



Pulse Policy Secure Profiler

Administration Guide

Product Release	9.0R3
Document Version	1.0
Published	December 2018

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 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

Contents

ABOUT THIS DOCUMENT	5
DOCUMENT CONVENTIONS	5
Notes, cautions, and warnings	5
Text formatting conventions	5
Command syntax conventions	5
SELF-HELP ONLINE TOOLS AND RESOURCES	6
REQUESTING TECHNICAL SUPPORT	6
OPENING A CASE WITH PSGSC	6
INTRODUCTION	7
DEPLOYMENT AND LICENSE REQUIREMENTS	8
DISCOVERING ENDPOINT DEVICES	9
PASSIVE COLLECTORS	9
DHCP collector	9
User Agent Collector	9
Network Infrastructure Device Collector	9
SNMP Trap	10
ACTIVE COLLECTORS	10
Nmap Collector	10
WMI Collector	10
SSH Collector	10
MDM Collector	10
CONFIGURING THE LOCAL PROFILER AUTHENTICATION SERVER	10
PROFILER REPORTS	14
DASHBOARD	14
PROFILER REPORT SCHEDULING	15
DEVICE DISCOVERY REPORT TABLE	17
ENDPOINT INFORMATION	17
ENDPOINT FILTERS	18
REPORT OPERATIONS	18
DEVICE OPERATIONS	18
ACCESS CONTROL	20
SPOOF DETECTION	20
DEVICE SPONSORING	20
PROFILE GROUPS	20
CONFIGURING ROLE-MAPPING RULES FOR PROFILED DEVICES	21
AGENTLESS HOST CHECKER WITH PROFILER	24
CONFIGURING AGENTLESS HOST CHECKER WITH PROFILER	24
IMPORT/EXPORT PROFILER DATABASE	30
IMPORT / EXPORT PROFILER DEVICE DATA IN BINARY FORMAT	30
IMPORT / EXPORT PROFILER DEVICE DATA IN CSV FORMAT	30
IMPORT/ EXPORT OF PROFILE MODIFICATIONS DATABASE IN BINARY FORMAT	31
TROUBLESHOOTING	32

TESTS32

PROFILER LOGS.....32

PROFILER DEPLOYMENT CASES..... 35

STANDALONE PROFILER35

REMOTE PROFILER35

PROFILING DEVICES IN BRANCH OFFICES36

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.
<i>italic text</i>	Identifies emphasis. Identifies variables. Identifies document titles.
<code>Courier font</code>	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.
<i>italic text</i>	Identifies a variable.
Value	A fixed value provided as input to a command option is printed in plain text, for example, <code>--show WWN</code> .
[]	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

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.

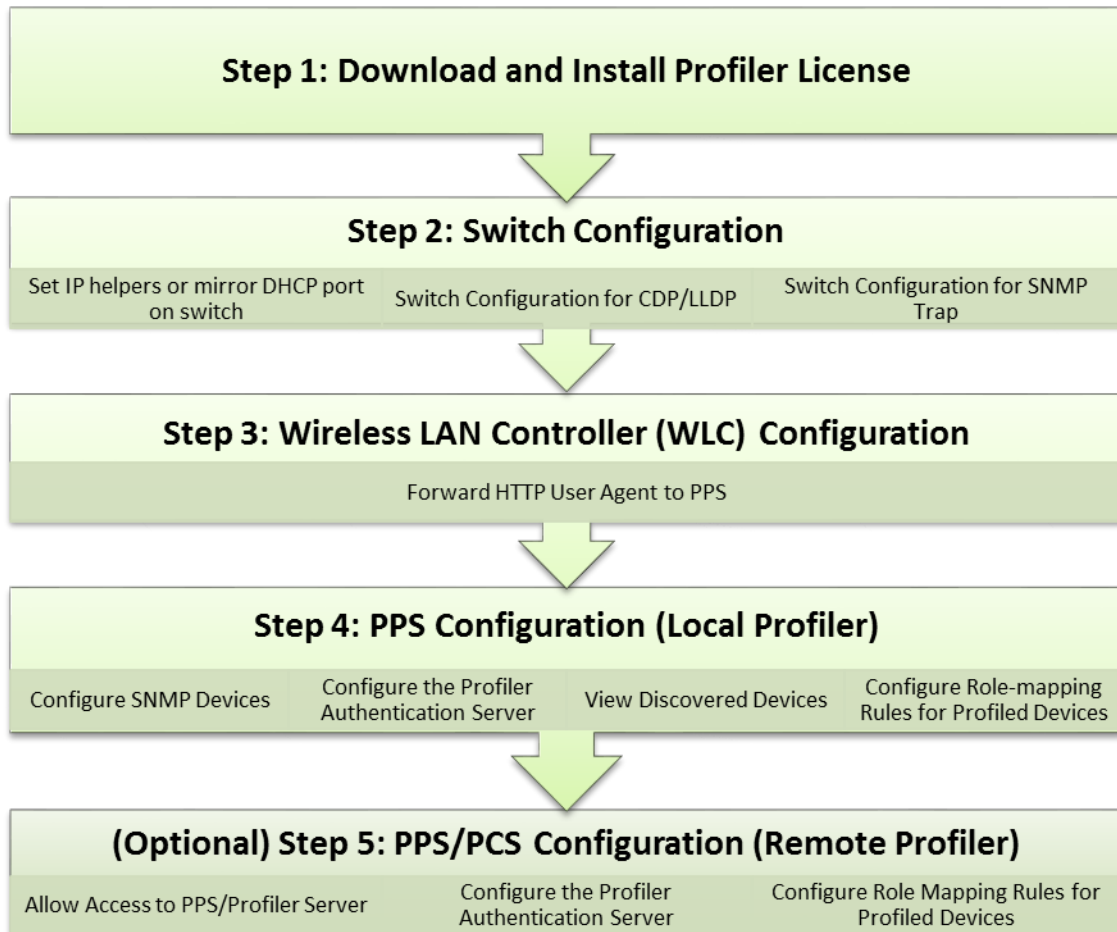
The Pulse Secure Profiler dynamically identifies and classifies both managed and unmanaged endpoint devices, enabling control of access to networks and resources based on the type of the device.

