Pulse Policy Secure Profiler: Administration Guide

9.1R8

Product Release	9.1R8
Published	July 2020
Document Version	1.6

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Pulse Policy Secure Profiler: Administration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

The following table lists changes made to this document:

Document Revision	Release	Date	Feature	Changes
1.6	9.1R8	July 2020	TCP, SMB, and Device Attributes server collectors Profiler UI changes Time-Bound-Approval Customized reports	Added new collectors, changed all procedures and screen shots to reflect UI changes with new flow.
1.5	9.1R5	April 2020	Backup and Recovery for Profiler deployments	Included the Profiler Backup and recovery mechanisms for various deployment cases.
1.4	9.1R4	January 2020	Role Mapping based on LDAP attributes and Device attributes	Included LDAP Collector section. Updated the Configuring the Local Profiler Authentication Server section with updates.
1.3	9.1R3	October 2019	--	Included a note for minimum required fingerprint package in Configuring the Local Profiler Authentication Server section.
1.2	9.1R2	July 2019	Profile Groups	Included Creating Rules for Profile Groups section
1.0	9.1 R1	April 2019	SNMP HOST Collector	Included SNMP HOST collector section.Updated the Configuring the Local Profiler Authentication Server section with updates. Included Diagnostic Logs section Updated Profiling Devices in Branch Office section.

Contents

Preface

Document conventions

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

Text formatting conventions

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

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier Font`	Identifies command 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.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

Convention	Description
{ **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 elements.
< >	Non-printing 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.
bold text	Identifies command names, keywords, and command options.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

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

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides 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: https://support.pulsesecure.net
- Find product documentation: https://www.pulsesecure.net/techpubs
- Download the latest versions of software and review release notes: https://support.pulsesecure.net

- Open a case online in the CSC Case Management tool: https://support.pulsesecure.net
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://support.pulsesecure.net

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: https://kb.pulsesecure.net
- Ask questions and find solutions at the Pulse Community online forum: https://community.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, US).

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

Reporting Documentation Issues

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, contact Pulse Secure Technical Support (https://support.pulsesecure.net). Include a full description of your issue or suggestion and the document(s) to which it relates.

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.

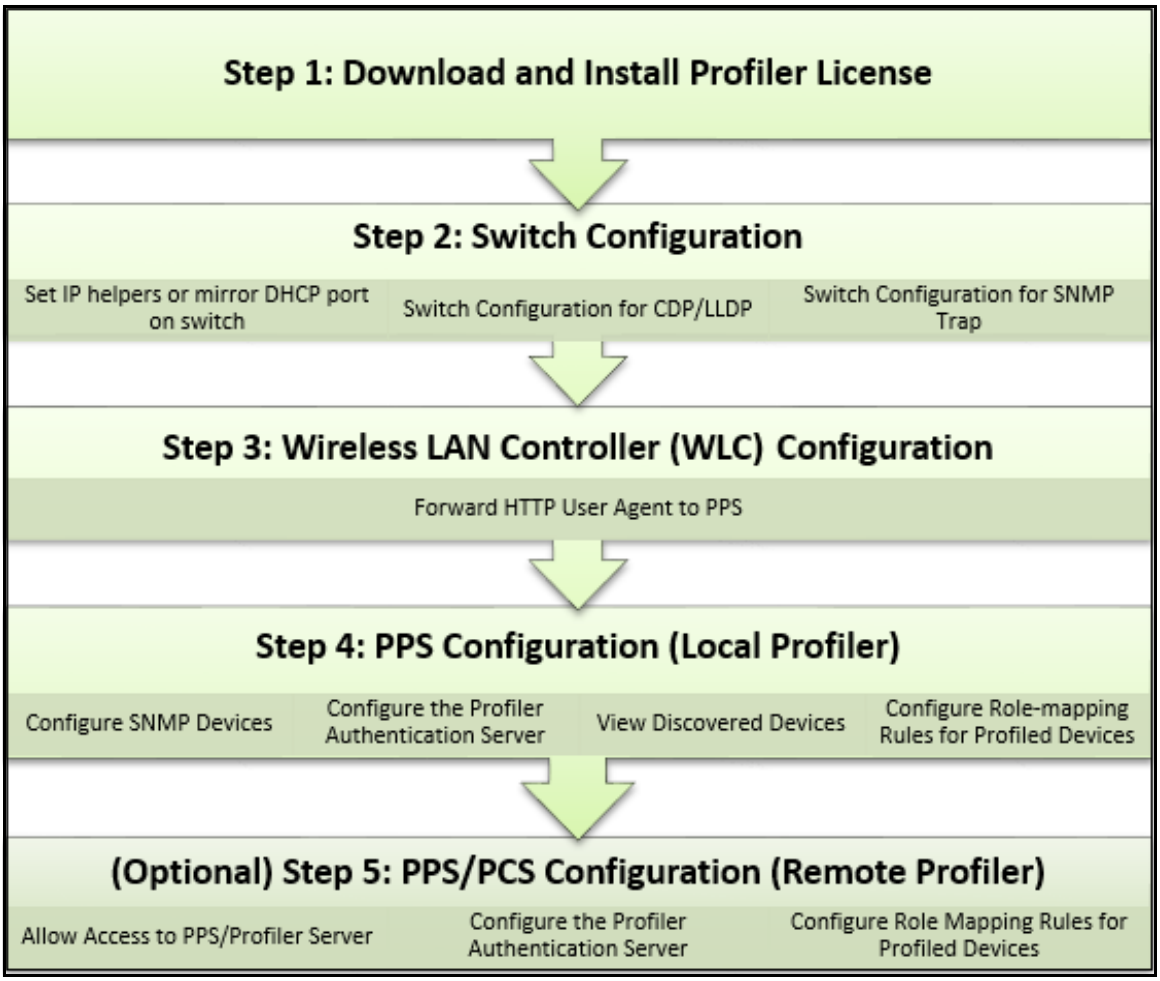
Pulse Policy Secure(PPS) integrates with the Profiler to provide visibility and control of endpoint devices. This document focuses on features of the Profiler in a network with an existing Policy Secure deployment already configured with the basic elements required to provide network access, including authentication servers, sign-in policies, roles, realms, and SNMP-based enforcement or RADIUS attributes policies for enforcement based on 802.1X / MAC authentication. Refer to the *Pulse Policy Secure Administrator 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 *Pulse Connect Secure Administrator Guide*, *Pulse Policy Secure Administrator Guide*, 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.

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.

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.

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 provide 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.

SMB Collector

Profiler passively parses the Server Message Block (SMB) packets to get the operating system and host-name of the endpoints. The SMB protocol allows computers connected to the same network or domain to access files from other local computers as easily as a local hard drive. SMB also allows computers to share printers and serial ports from other computers within the network. SMB provides host name that is used by LDAP collector to collect the information from LDAP server.

SMB collector runs only on external interface. SMB collector needs an external interface dedicated to port mirroring and directly connected to the switch port mirroring destination. Since, switches do not allow ingress packets on destination mirrored port, internal or management interface is used for regular traffic.

In some environments, it is easier to forward traffic to the Profiler using the SPAN/RSPAN configuration.

TCP Collector

Profiler uses TCP SYN/SYN-ACK packets to profile the devices. Profiler discovers the devices when the device transmits TCP Syn/Syn-ACK packets instead of waiting for SNMP polling to begin and also trigger active collectors to fetch the information.

The profiler discovers and classifies the unrouted mirror traffic received by external interface. For routed traffic, the profiler only classifies the endpoints already discovered by other collectors. TCP connections do not require to keep a port always open. Endpoints may open or close TCP connections as required. The TCP/IP packets helps to identify the various configuration attributes of a networked device along with the OS of the endpoint.

TCP collector runs only on external interface. TCP collector needs an external interface dedicated to port mirroring and directly connected to the switch port mirroring destination. Since, switches do not allow ingress packets on destination mirrored port, internal or management interface is used for regular traffic.

In some environments, it is easier to forward traffic to the Profiler using the SPAN/RSPAN configuration.

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.

MDM Collector

Pulse Policy Secure(PPS) 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.

Device Attribute Server collector

Third Party controllers have the capability to fetch details of ICS devices managed by Operational Technology. Operational technology devices include valves, transmitters, switches, sensors and actuators. These devices rely on custom protocols for managing and communication.

The controller is configured as a HTTP Attribute Server and is available under Device Attribute Server settings. The server is manually selected as an active collector to collect information that is used to classify and categorize the devices. The attributes information helps for role mapping.

Note: For release 9.1R8, profiler supports only Nozomi Controller as the third party collector. The collector can only read devices that have a confirmed MAC address and are stored in the profiler.

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.

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.

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.

LDAP Collector

The LDAP collector fetches attributes from the configured LADAP server based on the device attributes from the profiler.

Note: Configure the LDAP Server under Authentication Servers using <HOSTNAME> or <USER> as filter.

Configuring the Local Profiler

Before You Begin

Ensure you perform the following tasks before proceeding with the Profiler Authentication server configuration.

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

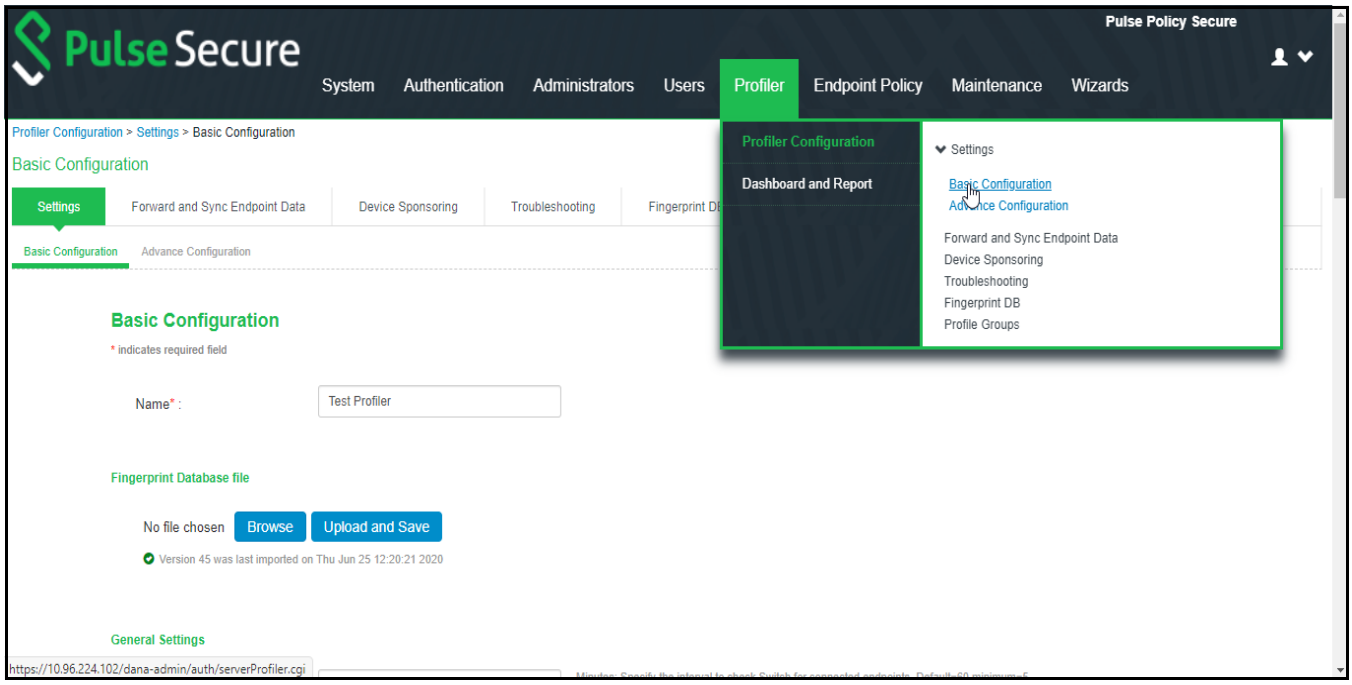
Note: The following configuration steps are applicable only to the new User Interface and cannot be accessible through old UI.

Basic Profiler Configuration

To configure basic settings for the Local Profiler:

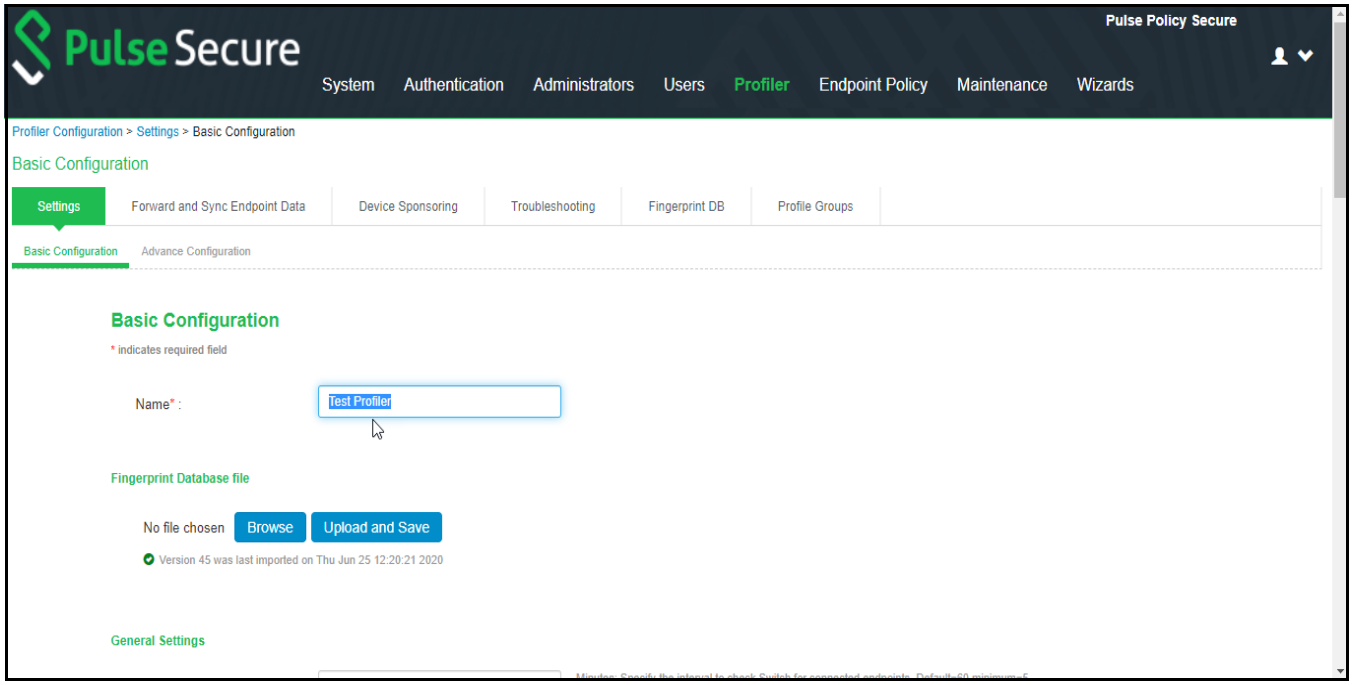
1. Navigate to **Profiler > Profiler Configuration > Basic Configuration**.

