Pulse Policy Secure: McAfee ePO

Integration Guide

Product Release	9.1R8
Published	July 2020
Document Version	1.0

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

www.pulsesecure.net

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) Server

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

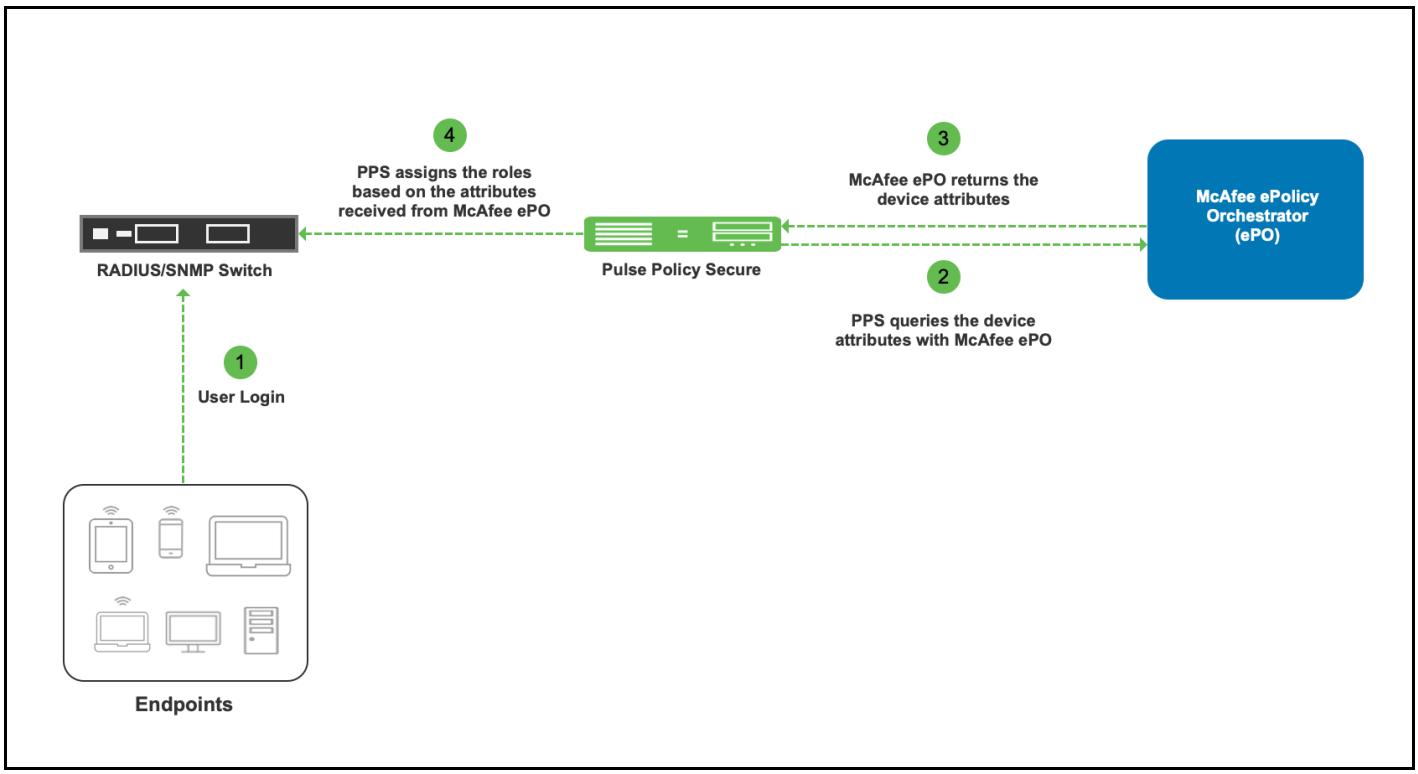
The following use cases are supported with PPS and McAfee ePO server integration:

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

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

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

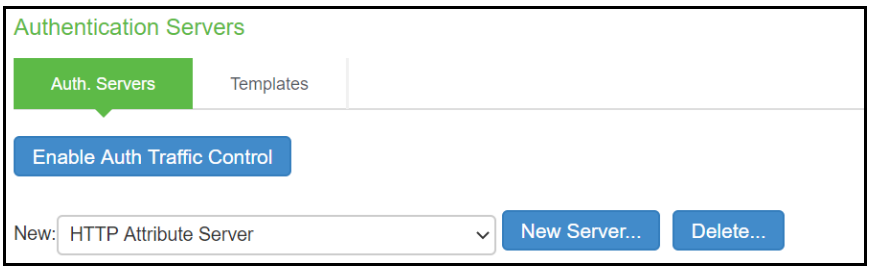


Figure 3 Template

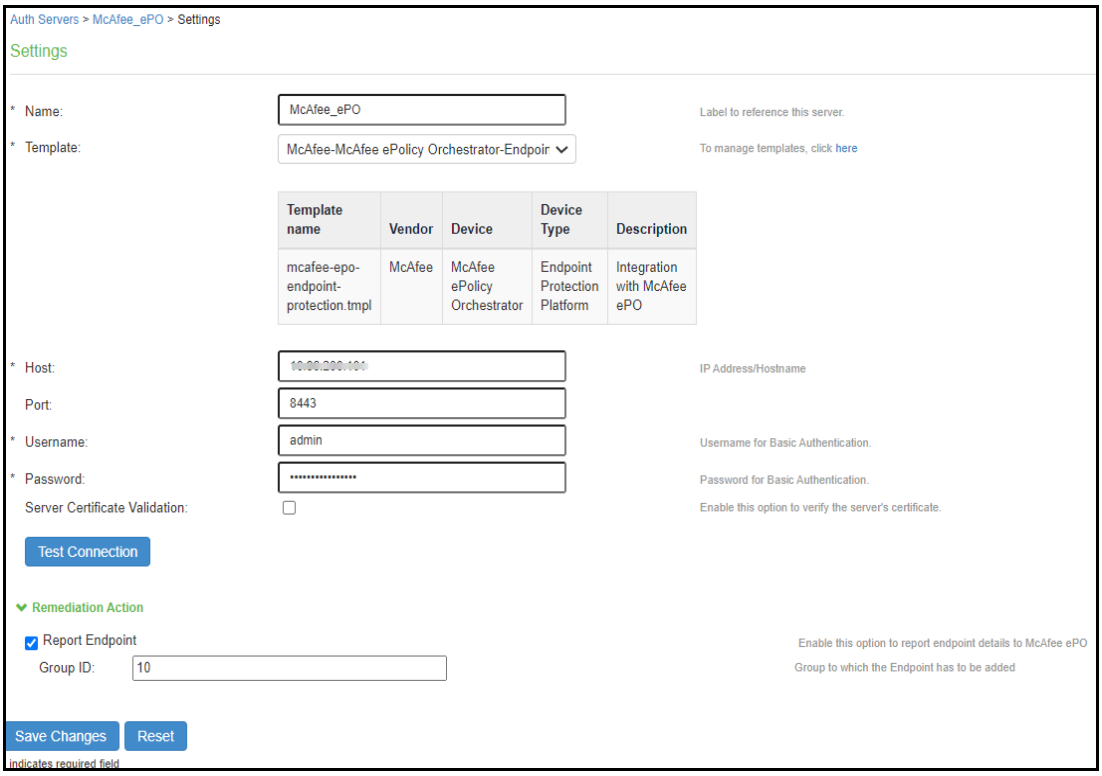
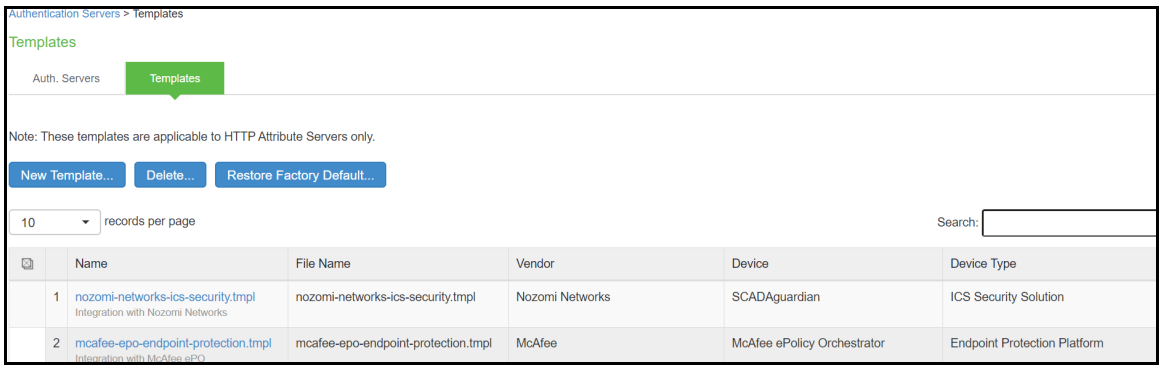


