

Pulse Policy Secure: McAfee ePO Integration Guide

Product Release9.1R8PublishedJuly 2020Document Version1.0

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

www.pulsesecure.net

© 2020 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Policy Secure: 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.

ENDPOINT PROTECTION WITH MCAFEE EPOLICY ORCHESTRATOR (EPO) SERVER3
Overview
Prerequisites
Use Cases
SUMMARY OF CONFIGURATION
CONFIGURING PPS WITH MCAFEE EPO SERVER5
Configuring HTTP Attribute Server5
McAfee ePO Server Configuration
Server Task to Install McAfee Agent on Unmanaged Devices
IDENTIFYING THE GROUP ID
TROUBLESHOOTING
Appendix
ALERT-BASED ADMISSION CONTROL WITH MCAFEE EPOLICY ORCHESTRATOR (EPO)19
Overview
Prerequisites
SUMMARY OF CONFIGURATION
Configuring PPS with McAfee ePO server
Admission Control Template21
Admission Control Client22
Admission Control Policies
Configuring McAfee ePO Server25
Install Pulse Policy Secure Extension for McAfee ePO
McAfee ePO Server Configuration
TROUBLESHOOTING
Requesting Technical Support32
Self-Help Online Tools and Resources
OPENING A CASE WITH PSGSC
Reporting Documentation Issues

Endpoint protection with McAfee ePolicy Orchestrator (ePO) Server

•	Overview	3
•	Summary of Configuration	4
•	Configuring PPS with McAfee ePO Server	5
•	McAfee ePO Server Configuration	10
•	Troubleshooting	13

Overview

This section describes how to integrate McAfee ePO server with PPS to support endpoint protection in your network. It describes Pulse Policy Secure (PPS) integration with McAfee ePO server to assess device security posture by querying device attributes details and use them in role mapping rules to make access control decisions.

Prerequisites

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

- Pulse Policy Secure at version 9.1R8.
- McAfee ePolicy Orchestrator (ePO) server version 5.10.0 and above

Pulse Policy Secure (PPS) integration with the McAfee ePolicy Orchestrator (ePO) server provides complete visibility of network endpoints and provide end to end network security. McAfee ePO server maintains the endpoint information that it manages in its database.

The PPS integration with McAfee ePO server allows Admin to use the host property values of the endpoints managed by ePO to access device security posture. This document talks about the REST APIs exposed by McAfee ePO server, which can be used by PPS to fetch the endpoint details, attributes that are needed for accessing device security posture and also about the remote command to take remediation action on the endpoint using McAfee ePO server.

Use Cases

The following use cases are supported with PPS and McAfee ePO server integration:

- 1. Role Based Access Control (RBAC) for the endpoints based on the device attributes received from HTTP attribute server (McAfee ePO).
- 2. Periodic compliance check for the endpoint using HTTP attribute server.
- 3. Report the unmanaged endpoint IP address to McAfee ePO server for McAfee agent installation on the endpoint.

The authentication process is described below:

- 1. When endpoint tries to connect to the network, PPS authenticates the user and queries the third-party server for the endpoint device attribute values using endpoint identifier.
- 2. Roles are assigned based on the attribute values received from external server and user is given the corresponding access.
- 3. PPS periodically queries the external server for change in attribute values and assigns the role accordingly. Endpoint identifier can be IP address, MAC address, or user certificate.



Figure 1 Deployment using PPS and McAfee ePO server

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

- "Configuring PPS with McAfee ePO Server" on page 5
- McAfee ePO Server Configuration 10

Configuring PPS with McAfee ePO Server

The PPS configuration requires defining the McAfee ePO server as HTTP attribute server in PPS.

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 HTTP attribute server in PPS.
- 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.
- Configured HTTP attribute server has to be mapped as a "Device Attributes" under the realm configuration and role mapping rules can be used to assign the roles based on the attributes values received from the attribute server.
- Admin can optionally configure the remediation action to report the unmanaged endpoint IP address to McAfee ePO server.

This section covers the following topics:

- Configuring HTTP Attribute Server 5
- Server Task to Install McAfee Agent on Unmanaged Devices 10

Configuring HTTP Attribute Server

The default McAfee template provides the list of possible attributes that can be received from the network security device along with attribute value. The template also provides possible remediation actions that can be taken for an attribute. PPS is loaded with default template for McAfee ePolicy Orchestrator (ePO).

To add the HTTP Attribute server in PPS:

- 1. Select Authentication > Auth.Servers, select HTTP Attribute Server under New and Click New Server.
- 2. Enter the name.
- 3. Select McAfee-McAfee ePolicy Orchestrator Endpoint Protection Platform as template.
- 4. Enter the IP address or hostname of McAfe ePO server.
- 5. Enter the port number. Default is 8443.
- 6. Enter the username and password (Admin credentials of McAfee ePO server).
- 7. Click **Test Connection** to test connectivity between PPS and McAfee ePO server.
- 8. (Optional) Under **Remediation Action**, enable **report endpoint** to report endpoint details to McAfee ePO server and enter the **Group ID** to which the endpoint has to be added on McAfee ePO server. See Identifying the Group ID 13 to identify the Group ID.

Note:

- Profiler has to be configured to take remediation action for endpoints authenticating through native supplicant.
- Remediation action of reporting endpoint IP address is not supported for unmanaged devices (For example, Printers, Scanners), VoIP phones and Mobile devices.
- Remediation action of reporting endpoint is supported only with Windows, Linux, and Mac OS.
- 9. Click Save Changes.

Figure 2 HTTP Attribute Server

Authentication Servers											
Auth. Servers	Templates										
Enable Auth Traffic Control											
New: HTTP Attribute	Server		New Server	Delete							

Figure 3 Template

Auth Servers > McAfee_ePO > Settings										
Settings										
	r			_						
* Name:	McAfee_ePO					Label to reference this server.				
* Template:	McAfee-McAfee	ePolicy Or	chestrator-End	ooin 🗸		To manage templates, click here				
	Template name	Vendor	Device	Device Type	Description					
	mcafee-epo- endpoint- protection.tmpl	McAfee	McAfee ePolicy Orchestrator	Endpoint Protection Platform	Integration with McAfee ePO					
				_		а 				
* Host:	10.00.000.101					IP Address/Hostname				
Port:	8443									
* Username:	admin					Username for Basic Authentication.				
* Password:						Password for Basic Authentication.				
Server Certificate Validation:						Enable this option to verify the server's certificate.				
Test Connection										
✓ Remediation Action										
Report Endpoint						Enable this option to report endpoint details to McAfee ePO				
Group ID: 10]			Group to which the Endpoint has to be added				
Save Changes Reset										
indicates required field										



	ultrative discuss a Template												
Authe	Internaciation Servers > templates												
Tem	Templates												
A	Auth. Servers Templates												
Note:	Note: These templates are applicable to HTTP Attribute Servers only. New Template Delete Restore Factory Default												
10		✓ records per page			5	Search:							
		Name	File Name	Vendor	Device	Device Type							
1 nozomi-networks-ics-security.tmp1 nozomi-networks-ics-security.tmp1 Nozomi Networks SCADAguardian ICS Security Solution													
	2 mcafee-epo-endpoint-protection.tmpl mcafee-epo-endpoint-protection.tmpl McAfee Policy Orchestrator Endpoint Protection Platform												

Note: A subset of attributes supported by McAfee ePO server 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 attributes apart from the one's in the default template. See the template creation guide for template creation.

