McAfee MVISION Connector App for QRadar

Contents

Overview 2
Terms and Definitions 2
Architecture 2
Pre-requisites 3
    Apply MVISION ePO Tag 3
    MVISION ePO Device Details 3
    Poll Threat Events from MVISION ePO 4
    Software version and platform details 8
Step by Step Instruction to use McAfee MVISION Connector for QRadar App 8
    Acquiring client credentials from McAfee Marketplace 8
    Configure/Provision McAfee MVISION Connector for QRadar App 8
    Apply MVISION ePO Tags 13
    MVISION ePO Device Details 16
    Create/Update EDR Investigation for an offense in QRadar 17
    Poll Threat Events from MVISION ePO to Log Activity on QRadar 20
        Poll Configuration 21
    Audit Log 24
Important things to know 24
    Steps to follow if exception is displayed while clicking on Create/Update EDR Investigation button 24
    Steps to follow if ‘SSL: CERTIFICATE_VERIFY_FAILED’ message appears in app log 25

Overview

As part of our “Together is Power” strategy, we have built a new eco system wherein we have enabled our key McAfee products (MVISION ePO and MVISION EDR) features inside the IBM’s QRadar (SIEM) server. We have created “McAfee MVISION Connector” for QRadar app to implement this eco system and it will provide the following actions for IBM QRadar admin users:

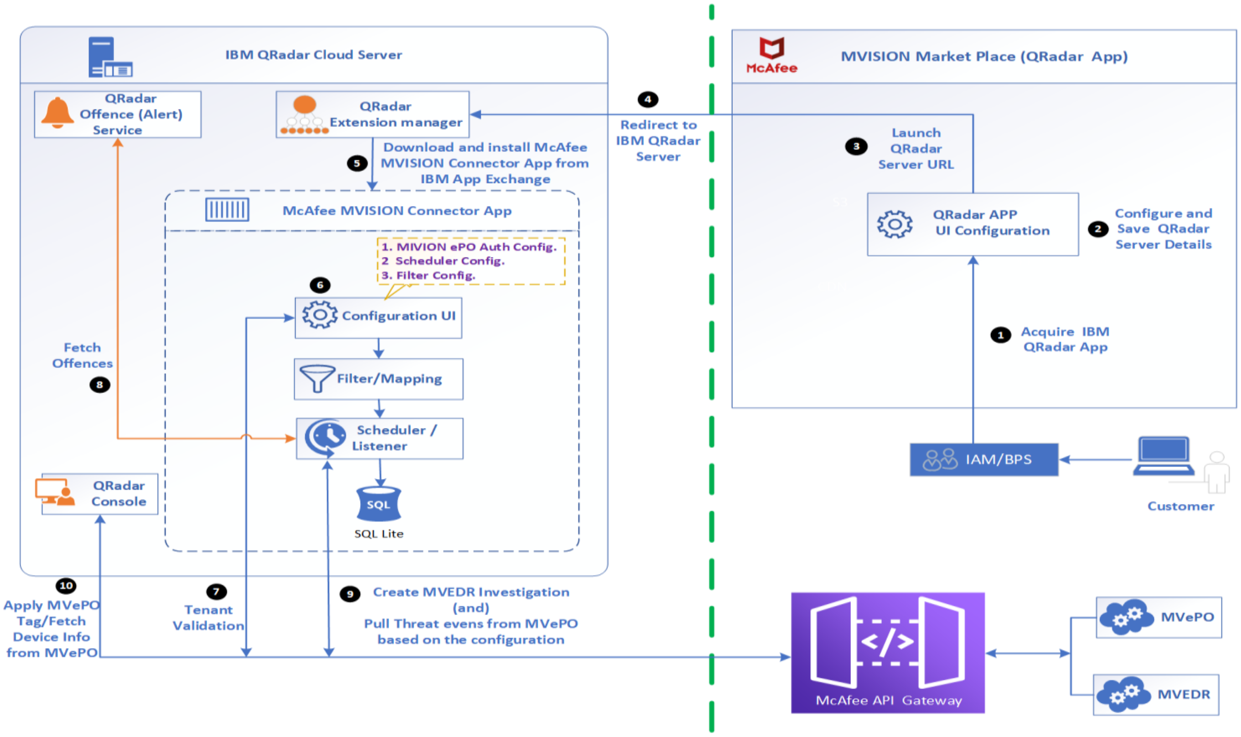
- Can create/update an EDR investigation for an offense from IBM QRadar console. An EDR SOC admin will continue the investigation for the given endpoint (IP, Hostname). Investigation contains IP, Severity and offense description.
- Can apply MVISION ePO policy, based on a tag assigned at IBM QRadar console to an IP.
- Can enrich endpoint system data from MVISION ePO to IBM QRadar console.
- Can ingest MVISION ePO threat events in IBM QRadar event logs for correlation.

