

# Pulse Policy Secure Profiler

## Administration Guide

Product Release9.1R2Document Version1.0PublishedJuly 2019

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

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 Connect Secure/Pulse Policy Secure License Configuration for PSA-V: On-Premise and Public Clouds 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 **https://www.pulsesecure.net/support/eula**. By downloading, installing or using such software, you agree to the terms and conditions of that EULA."

## Contents

ABOUT THIS DOCUMENT	5
Document conventions	5
Notes, cautions, and warnings	5
Text formatting conventions	
Command syntax conventions	
Self-Help Online Tools and Resources	
Requesting Technical Support Opening a Case with PSGSC	
INTRODUCTION	
DEPLOYMENT AND LICENSE REQUIREMENTS	
DISCOVERING ENDPOINT DEVICES	9
Passive Collectors	
DHCP collector	
User Agent Collector	
Network Infrastructure Device Collector SNMP Trap	
Active Collectors	
Nmap Collector	
WMI Collector	
SSH Collector	
MDM Collector	
SNMP HOST Collector Configuring the Local Profiler Authentication Server	
PROFILER REPORTS	
Dashboard	
Profiler Report Scheduling	
DEVICE DISCOVERY REPORT TABLE	
ENDPOINT INFORMATION	
ENDPOINT FILTERS	
Report Operations Device Operations	
ACCESS CONTROL	21
Spoof Detection	
Device Sponsoring	
Profile Groups Creating Rules for Profile Groups	
Configuring Role-Mapping Rules for Profiled Devices	
AGENTLESS HOST CHECKER WITH PROFILER	
Configuring Agentless Host Checker with Profiler	
IMPORT/EXPORT PROFILER DATABASE	
Import / Export Profiler Device Data in Binary format	
IMPORT / EXPORT PROFILER DEVICE DATA IN DIVART FORMAT	
IMPORT/ EXPORT OF PROFILE MODIFICATIONS DATABASE IN BINARY FORMAT	

TROUBLESHOOTING	
Tests Diagnostic Logs	
Profiler Logs	
PROFILER DEPLOYMENT CASES	
Standalone Profiler	
Remote Profiler	
Profiling devices in branch offices	
Using Profiler Forwarder	
Using Linked Profiler (With PPS Functionality)	

## 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, <b>show</b> WWN.	
0	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.	
х   у	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].	
١	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://support.pulsesecure.net
- Search for known bugs: <u>https://support.pulsesecure.net</u>
- Find product documentation: <u>https://www.pulsesecure.net/techpubs</u>
- Find solutions and answer questions using our Knowledge Base: <u>https://support.pulsesecure.net/knowledge-base-and-security-advisories/</u>
- Download the latest versions of software and review release notes: https://support.pulsesecure.net
- Open a case online in the CSC Case Management tool: <u>https://support.pulsesecure.net</u>

### **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://support.pulsesecure.net.
- Call 1- 844-751-7629 (toll-free in the USA).

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

## Introduction

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.

The Pulse Secure 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.

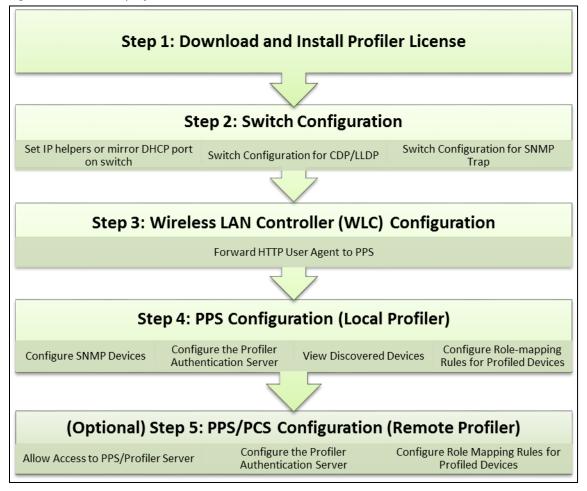
Pulse Policy Secure integrates with the Profiler to provide visibility and control of endpoint devices. This document focuses on features of the Profiler in a network with an existing Policy Secure deployment already configured with the basic elements required to provide network access, including authentication 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**.

#### Figure 1: Profiler Deployment Process



## **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 an 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.

### SNMP HOST Collector

SNMP-HOST Collector is a collection method that receives endpoint information where the endpoints are monitored through SNMP.

Note: In release 9.1R1, SNMP HOST collector is applicable for Windows and Pulse-Appliances only.

### 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 2: Creating a Local Profiler Authentication Server

New:	Local Profiler	New Server	Delete
10	(Select server type) Local Authentication NIS Server ACE Server		
	LDAP Server RADIUS Server	vers	
	Active Directory / Windows NT Anonymous Server		
	SiteMinder Server Certificate Server		
	MAC Address Authentication SQL Auth Server		
	Remote Profiler Local Profiler		
	MDM Server	]	
	System Local		

3. Enter a name for the Authentication server.

#### Figure 3: Naming a Local Profiler Authentication Server

New Local Profiler	Auth Serv	ers > New Local Profiler	
* Name	New Local Profiler		
* Name: Profiler			
"Name. Fromer Laber to reference this serve	* Name:	Profiler	Label to reference this server.

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

#### Figure 4: Uploading Device Fingerprints Package



- 5. (Optional) The SNMP/SSH scan for Network Infrastructure Devices would trigger and look for connected endpoints after a predefined Poll interval.
  - Set SNMP Poll interval, if any Network Infrastructure Devices are configured. By default, the poll interval is set as 60 minutes.
  - Select the DHCP forward mode. RSPAN for external ports and DHCP Helper for internal ports.
  - Select the interval to purge older devices from the database periodically. By default, the interval is set to Never.

