



Pulse Policy Secure Profiler: Deployment Guide

Published	15 January, 2020
Document Version	1.4

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

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: PORTS USED FOR PROFILING	45

Introduction

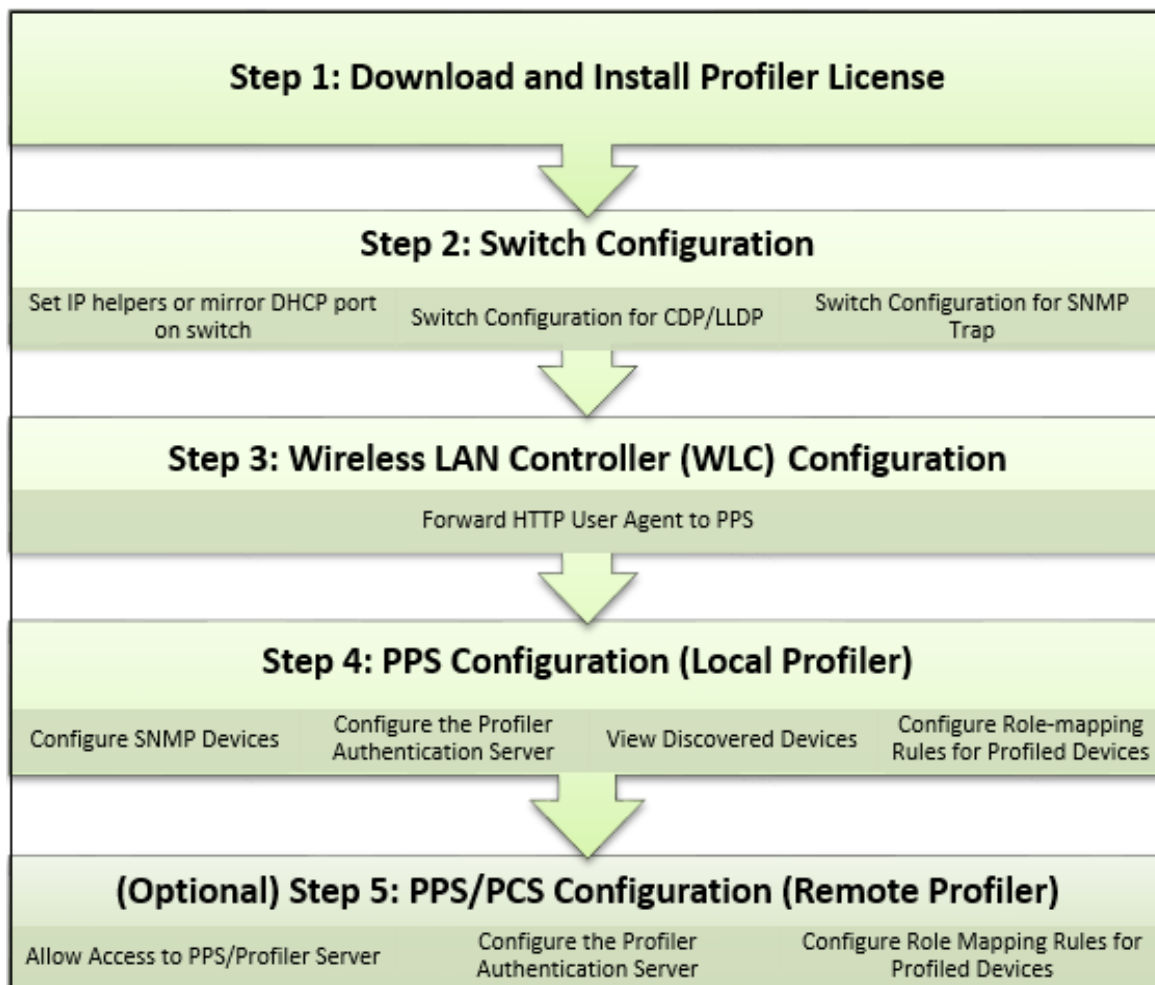
The Profiler dynamically identifies and classifies both managed and unmanaged endpoint devices, enabling control of access to networks and resources based on the type of the device.

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



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, 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

Configuration > Licensing > Download License

Download License

Configuration
Licensing

Licensing | Configure Server | **Download Licenses**

Periodic license downloads

Use this section to modify settings for periodic license downloads.