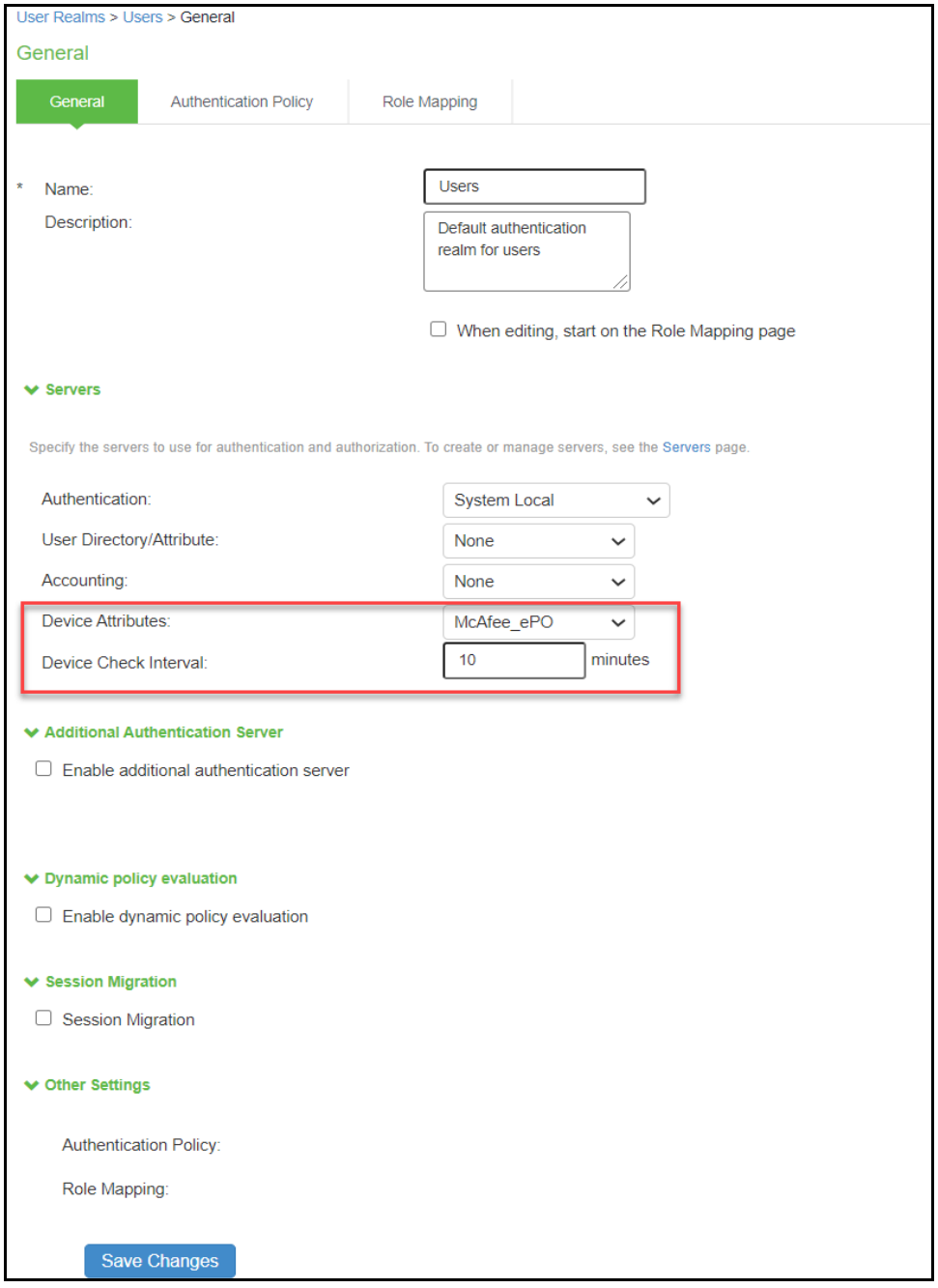
Figure 4 Available Templates



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.

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

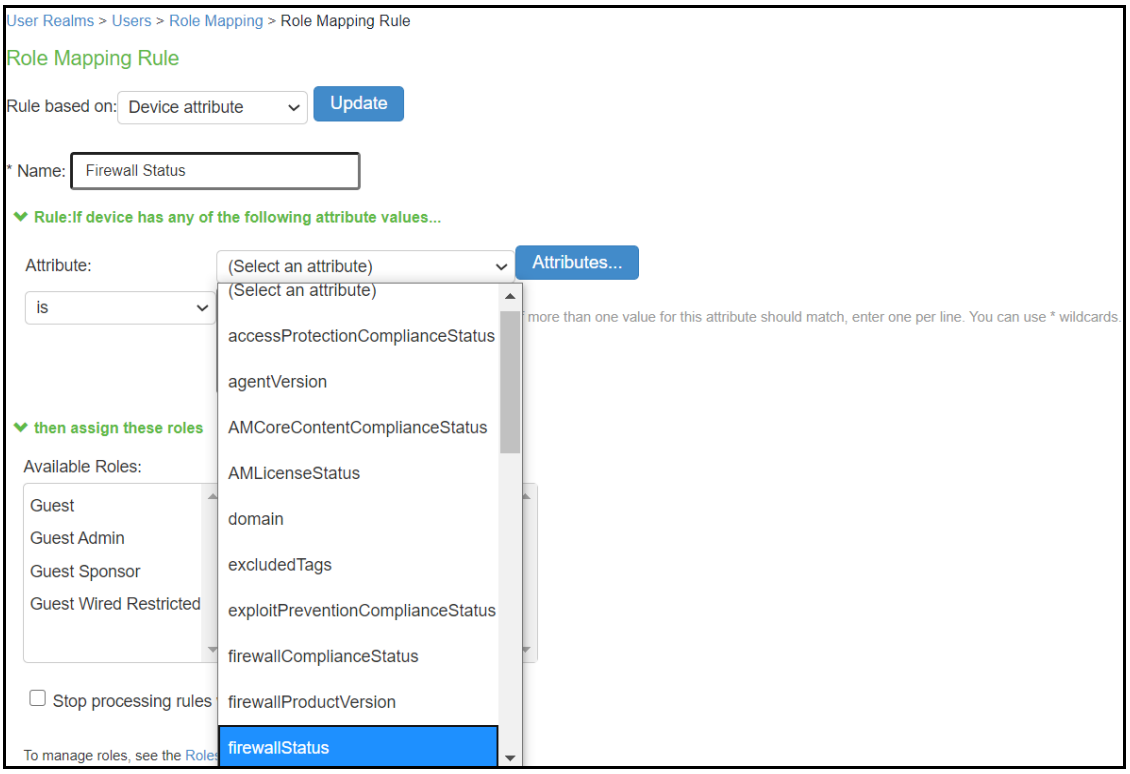
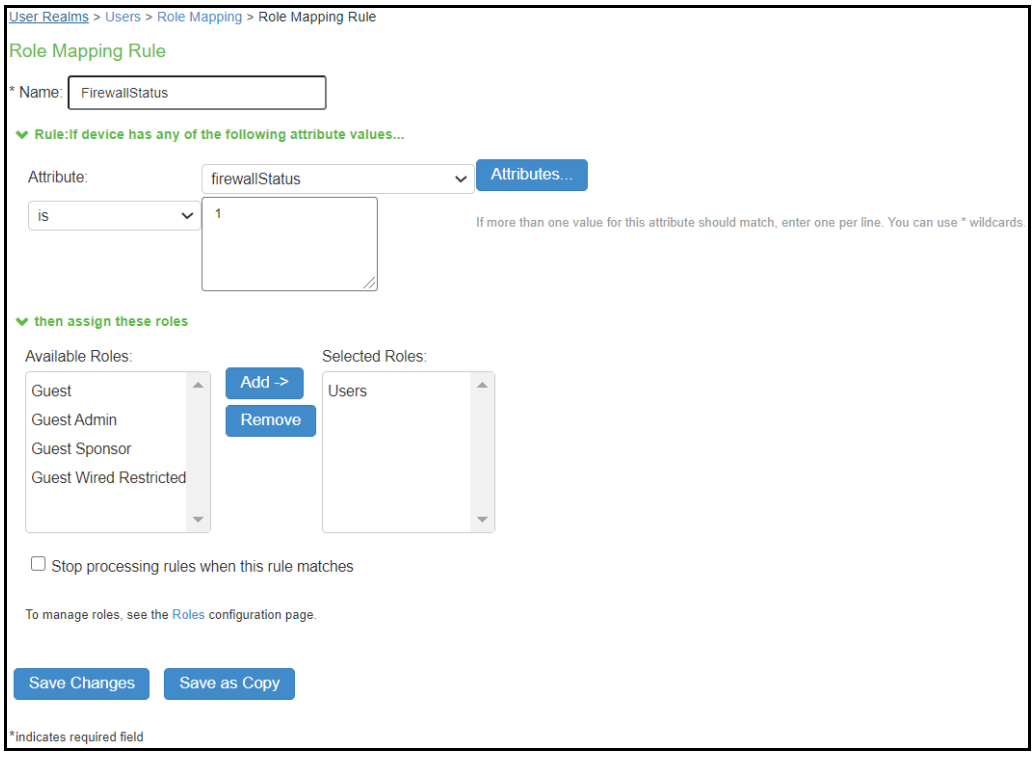


Figure 7 Role Mapping Rules



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

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.

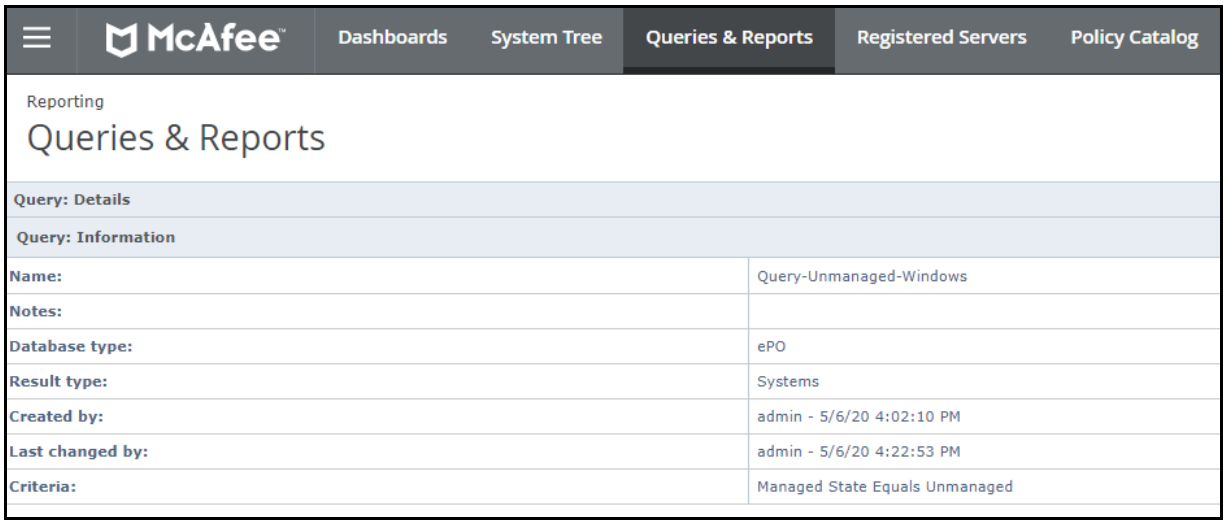
McAfee ePO Server Configuration

Server Task to Install McAfee Agent on Unmanaged Devices

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.