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](#).



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

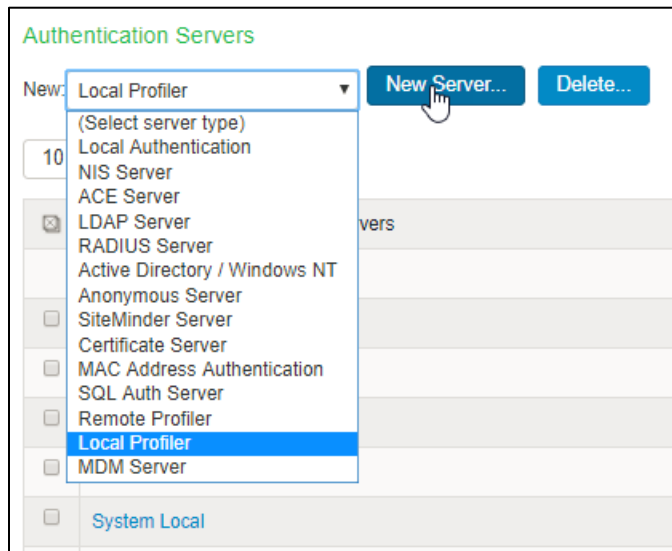
Ensure the following tasks are performed before proceeding with the Profiler Authentication server configuration.

- 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:

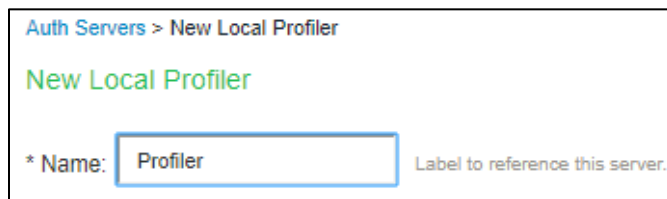
1. Select **Authentication > Auth. Servers**.
2. Select **Local Profiler** from the server type drop-down list and click **New Server**.

Figure 1: Creating a Local Profiler Authentication Server



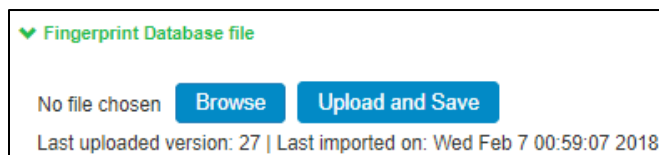
3. Enter a name for the Authentication server.

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](#).
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 5: Device Sponsoring

Device Sponsoring

Select device categories that will trigger an email to the admin for approval. Create a role-mapping rule based on "status" attribute to assign the device to the respective role before and after approval.
 Note: Devices can be approved or unapproved from the [Device Discovery Report](#)

☐ BSD
☐ Linux
☐ Other OS
☐ Routers and APs
☐ Video Conferencing

☐ Datacenter appliance
☐ Macintosh
☐ Physical Security
☐ Smartphones/PDAs/Tablets
☐ VoIP Phones/Adapters

☐ Gaming Consoles
☐ Medical Device
☐ Point of Sale devices
☐ Storage Devices
☐ Windows

☐ Home Audio/Video Equipment
☐ Monitoring Devices
☐ Printers/Scanners
☐ Switches

☐ Internet of Things (IoT)
☐ Network Boot Agents
☐ Projectors
☐ Thin Clients

Set approver's email address(es) to send notifications. Emails will be sent whenever a new endpoint is classified under an 'unapproved' category.

☐ Use emails from [General Settings](#)
☒ Custom
 The emails will be sent to following email addresses. Multiple addresses can be separated by a semicolon(;).
 [Test Settings](#)

☒ SMTP server configuration is required for sending emails. Currently SMTP Server is configured and enabled. [Click here](#) to change the settings.

* URL for Device Discovery Report.
 It will appear in the notification email as a link for quick access to the devices that need approval. Profiler hostname or IP address is needed to complete the URL.
https://10.96.102.2/dana-admin/reporting/report_device_discovery.cgi

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

Figure 6: Adding One or More Subnets

Endpoints to scan using NMAP/WMI/SSH

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

On-Demand Scan: Trigger one time scan, which scans the subnets selected in above table with selected collectors.
 Note that the regular profiler classification for these collectors will be halted and resumed after scan.