Figure 2 Creating a Local Profiler



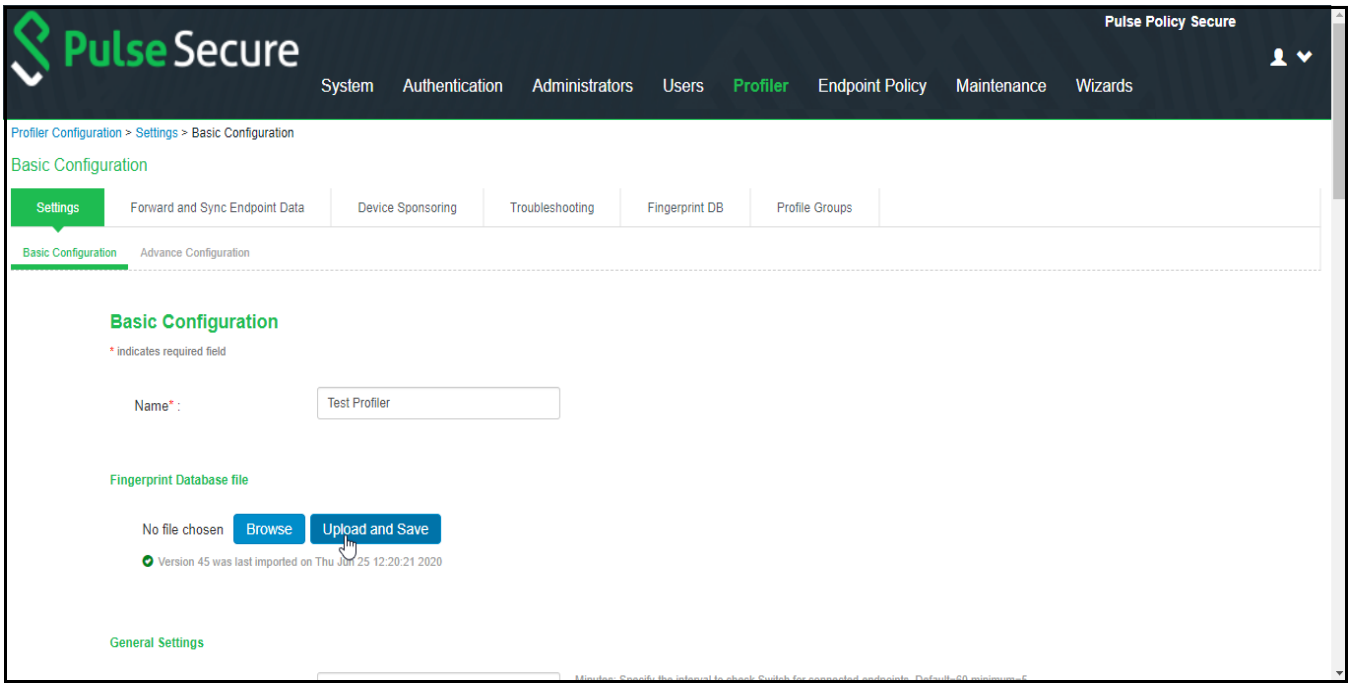
2. Enter a name for the Profiler.

Figure 3 Naming a Local Profiler Authentication Server



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

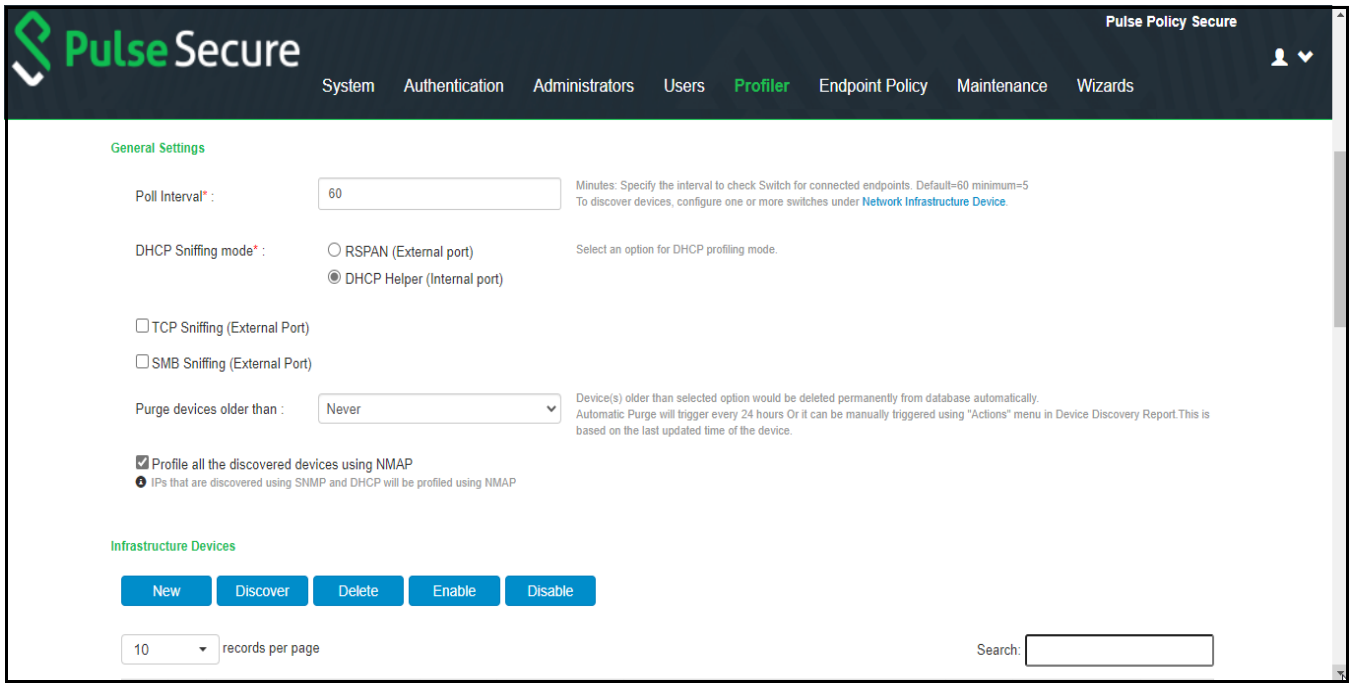
Figure 4 Uploading Device Fingerprints Package



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

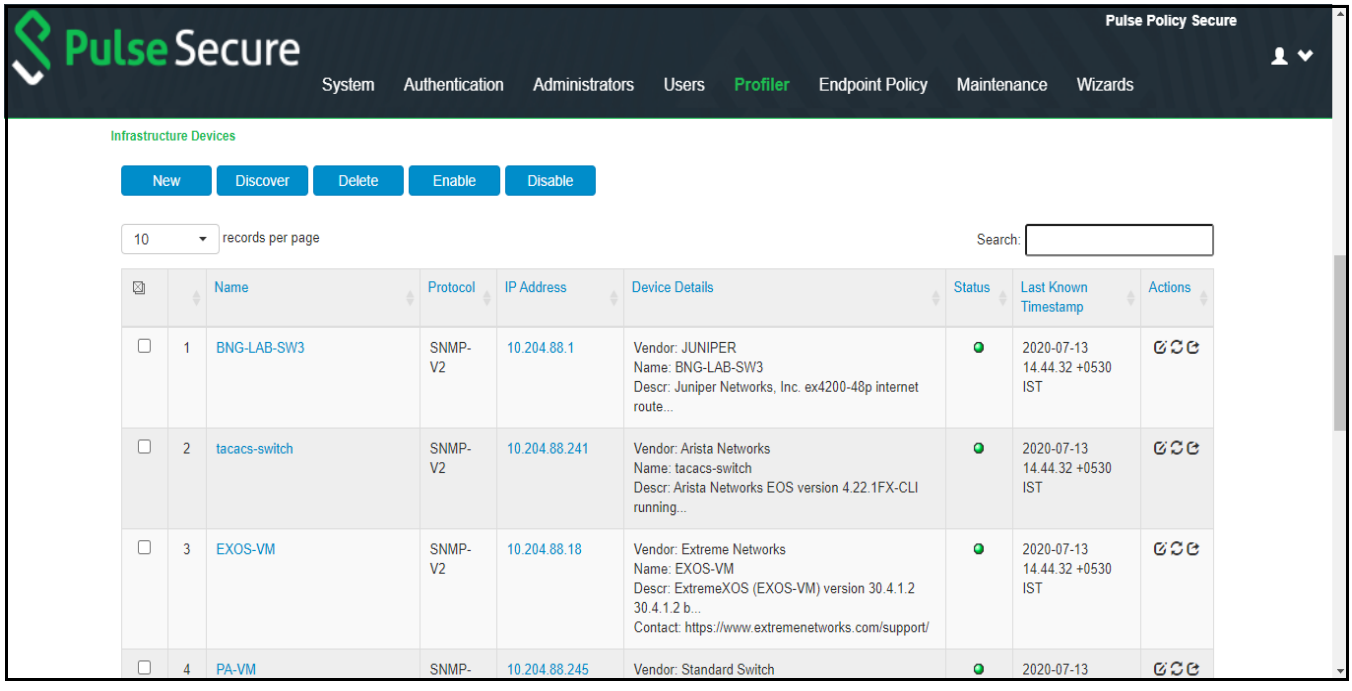
   - Set SNMP **Poll interval**, for polling the Network Infrastructure Devices. By default, the poll interval is set to 60 minutes.
   - Select the **DHCP Sniffing mode**. RSPAN for external ports and DHCP Helper for internal ports. Optionally, select the TCP or SMB Sniffing modes to profile devices using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

Figure 5 General Settings



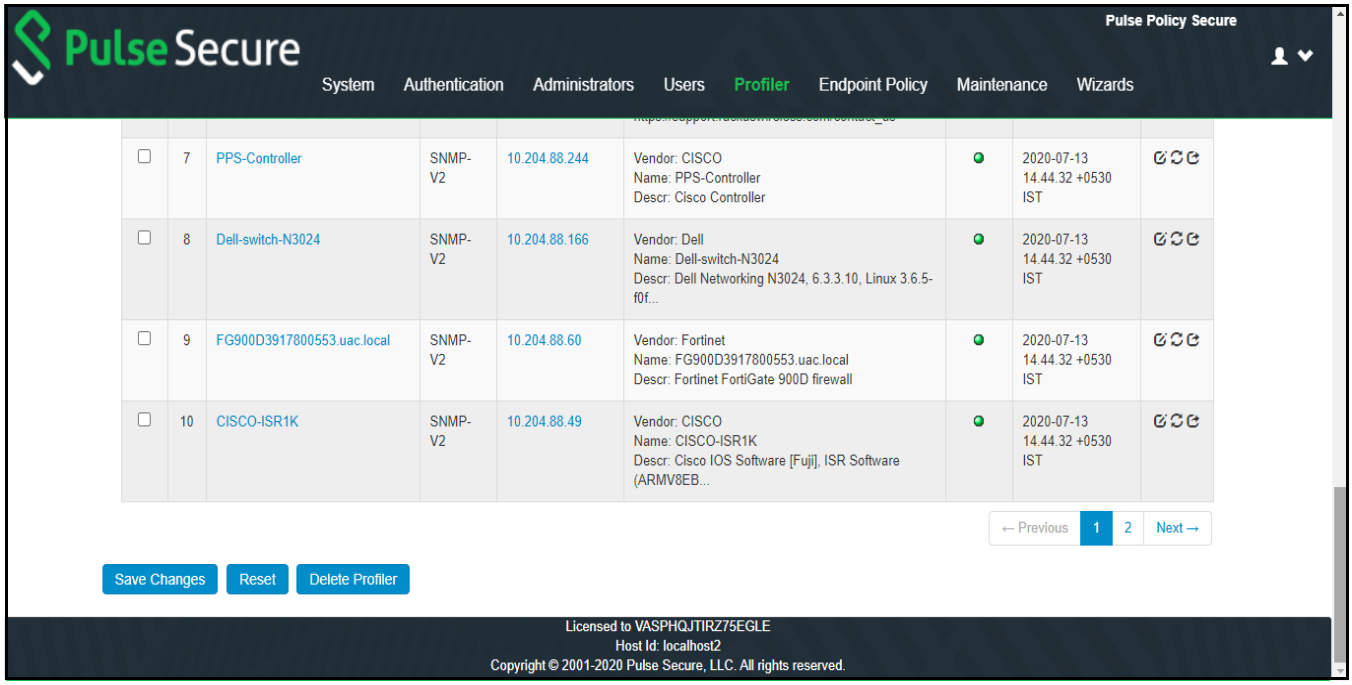
5. The SNMP/SSH scans and lists the **Infrastructure Devices** and connected endpoints after a predefined Poll interval with details.

   - Use **New** to add devices, **Discover** to find a range of devices in the network by entering the details in the pop-up window.
   - For each device, use the icons in the **Actions** column to Edit, Refresh, or Duplicate the device details.



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

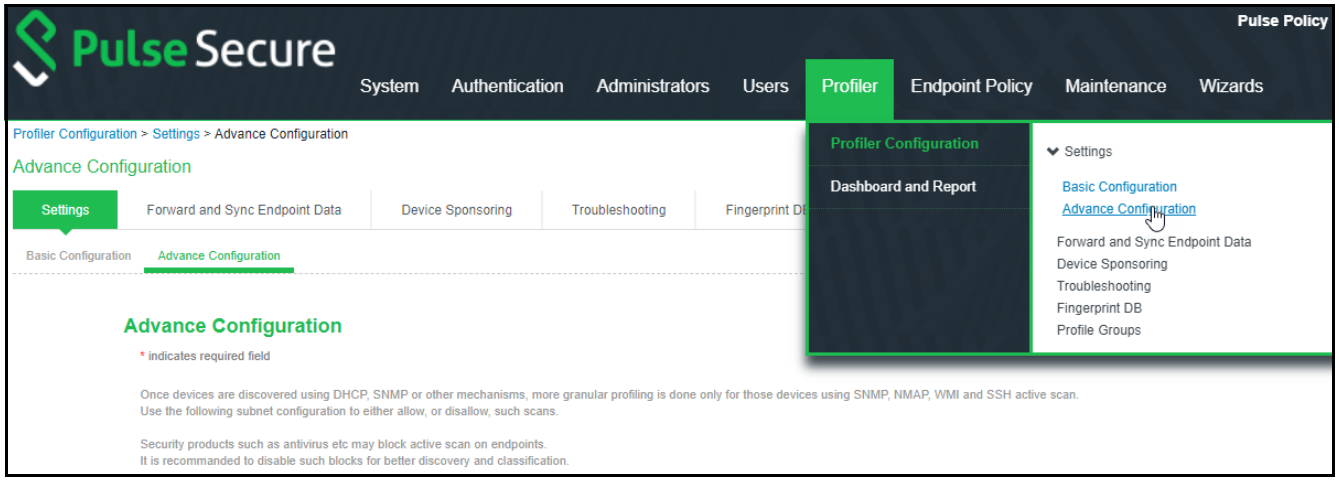
Figure 6 Save Profiler Basic Configuration



