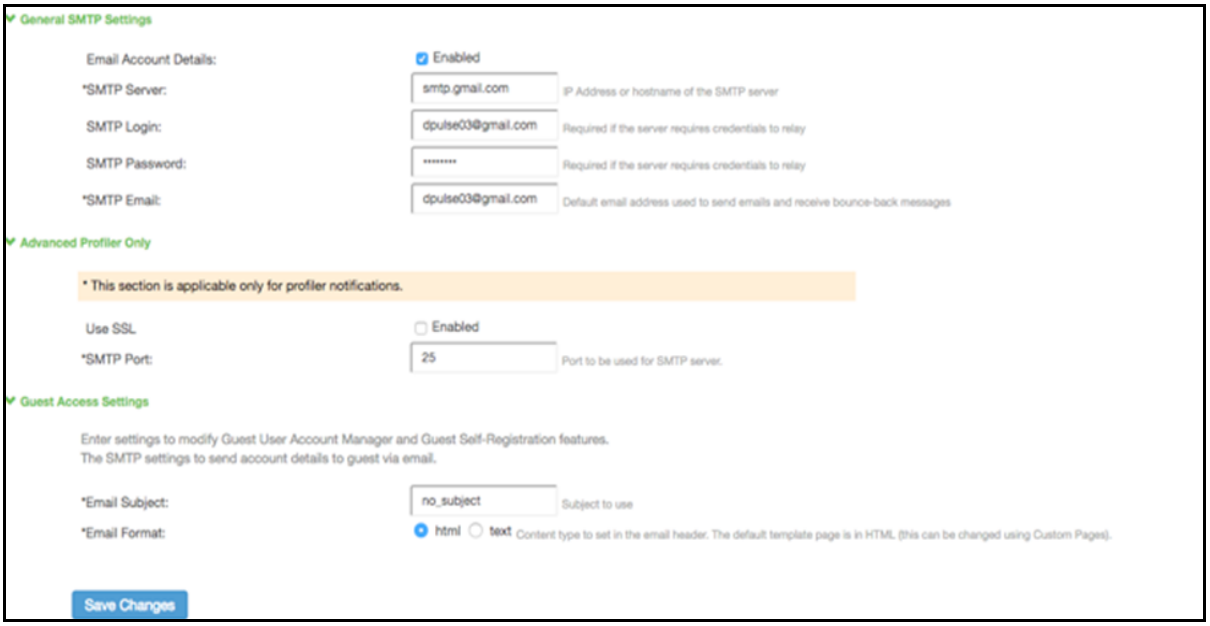
   Figure 30 Device Sponsoring



3. Configure the SMTP server.

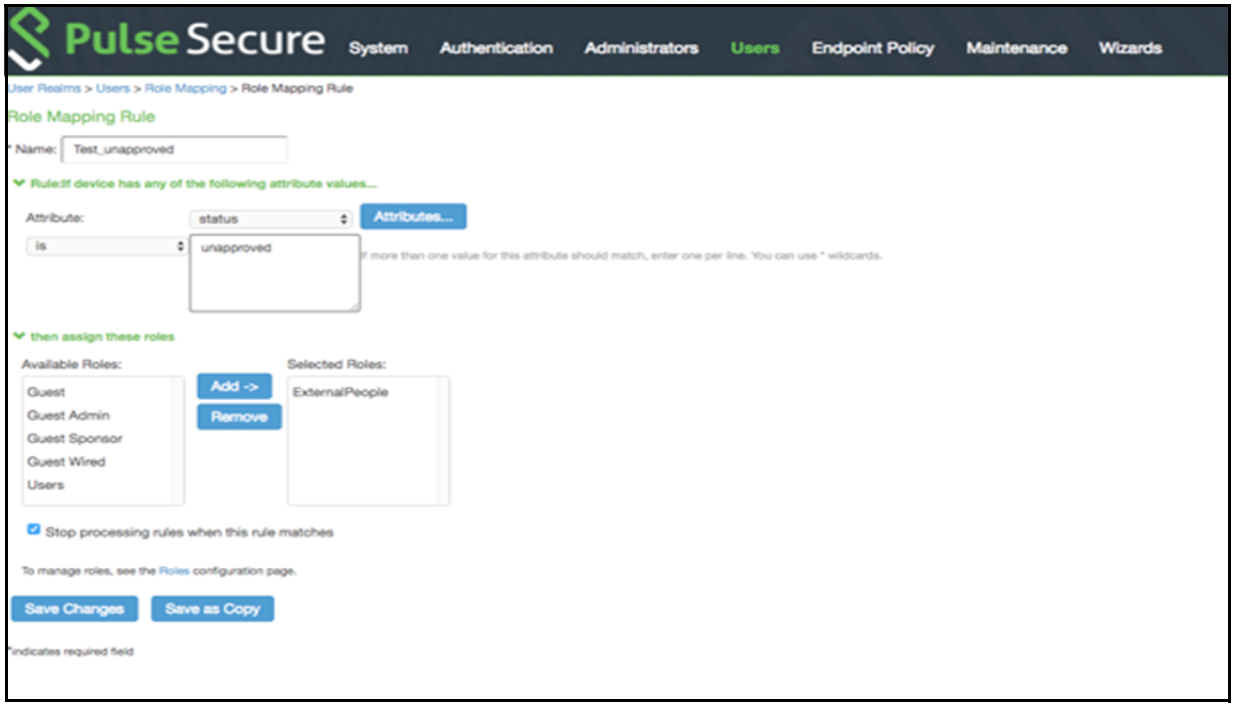
© 2020 Pulse Secure, LLC.

Figure 31 Configuring SMTP Server



4. Write role mapping rule based on attribute **status** such that approved and unapproved devices have correct roles. Use **unapproved** or **approved** as the values in matching the rule.

   Note: If the device is not profiled, there is no status associated with it. To write status based rule for unprofiled and unapproved devices, use rules like `deviceAttr.status != 'approved'`.



