Pulse Policy Secure

Profiler

Administrator Guide

Product Release	9.0R2
Document Version	1.0
Published	August 2018

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

Pulse Policy Secure Profiler Administrator 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 www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA."

Palo Alto Networks, the Palo Alto Networks Logo, Palo Alto Networks Firewall, PAN-OS, User-ID, App-ID, and Panorama are trademarks of Palo Alto Networks, Inc. For additional information on Palo Alto Networks products, visit www.paloaltonetworks.com

Document Revision history

Document Version	Updated Topics	Description
August 2018	Updated Release number and formatting changes	No content changes from 9.0R1

Contents

About This Document

This guide describes the feature configuration tasks and administrator tasks for the Profiler integrated with Pulse Policy Secure.

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

A Note provides a tip, guidance, or advice, emphasizes valuable information, or provides a reference to related information.

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names. Identifies keywords and operands. Identifies the names of GUI elements. Identifies text to enter in the GUI.
italic text	Identifies emphasis. Identifies variables. Identifies document titles.
Courier font	Identifies CLI output. Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	A fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x |y |z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | y	A vertical bar separates mutually exclusive element.
<>	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member [member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure, LLC has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features.

- Find CSC offerings: https://www.pulsesecure.net/support
- Search for known bugs: https://www.pulsesecure.net/support
- Find product documentation: https://www.pulsesecure.net/techpubs
- Find solutions and answer questions using our Knowledge Base: https://www.pulsesecure.net/support
- Download the latest versions of software and review release notes: https://www.pulsesecure.net/support
- Search technical bulletins for relevant hardware and software notifications: www.pulsesecure.net/support
- Open a case online in the CSC Case Management tool: https://www.pulsesecure.net/support

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—For product warranty information, visit https://www.pulsesecure.net.

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at https://www.pulsesecure.net/support.
- Call 1- 844-751-7629 (toll-free in the USA).

For international or direct-dial options in countries without toll-free numbers, see www.pulsesecure.net/support.

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.

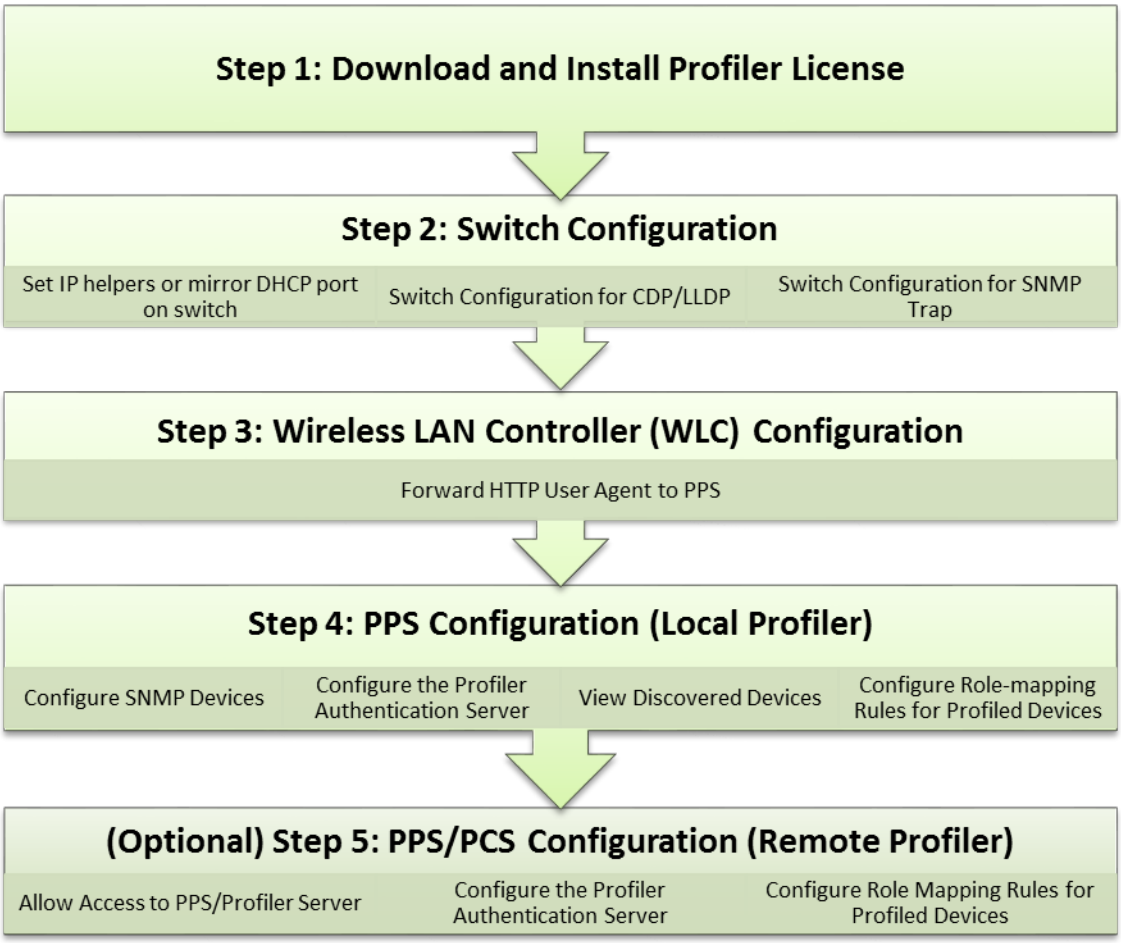
Pulse Policy Secure (PPS), an industry recognized network access control (NAC) solution, authenticates users, ensures that endpoints meet security policies, and then dynamically provisions access through an enforcement point (such as a firewall or switch) based on the resulting user session information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

Deployment and License Requirements

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

A high-level overview of the deployment steps needed to set up and run the Profiler is shown below. For detailed information, see Profiler Deployment Guide.