Preferred Network:

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

Periodic license downloads

☐ Enabled

☒ Disabled

Save Changes

On demand license downloads

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

Download and Install

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

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

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

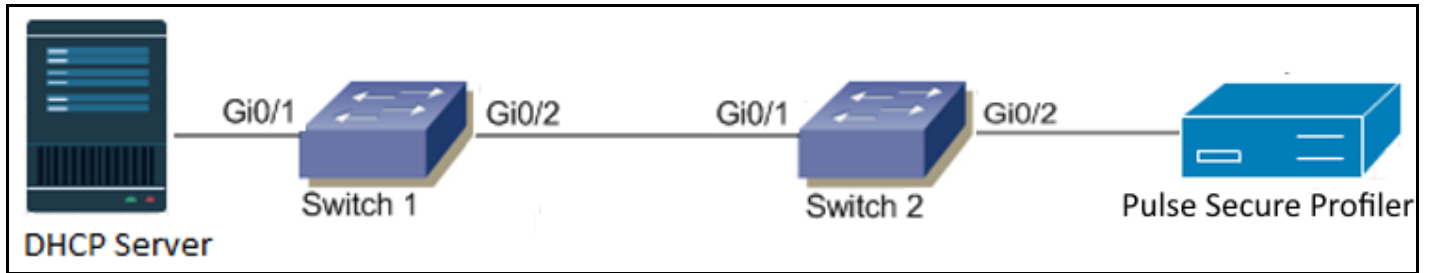
The Profiler uses the Link Up/Down and MAC notification traps to:

- 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.

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.

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)

• 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.

Figure 4 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: Device Vendor.

SNMP enforcement ☐ Use this device for SNMP policy enforcement.

▼ **SNMP Settings**

Same credentials for Trap user ☒

*Read Community String:

Save Changes

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

Figure 5 SNMP Device Configuration Table

Network Access > SNMP Device Configuration

SNMP Device Configuration

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

Configuration | Discovery

New SNMP Device | Duplicate | Delete | Enable | Disable

10 records per page

Search:

	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: bnb4-104_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 Local Profiler Authentication Server

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

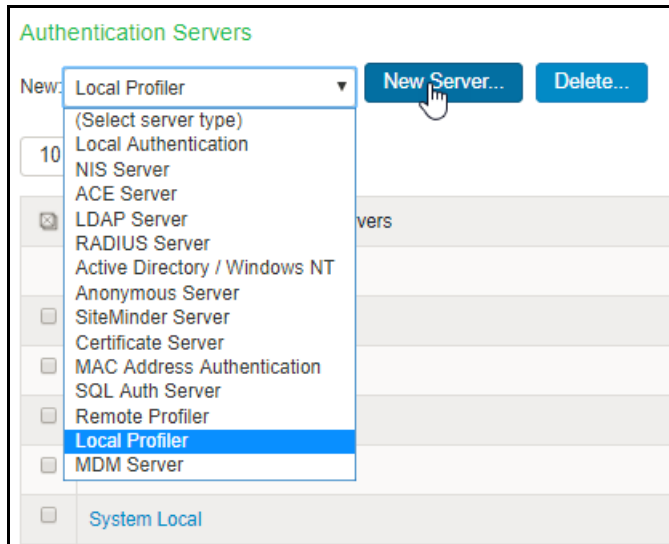
- If you wish to use DHCP fingerprinting, you have configured the switch(es) to forward DHCP packets to the PPS.
- If you wish to use SNMP/SSH-based profiling from Network Infrastructure Devices, you have configured one or more switches in the Network Infrastructure Device page of the PPS Administrator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

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

To create a new Local Profiler Authentication Server:

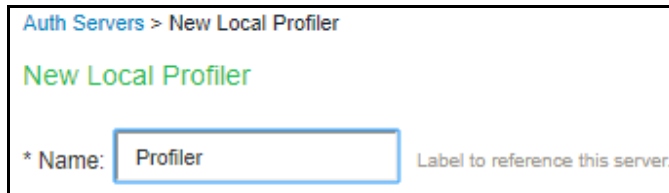
1. Select **Authentication > Auth.Servers**.
2. Select **Local Profiler** from the server type drop-down list and click **New Server**.

Figure 6 Creating a Local Profiler Authentication Server



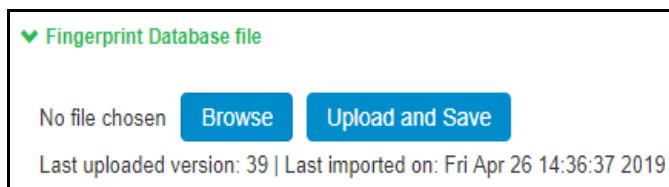
3. Enter a name for the Authentication server.

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.