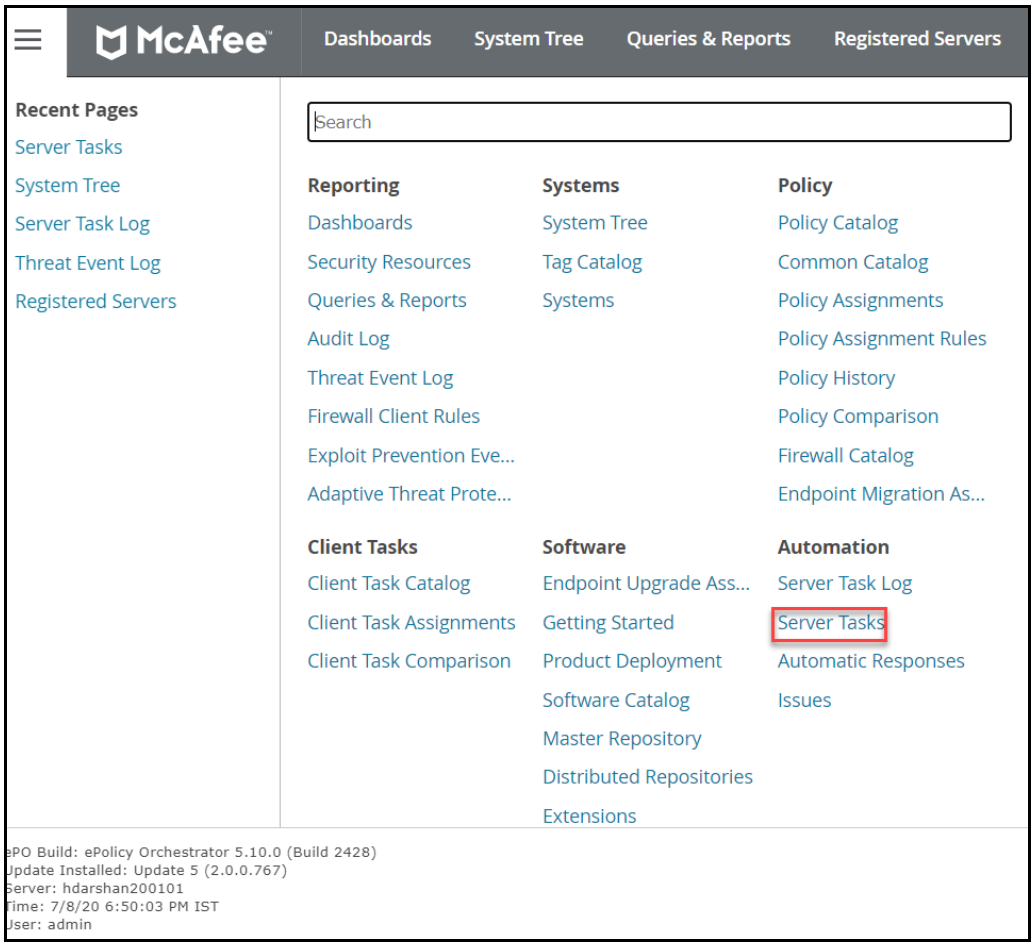
1. Sample Query to list unmanaged devices.

   Figure 9 Sample Query



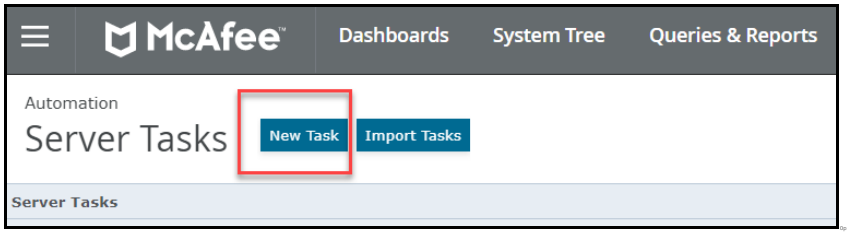
2. To create a Server Task, login to McAfee ePO server and under Automation, select **Server Tasks**.

Figure 10 Server Tasks



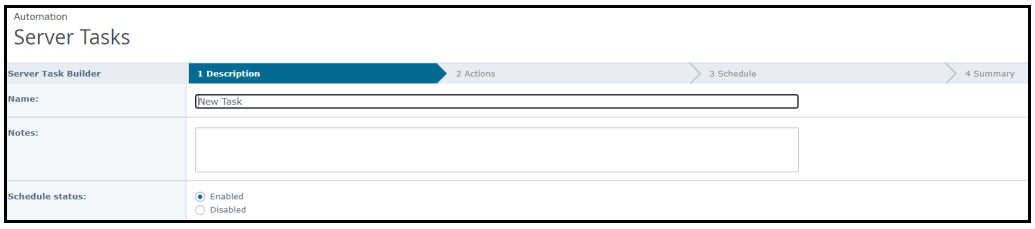
3. Click **New Task**.

Figure 11 Task



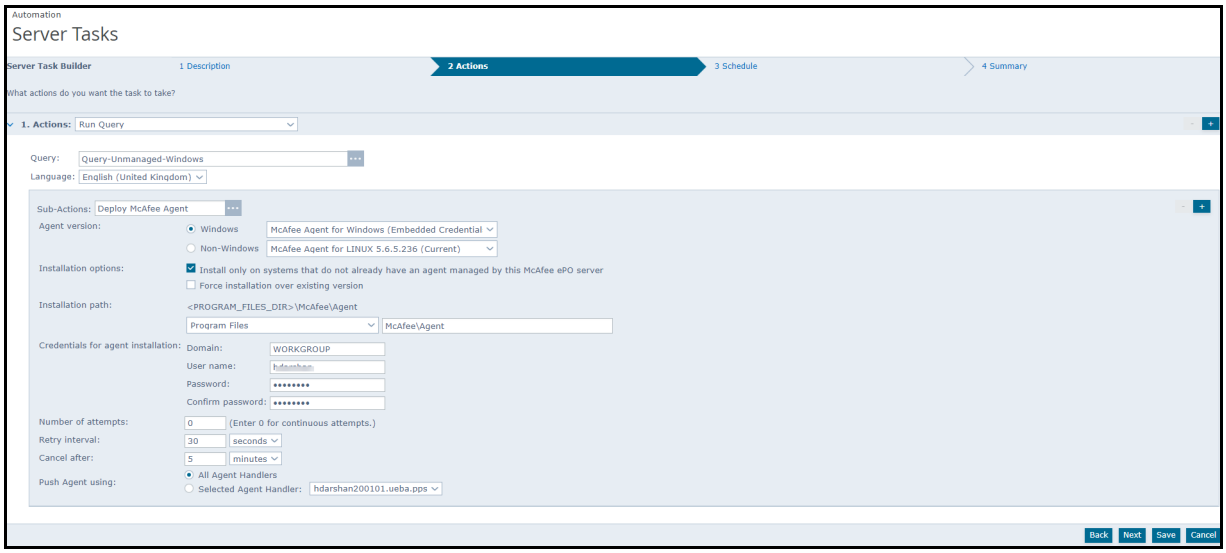
4. Enter the name for the task.