Discovering Endpoint Devices

The profiler uses a combination of active and passive scanning techniques to discover and collect information about all the endpoints on a network. Collectors are used to collect this information.

Collectors are broadly classified into active and passive collectors.

Passive Collectors

Passive collectors are initiated based on network events or timer events. For example, a new DHCP packet is received from the network which triggers the DHCP collector to profile the device.

DHCP collector

The profiler uses DHCP fingerprinting for endpoint classification of the end points such as laptops and desktops that are configured to have a DHCP IP address. One or more switched or WLAN controllers must 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 is easier to forward DHCP traffic to the Profiler using the SPAN/RSPAN configuration.

User Agent Collector

Some devices, like mobile phones, may not be profiled exactly with DHCP fingerprints. For example, an iPhone 6s phone is profiled as an iOS device or a Samsung Android 5.1 phone is profiled as Generic Android. The user agent information (contains granular information about the operating systems / OS versions) helps to profile these types of devices with more precision. The Profiler uses HTTP User Agent data that is captured from network traffic of the device to classify the devices.

Network Infrastructure Device Collector

While DHCP fingerprinting is useful for endpoints with a DHCP-assigned IP address, it cannot detect devices that are assigned static IP addresses. The Profiler can detect statically addressed endpoints by fetching the ARP/CAM table from Network Infrastructure Device using SNMP or SSH.

> Note: The ARP/MAC tables are fetched from the Network Infrastructure Device periodically. The poll interval can be configured by the administrator.

CDP and LLDP collection methods is also supported by any other devices that send CDP or LLDP announcements. CDP and LLDP data provides more accurate version of OS, model, and category information. The discovery protocols are enabled by default in most of the network infrastructure devices.

Network Infrastructure Device Collector -- SNMP

Network Infrastructure Devices that support standard SNMP MIBs are queried through SNMP to get the list of endpoints connected to them. The list of managed or unmanaged devices is available by querying the MAC table and ARP tables.

Network Infrastructure Device Collector -- SSH

For Network Infrastructure Devices that do not support standard SNMP MIBs, the Profiler uses SSH sessions to read the ARP/CAM tables.

> **Note:** In this release, this feature is supported for Palo Alto Network vendors only.

SNMP Trap

Profiler supports SNMP Trap based discovery which helps to accurately detect when the endpoint is connected to

or disconnected from the switch using link down, link up and mac change notification SNMP traps. This specifically helps in detecting the endpoints that are connected to the switches for brief period of times that are in between Profiler Poll interval for Network Infrastructure Devices.

Active Collectors

Active collectors are initiated by Profiler. Once devices are discovered using DHCP, SNMP or other mechanisms, more granular profiling is done only for those devices using various active collectors.

Nmap Collector

Nmap scan runs on all endpoints that have an IP address that are in white listed subnets, as and when they have discovered by other collectors.

WMI Collector

The Profiler runs WMI scan to collect more accurate and detailed information of Windows endpoints.

SSH Collector

SSH is another active collection method that can be used to gather detailed information which would help to profile endpoints accurately.

Note: In this release, this mechanism is supported for MAC OSX endpoints only.

MDM Collector

Pulse Policy Secure can communicate with Mobile Device Management Platforms such as AirWatch and MobileIron to retrieve more information about managed mobile endpoints.

As both an MDM server and the Profiler acts as a device attribute server, it is important to provide the administrator an aggregated view of the attributes. The attributes that are retrieved from the MDM are merged with the device attributes computed by the Profiler to offer better classification and manageability of those endpoints.

Configuring the Local Profiler Authentication Server

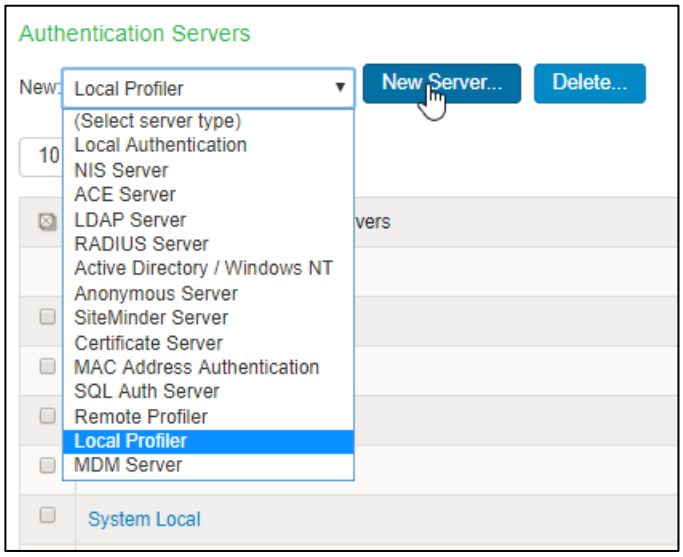
Ensure the following tasks are performed before proceeding with the Profiler Authentication server configuration.

- If you wish to use DHCP fingerprinting, you have configured the switch(s) to forward DHCP packets to the PPS.
- If you wish to use SNMP/SSH-based profiling from Network Infrastructure Devices, you have configured one or more switches in the Network Infrastructure Device page of the PPS Administrator User.
- You have downloaded the latest device fingerprints package from the support portal.

To create a new Local Profiler Authentication Server:

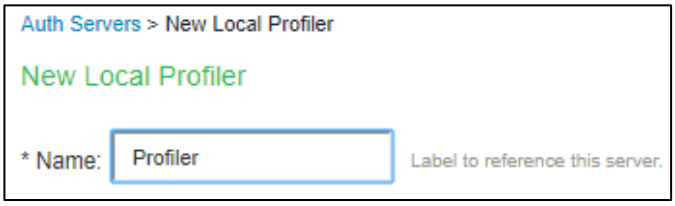
1. Select **Authentication > Auth. Servers**.
2. Select **Local Profiler** from the server type drop-down list and click **New Server**.

