Pulse Secure®

Pulse Policy Secure: Admission Control using McAfee ePO

Deployment Guide

Product Release	9.1R5
Published	June 2020
Document Version	1.0

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

www.pulsesecure.net

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: Admission Control using McAfee ePO

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.

Alert-Based Admission Control with McAfee ePolicy Orchestrator (ePO)

Purpose of this Guide

This guide describes how to configure Pulse Policy Secure (PPS) to provide Alert-based admission control protection for your network using McAfee ePolicy Orchestrator (ePO).

Overview

This section describes how to integrate McAfee ePO device with PPS to support alert-based admission control in your network.

Prerequisites

This guide assumes you are familiar with the use of the following products and their related terminology.

- Pulse Policy Secure at version 9.1R5.
- McAfee ePolicy Orchestrator (ePO) version 5.9.0 and above

Pulse Policy Secure (PPS) integration with the McAfee ePolicy Orchestrator (ePO) provides complete visibility of network endpoints and provide end to end network security. The PPS integration with McAfee ePO allows Admin to perform user access control based on alerts received from the McAfee ePO.

If ePO detects that an endpoint on the network has become non-compliant, ePO can send PPS the non-compliant IP address and an event label. PPS resolves the event as a property on the endpoint, and can take automated actions until the endpoint is remediated and becomes compliant.

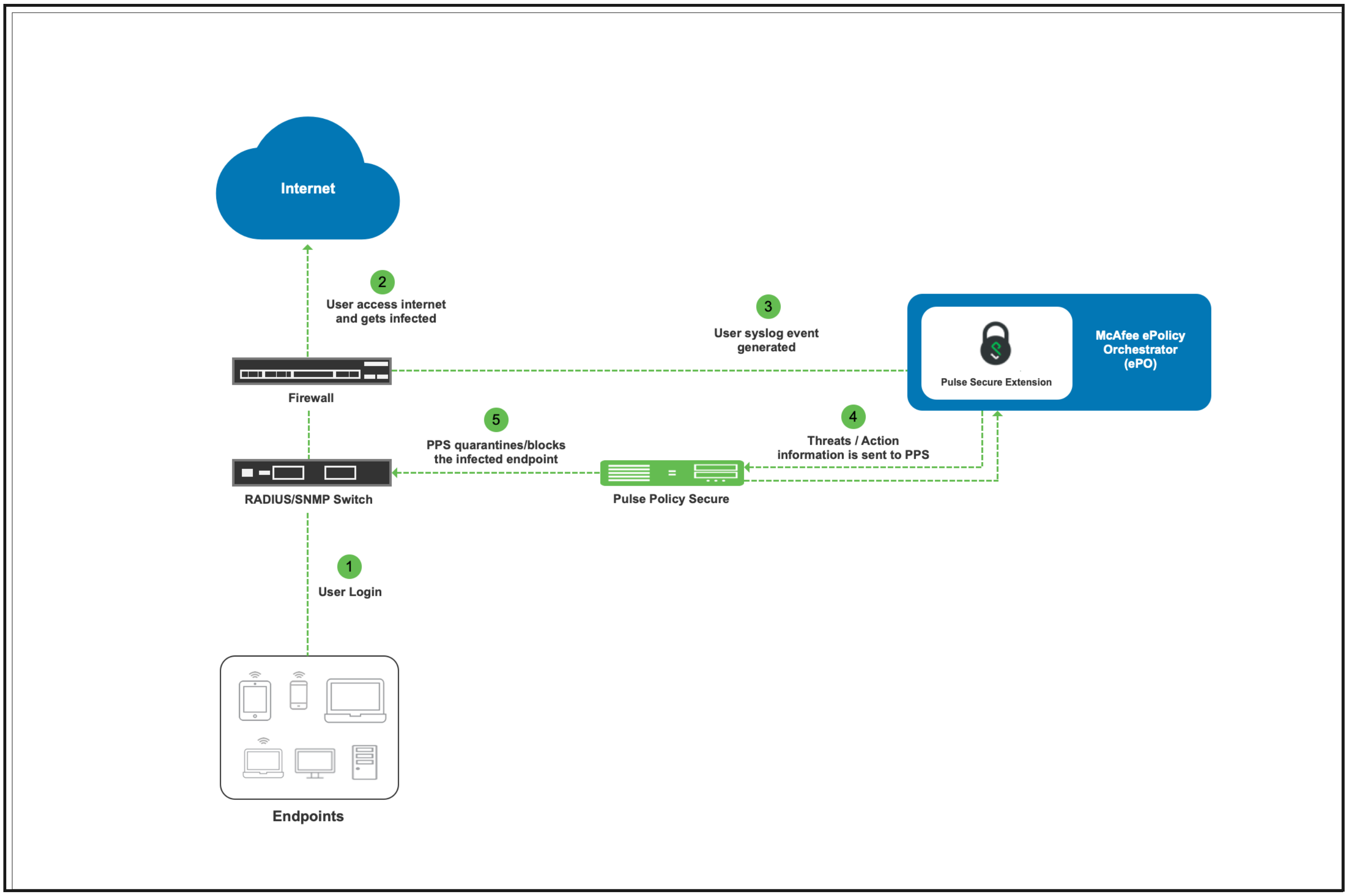
The authentication process is described below:

1. User downloads a malicious file from the Internet. The perimeter firewall scans the file and, based on user-defined policies, sends the file for analysis.
2. McAfee agent running on the Endpoint detects the malicious activity and sends the information to McAfee ePO.
3. Based on the alert rules configured on McAfee ePO, it generates alerts and sends automatically to PPS with the help of Pulse Policy Secure Extension.

4. McAfee ePO sends alert to PPS to isolate the endpoint from the network. The Alert includes severity for the affected endpoint to PPS.
5. The PPS server quarantines/blocks the endpoint based on the configured Admission control policies.

Note: McAfee ePO receives Threat events from different Endpoint Security (ENS) modules like Firewall, Threat Intelligence Exchange (TIE)/Adaptive Threat Protection (ATP), Threat Prevention and others.

Figure 1 Deployment using PPS, McAfee ePO and Firewall


Internet
2
User access internet and gets infected
3
User syslog event generated
Pulse Secure Extension
McAfee ePolicy Orchestrator (ePO)
Firewall
5
PPS quarantines/blocks the infected endpoint
4
Threats / Action information is sent to PPS
RADIUS/SNMP Switch
Pulse Policy Secure
1
User Login
Endpoints

In this example, the endpoint is connected to a third-party switch. The switch has 802.1X/MAB authentication enabled. As an alternate, SNMP enforcement mechanism can also be used.

Summary of Configuration

To prepare your network to perform alert-based admission control using Pulse Policy Secure, McAfee ePolicy Orchestrator (ePO) and Firewall, perform the following tasks:

- "Configuring PPS with McAfee ePO" on page 5
- "Configuring McAfee ePO" on page 9

The following sections describe each of these steps in detail.

Configuring PPS with McAfee ePO

The PPS configuration requires defining the McAfee ePO as a client in PPS. PPS acts as a REST API server for McAfee ePO.

A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the basic PPS configurations such as creating an authentication server, authentication realm, user roles, and role mapping rules.
- Configure McAfee ePolicy Orchestrator (ePO) as a client in PPS. PPS acts as a REST API Server for McAfee ePO. The REST API access for the admin user needs to be enabled by accessing the serial console or alternatively from the PPS admin UI (Authentication > Auth Server > Administrators > Users > click “admin”, enable Allow access to REST APIs).
- Configure PPS to block/quarantine the endpoint based on the threat prevention policy.
- Configure the Switches/WLC as RADIUS Client in PPS (Endpoint Policy > Network Access > Radius Clients > New Radius Client). Switch should be configured with PPS as a RADIUS server.
- Configure RADIUS return attribute policies to define the action upon receiving the event.