5. An e-mail is sent with instructions to approve the devices.

© 2020 Pulse Secure, LLC.

Export/Import

All configuration changes or settings can be exported/imported in XML or binary format. However, the Profiler database and the fingerprint database cannot be exported.

Detecting Spoof

The profiler allows a mechanism to suspect MAC address spoofing, , provided MAC spoofing results in a profile change of the device. Profile change would be indicated by the previous_os and previous_category fields.

For example, MAC address spoofing can be detected if an endpoint was a printer in the stored profile and the latest profile indicates the same device as a Linux endpoint.

To detect spoof for a specific device, use the following Regexp in role mapping rule:

```
deviceAttr.previous_os != ''  AND (deviceAttr.previous_os = 'Cisco VoIP' AND
deviceAttr.os != 'Cisco VoIP')
```

Use the following Regexp, which is common for all Operating Systems:

```
deviceAttr.previous_os != ''  AND (deviceAttr.previous_os != deviceAttr.os)
```

Note: This feature works only when the actual device is profiled with information of OS and categories before spoofed device connects and profiled. Mac spoof suspect might not work when same OS or Category information is identified for original and spoofed device.

© 2020 Pulse Secure, LLC.

Troubleshooting

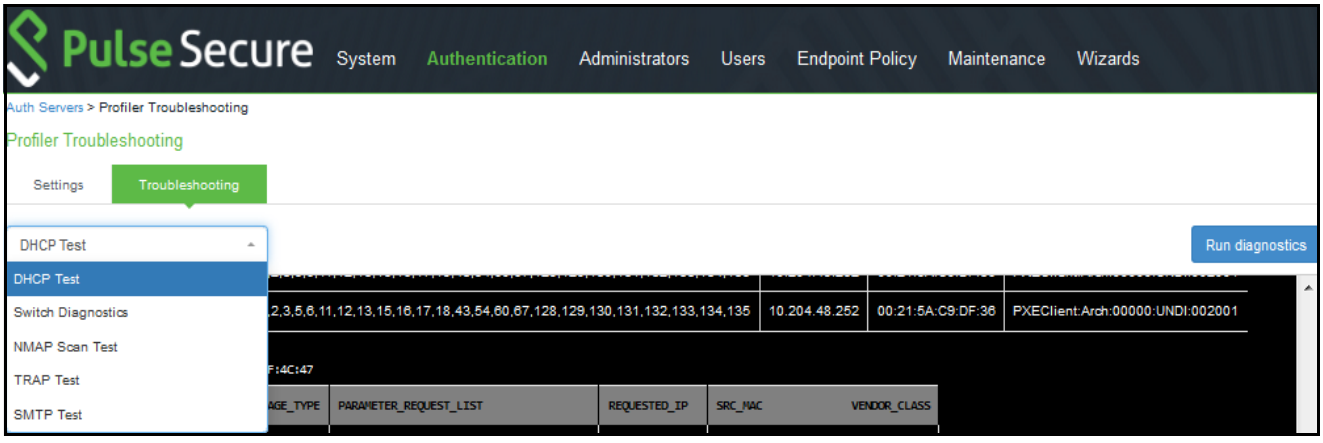
The following tests helps to identify and solve basic problems associated with configurations of the Profiler.

Test	Result
"DHCP Test Example"	• Verify if ports are receiving the DHCP packets. • Detect a device when connected to network during the diagnostic run.
"Switch Diagnostics Example"	• Verify switches are enabled • Check if SNMP walk is successful or not • Check if Profiler can successfully read ARP table, CAM table, and SSID information
SNMP (HOST) Test	• Check if the Profiler can fetch the Endpoint information through SNMP.
"NMAP Scan Test Example"	• Check if NMAP scan is working for an IP address, which is prompted during diagnostic run
"SMTP Test"	• Verify if trap is collected or not for a switch event. • Detect a device when connected to network during the diagnostic run.
"SMTP Test"	• Troubleshoot any problem in configuration/reachability of SMTP server. Device sponsoring is available with email notification feature. It sends an email through configured SMTP server and displays the status.

To execute the tests, perform the following steps:

1. Select **Authentication > Auth Servers > <Profiler page>** and select the **Troubleshooting** tab.
2. From the drop-down list, select **the required test** and click **Run diagnostics**.