Figure 1: Creating a Local Profiler Authentication Server



3. Enter a name for the Authentication server.

Figure 2: Naming a Local Profiler Authentication Server



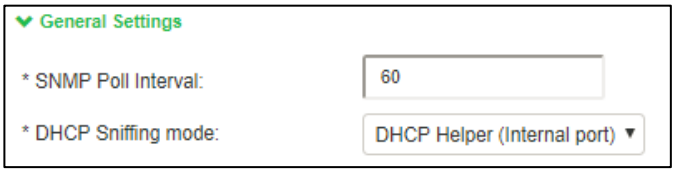
4. Click **Browse** and upload the device fingerprints package.

Figure 3: Uploading Device Fingerprints Package

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

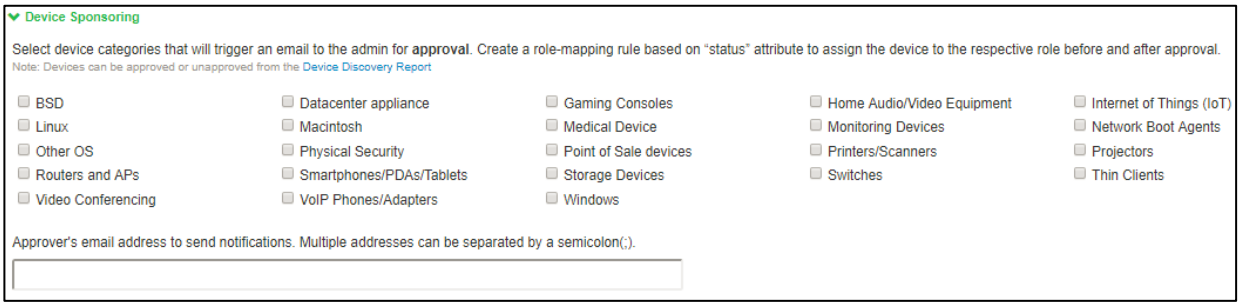
   Set SNMP Poll interval, if any Network Infrastructure Devices are configured. By default, the poll interval is set as 60 minutes.

Figure 4: General Settings



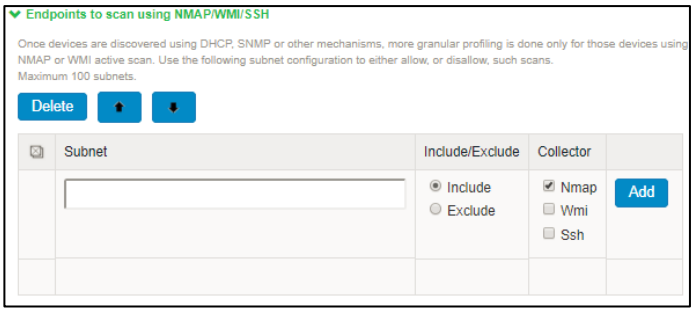
6. (Optional) Select device categories which trigger e-mail(s) to the administrator for approval. Also create a role-mapping rule based on **status** attribute to assign the device to the respective role before and after approval. For more information see, Device Sponsoring.

Figure 5: Device Sponsoring



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

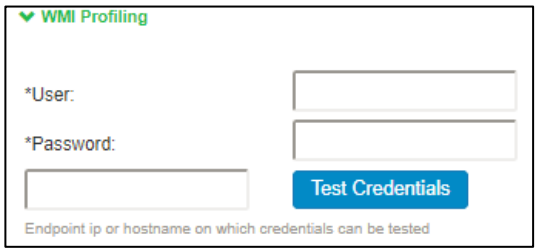
Figure 6: Adding One or More Subnets



8. (Optional) In the WMI profiling section, specify the domain administrator or user with administrator credentials to fetch accurate endpoint information from remote desktops running Microsoft Windows.

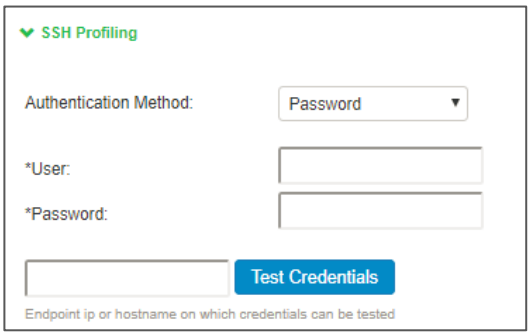
Note: If multiple antivirus software is installed on the remote desktops, WMI fetches information about only one of the antivirus. WMI does not fetch information about *Windows Defender*.

Figure 7: WMI Profiling



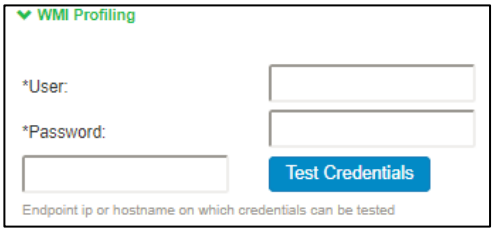
9. (Optional) In the SSH Profiling section, select the Authentication Method and enter credentials as applicable. Enter the Endpoint IP or hostname to test the credentials.

Figure 8: SSH Profiling



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

    Figure 9: MDM Server



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

Devices that are discovered are profiled and updated in the Device Discovery Table and an overall summary is shown in the Device Profiles Dashboard.

Profiler Dashboard

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

Click on each chart or numbered panel to view detailed information in the device discovery report.

