



Pulse Policy Secure Profiler: Deployment Guide

Published **July 2020**

Document Version **1.6**

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
STANDALONE PROFILER.....	3
BACKUP AND RECOVERY	3
REMOTE PROFILER	4
BACKUP AND RECOVERY	4
PROFILING DEVICES IN BRANCH OFFICES	4
USING PROFILER FORWARDER	4
BACKUP AND RECOVERY	5
USING LINKED PROFILER (WITH PPS FUNCTIONALITY).....	6
BACKUP AND RECOVERY	6
DOWNLOAD AND INSTALL PROFILER LICENSE	7
SWITCH CONFIGURATION.....	8
FORWARDING DHCP REQUESTS TO PPS	8
SWITCH CONFIGURATION FOR CDP/LLDP.....	8
SWITCH CONFIGURATION FOR SNMP TRAPS.....	8
CONFIGURING THE PROFILER TO WORK WITH RSPAN CONFIGURATION	8
WIRELESS LAN CONTROLLER (WLC) CONFIGURATION	10
FORWARDING HTTP USER AGENT TO PPS	10
PPS CONFIGURATION (LOCAL PROFILER).....	11
CONFIGURING SNMP DEVICES	11
CONFIGURING THE LOCAL PROFILER AUTHENTICATION SERVER	12
BASIC PROFILER CONFIGURATION	12
ADVANCE PROFILER CONFIGURATION.....	16
WMI CONFIGURATION	16
SSH CONFIGURATION.....	17
SNMP (HOST) CONFIGURATION	18
DEVICE ATTRIBUTE SERVER CONFIGURATION	19
ADDITIONAL DATA COLLECTORS CONFIGURATION	19
SUBNETS CONFIGURATION	20
FORWARD AND SYNC ENDPOINT DATA	20
VIEW DISCOVERED DEVICES	21
DASHBOARD VIEW.....	21
DEVICE DISCOVERY REPORT VIEW	22

CONFIGURING PROFILE GROUPS.....	23
CONFIGURING ROLE-MAPPING RULES FOR PROFILED DEVICES.....	24
PPS/PCS CONFIGURATION (REMOTE PROFILER).....	27
ALLOWING ACCESS TO THE PROFILER	27
CONFIGURING REMOTE PROFILER AUTHENTICATION SERVER.....	28
CONFIGURING ROLE-MAPPING RULES FOR PROFILED DEVICES.....	29
TESTS.....	30
DIAGNOSTIC LOGS	31
PROFILER LOGS.....	31
APPENDIX: CONFIGURING CISCO SWITCHES	34
CONFIGURE DHCP FORWARDING.....	34
CONFIGURE CDP/LLDP	34
CONFIGURE SNMP TRAPS	34
CONFIGURE RSPAN.....	35
FORWARD HTTP USER AGENT DATA.....	36
APPENDIX: CONFIGURING JUNIPER SWITCHES	38
CONFIGURE DHCP FORWARDING.....	38
CONFIGURE LLDP	38
CONFIGURE SNMP TRAPS	38
CONFIGURE RSPAN.....	39
APPENDIX: CONFIGURING HP (PROCURVE) SWITCHES	41
CONFIGURE DHCP FORWARDING.....	41
CONFIGURE LLDP	41
CONFIGURE SNMP TRAPS	41
CONFIGURE RSPAN.....	41
APPENDIX: CONFIGURING VIPTELA SWITCHES.....	42
CONFIGURE SNMP ON VIPTELA SWITCH	42
SAMPLE CONFIGURATION.....	42
APPENDIX: PORTS USED FOR PROFILING	44

Introduction

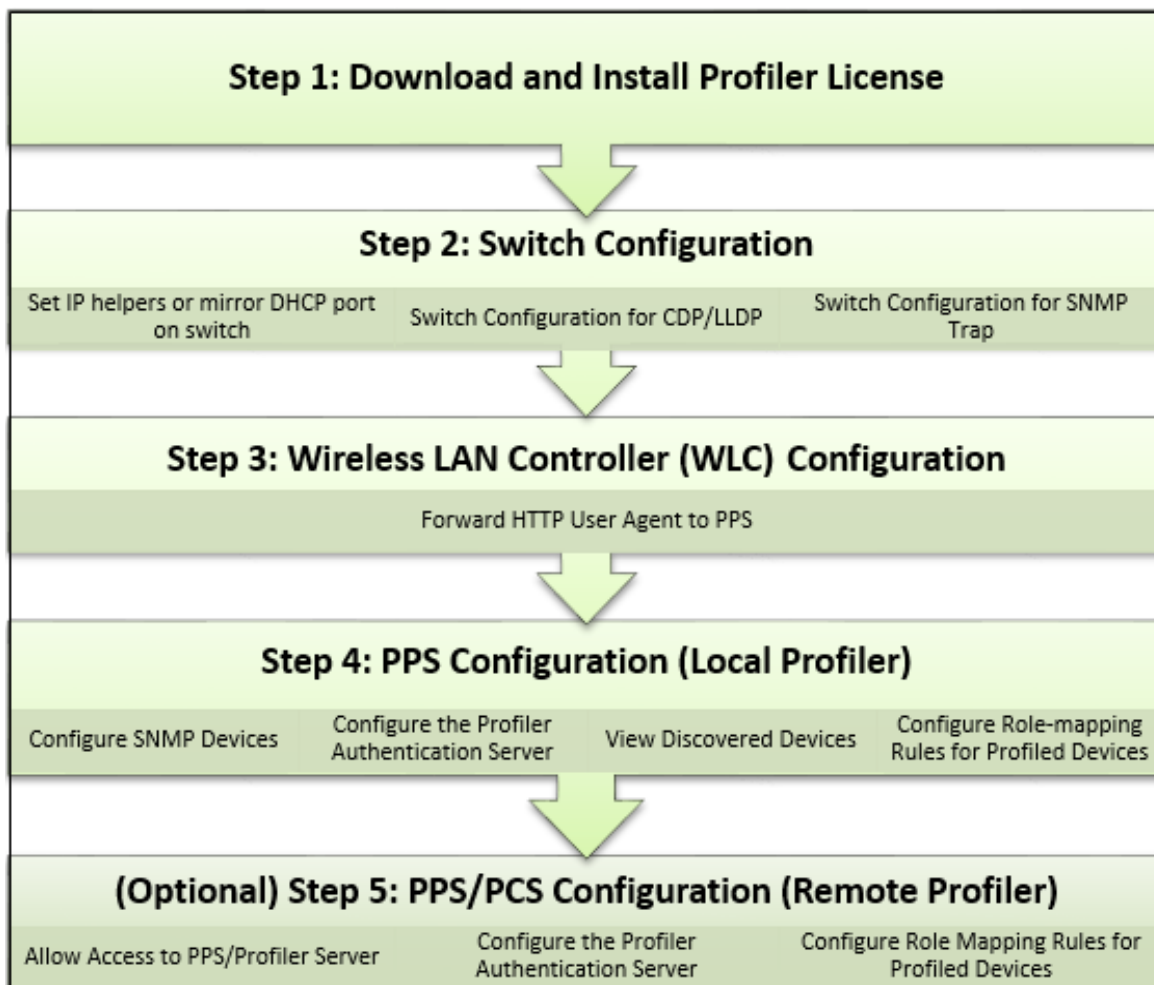
The Profiler dynamically identifies and classifies both managed and unmanaged endpoint devices, enabling control of access to networks and resources based on the type of the device.

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

Profiler Deployment Cases

- **Standalone Profiler** 3
- **Remote Profiler** 4
- **Profiling devices in branch offices** 4

The Profiler can be deployed on a standalone, remote, or distributed networks.

Standalone Profiler

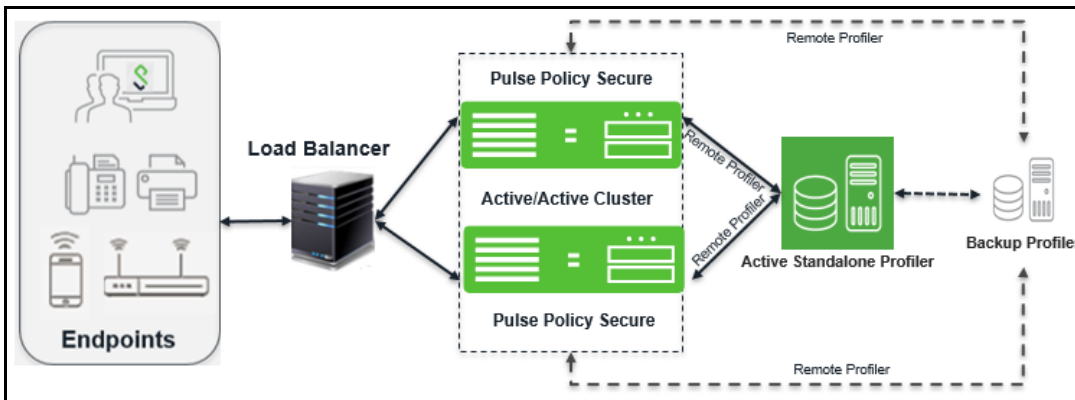
Standalone Profiler can be deployed as an independent appliance. All PPS and PCS appliances communicate with this Standalone Profiler for authorization.

A Standalone Profiler is 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 unclustered set) of PPS appliances.

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

Figure 2 Example of a Standalone Profiler deployed in a typical PPS Active/Active cluster



When user connects to a 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 Profiler.
- The Profiler returns Device OS, Device Manufacturer, Device Category and Session Identifier to PPS/PCS.
- The Profiler updates the PCS/PPS session with the device attributes and triggers role re-evaluation.

Backup and recovery

When the forwarder fails to connect to the Standalone Profiler, the forwarder sends the profiled endpoint information to the Backup Standalone server. On establishing the connection with the primary standalone profiler, the forwarder sends the latest information to sync with the primary standalone profiler.