Terms and Definitions

Term	Definition
MVISION ePO	MVISION e-Policy Orchestrator
MVISION EDR	MVISION Endpoint Detection & Response

Architecture

The high-level architecture of “McAfee Connector for QRadar” app is shown below:


IBM QRadar Cloud Server
QRadar Offence (Alert) Service
QRadar Extension manager
5 Download and install McAfee MVISION Connector App from IBM App Exchange
McAfee MVISION Connector App
1. MIVION ePO Auth Config.
2 Scheduler Config.
3. Filter Config.
6
Configuration UI
Filter/Mapping
Scheduler / Listener
SQL
SQL Lite
Fetch Offences
8
QRadar Console
10 Apply MVePO Tag/Fetch Device Info from MVePO
7 Tenant Validation
9 Create MVEDR Investigation (and) Pull Threat evens from MVePO based on the configuration
4 Redirect to IBM QRadar Server
McAfee
MVISION Market Place (QRadar App)
3 Launch QRadar Server URL
QRadar APP UI Configuration
2 Configure and Save QRadar Server Details
1 Acquire IBM QRadar App
IAM/BPS
Customer
McAfee API Gateway
MVePO
MVEDR

Pre-requisites

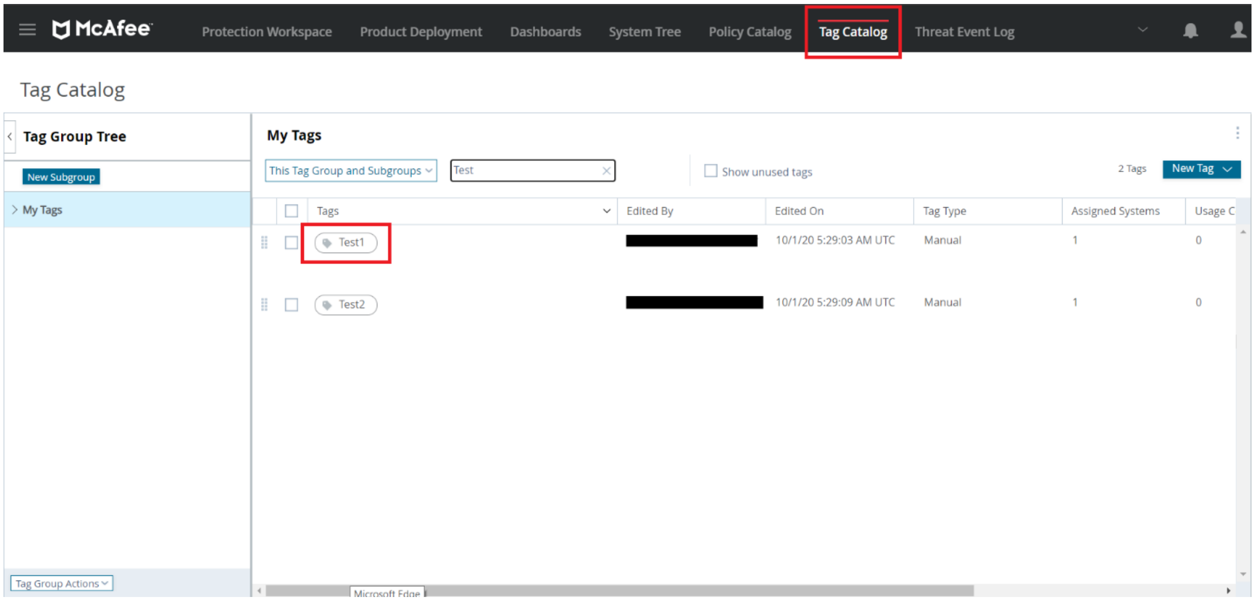
User must be **QRadar admin** to access all the functionalities of “McAfee MVISION Connector” app.
Note: If you are a non-admin user you could see a white screen on “McAfee MVISION Connector” tabs.