Note: Ensure that PPS has the endpoint IP Address for the enforcement to work correctly.

This section covers the following topics:

- “Admission Control Template” on page 5
- “Admission Control Client” on page 6
- “Admission Control Policies” on page 7

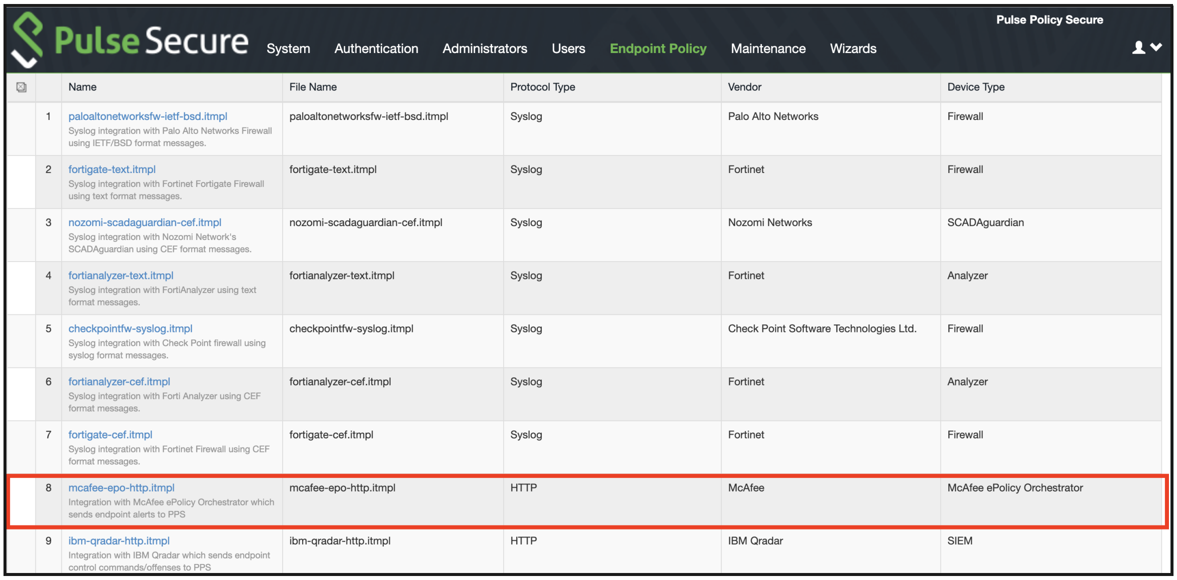
Admission Control Template

The admission control template provides the list of possible events that can be received from the network security device along with regular expression to parse the message. The template also provides possible actions that can be taken for an event. PPS is loaded with default templates for McAfee ePolicy Orchestrator (ePO).

To view the admission control template in PPS:

1. Select **Endpoint Policy** > **Admission Control** > **Templates**.

Figure 2 McAfee ePO Template



	Name	File Name	Protocol Type	Vendor	Device Type
1	paloaltonetworksfw-ietf-bsd.itmpl Syslog integration with Palo Alto Networks Firewall using IETF/BSD format messages.	paloaltonetworksfw-ietf-bsd.itmpl	Syslog	Palo Alto Networks	Firewall
2	fortigate-text.itmpl Syslog integration with Fortinet Fortigate Firewall using text format messages.	fortigate-text.itmpl	Syslog	Fortinet	Firewall
3	nozomi-scadaguardian-cef.itmpl Syslog integration with Nozomi Network's SCADAguardian using CEF format messages.	nozomi-scadaguardian-cef.itmpl	Syslog	Nozomi Networks	SCADAguardian
4	fortianalyzer-text.itmpl Syslog integration with FortiAnalyzer using text format messages.	fortianalyzer-text.itmpl	Syslog	Fortinet	Analyzer
5	checkpointfw-syslog.itmpl Syslog integration with Check Point firewall using syslog format messages.	checkpointfw-syslog.itmpl	Syslog	Check Point Software Technologies Ltd.	Firewall
6	fortianalyzer-cef.itmpl Syslog integration with Forti Analyzer using CEF format messages.	fortianalyzer-cef.itmpl	Syslog	Fortinet	Analyzer
7	fortigate-cef.itmpl Syslog integration with Fortinet Firewall using CEF format messages.	fortigate-cef.itmpl	Syslog	Fortinet	Firewall
8	mcafee-epo-http.itmpl Integration with McAfee ePolicy Orchestrator which sends endpoint alerts to PPS	mcafee-epo-http.itmpl	HTTP	McAfee	McAfee ePolicy Orchestrator
9	ibm-qradar-http.itmpl Integration with IBM Qradar which sends endpoint control commands/offenses to PPS	ibm-qradar-http.itmpl	HTTP	IBM Qradar	SIEM

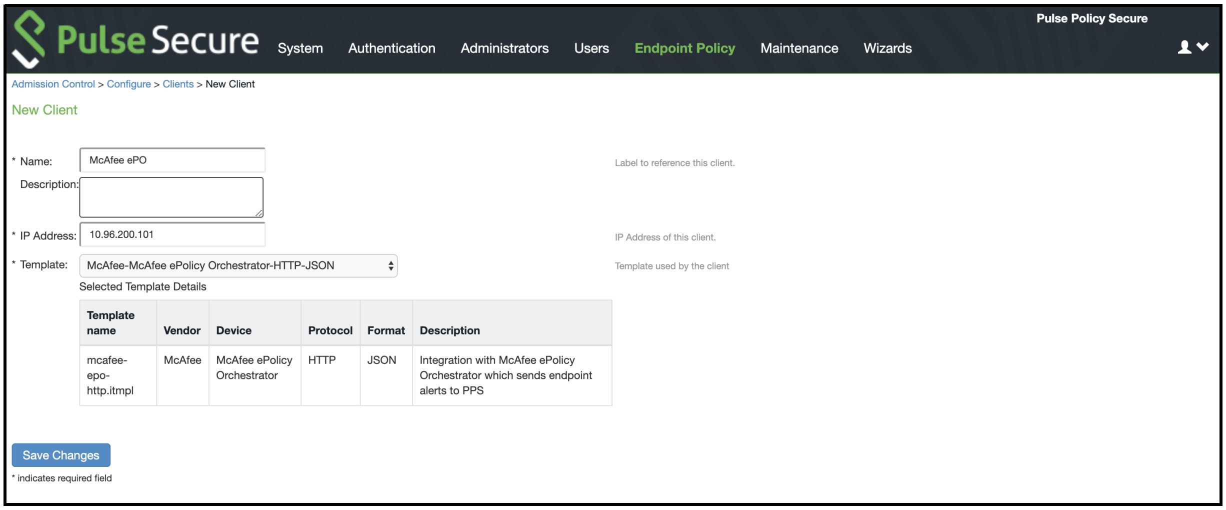
Admission Control Client

The admission control clients are the network security devices on which the REST API is enabled. McAfee ePO forwards the events to PPS through REST API interface.

To add McAfee ePO as a client:

1. Select **Endpoint Policy** > **Admission Control** > **Clients**.
2. Click **New Client**.
3. Enter the name.
4. Enter the description.
5. Enter the IP address of the client.
6. Under Template, select **McAfee-McAfee ePolicy Orchestrator-HTTP-JSON**.
7. Click **Save Changes**.

Figure 3 Template



Admission Control > Configure > Clients > New Client

New Client

* Name: McAfee ePO — Label to reference this client.

Description:

* IP Address: 10.96.200.101 — IP Address of this client.