Advance Profiler Configuration

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

Figure 7 Advance configuration of a Local Profiler

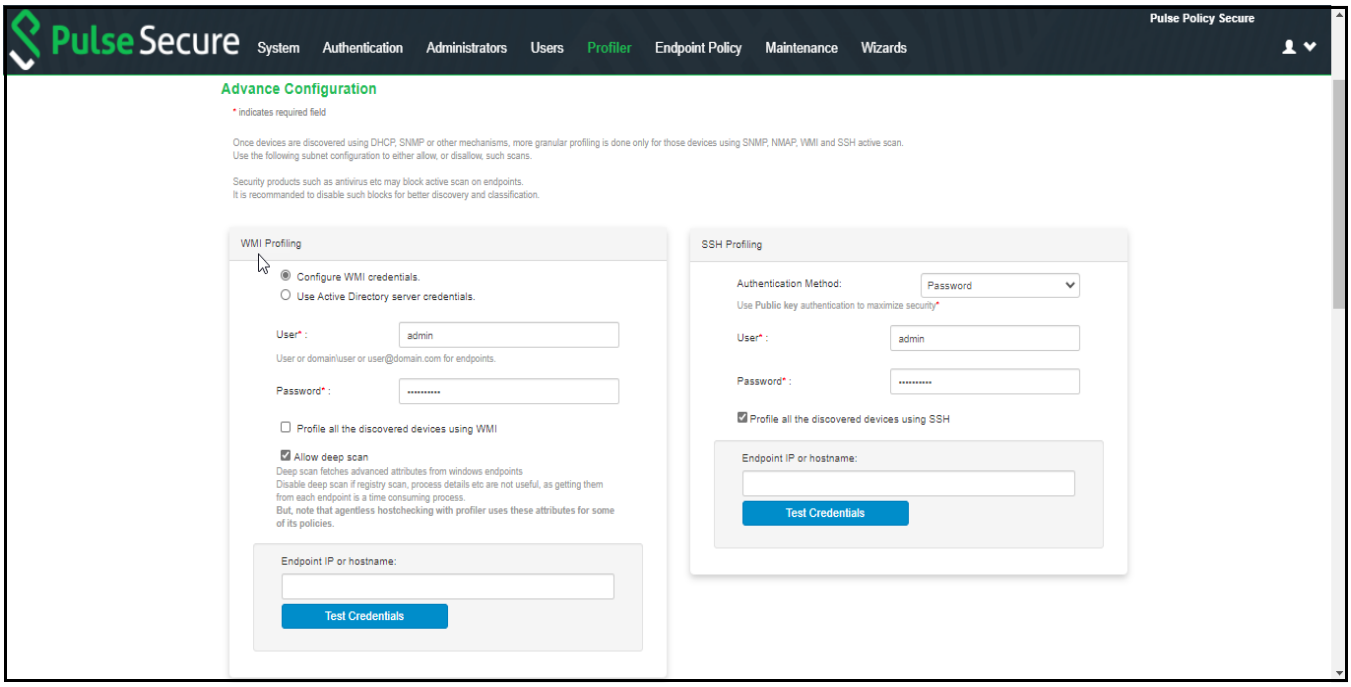


WMI Configuration

To configure WMI profiling:

- Select **Configure WMI credentials** and specify the domain administrator or user with administrator credentials to fetch accurate endpoint information from remote desktops running Microsoft Windows. Select **Use Active Directory server credentials** to use existing Active Directory server credentials.
- Optionally, select the option to profile all the discovered devices using WMI. If the number of discovered devices is exceeding 1000, it is recommended to add subnets manually to scan only Windows devices.
- Select **Allow deep scan** to control the level of information to fetch from the Endpoint remotely through WMI. Deep Scan includes information on ports, process, and security product details such as product version, signature version, signature date attributes. This option is required if Agentless Host checker with Profiler policies are configured for endpoint posture assessment.
- Enter the Endpoint IP or hostname to test the credentials.

Figure 8 WMI Profiling

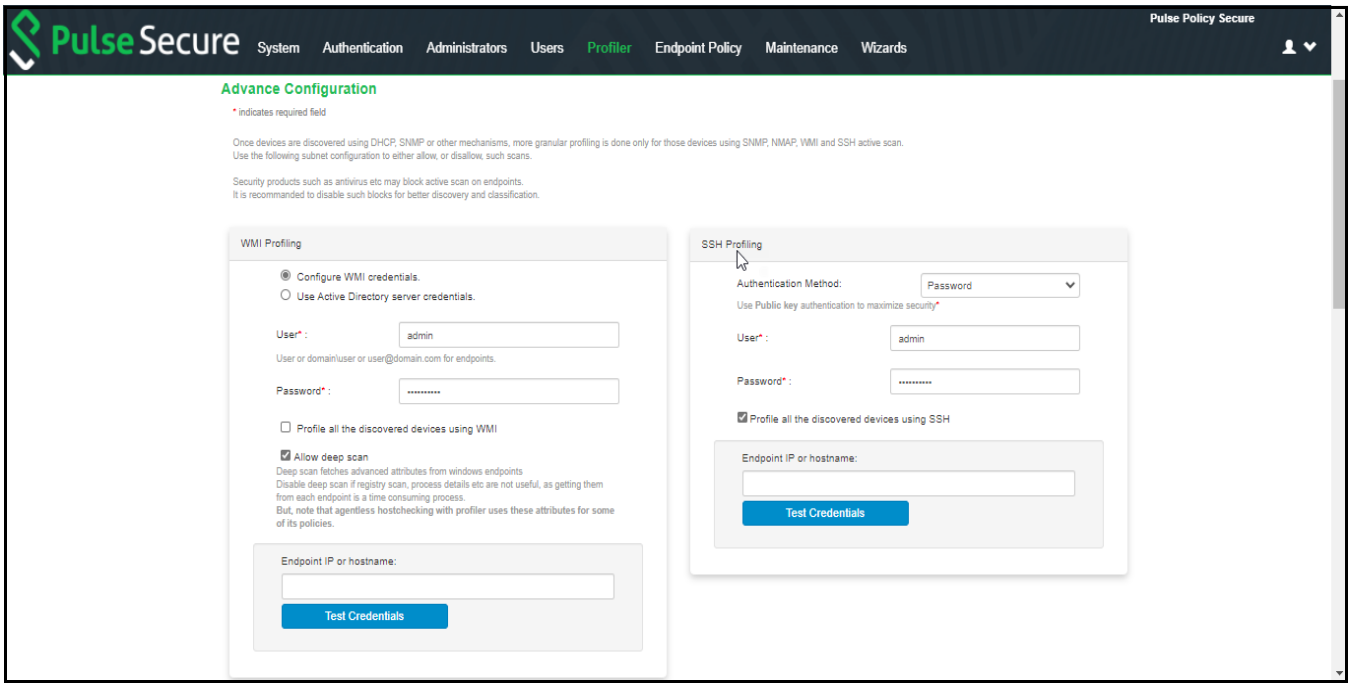


SSH Configuration

To configure SSH Profiling:

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

Figure 9 SSH Profiling

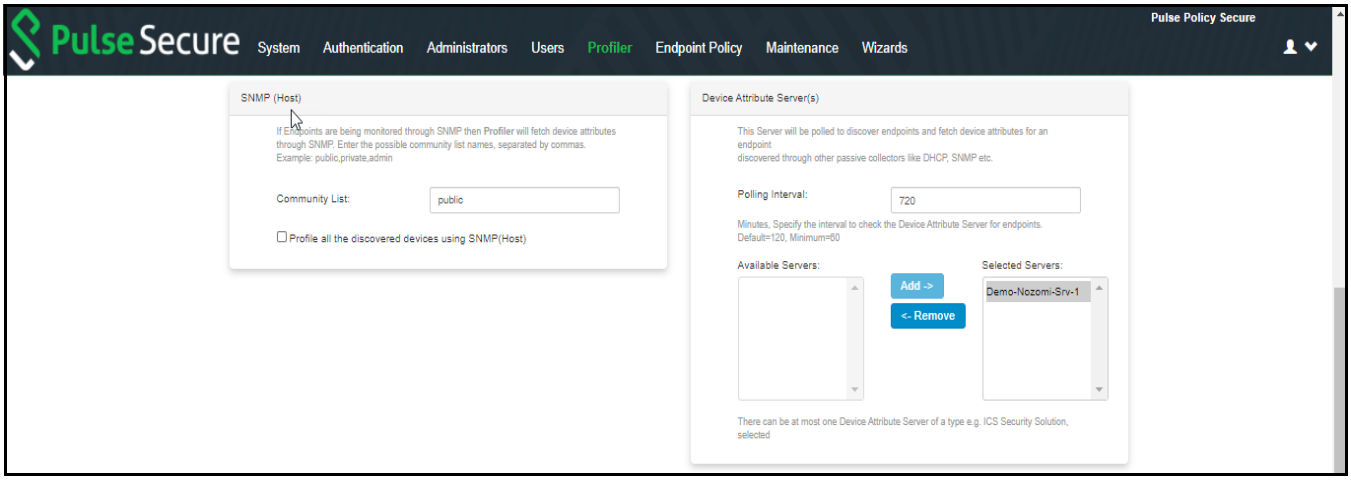


SNMP (Host) Configuration

To configure SNMP (Host) Profiling:

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

Figure 10 SNMP (Host) Profiling



Device Attribute Server Configuration

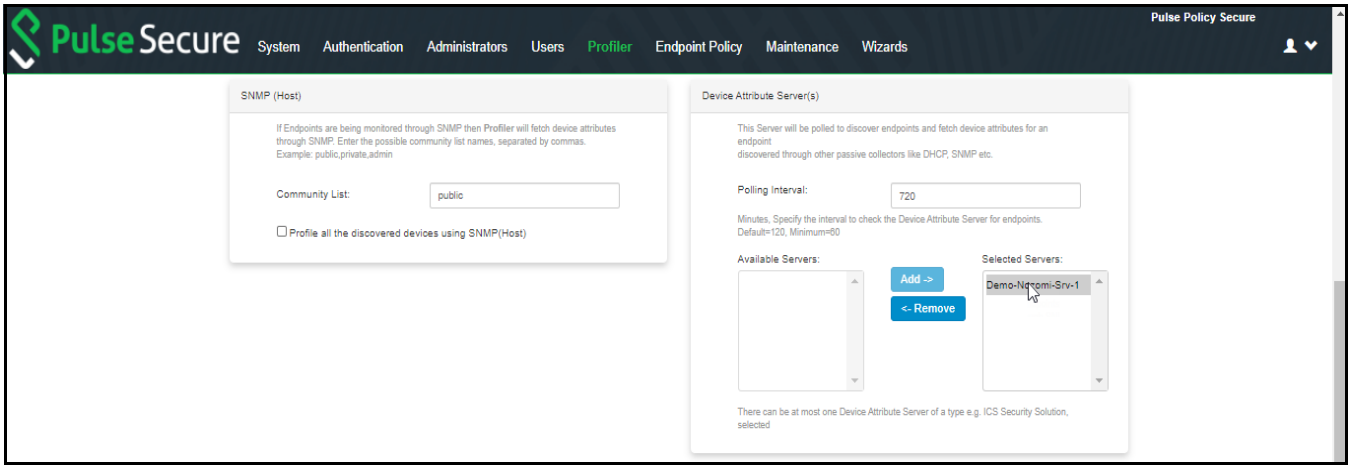
The profiler polls the device attribute server at regular interval to collect the device attributes for the endpoints discovered using passive collectors. The controller is configured as a HTTP Attribute Server and is available under Device Attribute Server settings.

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

To configure profiling using the device attribute server:

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

Figure 11 Device Attribute server configuration



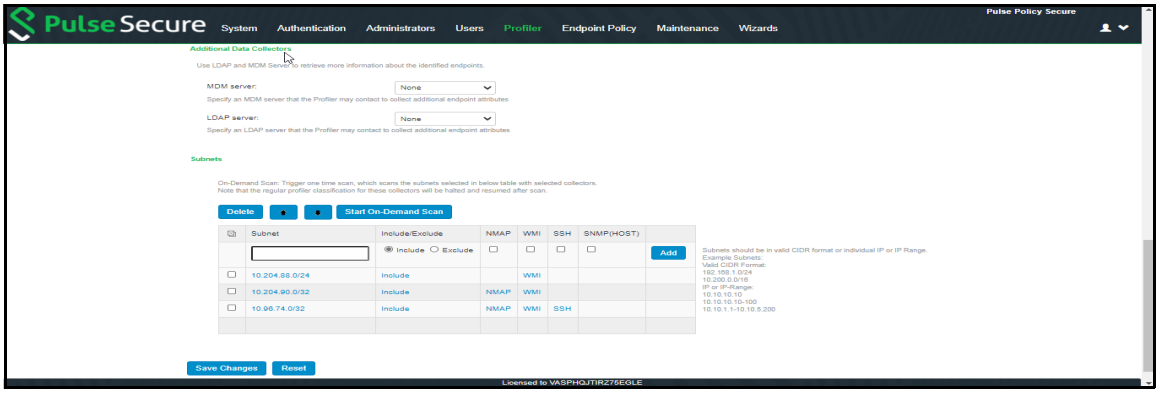
Additional Data Collectors configuration