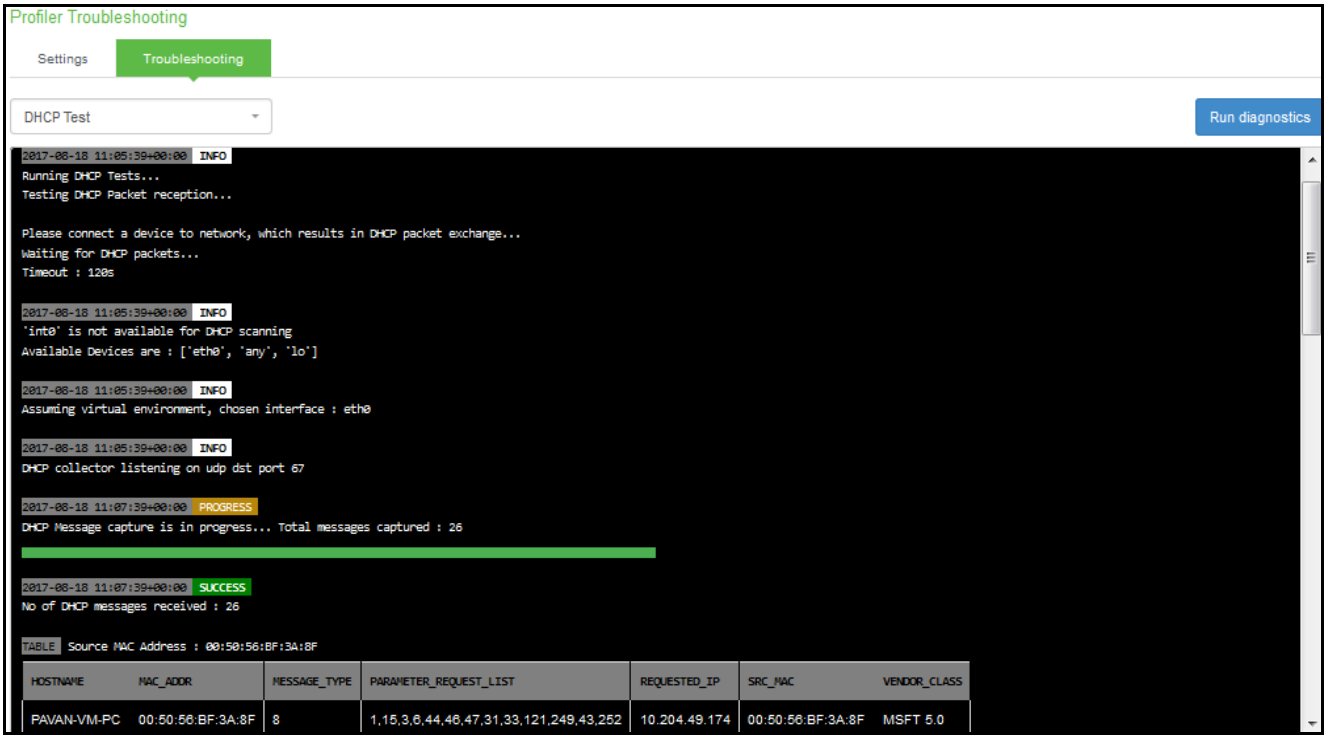
Figure 32 Troubleshooting



© 2020 Pulse Secure, LLC.