Figure 12 Task



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

Figure 13 Actions



6. Schedule the installation.

Figure 14 Server Tasks

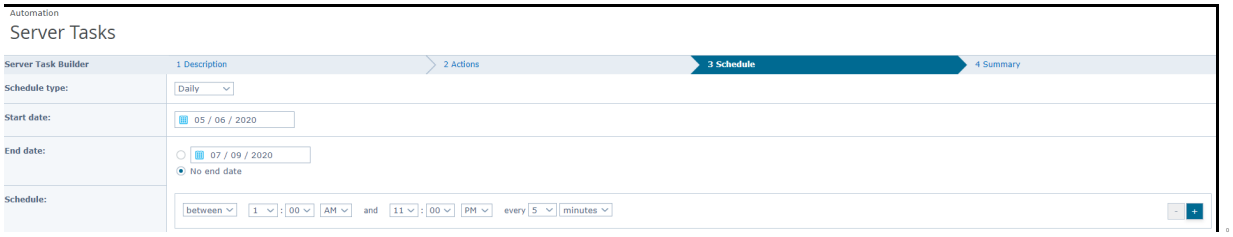


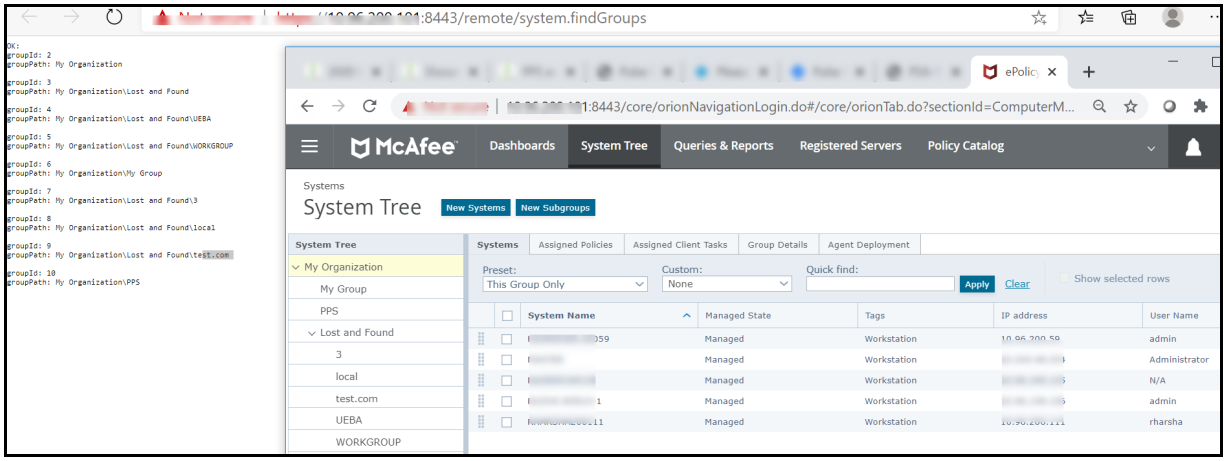
Figure 15 Summary

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



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

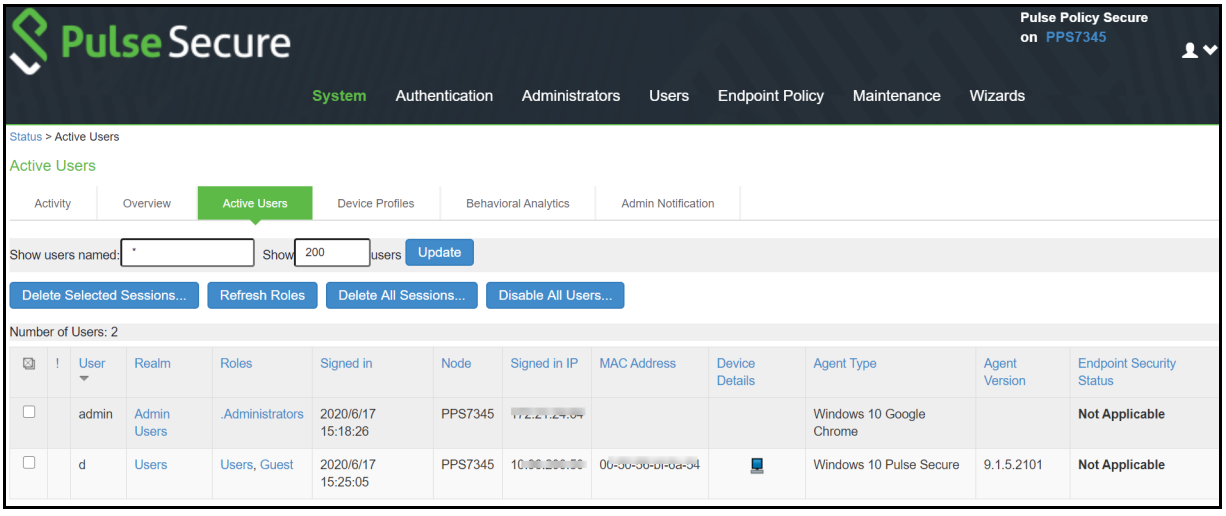
Troubleshooting

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 Active Users



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

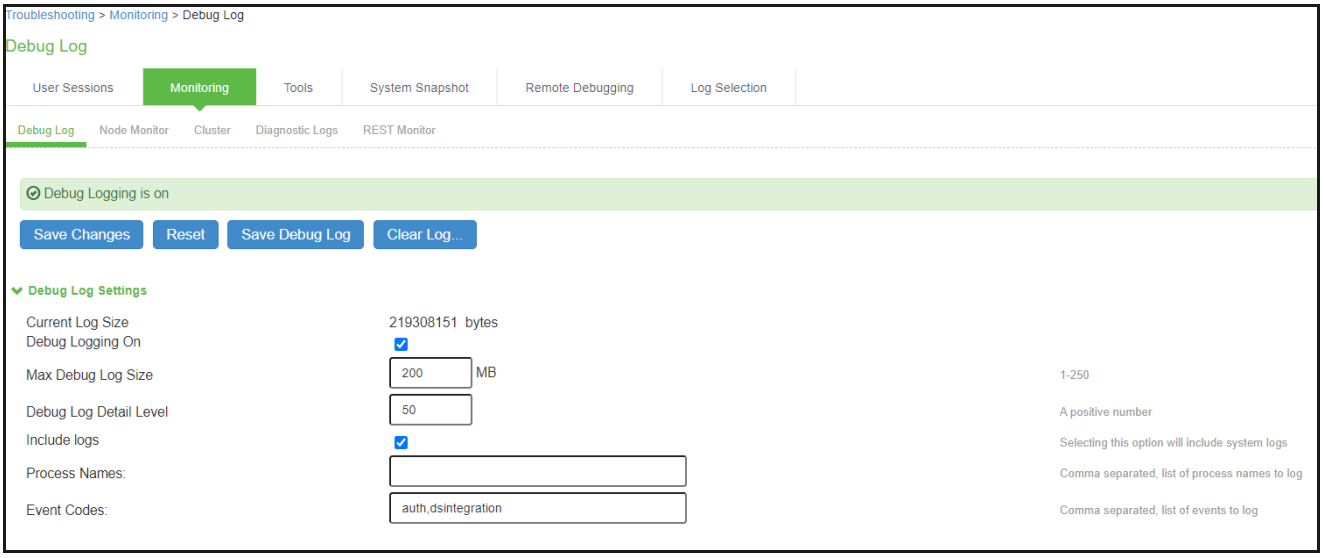


Figure 18 Attribute Server Events

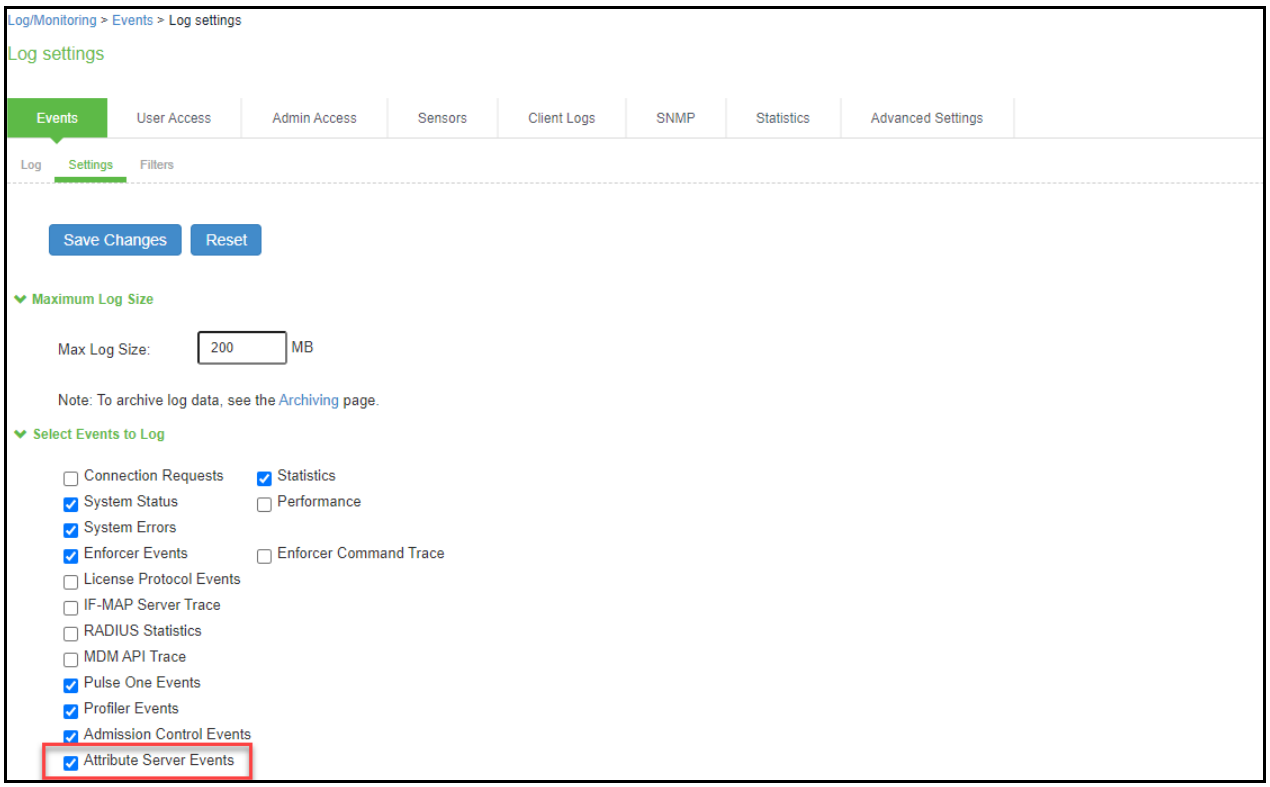
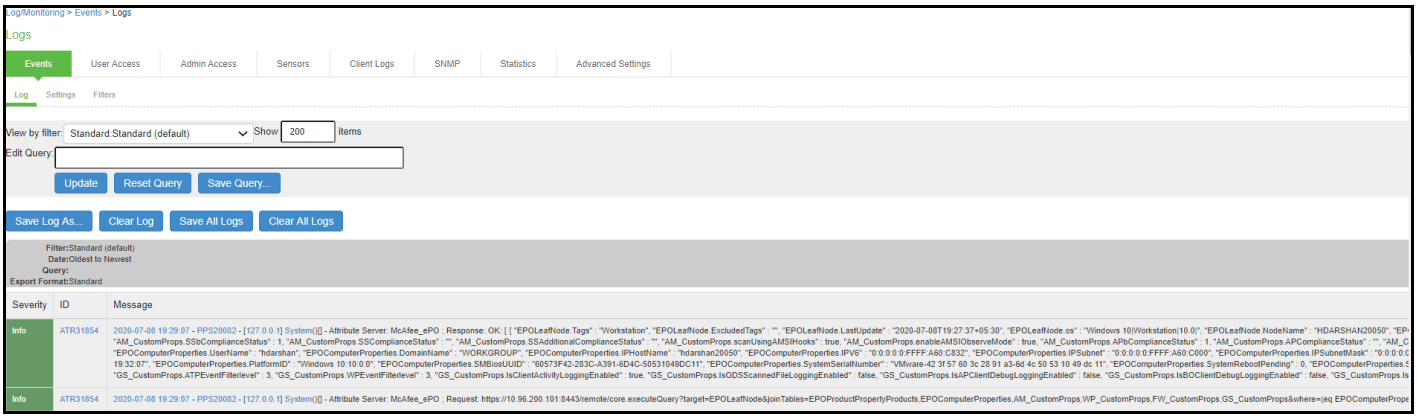


Figure 19 Logs



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: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

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.

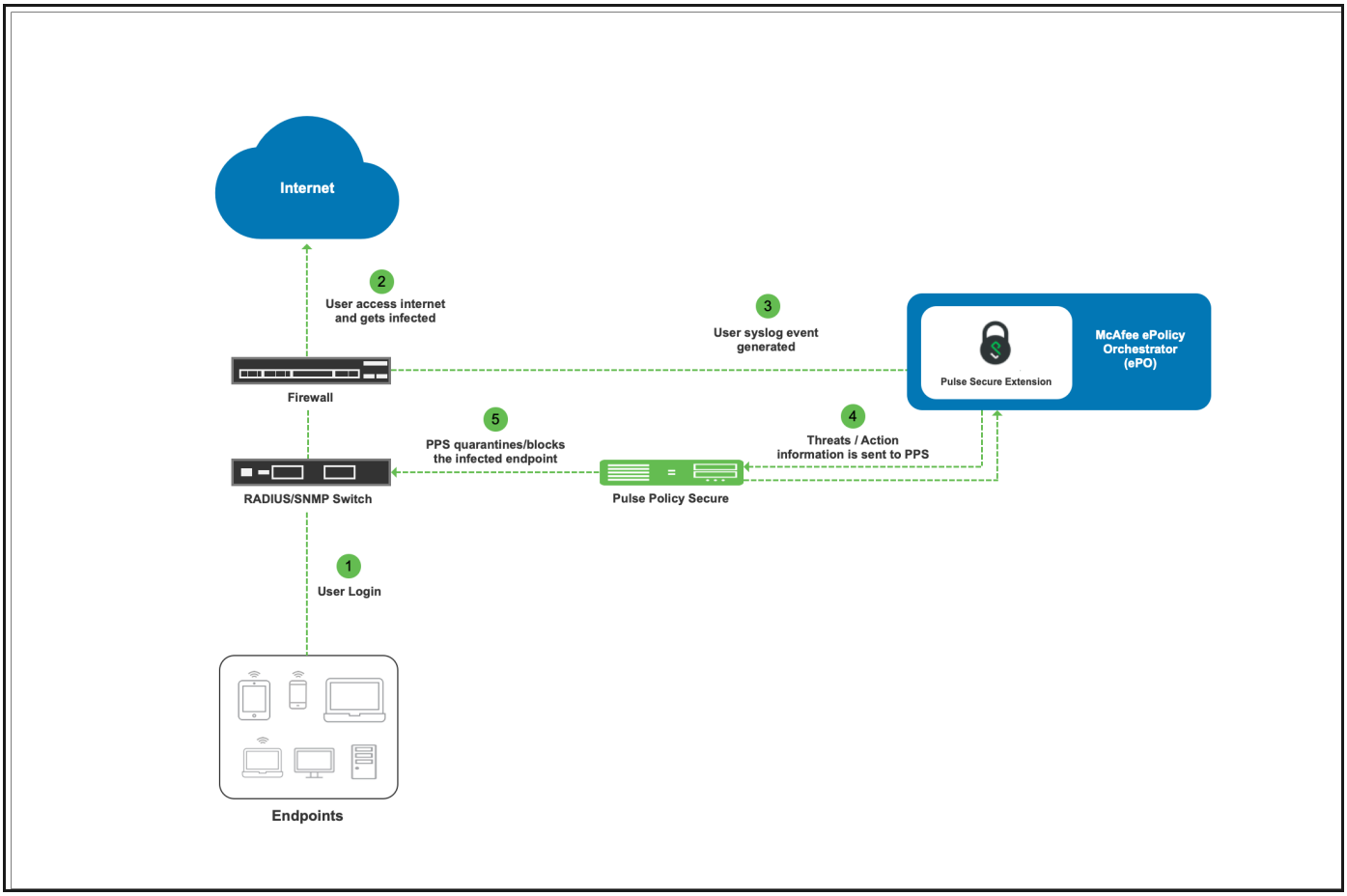
If ePO detects that an endpoint on the network has become non-compliant, ePO can send PPS the non-compliant IP address and an event label. PPS resolves the event as a property on the endpoint, and can take automated actions until the endpoint is remediated and becomes compliant.