#### Figure 5: General Settings

✓ General Settings	
* Poll Interval:	60
* DHCP Sniffing mode:	DHCP Helper (Internal port) 🔻
* Purge devices older than:	Never •

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, <u>Device Sponsoring</u>.

Select **Use emails from General Settings** to send e-mails to address specified in General Settings or select **Custom** and enter the e-mail addresses separated by semicolon.

Enter the Profiler hostname or IP address to fill the URL. This link in the e-mail notification allows to quickly to access the Device Discovery Report and take appropriate action for devices that require approval.

#### Figure 6: Device Sponsoring

✓ Device Sponsoring				
Select device categories that will trigger a Note: Devices can be approved or unapproved fr		role-mapping rule based on "status" attribut	te to assign the device to the respective role	before and after approval.
BSD BSD	Datacenter appliance	Gaming Consoles	Home Audio/Video Equipment	Internet of Things (IoT)
Linux	Macintosh	Medical Device	Monitoring Devices	Network Boot Agents
Other OS	Physical Security	Point of Sale devices	Printers/Scanners	Projectors
Routers and APs	Smartphones/PDAs/Tablets	Storage Devices	Switches	Thin Clients
Video Conferencing	VoIP Phones/Adapters	Windows		
Set approver's email address(es) to send notifications. Emails will be sent whenever a new endpoint is classified under an 'unapproved' category.  Use emails from General Settings  Custom The emails will be sent to following email addresses. Multiple addresses can be separated by a semicolon(;).				
Test Settings				
SMTP server configuration is required for sending emails. Currently SMTP Server is configured and enabled. Click here to change the settings.				
* URL for Device Discovery Report. It will appear in the notification email as a link for quick access to the devices that need approval. Profiler hostname or IP address is needed to complete the URL.				
https:// 10.96.102.2	/dana-admin/reporting/report_device_disco	very.cgi		

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

On-Demand Scan can be triggered anytime on the subnets for selected collectors.

#### Figure 7: Adding One or More Subnets

Y Endp	oints to scan using Active Collectors			
WMI an	evices are discovered using DHCP, SNMP or other mechanisms, more gran d SSH active scan. Use the following subnet configuration to either allow, o rm 100 subnets.		nly for those devices using	g SNMP, NMAP,
	y products such as antivirus etc may block active scan on endpoints. ommanded to disable such blocks for better discovery and classification.			
Note the	nand Scan: Trigger one time scan, which scans the subnets selected in abo at the regular profiler classification for these collectors will be halted and res		collectors.	
Dele	ete 🔹 🔹 Start On-Demand Scan			
	Subnet	Include/Exclude	Collector	
		<ul> <li>Include</li> <li>Exclude</li> </ul>	<ul><li>✓ NMAP</li><li>WMI □ SSH</li><li>■ SNMP(HOST)</li></ul>	Add
	10.204.0.0/16	Include	NMAP, WMI	
	172.21.0.0/16	Include	SSH	

8. (Optional) In the SNMP (HOST) Profiling section, enter the possible names for the community list for the endpoints monitored through SNMP.

#### Figure 8: Community List

SNMP(HOST) Profili	ng	
If Endpoints are being mo	nitored through SNMP then Profiler will fetch device attribut	tes through SNMP.
Community List:		

9. (Optional) In the WMI profiling section, select **Configure WMI credentials** and specify the domain administrator or user with administrator credentials to fetch accurate endpoint information from remote desktops running Microsoft Windows. Select **Use Active Directory server credentials** to use existing Active Directory server credentials.

Select **Allow deep scan** to control the level of information to fetch from the Endpoint remotely through WMI. Deep Scan includes information on ports, process, and security product details such as product version, signature version, signature date attributes. This option is required if Agentless Host checker with Profiler policies are configured for endpoint posture assessment.

#### Figure 9: WMI Profiling

✓ WMI Profiling		
Configure WMI credentials.	Use Active Directory set	rver credentials.
*User:	flower\administrator	User or domain\user or user@domain.com for endpoints.
*Password:		
	Test Credentials	
Endpoint ip or hostname on which cred	lentials can be tested	
Allow deep scan	Deep scan fetches advanced attributes from windows endpoints	
Disable deep scan if registry scan, pro But, note that agentless hostcheckin		etting them from each endpoint is a time consuming process. Ites for some of its policies.

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

#### Figure 10: SSH Profiling

✓ SSH Profiling	
Authentication Method:	Public key 🔻
*User:	
*Private key:	
passphrase:	
	Test Credentials
Endpoint ip or hostname on which	n credentials can be tested

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

Figure	11:	MDM	Server
--------	-----	-----	--------

✓ MDM Server		
MDM server:	mobilemdm	•

12. 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 <u>Device Profiles Dashboard</u>.

The devices can be grouped based on group name and rules using device attributes. For more information see, <u>Profile Groups</u>.

## **Profiler Reports**

### 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:

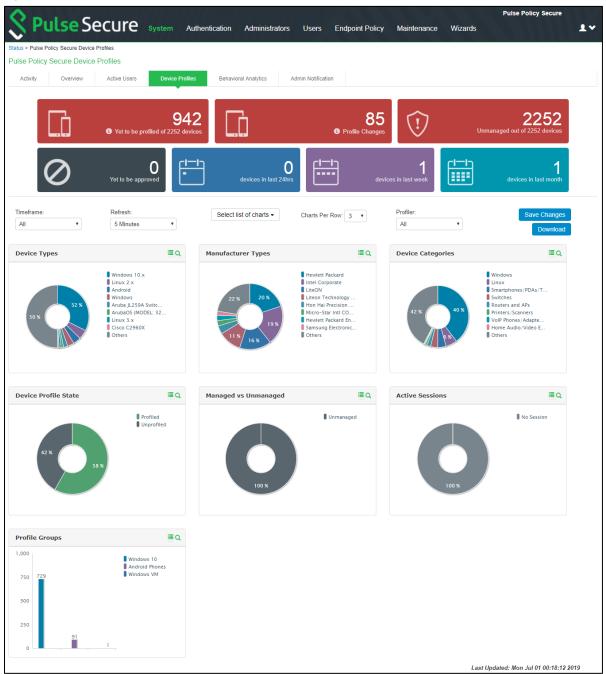
- Devices waiting to be Profiled
- Devices for which the profile has changed
- Unmanaged devices
- Devices waiting for administrator approval
- Devices added in last 24 hours
- Devices added last week
- Devices added last month

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 categories 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.
- **Profile Groups**: Represents the profile groups based on the device classification. See <u>Profile Groups</u> for more information.