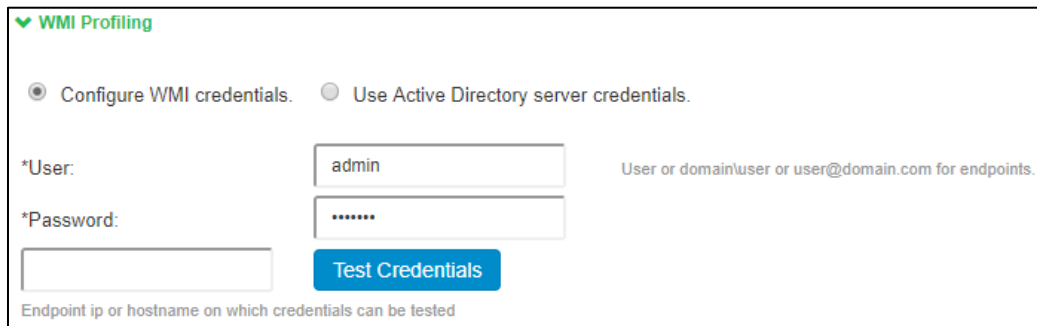
[Delete](#)
[↑](#)
[↓](#)
[Start On-Demand Scan](#)

<input type="checkbox"/>	Subnet	Include/Exclude	Collector	
<input type="checkbox"/>	<input type="text"/>	<input checked="" type="radio"/> Include <input type="radio"/> Exclude	<input checked="" type="checkbox"/> NMAP <input type="checkbox"/> WMI <input type="checkbox"/> SSH	Add
<input type="checkbox"/>				

8. (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.

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



WMI Profiling

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

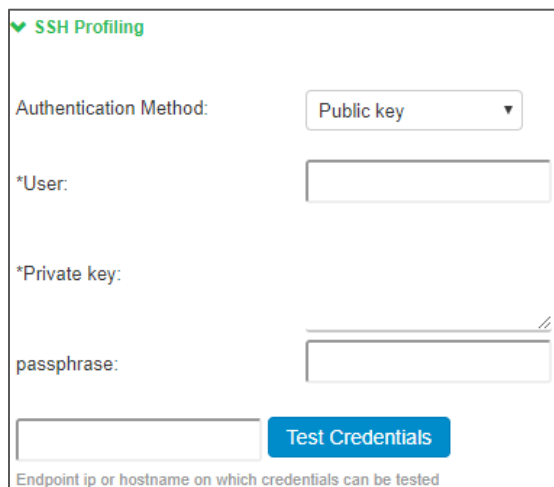
*User: User or domain\user or user@domain.com for endpoints.

*Password:

Endpoint ip or hostname on which credentials can be tested

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



SSH Profiling

Authentication Method:

*User:

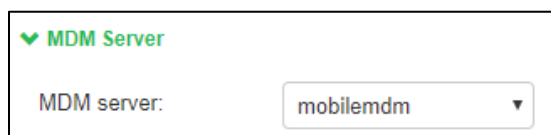
*Private key:

passphrase:

Endpoint ip or hostname on which credentials can be tested

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

Figure 9: MDM Server



MDM Server

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](#).

The devices can be grouped based on group name and rules using device attributes. For more information see, [Profile Groups](#).

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 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



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 → Configuration → Notification → 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 11: Report Scheduling

The screenshot displays the Pulse Secure Profiler Administration interface. The top navigation bar includes the Pulse Secure logo and a menu with items: System, Authentication, Administrators, Users, Endpoint Policy, Maintenance, and Wizards. The breadcrumb trail shows Configuration > Notification > Email Notifications. The main content area is titled 'Email Notifications' and features a tabbed interface with tabs for Licensing, Pulse One, Security, Certificates, DMI Agent, Sensors, Client Types, Guest Access, and Notification (which is currently selected). Under the Notification tab, there are two sub-tabs: General and Email Notification (which is selected). The 'Email Notification' sub-tab contains the 'Profiler Reports Scheduling' section. This section includes instructions to set a schedule and email address for receiving Detailed Profiler reports. It has two radio buttons: 'Use emails from General Settings' (selected) and 'Custom'. Below the radio buttons is a text input field containing 'surendra@pulsesecure.net' and a 'Test Settings' button. A status message indicates that SMTP server configuration is required and currently enabled, with a link to change settings. The 'Email Schedule' is set to 'Daily' (with a dropdown arrow) and 'Generate Full Report' is unchecked. A note explains that the 'Daily' schedule is at 7AM and that the 'Generate Full Report' checkbox is for full reports generated every time. At the bottom of the section are 'Save Changes' and 'Reset' buttons. A footnote at the bottom left states '* Indicates required field'.

Pulse Secure

System Authentication Administrators Users Endpoint Policy Maintenance Wizards

Pulse Policy Secure

Configuration > Notification > Email Notifications

Email Notifications

Licensing Pulse One Security Certificates DMI Agent Sensors Client Types Guest Access Notification

General Email Notification

▼ Profiler Reports Scheduling

Set appropriate schedule and emails to receive Detailed Profiler reports (PDF format), in your inbox.

☒ Use emails from [General Settings](#) ☐ Custom

The emails will be sent to following email addresses.

surendra@pulsesecure.net Test Settings

✔ SMTP server configuration is required for sending emails. Currently SMTP Server is configured and enabled. [Click here](#) to change the settings.

Email Schedule: Daily ☐ Generate Full Report

Daily - 7AM.