10. Under **User Realms > Users > General**, select the McAfee HTTP attribute server created in Device Attributes or **Endpoint Policy > MAC Address Realms** click New to create the authentication realm. Under Device Attributes, select the McAfee ePO HTTP attribute server created earlier.

User Realms > Users > General									
General									
General Authentication Policy Role Ma	pping								
* Name:	lsers								
Description:									
Description:	Default authentication								
	//								
C	When editing, start on the Role Mapping page								
✓ Servers									
Specify the servers to use for authentication and authorization. To	create or manage servers, see the Servers page.								
Authentication:	System Local								
User Directory/Attribute:	None 🗸								
Accounting:	None 🗸								
Device Attributes:	McAfee_ePO 🗸								
Device Check Interval:	10 minutes								
✓ Additional Authentication Server									
Enable additional authentication server									
✤ Dynamic policy evaluation									
Enable dynamic policy evaluation									
✓ Session Migration									
Session Migration									
✓ Other Settings									
Authentication Policy:									
Role Mapping:									
Save Changes									

Figure 5 User Realms

11. Configure rules based on Device Attributes from User Realms > Users > Role Mapping > Role Mapping Rule or Endpoint Policy > MAC Address Realms and click Role Mapping > Role Mapping Rule.



Figure 6 Device Attributes

Figure 7	Role Mapping Rules
1 901 0 /	

User Realms > Users > Role M	apping > Role Mapp	oing Rule				
Role Mapping Rule						
* Name: FirewallStatus		ו				
Themailotatus		J				
	the following attrib	oute values				
Attribute:	firewallStatus	~	Attributes			
is 🗸	1		If more than one va	alue for this attribute sh	nould match, enter on	e per line. You can use * wildcard
		11				
✓ then assign these roles						
Available Roles:		Selected Roles:				
Guest	Add ->	Users				
Guest Admin	Remove					
Guest Sponsor						
Guest Wired Restricted						
	-		-			
Stop processing rules	when this rule mat	ches				
To manage roles, see the Role	s configuration page.					
Save Changes Sa	ve as Copy					
*indicates required field						

12. Click Save Changes.

Once the role mapping rule is created. You can see the summary page as shown below. The following page shows the different rules created with the corresponding roles assigned.

Figure 8	Summary
----------	---------

User R	Jser Realms > Users > Role Mapping										
Role	Role Mapping										
G	General Authentication Policy Role Mapping										
Specif Nev	Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in. New Rule Duplicate Delete Image: Changes										
		٠	When users meet these conditions		assign these roles	Rule Name	Stop				
	1.		device attribute "firewallStatus" is "1"	\rightarrow	Users	FirewallStatus					
	2.		username is "*"	\rightarrow	Guest	rule 0					

Note: MAC Address is used as a device identifier to query attributes from McAfee ePO server. Without Host Checker, PPS doesn't learn the MAC address. For agent less sessions, Host Checker should be enabled to learn MAC address. For Agentless sessions/logins, pre-auth Host Checker must be enabled.

McAfee ePO Server Configuration

•	Server Task to Install McAfee Agent on Unmanaged Devices	10
•	Identifying the Group ID	13

Server Task to Install McAfee Agent on Unmanaged Devices

When an endpoint is not managed by McAfee ePO server, PPS can take action to report the endpoint details to McAfee ePO server. Reported endpoint will be in "Unmanaged" state in McAfee ePO server, since McAfee agent is not installed on the endpoint. Admin has to configure a custom query on McAfee ePO server to list all unmanaged devices and create a server task to install the McAfee agent on these unmanaged devices.

1. Sample Query to list unmanaged devices.



	Dashboards	System Tree	Queries & Reports	Registered Servers	Policy Catalog
Queries & Reports	5				
Query: Details					
Query: Information					
Name:			Query-Un	managed-Windows	
Notes:					
Database type:			ePO		
Result type:			Systems		
Created by:			admin - 5	/6/20 4:02:10 PM	
Last changed by:			admin - 5	/6/20 4:22:53 PM	
Criteria:			Managed	State Equals Unmanaged	

2. To create a Server Task, login to McAfee ePO server and under Automation, select Server Tasks.

■ McAfee [®]	Dashboards Syster	n Tree Queries & Repo	orts Registered Servers
Recent Pages Server Tasks	Search		
System Tree	Reporting	Systems	Policy
Server Task Log	Dashboards	System Tree	Policy Catalog
Threat Event Log	Security Resources	Tag Catalog	Common Catalog
Registered Servers	Queries & Reports	Systems	Policy Assignments
	Audit Log		Policy Assignment Rules
	Threat Event Log		Policy History
	Firewall Client Rules		Policy Comparison
	Exploit Prevention Eve		Firewall Catalog
	Adaptive Threat Prote		Endpoint Migration As
	Client Tasks	Software	Automation
	Client Task Catalog	Endpoint Upgrade Ass	Server Task Log
	Client Task Assignments	Getting Started	Server Tasks
	Client Task Comparison	Product Deployment	Automatic Responses
		Software Catalog	lssues
		Master Repository	
		Distributed Repositories	
		Extensions	
PO Build: ePolicy Orchestrator 5.10.0 Jpdate Installed: Update 5 (2.0.0.767 Server: hdarshan200101 fime: 7/8/20 6:50:03 PM IST Jser: admin	(Build 2428))		

Figure 10 Server Tasks

3. Click New Task.

Figure 11 Task



4. Enter the name for the task.

Figure	12	Task
--------	----	------

Automation Server Tasks				
Server Task Builder	1 Description	2 Actions	3 Schedule	4 Summary
Name:	New Task			
Notes:				
Schedule status:	Enabled Disabled			

