Pulse Policy Secure

Profiler

Deployment Guide

Document Version	1.1
Published	April 2019

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

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

Document Revision History

Feature	Add/Update/Remove	Document Published Date/ Document Version	Effective Release	Notes
PPS/PCS Configuration (Remote Profiler)	Updated	March 2019/1.1	9.0R3	Updated the note to clarify the clustering support
Configuring Juniper Switches	Updated	December 2018/1.0	9.0R3	Updated DHCP forwarding commands for Juniper Switch OS version 15.x and above
SMTP Test	Updated	December 2018/1.0	9.0R3	SMTP Test to troubleshooting screen shot updated
Detecting Spoof	Updated.	December 2018/1.0	9.0R3	Updated note for spoof suspected devices
Configuring Profile Groups	Added	December 2018/1.0	9.0R3	Added a section that the devices can be grouped based on group name

Contents

Table of Figures

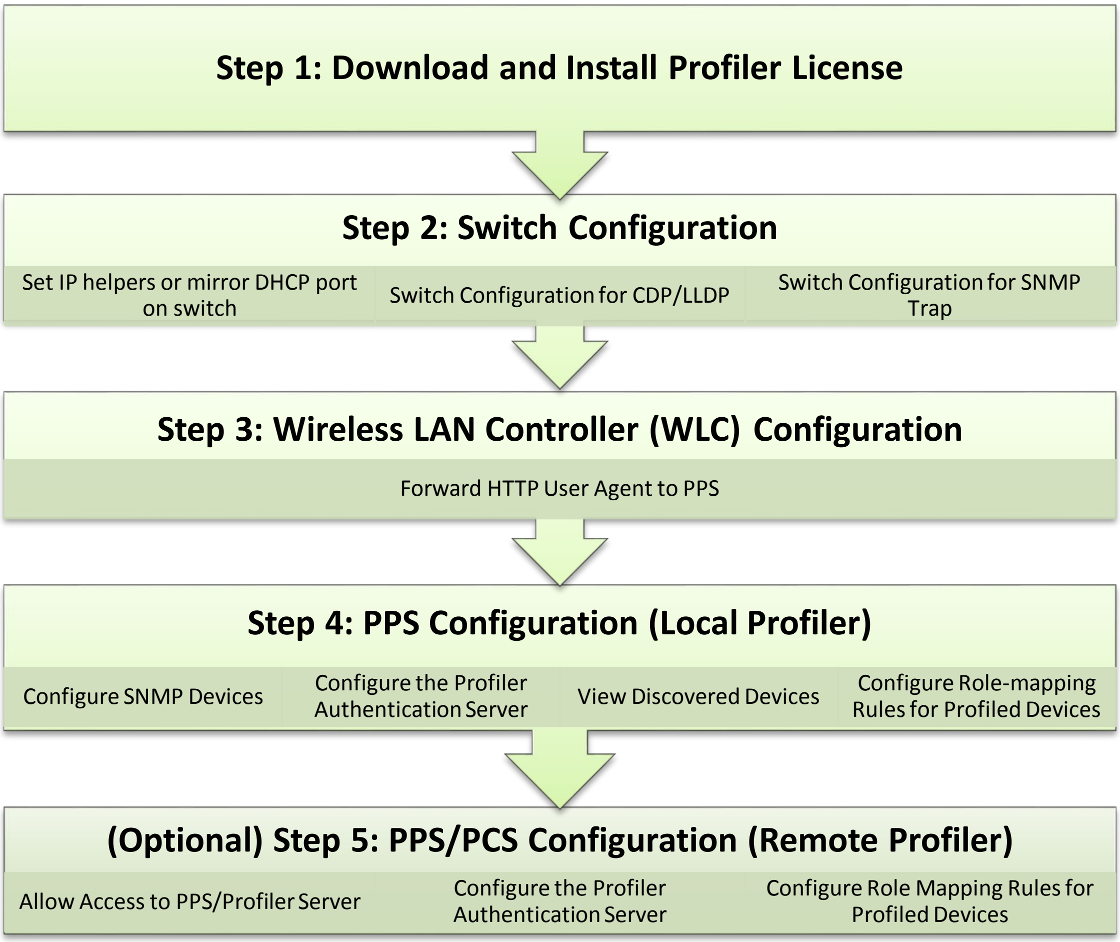
Introduction

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 below. Click each step to directly jump to the related instructions.



Step 1: Download and Install Profiler License

Step 2: Switch Configuration

- Set IP helpers or mirror DHCP port on switch
- Switch Configuration for CDP/LLDP
- Switch Configuration for SNMP Trap

Step 3: Wireless LAN Controller (WLC) Configuration

- Forward HTTP User Agent to PPS

Step 4: PPS Configuration (Local Profiler)

- Configure SNMP Devices
- Configure the Profiler Authentication Server
- View Discovered Devices
- Configure Role-mapping Rules for Profiled Devices

(Optional) Step 5: PPS/PCS Configuration (Remote Profiler)

- Allow Access to PPS/Profiler Server
- Configure the Profiler Authentication Server
- Configure Role Mapping Rules for Profiled Devices

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

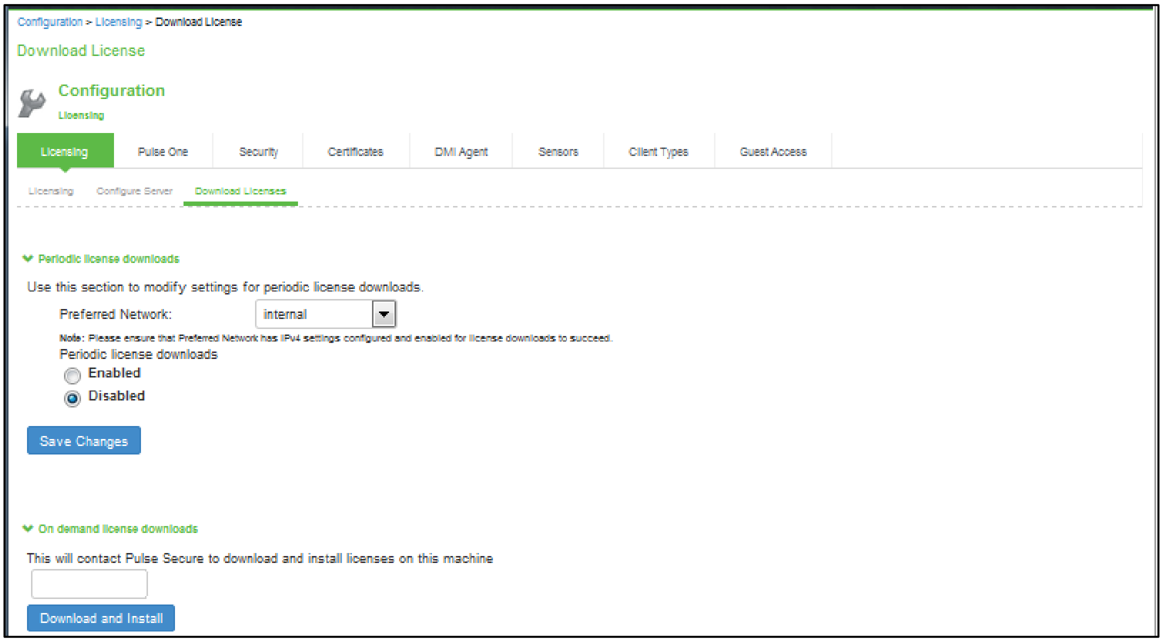
Download and Install Profiler License

From Profiler v1.3 onwards, new license SKUs are available for customers on Pulse Secure license portal, for example, PS-PROFILER-LG SKU. The Profiler SKUs are device count based licenses. For more information, see Profiler License.

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 1: Download and Install License



Use this section to modify settings for periodic license downloads.

Preferred Network: internal

Note: Please ensure that Preferred Network has IPv4 settings configured and enabled for license downloads to succeed.

Periodic license downloads

○ Enabled

● Disabled

This will contact Pulse Secure to download and install licenses on this machine

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

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

Switch Configuration

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
- Appendix: Configuring Juniper Switches
- Appendix: Configuring HP Switches

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

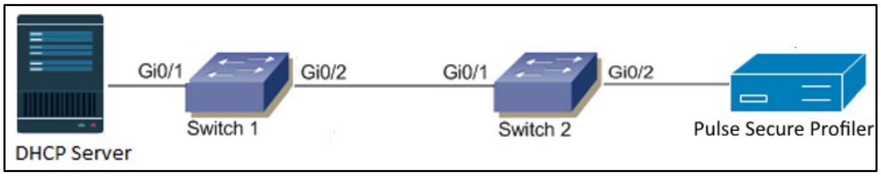
The Profiler uses the Link Up/Down and MAC notification traps to:

- 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.

Figure 2: 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.

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.

PPS Configuration (Local Profiler)

The following sections describe the steps to configure the Local Profiler.

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.

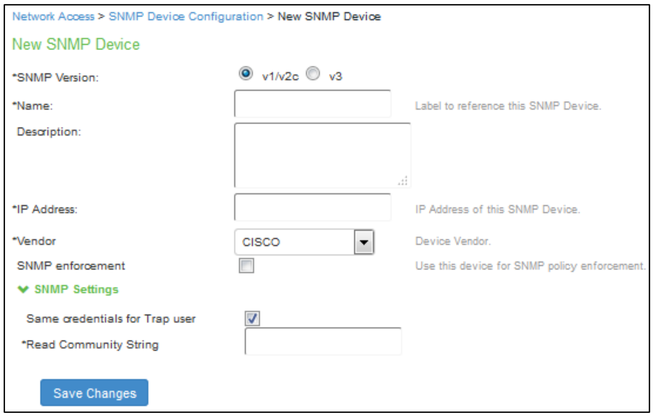
1. Select **Endpoint Policy > Network Access > SNMP Device > Configuration > New SNMP Device** and add one or more switches.

   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.

Figure 3: Configuring New SNMP Device



Network Access > SNMP Device Configuration > New SNMP Device

New SNMP Device

*SNMP Version: ● v1/v2c ○ v3

*Name: Label to reference this SNMP Device.

Description:

*IP Address: IP Address of this SNMP Device.

*Vendor CISCO Device Vendor.

SNMP enforcement □ Use this device for SNMP policy enforcement.