#### Figure 12: Dashboard View

The charts can be viewed on the dashboard or can be downloaded as a report in PDF format. The reports can be scheduled to be emailed as well.

### Profiler Report Scheduling

The Profiler reporting can be scheduled, and the reports can be delivered in the e-mail notifications to the specified addresses.

- 1. Navigate to System  $\rightarrow$  Configuration  $\rightarrow$  Notification  $\rightarrow$  Email Notification.
- 2. 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.
- 3. Select the interval to generate and send the report e-mail notifications. The reports are sent daily, weekly

or monthly.

- 4. Select **Generate Full Report** to generate and send complete report every time. If the option is not selected, the report with only the incremental changes are generated.
- 5. Click Save Changes.

### Figure 13: Report Scheduling

0									F	ulse Policy Secure	
2 Pu	lse Se	cure	System	Authentication	Administrators	Users	Endpoint Policy	Maintenance	Wizards		<b>*</b> *
Configuration > No	tification > Email Notif	fications									
Email Notificat	ions										
Licensing	Pulse One	Security	Certificate	s DMI Agent	Sensors	Client Types	SAML	Guest Access	Advanced Networking	Notification	
General Emai	Notification									•	
Set appropriate	<ul> <li>Profiler Reports Scheduling</li> <li>Set appropriate schedule and emails to recieve Detailed Profiler reports (PDF format), in your inbox.</li> <li>Use emails from General Settings          Custom         The emails will be sent to following email addresses. Multiple addresses can be separated by a semicolon().</li> </ul>										
forexample	@domain.com					Те	st Settings				
Email Schedule Save Changes	SMTP server configuration is required for sending emails. Currently SMTP Server is configured and enabled. Click here to change the settings.      Email Schedule:     Daily     O     Generate Full Report     Select an option based on your email schedule frequency.     Select the checkbox if full reports needs to be generated every time.      Save Changes     Reset     indicates required field										

## 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 14: Device Discovery Report Table

Q Dulco	Sac											Pulse Policy Sec		
🖇 Pulse	Sec	ure	System	Authentication	n Administ	rators Users	Endpoin	t Policy	Maintenance	Wiza	rds			<b>.</b> '
ports > Device Discovery Rep	port													
Reports Device Discovery Report														
User Summary Si	ngle User Act	tivities	Device Summa	ry Single D	Device Activities	Device Disco	very Au	uthentication	Compliance	В	ehavioral Anal	ytics Infecte	ed Devices	
Clear All	^ Ţ	Showin	ig 1 to 10 of 1,510 er	ntries 10 •	records per pa	ige				Θ	Basic 👻 S	Search	Actie	ion
Profiler		A	MAC Address 💧	IP Address	Hostname 💧	Manufacturer 💧	Operating	Categor	Session	First	Last	Profiler(s)	Groups	
		v	IIIAC Address 🕌	ii Address 🕌	nostiune 🚽		System	Cuttyon	User V	Seen 🔻	Updated		Groups	P.
		Ħ	2e:b6:93:09:b9:1f	10.204.56.84			Linux 3.x	Linux		Tue, 26 Mar 2019	Tue, 26 Mar 2019	- Local Profiler		
ast 24hrs										13:09:28	13:09:46			
ast Week		Ē	00.50.50.00	40.00 77 470		MANNER INC.				Tue, 26 Mar	Tue, 26 Mar 2019	– Local Profiler		
ast Month		Ŧ	00:50:56:83:cd:be	10.90.77.173		VMware, Inc.				2019 13:09:26	13:09:26	- Local Promer		
Inprofiled Devices										Tue, 26	Tue, 26			
Profiled Devices		Ŧ	00:50:56:83:6b:c0	10.96.77.174		VMware, Inc.				Mar 2019 13:09:24	Mar 2019 13:09:24	- Local Profiler		
Profile Changed Devices										Tue, 26				
Active Sessions		Ŧ	de:c1:31:b9:3d:dc	10.204.58.34			Linux 3.x	Linux		Mar 2019	Tue, 26 Mar 2019 13:09:46	- Local Profiler		
Remote Sessions										13:09:24	13.09.40			
On-premise Sessions		Ħ	52:54:00:58:f6:16	10.209.116.212						Tue, 26 Mar	Tue, 26 Mar 2019	- Local Profiler		
Manually Controlled										2019 12:09:32	13:09:32			
Devices with Notes		Ē	10. 7.74.24.265	40 204 00 05		HUAWEI				Tue, 26 Mar	Tue, 26	Land Decilies		
		Ŧ	d8:c7:71:34:2f:fa	10.204.90.65		TECHNOLOGIES CO.,LTD				2019 12:09:32	Mar 2019 12:11:34	<ul> <li>Local Profiler</li> </ul>		
Inmanaged Devices										Tue, 26	Tue, 26			
lanaged Devices		Ŧ	00:50:56:83:13:81	10.96.78.21		VMware, Inc.				Mar 2019 12:09:31	Mar 2019 13:09:31	- Local Profiler		
Inapproved Devices										Tue, 26	<b>T</b> 00			
pproved Devices		Ŧ	c0:ee:fb:f3:5b:04	10.204.90.86		OnePlus Tech (Shenzhen) Ltd				Mar 2019	Tue, 26 Mar 2019 13:09:29	- Local Profiler		
										12:09:29	13.03.23			
Advanced Filters		Ŧ	ca:ac:b4:b4:26:2b	10.204.58.28			Linux 3.x	Linux		Tue, 26 Mar 2019	Tue, 26 Mar 2019	- Local Profiler		
FIUII										12:09:27	13:09:28			
		m	00-50-56-00-64-00	10.06.77.172		Vittures Inc.				Tue, 26 Mar	Tue, 26	Lecal Droffic-		
Till		Ŧ	00:50:56:83:61:03	10.90.77.172		VMware, Inc.				2019 11:09:29	Mar 2019 11:09:29	<ul> <li>Local Profiler</li> </ul>		
								_						_
Manufacturer	-							F	irst Previous	1 2	3 4	5 151	Next	l