The upper part of the dashboard displays the number panels representing the number of devices for each of the following status:

- Devices waiting to be Profiled
- Devices for which the profile has changed
- Unmanaged devices
- Devices waiting for administrator approval
- Devices added in last 24 hours
- Devices added last week
- Devices added last month

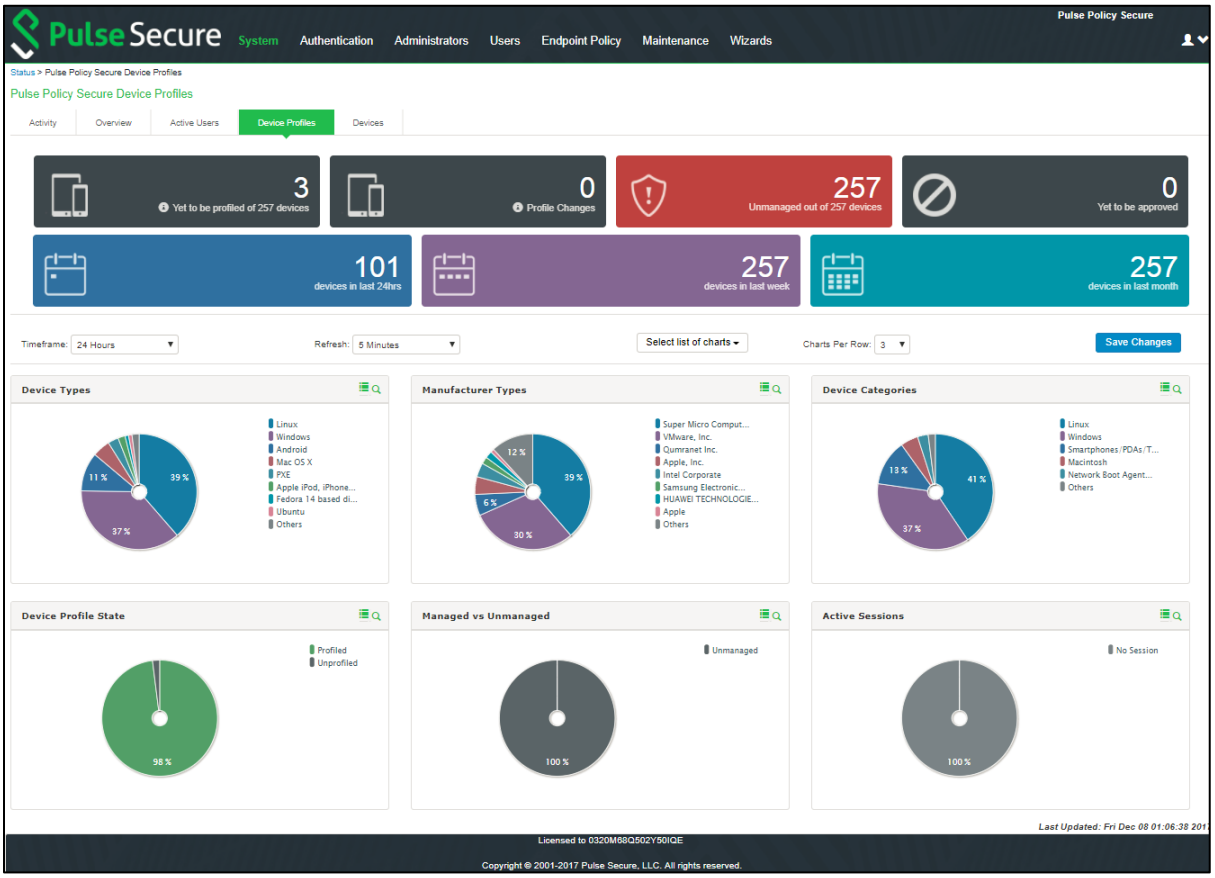
The charts in the dashboard can be customized by the administrator by setting the following parameters:

- Timeframe: The charts display information for the specified timeframe. By default, the information for the last 24 hours is displayed. The timeframe can also be set to 7 days, 30 days, or All.
- Refresh: The refresh time interval to update the charts. By default, the charts refresh every 5 mins. The time interval can also be set to disabled, 10 minutes, 30 minutes, or 60 minutes.
- Select list of charts: List of charts to select to display in the dashboard.
- Charts Per Row: Number of charts to display in a row on the dashboard. By default, 3 charts are displayed in a row. 1 or 2 charts can be displayed in each row.
- Profiler: The profiler for which the information is displayed. By default, information for all profilers are displayed.

The following charts are displayed in the dashboard:

- Device Profile State: Represents the device classification based on Profile status such as Profiled devices, Unprofiled devices, Profile changed devices.
- Manufacturer Types: Represents the device classification based on the device manufacturer. For example, VMware. Inc, Apple. Inc
- Device Categories: Represents the device classification based on the device category such as smartphones, laptops, windows.
- Device Types: Represents the device classification based on device types. For example, Windows, Apple iPod, iPhone.
- Managed vs Unmanaged: Represent the device classification on the managed and unmanaged device status. Managed devices are detected by the MDM or a Pulse Client session is established on the device.
- Active Sessions: Represent the devices based on the device sessions such as Remote sessions and On-Premise session.