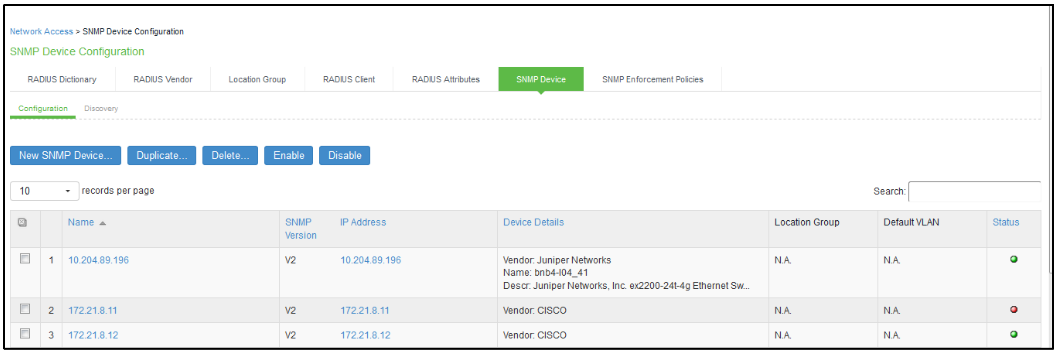
SNMP Settings

Same credentials for Trap user ☑

*Read Community String

2. Save the changes. The SNMP Device Configuration table is updated as shown in Figure 4.

Figure 4: SNMP Device Configuration Table



Network Access > SNMP Device Configuration

SNMP Device Configuration

☒		Name ▲	SNMP Version	IP Address	Device Details	Location Group	Default VLAN	Status
□	1	10.204.89.196	V2	10.204.89.196	Vendor: Juniper Networks Name: bnb4-I04_41 Descr: Juniper Networks, Inc. ex2200-24t-4g Ethernet Sw...	N.A.	N.A.	●
□	2	172.21.8.11	V2	172.21.8.11	Vendor: CISCO	N.A.	N.A.	●
□	3	172.21.8.12	V2	172.21.8.12	Vendor: CISCO	N.A.	N.A.	●

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 Profiler Authentication Server

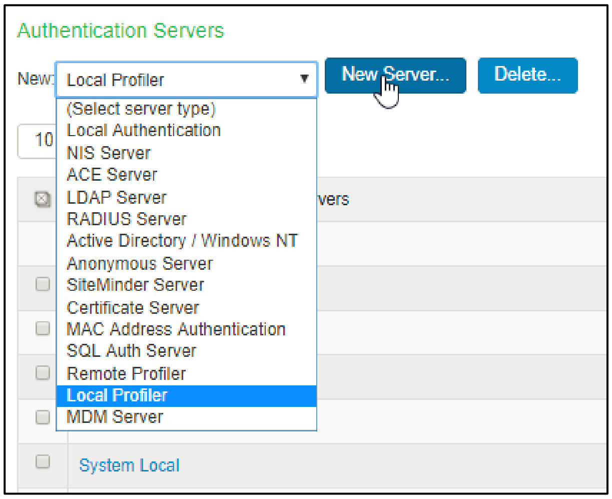
Ensure the following tasks are performed before proceeding with the Profiler Authentication server configuration.

- If you wish to use DHCP fingerprinting, you have configured the switch(s) to forward DHCP packets to the PPS as described in the previous section.
- If you wish to use SNMP-based profiling, you have configured one or more switches in the SNMP Device Configuration page of the PPS Administrator UI as described in the previous section.
- 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 5: Creating a Local Profiler Authentication Server

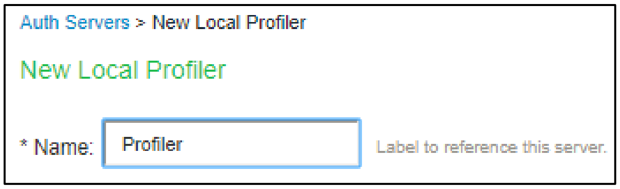


Authentication Servers

New: Local Profiler

3. Enter a name for the Authentication server.

Figure 6: Naming a Local Profiler Authentication Server



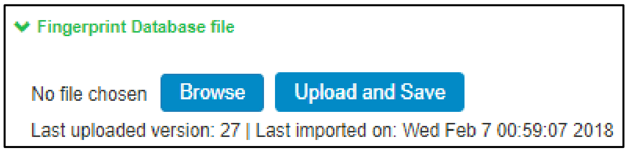
Auth Servers > New Local Profiler

New Local Profiler

* Name: Profiler Label to reference this server.

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

Figure 7: Uploading Device Fingerprints Package



Fingerprint Database file

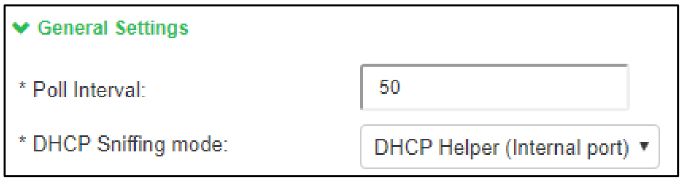
No file chosen

Last uploaded version: 27 | Last imported on: Wed Feb 7 00:59:07 2018

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.

Figure 8: General Settings



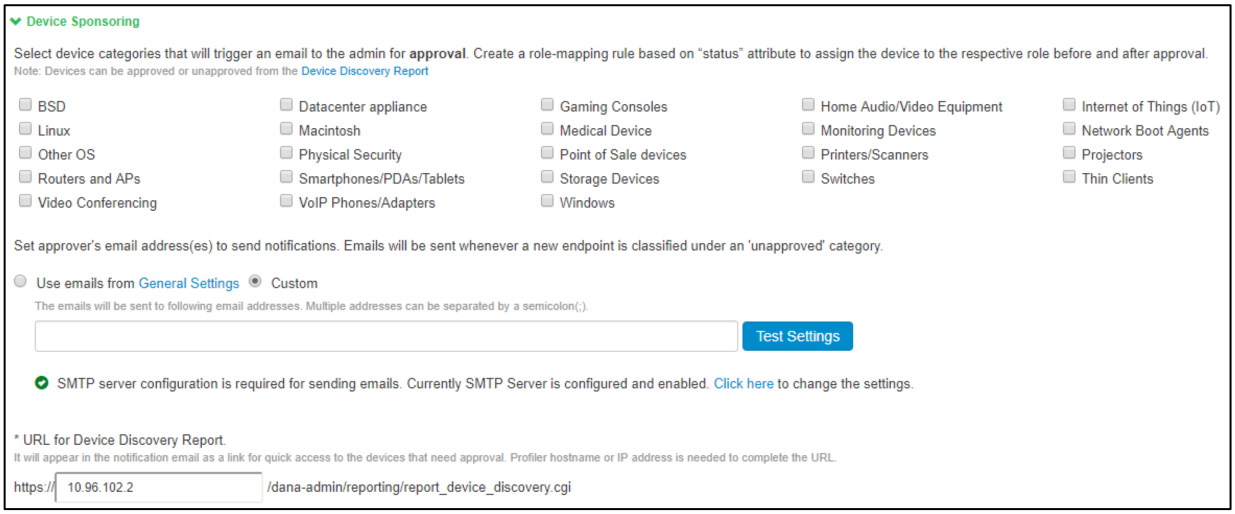
General Settings

* Poll Interval: 50

* DHCP Sniffing mode: DHCP Helper (Internal port)

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.
   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 9: Device Sponsoring



Device Sponsoring

Select device categories that will trigger an email to the admin for **approval**. Create a role-mapping rule based on "status" attribute to assign the device to the respective role before and after approval.

Note: Devices can be approved or unapproved from the Device Discovery Report

□ BSD
□ Linux
□ Other OS
□ Routers and APs
□ Video Conferencing
□ Datacenter appliance
□ Macintosh
□ Physical Security
□ Smartphones/PDAs/Tablets
□ VoIP Phones/Adapters
□ Gaming Consoles
□ Medical Device
□ Point of Sale devices
□ Storage Devices
□ Windows
□ Home Audio/Video Equipment
□ Monitoring Devices
□ Printers/Scanners
□ Switches
□ Internet of Things (IoT)
□ Network Boot Agents
□ Projectors
□ Thin Clients

Set approver's email address(es) to send notifications. Emails will be sent whenever a new endpoint is classified under an 'unapproved' category.

○ Use emails from General Settings ● Custom

The emails will be sent to following email addresses. Multiple addresses can be separated by a semicolon(;).

SMTP server configuration is required for sending emails. Currently SMTP Server is configured and enabled. Click here to change the settings.

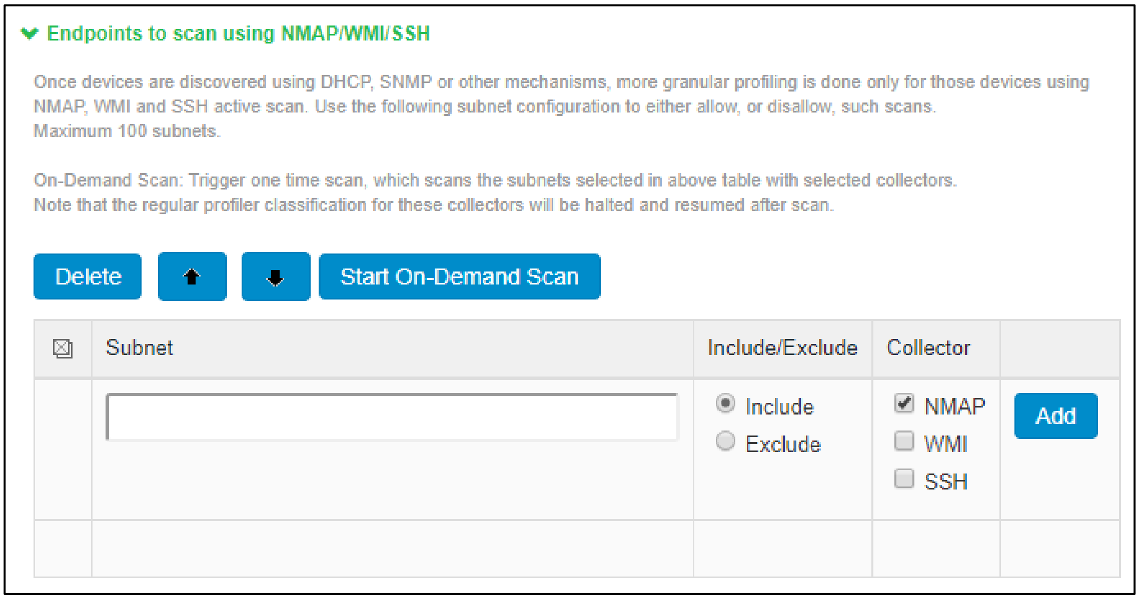
* URL for Device Discovery Report.