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 12: Device Discovery Report Table

Profiler	MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	Session User	First Seen	Last Updated	Profiler	Groups
	00:21:cc:bf:52:f9	10.204.90.23		Electronics International				Wed, 12 Sep 2018 14:38:28	Wed, 12 Sep 2018 15:06:55	forwarder	
	ac:1f6b:61:4d:bc	10.96.74.73		Super Micro Computer, Inc.	PXE	Network Boot Agents		Wed, 12 Sep 2018 12:23:07	Wed, 12 Sep 2018 15:07:05	profiler	
	c4:0b:cb:db:8e:83		Redmi3S-AbraAhmed	Xiaomi Communications Co Ltd	Android	Smartphones/PDAs/Tablets		Wed, 12 Sep 2018 12:17:41	Wed, 12 Sep 2018 12:17:56	profiler	
	98:9c:57:a5:a7:1a	10.209.123.141	Honor_View10-daa6a7b585a5	HUAWEI TECHNOLOGIES CO.,LTD	Android	Smartphones/PDAs/Tablets		Wed, 12 Sep 2018 11:57:17	Wed, 12 Sep 2018 15:07:04	profiler	
	ac:1f6b:25:96:7c	10.204.90.49		Super Micro Computer, Inc.	PXE	Network Boot Agents		Wed, 12 Sep 2018 11:30:57	Wed, 12 Sep 2018 15:07:04	profiler	
	3c:a9:f4:b0:e1:7c	10.204.90.87	RADISYS-PC7	Intel Corporate	Windows	Windows		Wed, 12 Sep 2018 10:52:26	Wed, 12 Sep 2018 15:07:04	profiler	
	80:ad:16:c6:95:92	10.204.90.47	RedmiNote5pro-Redmi	Xiaomi Communications Co Ltd	Android	Smartphones/PDAs/Tablets		Wed, 12 Sep 2018 10:43:10	Wed, 12 Sep 2018 15:07:04	profiler	
	ac:1f6b:62:28:bb			Super Micro Computer, Inc.	Linux	Linux		Wed, 12 Sep 2018 10:20:25	Wed, 12 Sep 2018 10:24:18	profiler	
	ac:1f6b:61:4d:ee			Super Micro Computer, Inc.	PXE	Network Boot Agents		Wed, 12 Sep 2018 10:12:14	Wed, 12 Sep 2018 10:12:50	profiler	
	ac:1f6b:25:99:07			Super Micro Computer, Inc.	PXE	Network Boot Agents		Wed, 12 Sep 2018 10:11:36	Wed, 12 Sep 2018 10:11:44	profiler	

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 13: History based on IP Address

00:50:56:83:b1:49

10.204.90.45

VMware, Inc.

Fri, 07 Sep 2018 07:07:45

Fri, 07 Sep 2018 07:57:45

profiler

Details

History

Showing last 10

IP Addresses

for the selected device

Profiler Details	Source	Change Detected	Hostname	IP Address
profiler	snmp	Fri, 07 Sep 2018 07:07:45		10.204.90.45

Endpoint Filters

A list of filters is available for quick analysis of discovered devices. The filters 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.

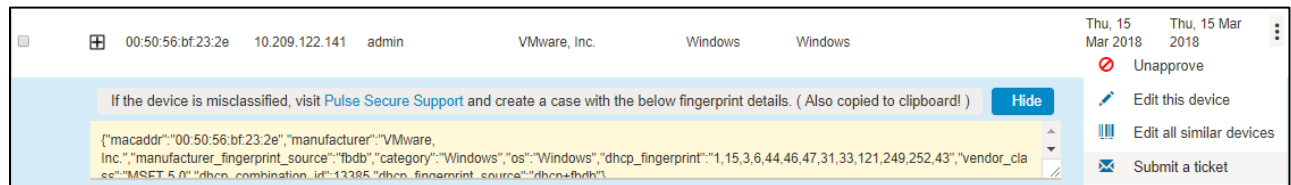
- **Records per page:** Allows to customize the number of records displayed in the page.
- **Head row:** Lists the main attributes for the devices such as IP Address, MAC Address etc. Click the column head to sort the table with respect to the column. Double click to sort in reverse order.
- **Search:** 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 unapprove a specific device. See [Device Sponsoring](#) for more information.
- **Edit:** Allows to edit **Manufacturer**, **Category** and **Operating System** fields. Manually Added or Edited device attributes are auto updated when the classifier updates its attributes. If you want to avoid updates from classifier, select **Override any updates by the profiler and use this profile always for the device**.

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



- **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 might not work when same OS or Category information is identified for original and spoofed device.

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 → Auth. Servers**.
2. Select **Profile Groups** tab, select the **New Profile Group** and enter the Group Name and Rule.: The rules can be written with device attributes and suggested operators can be chosen from the list. As an optional step, emails also can be configured which results in notifications for any group related changes.
To create rules for all values including null, use the format: rule: category ="" or category ="".
3. Click **Save**.


 **Note:** Updating the profile groups for existing devices may take time if a rule covers more devices. Navigating away from the page cancels the update for the existing devices. But, the group names are updated when the device receive updates during regular profiling.