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

Figure 9 General Settings

General Settings

* Poll Interval:

* DHCP Sniffing mode:

* Purge devices older than:

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

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](#)

<input type="checkbox"/> BSD	<input type="checkbox"/> Datacenter appliance	<input type="checkbox"/> Gaming Consoles	<input type="checkbox"/> Home Audio/Video Equipment	<input type="checkbox"/> Internet of Things
<input type="checkbox"/> Linux	<input type="checkbox"/> Macintosh	<input type="checkbox"/> Medical Device	<input type="checkbox"/> Monitoring Devices	<input type="checkbox"/> Network Bridge
<input type="checkbox"/> Other OS	<input type="checkbox"/> Physical Security	<input type="checkbox"/> Point of Sale devices	<input type="checkbox"/> Printers/Scanners	<input type="checkbox"/> Projectors
<input type="checkbox"/> Routers and APs	<input type="checkbox"/> Smartphones/PDAs/Tablets	<input type="checkbox"/> Storage Devices	<input type="checkbox"/> Switches	<input type="checkbox"/> Thin Client
<input type="checkbox"/> Video Conferencing	<input type="checkbox"/> VoIP Phones/Adapters	<input type="checkbox"/> Windows		

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(,).

[Test Settings](#)

☒ 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.

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.

Figure 11 Adding One or More Subnets

▼ Endpoints to scan using Active Collectors

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

Security products such as antivirus etc may block active scan on endpoints.
It is recommended to disable such blocks for better discovery and classification.

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.

<input type="checkbox"/>	Subnet	Include/Exclude	Collector	
<input type="checkbox"/>	<input type="text"/>	<input checked="" type="radio"/> Include <input type="radio"/> Exclude	<input checked="" type="checkbox"/> NMAP <input type="checkbox"/> WMI <input type="checkbox"/> SSH <input type="checkbox"/> SNMP(HOST)	<input type="button" value="Add"/>
<input type="checkbox"/>	10.204.0.0/16	Include	NMAP, WMI	
<input type="checkbox"/>	172.21.0.0/16	Include	SSH	

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

▼ SNMP(HOST) Profiling

If Endpoints are being monitored through SNMP then Profiler will fetch device attributes through SNMP.

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

▼ WMI Profiling

☒ Configure WMI credentials.
 ☐ Use Active Directory server credentials.

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

*Password:

Endpoint ip or hostname on which credentials can be tested

☒ Allow deep scan Deep scan fetches advanced attributes from windows endpoints

Disable deep scan if registry scan, process details etc are not useful, as getting them from each endpoint is a time consuming process. But, note that agentless hostchecking with profiler uses these attributes for some of its policies.

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

SSH Profiling

Authentication Method: Public key

*User:

*Private key:

passphrase:

Test Credentials

Endpoint ip or hostname on which credentials can be tested

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

Figure 15 MDM Server

MDM Server

MDM server: mobilemdm

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

Figure 16 LDAP Server

LDAP Server

LDAP server: 10.209.116.151

13. (Optional) In the Forward and Sync endpoints section, enter the FQDN or the IP address of the linking local 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

Forward and Sync endpoints

Forward and sync this profiler's data to a another local profiler

*Local Profiler to link: Fully qualified domain name (FQDN) or IP address

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

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](#)