Remote Profiler

A Remote Profiler can be configured on a PCS/PPS appliance to profile devices that are connected to them. To configure the remote profiler, the IP address of the standalone Profiler is configured on the PCS/PPS. The remote profiler is configured as device attribute server and used in role mapping rules.

A Remote Profiler is useful to view all endpoints inside and outside the network.

Figure 3 Example of a Remote Profiler

The screenshot shows the 'New Remote Profiler' configuration form. At the top, there is a breadcrumb 'Auth Servers > New Remote Profiler' and a title 'New Remote Profiler'. The form contains several fields with asterisks indicating they are required:

- *Name:** A text input field with a placeholder 'Label to reference this server.'
- *Remote Profiler:** A text input field with a placeholder 'Fully qualified domain name (FQDN) or IP address'.
- *API Key:** A text input field with a 'Get API Key' button next to it. The placeholder is 'Auto-completed when API key is retrieved'.
- Backup Standalone Profiler:** A text input field with a placeholder 'Fully qualified domain name (FQDN) or IP address'.
- API Key:** A text input field with a 'Get API Key' button next to it. The placeholder is 'Auto-completed when API key is retrieved'.

At the bottom of the form, there are two buttons: 'Save Changes' and 'Reset'. A note at the bottom left states '* indicates required field'.

Backup and recovery

A Backup remote Profiler can be configured in the local Profiler. If the connection to the remote profiler fails, the local profiler cannot enforce remote profiler for information. The local Profiler queries Backup Standalone Profiler for device attributes and updates the session information.

Profiling devices in branch offices

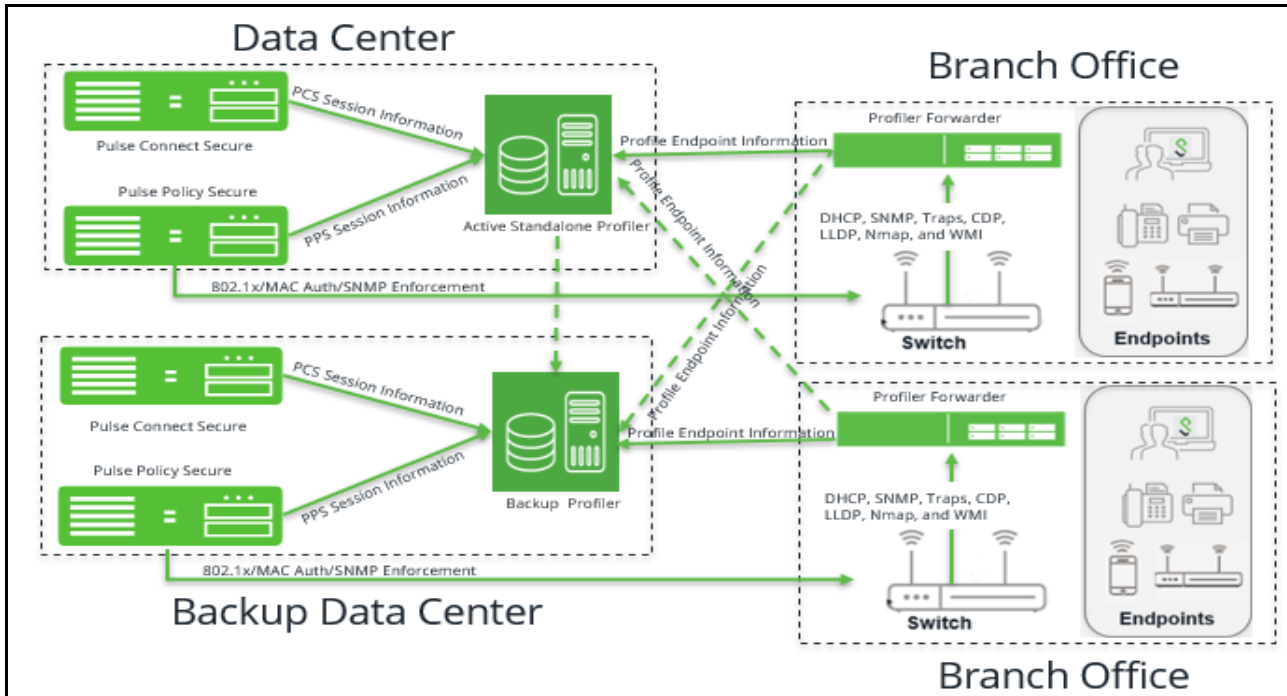
If forwarder uses 9.1R8 version, the standalone profiler must also use 9.1R8 version. Standalone profiler less than 9.1R8 version is not supported.

Using Profiler Forwarder

The Profiler forwarder without PPS functionality deployment scenario is useful in following cases:

- You want to profile devices spread across WAN links.
- You have PPS appliances clustered in one or more data centers.

Figure 4 Example of a Profiler and Forwarder deployed across WAN



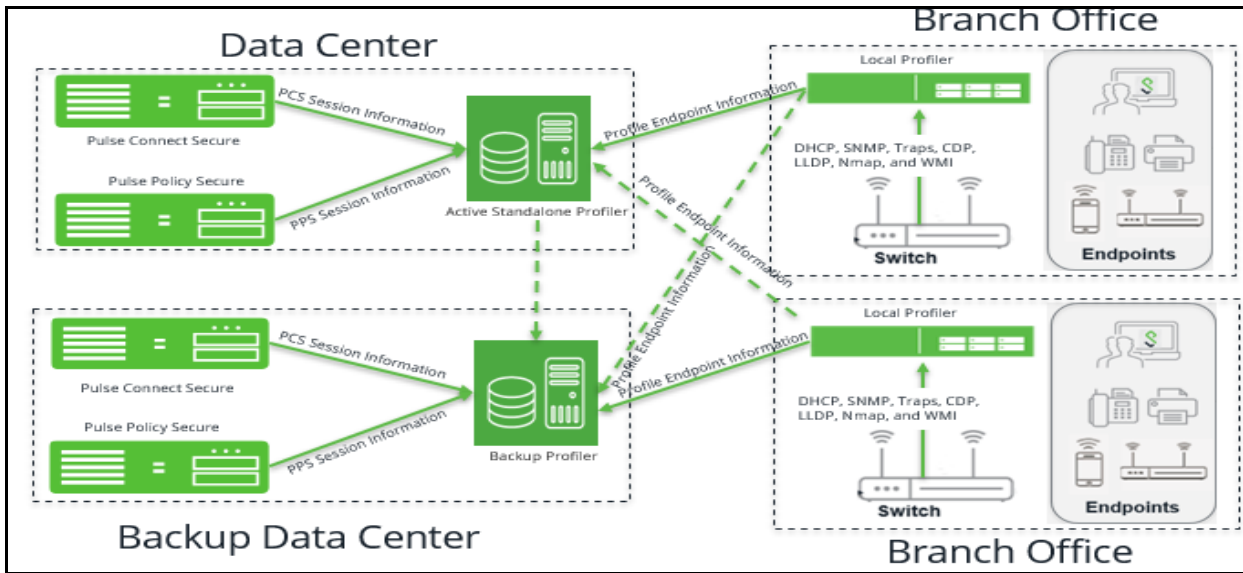
The Profiler Forwarder is a physical or virtual appliance with distinctive feature license called Profiler Forwarder license. The Profiler Forwarder enables the Profiler to run locally, profile the endpoints, and send the profiled information to the central Standalone Profiler periodically (default: 5 minutes). The profiler forwarder can be configured to include the branch name in the Device Discovery Report.

Backup and recovery

A backup central Profiler can be configured for the profiler forwarder. If the connection to the standalone profiler fails, the forwarder sends the information to the backup central profiler.

Using Linked Profiler (With PPS Functionality)

Figure 5 Example of a Profiler with PPS functionality deployed across WAN



The Profiler running along with the PPS in a branch, allows to profile the devices and edit attributes on the devices. PPS sends the information to the central Standalone Profiler periodically. It enables to have a consolidated view of all endpoints and maintain a history of the endpoints when moved across branches.

Backup and recovery

A backup central Profiler can be configured for the local profiler. If the connection to the standalone profiler fails, the local profiler sends the information to the backup central profiler.

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 6 Download and Install License

Configuration > Licensing > Download License

Download License

Configuration
Licensing

Licensing | Pulse One | Security | Certificates | DMI Agent | Sensors | Client Types | SAML | Guest Access | Advanced Networking | Notification

License Summary | Configure Server | **Download Licenses**

▼ **License downloads settings**

Use this section to modify network settings for license server.