Figure 10: Dashboard View

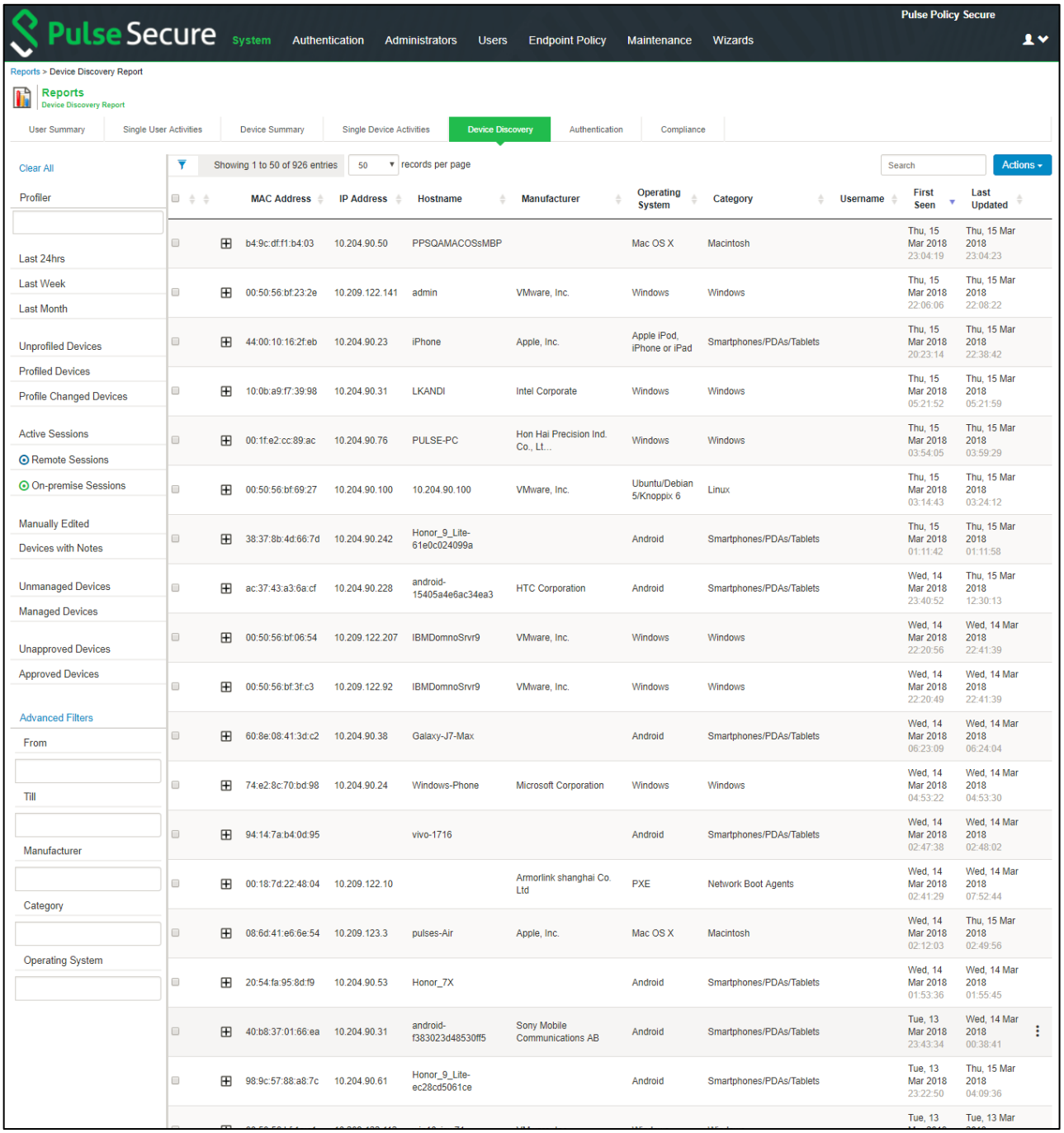


Device Discovery Report Table

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.

Select **System > Reports > Device Discovery** to display the table.

Figure 11: Device Discovery Report Table

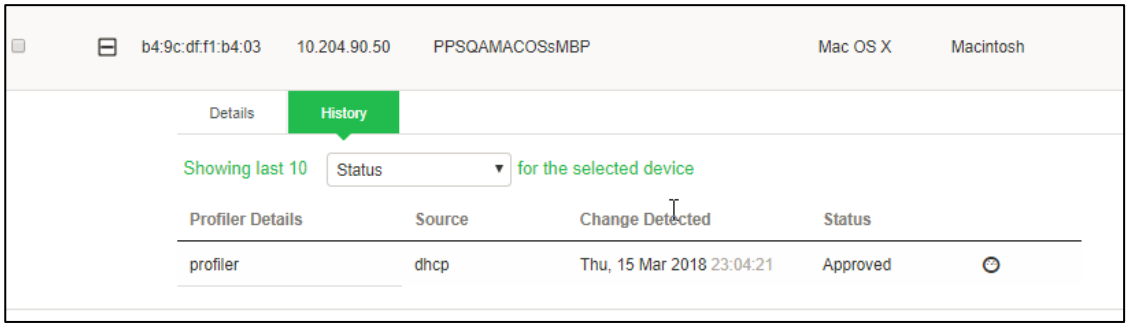


Endpoint Information

All current and historical information for a device is displayed in an expanded view based on IP address, sessions

(remote, local) or profiles changes.
Expand the required endpoint to display current Details and History.

Figure 12: History based on IP Address



Endpoint Filters

A list of filters is available for quick analysis of discovered devices. The filers are displayed to the left of the table.

- Filters based on time – Last 24 hours, Last week, Last month
- Filters based on sessions – Active sessions, Remote sessions, On-premise sessions
- Filters based on actions of the discovered devices – Managed devices, Unmanaged devices, Profiled devices, Approved and unapproved devices, Unprofiled devices, Profile changed devices. Manually edited devices, Devices with Notes

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

Report Operations

The Device Discovery Report Table allows the following operations on all the discovered devices.

- **Records per page:** Allows to customize the number of records displayed in the page.
- **Head row:** Lists the main attributes for the devices such as IP Address, MAC Address etc. Click the column head to sort the table with respect to the column. Double click to sort in reverse order.
- **Search**: Allows to search devices based on the Address or other device attributes.
- **Actions**: Allows the following functions:
    - **Approve/Unapprove selected devices**: Allows to manually approve or unapproved the selected devices.
    - **Add Device**: Allows to add new devices. Enter important attributes like MAC Address, Manufacturer, Operating system, and category.
    - **Download Report**: Allows to download and save the report in CSV format.
    - **Delete Selected**: Allows to delete the selected devices.