It will appear in the notification email as a link for quick access to the devices that need approval. Profiler hostname or IP address is needed to complete the URL.

https:// 10.96.102.2 /dana-admin/reporting/report_device_discovery.cgi

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 and NMAP. Maximum 100 subnets configuration are supported. On-Demand Scan can be triggered anytime on the subnets for selected collectors.

Figure 10: Adding One or More Subnets



Endpoints to scan using NMAP/WMI/SSH

Once devices are discovered using DHCP, SNMP or other mechanisms, more granular profiling is done only for those devices using NMAP, WMI and SSH active scan. Use the following subnet configuration to either allow, or disallow, such scans. Maximum 100 subnets.

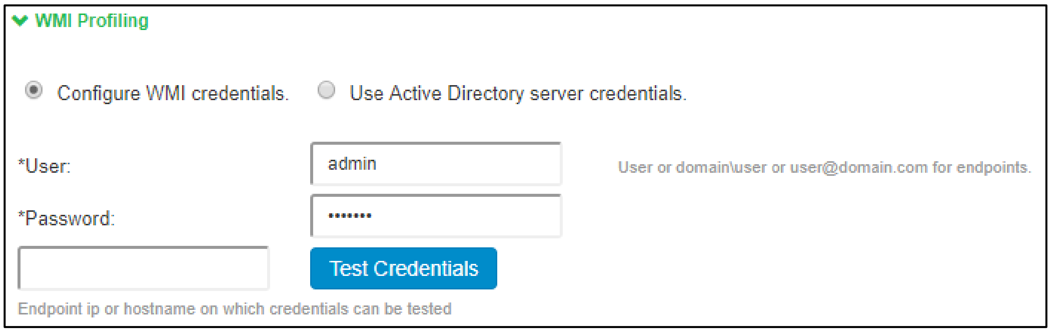
On-Demand Scan: Trigger one time scan, which scans the subnets selected in above table with selected collectors. Note that the regular profiler classification for these collectors will be halted and resumed after scan.

☒	Subnet	Include/Exclude	Collector	
		● Include ○ Exclude	☑ NMAP ☐ WMI ☐ SSH	Add

8. (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.

Note: If multiple antivirus software is installed on the remote desktops, WMI fetches information about only one of the antivirus. WMI does not fetch information about *Windows Defender*.

Figure 11: WMI Profiling



WMI Profiling

● Configure WMI credentials. ○ Use Active Directory server credentials.

*User: admin

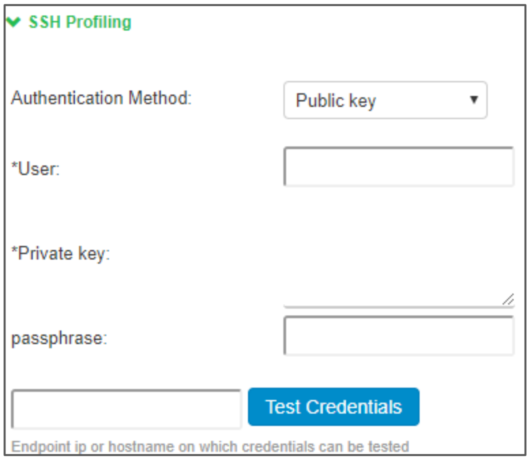
User or domain\user or user@domain.com for endpoints.

*Password: •••••••

Endpoint ip or hostname on which credentials can be tested

9. (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 12: SSH Profiling



SSH Profiling

Authentication Method: Public key

*User:

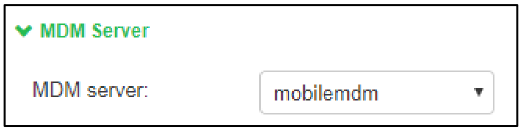
*Private key:

passphrase:

Endpoint ip or hostname on which credentials can be tested

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

Figure 13: MDM Server



MDM Server

MDM server: mobilemdm

11. 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 Device Profiles Dashboard.

The devices can be grouped based on group name and rules using device attributes. For more information see, Profiler Groups.

View Discovered Devices

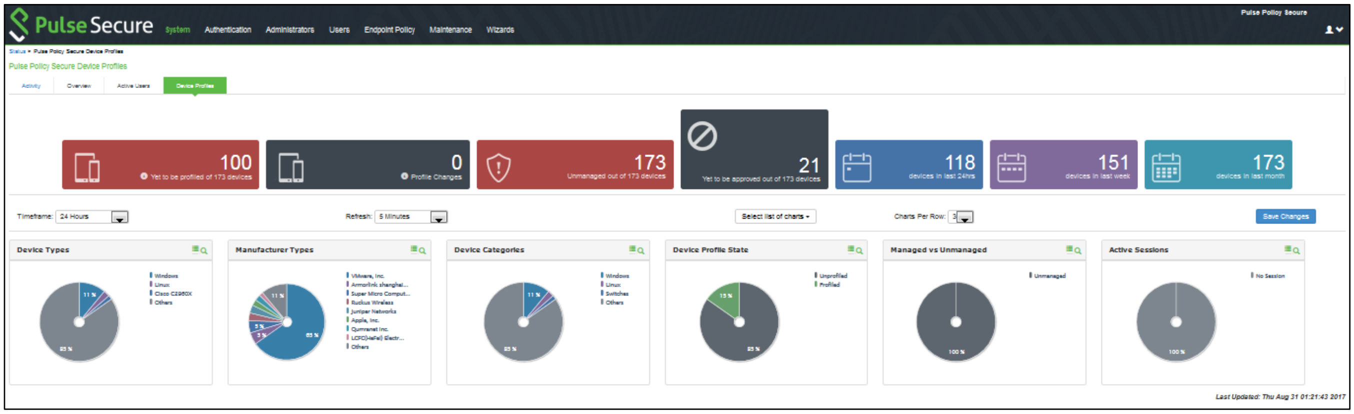
Dashboard View

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**.
2. Set the desired timeframe. Choose 24 hours, 7 days or 30 days.
3. See the following charts:
   - Device Profile State
   - Manufacturer Types
   - Device Categories
   - Device Types
   - Managed vs Unmanaged
   - Active Sessions

Figure 14: Dashboard View



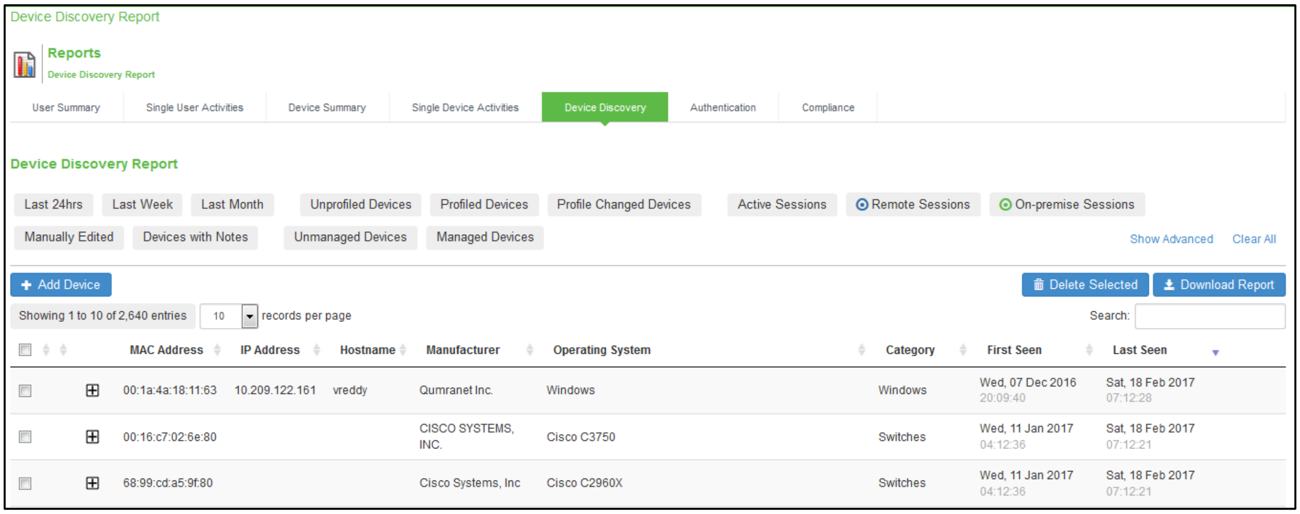
Device Discovery Report View

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.

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

Figure 15: Device Discovery Report Table


Device Discovery Report

Reports
Device Discovery Report

User Summary | Single User Activities | Device Summary | Single Device Activities | Device Discovery | Authentication | Compliance

Device Discovery Report

Last 24hrs | Last Week | Last Month | Unprofiled Devices | Profiled Devices | Profile Changed Devices | Active Sessions | ○ Remote Sessions | ○ On-premise Sessions
Manually Edited | Devices with Notes | Unmanaged Devices | Managed Devices | Show Advanced | Clear All

+ Add Device | Delete Selected | Download Report

Showing 1 to 10 of 2,640 entries | 10 records per page | Search:

□		MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	First Seen	Last Seen
□	⊞	00:1a:4a:18:11:63	10.209.122.161	vreddy	Qumranet Inc.	Windows	Windows	Wed, 07 Dec 2016 20:09:40	Sat, 18 Feb 2017 07:12:28
□	⊞	00:16:c7:02:6e:80			CISCO SYSTEMS, INC.	Cisco C3750	Switches	Wed, 11 Jan 2017 04:12:36	Sat, 18 Feb 2017 07:12:21
□	⊞	68:99:cd:a5:9f:80			Cisco Systems, Inc	Cisco C2960X	Switches	Wed, 11 Jan 2017 04:12:36	Sat, 18 Feb 2017 07:12:21

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 → 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**.

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.

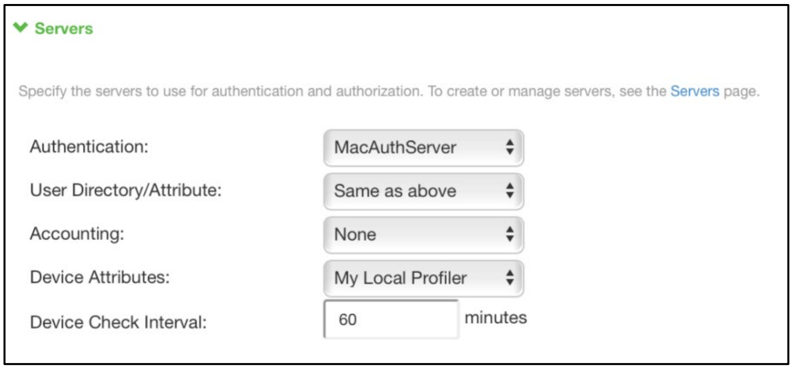
Configuring Role-Mapping Rules for Profiled Devices

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 Auth. Server** as the Device Attributes Server as shown below.