* Template: McAfee-McAfee ePolicy Orchestrator-HTTP-JSON — Template used by the client

Selected Template Details

Template name	Vendor	Device	Protocol	Format	Description
mcafee-epo-http.itmpl	McAfee	McAfee ePolicy Orchestrator	HTTP	JSON	Integration with McAfee ePolicy Orchestrator which sends endpoint alerts to PPS

Save Changes

* indicates required field

Note: A subset of events supported by McAfee ePO is added in the default template. A new template can be created by Admin and has to be uploaded on PPS for supporting any additional events apart from the one's in the default template.

Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity information received from the network security device.

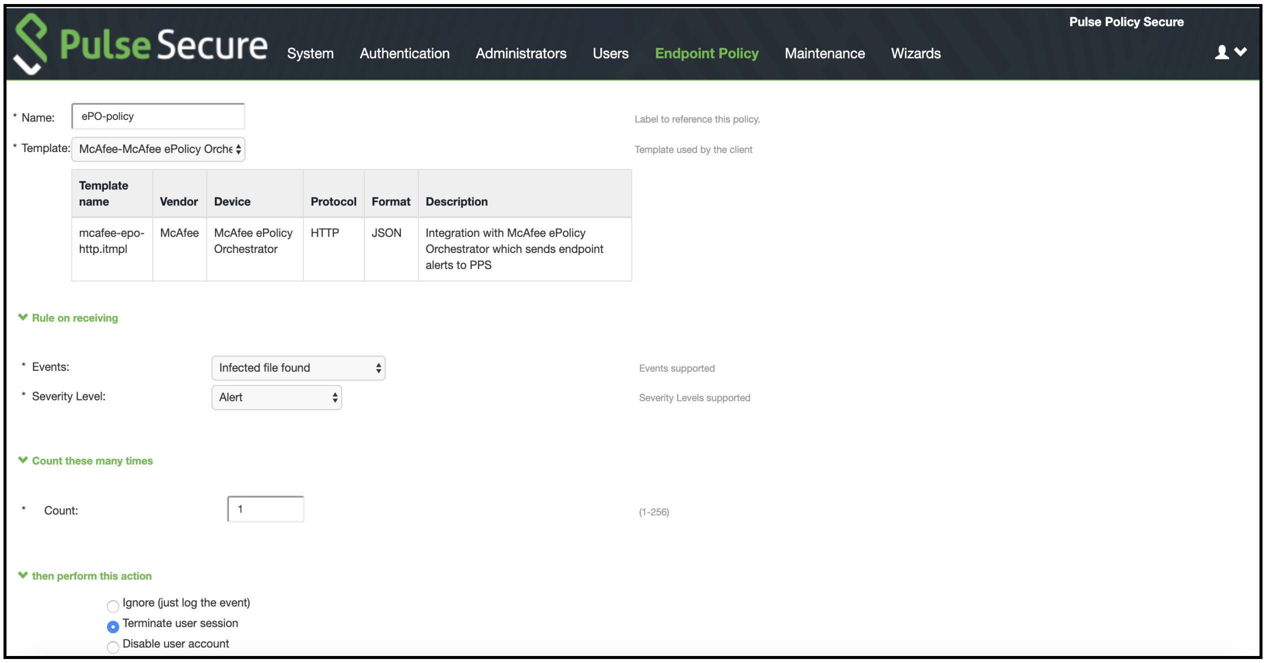
1. To view and add the new integration policy:
2. Select **Endpoint Policy > Admission Control > Policies**.
3. Click **New Policy**.
4. Enter the policy name.
5. Select **McAfee-McAfee ePolicy Orchestrator-HTTP-JSON** as a template.
6. Under Rule on Receiving, select the event type and the severity level. The event types and the severity level are based on the selected template.
7. Under then perform this action, select the desired action.
   - Ignore (log the event) —Received event details are logged on the PPS and no specific action is taken.
   - Terminate user session—Terminates the user session on the PPS.
   - Disable user account—Disables the user account.
   - Replace user’s role with the configured remediation role. For example, Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted, Users.
   - Block the endpoint from authenticating the network.

   Note: Admission Control Policy action is not taken for endpoints behind Network Address Translation (NAT).

8. Under Roles, specify:

   - Policy applies to ALL roles—To apply the policy to all users.
   - Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
   - Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

Figure 4 Configuration Policies



* Name: ePO-policy — Label to reference this policy.
* Template: McAfee-McAfee ePolicy Orche — Template used by the client

Template name	Vendor	Device	Protocol	Format	Description
mcafee-epo-http.itmpl	McAfee	McAfee ePolicy Orchestrator	HTTP	JSON	Integration with McAfee ePolicy Orchestrator which sends endpoint alerts to PPS

Rule on receiving

* Events: Infected file found — Events supported
* Severity Level: Alert — Severity Levels supported

Count these many times

* Count: 1 — (1-256)

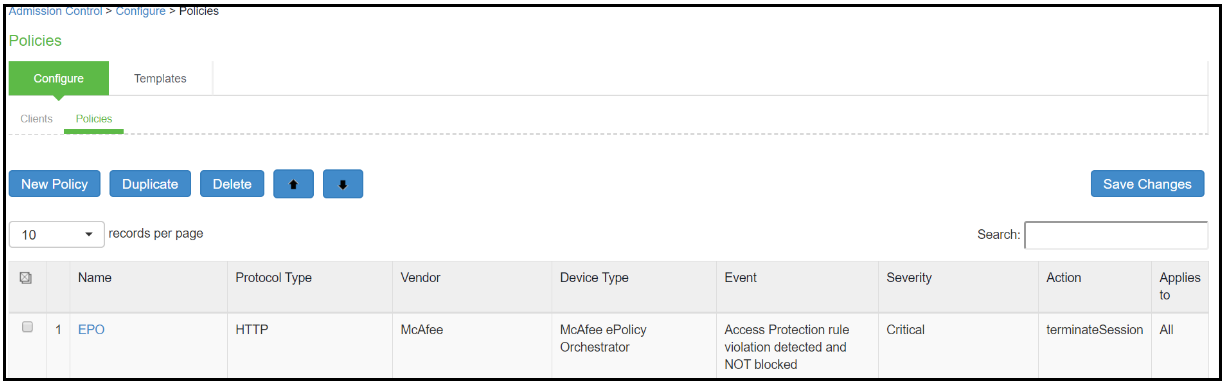
then perform this action

○ Ignore (just log the event)
● Terminate user session
○ Disable user account

9. Click **Save Changes**.

   Once the policy is created. You can see the summary page as shown below. The following page shows the different policies created for different events with different user roles.

Figure 5 Summary



10 records per page

☐		Name	Protocol Type	Vendor	Device Type	Event	Severity	Action	Applies to
☐	1	EPO	HTTP	McAfee	McAfee ePolicy Orchestrator	Access Protection rule violation detected and NOT blocked	Critical	terminateSession	All

Configuring McAfee ePO

This section covers the following topics:

- "Install Pulse Policy Secure Extension for McAfee ePO" on page 9
- "McAfee ePO Configuration" on page 10