5. Run the query under actions. Specify the agent version, path, credentials and Click Next.

Figure 13 Actions

Automation					
Server Tasks					
erver Tack Builder	Description	2 Actions	3 Schedule	4 Summary	
erver rask builder	Description	2 ACTIONS	3 Streade		
hat actions do you want the task to take?					
1. Actions: Run Query	~				• •
Query: Ouery-Unmanaged-Win	dows				
Language: English (United Kingdor	n) ~				
Sub-Actions: Deploy McAtee Agen	.t				
Agent version:	Windows McAfee Agent for Windows	(Embedded Credential ~			
	O Non-Windows McAfee Agent for LINUX 5	6.5.236 (Current) ~			
Installation options:	Install only on systems that do not already	have an agent managed by this McAfee ePO server			
	Force installation over existing version				
Installation path:	<program_files_dir>\McAfee\Agent</program_files_dir>				
	Program Files ~	McAfee\Agent			
Credentials for agent installation:	Domain: WORKGROUP				
	User name: hdomban				
	Password:				
	Confirm password:				
Number of attempts:	0 (Enter 0 for continuous attempts)				
Retry interval:	30 seconde x				
Cancel after:	5 minutes V				
	All Agent Handlers				
Push Agent using:	O Selected Agent Handler: hdarshan20010	.ueba.pps 🗸			
					_
				Back Next Sav	ve Cance

6. Schedule the installation.

Figure 14 Server Tasks

Automation Server Tasks				
Server Task Builder	1 Description	2 Actions	3 Schedule	4 Summary
Schedule type:	Daily ~			
Start date:	105 / 06 / 2020			
End date:	 III 07 / 09 / 2020 No end date 			
Schedule:	between \checkmark 1 \checkmark :00 \checkmark AM \checkmark and 11 \checkmark :	00 v PM v every 5 v minutes v		- +

Figure 15 Summary

Automation Server Tasks				
Server Task Builder	1 Description 2 Actions		3 Schedule	4 Summary
Name:	Install Agent Task			
Notes:	No notes available			
Task owner:	admin			
Schedule status:	Enabled			
Schedule:	Start date: 5/6/20 End date: No end date Schedule: Dally Detween 1:00 AM and 11:00 PM, repeating every 5 minutes Next runtime: 7/8/20 7:30 PM 7/8/20 7:30 PM 7/8/20 7:30 PM			
Actions:	I. Run Query Query name: Query-Ummanaged-Windows , Language: English (United King L. Deploy McMee Agent Agent version: Install only on systems that do not already have an agent managed by this McAf Force installation over soluting version Installation opath: Domain: Work name: Number of altempta: Retry instrual; Cancel after; Puh Agent using:	pdom) KGMee Agent for Windows (Embedded Gred ee ePD server true False «PROGRAM_FILES_DIR>/MoMee Agent WORKGROUP Industan Continuous 30 seconde 5 minutes Al Agent transfern	tentials) 5.6.5.236 (Current)	

Pulse Policy Secure on PPS7345

1.

Identifying the Group ID

Group/Sub Group information has to be configured on the McAfee ePO server. See McAfee documentation for Group/SubGroup creation. The corresponding Group ID value can be fetched from McAfee ePO server using the URL/API:

https:<IP-Address of McAfee ePO server>:Port/remote/system.findGroups Figure 16 Sample Screenshot of API/Group ID configured on McAfee ePO

$\leftarrow \rightarrow \circ$	//10.06.200.101:8443/r	emote,	/system.findGro	ups				Å,	臣	
OK: groupId: 2 groupPath: My Organization groupId: 3		= []]			• + (🔰 ePolic	× +		
groupPath: Hy Organization\Lost and Found groupId: 4 groupPath: Hy Organization\Lost and Found\UEBA	← → C ▲ ****		1:8443	/core/orionN	lavigationLogin	.do#/core/orionTab.d	lo?sectionId=Compu	terM G	2 🕁	0 #
groupEi: 5 groupEi: 9 groupEi: 6 groupEi: 7 groupEi: 7 groupEi: 7 groupEi: 8 groupEi: 8 groupEi: 8	E McAfee [™] System Tree New	Dash Systems	boards System	Tree Que	ries & Reports	Registered Servers	Policy Catalog			~
groupId: 9	System Tree	System	Assigned Policies	Assigned Clien	t Tasks Group De	tails Agent Deployment				
proupPath: My Organization\PPS	V My Organization My Group	Preset: This G	iroup Only	V None	:: ~	Quick find:	Apply Clear	Show	selected	rows
	PPS		System Name	^	Managed State	Tags	IP addr	855		User Name
	\checkmark Lost and Found		1)59		Managed	Workstatio	10.06.2	00.50		admin
	3	1 0	1		Managed	Workstation	n	4		Administrator
	local	1 0	1		Managed	Workstatio	n	5		N/A
	test.com	1 0	1 1		Managed	Workstatio	n	5		admin
	UEBA	1 🗆	h		Managed	Workstatio	n 10.90.2			rharsha
	WORKGROUP									

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

Troubleshooting

To verify the event logs on PPS, select System > Log/Monitoring > Events. You can verify that the event logs are generated every time when an event is received from McAfee ePO server.

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 view the System > Active Users page to see the users along with the device details.

Figure 17 Ac	live Users					
💲 Pulse S	Secure					
		System	Authentication	Administrators	Users	Endpoint Policy
Status > Active Users						
Active Users						
Activity Overview	Active Users	Device F	Profiles Behav	oral Analytics	Admin Notificatio	n
Show users named:	Show	200 us	sers Update			
Delete Selected Sessions	Refresh Roles	Delete	All Sessions	Disable All Users		

Figure 17 Active Llears

					System	Authentication	Administra	ators Users	Endpoint	Policy Maintenance	Wizards	
Status	> Act	ive Users										
Activ	e Us	sers										
A	tivity		Overview	Active Users	Device Pr	ofiles Behavi	oral Analytics	Admin Notificatio	n			
		ſ										
Show	usen	s named:		Show 2	00 use	ers Update						
Del	ete S	Selected S	Sessions	Refresh Roles	Delete A	Il Sessions	Disable All Use	rs				
Numb	er of	Users: 2										
	1	User T	Realm	Roles	Signed in	Node	Signed in IP	MAC Address	Device Details	Agent Type	Agent Version	Endpoint Security Status
		admin	Admin Users	.Administrators	2020/6/17 15:18:26	PPS7345	112.21.27.07			Windows 10 Google Chrome		Not Applicable
		d	Users	Users, Guest	2020/6/17 15:25:05	PPS7345	10.00.200.00	06-50-50-bi-0a-54		Windows 10 Pulse Secure	e 9.1.5.2101	Not Applicable