Before start using “McAfee MVISION Connector” App, user must make sure that the following applications are up and running and the same should be accessible by them from QRadar server network.

- MVISION ePO Server
- MVISION EDR

Apply MVISION ePO Tag:

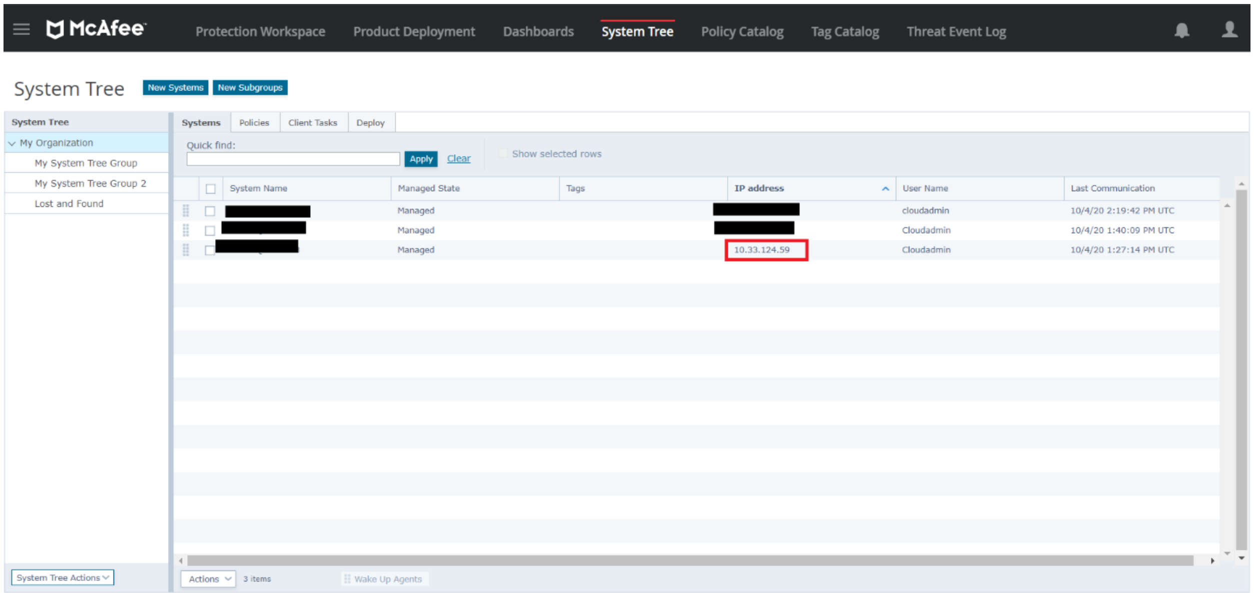
- Before applying MVISION ePO tags action, user must make sure the tags to be applied on the system(s) are created in MVISION ePO server Tag Catalog. For e.g. - Create a tag with name - Test1.
- Refer the screenshot below -



	Tags	Edited By	Edited On	Tag Type	Assigned Systems	Usage C
□	Test1	[redacted]	10/1/20 5:29:03 AM UTC	Manual	1	0
□	Test2	[redacted]	10/1/20 5:29:09 AM UTC	Manual	1	0

MVISION ePO Device Details:

- Before fetching MVISION ePO Device Details, user must make sure the device for which the details need to obtain should be managed in the MVISION ePO. For e.g.- system IP - 10.33.124.59 is managed in ePO.
- Refer the screenshot below:



System Tree

System Tree
- My Organization
  - My System Tree Group
  - My System Tree Group 2
  - Lost and Found