Figure 14: Profile Groups

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 15: 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 16: Rule based on attribute

Rule based on: Device attribute Update

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

7. Enter a name for the rule (if creating a new one).
8. Create the new role mapping 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 17: Creating New Role Mapping Rule

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

Attribute: (Select an attribute) Attributes...

is (Select an attribute)

antivirus_name
antivirus_status
antivirus_version
category
custom
first_seen
groups
hostname
last_seen
macaddr
manufacturer
os
os_patch
previous_category
previous_os
profiler_name
status
tcp_open_ports
udp_open_ports

then assign these roles

Available Roles:

ExternalPeople
Guest
Guest Admin
Guest Sponsor
Guest Wired
...
☐ Stop processing rules

Roles:

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

Save Changes Save + New

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.	Administrator 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	Administrator 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 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 administrator 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

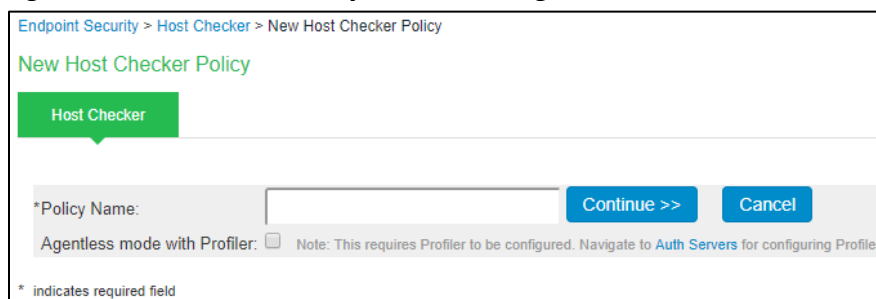
 **Note: Agentless Host Checker is supported on ESAP package 3.3.3.**

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**.

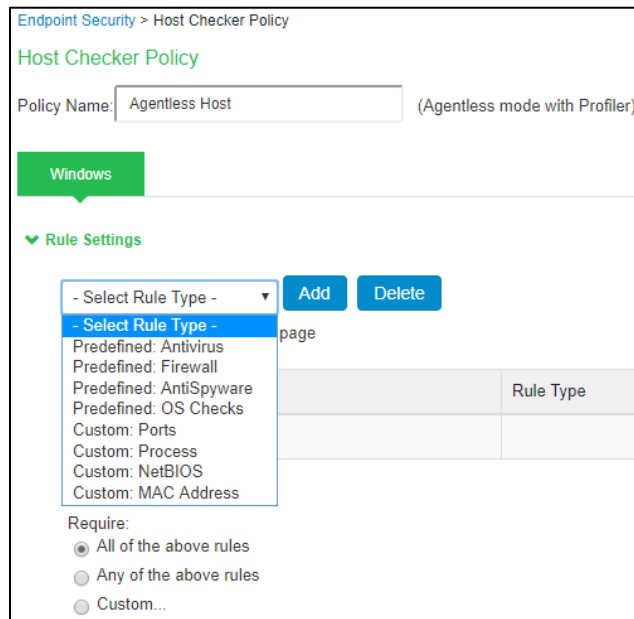
Figure 18: Host Checker Policy Creation for Agentless mode



 **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**.

Figure 19: Host Checker Rule Types for Agentless mode



Endpoint Security > Host Checker Policy

Host Checker Policy

Policy Name: (Agentless mode with Profiler)

Windows

▼ Rule Settings

- Select Rule Type -

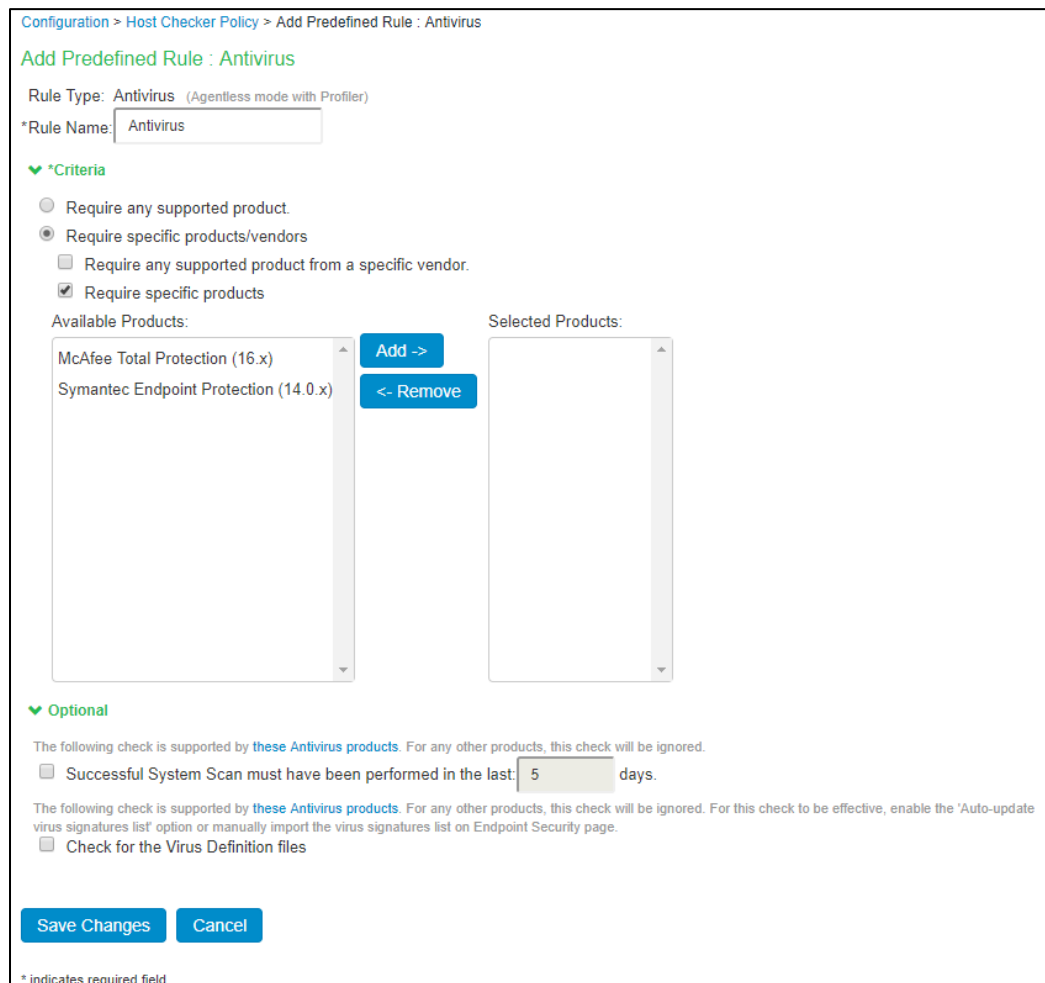
Predefined: Antivirus
Predefined: Firewall
Predefined: AntiSpyware
Predefined: OS Checks
Custom: Ports
Custom: Process
Custom: NetBIOS
Custom: MAC Address