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 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:

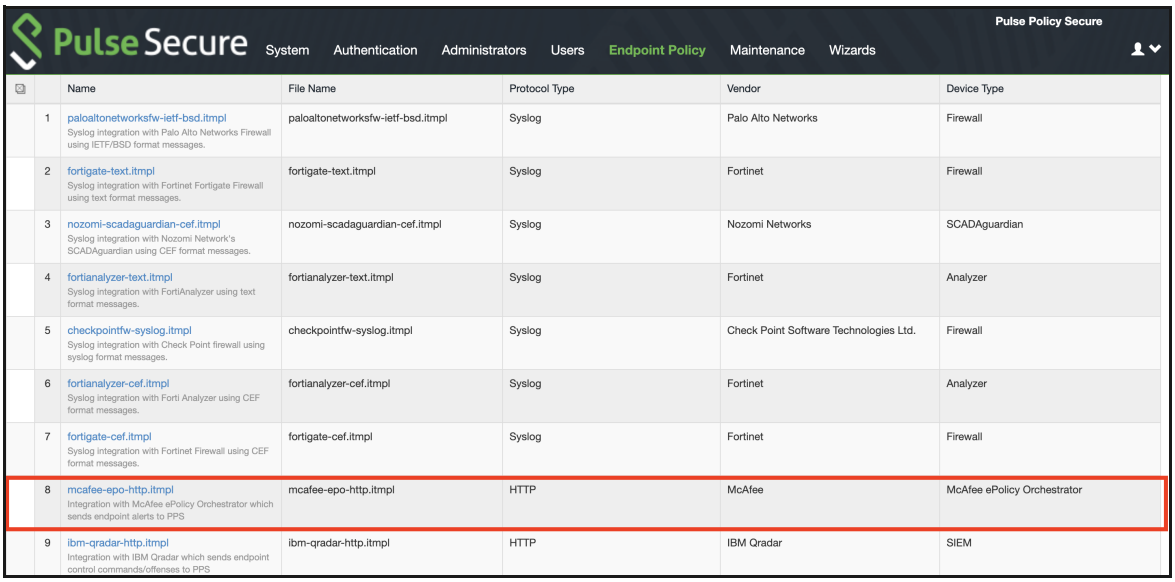
Admission Control Template

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



	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

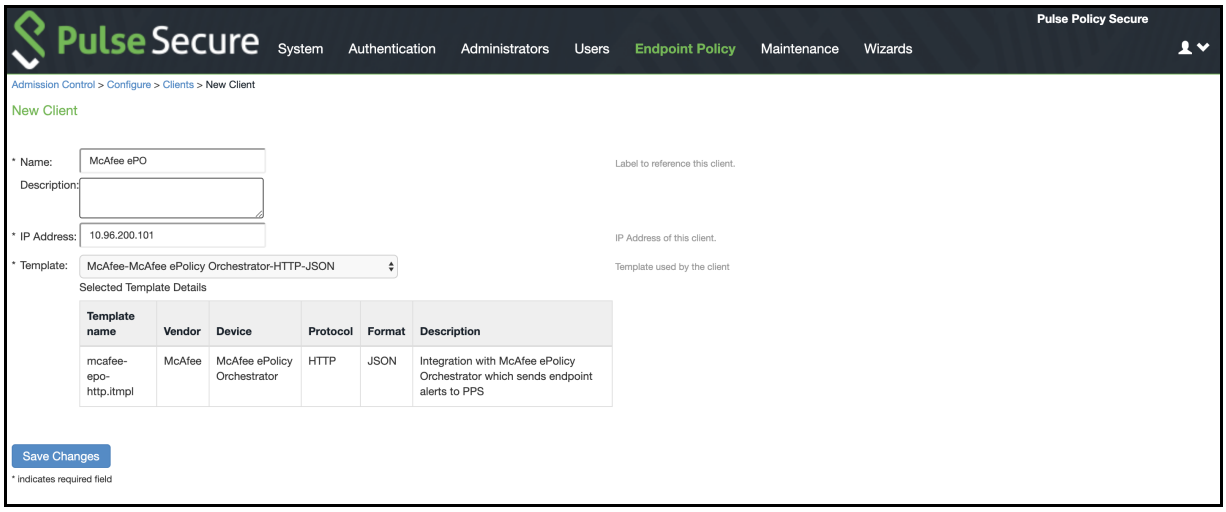
Admission Control Client

The admission control clients are the network security devices on which the REST API is enabled. McAfee ePO 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 Template



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.

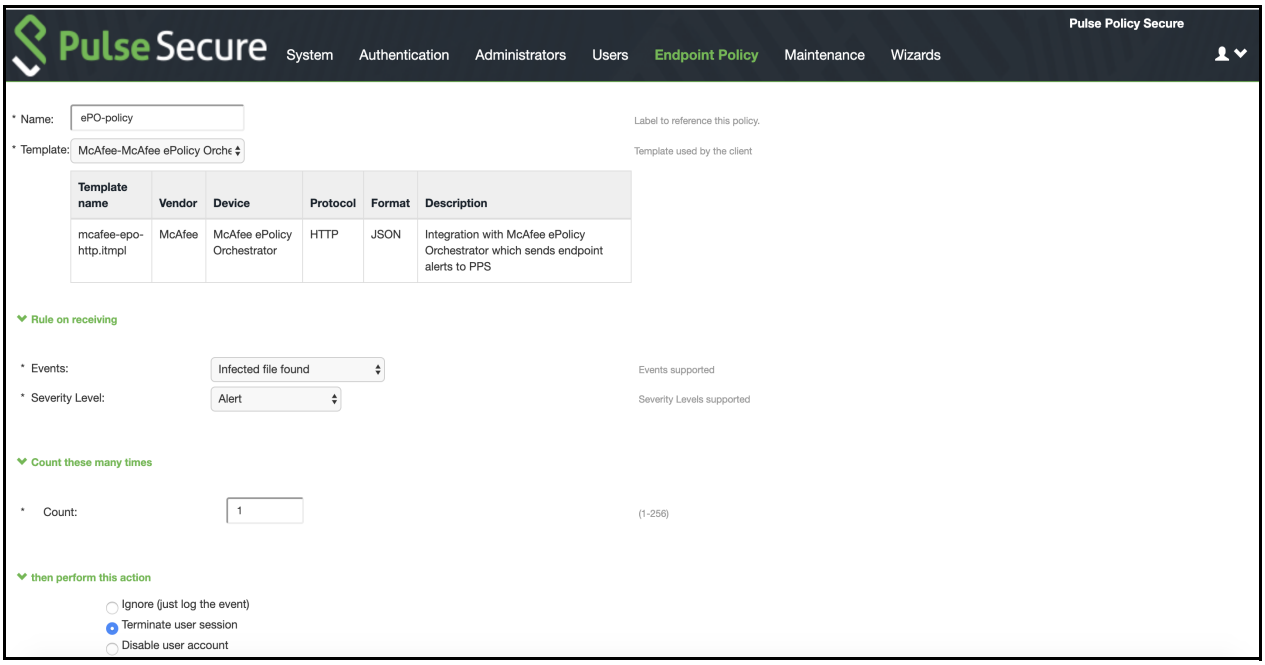
1. To view and add the new integration policy:
2. Select **Endpoint Policy > Admission Control > Policies**.
3. Click **New Policy**.
4. Enter the policy name.
5. Select **McAfee-McAfee ePolicy Orchestrator-HTTP-JSON** as a template.
6. Under Rule on Receiving, select the event type and the severity 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.