   Figure 16: Device Attributes

   Servers

   Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

   Authentication: MacAuthServer

   User Directory/Attribute: Same as above

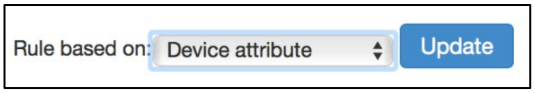
   Accounting: None

   Device Attributes: My Local Profiler

   Device Check Interval: 60 minutes

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

   Figure 17: Rule based on attribute

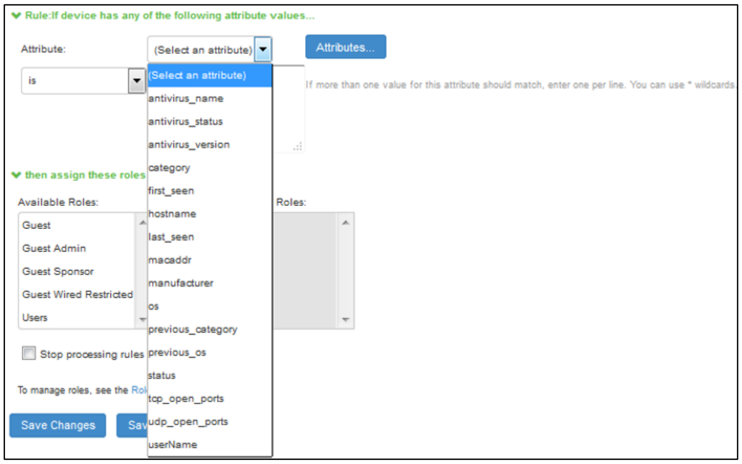
   

   Rule based on: Device attribute

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 rule 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 18: Creating New Role Mapping Rule



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

Attribute: (Select an attribute)

is

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, Guest Admin, Guest Sponsor, Guest Wired Restricted, Users

□ Stop processing rules

To manage roles, see the Rol

9. After assigning the roles, 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.

PPS/PCS Configuration (Remote Profiler)

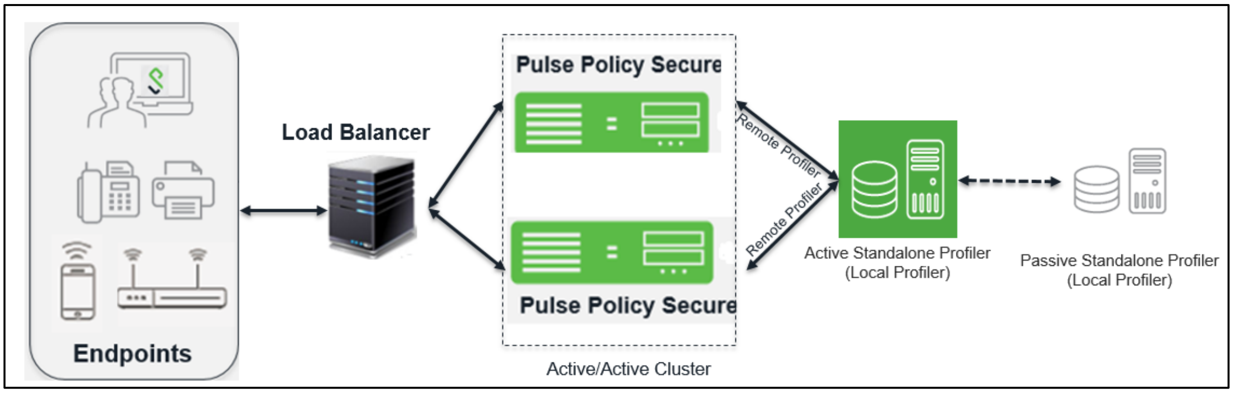
This configuration procedure is optional.

A Remote Profiler can be useful in the following cases:

1. You want to profile devices that are outside the enterprise network and connected via PCS.
2. 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 19: 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.

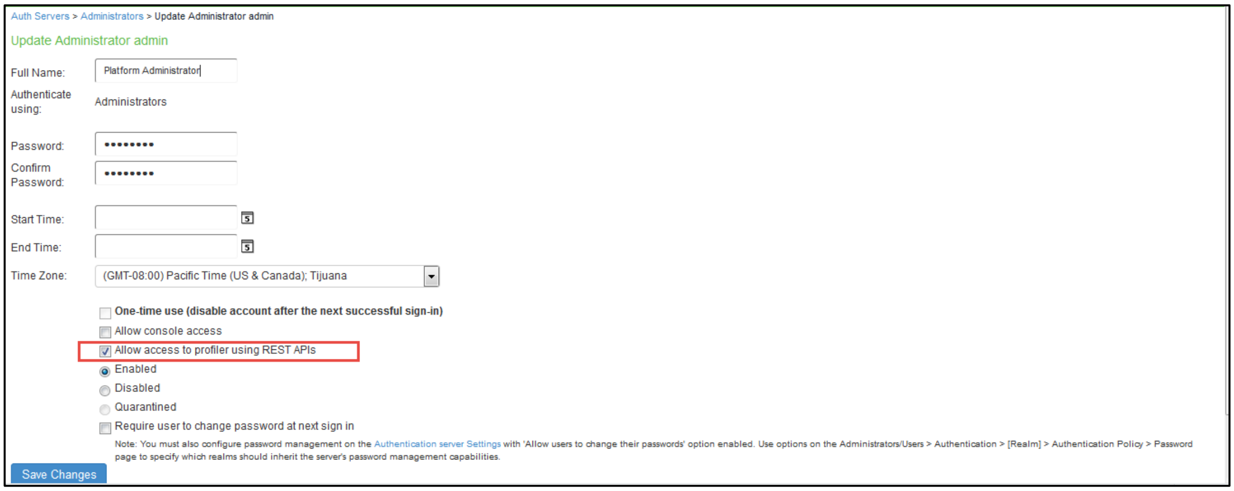
Allowing Access to the Profiler

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.
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 20: Allow Access to the Profiler



Auth Servers > Administrators > Update Administrator admin

Update Administrator admin

Full Name: Platform Administrator

Authenticate using: Administrators

Password: ••••••••

Confirm Password: ••••••••

Start Time:

End Time:

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

□ One-time use (disable account after the next successful sign-in)

□ Allow console access

☑ Allow access to profiler using REST APIs

● Enabled

○ Disabled

○ Quarantined

□ Require user to change password at next sign in

Note: You must also configure password management on the Authentication server Settings with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

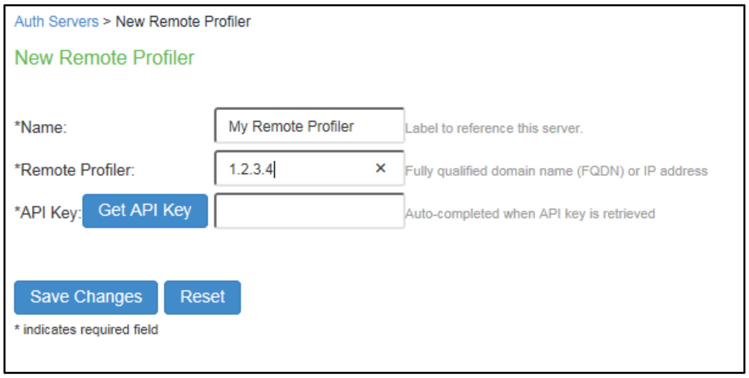
Configuring Remote Profiler Authentication Server

To configure Remote Profiler Authentication Server, follow the procedure Configuring the Profiler Authentication Server.

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 21: New Remote Profiler



Auth Servers > New Remote Profiler

New Remote Profiler

*Name: My Remote Profiler — Label to reference this server.

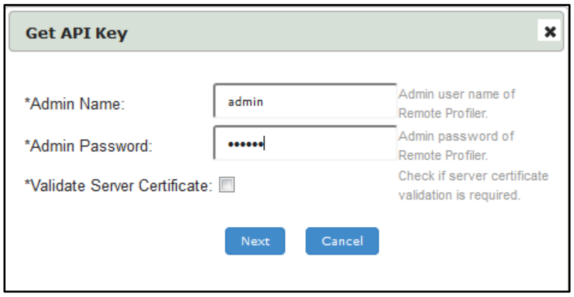
*Remote Profiler: 1.2.3.4 — Fully qualified domain name (FQDN) or IP address

*API Key: — Auto-completed when API key is retrieved

* indicates required field

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 Allowing Access to the Profiler) and click **Next**. The API key will be generated and displayed in the API Key field.

Figure 22: Get API Key



Get API Key

*Admin Name: admin

Admin user name of Remote Profiler.

*Admin Password: ••••••

Admin password of Remote Profiler.

*Validate Server Certificate: □

Check if server certificate validation is required.

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.

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.

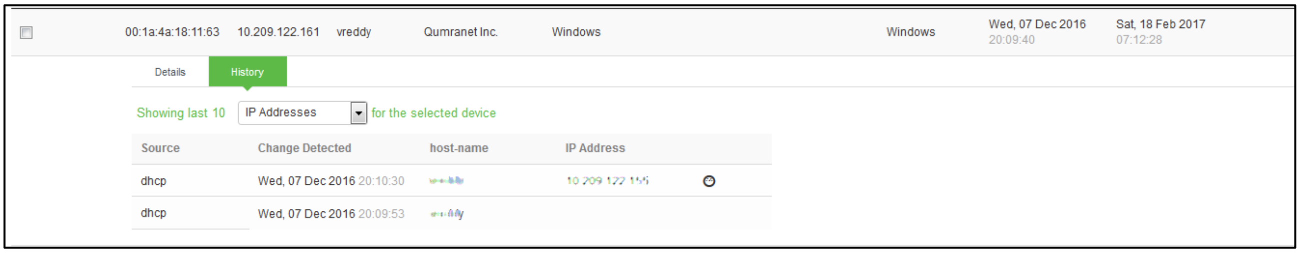
Expiry: Upon expiry of Profiler license or on reaching profiled devices limit, a warning is displayed at the top of Dashboard and Overview pages similar to existing license warnings.