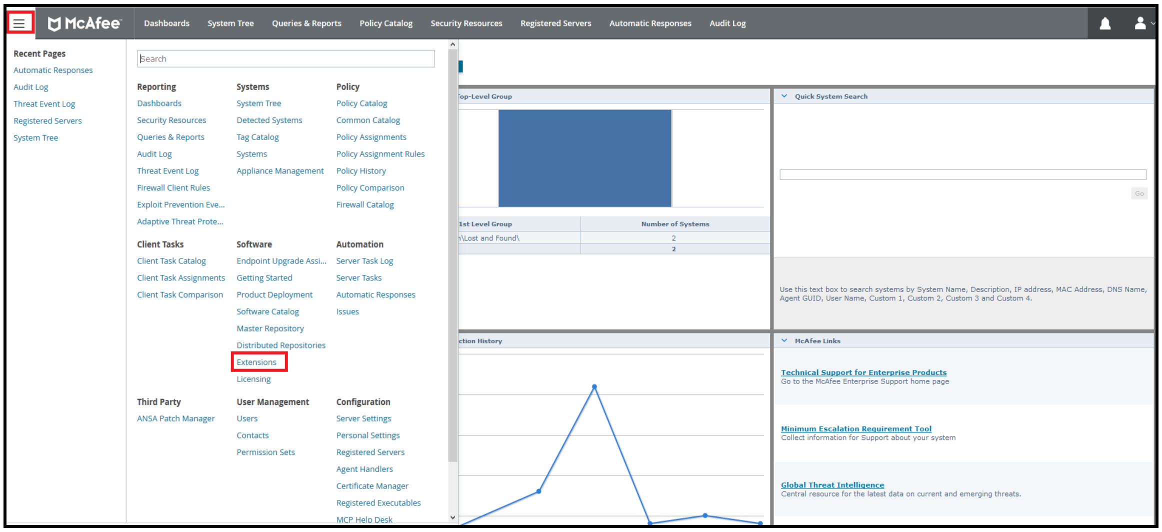
Install Pulse Policy Secure Extension for McAfee ePO

Download the PulsePolicySecureExt_1.0.0.zip file from Pulse Secure software downloads location and install it onto your McAfee ePO server.

To configure the Pulse Policy Secure extension on ePO server:

1. Log into McAfee ePO as an Admin user.
2. In the McAfee Dashboard, select the **Extensions**.

   Figure 6 McAfee extension



Use this text box to search systems by System Name, Description, IP address, MAC Address, DNS Name, Agent GUID, User Name, Custom 1, Custom 2, Custom 3 and Custom 4.

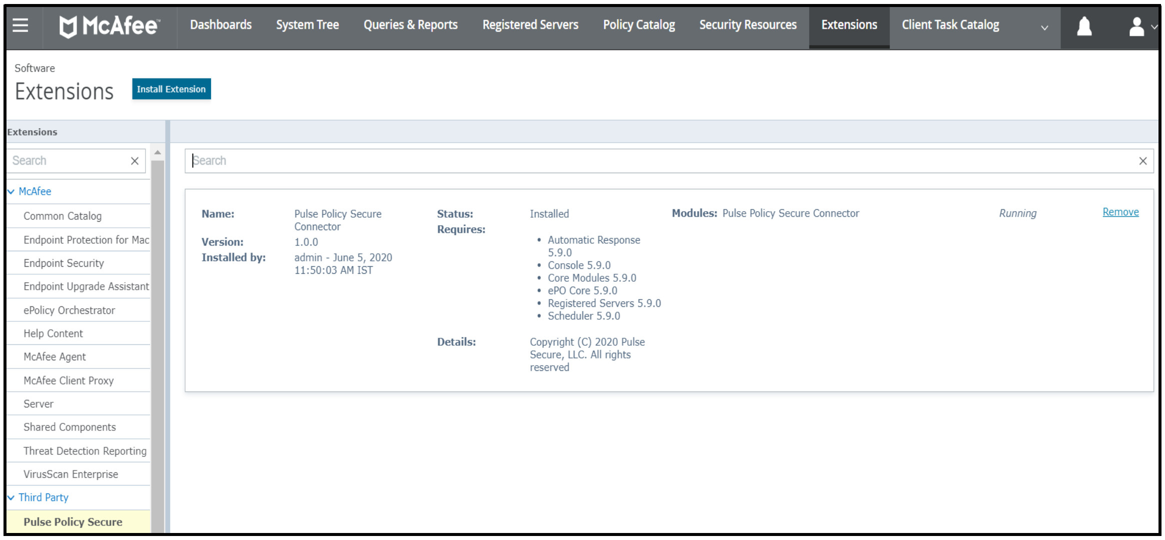
Go to the McAfee Enterprise Support home page

Collect information for Support about your system

Central resource for the latest data on current and emerging threats.

3. Click **Install Extension**.

   Figure 7 Install Extension



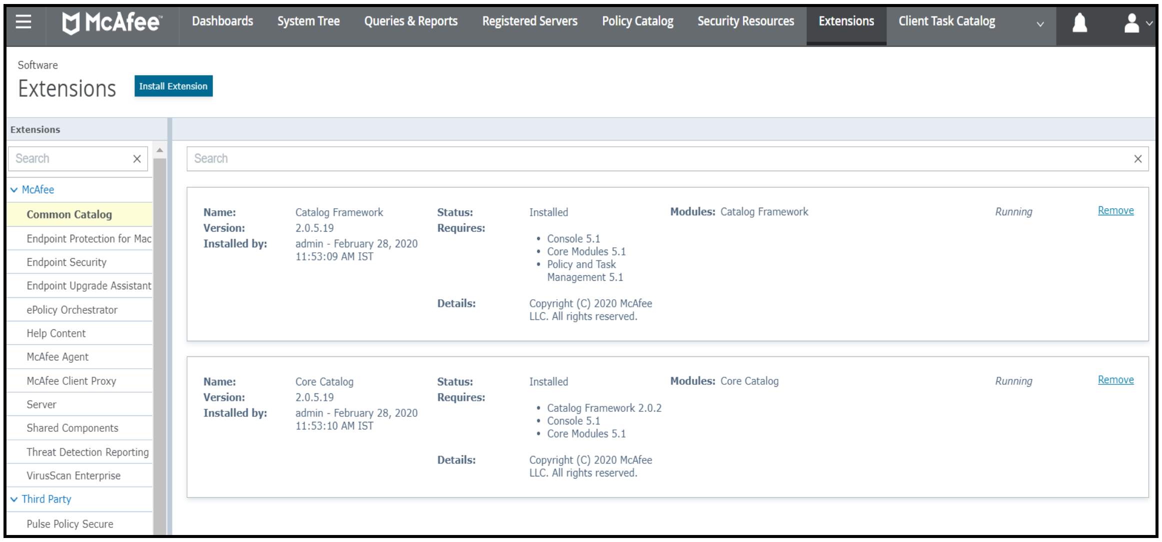
Name: Pulse Policy Secure Connector
Version: 1.0.0
Installed by: admin - June 5, 2020 11:50:03 AM IST
Status: Installed
Requires:
- Automatic Response 5.9.0
- Console 5.9.0
- Core Modules 5.9.0
- ePO Core 5.9.0
- Registered Servers 5.9.0
- Scheduler 5.9.0

Details: Copyright (C) 2020 Pulse Secure, LLC. All rights reserved
Modules: Pulse Policy Secure Connector
Running

4. Click Browse and upload the PulsePolicySecureExt_1.0.0.zip file to install the Pulse Policy Secure extension for McAfee.

5. After installation, Pulse Policy Secure extension for McAfee appears under Third Party section.

Figure 8 Pulse Policy Secure extension



Name: Catalog Framework
Version: 2.0.5.19
Installed by: admin - February 28, 2020 11:53:09 AM IST
Status: Installed
Requires:
- Console 5.1
- Core Modules 5.1
- Policy and Task Management 5.1

Details: Copyright (C) 2020 McAfee LLC. All rights reserved.
Modules: Catalog Framework
Running

Name: Core Catalog
Version: 2.0.5.19
Installed by: admin - February 28, 2020 11:53:10 AM IST
Status: Installed
Requires:
- Catalog Framework 2.0.2
- Console 5.1
- Core Modules 5.1

Details: Copyright (C) 2020 McAfee LLC. All rights reserved.
Modules: Core Catalog
Running

McAfee ePO Configuration

McAfee ePO framework supports extension/plugin specific to the vendors which can be used to send the information in the way understood by the vendors. There are two basic components which is used for this purpose in ePO:

- "Registered Servers" on page 11
- "Automatic Response" on page 12

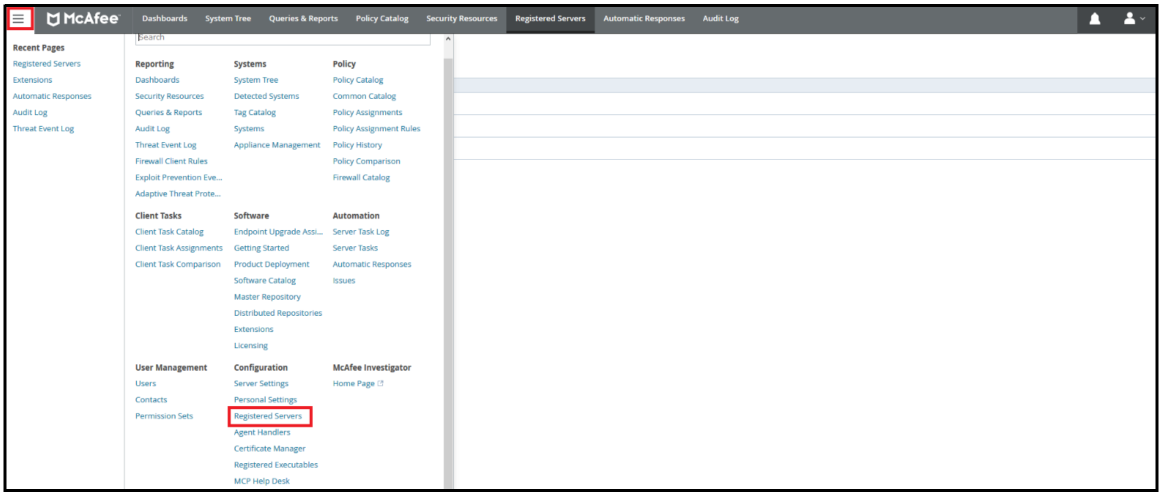
Registered Servers

Registered server in ePO is a server which is interested in the information/events received by ePO. ePO supports LDAP, SNMP, Syslog or ePO itself as Registered server by default. When extension/plugin is installed, PPS will be listed as Registered server, which is interested in Threat related events.

PPS can manage hosts in multiple subnets or multiple PPS devices can manage the hosts in the same subnet.

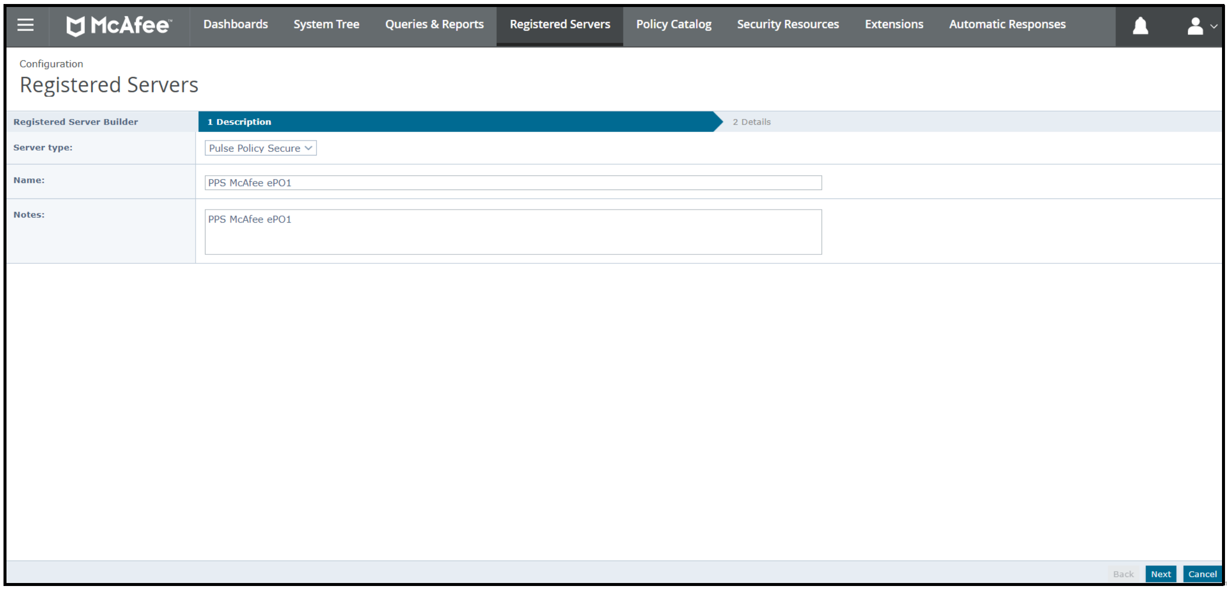
1. Log into McAfee ePO as an Admin user.
2. Open the Main Menu, under Configuration Click **Registered Servers**.

Figure 9 Configuration



3. Click **New Server**.
4. Select Server Type as **Pulse Policy Secure**.
5. Enter the name of the server.
6. Click **Next**.

Figure 10 Registered Servers



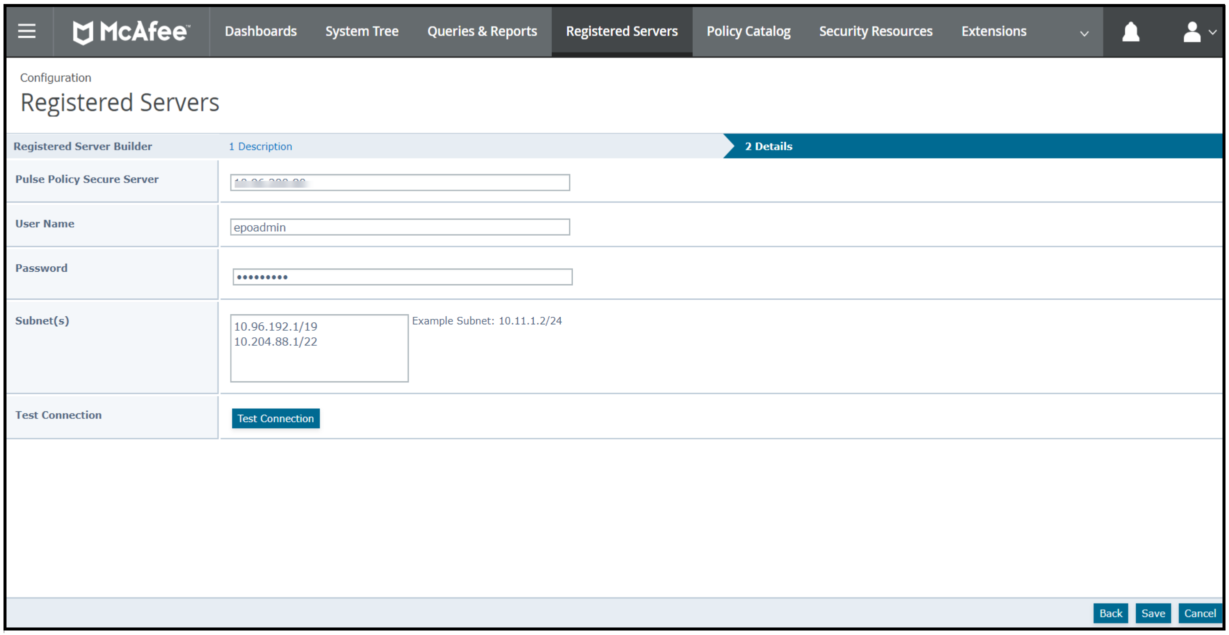
Server type: Pulse Policy Secure

Name: PPS McAfee ePO1

Notes: PPS McAfee ePO1

7. Enter PPS details: IP address of PPS, User Name, Password, Endpoint subnet(s) that PPS manages.
8. Click **Test Connection** to test the connectivity between PPS and McAfee ePO.
9. Click **Save**.