### **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 15: History based on IP Address

00:1a:4a:18:11:63 10	0.209.122.161 vreddy	Qumranet Inc.	Windows		Windows	Wed, 07 Dec 2016 20:09:40	Sat, 18 Feb 2017 07:12:28
Details His	tory						
Showing last 10	IP Addresses 🔹 for the s	elected device					
Source	Change Detected	host-name	IP Address				
dhcp	Wed, 07 Dec 2016 20:10:30	w+-laft	10 209 122 155	0			
dhcp	Wed, 07 Dec 2016 20:09:53	washily					

### **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 MAC Address, IP Address, or other device attributes. Click? for help.
  - Basic Search allows to search the device discovery report with any text or keyword.
  - Advanced Search allows to enter the expression with operators and wildcards to obtain specific search results. For example, (snmp.switch\_ip = "10.204.58.??" and manufacturer != "\*juniper\*") or (os != "\*juniper\*" and ip = "10.204\*").
- 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, category, IP Address, and Profiler Name. Allows to override the automatic updates by the profiler and retain the details.
  - Download Report: Allows to download and save the report in CSV format.
  - Delete Selected: Allows to delete the selected devices.
  - **Purge Aged Out Devices**: Allows to manually purge devices older than the specified interval in the server configuration. Scheduled purging of the devices happens automatically.

### **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 Added or Edited device attributes are auto updated when the classifier updates its attributes. If you want to avoid updates from classifier, select Override any updates by the profiler and use this profile always for the device.
- Edit all similar devices: Allows to edit all similar devices which have same fingerprint. When similar devices are added, the updated fingerprint is used for profiling.
- Submit a ticket: The Profiler uses Fingerbank database to classify devices. It is possible that some devices are not correctly classified in this process. In such cases, the administrator can use the Copy Fingerprint option to copy the fingerprint and send the relevant information about the wrongly classified device to the Pulse Secure using an E-mail. This information is verified before updating the Custom Fingerprint database.

#### Figure 16: Submit a ticket



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

## 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 suspect MAC address spoofing, , provided MAC spoofing results in a profile change of the device. Profile change would be indicated by the *previous\_os* and *previous\_category* fields.

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

To detect spoof for a specific device, use the following Regexp in role mapping rule: deviceAttr.previous\_os != '' AND (deviceAttr.previous\_os = 'Cisco VoIP' AND deviceAttr.os != 'Cisco VoIP') Use the following Regexp, which is common for all Operating Systems:

deviceAttr.previous os != '' AND (deviceAttr.previous os != deviceAttr.os)

**Note:** This feature works only when the actual device is profiled with information of OS and categories before spoofed device connects and is profiled. Mac spoof suspect may not work when same OS or Category information is identified for original and spoofed device. Mac spoof suspect may not work when two different collectors collect valid information, but there is no classification change because of priority order of the collectors. The Priority of the collectors in order follows, MDM, WMI, SSH, SNMP/TRAP, DHCP, NMAP.

### 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.

### Profile Groups

The devices can be grouped based on group name and rules for easy access and identification. Group names can be used in role mapping rules, resource policies, filtering etc.

- 1. Select the Profiler server under Authentication  $\rightarrow$  Auth. Servers.
- Select Profile Groups tab, select the New Profile Group and enter the Group Name and Rule.: The rules can be written with device attributes and suggested operators can be chosen from the list. To create rules for all values including null, use the format: rule: category ="\*" or category ="".
- 3. **(Optional)** Enable **Needs manual approval** option to approve the devices added to the profile group manually by the administrator. The devices in the group are Unapproved by default.
- 4. (Optional) Email notifications can be enabled to notify when new devices are added to the group.
- 5. Select the interval from the list to purge the older devices in the group automatically.
- 6. Click Save.

**V** 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.

### Figure 17: Profile Groups

	Pulse Policy Secure	
Secu	UTE System Authentication Administrators Users Endpoint Policy Maintenance Wizards	• •
Auth Servers > Profile Groups		
Profile Groups		
Settings Troubleshooting	Browse Fingerprints Profile Groups	
+ New Profile Group		
	* Create new Profile Group	
	Group Name *	
	Rule	
	The rules can be written as a 'query' using profiler attributes. Start typing to get autofiling options. Example: Switches by Cisco can be grouped as: category = **switch** and manufacturer = **cisco**	
	A complex rule using inner altributes: (snmp switch_ip = "10.204.58.??" and manufacturer i= "juniper") or (os i= "juniper" and ip = "10.204")	
	· · · · · · · · · · · · · · · · · · ·	
	Needs manual approval (Devices entering this group will be made unapproved by default )	
	Send email notifications whenever a new device enters this group.	
	Use emails from General Settings  Custom The emails will be sent to following email addresses. Multiple addresses can be separated by a semicolon(;).	
	forexample@domain.com	
	SMTP server configuration is required for sending emails. Currently SMTP Server is configured and enabled. Click here to change the settings.	
	Purge devices older than:	
	6 Months -	
	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.	
	H Save	

### Creating Rules for Profile Groups

To create rules for profile groups, type the expressions in the **Rules** field. The list appears with suggested device attributes and operators as you type the expression.