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

Troubleshooting > Monitoring > Debug Log			
Houbleshooling > Monitoring > Debug Eog			
Debug Log			
User Sessions Monitoring Tools Sy	stem Snapshot Remote Debugging	Log Selection	
Debug Log Node Monitor Cluster Diagnostic Logs RE	ST Monitor		
O Debug Logging is on			
Save Changes Reset Save Debug Log	Clear Log		
✓ Debug Log Settings			
Current Log Size	219308151 bytes		
Max Debug Log Size	200 MB		1-250
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:	auth,dsintegration		Comma separated, list of events to log

Figure 18 Attribute Server Events

Log/Monitoring >	Events > Log settings							
Log settings								
Events	User Access	Admin Access	Sensors	Client Logs	SNMP	Statistics	Advanced Settings	
Log Setting	Filters							
Save (Changes Rese	et						
✓ Maximum Lo	og Size							
Max Log	Size: 200	мв						
Note: To	archive log data, se	e the Archiving page.						
Select Event	is to Log	51-5-						
· concertion								
Con	nection Requests	Statistics						
🔽 Sys	tem Status	Performance						
🔽 Sys	tem Errors							
Enfo	orcer Events	Enforcer Comma	ind Trace					
Lice	nse Protocol Events							
□ IF-N	IAP Server Trace							
	OIUS Statistics							
	M API Trace							
🔽 Puls	e One Events							
🔽 Prof	iler Events							
🔽 Adn	nission Control Even	ts						
🔽 Attri	bute Server Events							

Figure 19 Logs

Log/Monitor	ng > Events :	Logs							
Logs									
Events	Use	Access Admin Access Sensors Client Logs SNMP Statistics Advanced Settings							
Log Si	ttings Filte	5							
View by filt	er: Standard	-Standard (default) 🗸 Show 200 Items							
Edit Query:	Update	Reset Query Save Query							
Save Lo	g As	Cléar Log Save All Logs Cléar All Logs							
Fi D Qu Export For	Iter:Standard (ate:Oldest to f ery: nat:Standard	default, levest							
Severity	ID	Message							
Info	ATR31854	4 2020-07.68 19/29 07 - PPS2002 - (127.8.0 1] System()] - Ashibute Server McAlee, ePO, Response OK. [["EPOLeaflided.tags": "Vortstation"; "EPOLeaflided.Lastlipdate": "2020-07.68 119:27.37-65.30"; "EPOLeaflided.tags": "Window 10(Vortstation); 10(";"EPOLeaflided.tags": "Vortstation"; "EPOLeaflided.Lastlipdate": "2020-07.68 119:27.37-65.30"; "EPOLeaflided.tags": "Window 10(Vortstation); 11, 24, CustomProps APComplaneeStatus": "14, CustomProps APComplaneeStatus": "15, 03, 05, 05, 05, 05, 05, 05, 05, 05, 05, 05							
info	ATR31854	2020-57-38 19 28 07 - PPS20082 - [127 0.6 i] System(i] - Altitude Server, McAfePPO , Request: https://19.80.200.101.8433/rende/computer/eps//							

Appendix

Attributes exposed by the default McAfee ePO server template. Admin can add more attributes to the list by creating a new template and uploading it to PPS.

```
{"EPOLeafNode.ManagedState" : "managedState"},
{"EPOLeafNode.AgentVersion" : "agentVersion"},
{"EPOLeafNode.LastUpdate" : "lastUpdate"},
{"EPOLeafNode.Tags" : "tags"},
{"EPOLeafNode.ExcludedTags" : "excludedTags"},
{"EPOComputerProperties.OSType" : "os"},
{"EPOComputerProperties.OSVersion" : "osVersion"},
{"EPOComputerProperties.OSPlatform" : "osPlatform"},
{"EPOComputerProperties.DomainName" : "domain"},
{"EPOComputerProperties.IPHostName" : "hostname"},
{"EPOComputerProperties.NetAddress" : "macaddr"},
{"AM_CustomProps.OASbComplianceStatus" : "onAccessScanComplianceStatus"},
{"AM CustomProps.ODSbComplianceStatus" : "onDemandScanComplianceStatus"},
{"AM CustomProps.AVCMGRbComplianceStatus" : "AMCoreContentComplianceStatus"},
{"AM CustomProps.BObComplianceStatus" : "exploitPreventionComplianceStatus"},
{"AM CustomProps.SSbComplianceStatus" : "scriptScanComplianceStatus"},
{"AM CustomProps.APbComplianceStatus" : "accessProtectionComplianceStatus"},
{"AM CustomProps.bOASEnabled" : "isOnAccessScanEnabled"},
{"AM_CustomProps.bAPEnabled" : "isAccessProtectionEnabled"},
{"AM CustomProps.bBOEnabled" : "isExploitPreventionEnabled"},
{"AM CustomProps.bScriptScanEnabled" : "isScriptScanEnabled"},
{"AM CustomProps.LicenseStatus" : "AMLicenseStatus"},
{"FW_CustomProps.ComplianceStatus" : "firewallComplianceStatus"},
{"FW CustomProps.FWStatus" : "firewallStatus"},
{"FW CustomProps.ProductVer" : "firewallProductVersion"},
{"WP CustomProps.WPbComplianceStatus" : "webControlComplianceStatus"},
{"WP CustomProps.bWPEnabled" : "isWebControlEnabled"},
{"WP CustomProps.LicenseStatus" : "webControlLicenseStatus"},
{"WP CustomProps.WCStatus" : "webControlStatus"},
{"GS_CustomProps.IsSPEnabled" : "isGeneralSecurityEnabled"},
{"GS CustomProps.SPbComplianceStatus" : "generalSecurityComplianceStatus"},
{"GS CustomProps.LicenseStatus" : "generalSecurityLicenseStatus"}
```