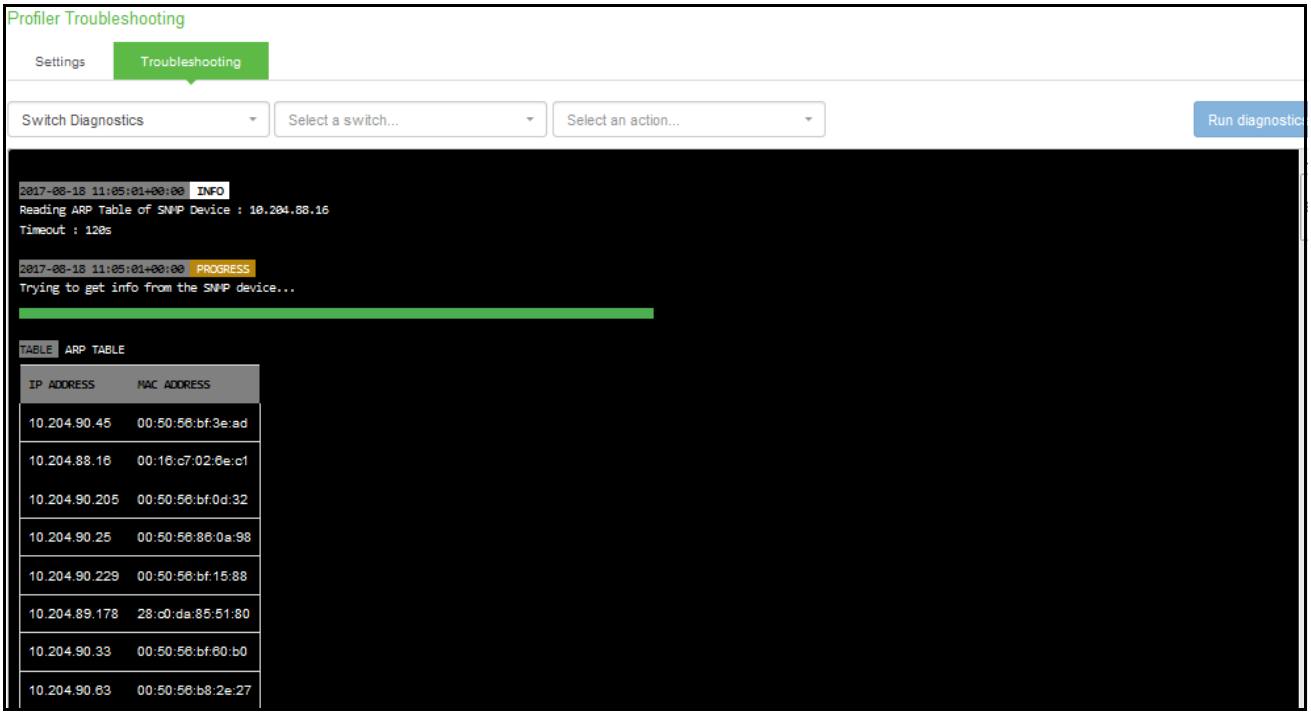
DHCP Test Example

Figure 33 DHCP Test



Switch Diagnostics Example

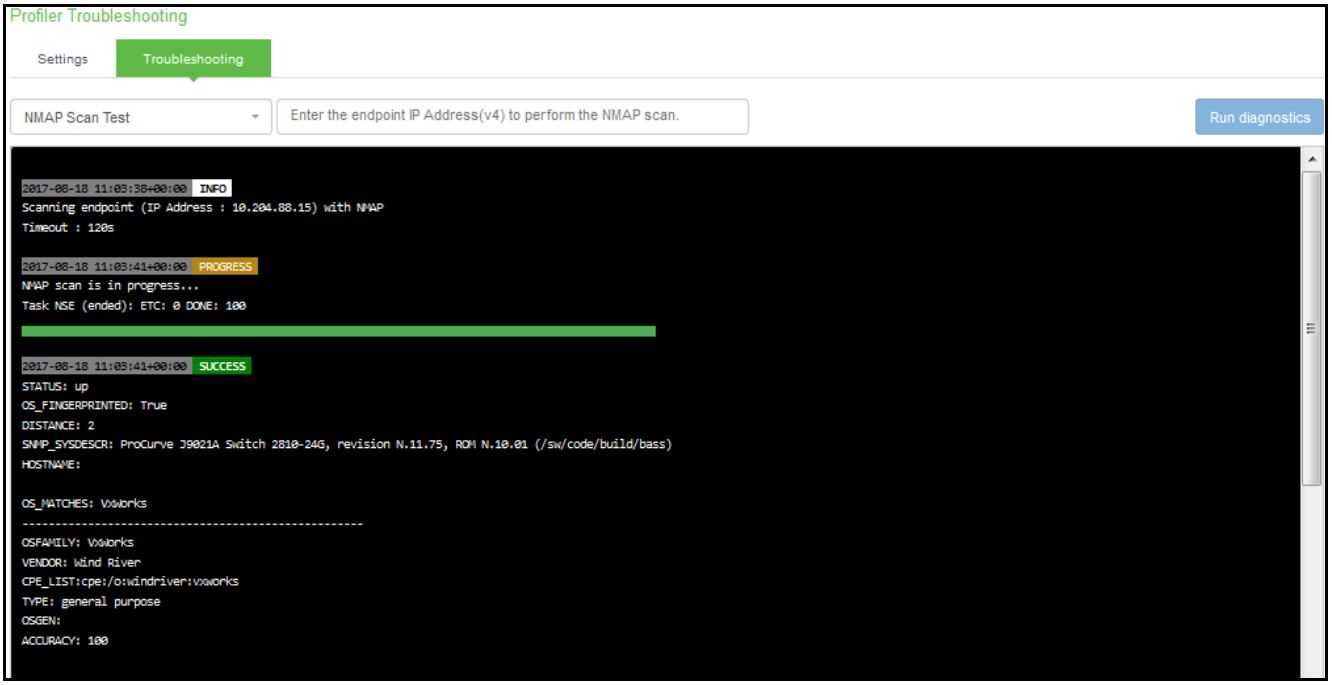
Figure 34 Switch Diagnostics



© 2020 Pulse Secure, LLC.

