Pulse Policy Secure Profiler: Deployment Guide

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
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

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP</td>
<td>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.</td>
</tr>
<tr>
<td>Concurrent Users</td>
<td>Total number of users connected to Pulse Connect Secure or Pulse Policy Secure simultaneously.</td>
</tr>
<tr>
<td>LLDP</td>
<td>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.</td>
</tr>
<tr>
<td>Managed Devices</td>
<td>Managed devices can be detected by the MDM or a Pulse Client session is established on the device.</td>
</tr>
<tr>
<td>MDM</td>
<td>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.</td>
</tr>
<tr>
<td>Profile</td>
<td>A profile is the combination of the MAC OUI, Category and OS for a device.</td>
</tr>
<tr>
<td>Profile Change</td>
<td>A profile change occurs when a device changes its OS or category.</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Instrumentation</td>
</tr>
</tbody>
</table>
Profiler Deployment Cases

- Standalone Profiler
- Remote Profiler
- Profiling devices in branch offices

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.

![Example of a Remote Profiler](image)

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.
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**.

![Download and Install License](image)

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
- Switch Configuration for CDP/LLDP
- Switch Configuration for SNMP Traps
- Configuring the Profiler to Work with RSPAN Configuration

The profiler interacts with switches from various vendors. The switch configuration varies for each switch type. See the following sections for general switch configuration procedures for widely used switches.

- “Appendix: Configuring Cisco Switches” 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.
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
2. Save the changes. The SNMP Device Configuration table is updated.

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**.

   ![Creating a Local Profiler](image)

   **Figure 10**  Creating a Local Profiler

2. Enter a name for the Profiler.

   ![Naming a Local Profiler Authentication Server](image)

   **Figure 11**  Naming a Local Profiler Authentication Server

3. Click **Browse** and upload the 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.
5. 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.
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**

![WMI Profiling Diagram](image)

### 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.
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.
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

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
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.

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.

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

Figure 23  Forward and Sync endpoints configuration

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.
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.
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**

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

b. If LDAP server is configured in profiler, select the LDAP attribute from the list or click Attributes to create new LDAP attributes.
9. Assign the roles and click **Save Changes**.

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

**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](image)
5. 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.

![Get API Key](image)

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

6. **Save** changes.

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

**Configuring Role-Mapping Rules for Profiled Devices**

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

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

To execute the tests, perform the following steps:

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

Table 1 Profiler logs

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM31405</td>
<td>Network Infrastructure Device Poll Interval Updated</td>
<td>Admin logs</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>ADM31444</td>
<td>WMI User added</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31445</td>
<td>WMI User modified</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31446</td>
<td>WMI User deleted</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31458</td>
<td>Profiler API keys retrieved Success/Failure</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31573</td>
<td>Device(s) are deleted from Device Discovery Report</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31591</td>
<td>Device updated in Device Discovery report.</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31595</td>
<td>Device added in Device Discovery report.</td>
<td>Admin Logs</td>
</tr>
<tr>
<td>ADM31631</td>
<td>Device addition failed in Device Discovery Report</td>
<td>Admin Logs</td>
</tr>
<tr>
<td>ADM31634</td>
<td>Profile modified successfully</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31635</td>
<td>Profile modification is deleted successfully</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31636</td>
<td>Import from CSV succeeded</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31637</td>
<td>Import from CSV failed</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31701</td>
<td>On-Demand Subnet Scan triggered by admin [With subnet and collector details]</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31702</td>
<td>On-Demand Subnet Scan stopped by admin</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31730</td>
<td>Profile Group created</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31731</td>
<td>Profile Group updated</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31732</td>
<td>Profile Group deleted</td>
<td>Admin logs</td>
</tr>
<tr>
<td>ADM31759</td>
<td>Purge Initiated! Device(s) will be aged out from Device Discovery Report.</td>
<td>Admin logs</td>
</tr>
<tr>
<td>PRO31368</td>
<td>New Device discovered and profiled by Profiler</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31369</td>
<td>Device Profile (OS/Category) changed and detected by Profiler</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31385</td>
<td>Start and End Indication of Network Infrastructure device scan</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31386</td>
<td>Details of Network Infrastructure Device which is undergoing the scan</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31387</td>
<td>Total Number of devices scanned on the Network Infrastructure Device during polling</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31387</td>
<td>SNMP polling completion message for a particular table (ARP/CAM/CDP/LLDP).</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31388</td>
<td>No Network Infrastructure Devices are configured for polling</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31443</td>
<td>Password Decryption Failure</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31447</td>
<td>WMI connection failed</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31448</td>
<td>WMI Query Failed</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31449</td>
<td>WMI Scanning a device</td>
<td>Event Logs</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>PRO31457</td>
<td>Device attributes are retrieved from profiler</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31459</td>
<td>Device attributes got updated</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31461</td>
<td>Encryption or decryption failed for config parameters</td>
<td>Admin logs</td>
</tr>
<tr>
<td>PRO31476</td>
<td>Fingerprint Database Initialization Failed</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31479</td>
<td>Failed to download fingerprint from peer</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31480</td>
<td>Fingerprint download Started from peer</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31481</td>
<td>Successfully downloaded fingerprint from peer</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31523</td>
<td>Performing Full Sync with the configured appliance</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31524</td>
<td>Successfully uploaded device(s) to Pulse One / Standalone Profiler</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31525</td>
<td>Upload of device(s) to Pulse One / Standalone Profiler failed</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31557</td>
<td>Profiler has exceeded the licensed device count including the grace count</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31572</td>
<td>Profiler has exceeded the licensed device count excluding the grace count.</td>
<td>Event Logs</td>
</tr>
<tr>
<td>PRO31592</td>
<td>Device(s) Email Notification sent for Approval</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31605</td>
<td>Performing a SSH scan on a device</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31606</td>
<td>SSH Connection failed, while performing SSH scan</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31607</td>
<td>SSH Command Failed, while performing SSH scan.</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31638</td>
<td>The registered Pulse One server is not capable to receive profiler device(s)</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31638</td>
<td>The registered Pulse One server is not capable to receive profiler endpoints. Hence, uploading endpoints to Pulse One is retried after sometime.</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31697</td>
<td>On-Demand Subnet Scan started (With Collector details)</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31698</td>
<td>On-Demand Subnet Scan completed for a particular subnet and collector</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31699</td>
<td>On-Demand Subnet Scan completed by a specific collector</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31700</td>
<td>On-Demand subnet failed due to an error</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31754</td>
<td>Purge Successful! 82 aged out device(s)(older than 1 days) deleted from Profiler database</td>
<td>Event logs</td>
</tr>
<tr>
<td>PRO31755</td>
<td>Purge Failed! No aged out devices deleted from Profiler Database.</td>
<td>Event logs</td>
</tr>
<tr>
<td>SYS31660</td>
<td>SMTP error</td>
<td>Event logs</td>
</tr>
<tr>
<td>SYS31686</td>
<td>Error while generating notification</td>
<td>Event logs</td>
</tr>
<tr>
<td>SYS31687</td>
<td>Notification generated successfully</td>
<td>Event logs</td>
</tr>
</tbody>
</table>
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)**

```bash
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**

```bash
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**

```bash
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)**

```bash
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](Image)
2. Select **WLANs** from the top menu and then click on the corresponding SSID.

![Figure 37: WLANs](image)

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

![Figure 38: HTTP Profiling](image)

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 SNMMP 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 $8$GDEzgygwNO8mB6VAniej2NX2fKk7G9QDNKcxa13HR+I=
priv                   aes-cfb-128
priv-password $8$pgr3pzv3qf9S0kGomJ0w2M1bkrUipEgHxCRWIw2D8=
group                  prf-group

Appendix: Ports Used for Profiling

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

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