Preferred Network:

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

Save Changes

▼ **On demand license downloads**

Enter Authentication Code in the below text box.
Saved auth code: bc0f-72d9-84a6-a561

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..... 8](#)
- [Switch Configuration for CDP/LLDP 8](#)
- [Switch Configuration for SNMP Traps 8](#)
- [Configuring the Profiler to Work with RSPAN Configuration 8](#)

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 34](#)
- [“Appendix: Configuring Juniper Switches” on page 38](#)
- [“Appendix: Configuring HP \(Procurve\) Switches” on page 41](#)

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

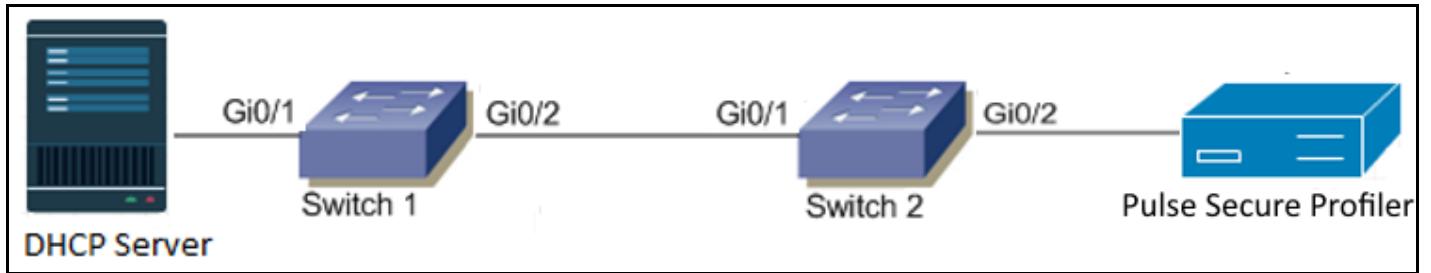
The Profiler uses the Link Up/Down and MAC notification traps to:

- 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 7 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.....	11
• Configuring the Local Profiler Authentication Server.....	12
• View Discovered Devices	21
• Configuring Profile Groups	23
• Configuring Role-Mapping Rules for Profiled Devices	24

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 8 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**

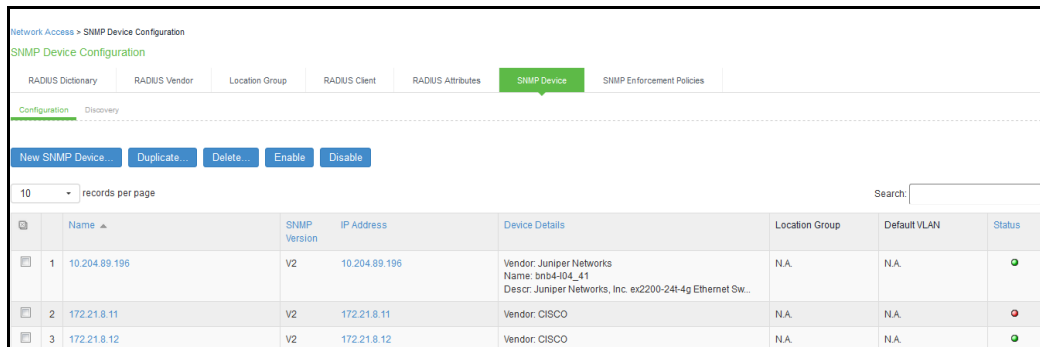
Same credentials for Trap user ☒

*Read Community String

Save Changes

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

Figure 9 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: bn04-104_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 you perform the following tasks before proceeding with the Profiler Authentication server configuration.

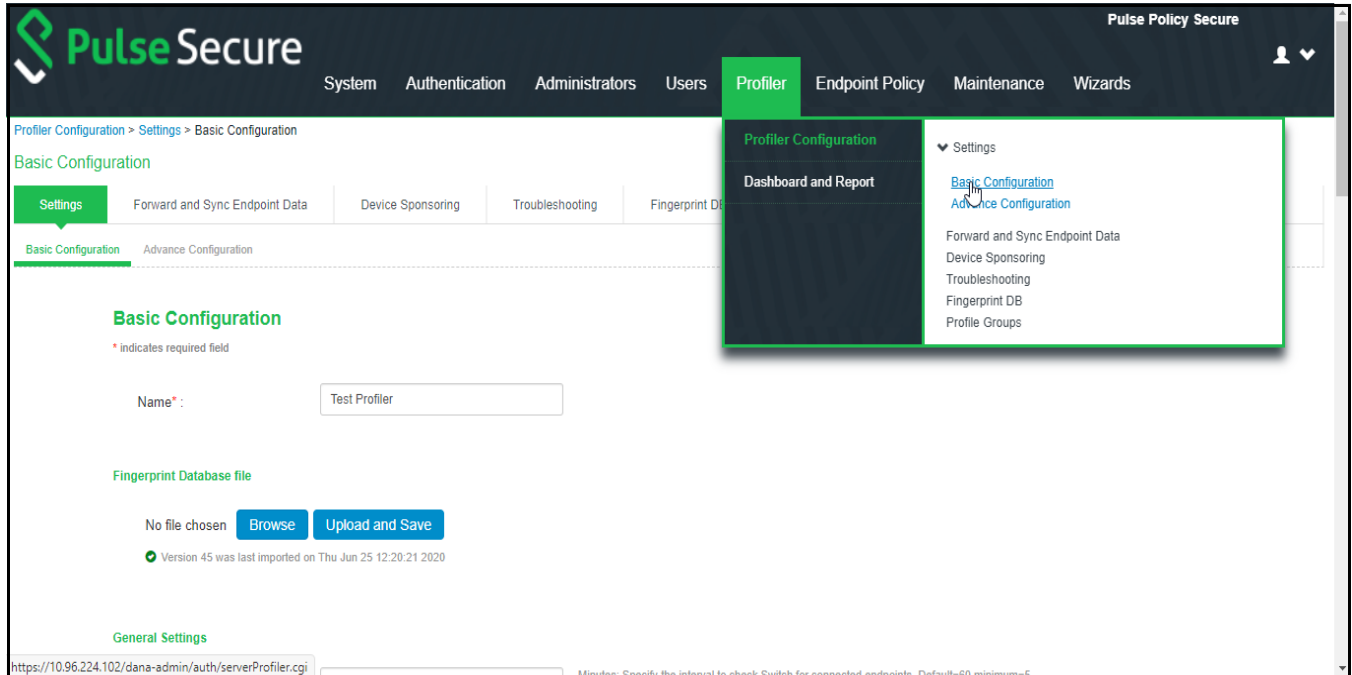
- To use DHCP fingerprinting, configure the switch(es) to forward DHCP packets to the PPS.
- To use SNMP/SSH-based profiling from Network Infrastructure Devices, configure one or more switches in the Network Infrastructure Device page of the PPS Administrator User.
- Download the latest device fingerprints package from the support portal. Minimum supported fingerprints database version for 9.1R8 is 45.

Basic Profiler Configuration

To configure basic settings for the Local Profiler:

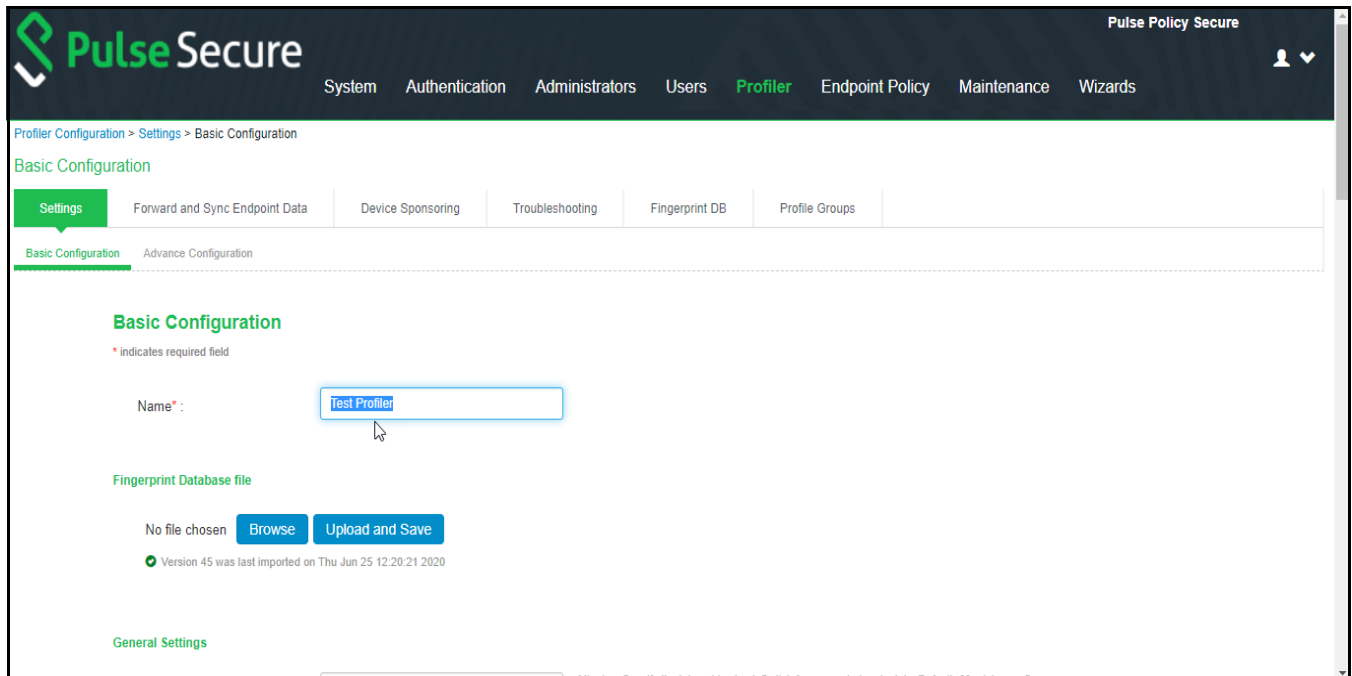
1. Navigate to **Profiler > Profiler Configuration > Basic Configuration**.