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

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

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

Figure 12 MDM Server and LDAP Server configuration



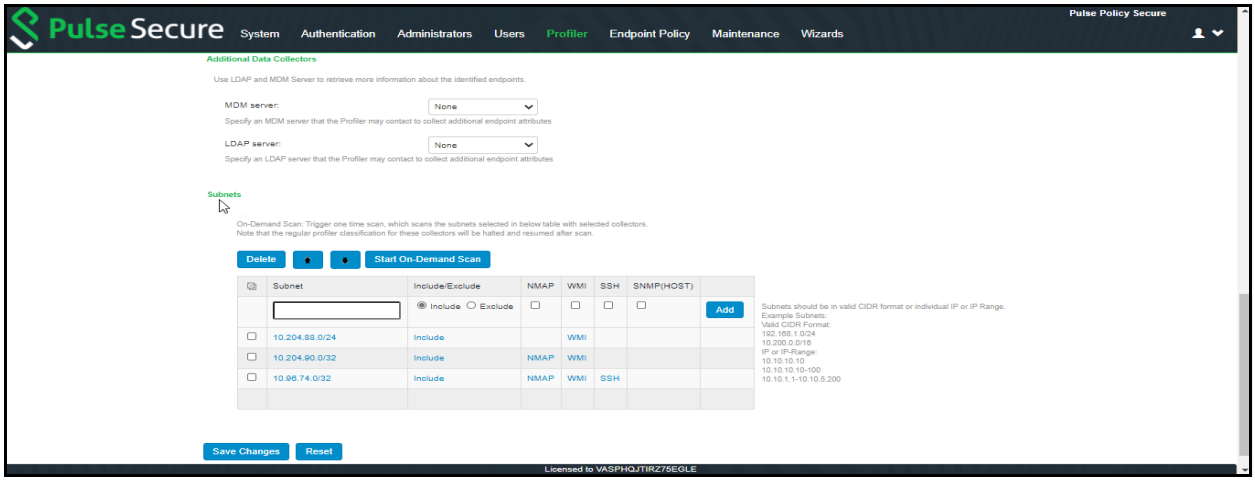
Subnets Configuration

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

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

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

Figure 13 Subnets Configuration

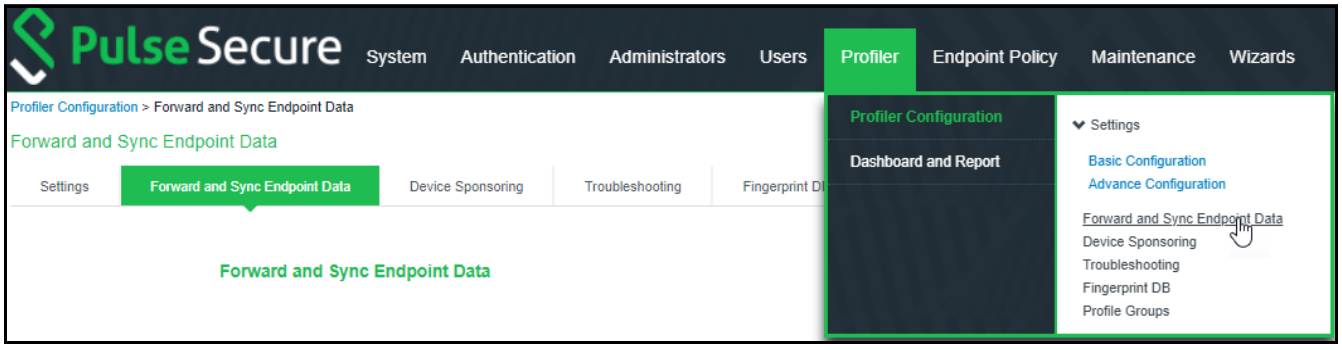


Forward and Sync Endpoint Data

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

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

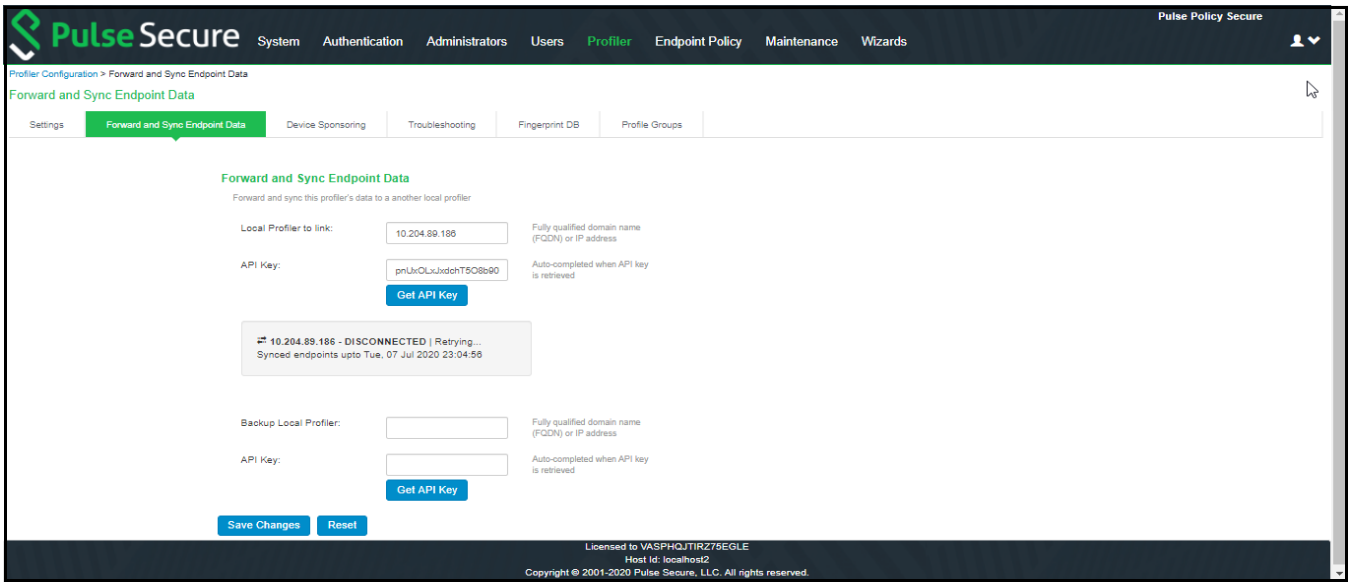
   Figure 14 Forward and Sync Endpoint Data



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

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

Figure 15 Forward and Sync endpoints configuration



Devices that are discovered are profiled and updated in the Device Discovery Table and an overall summary is shown in the “Dashboard” on page 20.

The devices can be grouped based on group name and rules using device attributes. For more information see, “Profile Groups” on page 30.

The 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” on page 29.

Profiler Reports

Dashboard

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

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

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

You can customize the charts in the dashboard 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.

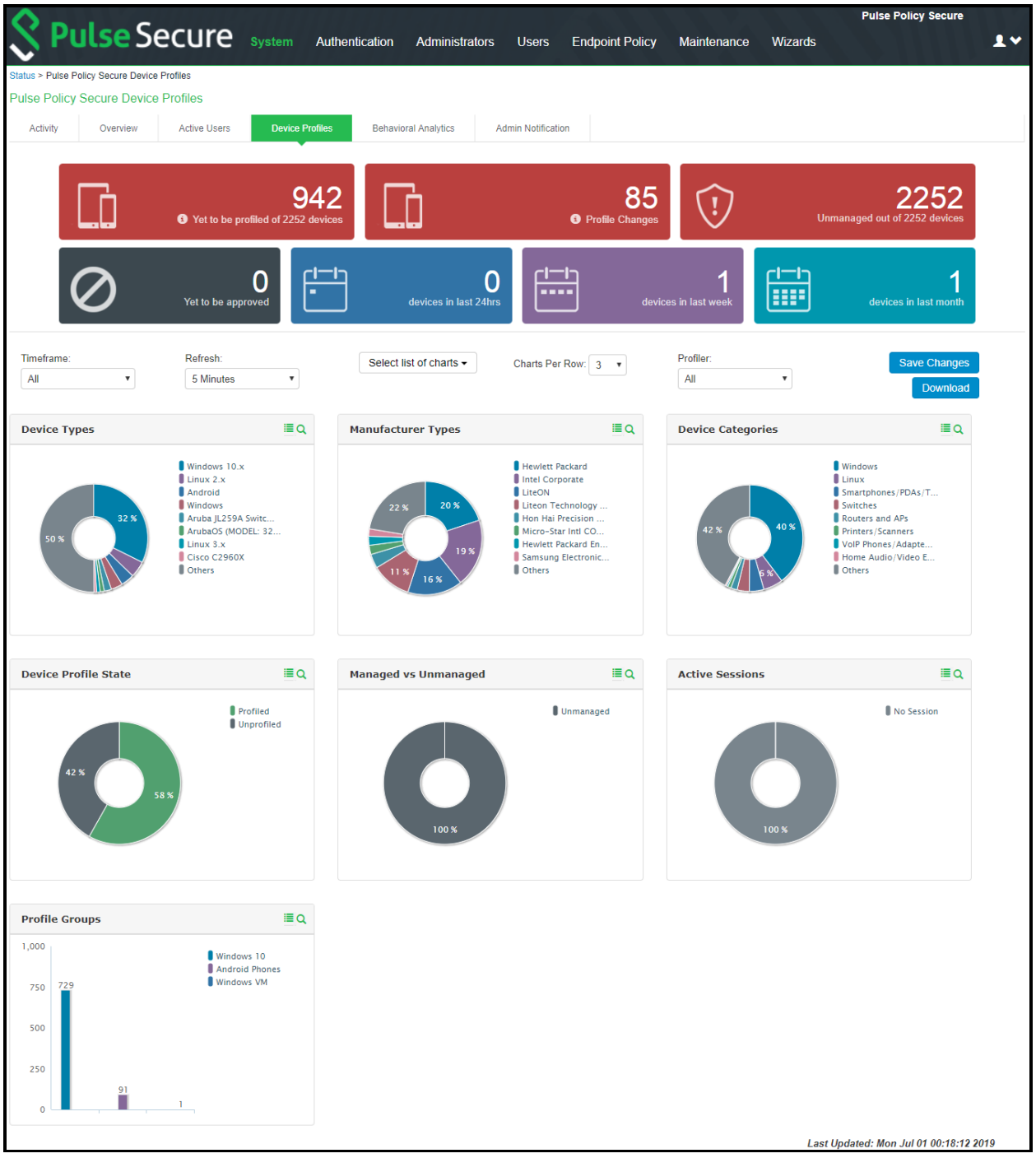
The dashboard displays the following charts:

- **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. For more information, see "Profile Groups" on page 30.

You can view the charts on the dashboard or download as a report in PDF format. You can also schedule to send the reports as an email.

Figure 16 Dashboard View

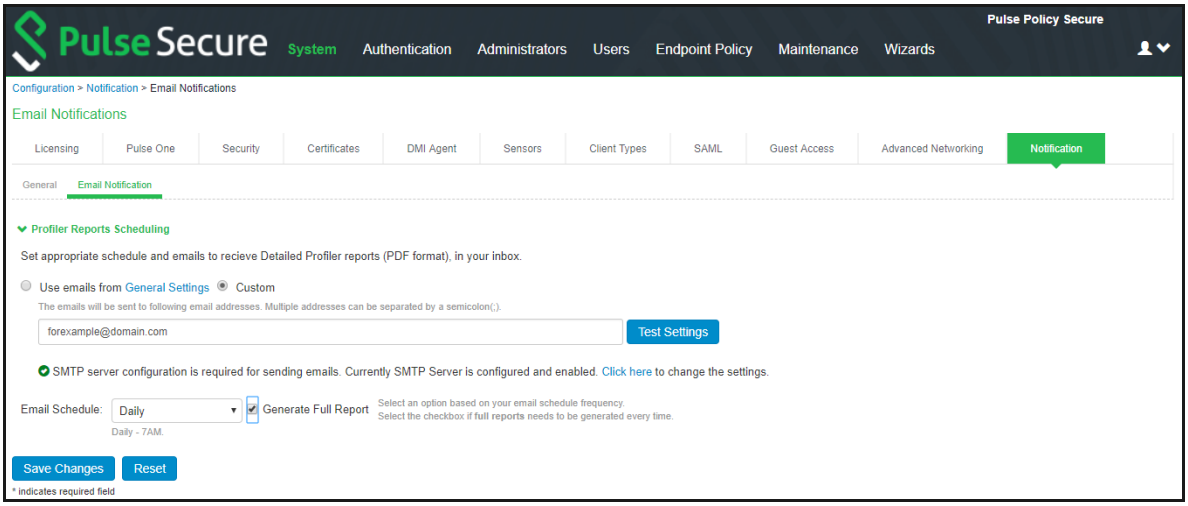


Profiler Report Scheduling

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 17 Report Scheduling



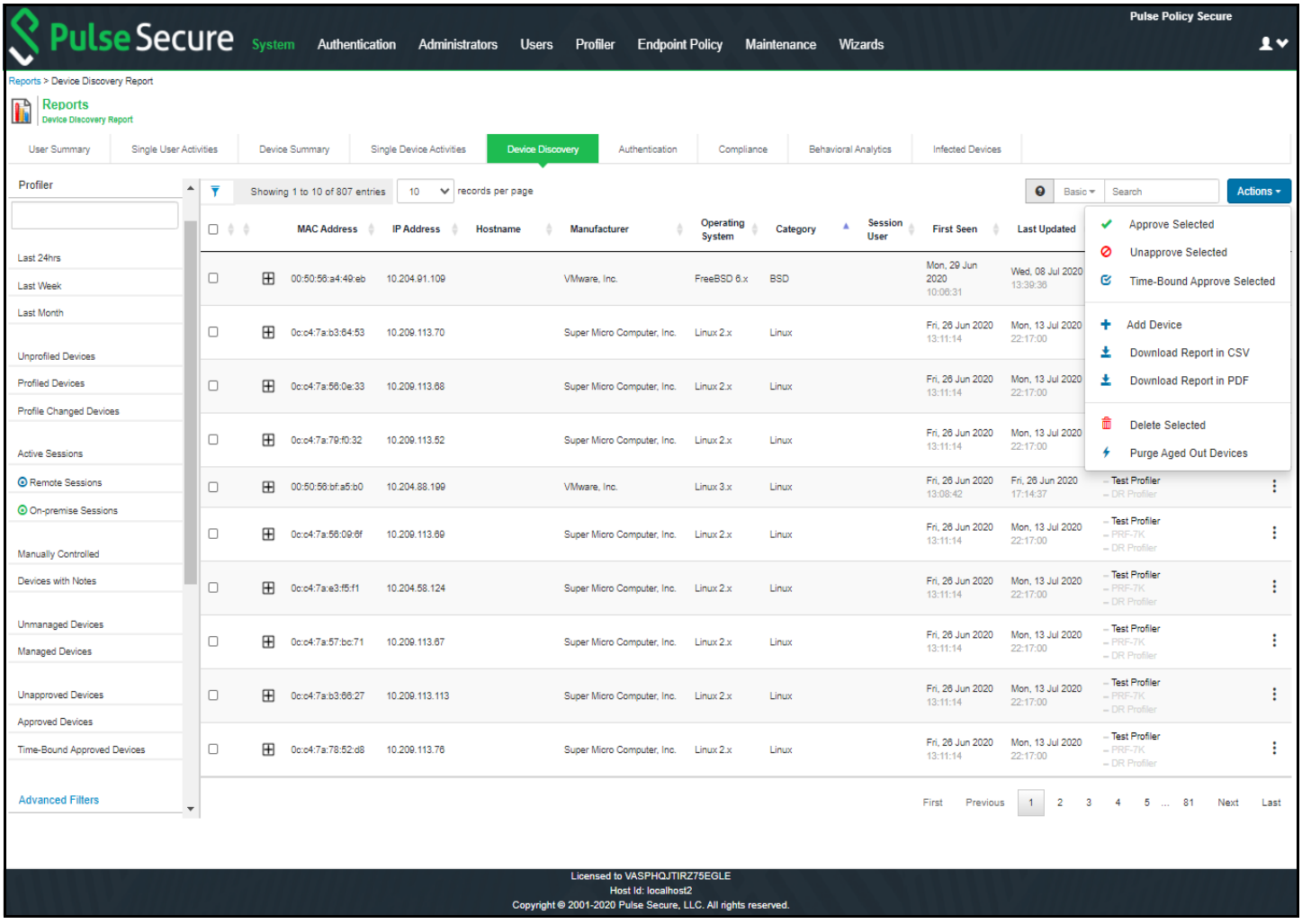
Device Discovery Report Table

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.

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

Figure 18 Device Discovery Report Table

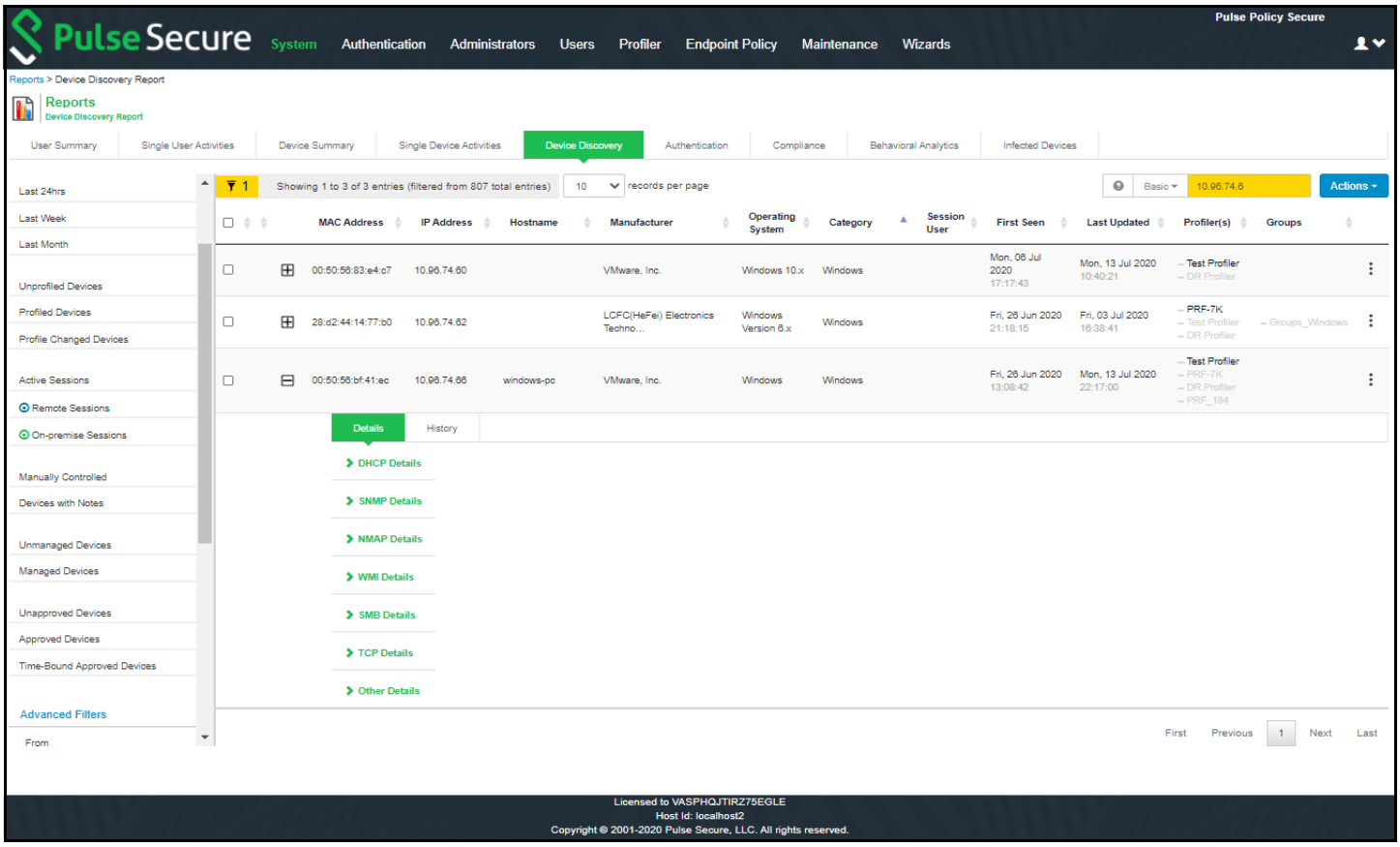


Endpoint Information

All current and historical information for a device is displayed in an expanded view based on IP address, sessions (remote, local) or profiles changes.