Create the rule expression using one or combination of the following set of qualified **rule attributes** and the **operators**.

Attribute Name	Rule Attribute	
Category	category	
Manufacturer	manufacturer	
Operating System	OS	
MAC Address	macaddr	
IP Address	ір	
Hostname	hostname	
Profiler Name	profiler_name	
SNMP Attributes		
SSID	snmp.ssid	
Switch IP Address	snmp.switch_ip	
Switch Name	snmp.switch_name	
WMI Attributes		
Classified Category	wmi.classified_category	
Classified OS	wmi.classified_os	
Domain	wmi.domain	
Hostname	wmi.hostname	
Status	wmi.status	
username	wmi.username	

#### Operators

- == (exactly equal)
- != (Not equal to)
- AND
- OR (enabled to add multiple sets of AND rules as shown in UI, which internally is called as 'OR')

#### Examples

- macaddr == "64:87\*" and manufacturer =="VMWare"
- ip =="10.204\*" and manufacturer== "VMWare\*" and (os != "linux" or os
  !="Linux\*")
- wmi.classified\_category == "Windows" or wmi.classified\_os == "Microsoft Windows 10 Pro 10.0.17134" or wmi.domain == "WORKGROUP" or wmi.hostname == " W71-PC" or wmi. status == "up" or wmi.username == "admin"

### Configuring Role-Mapping Rules for Profiled Devices

To configure role-mapping rules:

- 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 18: Device Attributes

✓ Servers		
Specify the servers to use for authentica	ation and authorization	. To create or ma
Authentication:	MacAuthSe	erver 🗘
User Directory/Attribute:	Same as al	bove 🗘
Accounting:	None	•
Device Attributes:	Local Profi	ler 🗘
Device Check Interval:	60	minutes

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

Figure 19: Rule based on attribute

Rule based on:	Device attribute	<b>+</b>	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 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.

Name: windows_rule		
Rule: If device has any or	f the following attribute	e values
Attribute:	os	Attributes
is 🔻	(Select an attribute) antivirus_name antivirus status	If more than one value for this attribute should match, enter one per line. You can use * wildcard
	antivirus_version category	
	custom	
then assign these roles	domain first seen	
Available Roles:	groups	Roles:
Guest	hostname last_seen	Cess
Guest Admin	macaddr manufacturer	
Guest Sponsor	os	
Guest Wired Restricted	os_patch previous category	
Remediation	previous_os	
L.	profiler_name status	
Stop processing rules		

Figure 20: 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	Outdated or Current
	up to date or not	
Category	The category of the device.	Windows, Linux, Android, etc.
	All devices are broadly classified into 30+ different	
	categories.	
Custom	The administrator defined value(s) for the device.	Administaror defined values
Domain	The domain name of the device	Administaror defined values
first_seen	The timestamp of the device discovery	2018-04-04
		06:52:16.993606+00:00
Groups	The list of groups and rules associated to the device	Administaror defined values
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	Windows 7.x, AC OS X, Ruckus,
	of the device.	Wireless AP, etc
os_patch	The patch information of the operating system installed	"Service Pack *"
	on the device	
previous_category	When a device category is changed, the device can be	N/A
	listed using the previous category of the device.	

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

## Agentless Host Checker with Profiler

Profiler allows to authorize users based on the user device attributes without the need to install agents on their machines.

Agentless Host checker allows to configure policies to check device compliance. Each policy consists of a set of rules to qualify the device to be compliant.

The user realms are configured with role mapping rules based on the policies and the users are assigned appropriate role based on device compliance.

The following rule types are supported for the Agentless Host Checker with Profiler on Windows devices:

Agentless Host Checker with Profiler is supported on Windows devices only. The following is the list of supported rule types.

- Antivirus
- Firewall
- Antispyware
- Operating System
- Ports
- Process
- NetBIOS
- Mac address

**O**Note: ESAP package **3.4.5** or higher supports the latest rule type updates.

### Configuring Agentless Host Checker with Profiler

To configure Agentless Host Checker mode, perform the following steps.

- 1. Select Authentication > Endpoint Security > Host Checker.
- 2. Under Policies, click New.
- 3. Enter a name for the policy, select Agentless mode with Profiler and click Continue.

Figure 21: Host Checker Policy Creation for Agentless mode

Endpoint Security > Host Checker > New H	Host Checker Policy	
New Host Checker Policy		
Host Checker		
•		
*Policy Name:	Continue >>	Cancel
Agentless mode with Profiler:	ote: This requires Profiler to be configured. Navigate to Auth \$	Servers for configuring Profiler
* indicates required field		

**Note:** Host checker Polices configured for Agentless Mode are listed and indicated as (Agentless Mode with Profiler), in the policies table under **Authentication > Endpoint Security > Host Checker**.

4. Click on the policy name to associate the rules to the policy. select the rule type under **Rule Settings** and click **Add**.

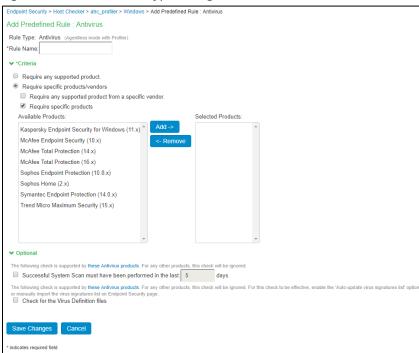
0			
Endpoint Security > Host Checker Pol	icy		
Host Checker Policy			
Policy Name: Agentless Host		(Agentless mode with Pro	filer)
Windows			
- Select Rule Type -	Add Del	lete	
- Select Rule Type - Predefined: Antivirus Predefined: Firewall	page		
Predefined: AntiSpyware Predefined: OS Checks		Rule Type	
Custom: Ports Custom: Process			
Custom: NetBIOS Custom: MAC Address			
Require:	-		
<ul> <li>Any of the above rules</li> </ul>			
Custom			

#### Figure 22: Host Checker Rule Types for Agentless mode

a. If you select **Predefined: Antivirus**, the rule requires endpoint to have specific antivirus installed and running.