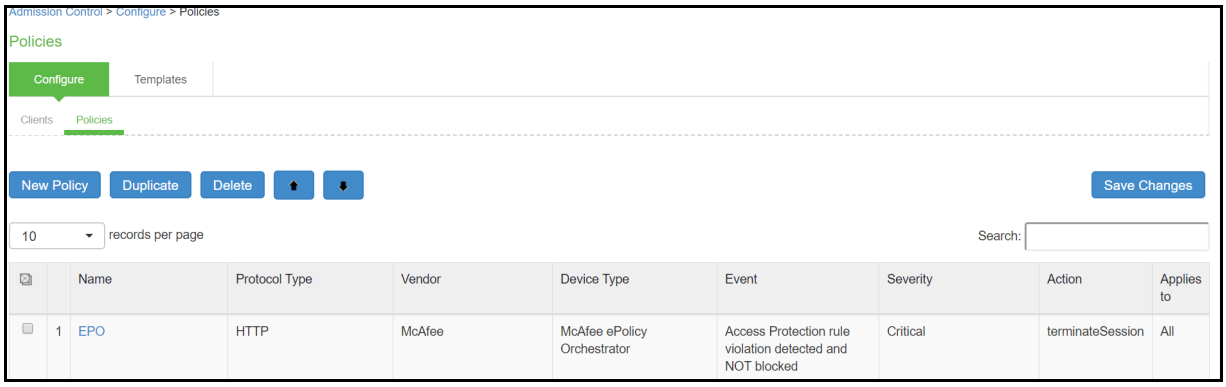
Figure 23 Configuration Policies



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



Configuring McAfee ePO Server

This section covers the following topics:

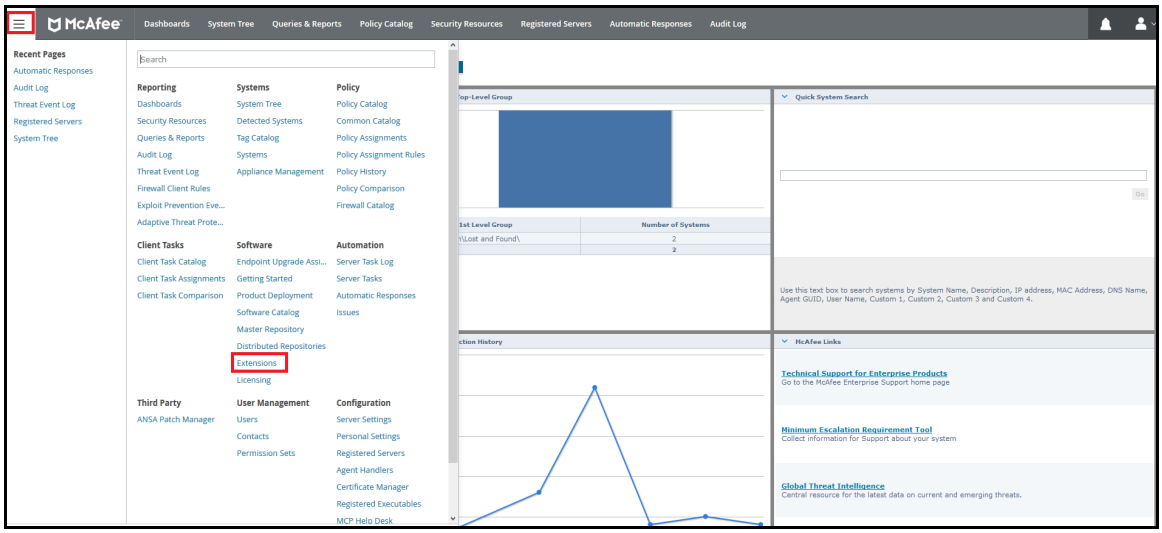
Install Pulse Policy Secure Extension for McAfee ePO

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:

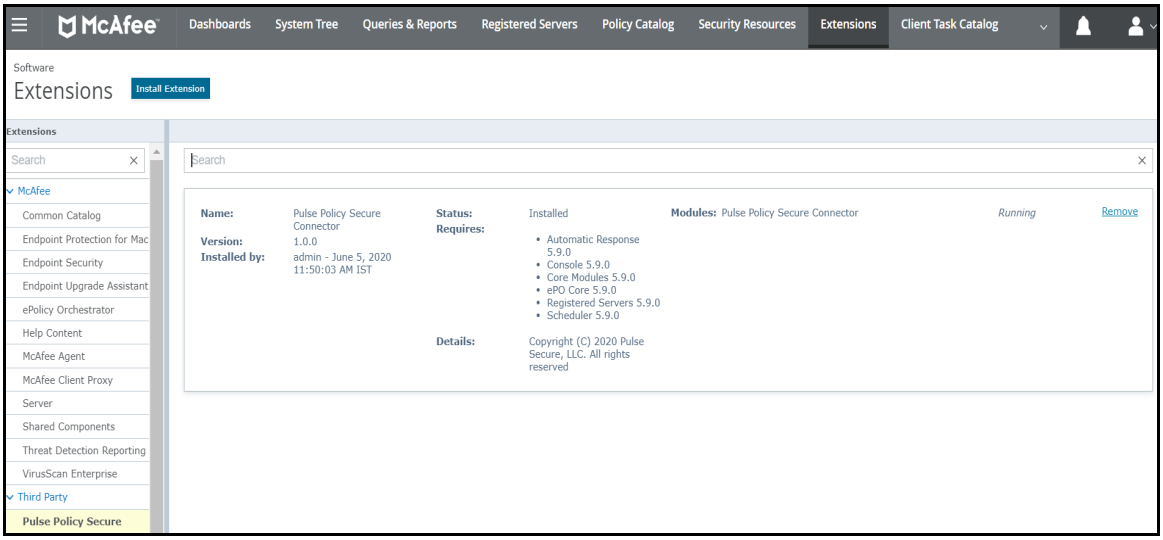
1. Log into McAfee ePO server as an Admin user.
2. In the McAfee Dashboard, select the **Extensions**.

   Figure 25 McAfee extension



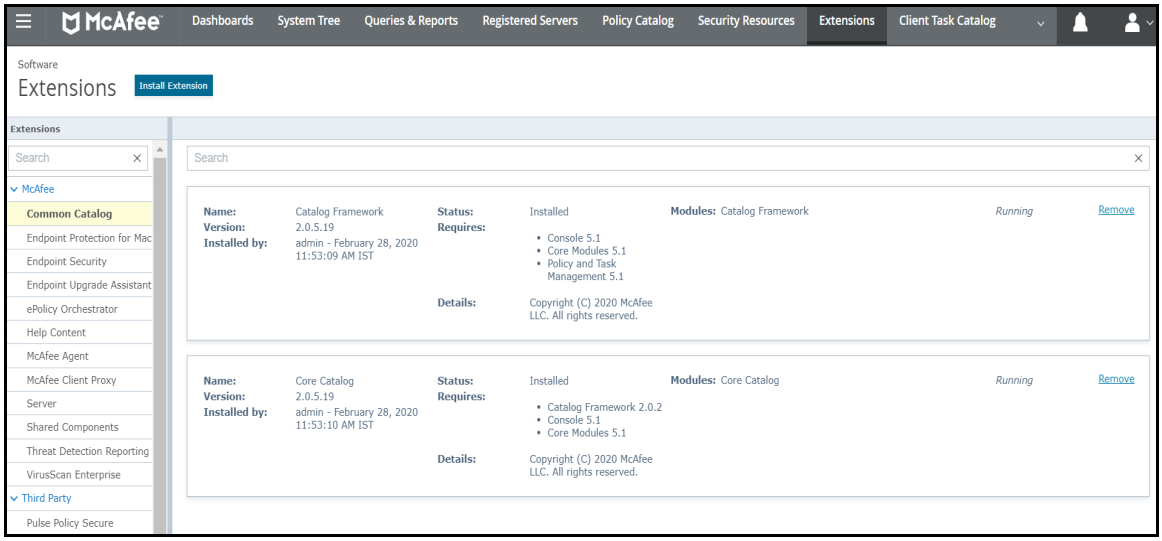
3. Click **Install Extension**.

   Figure 26 Install Extension



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 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

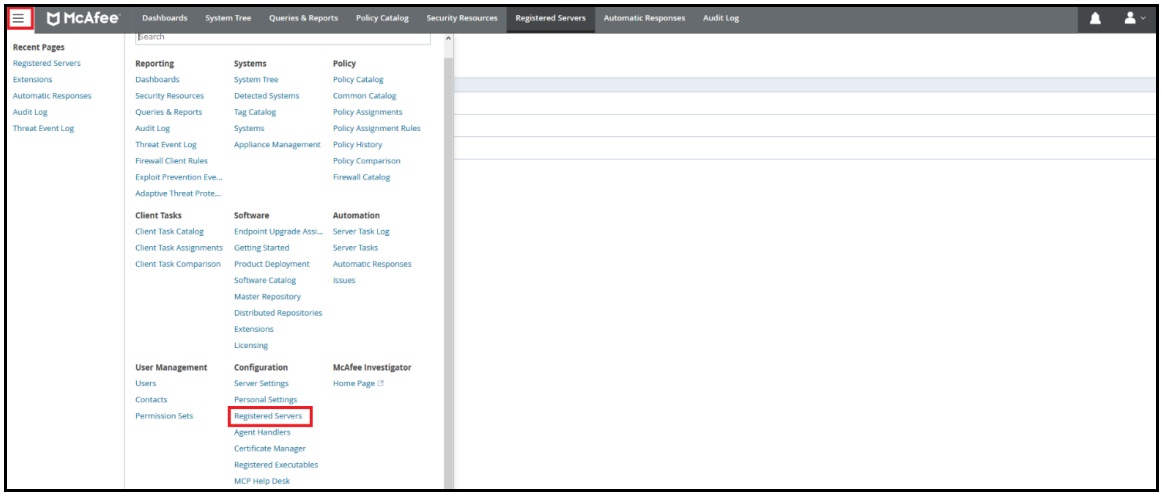
Registered Servers

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.

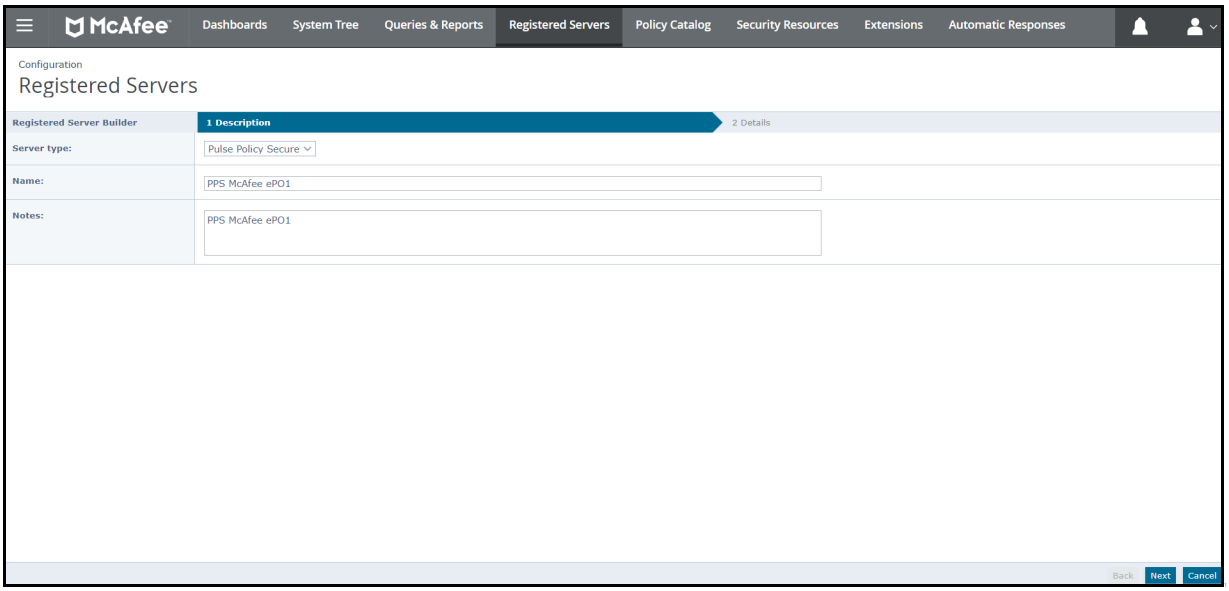
1. Log into McAfee ePO server as an Admin user.
2. Open the Main Menu, under Configuration Click **Registered Servers**.