Expand the required endpoint to display current Details and History.

Figure 19 History based on IP Address



Endpoint Filters

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

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

  Note: The Unapproved devices are indicated in Red and Time-Bound Approved devices are indicated in Yellow.

Note: If an endpoint is classified incorrectly, see the Troubleshooting 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.
  - **Time-Bound Approve Selected Devices**: Allows to select and approve devices for a specified time period by specifying start date, end date, and time zone.

    Note: If an endpoint is configured for time-bound settings in DDR, it takes precedence over profile group time-bound settings.
  - **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 in CSV format**: Allows to download and save the report in CSV format. Allows to download complete report or filtered report as required. To download complete report, clear all filters before downloading.
  - **Download Report in PDF format**: Allows to download and save the report in PDF format. Allows to download complete report or filtered report as required. To download complete report, clear all filters before downloading.

    Note: The maximum number of entries to download as PDF is 30K. If the report contains more entries, apply more filters to refine the report.
  - **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

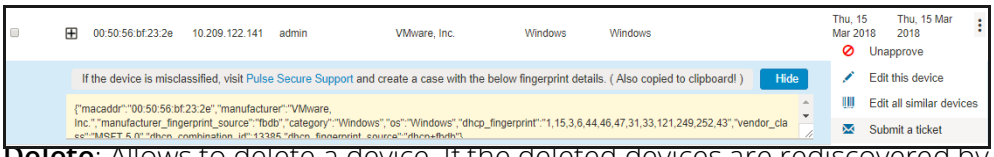
The Device Discovery Report Table allows the following operations for each of the listed devices.

- **Approve/Unapprove/TimeBound Approve**: Each endpoint has an attribute called status and allows to manually approve, time bound approve, or unappove a specific device. The time bound approved devices remains temporarily approved for a specified period in the specified timezone.

- **Edit this device**: 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 20 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.

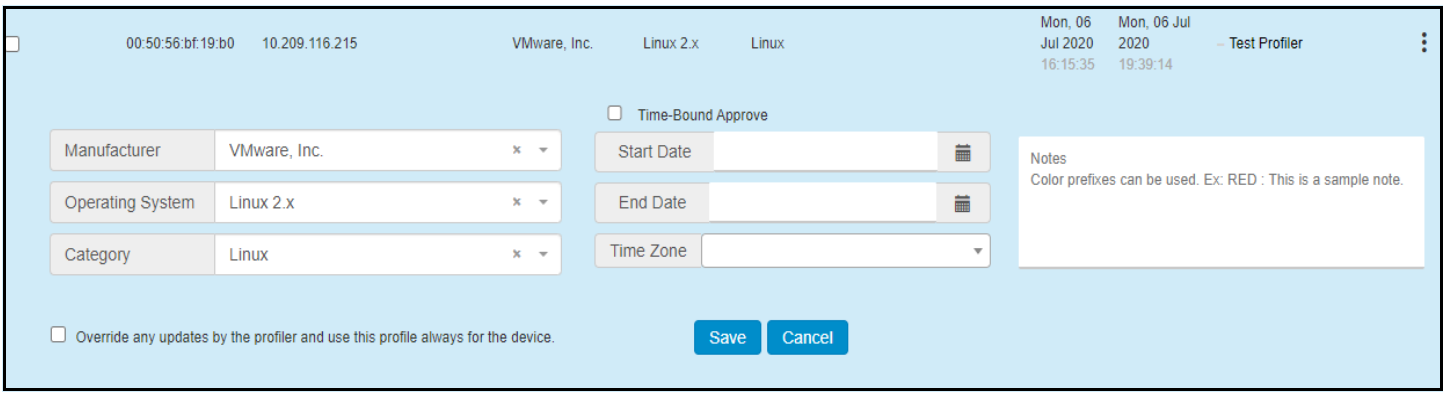
Overriding Device Approval Status

If the override option is selected for an endpoint in the DDR, the status does not change when there is any update, irrespective of configuration changes in Device Sponsoring page.

If the override option is not selected, the endpoint can change to any of the following status:

- When endpoint is in unapproved state, the endpoint remains in unapproved state inspite of an update.
- When endpoint is in temporary-approved state:
  - The endpoint remains in temporary-approved state if there is no category change.
  - The endpoint changes to unapproved state if there is a category change and the new category needs manual approval as per the configuration on Device Sponsoring page.
- Endpoint status changes to temporary-approved state when time bound approval time starts.
- Endpoint status changes to unapproved state when time bound approval time ends.
- Endpoint status changes to temporary-approved state immediately if start time is less than or equal to current time.

Figure 21 Override status



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 is 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, Device Attribute Server, WMI, SSH, SNMP/SNMP (Host), User Agent, DHCP, SMB, NMAP, TCP.

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 on the user interface or an E-Mail with a link to approve 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. The profiler allows to update status, IP, Manufacturer, OS, Category, Notes, Override, Profiler_Name attributes using the REST APIs.

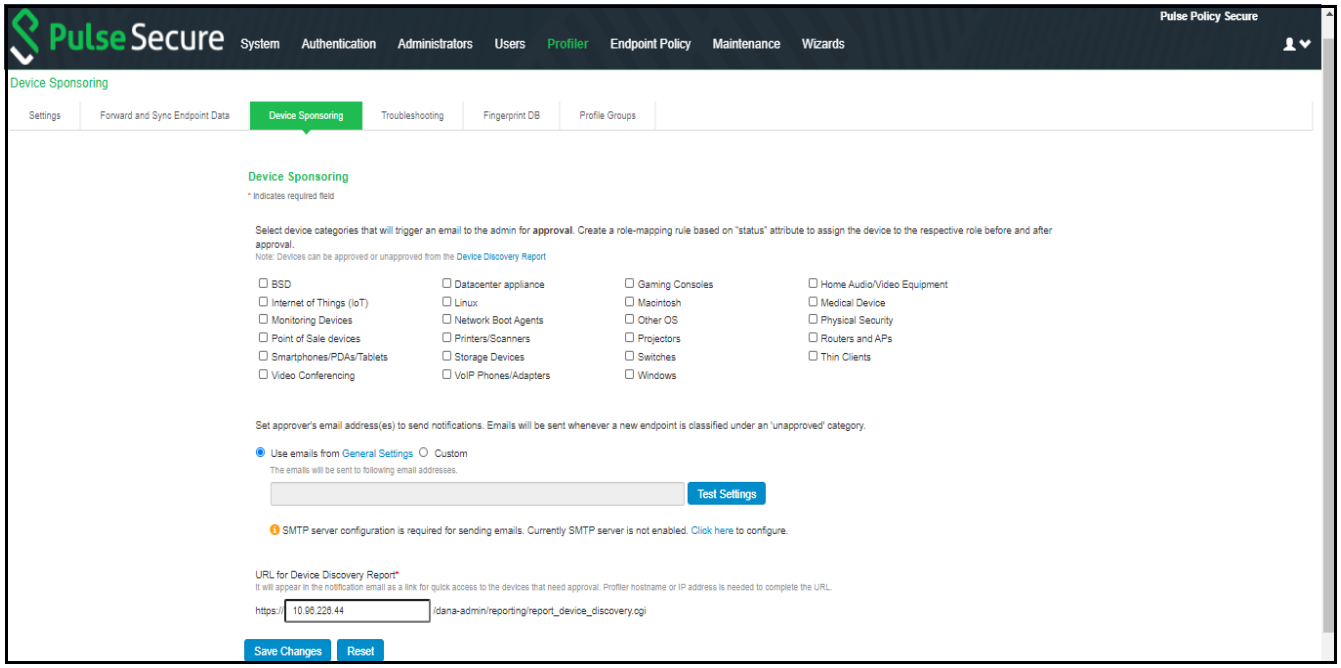
For more information on REST APIs, see *Pulse Connect Secure/Pulse Policy Secure REST API Solutions Guide*.

1. Navigate to **Profiler > Profiler Configuration > Device Sponsoring**.
2. Select device categories to 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.

   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 22 Device Sponsoring



Profile Groups

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

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

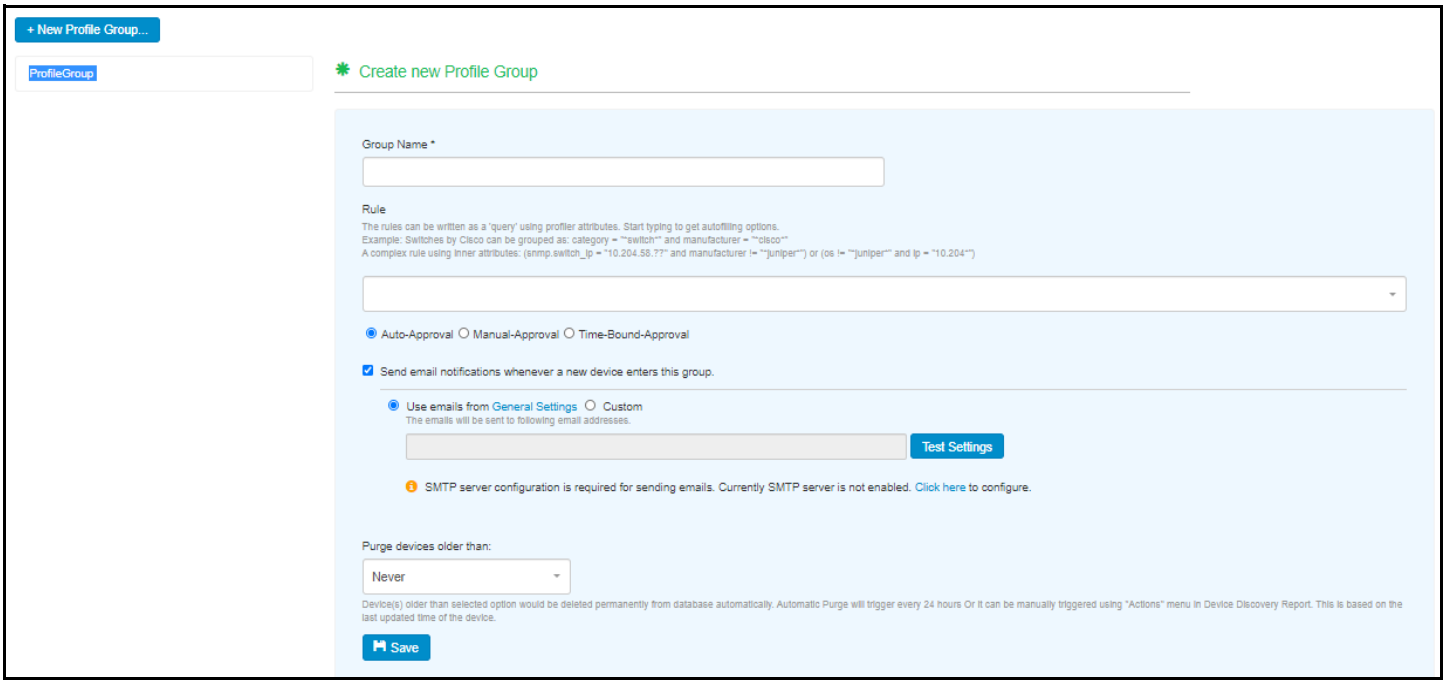
   To create rules for all values including null, use the rule: category ="*" or category ="".
3. Select the approval mode to approve the devices added to the profile group. Auto-Approval is the default option.
   - **Auto-Approval**: Automatically approves the devices.
   - **Manual-Approval**: Administrator manually approves the devices.

- **Time-Bound-Approval**: Devices approved for a specific time period and time zone. Enter the start date, end date, and time zone.

4. Select the option to send email notifications to notify when new devices are added to the group.
   - Choose **Use emails from General Settings** to send e-mails to address specified in General Settings or choose **Custom** and enter the e-mail addresses separated by semicolon.
5. Select the interval from the list to purge the older devices in the group automatically.
6. Click **Save**.

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

Figure 23 Profile Groups



To edit a profile group, select the group name from the lisx't on the left and make required changes and click **Save**.

To delete a profile group, select the group name from the list on the left and click **Delete this group** at the bottom of the page.

Precedence of Time Bound Approval

The endpoints marked for time bound approval in DDR or multiple groups has the following precedence:

- If an endpoint is configured for time-bound settings in DDR, it takes precedence over profile groups time-bound settings.

- When an endpoint belongs to multiple groups and the start date of the time bound approved groups are in future, the time bound settings for the group that has the start date that is closest to current date is applicable.
- When an endpoint belongs to multiple groups and the start date of any time bound approved groups are in past, the time bound settings for the group that has the farthest end date is applicable.