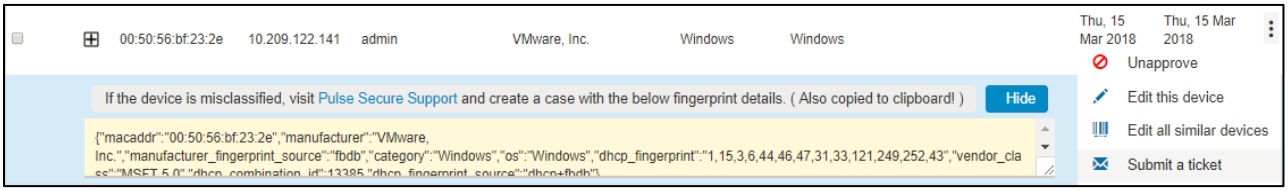
Device Operations

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

- **Approve/Unapprove:** Each endpoint has an attribute called **status** and allows to manually approve or unappove a specific device. See Device Sponsoring for more information.
- **Edit:** Allows to edit **Manufacturer**, **Category** and **Operating System** fields. Manually edited devices are not

overwritten by Profiler during update.

- Edit all similar devices: Allows to edit all similar devices which have same fingerprint. When similar devices are added, the updated fingerprint is used for profiling.
- Submit a ticket: The Profiler uses Fingerbank database to classify devices.
  It is possible that some devices are not correctly classified in this process. In such cases, the administrator can use the Copy Fingerprint option to copy the fringerprint and send the relevant information about the wrongly classified device to the Pulse Secure using an E-mail. This information is verified before updating the Custom Fingerprint database.



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

Access Control

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.

Spoof Detection

The profiler allows a mechanism to detect MAC address spoofing. The Profiler compares the stored information with the latest information to detect MAC address spoofing. Latest information about endpoints is fetched on a periodic basis.

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

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

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

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

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

Note: This works only when the actual device is profiled before spoofed device connects.

Device Sponsoring

This feature allows an administrator to manually approve devices that belong to a specific category on a production network. The administrator can configure categories that need approval and the profiler to identify the devices that belong to these categories. The profiler notifies the administrator when new devices are detected. The administrator can approve so that the role of the newly detected device changes according to the role mapping rules.

Configuring Role-Mapping Rules for Profiled Devices

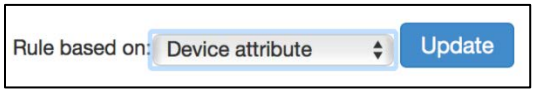
To configure role-mapping rules:

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

Figure 13: Device Attributes

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

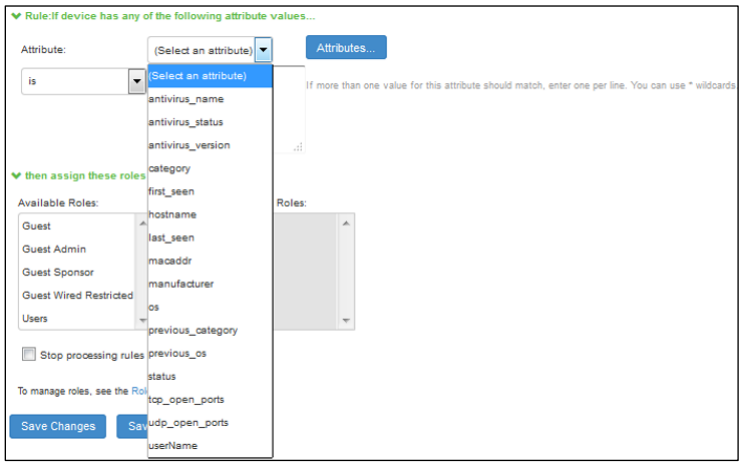
Figure 14: Rule based on attribute



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

7. Enter a name for the rule (if creating a new one).
8. Create the new role mapping rule based on the new device attributes that are now available in the attributes drop-down field. When setting the attribute value, make sure the value you enter is an exact match for the value displayed in the Device Discovery Report table. Wildcards (* and ?) can be used in the attribute value.

Figure 15: Creating New Role Mapping Rule



9. After assigning the roles, click **Save Changes**.

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

The Profiler can also work as a device attribute server for authentication. Wildcards (* and ?) can be used in the attribute value.

The following table lists the device attributes based on which you can create rules and assign to the user roles.

Attribute Name	Description	Values/Example
antivirus_name	The name of the antivirus running on the device	MacAfee, Symantec Endpoint Protection, etc.
antivirus_status	The status of the antivirus running on the device	**`Enabled`** or **`Disabled`**
antivirus_version	A check on the antivirus version running on the system is up to date or not	**`Outdated`** or **`Current`**
category	The category of the device. All devices are broadly classified into 30+ different categories.	Windows, Linux, Android, etc.
custom	The administrator defined value(s) for the device.	Administaror defined values
first_seen	The timestamp of the device discovery	2018-04-04 06:52:16.993606+00:00
hostname	The hostname of the device	Admin-pc
last_seen	The timestamp when the device was last updated	2018-04-06 05:38:43.877617+00:00
macaddr	The unique hardware address of the device	78:9c:57:4f:2c:**
manufacturer	The device manufacturer name	Lenovo*, HP*, etc
os	The Operating system running on the device or the type of the device.	Windows 7.x, AC OS X, Ruckus, Wireless AP, etc
os_patch	The patch information of the operating system installed on the device	"Service Pack *"
previous_category	When a device category is changed, the device can be listed using the previous category of the device.	N/A
previous_os	When a device operating system is changed, the device can be listed using the previous category of the device.	N/A
profiler_name	The name of the profiler used to profile the device	Local Profiler
status	The administartor approval status of the device	**`Approved`** or **`Unapproved`**
tcp_open_ports	The open TCP ports on the device	List of port values
udp_open_ports	The open UDP ports on the device	List of port values
userName	The username used to access the device	administrator

Import/Export Profiler Database

Profiler allows administrator to download the profiled data in CSV or CFG (binary import/export) format for readability or reporting purpose. The administrators can use this data to analyze and troubleshoot the configurations of devices. The file can be password protected for security reasons.