Figure 10 Creating a Local Profiler



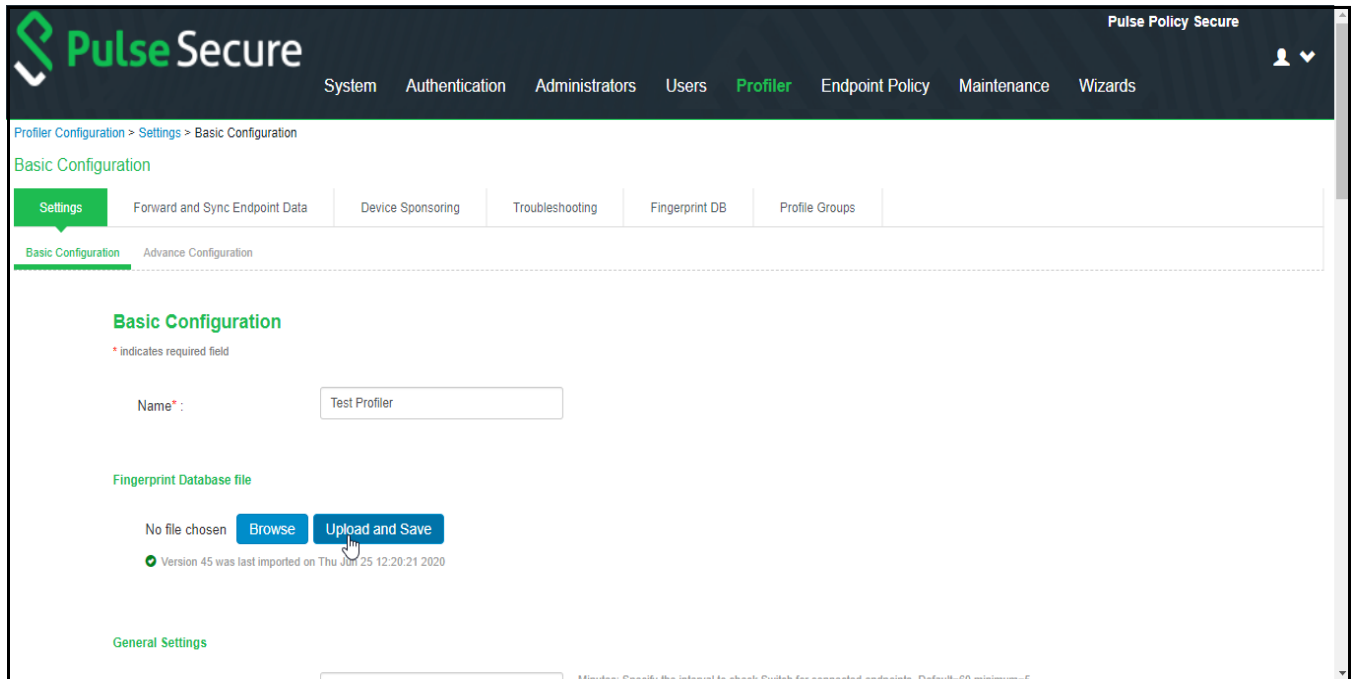
2. Enter a name for the Profiler.

Figure 11 Naming a Local Profiler Authentication Server



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

Figure 12 Uploading Device Fingerprints Package



4. Set the **General Settings** for the profiler:

- Set SNMP **Poll interval**, for polling the Network Infrastructure Devices. By default, the poll interval is set to 60 minutes.
- Select the **DHCP Sniffing mode**. RSPAN for external ports and DHCP Helper for internal ports. Optionally, select the TCP or SMB Sniffing modes to profile devices using TCP and SMB. External interface is connected to switch SPAN port.
- Select the interval to purge older devices from the database periodically. By default, the interval is set to *Never* that means purging is disabled.
- Optionally, select the option to profile all the discovered devices using NMAP.

Figure 13 General Settings

Pulse Secure Pulse Policy Secure

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

General Settings

Poll Interval*: Minutes: Specify the interval to check Switch for connected endpoints. Default=60 minimum=5
To discover devices, configure one or more switches under [Network Infrastructure Device](#).

DHCP Sniffing mode*: ☐ RSPAN (External port) Select an option for DHCP profiling mode.
☒ DHCP Helper (Internal port)

☐ TCP Sniffing (External Port)

☐ SMB Sniffing (External Port)

Purge devices older than: Device(s) older than selected option would be deleted permanently from database automatically.
Automatic Purge will trigger every 24 hours Or it can be manually triggered using "Actions" menu in Device Discovery Report. This is based on the last updated time of the device.

☒ Profile all the discovered devices using NMAP
IPs that are discovered using SNMP and DHCP will be profiled using NMAP

Infrastructure Devices

records per page Search:

- The SNMP/SSH scans and lists the **Infrastructure Devices** and connected endpoints after a predefined Poll interval with details.
 - Use **New** to add devices, **Discover** to find a range of devices in the network by entering the details in the pop-up window.
 - For each device, use the icons in the **Actions** column to Edit, Refresh, or Duplicate the device details.

Pulse Secure Pulse Policy Secure

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

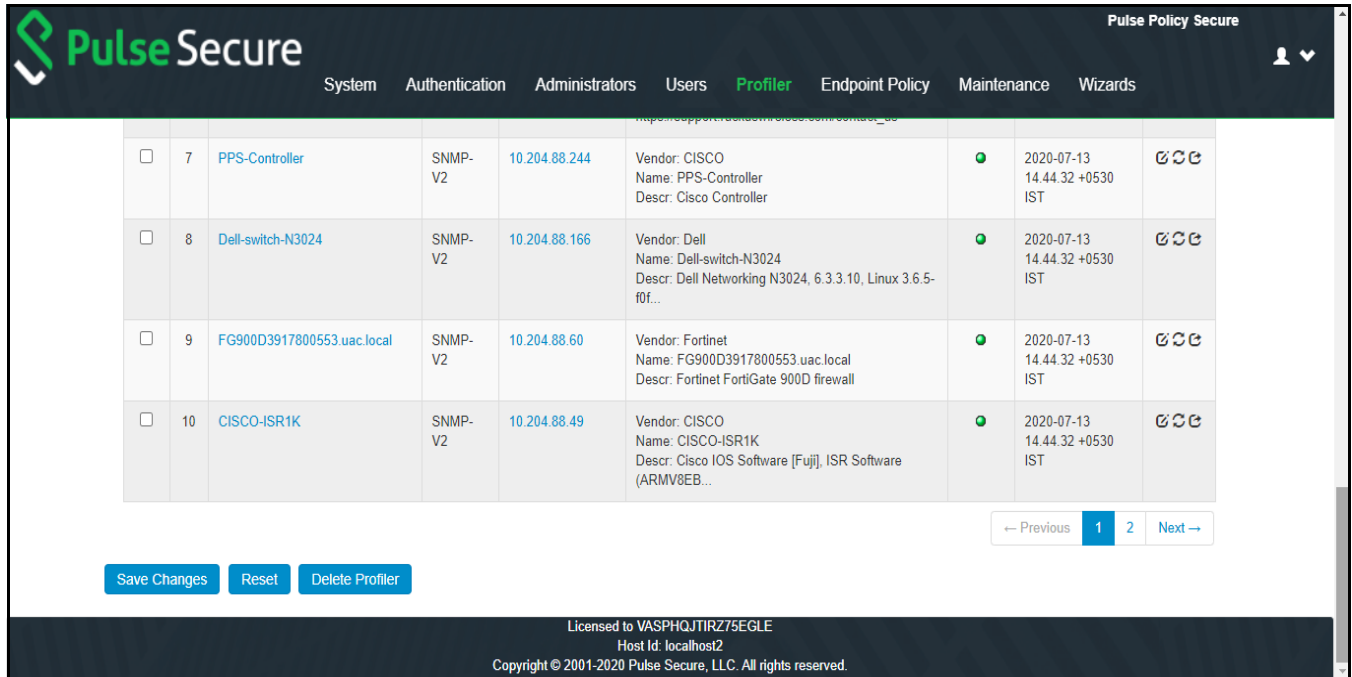
Infrastructure Devices

records per page Search:

		Name	Protocol	IP Address	Device Details	Status	Last Known Timestamp	Actions
<input type="checkbox"/>	1	BNG-LAB-SW3	SNMP-V2	10.204.88.1	Vendor: JUNIPER Name: BNG-LAB-SW3 Descr: Juniper Networks, Inc. ex4200-48p internet route...		2020-07-13 14:44:32 +0530 IST	
<input type="checkbox"/>	2	tacacs-switch	SNMP-V2	10.204.88.241	Vendor: Arista Networks Name: tacacs-switch Descr: Arista Networks EOS version 4.22.1FX-CLI running...		2020-07-13 14:44:32 +0530 IST	
<input type="checkbox"/>	3	EXOS-VM	SNMP-V2	10.204.88.18	Vendor: Extreme Networks Name: EXOS-VM Descr: ExtremeXOS (EXOS-VM) version 30.4.1.2 30.4.1.2 b... Contact: https://www.extremenetworks.com/support/		2020-07-13 14:44:32 +0530 IST	
<input type="checkbox"/>	4	PA-VM	SNMP-	10.204.88.245	Vendor: Standard Switch		2020-07-13	

6. Click **Save Changes** to save the basic profiler configuration, **Reset** to clear the settings and revert to default settings, or **Delete Profiler** to delete the profiler.

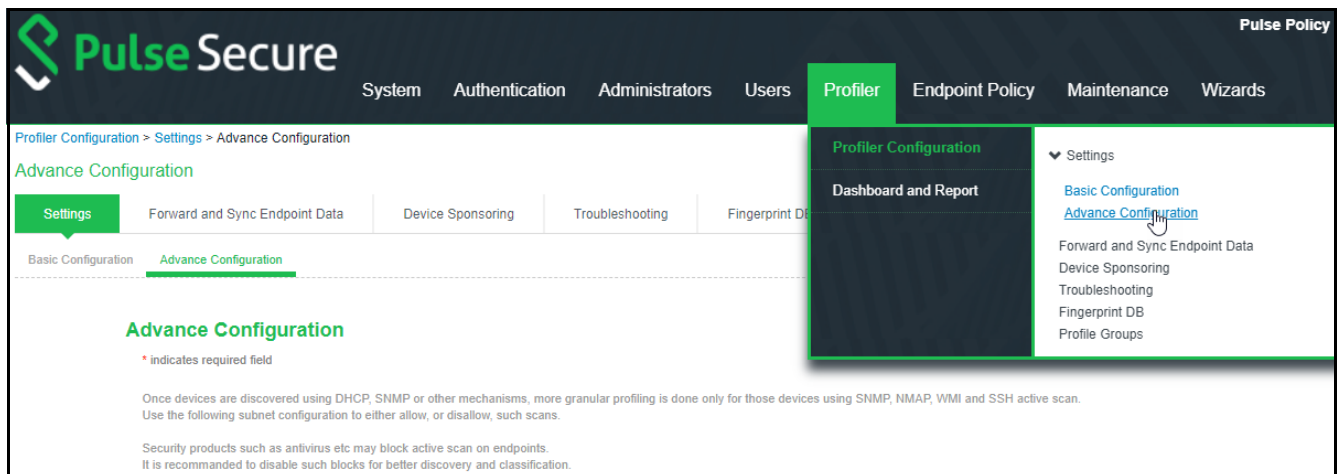
Figure 14 Save Profiler Basic Configuration



Advance Profiler Configuration

To configure advance settings for the Local Profiler, select **Profiler > Profiler Configuration > Advance Configuration**.