View Discovered Devices

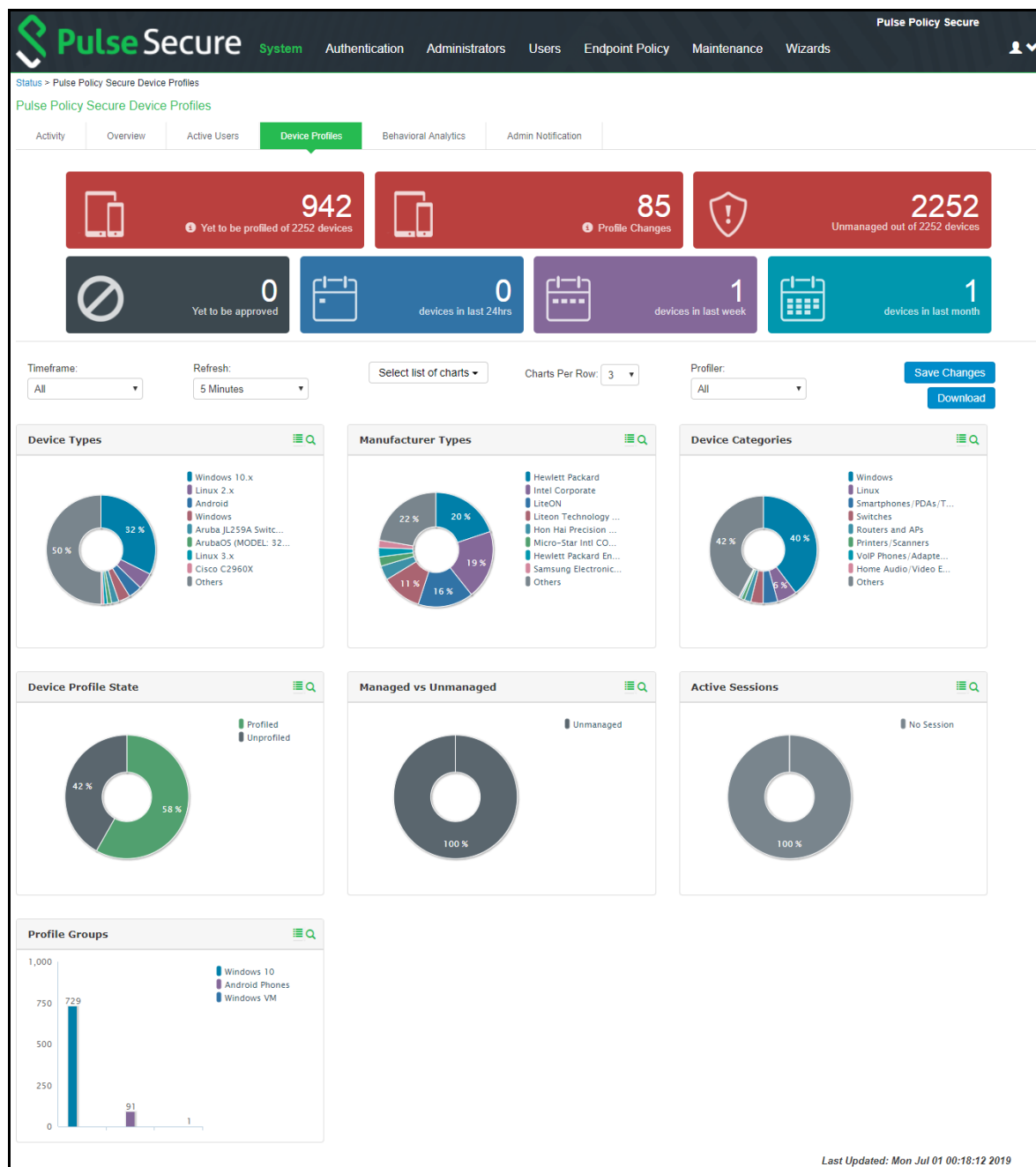
Dashboard View

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

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](#)

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

Figure 19 Device Discovery Report Table

Profiler	MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	Session User	First Seen	Last Updated	Profiler(s)	Groups
	2e:b6:93:09:b9:1f	10.204.56.84			Linux 3.x	Linux		Tue, 26 Mar 2019 13:09:28	Tue, 26 Mar 2019 13:09:46	- Local Profiler	
	00:50:56:83:cd:be	10.96.77.173		VMware, Inc.				Tue, 26 Mar 2019 13:09:26	Tue, 26 Mar 2019 13:09:26	- Local Profiler	
	00:50:56:83:6b:c0	10.96.77.174		VMware, Inc.				Tue, 26 Mar 2019 13:09:24	Tue, 26 Mar 2019 13:09:24	- Local Profiler	
	de:c1:31:b9:3d:dc	10.204.58.34			Linux 3.x	Linux		Tue, 26 Mar 2019 13:09:24	Tue, 26 Mar 2019 13:09:46	- Local Profiler	
	52:54:00:58:f6:16	10.209.116.212						Tue, 26 Mar 2019 12:09:32	Tue, 26 Mar 2019 13:09:32	- Local Profiler	
	d8:c7:71:34:2f:fa	10.204.90.65		HUAWEI TECHNOLOGIES CO.,LTD				Tue, 26 Mar 2019 12:09:32	Tue, 26 Mar 2019 12:11:34	- Local Profiler	
	00:50:56:83:13:81	10.96.78.21		VMware, Inc.				Tue, 26 Mar 2019 12:09:31	Tue, 26 Mar 2019 13:09:31	- Local Profiler	
	c0:ee:fb:f3:5b:04	10.204.90.88		OnePlus Tech (Shenzhen) Ltd				Tue, 26 Mar 2019 12:09:29	Tue, 26 Mar 2019 13:09:29	- Local Profiler	
	ca:ac:b4:b4:26:2b	10.204.58.28			Linux 3.x	Linux		Tue, 26 Mar 2019 12:09:27	Tue, 26 Mar 2019 13:09:28	- Local Profiler	
	00:50:56:83:61:03	10.96.77.172		VMware, Inc.				Tue, 26 Mar 2019 11:09:29	Tue, 26 Mar 2019 11:09:29	- Local Profiler	

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**.