Enter the Rule Name, select required Criteria, Optional rules and click Save Changes.

#### Figure 23: Antivirus Rule Type for Agentless mode



b. If you select **Predefined: Firewall,** the rule requires the endpoint to have a specific firewall installed and running.

Enter the Rule Name, select required Criteria and click Save Changes.

<pre>Endpoint Security &gt; Host Checker &gt; ahc_profiler &gt; Windows &gt; Add Predefined Rule : Firewall Add Predefined Rule : Firewall Rule Type: Firewall (Agentless mode with Profiler) *Rule Name.</pre>	• •	
Rule Type: Firewall (Agentless mode with Profiler)   *Rule Name:   * *Criteria • Require any supported product. • Require specific products/vendors • Require specific product from a specific vendor. • Require specific products Available Products: • Available Products: • Add -> • Career of the product of the pr	Endpoint Security > Host Checker > ahc_profiler > Windows >	Add Predefined Rule : Firewall
*Rule Name: ✓ • Criteria Require any supported product. Require specific products/vendors Require specific product from a specific vendor. Require specific product s Available Products: Kaspersky Endpoint Security for Windows (11.x) McAfee Endpoint Security (10.x) McAfee Total Protection (14.x) McAfee Total Protection (14.0.x) Symantec Endpoint Protection (14.0.x) Symantec Endpoint Protection (14.0.x)	Add Predefined Rule : Firewall	
<ul> <li>Require any supported product.</li> <li>Require specific products/vendors <ul> <li>Require specific product from a specific vendor.</li> <li>Require specific products</li> </ul> </li> <li>Stere and the specific product from a specific vendor.</li> <li>Require specific products: <ul> <li>Add -&gt;</li> <li>Carcel</li> </ul> </li> </ul> <li>Stere and the specific product from the specific vendor.</li> <li>Respecific products: <ul> <li>Add -&gt;</li> <li>Carcel</li> </ul> </li>	Rule Type: Firewall (Agentless mode with Profiler)	
<ul> <li>Require any supported product.</li> <li>Require specific products/vendors</li> <li>Require specific product from a specific vendor.</li> <li>Require specific products</li> </ul> Available Products: <ul> <li>Kaspersky Endpoint Security for Windows (11.x)</li> <li>McAfee Endpoint Security (10.x)</li> <li>McAfee Total Protection (14.x)</li> <li>McAfee Total Protection (14.0.x)</li> <li>Symantec Endpoint Protection (14.0.x)</li> <li>Store Endpoint Protection (14.0.x)</li> </ul>	*Rule Name:	
<ul> <li>Require specific products/vendors</li> <li>Require specific product from a specific vendor.</li> <li>Require specific products</li> <li>Available Products:</li> <li>Kaspersky Endpoint Security for Windows (11.x)</li> <li>McAfee Endpoint Security (10.x)</li> <li>McAfee Total Protection (14.x)</li> <li>McAfee Total Protection (16.0.x)</li> <li>Symantec Endpoint Protection (14.0.x)</li> <li>Swartec Endpoint Protection (14.0.x)</li> <li>Ster Changes</li> </ul>	✓ *Criteria	
<ul> <li>Require specific products/vendors</li> <li>Require specific product from a specific vendor.</li> <li>Require specific products</li> <li>Available Products:</li> <li>Kaspersky Endpoint Security for Windows (11.x)</li> <li>McAfee Endpoint Security (10.x)</li> <li>McAfee Total Protection (14.x)</li> <li>McAfee Total Protection (16.0.x)</li> <li>Symantec Endpoint Protection (14.0.x)</li> <li>Swartec Endpoint Protection (14.0.x)</li> <li>Ster Changes</li> </ul>	Require any supported product.	
<ul> <li>Require specific products</li> <li>Available Products:</li> <li>Kaspersky Endpoint Security for Windows (11.x) McAfee Endpoint Security (10.x) McAfee Total Protection (14.x) McAfee Total Protection (16.0.x) Symantec Endpoint Protection (14.0.x)</li> <li>Swantec Endpoint Protection (14.0.x)</li> </ul>		
Available Products: Kaspersky Endpoint Security for Windows (11.x) McAfee Endpoint Security (10.x) McAfee Total Protection (14.x) Symantec Endpoint Protection (14.0.x) Swartec Endpoint Protection (14.0.x)	Require any supported product from a specific version	endor.
Kaspersky Endpoint Security for Windows (11.x)       Add ->         McAfee Endpoint Security (10.x)       <-Remove	Require specific products	
Respense Changes       Cancel	Available Products:	
McAfee Total Protection (14.x) McAfee Total Protection (16.0.x) Symantec Endpoint Protection (14.0.x)	Kaspersky Endpoint Security for Windows (11.x)	Add ->
McAfee Total Protection (16.0.x) Symantec Endpoint Protection (14.0.x)	McAfee Endpoint Security (10.x)	<- Remove
Symantec Endpoint Protection (14.0.x)	McAfee Total Protection (14.x)	
Save Changes Cancel	McAfee Total Protection (16.0.x)	
	Symantec Endpoint Protection (14.0.x)	
	*	<b>*</b>
* indicates required field	Save Changes Cancel	
	* indicates required field	

#### Figure 24: Firewall Rule Type for Agentless mode

c. If you select **Predefined: AntiSpyware,** the rule checks for installed AntiSpyware on endpoints. Enter the **Rule Name**, select required **Criteria** and click **Save Changes**.