Figure 15 Advance configuration of a Local Profiler



WMI Configuration

To configure WMI profiling:

- 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.
- Optionally, select the option to profile all the discovered devices using WMI. If the number of discovered devices is exceeding 1000, it is recommended to add subnets manually to scan only Windows devices.
- 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.
- Enter the Endpoint IP or hostname to test the credentials.

Figure 16 WMI Profiling

The screenshot shows the 'Advance Configuration' page in the Pulse Secure Profiler. The page has a dark header with the Pulse Secure logo and navigation tabs: System, Authentication, Administrators, Users, Profiler (active), Endpoint Policy, Maintenance, and Wizards. Below the header, there's a section titled 'Advance Configuration' with a note: '* indicates required field'. A paragraph explains that 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. It also mentions that security products like antivirus may block active scan on endpoints and recommends disabling such blocks for better discovery and classification.

There are two main configuration panels:

- WMI Profiling:**
 - Radio buttons: ☒ Configure WMI credentials, ☐ Use Active Directory server credentials.
 - Fields: User* (admin), Password* (masked).
 - Text: User or domain\user or user@domain.com for endpoints.
 - Checkboxes: ☐ Profile all the discovered devices using WMI, ☒ Allow deep scan.
 - Text: 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.
 - Field: Endpoint IP or hostname: (empty).
 - Button: Test Credentials.
- SSH Profiling:**
 - Dropdown: Authentication Method: Password.
 - Text: Use Public key authentication to maximize security*.
 - Fields: User* (admin), Password* (masked).
 - Checkbox: ☒ Profile all the discovered devices using SSH.
 - Field: Endpoint IP or hostname: (empty).
 - Button: Test Credentials.

SSH Configuration

To configure SSH Profiling:

- Select the **Authentication Method**, select **Password** to authenticate using administrator credentials or **Public key** to authenticate using RSA credentials.
- Optionally, select the option to profile all the discovered devices using SSH. If the number of discovered devices is exceeding 1000, it is recommended to add subnets manually to scan only Windows devices.
- Enter the Endpoint IP or hostname to test the credentials.

Figure 17 SSH Profiling

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

Advance Configuration

* Indicates required field

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.

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

WMI Profiling

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

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

Password*:

☐ Profile all the discovered devices using WMI

☒ 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.

Endpoint IP or hostname:

Test Credentials

SSH Profiling

Authentication Method:

Use Public key authentication to maximize security*

User*:

Password*:

☒ Profile all the discovered devices using SSH

Endpoint IP or hostname:

Test Credentials

SNMP (Host) Configuration

To configure SNMP (Host) Profiling:

- Enter the possible community list names, separated by commas, to collect device attributes for the endpoints monitored through SNMP.
- Optionally, select the option to profile all the discovered devices using SNMP (Host). If the number of discovered devices is exceeding 1000, it is recommended to add subnets manually to scan only Windows devices.

Figure 18 SNMP (Host) Profiling

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

SNMP (Host)

If Endpoints are being monitored through SNMP then Profiler will fetch device attributes through SNMP. Enter the possible community list names, separated by commas. Example: public,private,admin

Community List:

☐ Profile all the discovered devices using SNMP(Host)

Device Attribute Server(s)

This Server will be polled to discover endpoints and fetch device attributes for an endpoint discovered through other passive collectors like DHCP, SNMP etc.

Polling Interval:
Minutes. Specify the interval to check the Device Attribute Server for endpoints. Default=120, Minimum=60

Available Servers:

Add -> **<- Remove**

Selected Servers:

There can be at most one Device Attribute Server of a type e.g. ICS Security Solution, selected

Device Attribute Server Configuration

The profiler polls the device attribute server at regular interval to collect the device attributes for the endpoints discovered using passive collectors. The controller is configured as a HTTP Attribute Server and is available under Device Attribute Server settings.

For information on configuring Authentication Servers refer to *Pulse Policy Secure Administrator Guide*.

To configure profiling using the device attribute server:

- Set the **Polling interval** in minutes. By default, the poll interval is set to 720 minutes.
- Add or remove the servers from or to the list of Available Servers and Selected Servers.

Figure 19 Device Attribute server configuration

The screenshot shows the 'Profiler' tab in the Pulse Secure interface. It contains two main configuration panels:

- SNMP (Host):** A panel with a text input for 'Community List' (containing 'public') and a checkbox labeled 'Profile all the discovered devices using SNMP(HOST)'.
- Device Attribute Server(s):** A panel with a 'Polling Interval' set to 720 minutes. It features two lists: 'Available Servers' (empty) and 'Selected Servers' (containing 'Demo-Nxcom-Srv-1'). Buttons for 'Add ->' and '<- Remove' are between the lists. A note at the bottom states: 'There can be at most one Device Attribute Server of a type e.g. ICS Security Solution, selected'.

Additional Data Collectors configuration

To configure additional data collectors to collect endpoint attributes through MDM and LDAP servers:

- Select an MDM authentication server for accurate profiling of mobile devices which are registered through MDM providers.
- Select an LDAP server where device information is stored.

For information on configuring Authentication Servers refer to *Pulse Policy Secure Administrator Guide*.

Figure 20 MDM Server and LDAP Server configuration

The screenshot shows the 'Additional Data Collectors' configuration page. It includes:

- Dropdown menus for 'MDM server' and 'LDAP server', both currently set to 'None'.
- A 'Subnets' section with a table for configuring on-demand scans.

Subnet	Include/Exclude	NMAP	WMI	SSH	SNMP(HOST)	Add
10.204.88.0/24	Include	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10.204.90.0/32	Include	NMAP	WMI			
10.96.74.0/32	Include	NMAP	WMI	SSH		

Buttons at the bottom include 'Delete', 'Start On-Demand Scan', 'Save Changes', and 'Reset'. A note on the right states: 'Subnets should be in valid CIDR format or individual IP or IP Range. Example Subnets: Valid CIDR Format: 10.10.10.0/24, 10.200.0.0/16, IP or IP Range: 10.10.10.10, 10.10.10.10-100, 10.10.1.1-10.10.5.200'.

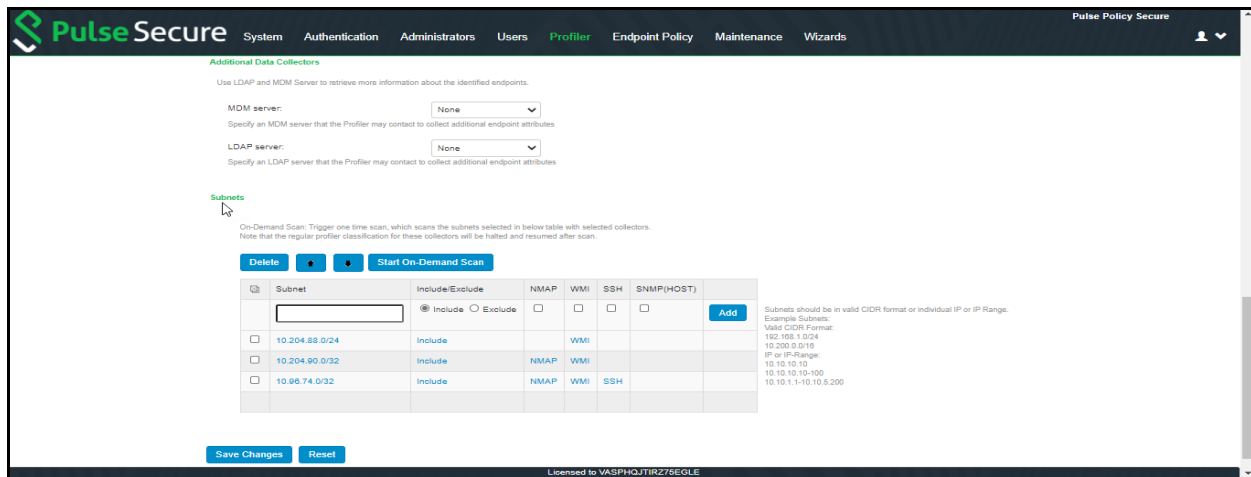
Subnets Configuration

Upon device discovery, using DHCP, SNMP or other mechanisms, granular profiling is performed on devices using various active collectors.

- Enter one or more subnets, select to include or exclude the listed collectors like SSH, WMI, SNMP (HOST), and NMAP and click **Add**. Maximum 100 subnets configuration are supported.
- Click **Start On-Demand Scan** to trigger a scan instantly on the selected subnets for selected collectors. The list of subnet must be ordered based on the IP address matching the first subnet from top to bottom. Use arrow buttons to change the order.

Note: For on-demand scan, NMAP is supported for devices in same subnet as PPS.