The Profiler supports Import / Export of Profiler Device Database in Binary or CSV formats. The database files can be used to troubleshoot, backup database, or restore the database in case of any crash or data loss.

Import / Export Profiler Device Data in Binary format

To avoid accidental loss of database due to Appliance Hardware failures, software upgrade or accidental deletion (if backed up), it is required to back up the database and restore whenever required. Profiler device database can be exported and imported in Binary format.

Binary Export

On export, profiler device data is encrypted and downloaded with filename **`Profiler*.cfg.`**

Binary Import

The device database import in Binary format erases the existing database completely. The endpoint session information is invalidated.

Import / Export Profiler Device Data in CSV format:

The CSV format allows the administrator to add additional endpoints into the profiler device database. The CSV format also allows to import some custom information into the database.

CSV Export:

On export, the complete device data information is exported into a CSV file. This is the same behavior as the Download Report in the Profiler DDR.

CSV Import:

- The CSV import to the profiler device database, appends the existing database. It does not erase the existing database completely.
- The CSV format allows to import only essential endpoint information such as Macaddr, IP, hostname, manufacturer, os, category, previous_os, previous_category, notes, first_seen, last_seen and custom.
- For existing devices, the data is overwritten for the supported fields from CSV. Remaining data remains as is.
- For devices that are marked as Manually Edited Devices, no further classification is performed on the imported endpoints
- Custom field can be provided in the CSV for import. This column is visible in the DDR only if customer has imported custom data. Custom field is available for role mapping rules.

Import/ Export of Profile Modifications database in Binary format

This functionality is used when the administrator performs profile modifications and wants the same modifications to reflect in other profilers (Standalone or forwarders). The profile modifications are appended to existing modifications on import.

Troubleshooting

Tests

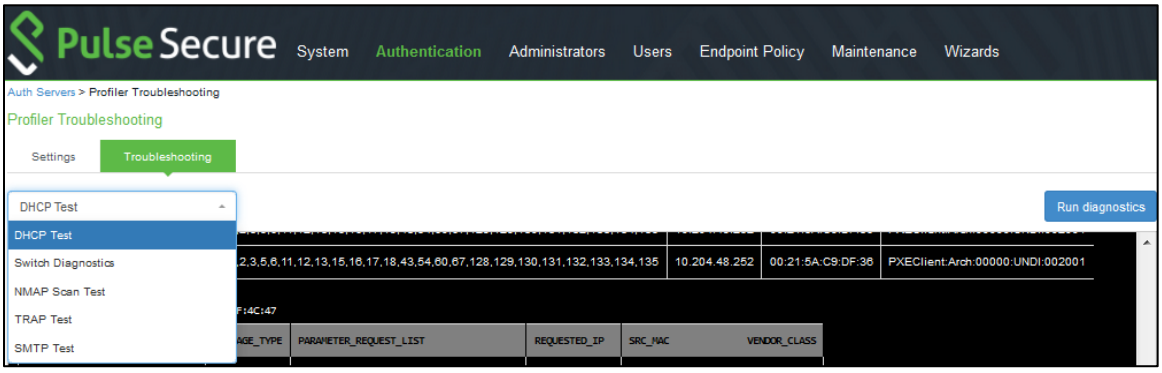
The following tests helps to identify and solve basic problems associated with configurations of the Profiler.

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

To execute the tests, perform the following steps:

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

Figure 16: Troubleshooting



Profiler Logs

The Profiler logs all its activities to the Event Log and Administrator Access Logs.

To see the Profiler logs in the Event log, select **Log/Monitoring > Events > Log Settings** and enable the "Profiler Events" checkbox.

Figure 17: List of Events to Log

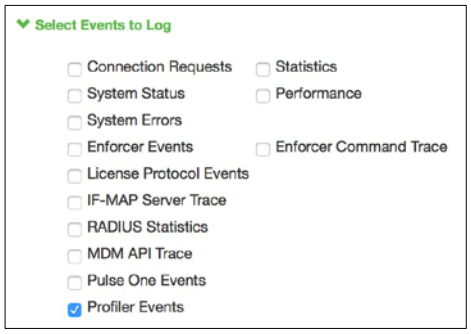


Table 1: Profiler logs

Event ID	Description	Log Type
PRO31368	New Device discovered and profiled by Profiler	Event logs
PRO31369	Device Profile (OS/Category) changed and detected by Profiler	Event Logs
PRO31592	Device(s) Email Notification sent for Approval	Event logs
PRO31572	Profiler has exceeded the licensed device count excluding the grace count.	Event Logs
PRO31557	Profiler has exceeded the licensed device count including the grace count	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
PRO31388	No Network Infrastructure Devices are configured for polling	Event Logs
ADM31595	Device added in Device Discovery report.	Admin Logs
ADM31631	Device addition failed in Device Discovery Report.	Admin Logs
ADM31591	Device updated in Device Discovery report.	Admin logs
ADM31573	Device(s) are deleted from 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
PRO31447	WMI connection failed	Event Logs
PRO31448	WMI Query Failed	Event logs
PRO31449	WMI Scanning a device	Event Logs
PRO31476	Fingerprint Database Initialization Failed	Event logs
PRO31443	Password Decryption Failure	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
PRO31638	The registered Pulse One server is not capable to receive profiler device(s)	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
PRO31459	Device attributes got updated	Event logs
PRO31480	Fingerprint download Started from peer	Event logs
PRO31481	Successfully downloaded fingerprint from peer	Event logs
PRO31479	Failed to download fingerprint from peer	Event logs
PRO31457	Device attributes are retrieved from profiler	Event logs
ADM31458	Profiler API keys retrieved Success/Failure	Admin logs
ADM31405	Network Infrastructure Device Poll Interval Updated	Admin logs
PRO31461	Encryption or decryption failed for config parameters	Admin logs
ADM31444	WMI User added	Admin logs
ADM31445	WMI User modified	Admin logs
ADM31446	WMI User deleted	Admin logs