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 23: History based on IP Address



□	00:1a:4a:18:11:63	10.209.122.161	vreddy	Qumranet Inc.	Windows	Windows	Wed, 07 Dec 2016 20:09:40	Sat, 18 Feb 2017 07:12:28

Showing last 10 IP Addresses for the selected device

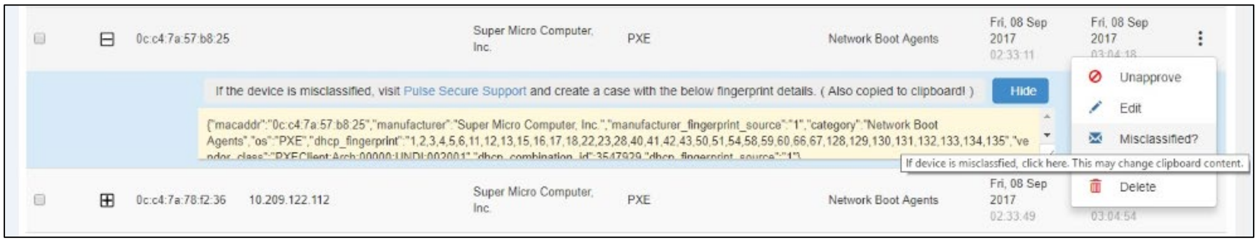
Source	Change Detected	host-name	IP Address
dhcp	Wed, 07 Dec 2016 20:10:30	[illegible]	[illegible]
dhcp	Wed, 07 Dec 2016 20:09:53	[illegible]	

- 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 device operations.

- 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.
- Edit: Allows to edit **Manufacturer**, **Category** and **Operating System** fields. Manually edited devices are not overwritten by Profiler during update.
- Misclassified devices: 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 update the relevant information about the wrongly classified device to Pulse Secure. This information is verified before updating the Custom Fingerprint database.



☐	⊟	0c:c4:7a:57:b8:25		Super Micro Computer, Inc.	PXE	Network Boot Agents	Fri, 08 Sep 2017 02:33:11	Fri, 08 Sep 2017 03:04:18
☐	⊞	0c:c4:7a:78:f2:36	10.209.122.112	Super Micro Computer, Inc.	PXE	Network Boot Agents	Fri, 08 Sep 2017 02:33:49	03:04:54

If the device is misclassified, visit Pulse Secure Support and create a case with the below fingerprint details. (Also copied to clipboard!)

```
{"macaddr":"0c:c4:7a:57:b8:25","manufacturer":"Super Micro Computer, Inc.","manufacturer_fingerprint_source":"1","category":"Network Boot
Agents","os":"PXE","dhcp_fingerprint":"1,2,3,4,5,6,11,12,13,15,16,17,18,22,23,28,40,41,42,43,50,51,54,58,59,60,66,67,128,129,130,131,132,133,134,135","ve
ndor_class":"PXEClient:Arch:00000:UNDI:002001","dhcp_combination_id":3547929,"dhcp_fingerprint_source":"1"}
```

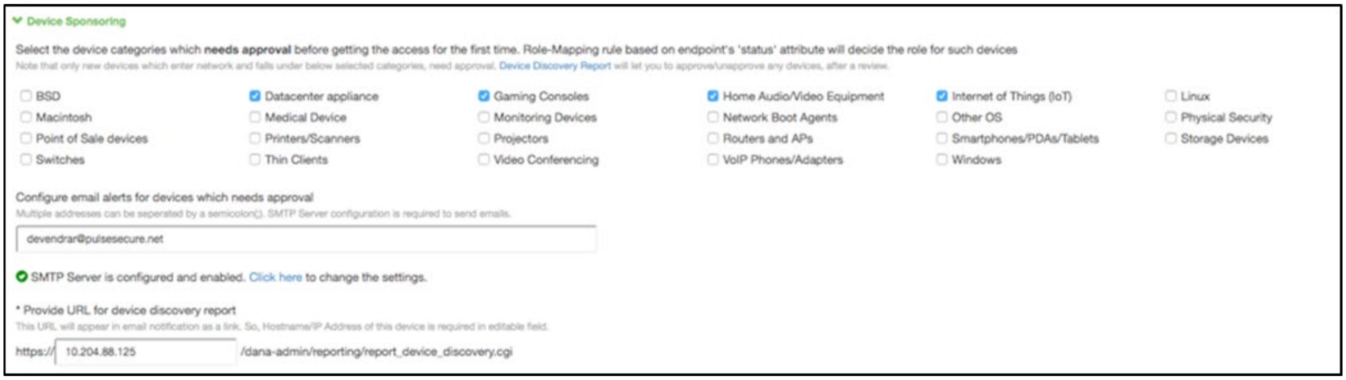
If device is misclassfied, click here. This may change clipboard content.

- **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.



Device Sponsoring

Select the device categories which **needs approval** before getting the access for the first time. Role-Mapping rule based on endpoint's 'status' attribute will decide the role for such devices

Note that only new devices which enter network and falls under below selected categories, need approval. Device Discovery Report will let you to approve/unapprove any devices, after a review.

☐ BSD	☑ Datacenter appliance	☑ Gaming Consoles	☑ Home Audio/Video Equipment	☑ Internet of Things (IoT)	☐ Linux
☐ Macintosh	☐ Medical Device	☐ Monitoring Devices	☐ Network Boot Agents	☐ Other OS	☐ Physical Security
☐ Point of Sale devices	☐ Printers/Scanners	☐ Projectors	☐ Routers and APs	☐ Smartphones/PDAs/Tablets	☐ Storage Devices
☐ Switches	☐ Thin Clients	☐ Video Conferencing	☐ VoIP Phones/Adapters	☐ Windows	

Configure email alerts for devices which needs approval

Multiple addresses can be seperated by a semicolon(;). SMTP Server configuration is required to send emails.

devendrar@pulsesecure.net

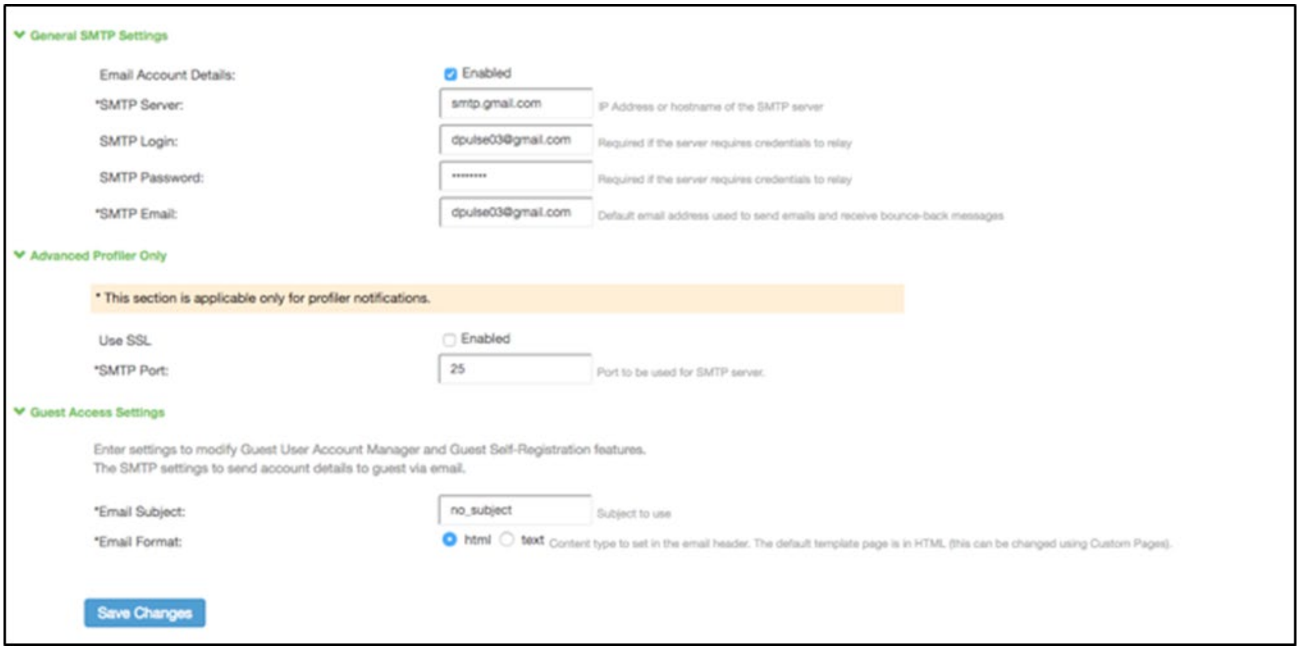
SMTP Server is configured and enabled. Click here to change the settings.

* Provide URL for device discovery report

This URL will appear in email notification as a link. So, Hostname/IP Address of this device is required in editable field.

https:// 10.204.88.125 /dana-admin/reporting/report_device_discovery.cgi

3. Configure the SMTP server.



General SMTP Settings

Email Account Details:	☑ Enabled	
*SMTP Server:	smtp.gmail.com	IP Address or hostname of the SMTP server
SMTP Login:	dpulse03@gmail.com	Required if the server requires credentials to relay
SMTP Password:	********	Required if the server requires credentials to relay
*SMTP Email:	dpulse03@gmail.com	Default email address used to send emails and receive bounce-back messages

Advanced Profiler Only

* This section is applicable only for profiler notifications.

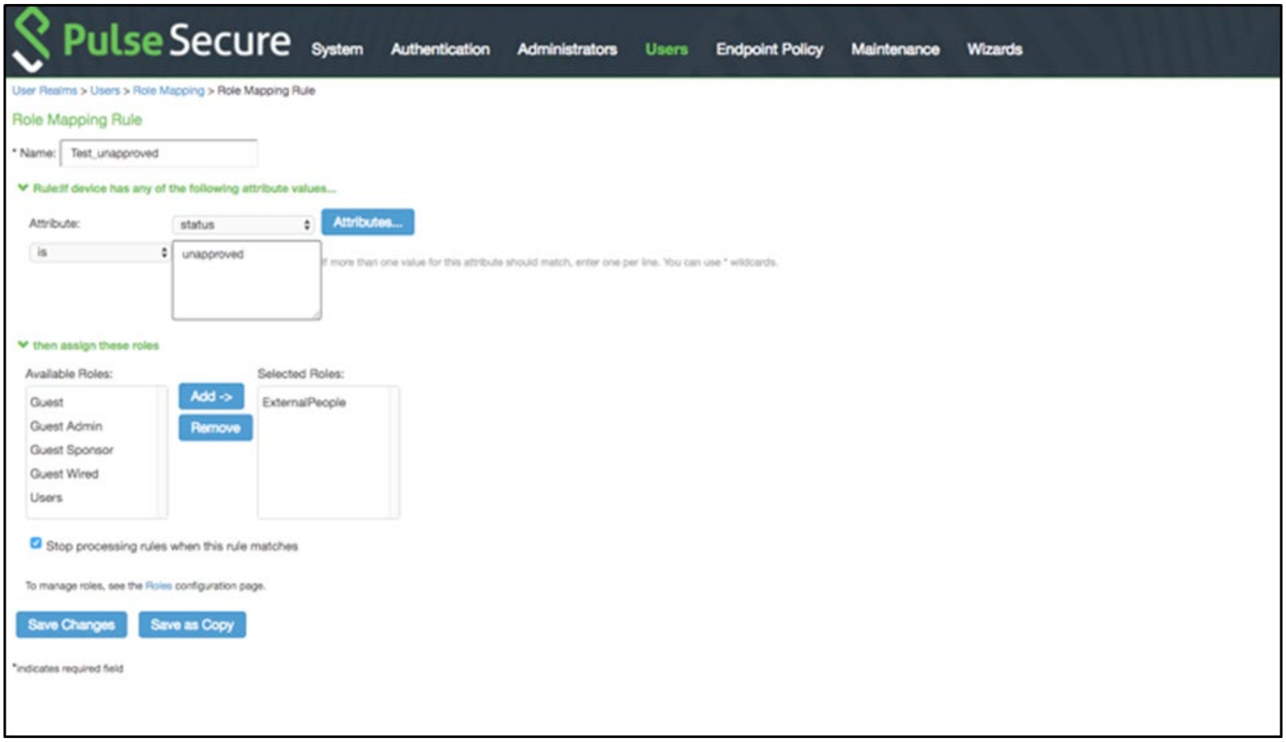
Use SSL	☐ Enabled	
*SMTP Port:	25	Port to be used for SMTP server.