Endpoint Security > Host Checker > ahc_profiler > Windows > Add Predefined Rule : AntiSpyware
Add Predefined Rule : AntiSpyware
Rule Type: AntiSpyware (Agentless mode with Profiler)
*Rule Name:
✓ *Criteria
Note: Anti-Virus products that provide both anti-virus and anti-spyware functionality are also listed in the Anti-spyware products II
Require specific products/vendors
Require any supported product from a specific vendor.
Require specific products
Available Products: Selected Products:
Kaspersky Endpoint Security for Windows (11.x) Add ->
McAfee Endpoint Security (10.x) <- Remove
McAfee Total Protection (14.x)
McAfee Total Protection (16.x)
Sophos Endpoint Protection (10.8.x)
Sophos Home (2.x)
Symantec Endpoint Protection (14.0.x)
Trend Micro Maximum Security (15.x)
• • • • •
Save Changes Cancel
* indicates required field

#### Figure 25: AntiSpyware Rule Type for Agentless mode

d. If you select **Predefined: OS Checks,** the rule checks the operating systems and minimum service pack versions listed.

Enter the Rule Name, select required Criteria and click Save Changes.

Figure	26: OS	Checks	Rule <sup>-</sup>	Type fo	r Agen <sup>.</sup>	tless	mode

Configuration > Host Checker Policy > Add	Predefined Rule : OS Che	ecks
Add Predefined Rule : OS Check	s	
Rule Type: OS Checks (Agentless mode	e with Profiler)	
*Rule Name:		
✓ *Criteria		
Windows 10		
Minimum Service Pack/Version:	Ignore •	
Windows 10-64-Bit	5	
Minimum Service Pack/Version:	Ignore •	
Windows 2008	5	
Minimum Service Pack/Version:	Ignore •	
Windows 2008-R2-64-Bit	0	
Minimum Service Pack/Version:	Ignore •	
Windows 2012-64-Bit		
Minimum Service Pack/Version:	Ignore •	
Windows 2012-R2-64-Bit		
Minimum Service Pack/Version:	Ignore •	
Windows 2016-64-Bit		
Minimum Service Pack/Version:	Ignore •	
Windows 7		
Minimum Service Pack/Version:	Ignore •	
Windows 7-64-Bit		
Minimum Service Pack/Version:	Ignore •	
Windows 8		
Minimum Service Pack/Version:	Ignore •	
Windows 8-64-Bit		
Minimum Service Pack/Version:	Ignore •	
Windows 8.1		
Minimum Service Pack/Version:	Ignore •	
Windows 8.1-64-Bit		
Minimum Service Pack/Version:	Ignore •	
Save Changes Cancel		
* indicates required field		

e. If you select Custom Rule: Ports, the rule controls the network connections that a client can generate during a session. This rule type checks. if restricted ports are open or required ports are not open, then endpoint gets limited connectivity to the network.
 Enter the Rule Name, enter port numbers to allow or deny under Criteria and click Save

Changes.

#### Figure 27: Ports Rule Type for Agentless mode

Configuration > Host Checker Policy > Add	Custom Rule : Ports
Add Custom Rule : Ports	
Rule Type: Ports (Agentless mode with Pr *Rule Name:	ofiler)
✓ *Criteria	
*Port List: Required  Deny	Enter port numbers seperated by comma or port range Example: 1,2,3,4,5-20
Save Changes Cancel	
* indicates required field	

f. If you select **Custom Rule: Process,** the rule controls the software that a client may run during a session.

Enter the Rule Name, enter Process Name to allow or deny under Criteria and click Save

#### Changes.

#### Figure 28: Process Rule Type for Agentless mode

Configuration > Host Checker Policy > Add Custom Rule : Process
Add Custom Rule : Process
Rule Type:         Process         (Agentless mode with Profiler)           *Rule Name:
✓ *Criteria
*Process Name:
Required      Deny
Save Changes Cancel
* indicates required field

g. If you select Custom Rule: NetBIOS, the rule checks the NetBIOS name of the client machine.
 Enter the Rule Name, enter NetBIOS Names to allow or deny under Criteria and click Save Changes.

#### Figure 29: NetBIOS Rule Type for Agentless mode

Configuration > Host Checker Policy > Add Custom Rule : N	etBIOS
Add Custom Rule : NetBIOS	
Rule Type: NetBIOS (Agentless mode with Profiler)	
*Rule Name:	
✓ *Criteria	
*NetBIOS Names:	One per line Example: WINDOWS-PC,WIN*-PC,*-PC,WINDOWS*
	1
Required Openy	
Save Changes Cancel	
* indicates required field	

h. If you select **Custom Rule: MAC Address,** the rule checks the MAC Address of the client machine.

Enter the **Rule Name**, enter MAC Addresses to allow or deny under **Criteria** and click **Save Changes**.

#### Figure 30: MAC Address Rule Type for Agentless mode

Configuration > Host Checker Policy > Add Custom Rule : M	AC Address
Add Custom Rule : MAC Address	
Rule Type: MAC Address (Agentless mode with Profiler)	
Rule Name:	
✓ *Criteria	
*MAC Addresses:	Example
	00:11:85:bb:8c 00:ff:*:*:*:*
	One per line
Required Openy	
Save Changes Cancel	
indicates required field	

5. On adding the Rule Types, select the required option for rules, **Remediation** and **Dashboard Reporting** options and click **Save Changes**.

 Enforce the policies for Agentless Mode with Profiler and implement the policy at the realm level. Navigate to Users > User Realms > Select Realm > Authentication Policy > Host Checker. Select Agentless mode with Profiler. Select the applicable policies from the list and click Save Changes.