Figure 11 Registered Servers- PPS



Pulse Policy Secure Server: [redacted]

User Name: epoadmin

Password: •••••••••

Subnet(s):
10.96.192.1/19
10.204.88.1/22

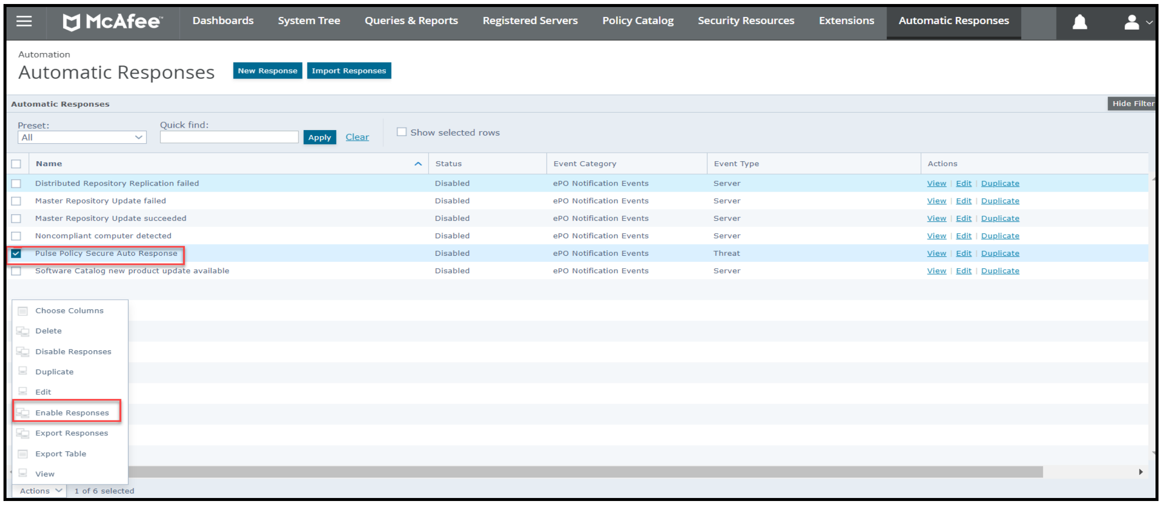
Example Subnet: 10.11.1.2/24

Automatic Response

Automatic response is a framework where admin can register for a specific Threat (or all the Threats/Events) information and invoke an action like "Send Mail", "Send SNMP Trap" and others. Automatic response is also listed. When PPS specific action is invoked, ePO will send the information to PPS (using REST API) configured as Registered server.

1. Login to ePO server as an Admin.
2. Under Automation, select **Automatic Response**.
3. Select **Pulse Policy Secure Auto Response** and click Actions and **Enable Responses**.

Figure 12 Auto Response



Automatic Responses

Preset: All

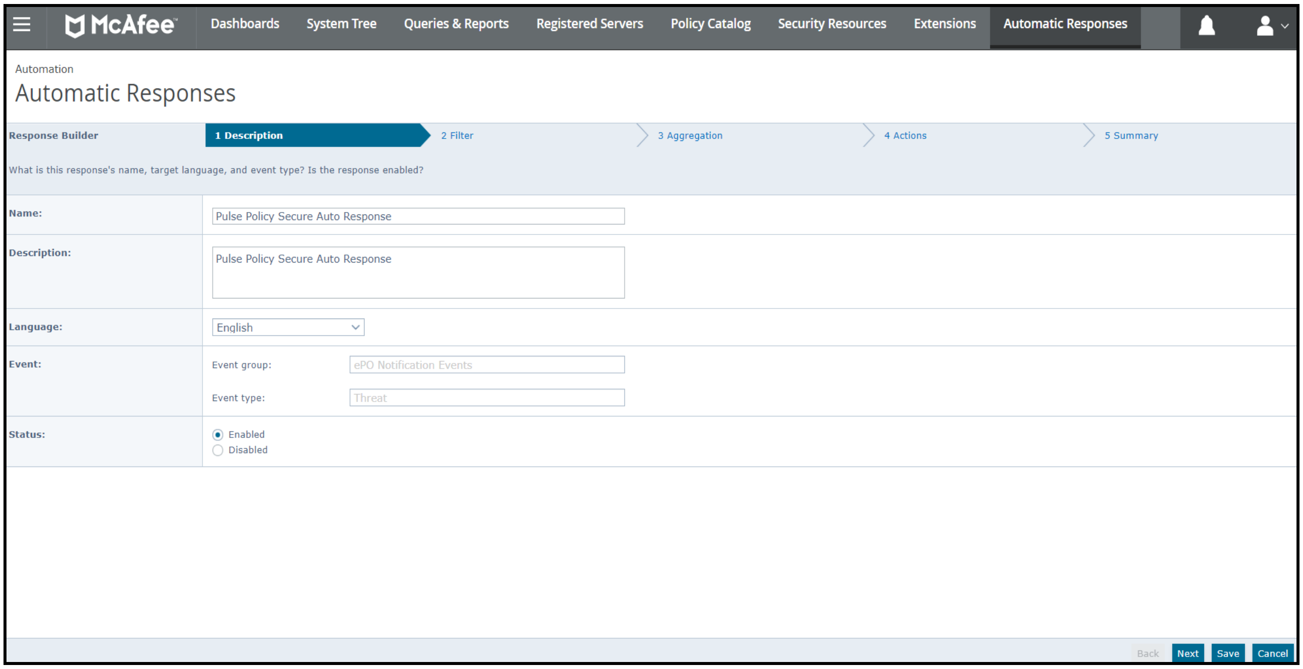
Quick find:

□ Show selected rows

	Name	Status	Event Category	Event Type	Actions
□	Distributed Repository Replication failed	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
□	Master Repository Update failed	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
□	Master Repository Update succeeded	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
□	Noncompliant computer detected	Disabled	ePO Notification Events	Server	View | Edit | Duplicate
☑	Pulse Policy Secure Auto Response	Disabled	ePO Notification Events	Threat	View | Edit | Duplicate
□	Software Catalog new product update available	Disabled	ePO Notification Events	Server	View | Edit | Duplicate

1 of 6 selected

Figure 13 Automatic Responses

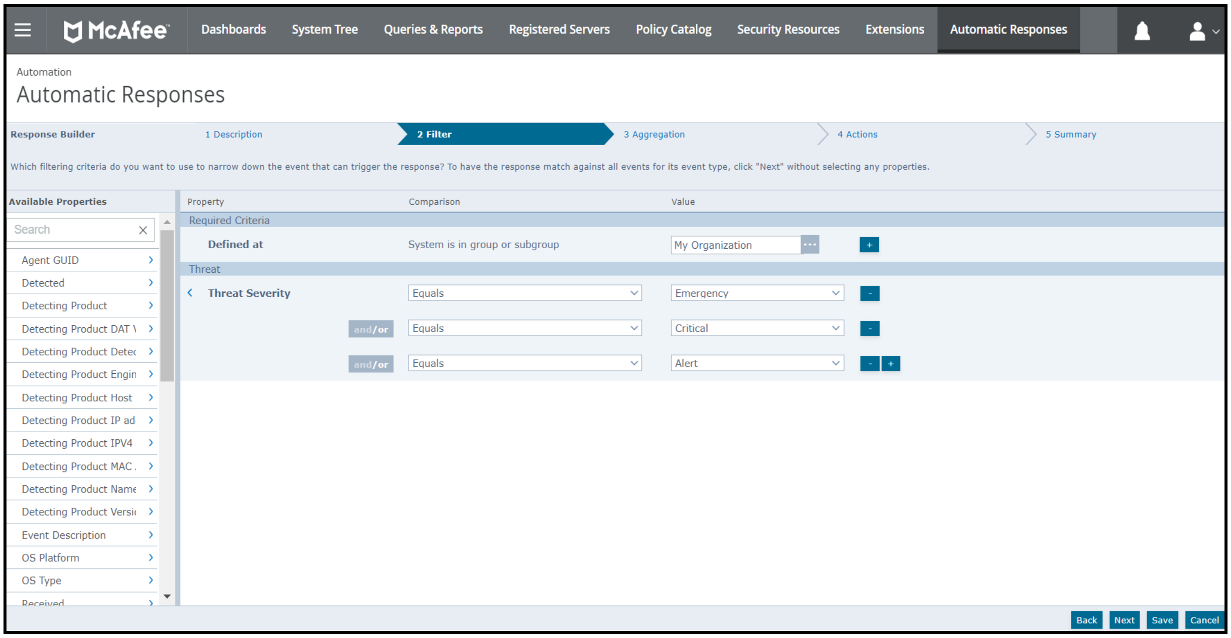


What is this response's name, target language, and event type? Is the response enabled?