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	ip
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:

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

   Figure 24 Device Attributes

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

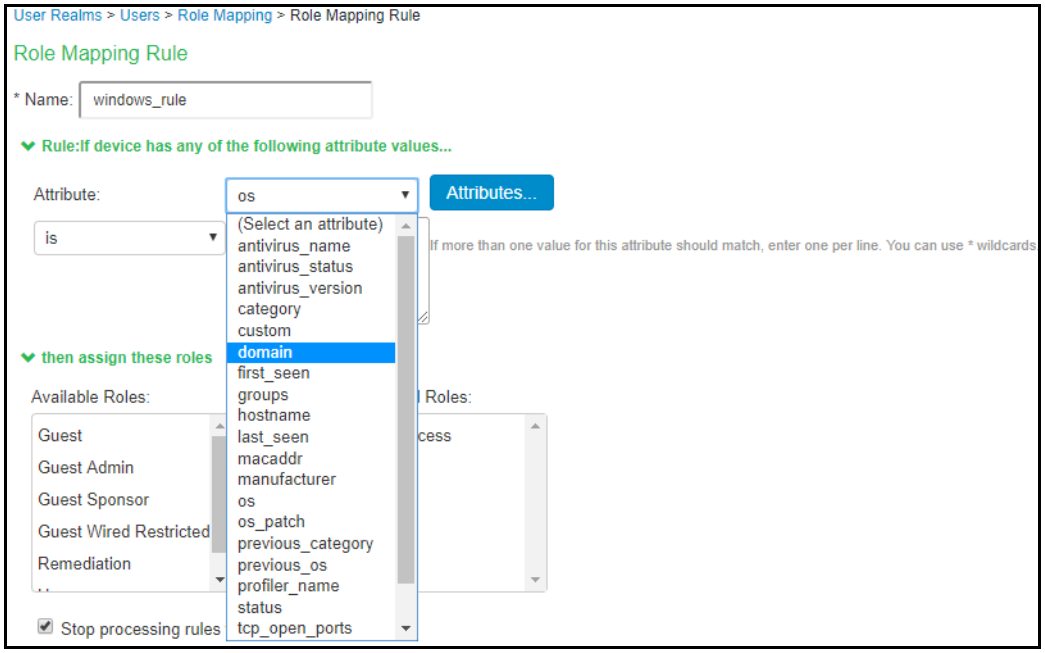
   Figure 25 Rule based on attribute

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

7. Enter a name for the rule (if creating a new one).
8. Create the new role mapping rules.

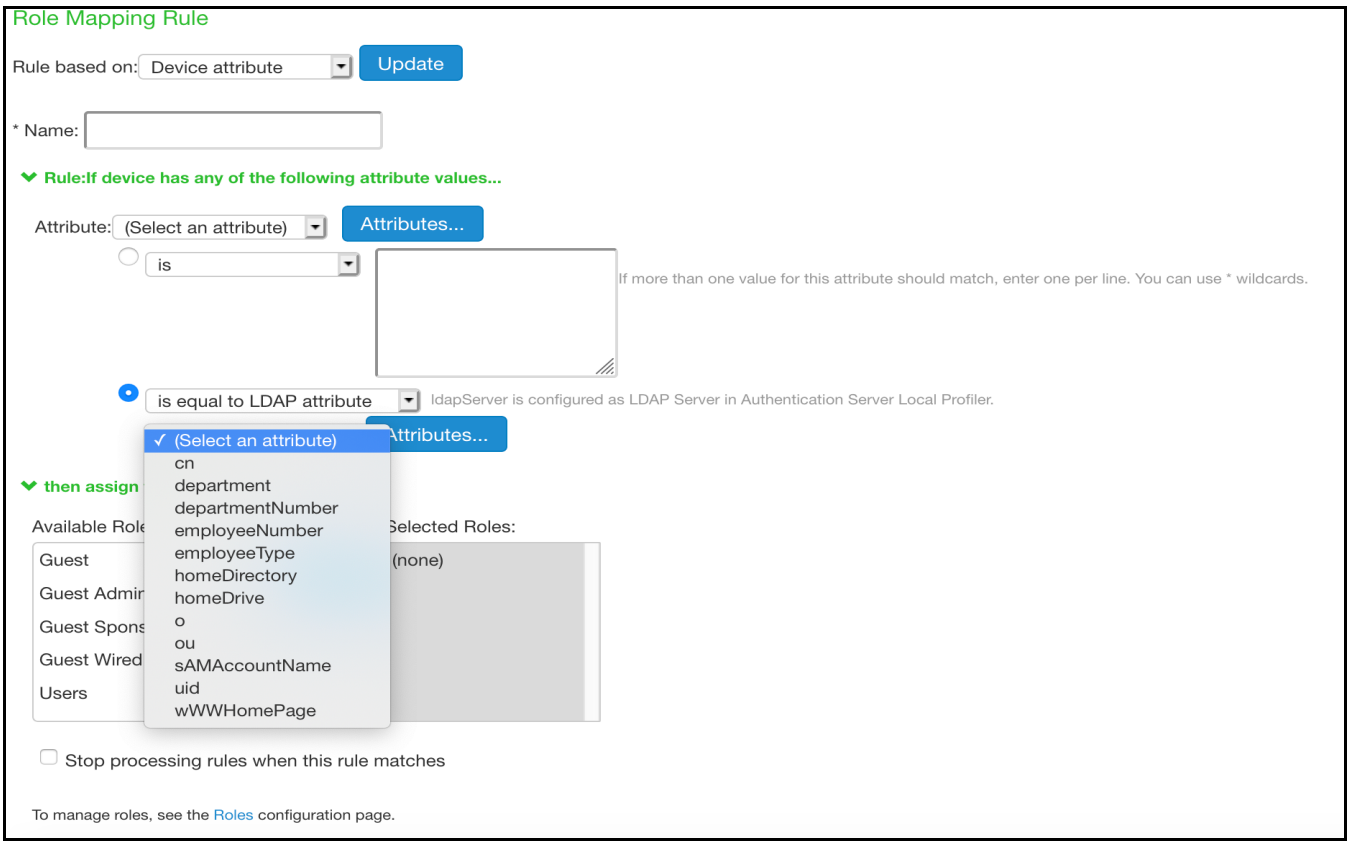
a. Select the attributes based on the new device attributes that are now available in the attributes drop-down field. When setting the attribute value, make sure the value you enter is an exact match for the value displayed in the Device Discovery Report table. Wildcards (* and ?) can be used in the attribute value.

Figure 26 Creating New Role Mapping Rule



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

Figure 27 Creating New Role Mapping Rule with LDAP Attributes



9. Assign the roles and click **Save Changes**.

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

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

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

Attribute Name	Description	Values/Example
antivirus_name	The name of the antivirus running on the device	MacAfee, Symantec Endpoint Protection, etc.
antivirus_status	The status of the antivirus running on the device	Enabled or Disabled
antivirus_version	A check on the antivirus version running on the system is up to date or not	Outdated or Current
Category	The category of the device. All devices are broadly classified into 30+ different categories.	Windows, Linux, Android, etc.
Custom	The administrator defined value(s) for the device.	Administaror defined values
Domain	The domain name of the device	Administaror defined values

Attribute Name	Description	Values/Example
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 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, Unapproved, or Temporarily Approved
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

Overview

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

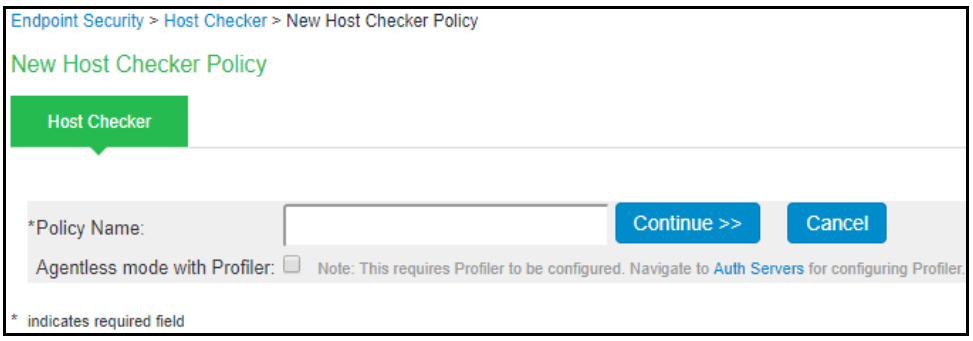
Note: ESAP package 3.4.5 or higher supports the latest rule type updates.

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.**

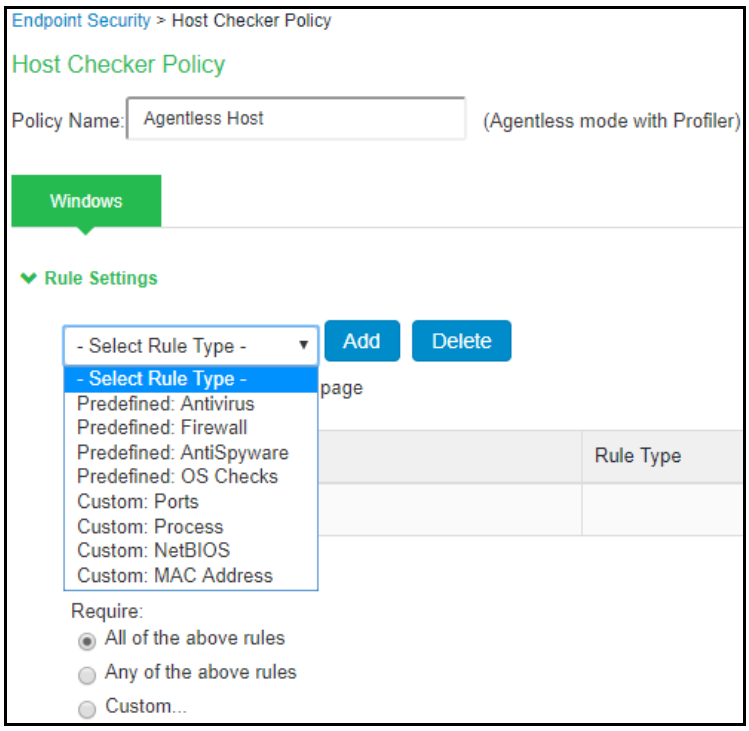
Figure 28 Host Checker Policy Creation for Agentless mode



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**.

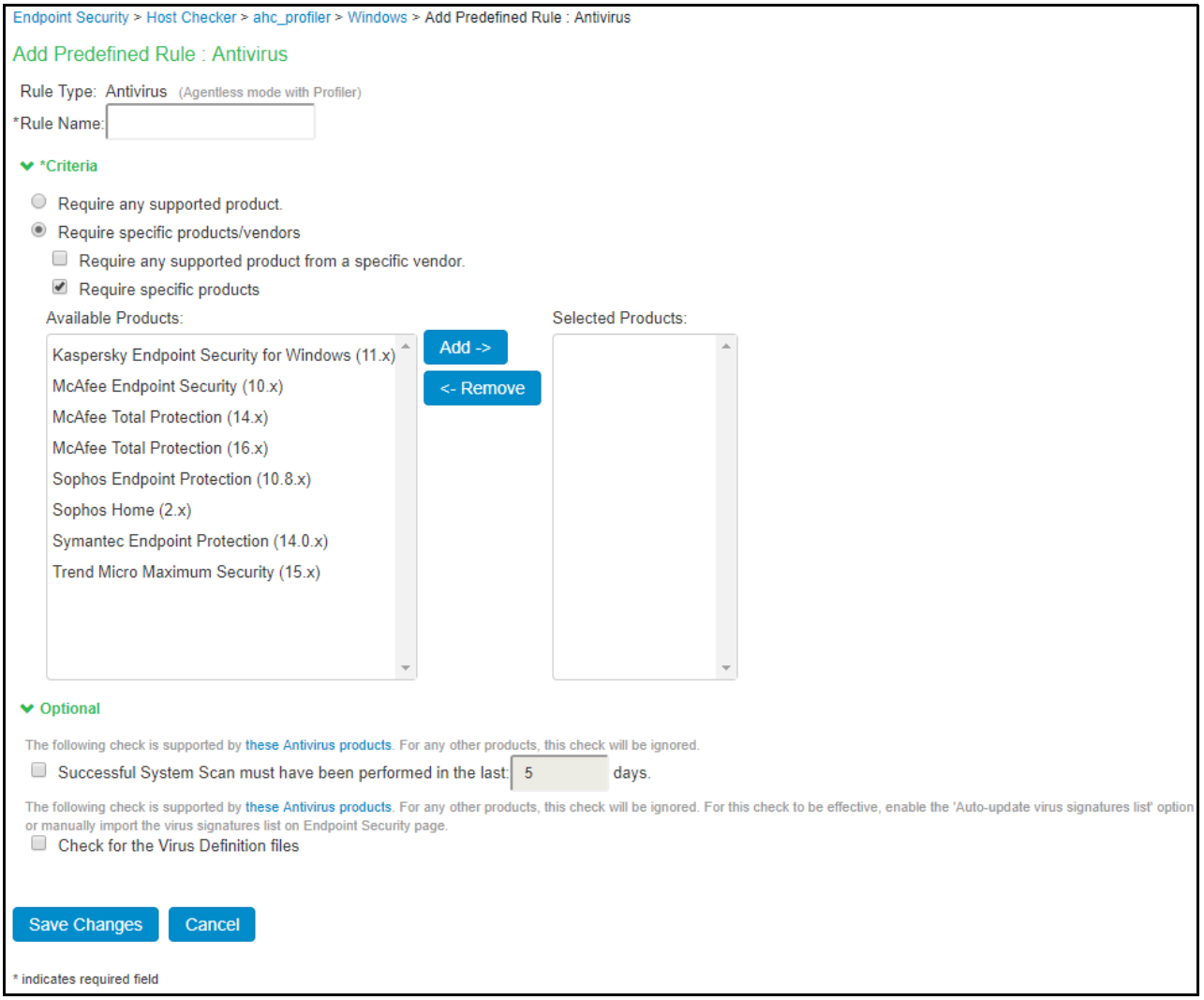
Figure 29 Host Checker Rule Types for Agentless mode



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**.

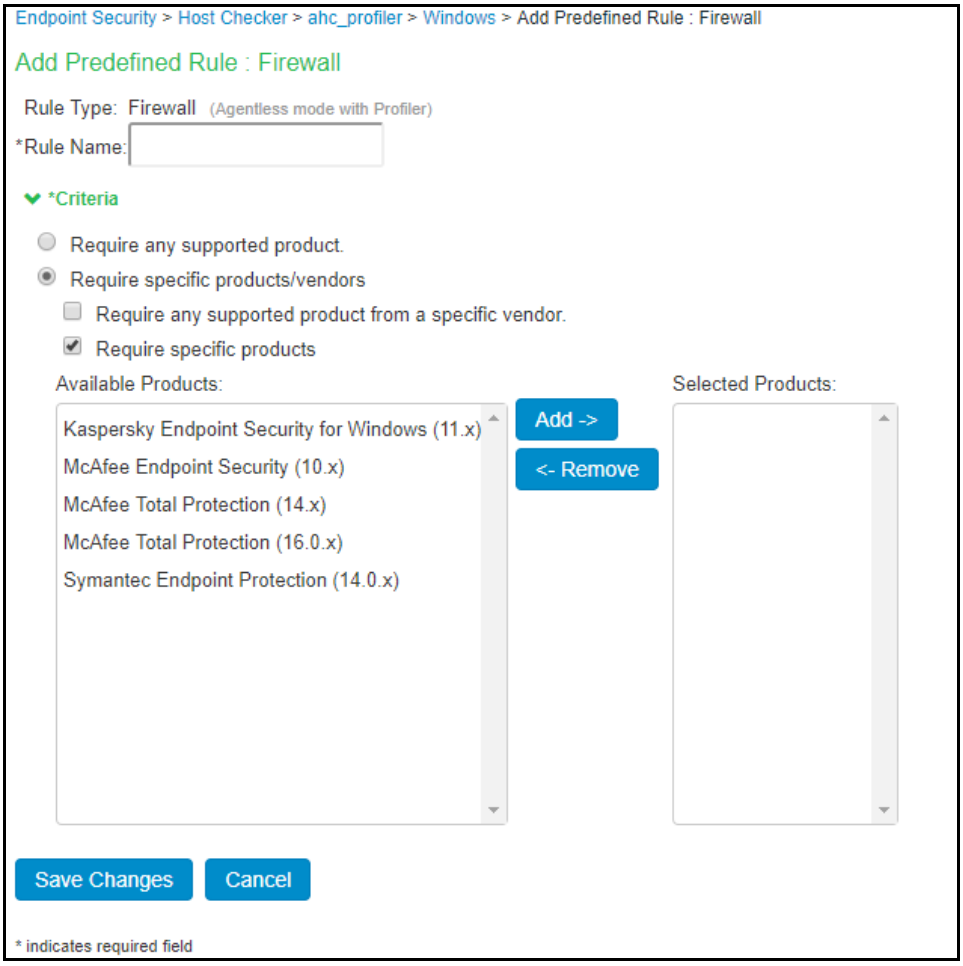
Figure 30 Antivirus Rule Type for Agentless mode