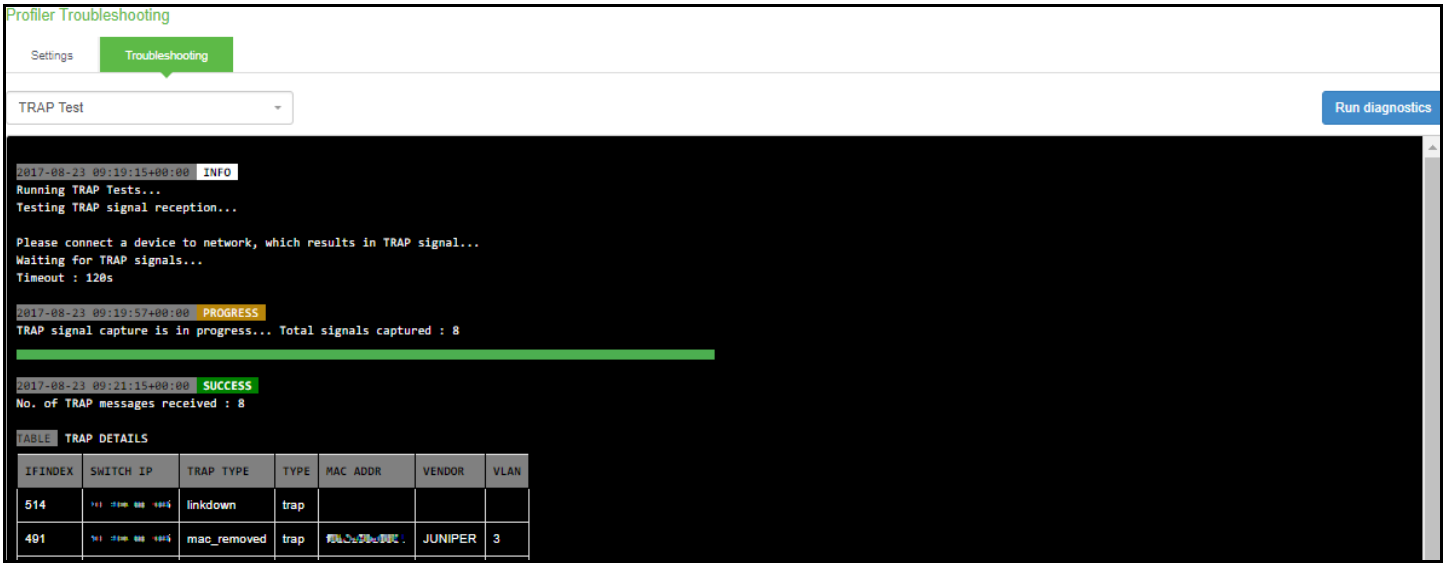
NMAP Scan Test Example

Figure 35 NMAP SCAN Test



Trap Test Example

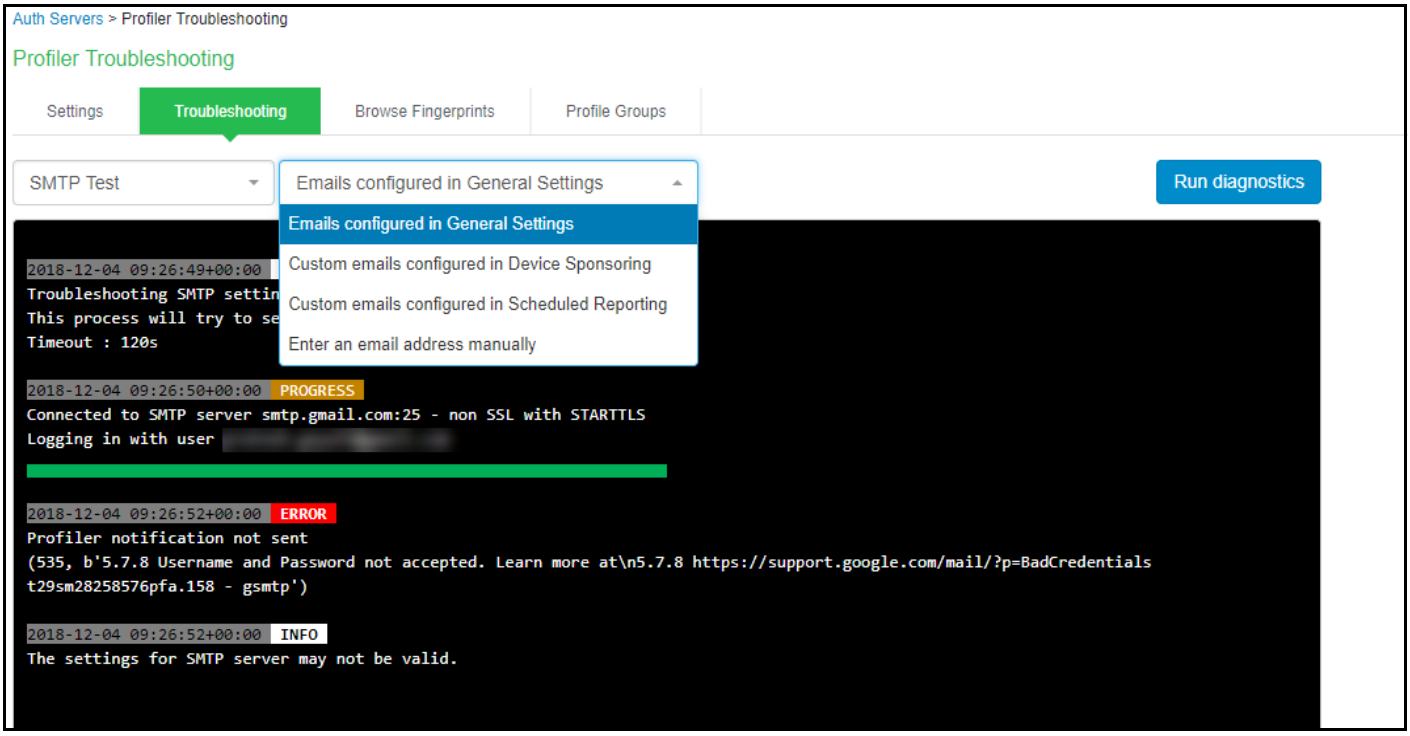
Figure 36 Trap Test



© 2020 Pulse Secure, LLC.

SMTP Test

Figure 37 SMTP Test



© 2020 Pulse Secure, LLC.

Profiler Logs

The Profiler logs all its activities to the Event Log and Administrator Access Logs. To see the Profiler logs in the Event log, select **Log/Monitoring > Events > Log Settings** and enable the “Profiler Events”.

Figure 38 List of Events to Log

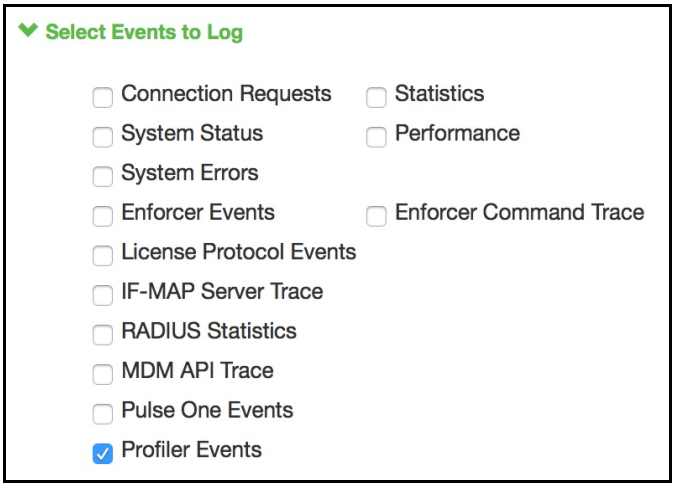


Table 1 Related logs

When	Where	What
System start	Event Log	Starting services:classifier Starting services: dhcp-collector Starting services: nmap-collector Starting services: snmp-collector
New device profiled	Event Log	Device (xxxxxxxxxxxx) is classified as Generic Android.
Device not profiled	Event Log	The Profiler is not able to classify Device (XX:XX:XX:XX:XX:XX)
Profile change	Event Log	Device (‘XX:XX:XX:XX:XX:XX ') has changed profile from 'Windows' to 'Linux'
Fingerprint DB initialization	Event Log	Warning: Fingerprint DB Initialization: Fingerprint database not found. Warning: Fingerprint DB Initialization: Fingerprint database is not the latest. Device profiles cannot be normalized.

© 2020 Pulse Secure, LLC.

When	Where	What
Polling SNMP switch	Event Log	Polling SNMP switch: 'Name: hp IP: XX.XX.XX.XX Version: 3'
		SNMP Scan: 'Start: Fri Jul 22 xx:xx:xx:xx 2016'
		SNMP endpoint count: For WLC named XX is XX
		SNMP endpoint count: For Switch named XXX is XX
		SNMP endpoint count: No endpoints connected to switch Or WLC named XXX
		SNMP endpoint count: Total XX
		SNMPPollError: authorizationError (access denied to that object) while getting info with OID: X.X.X.X.X from the Switch: XX.XX.XX.XX community: XXX context: XXX
		SNMPPollError: Switch (Name: XXX IP: XX.XX.XX.XX) is disabled under Endpoint Policy->Network Access->SNMP Device->Configuration. Please enable to start polling
		SNMPPollError: Unable to retrieve the CAM table from the switch. (Name: XXX IP: XX.XX.XX.XX). Please check the Switch configuration
Fetching devices from switches	Event Log	SNMP Endpoint Count: 'For Switch named nn:nn:nn:nn is 278'
Cluster replication	Event Log	Starting services: Profiler replicator
		Started syncing state
		Completed syncing state
WMI user related changes	Event Log	WMI Scanning endpoint: 'Mac:XX:XX:XX:XX:XX:XX ip:XX.XX.XX.XX'
WMI connection to endpoint fails	Event Log	WMI Connection failed: endpoint Mac:XX:XX:XX:XX:XX:XX ip:XX.XX.XX.XX reason XXX
		WMI Query failed: endpoint Mac:XX:XX:XX:XX:XX:XX ip:XX.XX.XX.XX query XXX

© 2020 Pulse Secure, LLC.