**Note**: Pre-authentication compliance check is not supported for agentless mode with Profiler. The **Require and Enforce** option is disabled for agentless policies.

Figure 31: Policy enforcement for Agentless mode with Profiler on User Realm

User Realms > Guest >	<ul> <li>Authentication Policy &gt; H</li> </ul>	Host Checker			
Host Checker					
General	Authentication Policy	Role Mapping			
Source IP Browser	r Certificate Passwo	ord Host Checker Limits RADIUS Request Policies			
Agentless mode	with Profiler Note: This re	equires Profiler to be configured. Navigate to Auth Servers for configuring Profiler.			
Allow users whose w	vorkstations meet the rea	equirements specified by required host-checker policies. If no policies are selected then all users will be allowed. "Evaluate Policies" will evaluate the	ne policy by the profiler.		
10 • rec	ords per page	\$	Search:		
Evaluate Policies	Require and Enforce	Available Policies			
		All			
		test_ahc (Agentless mode with Profiler)			
$\leftarrow \text{Previous}  1  \text{Next} \rightarrow$					
To manage Host Checker policies, see the Host Checker configuration page.					
Save Changes					

7. Allow access to devices that comply with Agentless Host Checker policies.

Navigate to Users > User Roles > Select Role > General > Restrictions > Host Checker add or remove the policies from the list and click Save Changes.

Figure 32: Policy enforcement for Agentless mode with Profiler on User Role

User Roles > Gu	uest > General > F	Restrictions > Host	Checker		
Host Checke	er				
General	Agent	Agentless			
Overview F	Restrictions Sea	ssion Options UI	Options		
Source IP	Browser Certifi	cate Host Check	er		
	sers (Host Check s whose worksta		quirements s	pecified by these Host C	Checker policies:
Available P	olicies:			Selected Policies:	
test_ahc (	Agentless mode	with Profiler)	Add ->		•
test_hc		Ŧ	Remove		Ŧ
Allow a	access to the rol	e if any ONE of th	ie selected p	olicies is passed.	
To manage H	lost Checker policie	es, see the Host Che	cker configurat	ion page.	
Save Chang	jes 🛛				

## 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, profiler\_name, groups 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
- To avoid the Operating and Category changes to the devices received by the classifier on importing the CSV file, include or edit the column **override** and set the value to TRUE for each device in the CSV file.
- 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	<ul> <li>Verify if ports are receiving the DHCP packets.</li> </ul>
	<ul> <li>Detect a device when connected to network during the diagnostic run.</li> </ul>
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	<ul> <li>Verify if trap is collected or not for a switch event.</li> </ul>
	<ul> <li>Detect a device when connected to network during the diagnostic run.</li> </ul>
SMTP Test	<ul> <li>Troubleshoot any problem in configuration/reachability of SMTP server.</li> </ul>
	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 33: Troubleshooting

									Pulse Policy Secure	
Se Pulse Se	ecure	System	Authentication	Administrators	Users	Endpoint Policy	Maintenance	Wizards		••
Auth Servers > Profiler Troubleshoot	ng									
Profiler Troubleshooting										
Settings Troubleshooti	ng Browse	Fingerprints	Profile Groups							
Select a diagnostic test							Run diagnostics			
DHCP Test										
Switch Diagnostics										
SNMP(HOST) Test										
NMAP Scan Test										
TRAP Test										
SMTP Test										

### **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 34: 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
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
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

r		1
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

## **Profiler Deployment Cases**

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

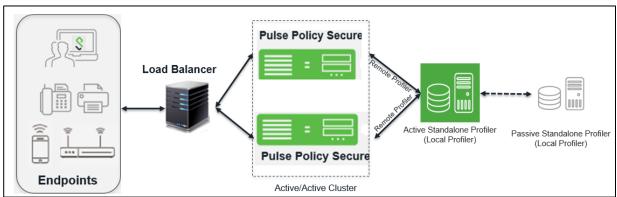
### Standalone Profiler

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.

 $^{\prime\prime}$  Note: The Profiler can be deployed in Active/Passive clusters or without clustering.



#### Figure 35: 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:

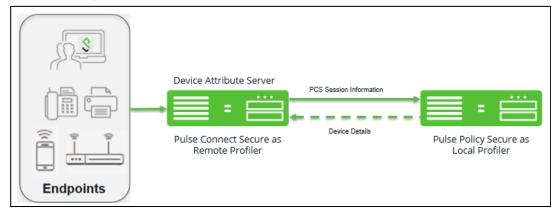
- Information such as hostname and IP address, device IP address and MAC address, session identifier, useragent are retrieved by the session and sent to the Profiler.
- The Profiler returns Device OS, Device Manufacturer, Device Category and Session Identifier to PPS/PCS.
- The Profiler updates the PCS/PPS 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 36: Example of a Remote Profiler

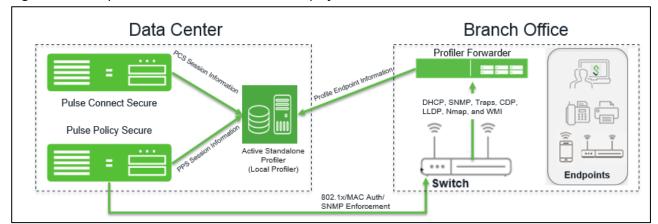


### Profiling devices in branch offices

### 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 37: 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.

### Using Linked Profiler (With PPS Functionality)

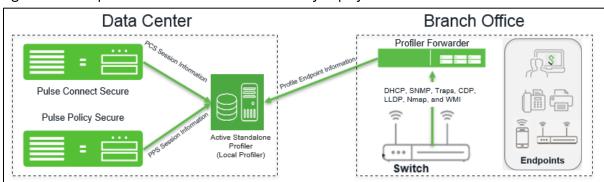


Figure 38: Example of a Profiler with PPS functionality deployed across WAN

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.