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

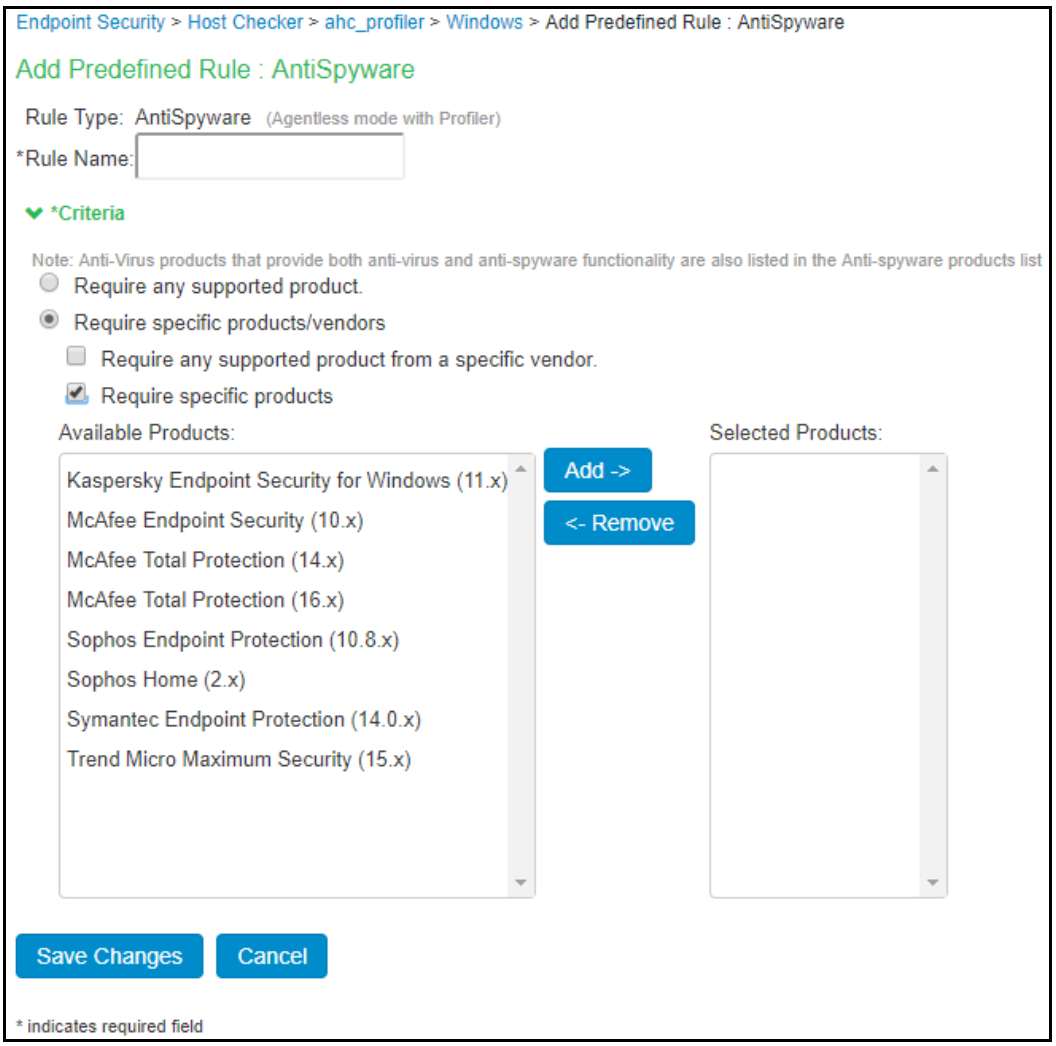
   Enter the **Rule Name**, select required **Criteria** and click **Save Changes**.

Figure 31 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**.

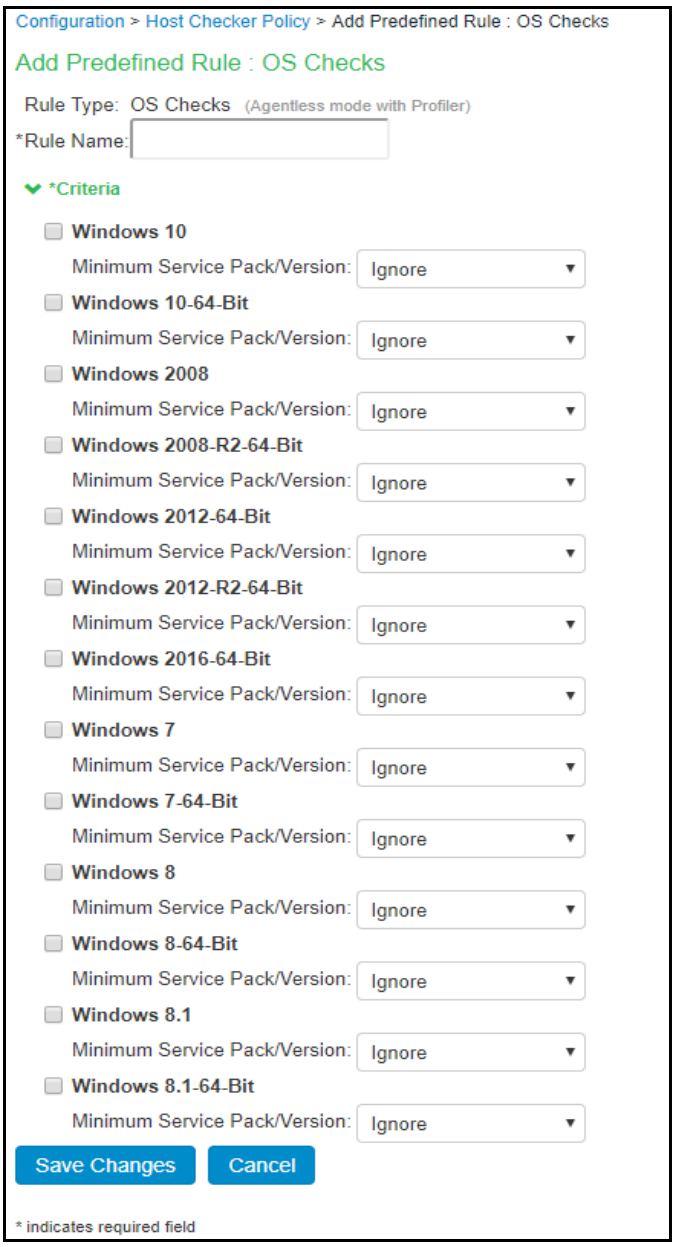
Figure 32 AntiSpyware Rule Type for Agentless mode



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**.

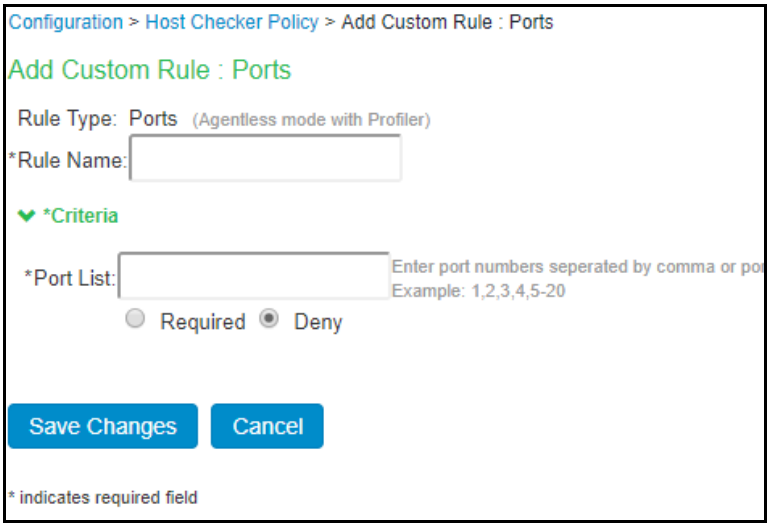
Figure 33 OS Checks Rule Type for Agentless mode



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**.

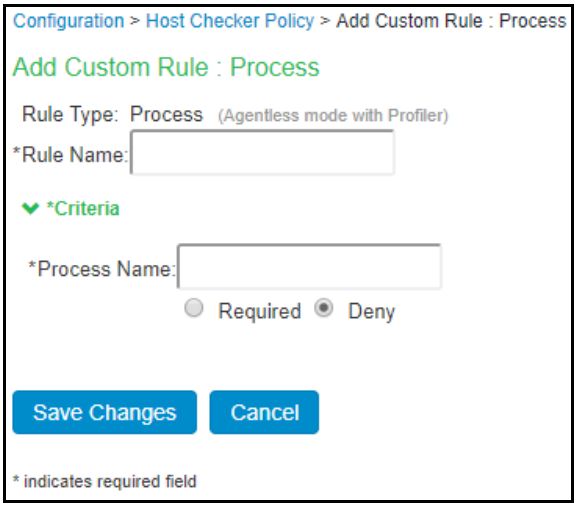
Figure 34 Ports Rule Type for Agentless mode



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**.

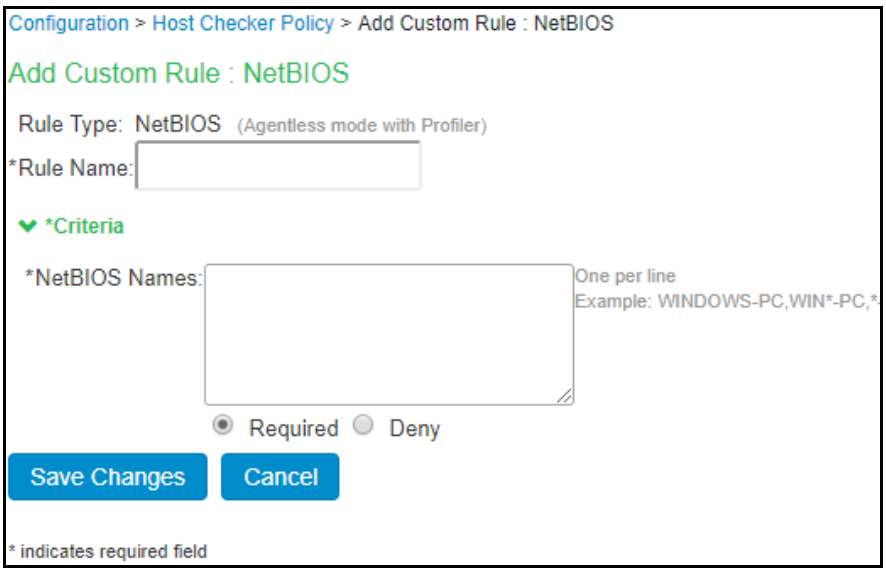
Figure 35 Process Rule Type for Agentless mode



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**.

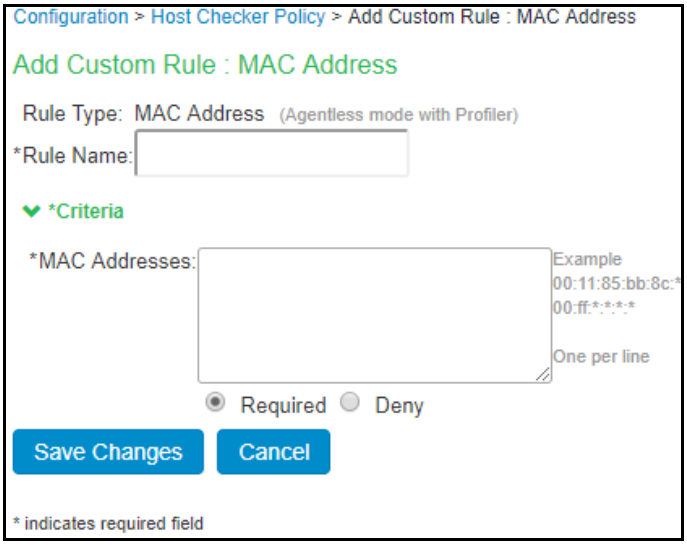
Figure 36 NetBIOS Rule Type for Agentless mode



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 37 MAC Address Rule Type for Agentless mode



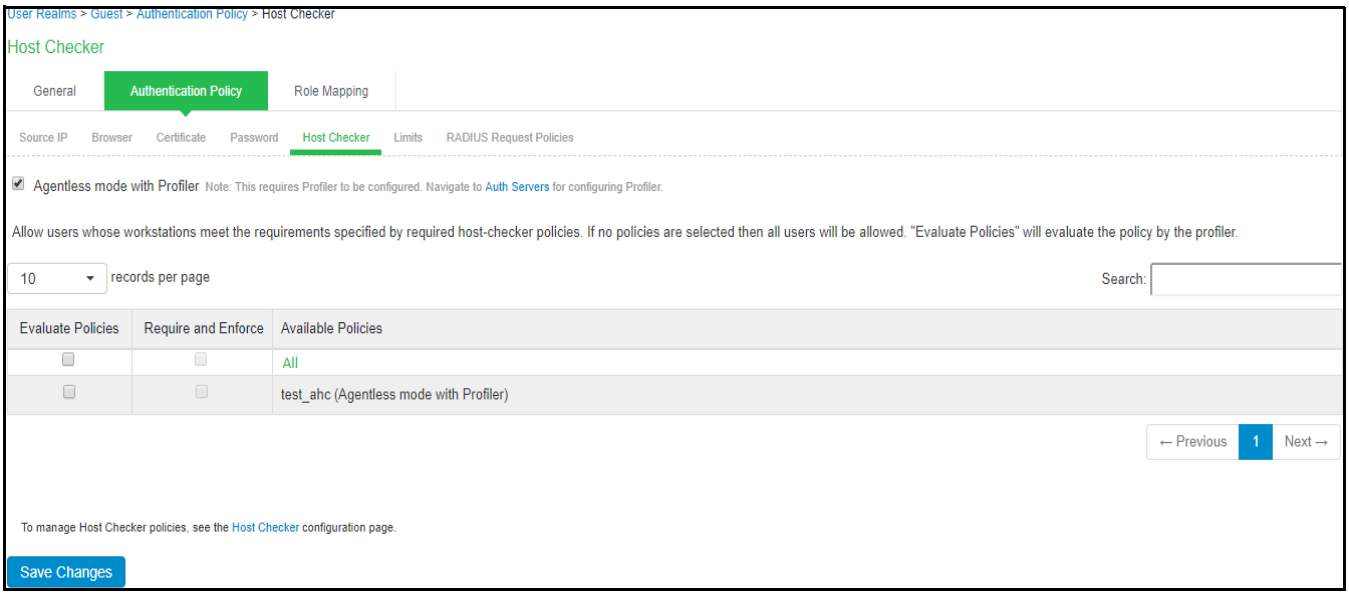
5. On adding the Rule Types, select the required option for rules, **Remediation** and **Dashboard Reporting** options and click **Save Changes**.

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.