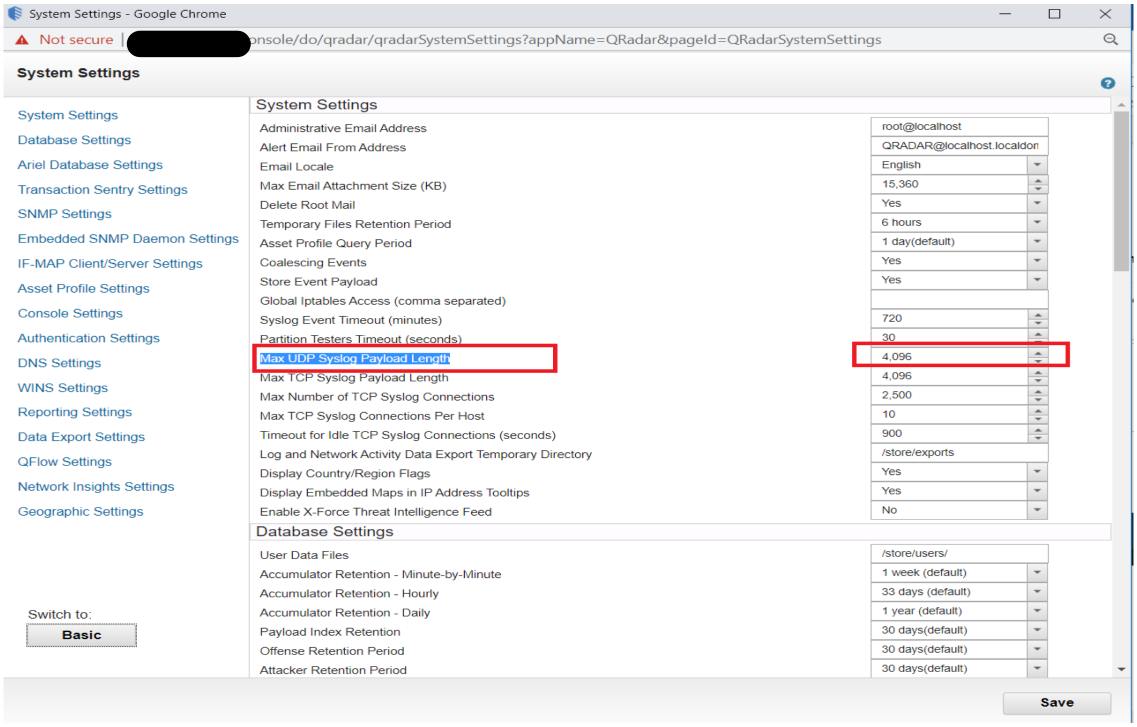
Quick find:

System Name	Managed State	Tags	IP address	User Name	Last Communication
[redacted]	Managed		[redacted]	cloudadmin	10/4/20 2:19:42 PM UTC
[redacted]	Managed		[redacted]	Cloudadmin	10/4/20 1:40:09 PM UTC
[redacted]	Managed		10.33.124.59	Cloudadmin	10/4/20 1:27:14 PM UTC

3 items

Poll Threat Events from MVISION ePO:

- Before starting poll for threat events make sure to increase **Max UDP Syslog Payload Length** to 4096 so that events are not truncated. To do this login to QRadar console and navigate to **Admin panel > click on System Settings icon > click Advanced** button on left bottom corner and then change **Max UDP Syslog Payload Length** to 4096 and click Save. Make sure to initiate a Full Configuration deployment so that changes are deployed for QRadar server as shown below:



[redacted]onsole/do/qradar/qradarSystemSettings?appName=QRadar&pageId=QRadarSystemSettings