Name:	Pulse Policy Secure Auto Response
Description:	Pulse Policy Secure Auto Response
Language:	English
Event:	Event group: ePO Notification Events Event type: Threat
Status:	● Enabled ○ Disabled

4. Add the filters for the incoming events. For example, Source IP address, Threat Event-ID, Threat severity and so on.

Figure 14 Automatic Responses

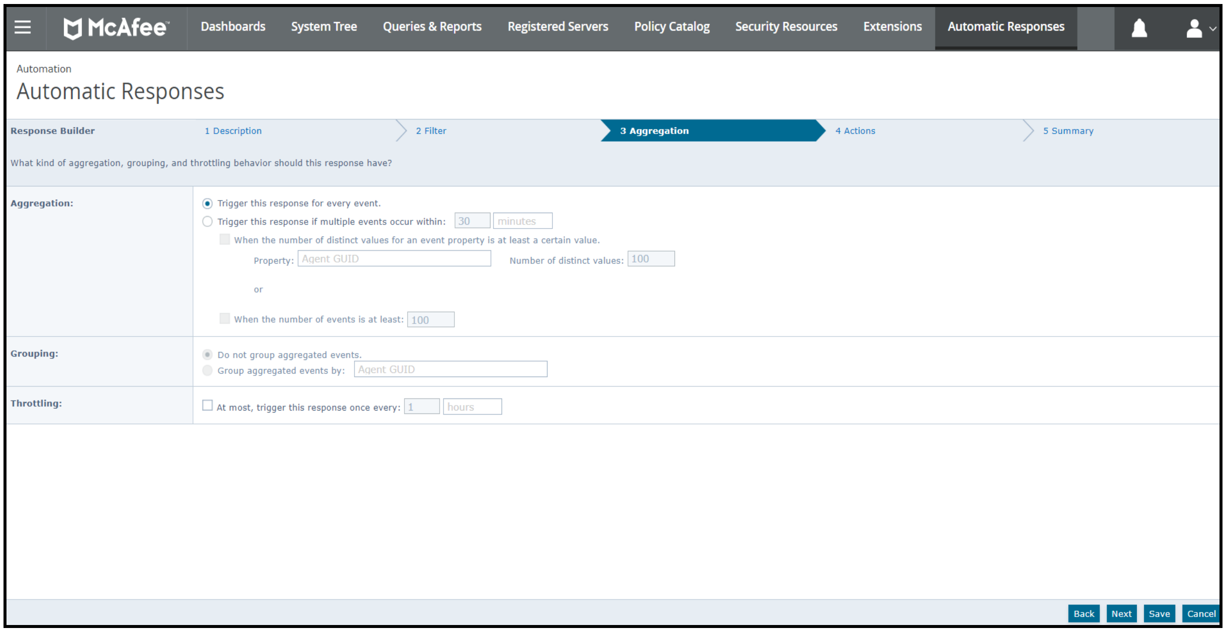


Which filtering criteria do you want to use to narrow down the event that can trigger the response? To have the response match against all events for its event type, click "Next" without selecting any properties.

Property	Comparison	Value
Required Criteria		
Defined at	System is in group or subgroup	My Organization
Threat		
Threat Severity	Equals	Emergency
and/or	Equals	Critical
and/or	Equals	Alert

5. Automatic response is sent for every event or specific event(s). The trigger conditions is defined on the "Aggregation" page.

Figure 15 Aggregation



What kind of aggregation, grouping, and throttling behavior should this response have?

Aggregation:

● Trigger this response for every event.

○ Trigger this response if multiple events occur within: 30 minutes

□ When the number of distinct values for an event property is at least a certain value.

Property: Agent GUID Number of distinct values: 100

or

□ When the number of events is at least: 100

Grouping:

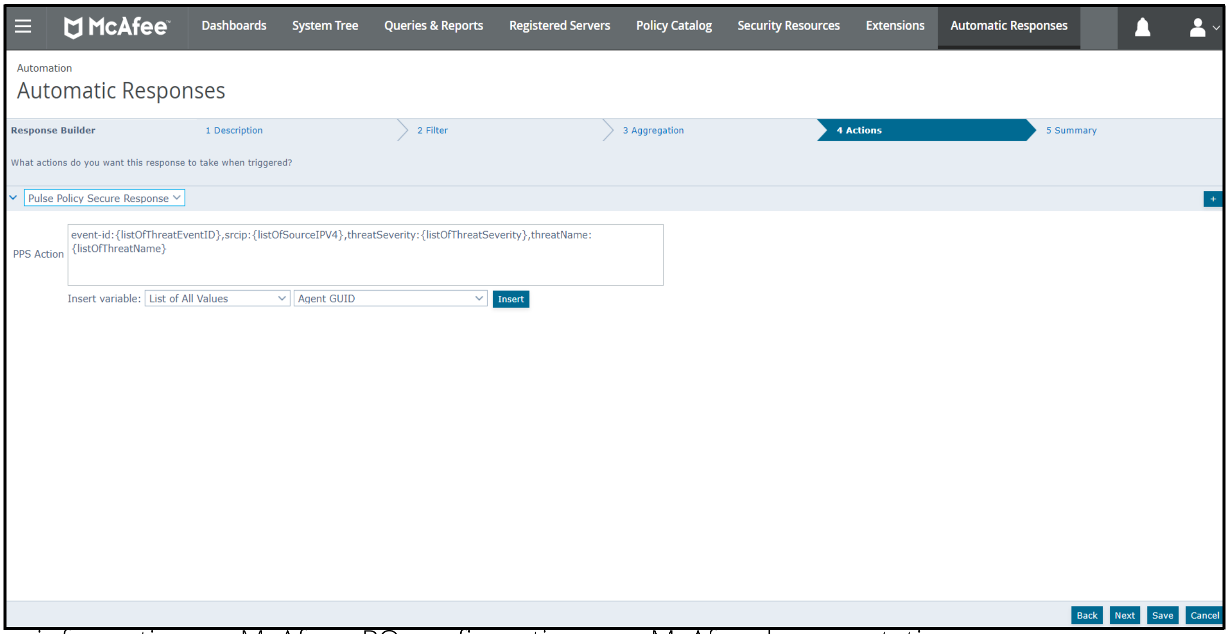
● Do not group aggregated events.

○ Group aggregated events by: Agent GUID

Throttling:

□ At most, trigger this response once every: 1 hours

6. Select **Pulse Policy Secure Response** from the drop down. Enter event information to be sent to PPS. You can also insert the variables from the drop down.



What actions do you want this response to take when triggered?

Pulse Policy Secure Response

PPS Action: event-id:{listOfThreatEventID},srcip:{listOfSourceIPV4},threatSeverity:{listOfThreatSeverity},threatName:{listOfThreatName}

Insert variable: List of All Values | Agent GUID

For more information on McAfee ePO configuration, see McAfee documentation.