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.

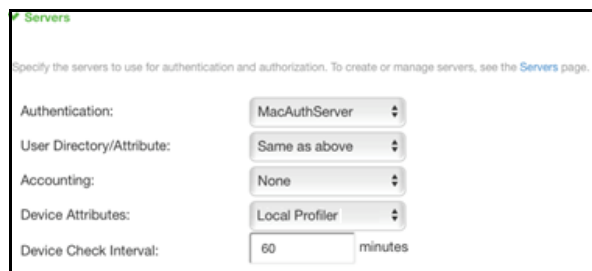
Configuring Role-Mapping Rules for Profiled Devices

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

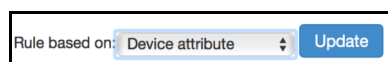


The screenshot shows the 'Servers' configuration page. It has a title 'Servers' with a green checkmark icon. Below the title is a subtitle: 'Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.' The main content area contains five rows of configuration options, each with a label and a dropdown menu or input field:

- Authentication: MacAuthServer
- User Directory/Attribute: Same as above
- Accounting: None
- Device Attributes: 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 click **Update**.

Figure 21 Rule based on attribute



The screenshot shows a 'Rule based on' dropdown menu. The dropdown is open, showing 'Device attribute' as the selected option. To the right of the dropdown is a blue button labeled 'Update'.

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.

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

Figure 23 Creating New Role Mapping Rule with LDAP Attributes

Role Mapping Rule

Rule based on: Device attribute Update

* Name:

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

Attribute: (Select an attribute) Attributes...

☐ is

☒ is equal to LDAP attribute ldapServer is configured as LDAP Server in Authentication Server Local Profiler. Attributes...

✓ **then assign**

Available Roles: Guest Guest Admin Guest Sponsor Guest Wired Users

Selected Roles: (none)

☐ Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

- 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.

PPS/PCS Configuration (Remote Profiler)

This configuration procedure is optional.

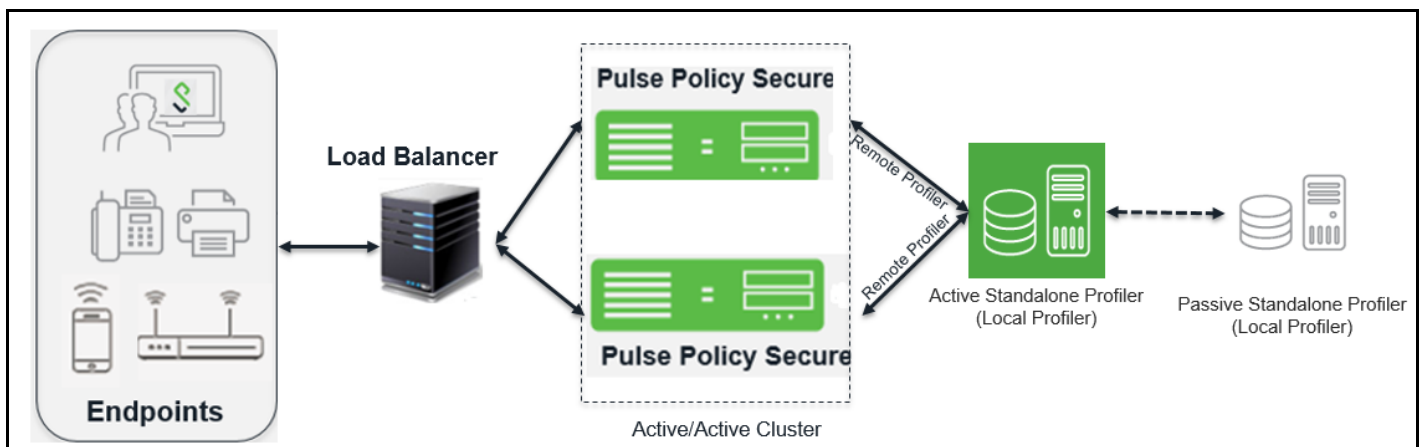
A Remote Profiler can be useful in the following cases:

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.