Figure 21 Subnets Configuration

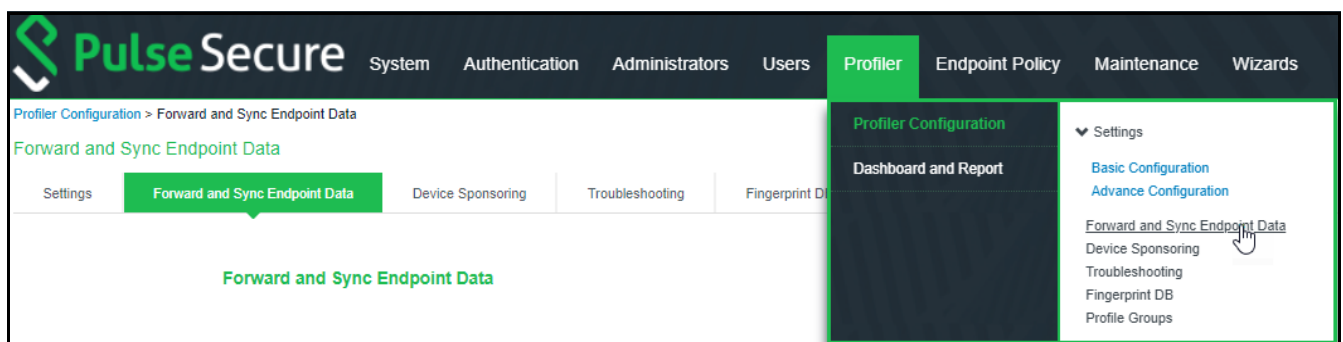


Forward and Sync Endpoint Data

To forward and sync endpoint data from current profiler to another local profiler:

1. Select **Profiler > Profiler Configuration > Forward and Sync Endpoint Data**.

Figure 22 Forward and Sync Endpoint Data



2. Enter the FQDN or the IP address of the linking local profiler and the backup local profiler.
3. Enter the API key, or click **Get API Key**. To get API key, enter the administrator credentials and select the option to validate server certificate to retrieve and auto fill the API Key.

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

Figure 23 Forward and Sync endpoints configuration

The screenshot shows the 'Forward and Sync Endpoint Data' configuration page in the Pulse Secure Profiler. The page has a dark header with the Pulse Secure logo and navigation tabs: System, Authentication, Administrators, Users, Profiler (selected), Endpoint Policy, Maintenance, and Wizards. Below the header, there's a breadcrumb trail: Profiler Configuration > Forward and Sync Endpoint Data. A sub-header 'Forward and Sync Endpoint Data' is followed by a tabbed interface with tabs: Settings, Forward and Sync Endpoint Data (selected), Device Sponsoring, Troubleshooting, Fingerprint DB, and Profile Groups. The main content area is titled 'Forward and Sync Endpoint Data' and includes the instruction 'Forward and sync this profiler's data to another local profiler'. It contains two sections for configuring a local profiler to link to. The first section has fields for 'Local Profiler to link:' (with value 10.204.89.186), 'API Key:' (with value pnUxOLuJxdchT5O8b80), and a 'Fully qualified domain name (FQDN) or IP address' field. Below these is a 'Get API Key' button. A status box shows '10.204.89.186 - DISCONNECTED | Retrying...' and 'Synced endpoints upto Tue, 07 Jul 2020 23:04:59'. The second section is for a 'Backup Local Profiler' with similar fields and a 'Get API Key' button. At the bottom are 'Save Changes' and 'Reset' buttons. The footer contains license information: 'Licensed to VASPHQJTRZ75EGLE, Host id: localhost2, Copyright © 2001-2020 Pulse Secure, LLC. All rights reserved.'

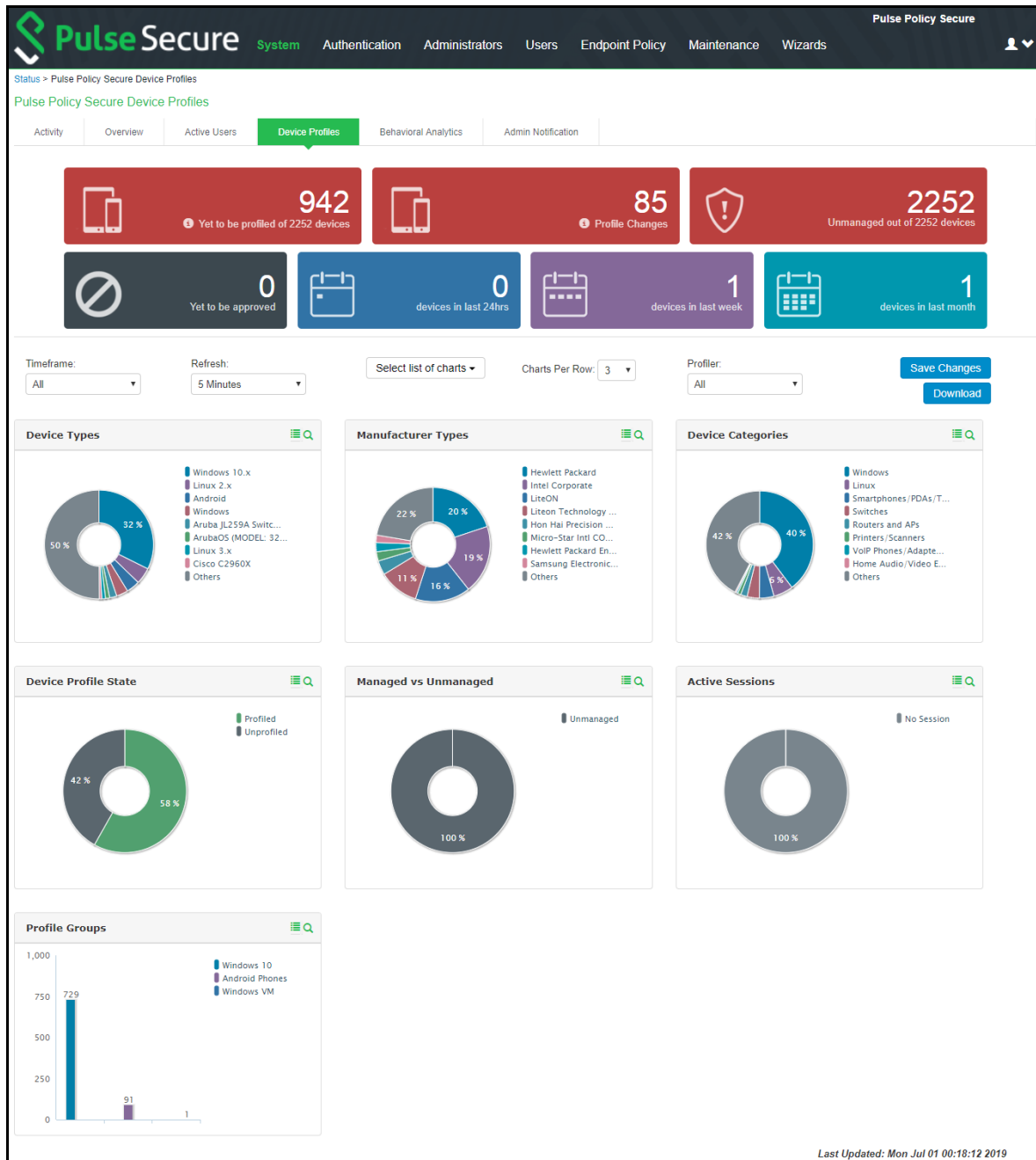
View Discovered Devices

Dashboard View

Once the Profiler is configured, profiling starts in the background. The Device Profiles Dashboard displays an overall summary of the devices that are discovered, profiled, and updated in the Device Discovery Table.

Navigate to **Profiler > Dashboard and report > Dashboard** or **System > Reports > Device Discovery** to display the device profiles page. Click on each chart or numbered panel to view detailed information in the device discovery report.

Figure 24 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.

Navigate to **System > Reports > Device Discovery** or **Profiler > Dashboard and Report > Device Discovery report** to display the table.

Figure 25 Device Discovery Report Table

Reports > Device Discovery Report

Reports
Device Discovery Report

User Summary Single User Activities Device Summary Single Device Activities **Device Discovery** Authentication Compliance Behavioral Analytics Infected Devices

Profiler

Showing 1 to 10 of 807 entries 10 records per page

	MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	Session User	First Seen	Last Updated	
<input type="checkbox"/>	00:50:56:a4:49:e0	10.204.91.109		VMware, Inc.	FreeBSD 6.x	BSD		Mon, 29 Jun 2020 10:08:31	Wed, 08 Jul 2020 13:39:36	<input checked="" type="checkbox"/> Approve Selected
<input type="checkbox"/>	0c:c4:7a:b3:64:53	10.209.113.70		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input type="checkbox"/> Unapprove Selected
<input type="checkbox"/>	0c:c4:7a:56:0e:33	10.209.113.68		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input checked="" type="checkbox"/> Time-Bound Approve Selected
<input type="checkbox"/>	0c:c4:7a:79:10:32	10.209.113.52		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input type="checkbox"/> Add Device
<input type="checkbox"/>	00:50:56:bf:a5:b0	10.204.88.199		VMware, Inc.	Linux 3.x	Linux		Fri, 26 Jun 2020 13:08:42	Fri, 26 Jun 2020 17:14:37	<input type="checkbox"/> Download Report in CSV
<input type="checkbox"/>	0c:c4:7a:56:09:6f	10.209.113.69		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input type="checkbox"/> Download Report in PDF
<input type="checkbox"/>	0c:c4:7a:e3:f5:f1	10.204.58.124		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input type="checkbox"/> Delete Selected
<input type="checkbox"/>	0c:c4:7a:57:bc:71	10.209.113.67		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input type="checkbox"/> Purge Aged Out Devices
<input type="checkbox"/>	0c:c4:7a:b3:66:27	10.209.113.113		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input type="checkbox"/> Test Profiler
<input type="checkbox"/>	0c:c4:7a:78:52:d8	10.209.113.76		Super Micro Computer, Inc.	Linux 2.x	Linux		Fri, 26 Jun 2020 13:11:14	Mon, 13 Jul 2020 22:17:00	<input type="checkbox"/> PRF-7K
										<input type="checkbox"/> DR Profiler

First Previous 1 2 3 4 5 ... 81 Next Last

Licensed to VASPHQJIRZ75EGLE
Host Id: localhost2
Copyright © 2001-2020 Pulse Secure, LLC. All rights reserved.