Guest Access Settings

Enter settings to modify Guest User Account Manager and Guest Self-Registration features.
The SMTP settings to send account details to guest via email.

*Email Subject:	no_subject	Subject to use
*Email Format:	● html ○ text	Content type to set in the email header. The default template page is in HTML (this can be changed using Custom Pages).

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.



User Realms > Users > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name: Test_unapproved

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

Attribute: status

is: unapproved

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, Guest Admin, Guest Sponsor, Guest Wired, Users

Selected Roles: ExternalPeople

☑ Stop processing rules when this rule matches

To manage roles, see the Roles configuration page.

*indicates required field

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.

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.

Troubleshooting

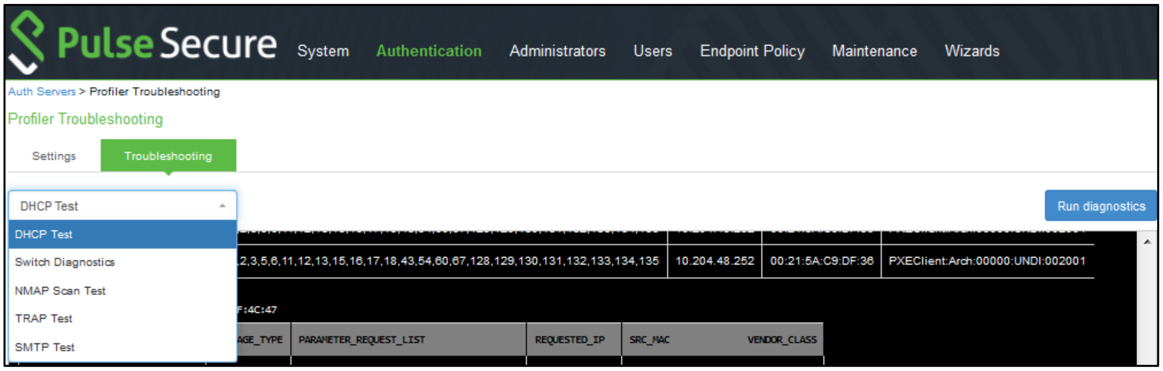
The following tests helps to identify and solve basic problems associated with configurations of the Profiler.

Test	Result
DHCP Test	• Verify if ports are receiving the DHCP packets. • Detect a device when connected to network during the diagnostic run.
Switch Diagnostics	• 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
NMAP Scan Test	• Check if NMAP scan is working for an IP address, which is prompted during diagnostic run
Trap 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**.

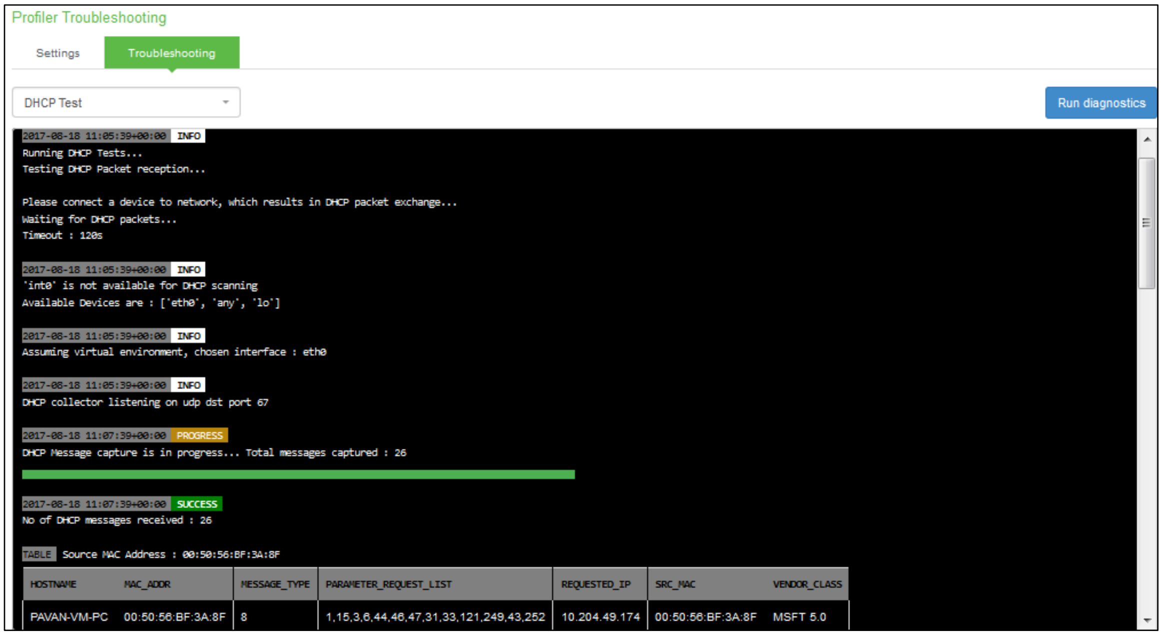
Figure 24: Troubleshooting



```
,2,3,5,6,11,12,13,15,16,17,18,43,54,60,67,128,129,130,131,132,133,134,135 | 10.204.48.252 | 00:21:5A:C9:DF:36 | PXEClient:Arch:00000:UNDI:002001

F:4C:47
AGE_TYPE | PARAMETER_REQUEST_LIST | REQUESTED_IP | SRC_MAC      VENDOR_CLASS
```

DHCP Test Example

Figure 25: DHCP Test

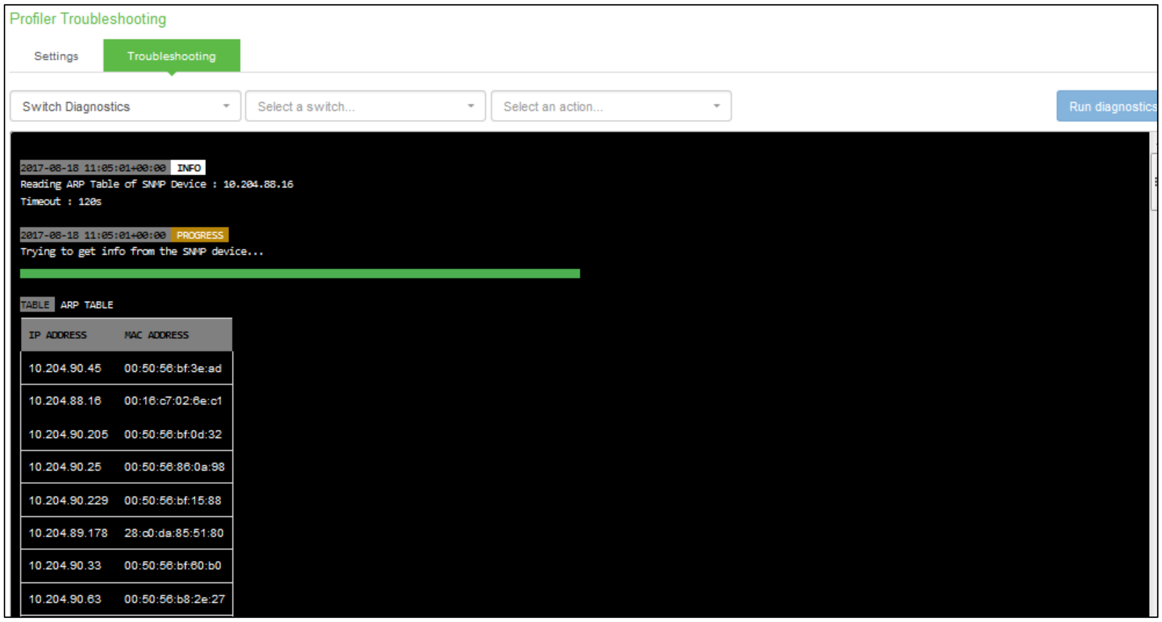


```
2017-08-18 11:05:39+00:00 INFO
Running DHCP Tests...
Testing DHCP Packet reception...

Please connect a device to network, which results in DHCP packet exchange...
Waiting for DHCP packets...
Timeout : 120s

2017-08-18 11:05:39+00:00 INFO
'int0' is not available for DHCP scanning
Available Devices are : ['eth0', 'any', 'lo']

2017-08-18 11:05:39+00:00 INFO
Assuming virtual environment, chosen interface : eth0

2017-08-18 11:05:39+00:00 INFO
DHCP collector listening on udp dst port 67

2017-08-18 11:07:39+00:00 PROGRESS
DHCP Message capture is in progress... Total messages captured : 26

2017-08-18 11:07:39+00:00 SUCCESS
No of DHCP messages received : 26

TABLE Source MAC Address : 00:50:56:BF:3A:8F
```

HOSTNAME	MAC_ADDR	MESSAGE_TYPE	PARAMETER_REQUEST_LIST	REQUESTED_IP	SRC_MAC	VENDOR_CLASS
PAVAN-VM-PC	00:50:56:BF:3A:8F	8	1,15,3,6,44,46,47,31,33,121,249,43,252	10.204.49.174	00:50:56:BF:3A:8F	MSFT 5.0