Profiler Deployment Cases

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

Standalone Profiler

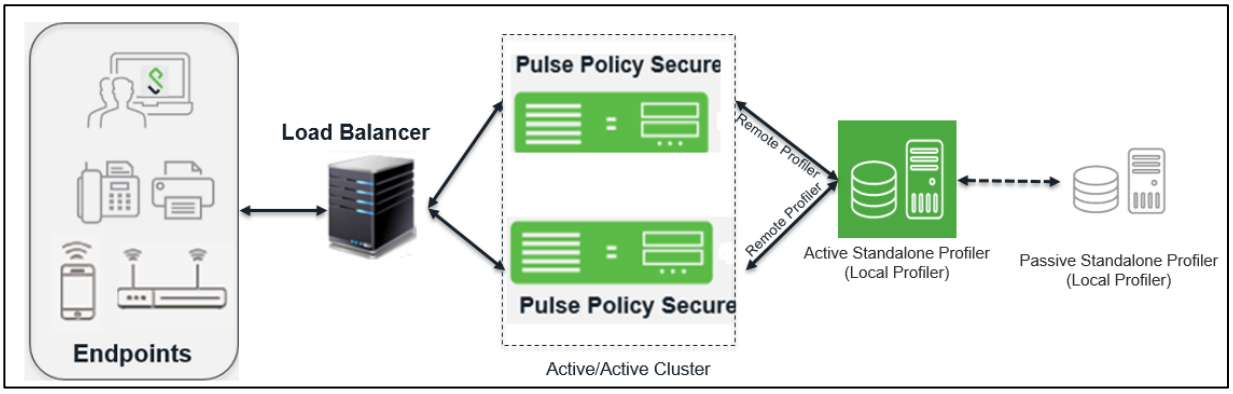
Standalone Profiler can be deployed as an independent appliance. All PPS and PCS appliances communicate with this Standalone Profiler for authorization.

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 un-clustered set) of PPS appliances.

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

Figure 18: 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:

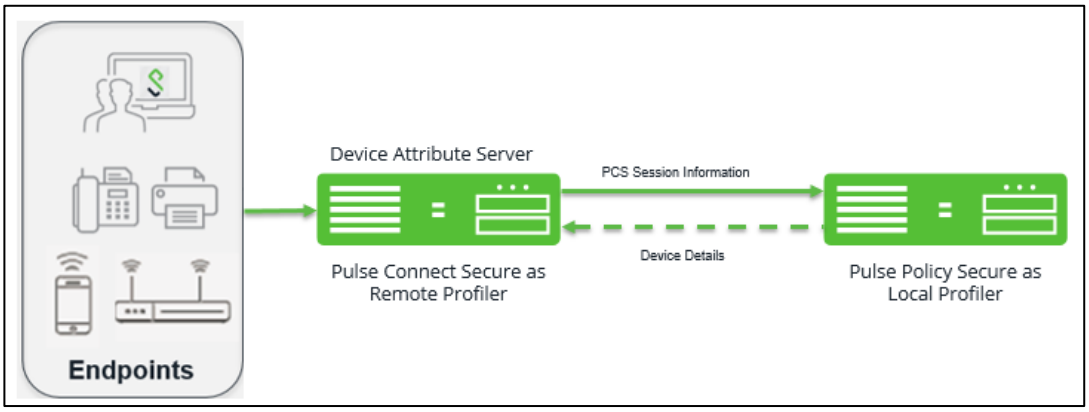
- Information such as hostname and IP address, device IP address and MAC address, session identifier, user-agent are retrieved by the session and sent to the Profiler.
- The Profiler returns Device OS, Device Manufacturer, Device Category and Session Identifier to PPS/PCS.
- The Profiler updates the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

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 19: Example of a Remote Profiler

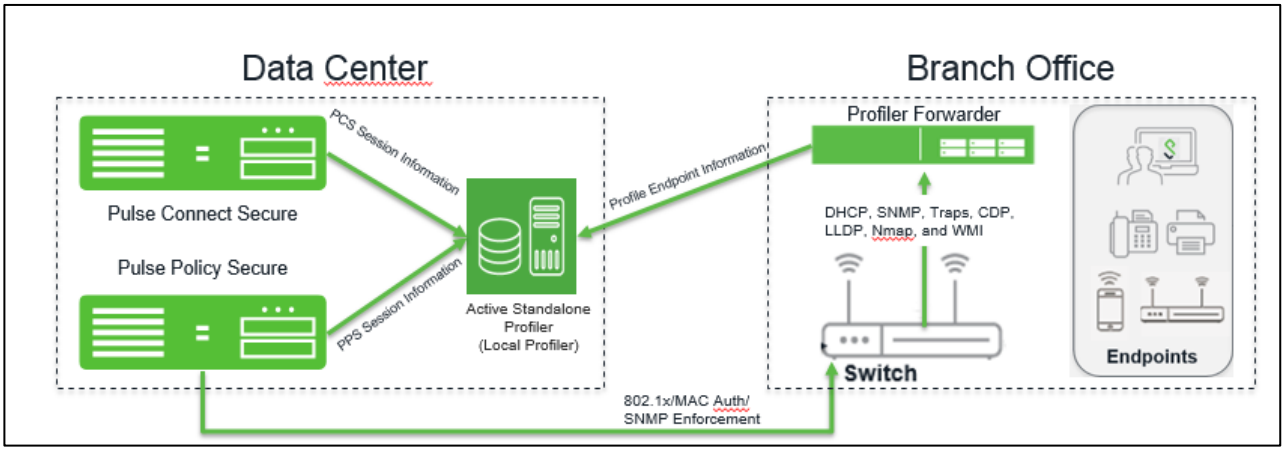


Profiling devices in branch offices

This 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 20: 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.