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. Navigate to **Profiler > Profiler Configuration > Profiler Groups**.
2. Enter the **Group Name** and **Rule**. The rules contain device attributes and operators. Manually enter the rule or choose from the list that dynamically displays the probable combinations.

To create rules for all values including null, use the rule: category = "*" or category = "".

3. Select the approval mode to approve the devices added to the profile group. Auto-Approval is the default option.
 - **Auto-Approval:** Automatically approves the devices.
 - **Manual-Approval:** Administrator manually approves the devices.
 - **Time-Bound-Approval:** Devices approved for a specific time period and time zone. Enter the start date, end date, and time zone.
4. Select the option to send email notifications to notify when new devices are added to the group.
 - Choose **Use emails from General Settings** to send e-mails to address specified in General Settings or choose **Custom** and enter the e-mail addresses separated by semicolon.
5. Select the interval from the list to purge the older devices in the group automatically.
6. 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.

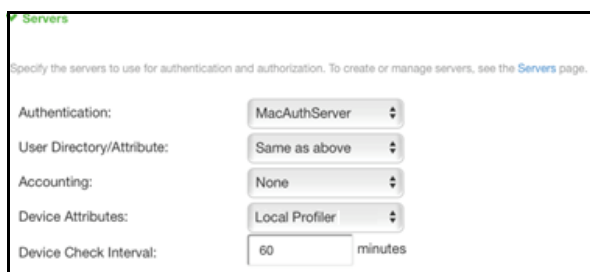
Configuring Role-Mapping Rules for Profiled Devices

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 26 Device Attributes



The screenshot shows a web interface titled 'Servers' with a subtitle 'Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.' Below this, there are five configuration rows, 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 27 Rule based on attribute

Rule based on: Device attribute [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 28 Creating New Role Mapping Rule

User Realms > Users > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name: windows_rule

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

Attribute: os (Select an attribute)

is (antivirus_name, antivirus_status, antivirus_version, category, custom, domain, first_seen, groups, hostname, last_seen, macaddr, manufacturer, os, os_patch, previous_category, previous_os, profiler_name, status, tcp_open_ports)

then assign these roles

Available Roles: Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted, Remediation

Roles:

☒ Stop processing rules

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

Figure 29 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 Attributes... ldapServer is configured as LDAP Server in Authentication Server Local Profiler.

✓ then assign

Available Roles: Selected Roles:

- Guest
- Guest Admin
- Guest Sponsor
- Guest Wired
- Users

☒ cn

☐ department

☐ departmentNumber

☐ employeeNumber

☐ employeeType

☐ homeDirectory

☐ homeDrive

☐ o

☐ ou

☐ sAMAccountName

☐ uid

☐ wwwHomePage

☐ 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.

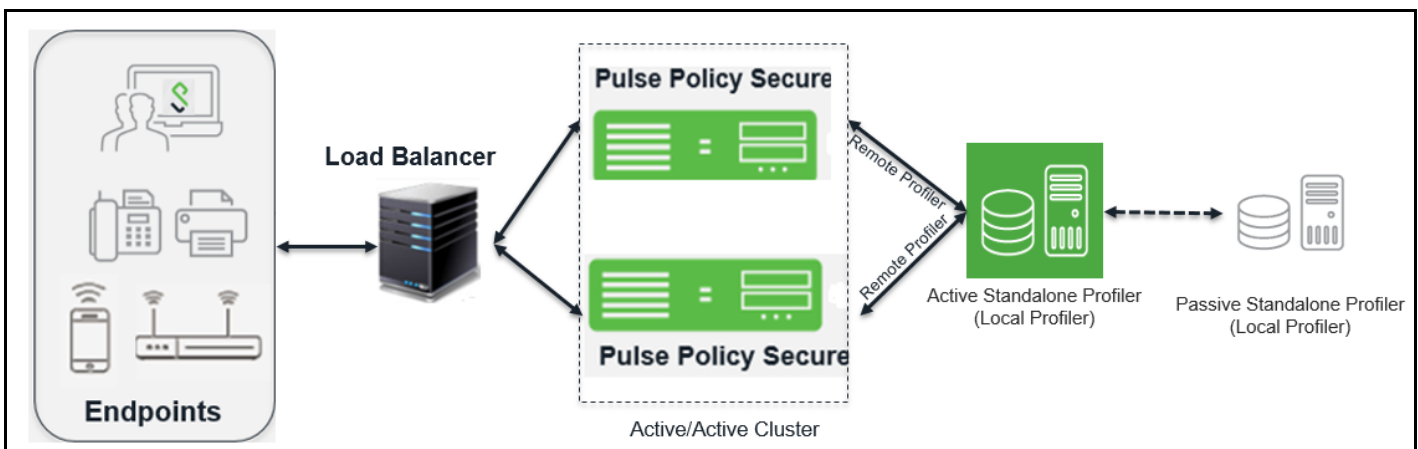
A Remote Profiler can be useful in the following cases:

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 30 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 REST APIs** and Save Changes.

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

Figure 31 Allow Access to the Profiler

Auth Servers > Administrators > Update Administrator admin

Update Administrator admin

Full Name: Platform Administrator

Authenticate using: Administrators

Password: [masked]

Confirm Password: [masked]

Start Time: [calendar icon]

End Time: [calendar icon]

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.

Save Changes

Configuring Remote Profiler Authentication Server

To configure Remote Profiler Authentication Server, follow the procedure “[Configuring the Local Profiler Authentication Server](#)” on page 12

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 for the Remote Profiler and the Backup Standalone Profiler.

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

Figure 32 New Remote Profiler

Auth Servers > New Remote Profiler

New Remote Profiler

*Name: [text box] Label to reference this server.

*Remote Profiler: [text box] Fully qualified domain name (FQDN) or IP address

*API Key: Get API Key [text box] Auto-completed when API key is retrieved

Backup Standalone Profiler: [text box] Fully qualified domain name (FQDN) or IP address

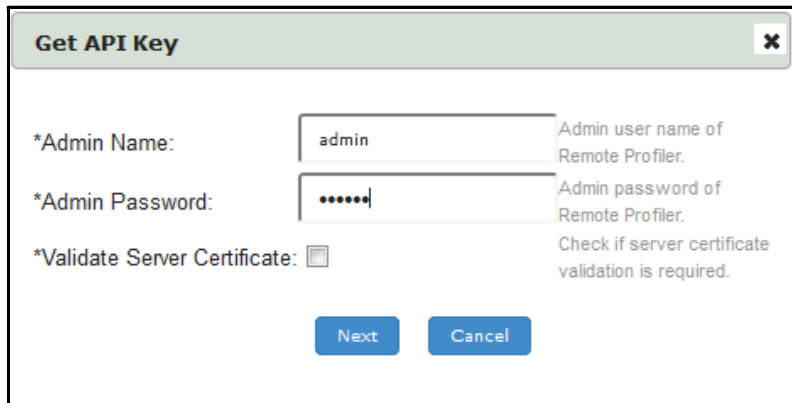
API Key: Get API Key [text box] Auto-completed when API key is retrieved

Save Changes Reset

* indicates required field

- Click the **Get API Key** button to create a new key for secure communication with the Profiler. In the Get API Key window, provide the credentials of valid administrator on PPS/Profiler server and click **Next**. The API key generates and displays in the API Key field.

Figure 33 Get API Key



Note:

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

- 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 29](#)

Troubleshooting

• Tests	30
• Diagnostic Logs	31
• Profiler Logs	31

Tests

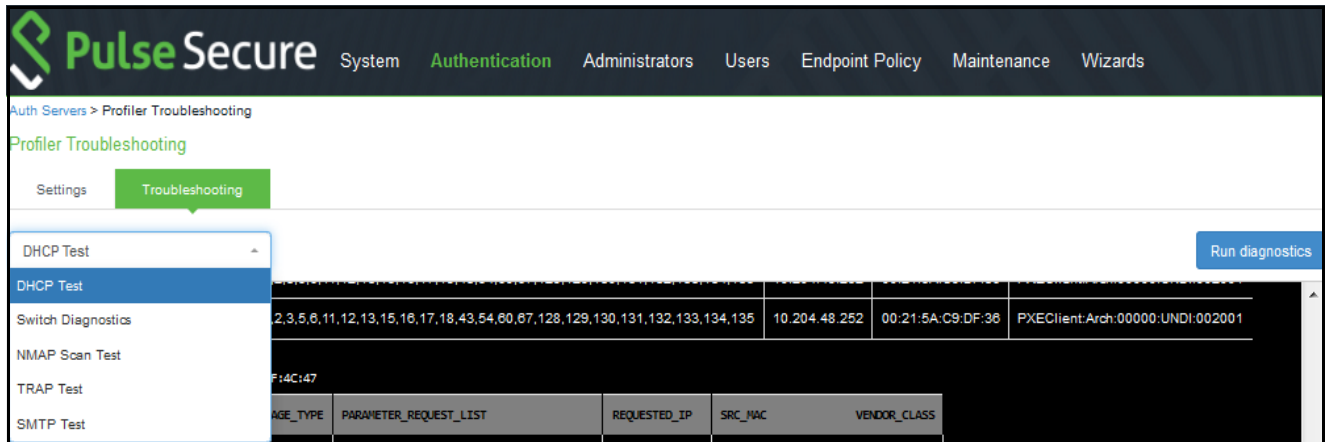
The following tests help to identify and solve basic problems associated with configurations of the Profiler.