   Figure 28 Configuration



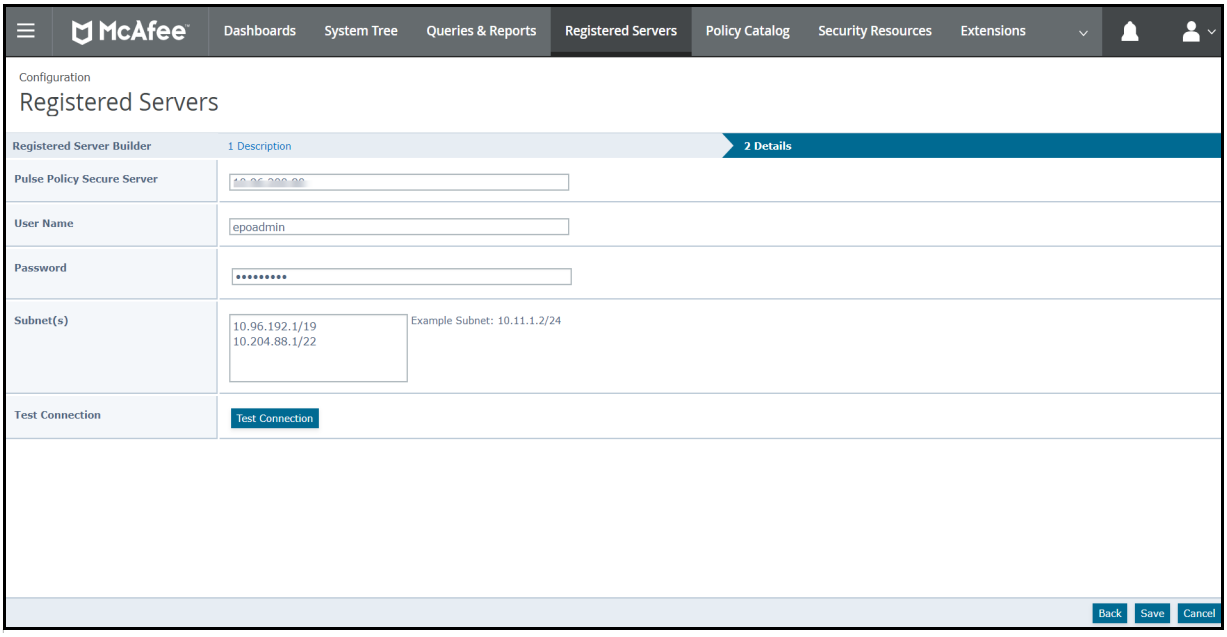
3. Click **New Server**.
4. Select Server Type as **Pulse Policy Secure**.
5. Enter the name of the server.
6. Click **Next**.

   Figure 29 Registered Servers



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



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

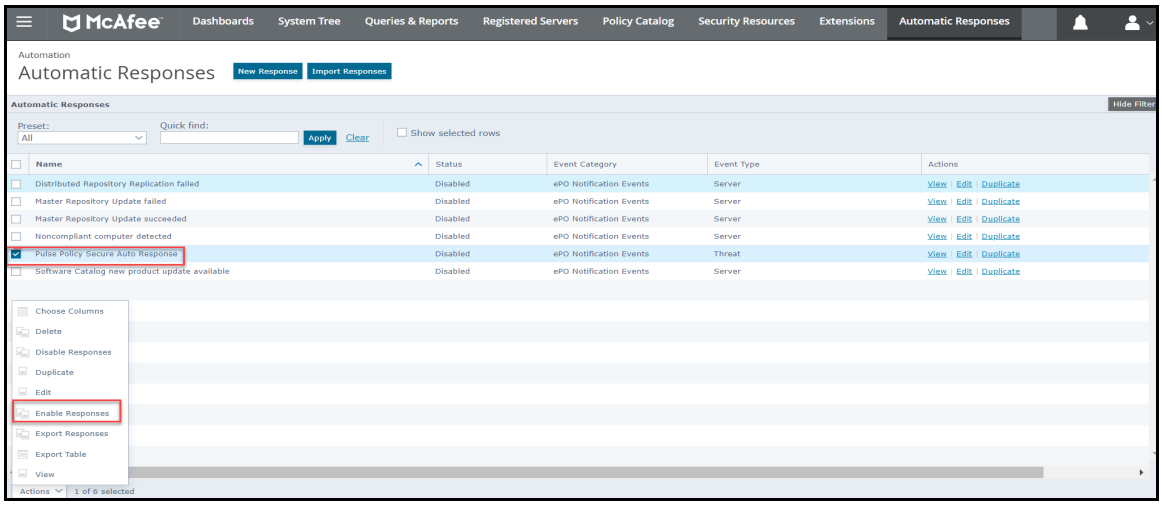
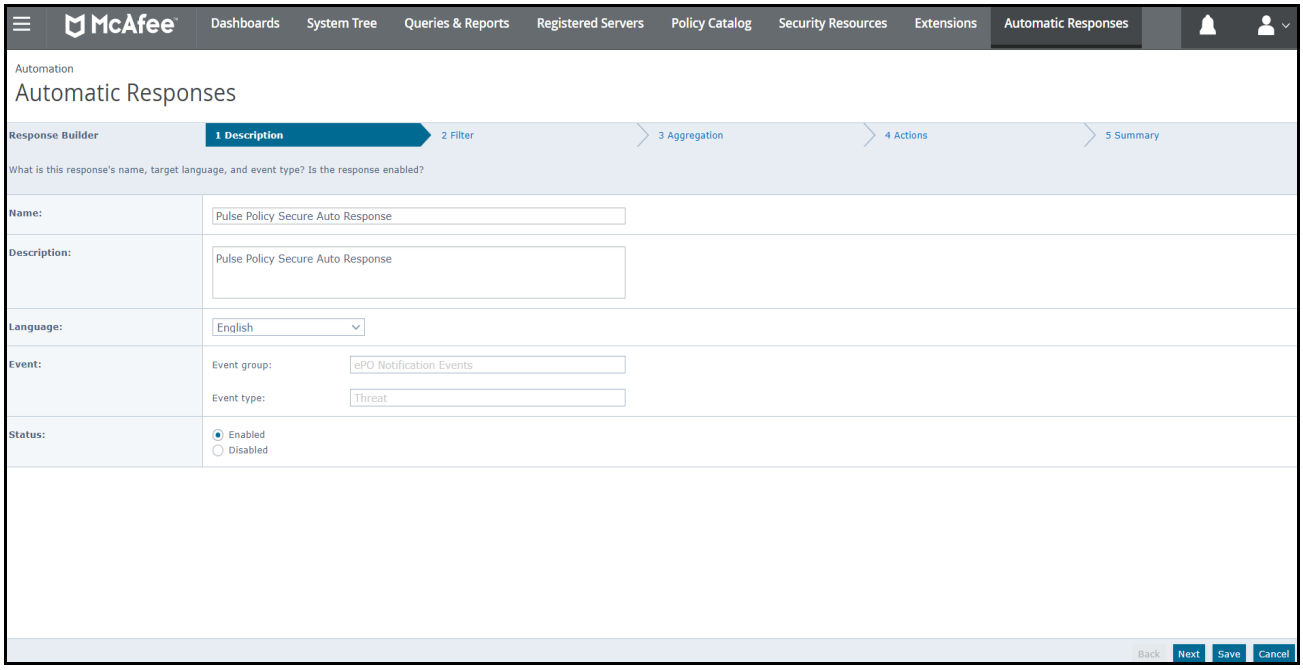
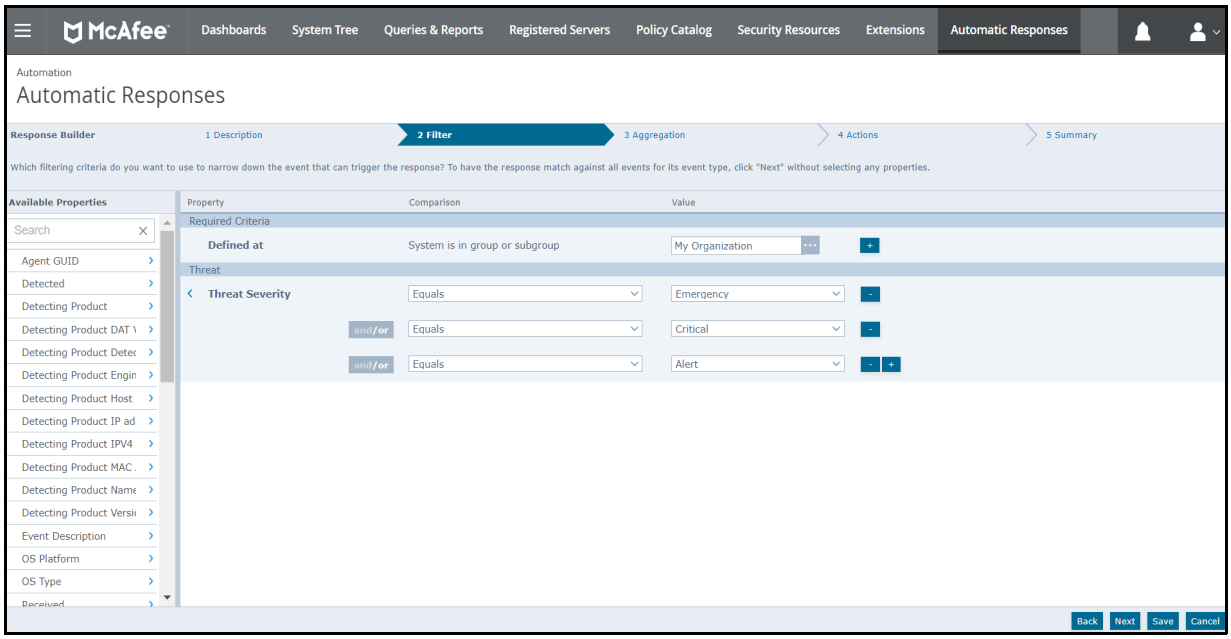