Require:

☒ All of the above rules
☐ Any of the above rules
☐ Custom...

- 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 20: Antivirus Rule Type for Agentless mode



Configuration > Host Checker Policy > Add Predefined Rule : Antivirus

Add Predefined Rule : Antivirus

Rule Type: Antivirus (Agentless mode with Profiler)

*Rule Name:

▼ *Criteria

☐ Require any supported product.
☒ Require specific products/vendors
☐ Require any supported product from a specific vendor.
☒ Require specific products

Available Products:

McAfee Total Protection (16.x)
Symantec Endpoint Protection (14.0.x)

Selected Products:

▼ Optional

The following check is supported by [these Antivirus products](#). For any other products, this check will be ignored.

☐ Successful System Scan must have been performed in the last days.

The following check is supported by [these Antivirus products](#). For any other products, this check will be ignored. For this check to be effective, enable the 'Auto-update virus signatures list' option or manually import the virus signatures list on Endpoint Security page.

☐ Check for the Virus Definition files

* indicates required field

- 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**.

Figure 21: Firewall Rule Type for Agentless mode

The screenshot shows the 'Add Predefined Rule : Firewall' configuration window. The breadcrumb trail is 'Configuration > Host Checker Policy > Add Predefined Rule : Firewall'. The title is 'Add Predefined Rule : Firewall'. The 'Rule Type' is 'Firewall (Agentless mode with Profiler)'. There is a required field for '*Rule Name:'. Under the '*Criteria' section, the following options are listed:

- ☐ Require any supported product.
- ☒ Require specific products/vendors
 - ☐ Require any supported product from a specific vendor.
 - ☒ Require specific products

 Below the criteria, there are two lists: 'Available Products' and 'Selected Products'. The 'Available Products' list contains:

- McAfee Total Protection (16.0.x)
- Symantec Endpoint Protection (14.0.x)

 Between the lists are 'Add ->' and '<- Remove' buttons. At the bottom are 'Save Changes' and 'Cancel' buttons. A footnote at the bottom left states '* indicates required field'.

- 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**.

Figure 22: AntiSpyware Rule Type for Agentless mode

The screenshot shows the 'Add Predefined Rule : AntiSpyware' configuration window. The breadcrumb trail is 'Configuration > Host Checker Policy > Add Predefined Rule : AntiSpyware'. The title is 'Add Predefined Rule : AntiSpyware'. The 'Rule Type' is 'AntiSpyware (Agentless mode with Profiler)'. There is a required field for '*Rule Name:'. Under the '*Criteria' section, the following options are listed:

- ☐ Require any supported product.
- ☒ Require specific products/vendors
 - ☐ Require any supported product from a specific vendor.
 - ☒ Require specific products

 Below the criteria, there are two lists: 'Available Products' and 'Selected Products'. The 'Available Products' list contains:

- McAfee Total Protection (16.x)
- Symantec Endpoint Protection (14.0.x)

 Between the lists are 'Add ->' and '<- Remove' buttons. At the bottom are 'Save Changes' and 'Cancel' buttons. A footnote at the bottom left states '* indicates required field'.

- 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 23: OS Checks Rule Type for Agentless mode

Configuration > Host Checker Policy > Add Predefined Rule : OS Checks

Add Predefined Rule : OS Checks

Rule Type: OS Checks (Agentless mode with Profiler)

*Rule Name:

▼ *Criteria

- ☐ Windows 10
Minimum Service Pack/Version:
- ☐ Windows 10-64-Bit
Minimum Service Pack/Version:
- ☐ Windows 2008
Minimum Service Pack/Version:
- ☐ Windows 2008-R2-64-Bit
Minimum Service Pack/Version:
- ☐ Windows 2012-64-Bit
Minimum Service Pack/Version:
- ☐ Windows 2012-R2-64-Bit
Minimum Service Pack/Version:
- ☐ Windows 2016-64-Bit
Minimum Service Pack/Version:
- ☐ Windows 7
Minimum Service Pack/Version:
- ☐ Windows 7-64-Bit
Minimum Service Pack/Version:
- ☐ Windows 8
Minimum Service Pack/Version:
- ☐ Windows 8-64-Bit
Minimum Service Pack/Version:
- ☐ Windows 8.1
Minimum Service Pack/Version:
- ☐ Windows 8.1-64-Bit
Minimum Service Pack/Version:

* 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 24: Ports Rule Type for Agentless mode

Configuration > Host Checker Policy > Add Custom Rule : Ports

Add Custom Rule : Ports

Rule Type: Ports (Agentless mode with Profiler)

*Rule Name:

▼ *Criteria

*Port List: Enter port numbers seperated by comma or port range
Example: 1,2,3,4,5-20

☐ Required ☒ Deny

* 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 25: Process Rule Type for Agentless mode

- 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 26: NetBIOS Rule Type for Agentless mode

- 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 27: MAC Address Rule Type for Agentless mode

5. On adding the Rule Types, select the required option for rules, and **Dashboard Reporting** options and click **Save Changes**.
6. 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 28: Policy enforcement for Agentless mode with Profiler on User Realm

User Realms > Guest > Authentication Policy > Host Checker

Host Checker

General Authentication Policy Role Mapping

Source IP Browser Certificate Password Host Checker Limits RADIUS Request Policies

☒ Agentless mode with Profiler. Note: This requires Profiler to be configured. Navigate to [Auth Servers](#) for configuring Profiler.

Allow users whose workstations meet the requirements specified by required host-checker policies. If no policies are selected then all users will be allowed. "Evaluate Policies" will evaluate the policy by the profiler.

10 records per page Search:

Evaluate Policies	Require and Enforce	Available Policies
<input type="checkbox"/>	<input type="checkbox"/>	All
<input type="checkbox"/>	<input type="checkbox"/>	test_ahc (Agentless mode with Profiler)

← Previous 1 Next →

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 29: Policy enforcement for Agentless mode with Profiler on User Role

User Roles > Guest > General > Restrictions > Host Checker

Host Checker

General Agent Agentless

Overview Restrictions Session Options UI Options

Source IP Browser Certificate Host Checker

☒ Allow all users (Host Checker not required)

☐ Allow users whose workstations meet the requirements specified by these Host Checker policies:

Available Policies:

- test_ahc (Agentless mode with Profiler)
- test_hc

Add -> Remove

Selected Policies:

☐ Allow access to the role if any **ONE** of the selected policies is passed.

To manage Host Checker policies, see the [Host Checker](#) configuration page.

[Save Changes](#)

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

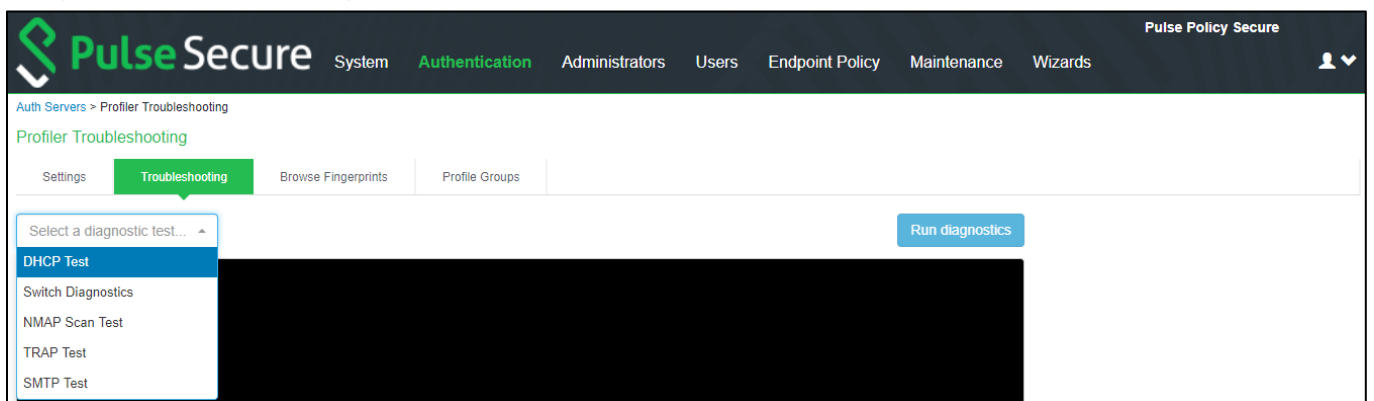
The following tests help to identify and solve basic problems associated with configurations of the Profiler.

Test	Result
DHCP Test	<ul style="list-style-type: none"> Verify if ports are receiving the DHCP packets. Detect a device when connected to network during the diagnostic run.
Switch Diagnostics	<ul style="list-style-type: none"> Verify switches are enabled Check if SNMP walk is successful or not Check if Profiler can successfully read ARP table, CAM table, and SSID information
NMAP Scan Test	<ul style="list-style-type: none"> Check if NMAP scan is working for an IP address, which is prompted during diagnostic run
Trap Test	<ul style="list-style-type: none"> Verify if trap is collected or not for a switch event. Detect a device when connected to network during the diagnostic run.
SMTP Test	<ul style="list-style-type: none"> Troubleshoot any problem in configuration/reachability of SMTP server. 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 30: 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 31: List of Events to Log



☐ Connection Requests
 ☐ Statistics

☐ System Status
 ☐ Performance

☐ System Errors
 ☐ Enforcer Command Trace

☐ Enforcer Events

☐ 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
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
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

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
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