Switch Diagnostics Example

Figure 26: Switch Diagnostics

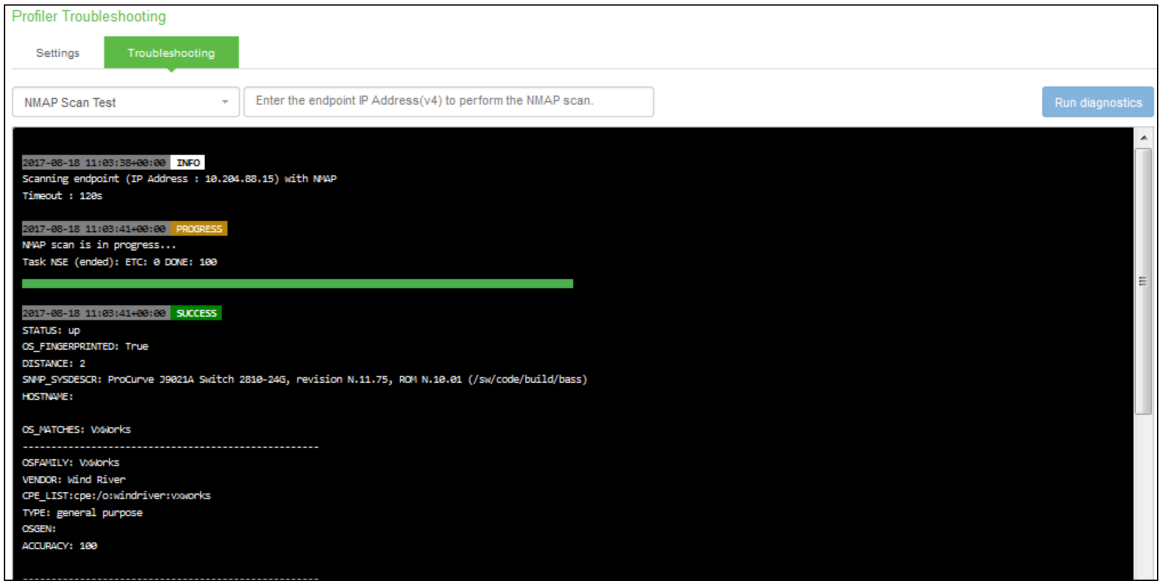


```
2017-08-18 11:05:01+00:00 INFO
Reading ARP Table of SNMP Device : 10.204.88.16
Timeout : 120s

2017-08-18 11:05:01+00:00 PROGRESS
Trying to get info from the SNMP device...

TABLE ARP TABLE
```

IP ADDRESS	MAC ADDRESS
10.204.90.45	00:50:56:bf:3e:ad
10.204.88.16	00:16:c7:02:6e:c1
10.204.90.205	00:50:56:bf:0d:32
10.204.90.25	00:50:56:86:0a:98
10.204.90.229	00:50:56:bf:15:88
10.204.89.178	28:c0:da:85:51:80
10.204.90.33	00:50:56:bf:60:b0
10.204.90.63	00:50:56:b8:2e:27

NMAP Scan Test Example

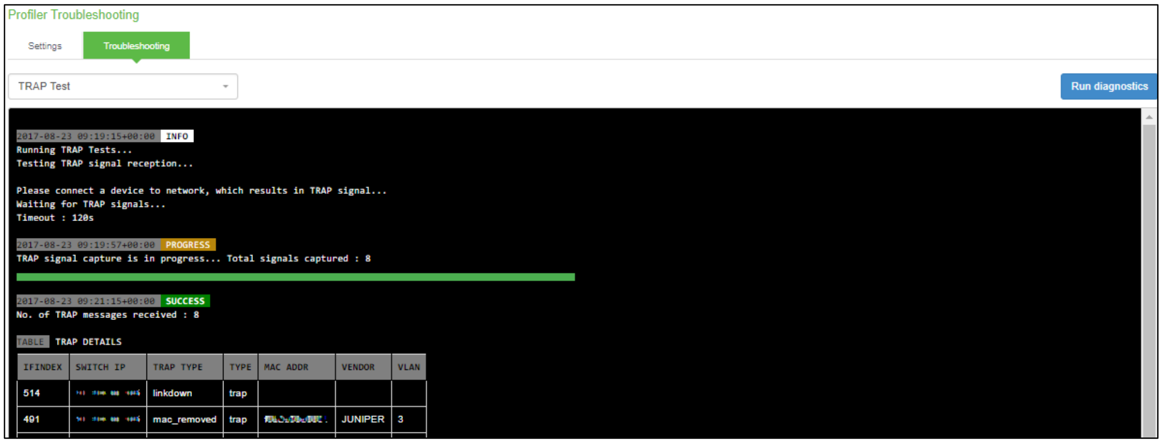
Figure 27: NMAP SCAN Test



```
2017-08-18 11:03:38+00:00 INFO
Scanning endpoint (IP Address : 10.204.88.15) with NMAP
Timeout : 120s

2017-08-18 11:03:41+00:00 PROGRESS
NMAP scan is in progress...
Task NSE (ended): ETC: 0 DONE: 100

2017-08-18 11:03:41+00:00 SUCCESS
STATUS: up
OS_FINGERPRINTED: True
DISTANCE: 2
SNMP_SYSDESCR: ProCurve J9021A Switch 2810-24G, revision N.11.75, ROM N.10.01 (/sw/code/build/bass)
HOSTNAME:

OS_MATCHES: VxWorks
---------------------------------------------------
OSFAMILY: VxWorks
VENDOR: Wind River
CPE_LIST:cpe:/o:windriver:vxworks
TYPE: general purpose
OSGEN:
ACCURACY: 100

---------------------------------------------------
```

Trap Test Example

Figure 28: Trap Test

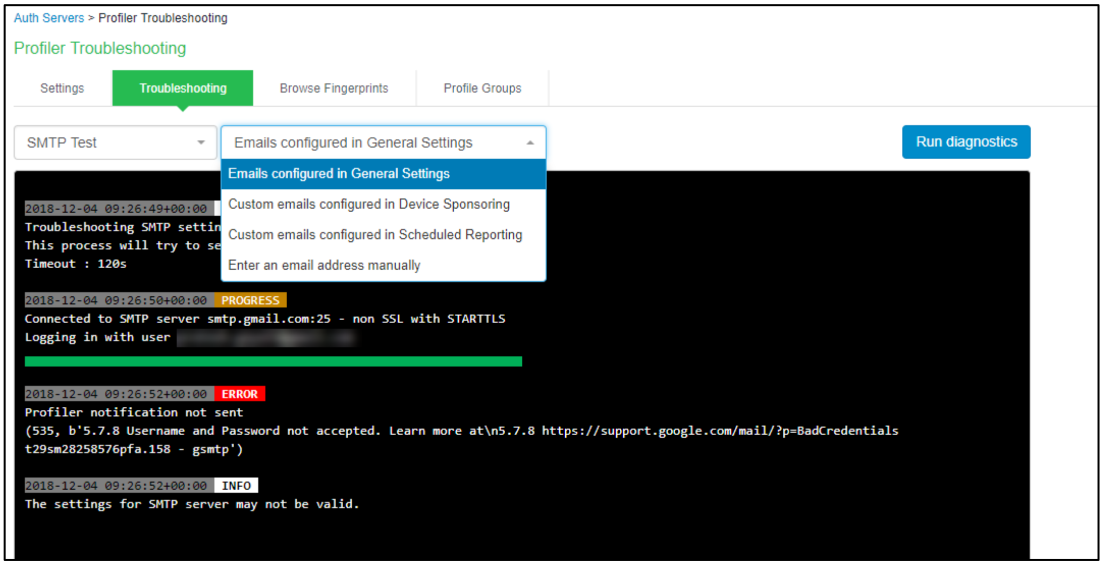


```
2017-08-23 09:19:15+00:00 INFO
Running TRAP Tests...
Testing TRAP signal reception...

Please connect a device to network, which results in TRAP signal...
Waiting for TRAP signals...
Timeout : 120s

2017-08-23 09:19:57+00:00 PROGRESS
TRAP signal capture is in progress... Total signals captured : 8

2017-08-23 09:21:15+00:00 SUCCESS
No. of TRAP messages received : 8

TABLE TRAP DETAILS
```

IFINDEX	SWITCH IP	TRAP TYPE	TYPE	MAC ADDR	VENDOR	VLAN
514	[redacted]	linkdown	trap			
491	[redacted]	mac_removed	trap	[redacted]	JUNIPER	3

SMTP Test

Figure 29: SMTP Test

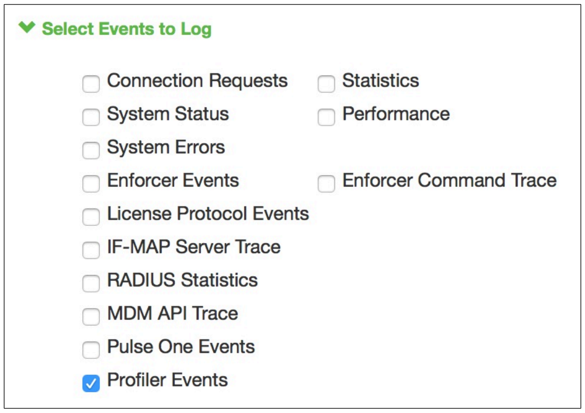

Auth Servers > Profiler Troubleshooting
Profiler Troubleshooting
Settings
Troubleshooting
Browse Fingerprints
Profile Groups
SMTP Test
Emails configured in General Settings
Emails configured in General Settings
Custom emails configured in Device Sponsoring
Custom emails configured in Scheduled Reporting
Enter an email address manually
Run diagnostics

```
2018-12-04 09:26:49+00:00
Troubleshooting SMTP settin
This process will try to se
Timeout : 120s

2018-12-04 09:26:50+00:00 PROGRESS
Connected to SMTP server smtp.gmail.com:25 - non SSL with STARTTLS
Logging in with user [redacted]

2018-12-04 09:26:52+00:00 ERROR
Profiler notification not sent
(535, b'5.7.8 Username and Password not accepted. Learn more at\n5.7.8 https://support.google.com/mail/?p=BadCredentials
t29sm28258576pfa.158 - gsmtp')

2018-12-04 09:26:52+00:00 INFO
The settings for SMTP server may not be valid.
```

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 30: List of Events to Log



Select Events to Log

□ Connection Requests □ Statistics
□ System Status □ Performance
□ System Errors
□ Enforcer Events □ Enforcer Command Trace
□ License Protocol Events
□ IF-MAP Server Trace
□ RADIUS Statistics
□ MDM API Trace
□ Pulse One Events
☑ Profiler Events

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.
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