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

The screenshot shows the 'Update Administrator admin' form. The 'Full Name' field is 'Platform Administrator'. The 'Authenticate using' dropdown is 'Administrators'. The 'Password' and 'Confirm Password' fields are masked with dots. The 'Start Time' and 'End Time' fields are empty. The 'Time Zone' dropdown is '(GMT-08:00) Pacific Time (US & Canada); Tijuana'. The 'Allow access to profiler using REST APIs' checkbox is checked and highlighted with a red box. Below it, the 'Enabled' radio button is selected. Other options include 'One-time use (disable account after the next successful sign-in)', 'Allow console access', 'Disabled', 'Quarantined', and 'Require user to change password at next sign in'. A note at the bottom states: '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 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

The screenshot shows the 'New Remote Profiler' form. The '*Name:' field is 'My Remote Profiler' with a tooltip 'Label to reference this server.'. The '*Remote Profiler:' field is '1.2.3.4' with a tooltip 'Fully qualified domain name (FQDN) or IP address' and a clear button. The '*API Key:' field has a 'Get API Key' button and a tooltip 'Auto-completed when API key is retrieved'. At the bottom are 'Save Changes' and 'Reset' buttons. A note at the bottom left states: '* indicates required field'.

- 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

Get API Key

*Admin Name: Admin user name of Remote Profiler.

*Admin Password: Admin password of Remote Profiler.

*Validate Server Certificate: ☐ Check if server certificate validation is required.

Next Cancel

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.

- 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](#)

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

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			
Details History			
Showing last 10 IP Addresses for the selected device			
Source	Change Detected	host-name	IP Address
dhcp	Wed, 07 Dec 2016 20:10:30	vreddy	10.209.122.161
dhcp	Wed, 07 Dec 2016 20:09:53	vreddy	

- **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

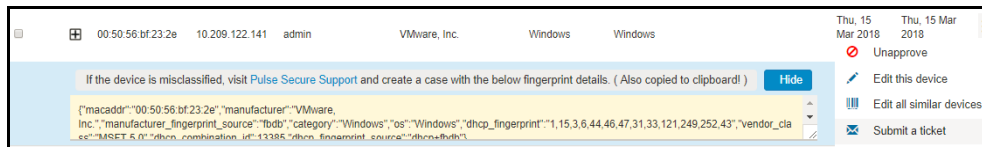
Note: If an endpoint is classified incorrectly, please see the Troubleshooting section to rectify the problem.

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 unapprove a specific device. See [Device Sponsoring](#) for more information.

- **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 fingerprint 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

✓ **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](#)

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

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(,).

[Test Settings](#)

✓ 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

3. Configure the SMTP server.

Figure 31 Configuring SMTP Server

General SMTP Settings

☒ Enabled
 *SMTP Server: IP Address or hostname of the SMTP server
 SMTP Login: Required if the server requires credentials to relay
 SMTP Password: Required if the server requires credentials to relay
 *SMTP Email: 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: 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: 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).

[Save Changes](#)

- 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'`.

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

User Reams > Users > Role Mapping > Role Mapping Rule

Role Mapping Rule

Name:

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

Attribute: [Attributes...](#)

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, Users

Selected Roles: ExternalPeople

☒ Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

[Save Changes](#) [Save as Copy](#)

*Indicates required field

- 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

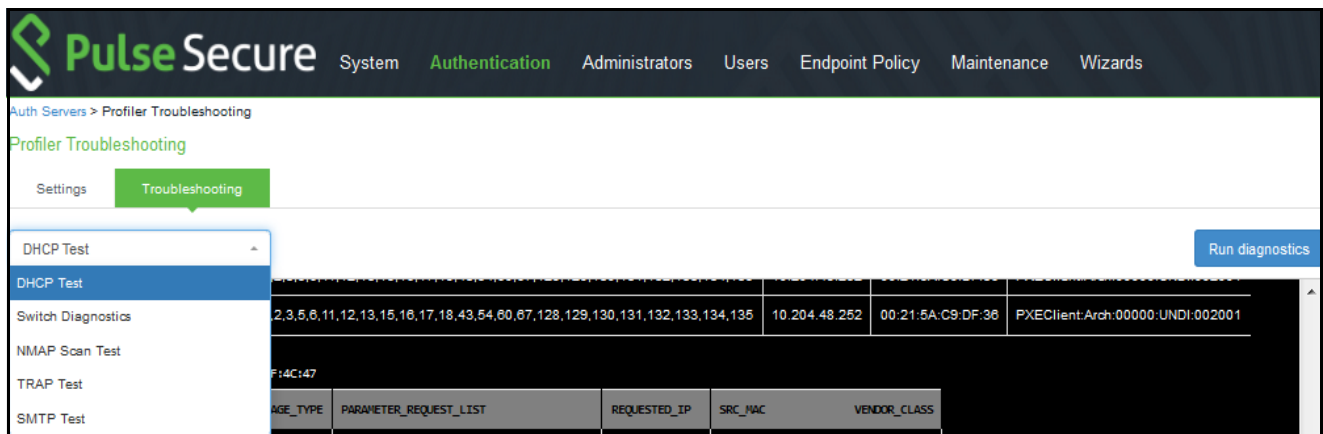
The following tests help to identify and solve basic problems associated with configurations of the Profiler.