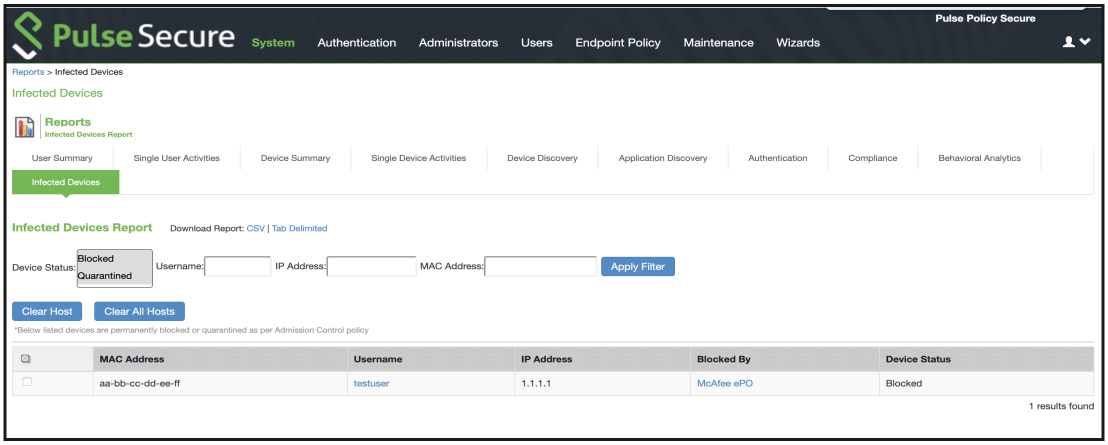
Troubleshooting

To verify the event logs on PPS, select System > Log/Monitoring > Events. Ensure Admission control events option is enabled in Event logs settings.

You can verify that the event logs are generated every time when an event is received from McAfee ePO.

To verify the user access logs, select System >Logs & Monitoring > User Access to verify the user login related logs like realm, roles, username and IP address.

You can also verify whether the quarantined/blocked host is listed in the Infected Devices report, which lists the mac address, IP address, and the device status. To verify the reports, select System > Reports > Infected Devices.



Infected Devices Report Download Report: CSV | Tab Delimited

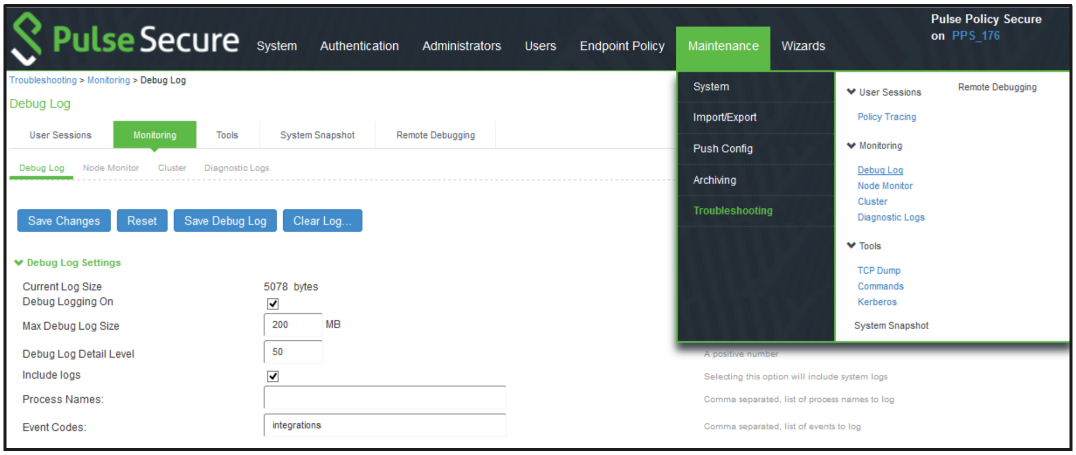
Device Status: Blocked Quarantined Username: IP Address: MAC Address:

*Below listed devices are permanently blocked or quarantined as per Admission Control policy

☒	MAC Address	Username	IP Address	Blocked By	Device Status
□	aa-bb-cc-dd-ee-ff	testuser	1.1.1.1	McAfee ePO	Blocked

1 results found

You can also enable debug logs to troubleshoot any issues. Select Maintenance > Troubleshooting > Monitoring > Debug Log to enable debug logs.



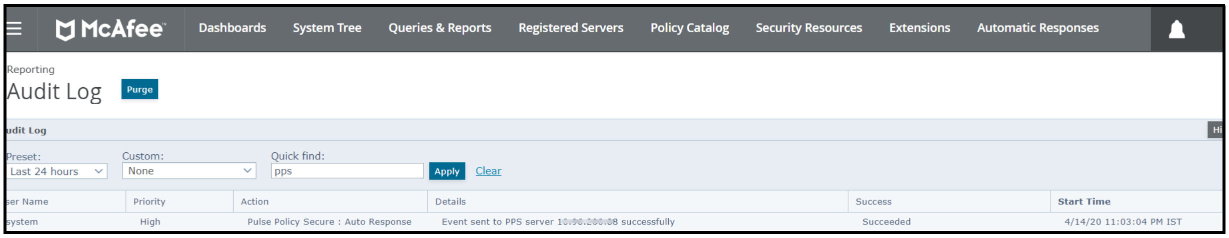
Debug Log

Debug Log Settings

Current Log Size 5078 bytes
Debug Logging On ☑
Max Debug Log Size 200 MB
Debug Log Detail Level 50 — A positive number
Include logs ☑ — Selecting this option will include system logs
Process Names: — Comma separated, list of process names to log
Event Codes: integrations — Comma separated, list of events to log

Verify Audit/Threat Event logs on McAfee ePO

Figure 16 Audit logs



Reporting

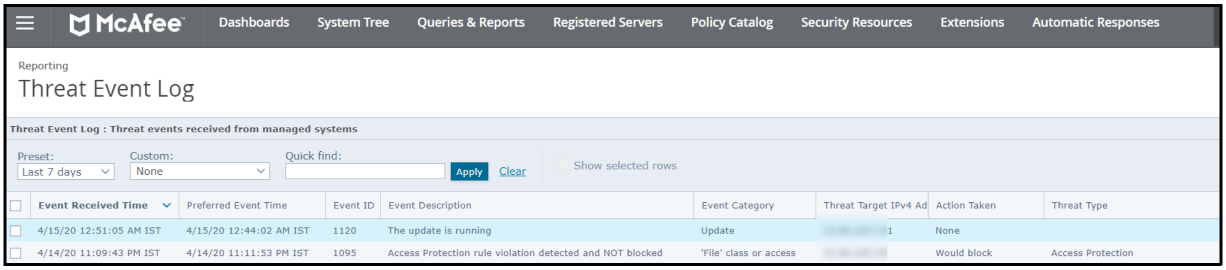
Audit Log

udit Log

Preset: Last 24 hours
Custom: None
Quick find: pps

ser Name	Priority	Action	Details	Success	Start Time
system	High	Pulse Policy Secure : Auto Response	Event sent to PPS server [redacted] successfully	Succeeded	4/14/20 11:03:04 PM IST

Figure 17 Threat Event Logs



Reporting

Threat Event Log

Threat Event Log : Threat events received from managed systems

Preset: Last 7 days
Custom: None
Quick find:
□ Show selected rows

□	Event Received Time	Preferred Event Time	Event ID	Event Description	Event Category	Threat Target IPv4 Ad	Action Taken	Threat Type
□	4/15/20 12:51:05 AM IST	4/15/20 12:44:02 AM IST	1120	The update is running	Update	[redacted]	None	
□	4/14/20 11:09:43 PM IST	4/14/20 11:11:53 PM IST	1095	Access Protection rule violation detected and NOT blocked	'File' class or access	[redacted]	Would block	Access Protection

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.