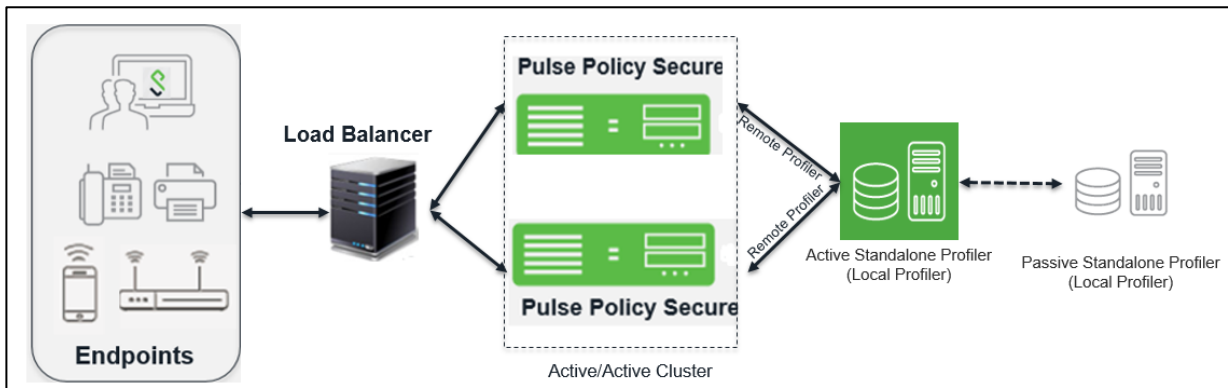
Standalone Profiler can be deployed as an independent appliance. All PPS and PCS appliances communicate with this Standalone Profiler for authorization.

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.

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

Figure 32: 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:

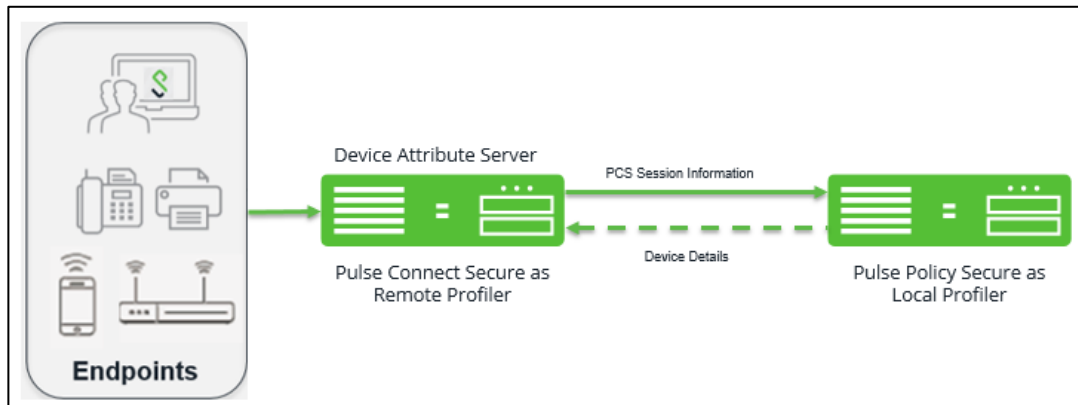
- Information such as hostname and IP address, device IP address and MAC address, session identifier, user-agent are retrieved by the session and sent to the Profiler.
- The Profiler returns Device OS, Device Manufacturer, Device Category and Session Identifier to PPS/PCS.
- The Profiler updates the 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 33: Example of a Remote Profiler

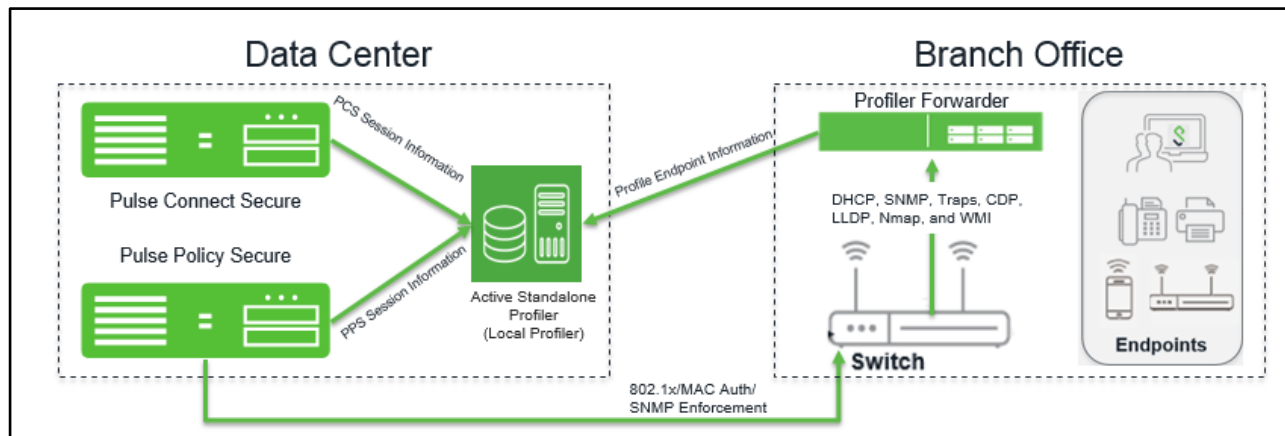


Profiling devices in branch offices

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 34: 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.