Appendix: Configuring Cisco Switches

Configure DHCP Forwarding

Use the following commands to configure DHCP forwarding across VLANs on Cisco switches.

```
interface <VLAN_NAME>
ip address <IP_ADDRESS> <NETMASK>
ip helper-address <DHCP_SERVER_IP>
ip helper-address <PPS_IP>
```

Configure CDP/LLDP

Use the following commands to enable CDP/LLDP on Cisco switches.

```
cdp run
lldp run
```

Configure SNMP Traps

Use the following commands to configure SNMP Traps on Cisco switches.

Interface level configuration

```
interface GigabitEthernet1/0/16
description <Description message >
switchport access vlan 74
switchport mode access
snmp trap mac-notification change added
snmp trap mac-notification change removed
snmp trap link-status permit duplicates
spanning-tree portfast

snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps mac-notification change move threshold
snmp-server host <PPS IPAddr> version 2c <snmp community String> mac-notification snmp
```

Mac-Notification

```
mac address-table notification change interval 0
mac address-table notification change
mac address-table notification mac-move
mac address-table aging-time 3600
```

Note: The MAC change notifications are not expected from the Trunk ports; the administrator should not enable MAC change notifications on the Trunk ports.

© 2020 Pulse Secure, LLC.

Configure RSPAN

Use the following steps to configure RSPAN on Cisco Catalyst switches:

1. Create a VLAN that will be used as an RSPAN-VLAN on both switches. In this example, we used VLAN ID 999 as the RSPAN-VLAN.
2. Allow the RSPAN-VLAN on the trunk port between Switch1 and Switch2.

The configuration details are as follows:

Switch 1 (Source switch)

```
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)# vlan 999
Switch1(config-vlan)# name RSPAN-Vlan
Switch1(config-vlan)# remote-span
Switch1(config-vlan)# exit
Switch1(config)# monitor session 1 source interface Gi0/1 rx
Switch1(config)# monitor session 1 destination remote vlan 999
Switch1(config)# end
```

Allow VLAN ID 999 on the Trunk Port Gi0/2

```
Switch1# sh run int g0/2
Building configuration...
Current configuration: 175 bytes
!
interface GigabitEthernet0/2
 description To-Switch2-port-Gi0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 999
 switchport mode trunk end
```

Switch2 (Destination switch)

```
Switch2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2(config)# vlan 999
Switch2(config-vlan)# name RSPAN-Vlan
Switch2(config-vlan)# remote-span
Switch2(config-vlan)# exit
Switch2(config)# monitor session 1 source remote vlan 999
Switch2(config)# end
```

Allow VLAN ID 999 on the Trunk Port Gi0/1

```
Switch2# sh run int g0/1
Building configuration...
Current configuration: 175 bytes
!
interface GigabitEthernet0/1
 description To-Switch1-port-Gi0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 999
 switchport mode trunk end
```


© 2020 Pulse Secure, LLC.

Add Native VLAN ID 60 and Allow VLAN ID 999 on Trunk Port Gi0/2

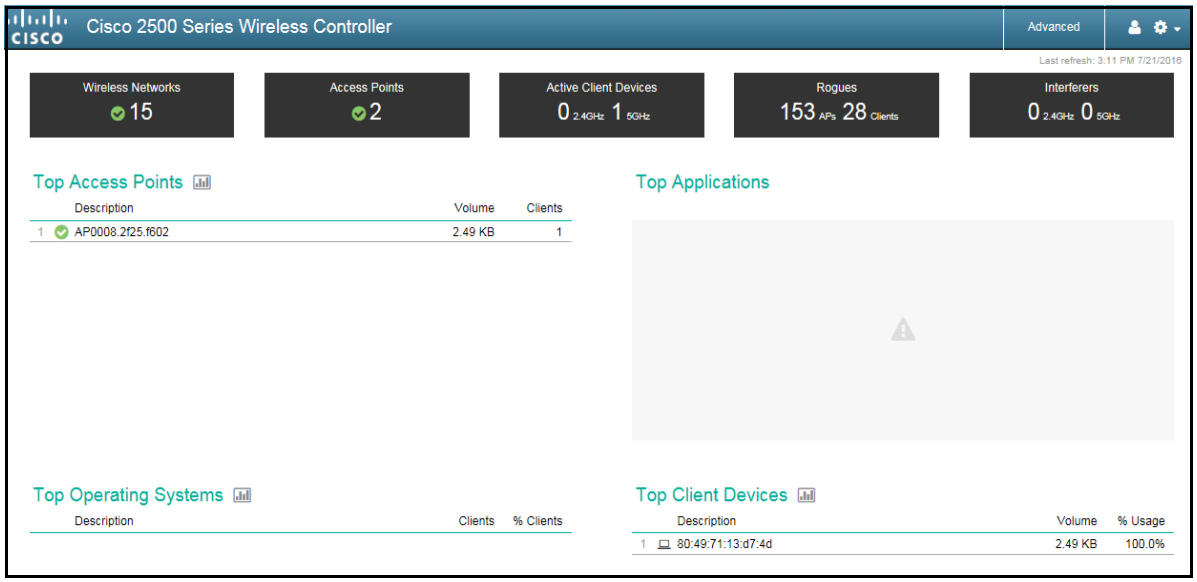
```
Switch1# sh run int g0/2
Building configuration...
Current configuration: 175 bytes
!
 interface GigabitEthernet0/2
 description To-Switch2-port-Gi0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 999
 switchport trunk native vlan 60
 switchport mode trunk end
```

Forward HTTP User Agent Data

Use the following steps to forward HTTP User Agent data from a Cisco WLC 2500 to PPS.
The steps may vary slightly if you are using a different model of Cisco WLC.