Test	Result
DHCP Test	<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	<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 is able to fetch the Endpoint information through SNMP.
NMAP Scan Test	<ul style="list-style-type: none"> Check if NMAP scan is working for an IP address, which is prompted during diagnostic run
Trap 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. <p>Device sponsoring is available with email notification feature. It sends an email through configured SMTP server and displays the status.</p>

To execute the tests, perform the following steps:

1. Navigate to **Profiler > Profiler Configuration > Troubleshooting**.
2. From the drop-down list, select the required test and click **Run diagnostics**.

Figure 34 Troubleshooting



Diagnostic Logs

The Profiler Diagnostic logs include detailed information about endpoints on uploading the endpoint information to Pulse One. Event IDs *PRO31748* and *PRO31749* represent the diagnostic log messages.

To enable Diagnostic logs, navigate to **Maintenance > Troubleshooting > Monitoring > Diagnostic Logs** and select **Profiler Diagnostic Logging On**.

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, navigate to **Log/Monitoring > Events > Log Settings** and select **Profiler Events**.

Figure 35 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 Profiler logs

Event ID	Description	Log Type
ADM31405	Network Infrastructure Device Poll Interval Updated	Admin logs

Event ID	Description	Log Type
ADM31444	WMI User added	Admin logs
ADM31445	WMI User modified	Admin logs
ADM31446	WMI User deleted	Admin logs
ADM31458	Profiler API keys retrieved Success/Failure	Admin logs
ADM31573	Device(s) are deleted from Device Discovery Report	Admin logs
ADM31591	Device updated in Device Discovery report.	Admin logs
ADM31595	Device added in Device Discovery report.	Admin Logs
ADM31631	Device addition failed in Device Discovery Report.	Admin Logs
ADM31634	Profile modified successfully	Admin logs
ADM31635	Profile modification is deleted successfully	Admin logs
ADM31636	Import from CSV succeeded	Admin logs
ADM31637	Import from CSV failed	Admin logs
ADM31701	On-Demand Subnet Scan triggered by admin [With subnet and collector details]	Admin logs
ADM31702	On-Demand Subnet Scan stopped by admin	Admin logs
ADM31730	Profile Group created	Admin logs
ADM31731	Profile Group updated	Admin logs
ADM31732	Profile Group deleted	Admin logs
ADM31759	Purge Initiated! Device(s) will be aged out from Device Discovery Report.	Admin logs
PRO31368	New Device discovered and profiled by Profiler	Event logs
PRO31369	Device Profile (OS/Category) changed and detected by Profiler	Event Logs
PRO31385	Start and End Indication of Network Infrastructure device scan	Event logs
PRO31386	Details of Network Infrastructure Device which is undergoing the scan	Event Logs
PRO31387	Total Number of devices scanned on the Network Infrastructure Device during polling	Event Logs
PRO31387	SNMP polling completion message for a particular table (ARP/CAM/ CDP/LLDP).	Event Logs
PRO31388	No Network Infrastructure Devices are configured for polling	Event Logs
PRO31443	Password Decryption Failure	Event logs
PRO31447	WMI connection failed	Event Logs
PRO31448	WMI Query Failed	Event logs
PRO31449	WMI Scanning a device	Event Logs

Event ID	Description	Log Type
PRO31457	Device attributes are retrieved from profiler	Event logs
PRO31459	Device attributes got updated	Event logs
PRO31461	Encryption or decryption failed for config parameters	Admin logs
PRO31476	Fingerprint Database Initialization Failed	Event logs
PRO31479	Failed to download fingerprint from peer	Event logs
PRO31480	Fingerprint download Started from peer	Event logs
PRO31481	Successfully downloaded fingerprint from peer	Event logs
PRO31523	Performing Full Sync with the configured appliance	Event Logs
PRO31524	Successfully uploaded device(s) to Pulse One / Standalone Profiler	Event logs
PRO31525	Upload of device(s) to Pulse One / Standalone Profiler failed	Event logs
PRO31557	Profiler has exceeded the licensed device count including the grace count	Event Logs
PRO31572	Profiler has exceeded the licensed device count excluding the grace count.	Event Logs
PRO31592	Device(s) Email Notification sent for Approval	Event logs
PRO31605	Performing a SSH scan on a device	Event logs
PRO31606	SSH Connection failed, while performing SSH scan	Event logs
PRO31607	SSH Command Failed, while performing SSH scan.	Event logs
PRO31638	The registered Pulse One server is not capable to receive profiler device(s)	Event logs
PRO31638	The registered Pulse One server is not capable to receive profiler endpoints. Hence, uploading endpoints to Pulse One is retried after sometime	Event logs
PRO31697	On-Demand Subnet Scan started (With Collector details)	Event logs
PRO31698	On-Demand Subnet Scan completed for a particular subnet and collector	Event logs
PRO31699	On-Demand Subnet Scan completed by a specific collector	Event logs
PRO31700	On-Demand subnet failed due to an error	Event logs
PRO31754	Purge Successful! 82 aged out device(s)(older than 1 days) deleted from Profiler database	Event logs
PRO31755	Purge Failed! No aged out devices deleted from Profiler Database.	Event logs
SYS31660	SMTP error	Event logs
SYS31686	Error while generating notification	Event logs
SYS31687	Notification generated successfully	Event logs

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.
3. Filter endpoints on TCP

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)# monitor session 1 filter ip access-group tcp-syn-only
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
```

Filter endpoints on TCP

```
Switch1# sh ip access-lists tcp-syn-only
Extended IP access list tcp-syn-only
 10 permit tcp any any syn
 20 permit tcp any any eq 445
 30 permit tcp any eq 445 any
 40 permit tcp any any ack
```

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)# monitor session 1 destination Gi1/0/1 , Gi1/0/12
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

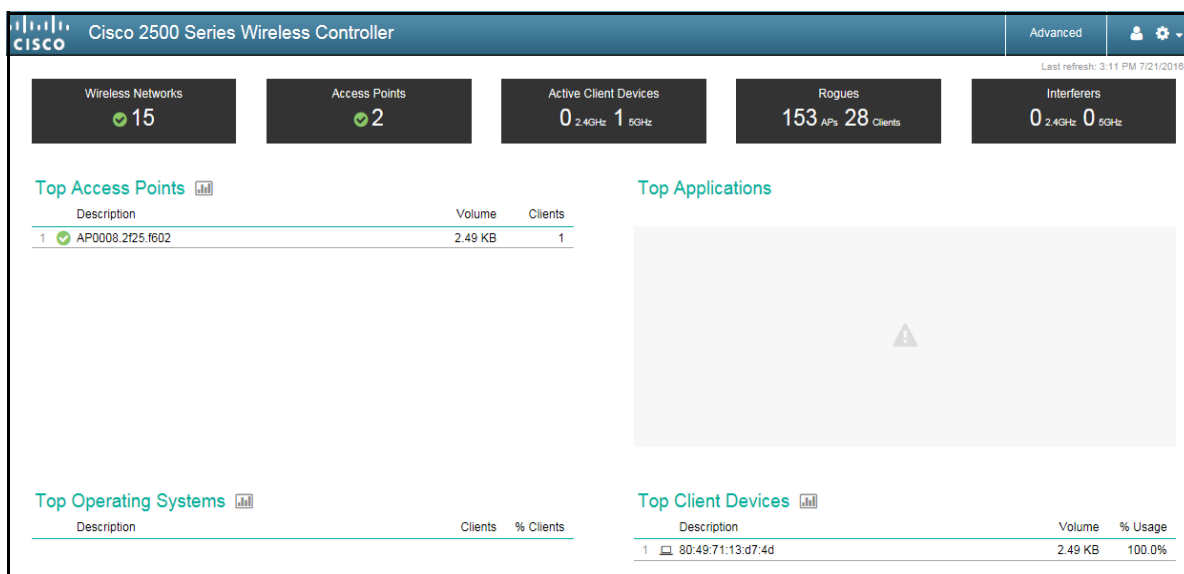
```
Switch1# sh run int g0/2
Building configuration...
Current configuration: 175 bytes
!
interface GigabitEthernet0/2
 description To-Switch2-port-Gi0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 999
 switchport trunk native vlan 60
 switchport mode trunk end
```

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 36 Wireless LAN Controller Web UI



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

Figure 37 WLANS

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)]
5	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 38 HTTP Profiling

WLANs > Edit 'ProfilerUA'

General Security QoS Policy-Mapping **Advanced**

Clear hotspot configuration ☐ Enabled

Client user idle timeout(15-100000) ☐

Client user idle threshold (0-10000000) Bytes

Radius NAI-Realm ☐

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

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.

```
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
```

4. Check SPAN for TCP and SMP monitoring

```
user@switch# show
ethernet-switching-options {
  analyzer employee-tcp-smb-monitor {
    output {
      interface ge-0/0/10.0;
    }
  }
}
...
firewall family ethernet-switching {
  filter watch-employee {
    term employee-to-corp {
      from {
        destination-address 192.0.2.16/28;
        source-address 192.0.2.16/28;
      }
      then accept {
      }
    }
    term employee-to-smb {
      from {
        destination-port 445;
      }
      then analyzer employee-tcp-smb-monitor;
    }
  }
}
```

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: Configuring Viptela Switches

Configure SNMP on Viptela Switch

Use the following commands to configure SNMP on Viptela switches.

SNMP View configuration

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

SNMP V3 configuration

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

SNMP V2 configuration

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

Sample Configuration

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

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

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)