Sample Query for fetching endpoint attributes from McAfee ePO server.

```
https://10.96.200.101:8443/remote/
core.executeQuery?target=EPOLeafNode&joinTables=EPOProductPropertyProducts,EPOComputerProp
erties, AM CustomProps, WP CustomProps, FW CustomProps, GS CustomProps&where=(eq
EPOComputerProperties.NetAddress "005056BF6A54") &: output=json
    {
       "EPOLeafNode.Tags": "Workstation",
        "EPOLeafNode.ExcludedTags": "",
        "EPOLeafNode.LastUpdate": "2020-04-20T15:00:18+05:30",
        "EPOLeafNode.os": "Windows 10|Workstation|10.0|",
        "EPOLeafNode.NodeName": "H20050",
        "EPOLeafNode.ManagedState": 1,
        "EPOLeafNode.AgentVersion": "5.5.1.342",
        "EPOLeafNode.AgentGUID": "35481B08-5154-11EA-3A04-005056BF6A54",
        "EPOLeafNode.ResortEnabled": true,
        "EPOLeafNode.TransferSiteListsID": false,
        "EPOLeafNode.SequenceErrorCount": 0,
        "EPOLeafNode.SequenceErrorCountLastUpdate": null,
        "EPOLeafNode.LastCommSecure": "1",
        "WP CustomProps.WPbComplianceStatus": 1,
        "WP CustomProps.WPComplianceStatus": "",
        "WP CustomProps.WPAdditionalComplianceStatus": "",
        "WP CustomProps.bWPEnabled": true,
        "WP CustomProps.Hotfixes": "",
        "WP CustomProps.Patch": "0",
        "WP CustomProps.Language": "0409",
        "WP CustomProps.LicenseStatus": 1,
        "WP CustomProps.LoadableIE": "0",
        "WP CustomProps.LoadableFF": "0",
        "WP CustomProps.LoadableCH": "0",
        "WP CustomProps.LoadableSafari": null,
        "WP CustomProps.WCStatus": "1",
        "GS CustomProps.IsTimeBasedPasswordEnabled": 0,
        "GS CustomProps.IsSPEnabled": true,
        "GS CustomProps.SPbComplianceStatus": 1,
        "GS CustomProps.SPComplianceStatus": "",
        "GS CustomProps.SPAdditionalComplianceStatus": "",
        "GS CustomProps.UIPasswordChanged": "1900-01-01T05:21:10+05:21",
        "GS CustomProps.clientUIAccessLevel": 0,
        "GS CustomProps.gtiProxyType": 0,
        "GS CustomProps.IsWindowsApplicationLoggingEnabled": true,
        "GS CustomProps.IsSendEventsToepoEnabled": true,
        "GS CustomProps.APEventFilterlevel": 3,
        "GS CustomProps.BOEventFilterlevel": 3,
        "GS CustomProps.FWEventFilterlevel": 3,
        "GS CustomProps.OASEventFilterlevel": 3,
        "GS CustomProps.ODSEventFilterlevel": 3,
        "GS CustomProps.ATPEventFilterlevel": 3,
        "GS CustomProps.WPEventFilterlevel": 3,
        "GS CustomProps.IsClientActivityLoggingEnabled": true,
        "GS CustomProps.IsODSScannedFileLoggingEnabled": false,
        "GS CustomProps.IsAPClientDebugLoggingEnabled": false,
        "GS CustomProps.IsBOClientDebugLoggingEnabled": false,
```

```
"GS CustomProps.IsOASClientDebugLoggingEnabled": false,
        "GS CustomProps.IsODSClientDebugLoggingEnabled": false,
        "GS CustomProps.IsFWClientDebugLoggingEnabled": false,
        "GS CustomProps.IsWPClientDebugLoggingEnabled": false,
        "GS CustomProps.IsATPClientDebugLoggingEnabled": false,
        "GS CustomProps.ClientActivityLogSizeMB": 10,
        "GS CustomProps.ClientDebugLogSizeMB": 50,
        "GS CustomProps.ClientLogFilesLocation": "C:\\ProgramData\\McAfee\\Endpoint
Security\\Logs",
        "GS CustomProps.AacVersion": "20.1.0.177",
        "GS CustomProps.Hotfixes": "",
        "GS CustomProps.Patch": "0",
        "GS CustomProps.LicenseStatus": null,
        "GS CustomProps.Language": "409",
        "GS CustomProps.GlobalExclusionStatus": 0,
       "EPOProductPropertyProducts.Products": "Endpoint Security Common, Endpoint Security
Firewall, Endpoint Security Threat Prevention, Endpoint Security Web Control, McAfee
Agent",
        "EPOComputerProperties.ComputerName": "H20050",
        "EPOComputerProperties.Description": null,
        "EPOComputerProperties.ComputerDescription": "H20050",
        "EPOComputerProperties.TimeZone": "India Standard Time",
        "EPOComputerProperties.DefaultLangID": "0409",
        "EPOComputerProperties.UserName": "epouser",
        "EPOComputerProperties.DomainName": "WORKGROUP",
        "EPOComputerProperties.IPHostName": "hd20050",
        "EPOComputerProperties.IPV6": "0:0:0:0:0:0:FFFF:A60:C832",
        "EPOComputerProperties.IPSubnet": "0:0:0:0:0:FFFF:A60:C000",
        "EPOComputerProperties.IPSubnetMask": "0:0:0:0:0:FFFF:FFFF:E000",
        "EPOComputerProperties.IPV4x": -1973368782,
        "EPOComputerProperties.IPXAddress": "N/A",
        "EPOComputerProperties.SubnetAddress": "10.96.192.0",
        "EPOComputerProperties.SubnetMask": "255.255.224.0",
        "EPOComputerProperties.NetAddress": "005056BF6A54",
        "EPOComputerProperties.OSType": "Windows 10",
        "EPOComputerProperties.OSVersion": "10.0",
        "EPOComputerProperties.OSCsdVersion": "",
        "EPOComputerProperties.OSBuildNum": 18363,
        "EPOComputerProperties.OSPlatform": "Workstation",
        "EPOComputerProperties.OSOEMID": "00330-80000-00000-AA986",
        "EPOComputerProperties.CPUType": "Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz",
        "EPOComputerProperties.CPUSpeed": 2200,
        "EPOComputerProperties.ManagementType": "EPOAGENTMETA",
        "EPOComputerProperties.NumOfCPU": 8,
        "EPOComputerProperties.CPUSerialNumber": "N/A",
        "EPOComputerProperties.TotalPhysicalMemory": 8589463552,
        "EPOComputerProperties.FreeMemory": 6216761344,
        "EPOComputerProperties.FreeDiskSpace": 94294,
        "EPOComputerProperties.TotalDiskSpace": 126931,
        "EPOComputerProperties.IsPortable": 0,
        "EPOComputerProperties.OSBitMode": 1,
        "EPOComputerProperties.UserProperty1": "",
        "EPOComputerProperties.UserProperty2": "",
        "EPOComputerProperties.UserProperty3": "",
```

```
"EPOComputerProperties.UserProperty4": "",
        "EPOComputerProperties.UserProperty5": "",
        "EPOComputerProperties.UserProperty6": ""
        "EPOComputerProperties.UserProperty7": "",
        "EPOComputerProperties.UserProperty8": "",
        "EPOComputerProperties.Free Space of Drive C": 94294,
        "EPOComputerProperties.Total Space of Drive C": 126931,
        "EPOComputerProperties.Vdi": 0,
        "EPOComputerProperties.EmailAddress": "N/A",
        "EPOComputerProperties.LastUpdate": "04/20/2020 15:03:56",
        "EPOComputerProperties.PlatformID": "Windows 10:10:0:0",
        "EPOComputerProperties.SMBiosUUID": "60573F42-283C-A391-6D4C-50531049DC11",
        "EPOComputerProperties.SystemSerialNumber": "VMware-42 3f 57 60 3c 28 89 v3-6d 4f
50 53 10 49 dc 11",
        "EPOComputerProperties.SystemRebootPending": 0,
        "EPOComputerProperties.SystemModel": "VMware Virtual Platform",
        "EPOComputerProperties.SystemManufacturer": "VMware, Inc.",
        "EPOComputerProperties.SystemBootTime": "2020-04-20 12:52:08",
        "EPOComputerProperties.NumOfHardDrives": 1,
        "EPOComputerProperties.EthernetMacAddressCount": 1,
        "EPOComputerProperties.WirelessMacAddressCount": 0,
        "EPOComputerProperties.OtherMacAddressCount": 0,
        "FW CustomProps.ComplianceStatus": 1,
        "FW CustomProps.ComplianceReason": 0,
        "FW CustomProps.AdditionalComplianceReason": null,
        "FW CustomProps.FWStatus": 1,
        "FW CustomProps.FWAdaptiveModeStatus": 0,
        "FW CustomProps.FWFault": 0,
        "FW CustomProps.FWMode": 0,
        "FW CustomProps.Hotfix": "",
        "FW CustomProps.Language": "409",
        "FW CustomProps.LastPolicyEnforcement": "2020-04-20T08:39:10",
        "FW CustomProps.LicenseStatus": 1,
        "FW CustomProps.Patch": "0",
        "FW CustomProps.PolicyNameClientUI": null,
        "FW CustomProps.PolicyNameFwOptions": "My Default",
        "FW CustomProps.PolicyNameFwRules": "My Default",
        "FW CustomProps.PolicyNameTrustedAppList": null,
        "FW CustomProps.PolicyNameTrustedNetworks": null,
        "FW CustomProps.ProductVersion": null,
        "FW CustomProps.RebootRequired": 0,
        "FW CustomProps.ServiceRunning": 1,
        "FW CustomProps.InstallDir32": null,
        "FW CustomProps.InstallDir64": null,
        "FW CustomProps.ProductVer": "10.7.0.1105",
        "AM CustomProps.bOASEnabled": true,
        "AM CustomProps.bAPEnabled": true,
        "AM CustomProps.bBOEnabled": true,
        "AM CustomProps.bScriptScanEnabled": true,
        "AM CustomProps.AVCMComplianceDays": null,
        "AM CustomProps.OASbComplianceStatus": 1,
        "AM CustomProps.OASComplianceStatus": "",
        "AM CustomProps.OASAdditionalComplianceStatus": "",
        "AM CustomProps.OASGTILevel": 3,
```