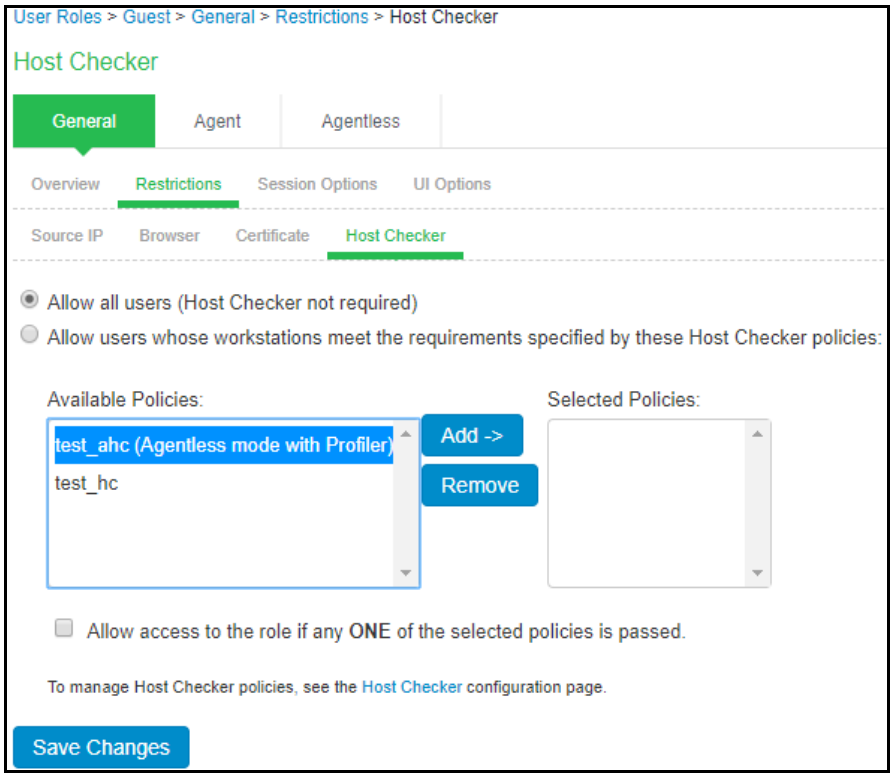
Figure 38 Policy enforcement for Agentless mode with Profiler on User Realm



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 39 Policy enforcement for Agentless mode with Profiler on User Role



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 helps to troubleshoot, backup database, or restore the database in case of any crash or data loss.

Navigate to **Maintenance > Import/Export** to import or export the profiler database.

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

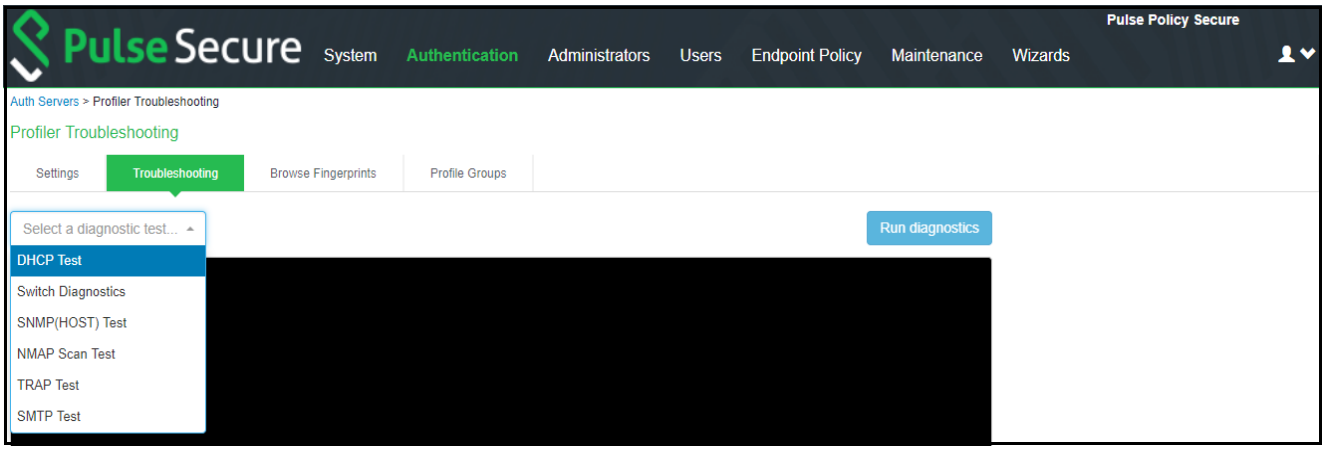
The following tests helps to identify and solve basic problems associated with configurations of the Profiler.

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

To execute the tests, perform the following steps:

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

Figure 40 Troubleshooting



Diagnostic Logs

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

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

Profiler Logs

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

To see the Profiler logs in the Event log, navigate to **Log/Monitoring** > **Events** > **Log Settings** and select **Profiler Events**.

Figure 41 List of Events to Log

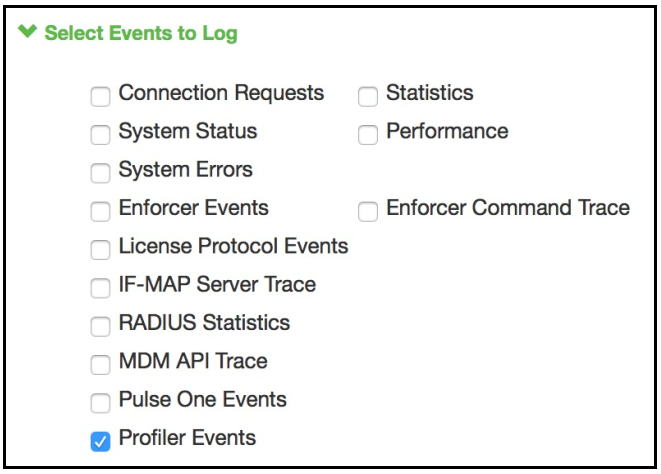


Table 1 Profiler logs

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

Event ID	Description	Log Type
ADM31444	WMI User added	Admin logs
ADM31445	WMI User modified	Admin logs
ADM31446	WMI User deleted	Admin logs
ADM31458	Profiler API keys retrieved Success/Failure	Admin logs
ADM31573	Device(s) are deleted from Device Discovery Report	Admin logs
ADM31591	Device updated in Device Discovery report.	Admin logs
ADM31595	Device added in Device Discovery report.	Admin Logs
ADM31631	Device addition failed in Device Discovery Report.	Admin Logs
ADM31634	Profile modified successfully	Admin logs
ADM31635	Profile modification is deleted successfully	Admin logs
ADM31636	Import from CSV succeeded	Admin logs
ADM31637	Import from CSV failed	Admin logs
ADM31701	On-Demand Subnet Scan triggered by admin [With subnet and collector details]	Admin logs
ADM31702	On-Demand Subnet Scan stopped by admin	Admin logs
ADM31730	Profile Group created	Admin logs
ADM31731	Profile Group updated	Admin logs
ADM31732	Profile Group deleted	Admin logs
ADM31759	Purge Initiated! Device(s) will be aged out from Device Discovery Report.	Admin logs
PRO31865	For start and stop of polling and which server is being polled currently	Event Logs
PRO31866	Any issues when polling occurs	Event 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

Event ID	Description	Log Type
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
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

Event ID	Description	Log Type
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

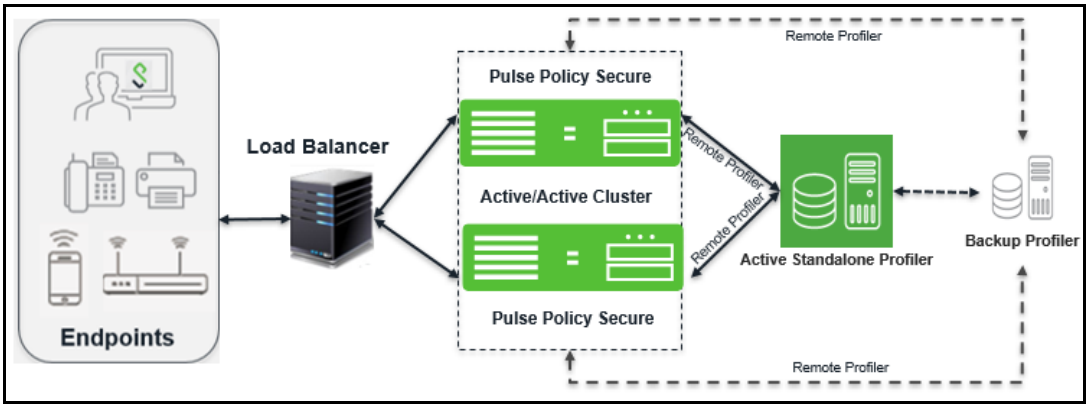
Standalone Profiler can be deployed as an independent appliance. All PPS and PCS appliances communicate with this Standalone Profiler for authorization.

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 unclustered set) of PPS appliances.

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

Figure 42 Example of a Standalone Profiler deployed in a typical PPS Active/Active cluster



When user connects to a PCS or PPS and starts a session:

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

Backup and recovery

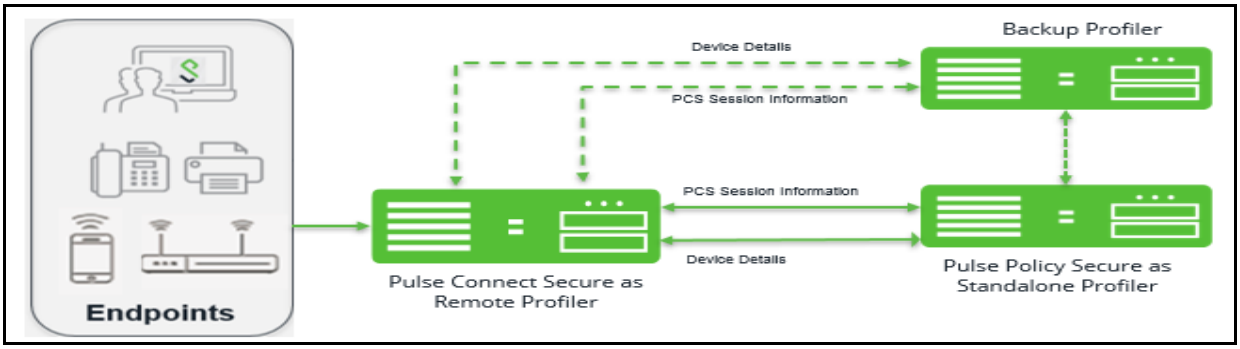
When the forwarder fails to connect to the Standalone Profiler, the forwarder sends the profiled endpoint information to the Backup Standalone server. On establishing the connection with the primary standalone profiler, the forwarder sends the latest information to sync with the primary standalone profiler.

Remote Profiler

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

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

Figure 43 Example of a Remote Profiler



Backup and recovery

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

Profiling devices in branch offices

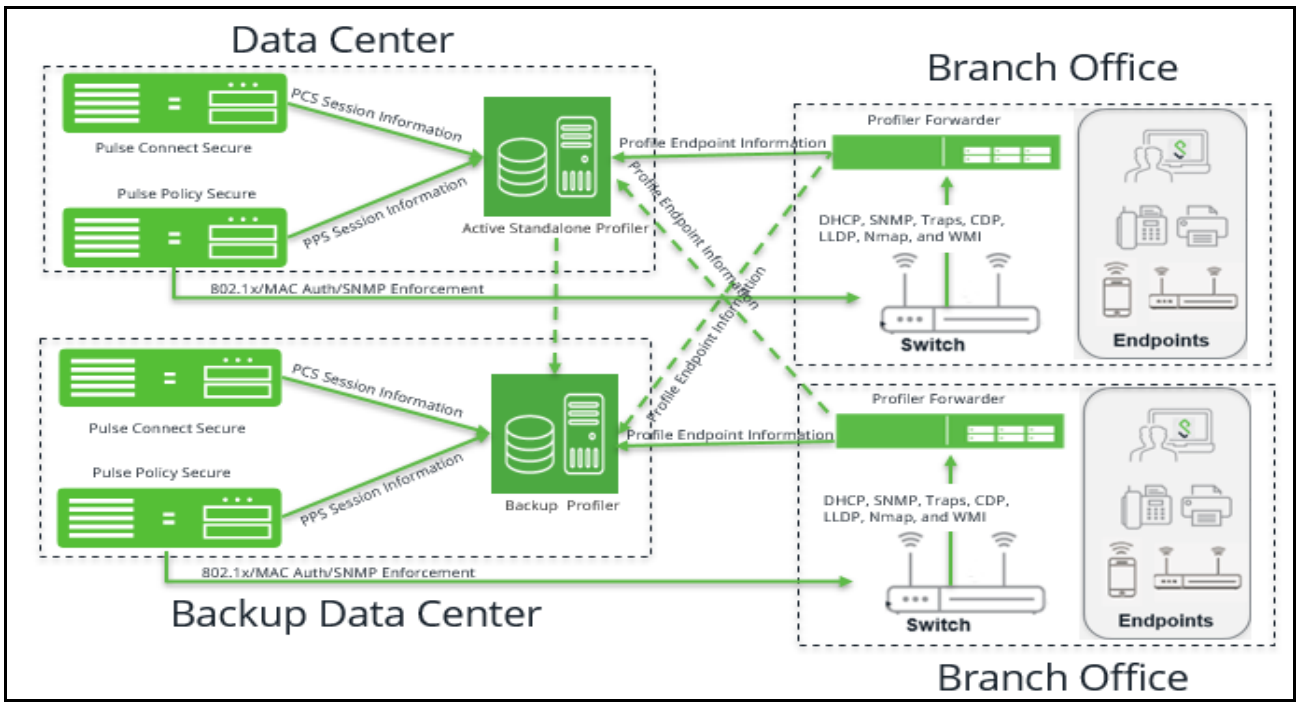
If forwarder uses 9.1R8 version, the standalone profiler must also use 9.1R8 version. Standalone profiler less than 9.1R8 version is not supported.

Using Profiler Forwarder

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

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

Figure 44 Example of a Profiler and Forwarder deployed across WAN



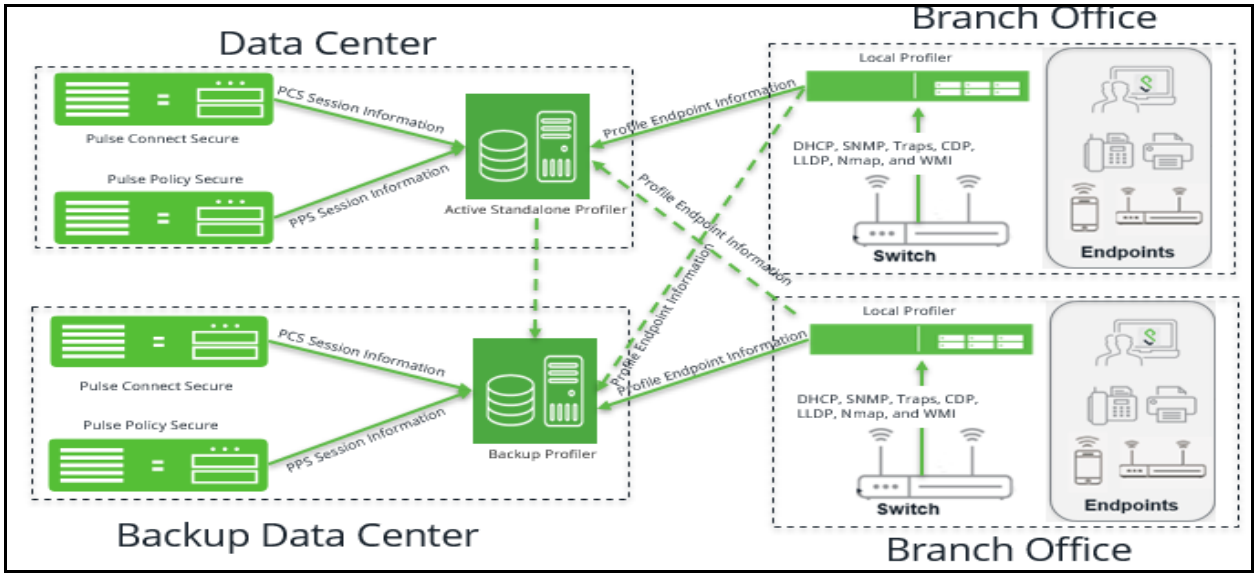
The Profiler Forwarder is a physical or virtual appliance with distinctive feature license called Profiler Forwarder license. The Profiler Forwarder enables the Profiler to run locally, profile the endpoints, and send the profiled information to the central Standalone Profiler periodically (default: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

Backup and recovery

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

Using Linked Profiler (With PPS Functionality)

Figure 45 Example of a Profiler with PPS functionality deployed across WAN



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

Backup and recovery

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