Figure 32 Automatic Responses



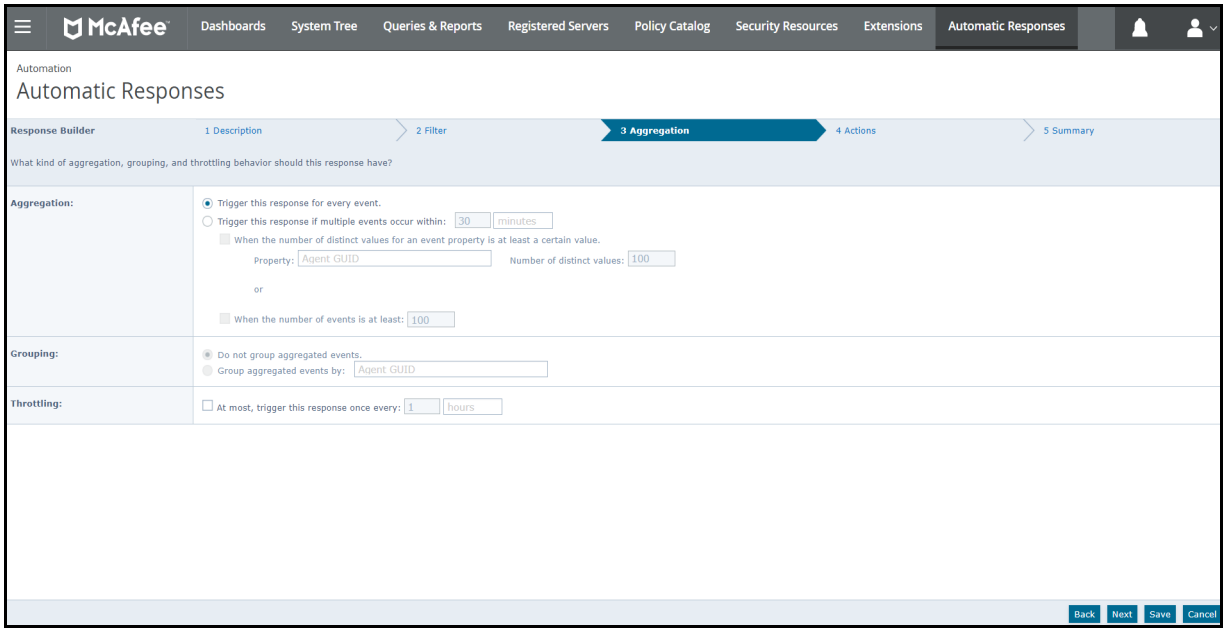
4. Add the filters for the incoming events. For example, Source IP address, Threat Event-ID, Threat severity and so on.

Figure 33 Automatic Responses

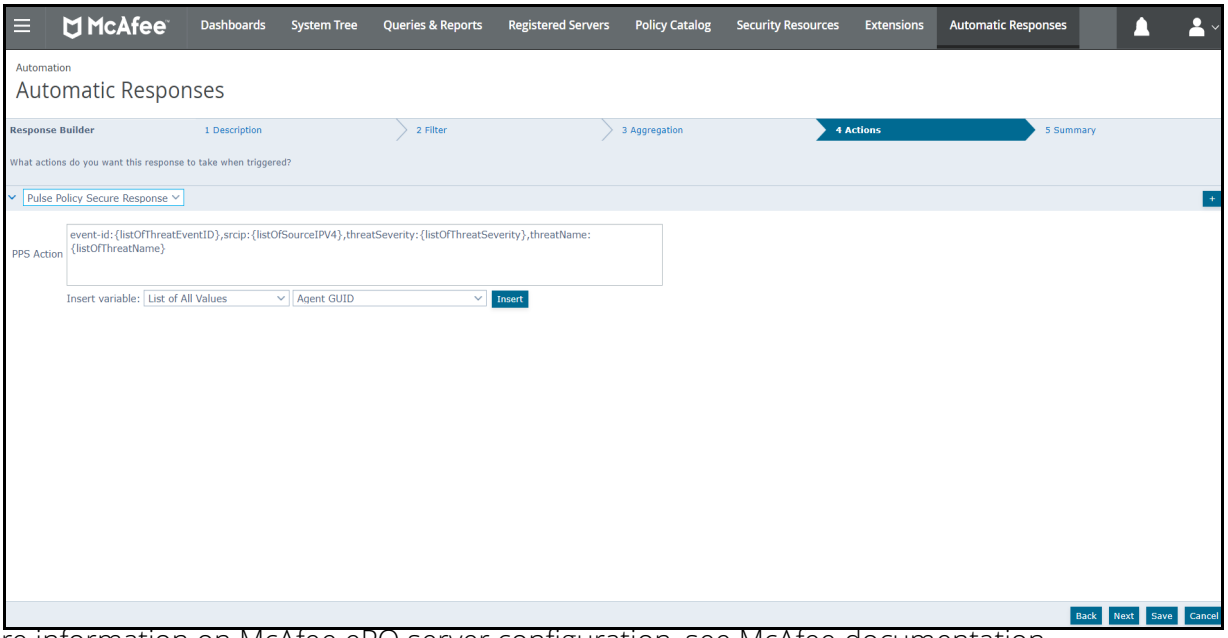


5. Automatic response is sent for every event or specific event(s). The trigger conditions is defined on the "Aggregation" page.

Figure 34 Aggregation



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.



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

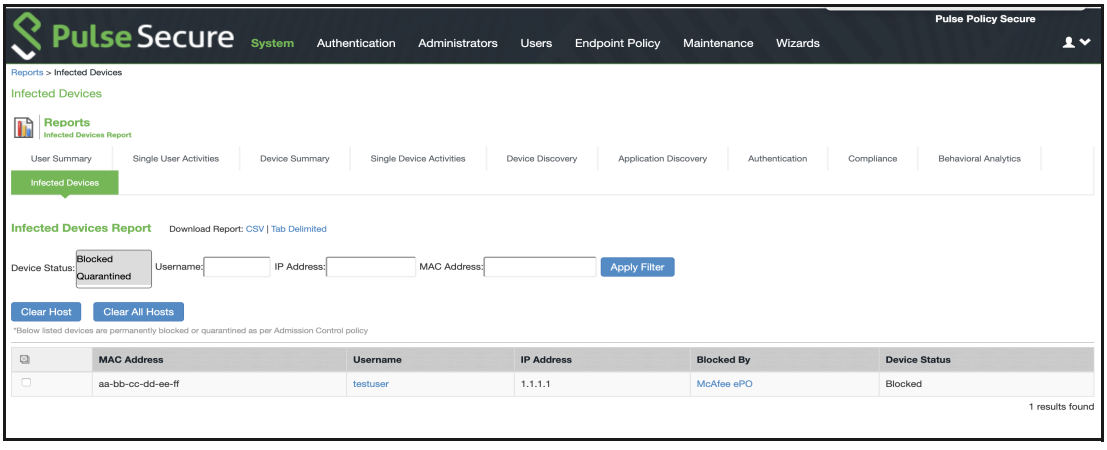
Troubleshooting

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

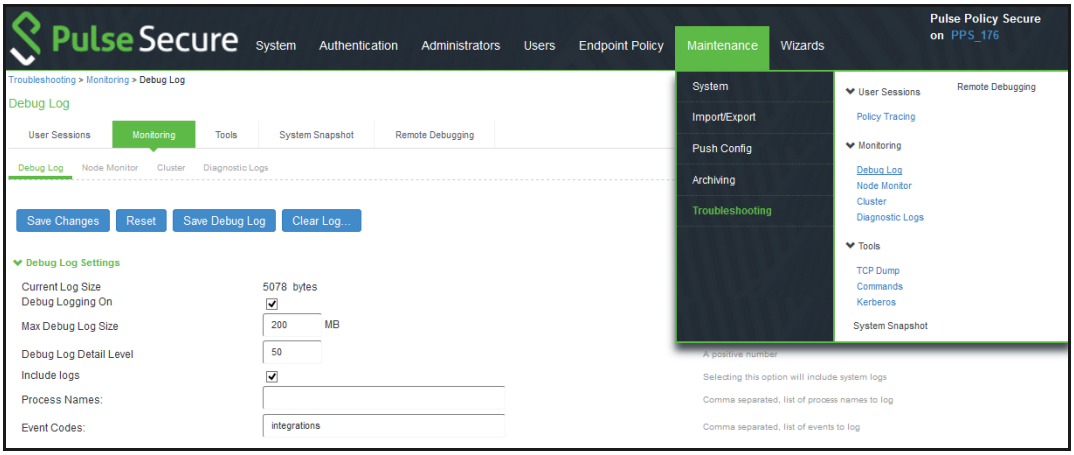
You can verify that the event logs are generated every time when an event is received from McAfee ePO.

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.



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



Verify Audit/Threat Event logs on McAfee ePO Server

Figure 35 Audit logs

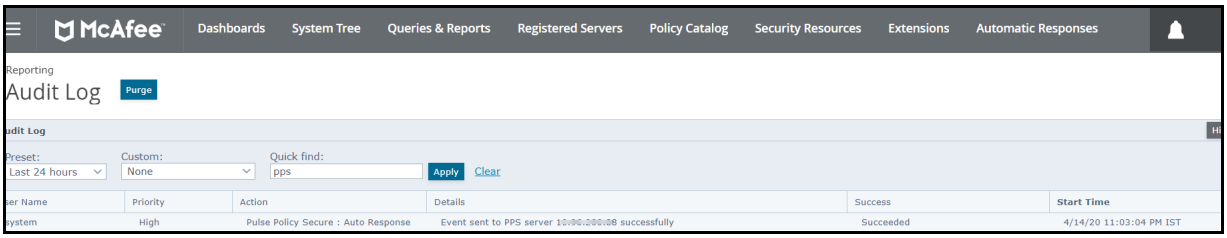
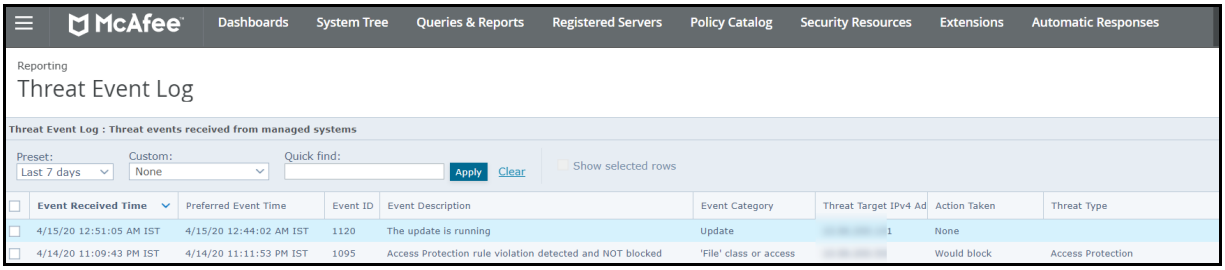


Figure 36 Threat Event Logs



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.