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

•	Overview	19
•	Summary of Configuration	20
•	Configuring PPS with McAfee ePO server	20
•	Configuring McAfee ePO Server	25
•	Troubleshooting	31

Overview

This section describes how to integrate McAfee ePO server with PPS to support alert-based admission control in your network. It describes how to configure Pulse Policy Secure (PPS) to provide Alert-based admission control protection for your network using McAfee ePolicy Orchestrator (ePO).

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) server 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 server allows Admin to perform user access control based on alerts received from the McAfee ePO server.

If ePO detects that an endpoint on the network has become non-compliant, ePO can send PPS the noncompliant 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 server.
- 3. Based on the alert rules configured on McAfee ePO server, it generates alerts and sends automatically to PPS with the help of Pulse Policy Secure Extension.
- 4. McAfee ePO server 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 server receives Threat events from different Endpoint Security (ENS) modules like Firewall, Threat Intelligence Exchange (TIE)/Adaptive Threat Protection (ATP), Threat Prevention and others.

Figure 20 Deployment using PPS, McAfee ePO and Firewall



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) server and Firewall, perform the following tasks:

- "Configuring PPS with McAfee ePO server" on page 20
- "Configuring McAfee ePO Server" on page 25

The following sections describe each of these steps in detail.

Configuring PPS with McAfee ePO server

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

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) server as a client in PPS. PPS acts as a REST API Server for McAfee ePO server. 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 21
- "Admission Control Client" on page 22
- "Admission Control Policies" on page 23

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 21 McAfee ePO Template

0					IN P. C. H. K.	Pulse Policy Secure
\sim		Pulse Secure sy	stem Authentication Administra	ators Users Endpoint Policy	Maintenance Wizards	1~
		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	НТТР	McAfee	McAfee ePolicy Orchestrator
	9	ibm-qradar-http.itmpl Integration with IBM Gradar which sends endpoint control commands/offenses to PPS	ibm-qradar-http.itmpl	НТТР	IBM Qradar	SIEM

Admission Control Client

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

To add McAfee ePO server 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	22	Temp	late
i igui c		remp	iuic

\diamond		-									Pulse Policy Secure	
2 Р	ulse.	Sec	ure sys	stem A	uthentica	tion Administrators	Users	Endpoint Policy	Maintenance	Wizards		1~
Admission Cor	trol > Configure :	> Clients > I	New Client									
New Client												
* Name:	McAfee ePO							Label to reference this client.				
Description:												
			6									
* IP Address:	10.96.200.101							IP Address of this client.				
* Template:	McAfee-McAf	ee ePolicv	Orchestrator-HTTF	P-JSON	\$			Template used by the client				
	Selected Templ	ate Details										
	Template											
	name	Vendor	Device	Protocol	Format	Description						
	mcafee-	McAfee	McAfee ePolicy	HTTP	JSON	Integration with McAfee ePolic	су					
	epo- http.itmpl		Orchestrator			Orchestrator which sends end alerts to PPS	lpoint					
Save Chan	iges											
* indicates requi	red field											

Note: A subset of events supported by McAfee ePO server 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 23 Configuration Policies

٥.		6			111					Pulse Policy Secure	
N F	ulse	Sec	cure sy	vstem ,	Authentic	cation Administrators Users	Endpoint Policy	Maintenance	Wizards		1~
* Name:	ePO-policy						Label to reference this policy.				
* Template:	McAfee-McAfe	ee 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 four	nd	\$		Events supported				
* Severity	Level:		Alert	\$			Severity Levels supported				
♥ Count t	ese many times	5									
* Coun	t:		1]			(1-256)				
✓ then per	form this action										
		e (just log t	he event)								
	 Termi Disab 	nate user s	ession								
		ne user acc	Journ								

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 24 Summary

Admis	sion	Control > Configure > Policies									
Polic	ies										
с	onfig	ure Templates									
Clier	ıts	Policies									
NI-											
Nev	W PO	Duplicate De						Save Cr	langes		
10		✓ records per page					Search:				
		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 Server

This section covers the following topics:

- "Install Pulse Policy Secure Extension for McAfee ePO" on page 25
- "McAfee ePO Server Configuration" on page 26

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 server as an Admin user.
- 2. In the McAfee Dashboard, select the **Extensions**.