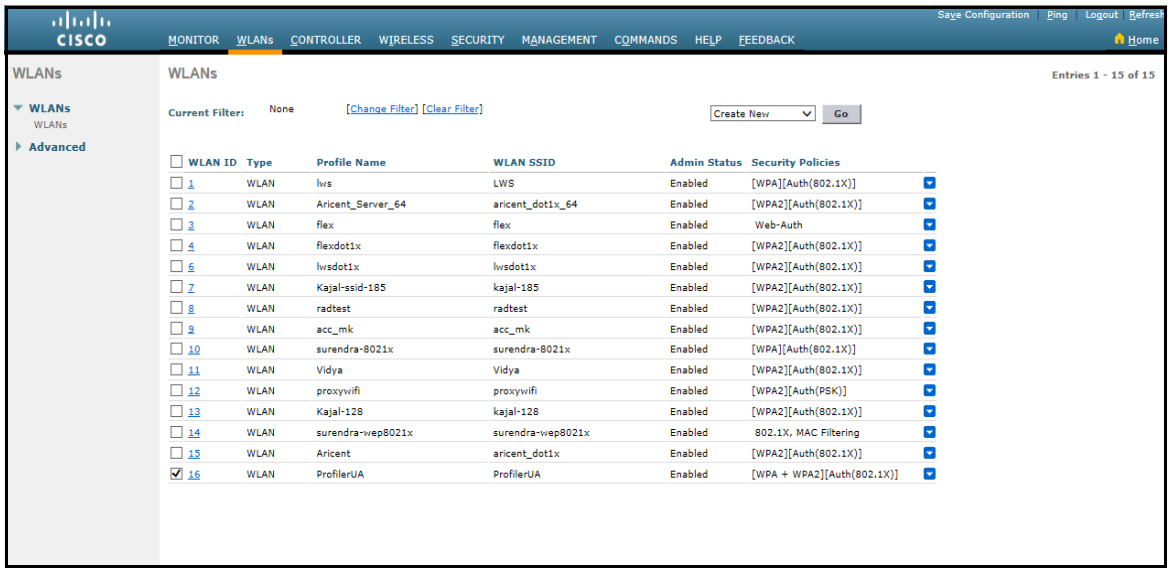
1. Log in to the web-based management console of the wireless LAN controller. Click the **Advanced** button at the top right corner of the page.

   Figure 39 Wireless LAN Controller Web UI



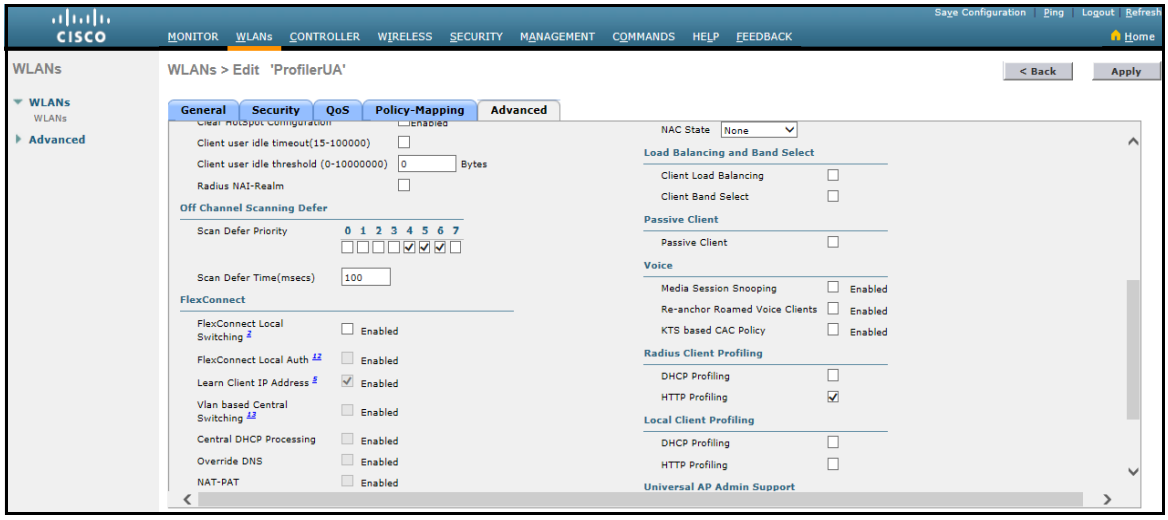
2. Select **WLANs** from the top menu and then click on the corresponding SSID.

Figure 40 WLANS



3. Click the **Advanced** tab and then select the **HTTP Profiling** check box.

Figure 41 HTTP Profiling



4. Click **Apply** to save the changes.

© 2020 Pulse Secure, LLC.

Appendix: Configuring Juniper Switches

Configure DHCP Forwarding

Use the following commands to configure DHCP forwarding across VLANs on Juniper switches.

```
set forwarding-options helpers bootp interface <VLAN_NAME>
set forwarding-options helpers bootp server <DHCP_SERVER_IP>
set forwarding-options helpers bootp server <PPS_IP>
```

For Juniper Switch OS version 15.x and above

```
set forwarding-options dhcp-relay server-group dhcp-server <DHCP Sever>
set forwarding-options dhcp-relay server-group dhcp-server <PPS IP>
set forwarding-options dhcp-relay active-server-group dhcp-server
set forwarding-options dhcp-relay group dhcp-server interface irb.X
set forwarding-options dhcp-relay group dhcp-server interface irb.y
```

Configure LLDP

Use the following commands to enable LLDP on Juniper switches:

```
set protocols lldp interface all
```

Configure SNMP Traps

Use the following commands to configure SNMP Traps on Juniper switches.