Appendix: Configuring Cisco Switches

Configure DHCP Forwarding

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

```
1. interface <VLAN_NAME>
2. ip address <IP_ADDRESS> <NETMASK>
3. ip helper-address <DHCP_SERVER_IP>
4. ip helper-address <PPS_IP>
```

Configure CDP/LLDP

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

```
1. cdp run
2. 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.

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
```

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

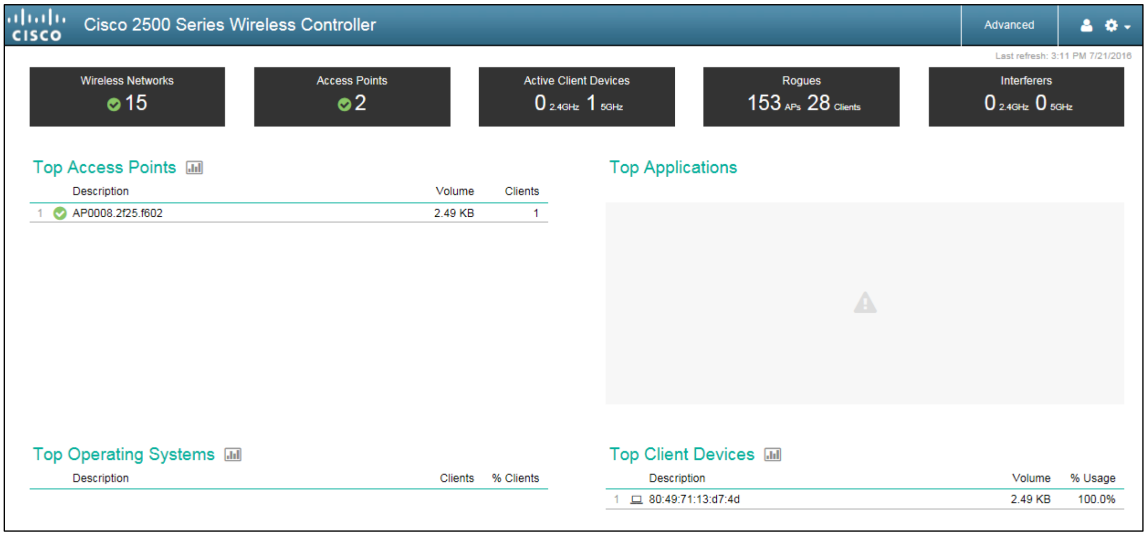
```
Switch1# sh run int g0/2
Building configuration...
Current configuration: 175 bytes
!
 interface GigabitEthernet0/2
 description To-Switch2-port-Gi0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 999
 switchport trunk native vlan 60
 switchport mode trunk end
```

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 31: Wireless LAN Controller Web UI



Top Access Points

	Description	Volume	Clients
1	AP0008.2f25.f602	2.49 KB	1

Top Operating Systems

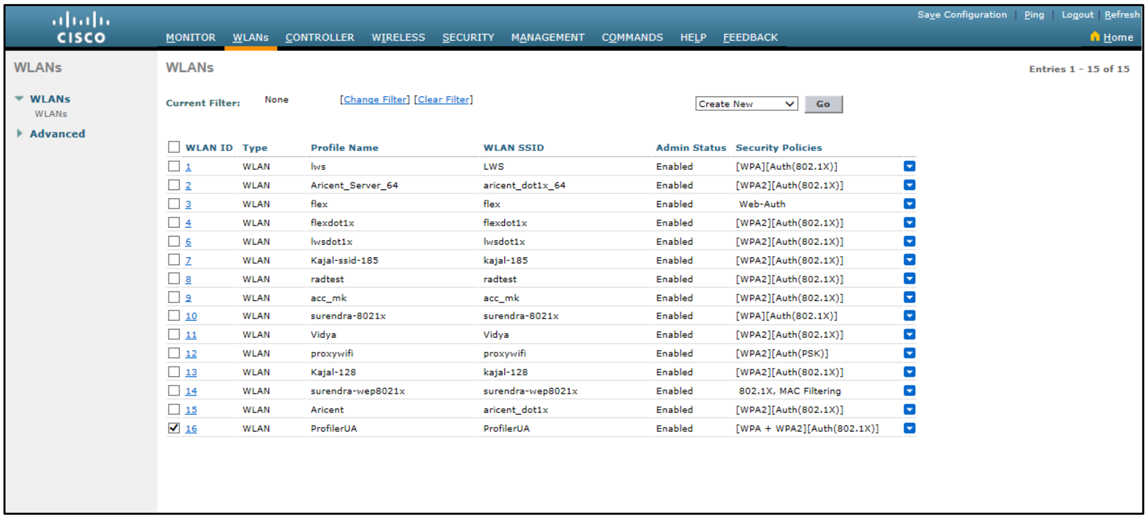
Description	Clients	% Clients

Top Client Devices

	Description	Volume	% Usage
1	80:49:71:13:d7:4d	2.49 KB	100.0%

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

Figure 32: WLANS



WLANs

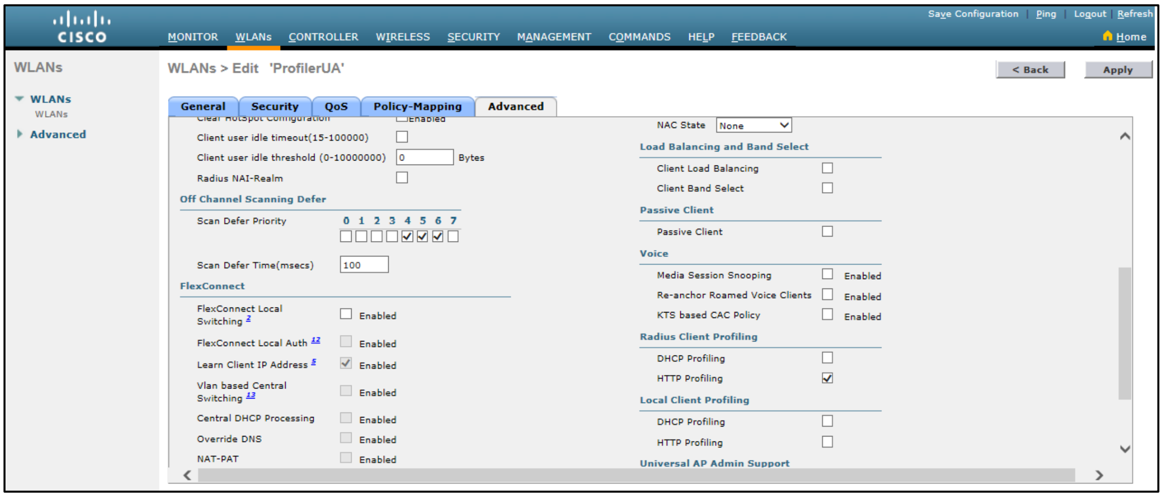
Entries 1 - 15 of 15

Current Filter: None

☐ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☐ 1	WLAN	lws	LWS	Enabled	[WPA][Auth(802.1X)]
☐ 2	WLAN	Aricent_Server_64	aricent_dot1x_64	Enabled	[WPA2][Auth(802.1X)]
☐ 3	WLAN	flex	flex	Enabled	Web-Auth
☐ 4	WLAN	flexdot1x	flexdot1x	Enabled	[WPA2][Auth(802.1X)]
☐ 6	WLAN	lwsdot1x	lwsdot1x	Enabled	[WPA2][Auth(802.1X)]
☐ 7	WLAN	Kajal-ssid-185	kajal-185	Enabled	[WPA2][Auth(802.1X)]
☐ 8	WLAN	radtest	radtest	Enabled	[WPA2][Auth(802.1X)]
☐ 9	WLAN	acc_mk	acc_mk	Enabled	[WPA2][Auth(802.1X)]
☐ 10	WLAN	surendra-8021x	surendra-8021x	Enabled	[WPA][Auth(802.1X)]
☐ 11	WLAN	Vidya	Vidya	Enabled	[WPA2][Auth(802.1X)]
☐ 12	WLAN	proxywifi	proxywifi	Enabled	[WPA2][Auth(PSK)]
☐ 13	WLAN	Kajal-128	kajal-128	Enabled	[WPA2][Auth(802.1X)]
☐ 14	WLAN	surendra-wep8021x	surendra-wep8021x	Enabled	802.1X, MAC Filtering
☐ 15	WLAN	Aricent	aricent_dot1x	Enabled	[WPA2][Auth(802.1X)]
☑ 16	WLAN	ProfilerUA	ProfilerUA	Enabled	[WPA + WPA2][Auth(802.1X)]

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

Figure 33: HTTP Profiling



WLANs > Edit 'ProfilerUA'

Clear HotSpot Configuration ☐Enabled

Client user idle timeout(15-100000) ☐

Client user idle threshold (0-10000000) 0 Bytes

Radius NAI-Realm ☐

Off Channel Scanning Defer

Scan Defer Priority 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5 ☑ 6 ☑ 7 ☐

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching [2] ☐ Enabled

FlexConnect Local Auth [12] ☐ Enabled

Learn Client IP Address [5] ☑ Enabled

Vlan based Central Switching [13] ☐ Enabled

Central DHCP Processing ☐ Enabled

Override DNS ☐ Enabled

NAT-PAT ☐ Enabled

NAC State None

Load Balancing and Band Select

Client Load Balancing ☐

Client Band Select ☐

Passive Client

Passive Client ☐

Voice

Media Session Snooping ☐ Enabled

Re-anchor Roamed Voice Clients ☐ Enabled

KTS based CAC Policy ☐ Enabled

Radius Client Profiling

DHCP Profiling ☐

HTTP Profiling ☑

Local Client Profiling

DHCP Profiling ☐

HTTP Profiling ☐

Universal AP Admin Support

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

Appendix: Configuring Juniper Switches

Configure DHCP Forwarding

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

```
1. set forwarding-options helpers bootp interface <VLAN_NAME>
2. set forwarding-options helpers bootp server <DHCP_SERVER_IP>
3. set forwarding-options helpers bootp server <PPS_IP>
```

For Juniper Switch OS version 15.x and above

```
4. set forwarding-options dhcp-relay server-group dhcp-server <DHCP Sever>
5. set forwarding-options dhcp-relay server-group dhcp-server <PPS IP>
6. set forwarding-options dhcp-relay active-server-group dhcp-server
7. set forwarding-options dhcp-relay group dhcp-server interface irb.X
8. 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 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
```

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:

   ```
   [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
   ```

Appendix: Configuring HP (Procurve) Switches

Configure DHCP Forwarding

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

```
1. vlan <VLAN_NAME>
2. ip helper-address <DHCP_SERVER_IP>
3. 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#>
```