Figure 25 McAfee extension



3. Click Install Extension.

Figure 26 Install Extension

≡ 🔰 McAfee	Dashboards	System Tree	Queries & Reports	Registered Servers	Policy Catalog	Security Resources	Extensions	Client Task Catalog	×	▲ ≛ ~
Software Extensions	Extension									
Extensions										
Search ×	Search									×
✓ McAfee										
Common Catalog	Name:	Pulse Policy S	ecure Statu	s: Installed	М	odules: Pulse Policy Secure	e Connector		Running	Remove
Endpoint Protection for Mac	Version:	1.0.0	Requi	• Automal	tic Response					
Endpoint Security	Installed by:	admin - June 5, 2020 11:50:03 AM IST	5, 2020 IST	Console	5.9.0					
Endpoint Upgrade Assistant				Core Mo ePO Cor	dules 5.9.0 e 5.9.0					
ePolicy Orchestrator				 Register Schedul 	ed Servers 5.9.0 er 5.9.0					
Help Content			Detail	s: Copyright (C	C) 2020 Pulse					
McAfee Agent				Secure, LLC	. All rights					
McAfee Client Proxy				TOSCI YOU						
Server										
Shared Components										
Threat Detection Reporting										
VirusScan Enterprise										
✓ Third Party										
Pulse Policy Secure										

- 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 27 Pulse Policy Secure extension

≡ 🔀 McAfee	Dashboards	System Tree Queries & R	eports Reg	gistered Servers Policy C	atalog Security Reso	urces Extensions	Client Task Catalog	× 🔺 🔺 🖌
Software Extensions	Extension							
Extensions								
Search ×	Search							×
✓ McAfee								
Common Catalog	Name:	Catalog Framework	Status:	Installed	Modules: Catalog Fr	amework	Running	Remove
Endpoint Protection for Mac	Installed by	2.0.5.19 admin - February 28, 2020	Requires:	Console 5.1				
Endpoint Security		11:53:09 AM IST		Core Modules 5.1 Policy and Task				
Endpoint Upgrade Assistant				Management 5.1				
ePolicy Orchestrator			Details:	Copyright (C) 2020 McAf LLC. All rights reserved.	ee			
Help Content								
McAfee Agent								
McAfee Client Proxy	Name:	Core Catalog	Status:	Installed	Modules: Core Cata	log	Running	Remove
Server	Installed by	2.0.5.19 admin - February 28, 2020	Requires:	Catalog Framework 2	.0.2			
Shared Components		11:53:10 AM IST		Console 5.1 Core Modules 5.1				
Threat Detection Reporting			Details:	Copyright (C) 2020 McAf	ee			
VirusScan Enterprise				LLC. All rights reserved.				
✓ Third Party								
Pulse Policy Secure								

McAfee ePO Server Configuration

McAfee ePO server 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 27
- "Automatic Response" on page 28

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 server as an Admin user.
- 2. Open the Main Menu, under Configuration Click Registered Servers.

Figure 28 Configuration

🔳 🖞 McAfee		m Tree Queries & Repo	orts Policy Catalog	Security Resources	Registered Servers	Automatic Responses	Audit Log		* ~
Recent Pages	Bearch			^					
Registered Servers	Reporting	Systems	Policy						
Extensions	Dashboards	System Tree	Policy Catalog						
Automatic Responses	Security Resources	Detected Systems	Common Catalog						
Audit Log	Queries & Reports	Tag Catalog	Policy Assignments						
Threat Event Log	Audit Log	Systems	Policy Assignment Rules						
	Threat Event Log	Appliance Management	Policy History						
	Firewall Client Rules		Policy Comparison						
	Exploit Prevention Eve		Firewall Catalog						
	Adaptive Threat Prote								
	Client Tasks	Software	Automation						
	Client Task Catalog	Endpoint Upgrade Assi	Server Task Log						
	Client Task Assignments	Getting Started	Server Tasks						
	Client Task Comparison	Product Deployment	Automatic Responses						
		Software Catalog	Issues						
		Master Repository							
		Distributed Repositories							
		Extensions							
		Licensing							
	User Management	Configuration	McAfee Investigator						
	Users	Server Settings	Home Page (2)						
	Contacts	Personal Settings	U U						
	Permission Sets	Registered Servers							
		Agent Handlers							
		Certificate Manager							
		Registered Executables							
		MCP Help Desk							

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

Figure 29 Registered Servers

≡ 🔀 McAfee	Dashboards	System Tree	Queries & Reports	Registered Servers	Policy Catalog	Security Resources	Extensions	Automatic Responses		^ ~
Configuration Registered Servers	5									
Registered Server Builder	1 Description					2 Details				
Server type:	Pulse Policy Sec	cure 🗸								
Name:	PPS McAfee ePC	01								
Notes:	PPS McAfee ePC	01								
									Rack Nov	Cancol

- 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 server.
- 9. Click Save.

Figure 30 Registered Servers- PPS

	🕽 McAfee	Dashboards	System Tree	Queries & Reports	Registered Servers	Policy Catalog	Security Resources	Extensions			. ~
Config Reg	uration gistered Server	S									
Registe	red Server Builder	1 Description				2 Details					
Pulse P	olicy Secure Server	10.00.000.00									
User Na	ame	epoadmin									
Passwo	ord	•••••									
Subnet	(s)	10.96.192.1/1 10.204.88.1/2	9 2	Example Subnet: 10.11.1.2/	24						
Test Co	onnection	Test Connection	1								
									E	ack Save	Cancel

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 31 Auto Response

	Reports Registered S	Servers Policy Catalog S	Security Resources Extensions	Automatic Responses	^ ~
Automation Automatic Responses New Response Import Responses					
Automatic Responses					Hide Filter
Preset: Quick find: Apply Clear SI	now selected rows				
Name A	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	
Choose Columns					
Delete					
Disable Responses					
Duplicate					
Edit					
Enable Personner					
Export Responses					
Export Table					
View					+
Actions > 1 of 6 selected					