Global Level Configuration

```
set groups global snmp community public authorization read-only
set groups global snmp trap-options
set groups global snmp trap-group profiler version all
set groups global snmp trap-group profiler targets <PPS IP Address>
set groups global snmp traceoptions file profiler
set groups global snmp traceoptions flag all
set groups gobal
set apply-groups global
```

Interface Level Configuration

```
set interfaces ge-0/0/0 enable
set interfaces ge-0/0/0 traps
```

SNMP Specific V2 Configuration

```
set snmp view all oid .1
set snmp community public view all
set snmp community public authorization read-only
set snmp trap-group profiler
```

© 2020 Pulse Secure, LLC.

MAC Notification

```
set switch-options mac-notification notification-interval 1
```

Configure RSPAN

Use the following steps to configure basic remote port mirroring.

Source Switch Configuration

1. Configure the VLAN tag ID for the remote-monitor VLAN.

   ```
   [edit vlans]
   user@switch# set remote-monitor vlan-id 999
   ```

2. Configure the interface on the network port connected to the destination switch for trunk mode and associate it with the remote-monitor VLAN.

   ```
   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members 999
   ```

3. Configure the ge-0/0/2 interface for egress-only traffic so that traffic can only egress from the interface.

   ```
   [edit vlans]
   user@switch# set remote-monitor interface ge-0/0/2 egress
   ```

4. Configure the employee-monitor analyzer.

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
   user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
   user@switch# set analyzer Port Mirroring employee-monitor loss-priority high
   user@switch# set analyzer employee-monitor output vlan remote-monitor
   ```

Destination Switch Configuration

1. Configure the VLAN tag ID for the remote-monitor VLAN:

   ```
   [edit vlans]
   user@switch# set remote-monitor vlan-id 999
   ```

2. Configure the interface on the destination switch for trunk mode and associate it with the remote-monitor VLAN:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching port-mode trunk
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching vlan members 999
   ```

3. Configure the interface connected to the destination switch for trunk mode and associate it with the remote-monitor VLAN:

© 2020 Pulse Secure, LLC.

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members 999
```

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.

Appendix: Configuring HP (Procurve) Switches

Configure DHCP Forwarding

Use the following commands to configure DHCP forwarding across VLANs on HP switches.

```
vlan <VLAN_NAME>
ip helper-address <DHCP_SERVER_IP>
ip helper-address <PPS_IP>
```

Configure LLDP

Use the following commands to enable LLDP on HP switches:

```
ProCurve Switch 2810-24G(config)# lldp run
```

Configure SNMP Traps

Use the following commands to configure SNMP Traps on HP switches.

```
snmp-server community "public"
snmp-server community "private" unrestricted
snmp-server host <PPS IP Address> community "public" trap-level all Trap
```

LinkUp/LinkDown Configuration

```
snmp-server enable traps link-change 5
Mac Notification
snmp-server enable traps mac-notify
```

Configure RSPAN

Use the following commands to configure remote mirroring from the command line interface.

Source Switch Configuration

Configure the switch mirror sessions.

```
ProCurve_source_switch(config)# mirror <1-4> [name <name>] remote ip <src-ip-add>
<srcudp-port> <dst-ip-add>
```

Destination Switch Configuration

Configure the switch mirror endpoint.

```
ProCurve_dst_switch(config)# mirror endpoint ip <src-ip-add> <src-udp-port> <dst-ip-
add> port <port#>
```

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.

Appendix: Configuring Viptela Switches

Configure SNMP on Viptela Switch

Use the following commands to configure SNMP on Viptela switches.

SNMP View configuration

```
Viptela(config)# snmp
Viptela(config-snmp)# no shutdown
Viptela(config-snmp)# view v2 oid 1.3.6.1
Viptela(config-snmp)# view viptela-private oid 1.3.6.1.4.1.41916
```

SNMP V3 configuration

```
Viptela(config)# snmp group group-name authentication
Viptela(config-group)# view view-name
Viptela(config)# snmp user username
Viptela(config-user)# auth authentication
Viptela(config-user)# auth-password password
Viptela(config-user)# priv privacy
Viptela(config-user)# priv-password password
Viptela(config-user)# group group-name
```

SNMP V2 configuration

```
Viptela(config-snmp)# community name
Viptela(config-community-name)# authorization read-only
Viptela(config-community-name)# view string
```

Sample Configuration

```
snmp
   no shutdown
   contact  profiler_team
   name     profilerViptelaSwitch
   location ESXServer
   view v2
      oid 1.3.6.1
      oid 1.3.6.1.4.1.41916
   !
   view viptela-private
      oid 1.3.6.1.4.1.41916
   !
   community public
      view          v2
      authorization read-only
   !
   group prf-group auth-priv
      view v2
   !
   user prfqa
```

© 2020 Pulse Secure, LLC.

```
    auth          md5
    auth-password $8$GDEzgygwNOr8mB6VAnej2NX2fKh7G9QDNKcxa13HR+I=
    priv          aes-cfb-128
    priv-password $8$pgr3pzv3qf9S0kGomJ0w2MlbkrUipecEgHxCRWIw2D8=
    group         prf-group
!
```


© 2020 Pulse Secure, LLC.

Appendix: Ports Used for Profiling

Ensure firewall allows traffic on the following Profiler ports for profiling devices.

Protocol	Associated Ports
Incoming	
DHCP	67 (UDP)
SNMP trap	162 (UDP)
RADIUS accounting	1813 (UDP) (for user agent classification from WLCs)
HTTP REST API	443
Outgoing	
SNMP	161 (UDP)
Nmap	• 53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 (UDP) • 21,22,23,25,53,80,88,110,135,139,143,443,445,830,3306,3389,8080,8085,8086 (TCP)
SSH	22 (TCP)
WMI	132 (TCP)

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.