Test	Result
"DHCP Test Example"	<ul style="list-style-type: none"> Verify if ports are receiving the DHCP packets. Detect a device when connected to network during the diagnostic run.
"Switch Diagnostics Example"	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Check if the Profiler can fetch the Endpoint information through SNMP.
"NMAP Scan Test Example"	<ul style="list-style-type: none"> Check if NMAP scan is working for an IP address, which is prompted during diagnostic run
"SMTP Test"	<ul style="list-style-type: none"> Verify if trap is collected or not for a switch event. Detect a device when connected to network during the diagnostic run.
"SMTP Test"	<ul style="list-style-type: none"> 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



DHCP Test Example

Figure 33 DHCP Test

Profiler Troubleshooting

Settings Troubleshooting

DHCP Test Run diagnostics

```

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	1,15,3,6,44,40,47,31,33,121,249,43,252	10.204.49.174	00:50:56:BF:3A:8F	MSFT 5.0

Switch Diagnostics Example

Figure 34 Switch Diagnostics

Profiler Troubleshooting

Settings Troubleshooting

Switch Diagnostics Select a switch... Select an action... Run diagnostic

```

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:bf3e:ad
10.204.88.16	00:16:c7:02:6e:c1
10.204.90.205	00:50:56:bf0d:32
10.204.90.25	00:50:56:80:0a:98
10.204.90.229	00:50:56:bf15:88
10.204.89.178	28:c0:da:85:51:80
10.204.90.33	00:50:56:bf60:b0
10.204.90.63	00:50:56:b8:2e:27

NMAP Scan Test Example

Figure 35 NMAP SCAN Test

Profiler Troubleshooting

Settings Troubleshooting

NMAP Scan Test Enter the endpoint IP Address(v4) to perform the NMAP scan. Run diagnostics

```

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 39021A Switch 2810-24G, revision N.11.75, ROM N.10.01 (/sw/code/build/bass)
HOSTNAME:

OS_WATCHES: Vxworks
-----
OSFAMILY: Vxworks
VENDOR: Wind River
CPE_LIST: cpe:/o:windriver:vxworks
TYPE: general purpose
OSGEN:
ACCURACY: 100
  
```

Trap Test Example

Figure 36 Trap Test

Profiler Troubleshooting

Settings Troubleshooting

TRAP Test Run diagnostics

```

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
  
```

IFINDEX	SWITCH IP	TRAP TYPE	TYPE	MAC ADDR	VENDOR	VLAN
514	10.204.88.15	linkdown	trap			
401	10.204.88.15	mac_removed	trap	00:00:00:00:00:00	JUNIPER	3

SMTP Test

Figure 37 SMTP Test

The screenshot displays the 'Profiler Troubleshooting' section of the Pulse Policy Secure Profiler interface. The 'Troubleshooting' tab is active, and the 'SMTP Test' dropdown menu is open, showing options: 'Emails configured in General Settings' (selected), 'Custom emails configured in Device Sponsoring', 'Custom emails configured in Scheduled Reporting', and 'Enter an email address manually'. A 'Run diagnostics' button is visible in the top right corner.