Figure 32 Automatic Responses

	Dashboards	System Tree	Queries & Reports	Registered Serve	rs Policy Catalog	Security Resources	Extensions	Automatic Responses		^ ~
Automatic Respon	ises									
Response Builder	1 Description		2 Filter		3 Aggregation	> 47	ctions	5 Summary		
What is this response's name, target lang	juage, and event typ	e? Is the response er	abled?							
Name:	Pulse Policy Sec	cure Auto Response								
Description:	Pulse Policy Sec	cure Auto Response								
Language:	English	~								
Event:	Event group:	ePO No								
	Event type:									
Status:	 Enabled Disabled 									
								Back	Next Save	Cancel

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

Figure 33 Automatic Responses

	e "	Dashboards	System Tree Q	ueries & Reports	Registered Servers	Policy Catal	og Security F	Resources	Extensions	Automatic Responses		L _ ~
Automatic Res	Automation Automatic Responses											
Response Builder 1 Description 2 Filter 3 Aggregation 4 Actions 5 S							> 5 Summ	ary				
Which filtering criteria do you war	hich 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.											
Available Properties		Property		Comparison		Value						
Search X	*	Required Criteria										
	-	Defined at		System is in group	or subgroup	My O	rganization	•••	+			
Agent GUID		Threat										
Detected >		Contract	у	Equals		 Emer 	gency	~	-			
Detecting Product >												
Detecting Product DAT \ >			and/or	Equals		 Critic 	al	~	1. A.			
Detecting Product Detec >			and for	Fauals		Alert		~				
Detecting Product Engin			anayor	Equais		AIGIC						
Detecting Product Host												
Detecting Product IP ad >												
Detecting Product IPV4 >												
Detecting Product MAC . >												
Detecting Product Name												
Detecting Product Versic >												
Event Description >												
OS Platform >												
OS Type												
Received >	-											
										В	ack Next	Save Cancel

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

Figure 34 Aggregation

\equiv \bigcup McAfee [*]	Dashboards System Ti	ee Queries & Reports	Registered Servers	Policy Catalog	Security Resources	Extensions	Automatic Responses			
Automatic Respon	ses									
Response Builder	1 Description	> 2 Filter	3 А	\ggregation	4 /	ctions	> 5 Summa	ary		
Vhat kind of aggregation, grouping, and throttling behavior should this response have?										
Aggregation:	Trigger this response for eve Trigger this response if multi When the number of dist Property: Agent G or When the number of eve	ry event. ple events occur within: 30 m inct values for an event property is at JID nts is at least: 100	inutes t least a certain value. Number of distinct values: 2	100						
Grouping:	 Do not group aggregated evo Group aggregated events by 	ents. Agent GUID								
Throttling:	At most, trigger this respons	e once every: 1 hours								
							В	ack Next Save Cano		

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.

≡	🕽 McAfee	Dashboards	System Tree	Queries & Reports	Registered Servers	Policy Catalog	Security Resources	Extensions	Automatic Responses		^ ~
Automati Auto	on Imatic Respo	nses									
Response What action	Builder 1s do you want this response	1 Description	ed?	2 Filter	\rangle	3 Aggregation	4.4	ctions	5 Sum	mary	
✓ Pulse P	Policy Secure Response 💙										٠
PPS Action	event-id: {listOfThreatEn {listOfThreatName}	ventID},srcip:{listO	ofSourceIPV4},threa	tSeverity: {listOfThreatSe	verity},threatName:						
	Insert variable: List of A	All Values	✓ Agent GUID	~	Insert						
										Back Next S	ave Cancel

For more information on McAfee ePO server 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.

0				N. S. B. W. B.	Pulse Policy Secure
N PU	LSE SECURE System Author	entication Administrators	Users Endpoint Policy	Maintenance Wizards	T •
Reports > Infected	Devices				
Infected Devic	es				
Reports	i ices Report				
User Summary	y Single User Activities Device Summary	Single Device Activities	Device Discovery Application Disc	overy Authentication Comp	Behavioral Analytics
Infected Devi	ces Report Download Report: CSV Tab Delimited				
Device Status: Qu	arantined Username: IP Address:	MAC Address:	Apply Filter		
Clear Host *Below listed device	Clear All Hosts s 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.

SPulse Secure	System Authentication Administrators	Users Endpoint Policy	Maintenance Wizards	Pulse Policy Secure on PPS_176
Troubleshooting > Monitoring > Debug Log			System	♥ User Sessions Remote Debugging
Debug Log			Import/Export	Policy Tracing
User Sessions Monitoring Tools	System Snapshot Remote Debugging		Push Config	✓ Monitoring
Debug Log Node Monitor Cluster Diagnostic Lo	iĝs		Archiving	Debug Log Node Monitor
Save Changes Reset Save Debug Lo	g Clear Log		Troubleshooting	Cluster Diagnostic Logs
♥ Debug Log Settings				✓ Tools
Current Log Size Debug Logging On	5078 bytes			Commands Kerberos
Max Debug Log Size	200 MB			System Snapshot
Debug Log Detail Level	50		A positive number	
Include logs			Selecting this option will includ	e system logs
Process Names:			Comma separated, list of proces	is names to log
Event Codes:	integrations		Comma separated, list of events	s to log

Verify Audit/Threat Event logs on McAfee ePO Server

Figure 35 Audit logs

≡ 🗂 McA	fee [®] Dashi	boards S	ystem Tree Qu	ueries & Reports	Registered Servers	Policy Catalog	Security Resources	s Extensions	Automatic Res	sponses	
Reporting Audit Log	Purge										
udit Log											Hi
Preset:	Custom: None	Quick	find:	Apply Clear							
ser Name	Priority	Action		Details			9	luccess		Start Time	
system	High	Pulse Policy	Secure : Auto Respons	se Event sent to P	PS server 10.00.200.08 succ	essfully		Succeeded		4/14/20 11:03:04 P	M IST

Figure 36 Threat Event Logs

	McAfee	Dashboards S	ystem Tre	e Queries & Reports	Registered Servers	Policy Catalog S	ecurity Resources	Extensions A	utomatic Responses	
Re T	Reporting Threat Event Log									
Thre	at Event Log : Threat events	received from managed sy	/stems							
Pre	Preset: Custom: Quick find: Last 7 days None Apply Clear 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	1	None		
	4/14/20 11:09:43 PM IST	4/14/20 11:11:53 PM IST	1095	Access Protection rule violation de	etected and NOT blocked	'File' class or access		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.