The main area shows the results of the SMTP test:

```
2018-12-04 09:26:49+00:00 Troubleshooting SMTP settings. This process will try to send an email. 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 https://support.google.com/mail/?p=BadCredentials&context=android')
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 38 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 (xxxxxxxxxxx) 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.

When	Where	What
Polling SNMP switch	Event Log	<p>Polling SNMP switch: 'Name: hp IP: XX.XX.XX.XX Version: 3'</p> <p>SNMP Scan: 'Start: Fri Jul 22 xx:xx:xx:xx 2016'</p> <p>SNMP endpoint count: For WLC named XX is XX</p> <p>SNMP endpoint count: For Switch named XXX is XX</p> <p>SNMP endpoint count: No endpoints connected to switch Or WLC named XXX</p> <p>SNMP endpoint count: Total XX</p> <p>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</p> <p>SNMPPollError: Switch (Name: XXX IP: XX.XX.XX.XX) is disabled under Endpoint Policy->Network Access->SNMP Device->Configuration. Please enable to start polling</p> <p>SNMPPollError: Unable to retrieve the CAM table from the switch. (Name: XXX IP: XX.XX.XX.XX). Please check the Switch configuration</p>
Fetching devices from switches	Event Log	SNMP Endpoint Count: 'For Switch named nn:nn:nn:nn is 278'
Cluster replication	Event Log	<p>Starting services: Profiler replicator</p> <p>Started syncing state</p> <p>Completed syncing state</p>
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	<p>WMI Connection failed: endpoint Mac:XX:XX:XX:XX:XX:XX ip:XX.XX.XX.XX reason XXX</p> <p>WMI Query failed: endpoint Mac:XX:XX:XX:XX:XX:XX ip:XX.XX.XX.XX query XXX</p>

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.

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

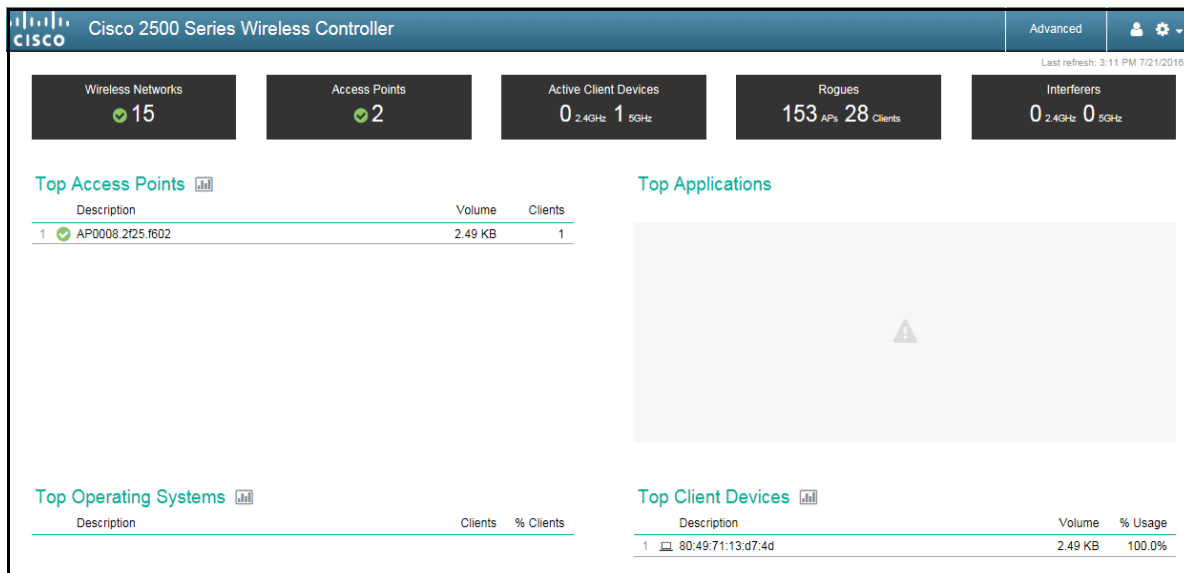
```
Switch1# sh run int g0/2
Building configuration...
Current configuration: 175 bytes
!
interface GigabitEthernet0/2
description To-Switch2-port-Gi0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 999
switchport trunk native vlan 60
switchport mode trunk end
```

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 39 Wireless LAN Controller Web UI



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

Figure 40 WLANs

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	lvs	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	lvsdot1x	lvsdot1x	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_mik	acc_mik	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	ProfilierUA	ProfilierUA	Enabled	[WPA + WPA2][Auth(802.1X)]

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

Figure 41 HTTP Profiling

WLANs > Edit 'ProfilierUA'

General Security QoS Policy-Mapping **Advanced**

Client user idle timeout(15-100000) ☐ Enabled

Client user idle threshold (0-10000000) Bytes

Radius NAI-Realm ☐ Enabled

Off Channel Scanning Defer

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

Scan Defer Time(msecs)

FlexConnect

FlexConnect Local Switching ☐ Enabled

FlexConnect Local Auth ☒ Enabled

Learn Client IP Address ☒ Enabled

Vlan based Central Switching ☐ Enabled

Central DHCP Processing ☐ Enabled

Override DNS ☐ Enabled

NAT-PAT ☐ Enabled

NAC State

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

- 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.

```
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
```

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.

```
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#>
```


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	<ul style="list-style-type: none"> 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)