System Settings

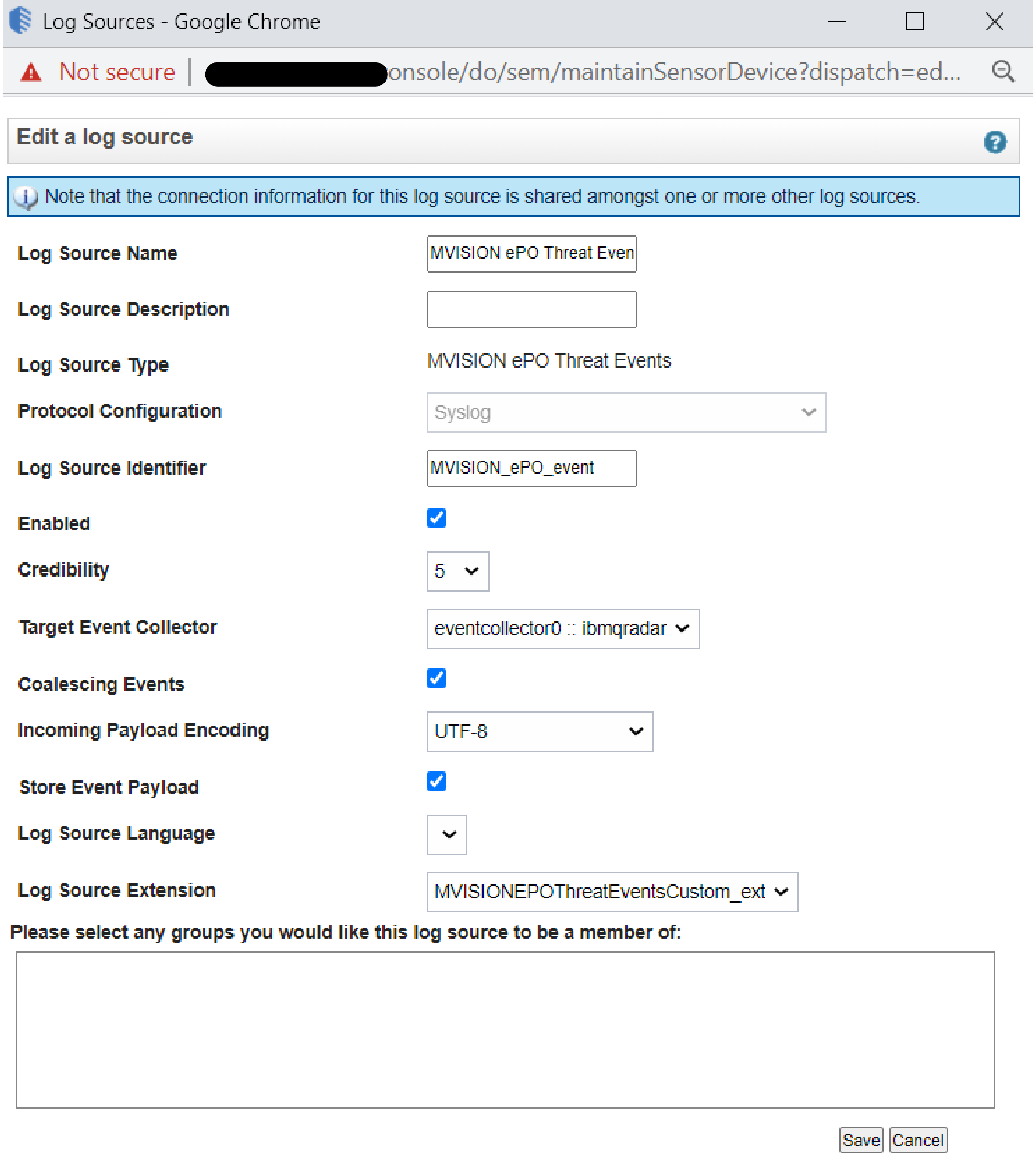
System Settings

Administrative Email Address	root@localhost
Alert Email From Address	QRADAR@localhost.localdon
Email Locale	English
Max Email Attachment Size (KB)	15,360
Delete Root Mail	Yes
Temporary Files Retention Period	6 hours
Asset Profile Query Period	1 day(default)
Coalescing Events	Yes
Store Event Payload	Yes
Global Iptables Access (comma separated)	
Syslog Event Timeout (minutes)	720
Partition Testers Timeout (seconds)	30
Max UDP Syslog Payload Length	4,096
Max TCP Syslog Payload Length	4,096
Max Number of TCP Syslog Connections	2,500
Max TCP Syslog Connections Per Host	10
Timeout for Idle TCP Syslog Connections (seconds)	900
Log and Network Activity Data Export Temporary Directory	/store/exports
Display Country/Region Flags	Yes
Display Embedded Maps in IP Address Tooltips	Yes
Enable X-Force Threat Intelligence Feed	No

Database Settings

User Data Files	/store/users/
Accumulator Retention - Minute-by-Minute	1 week (default)
Accumulator Retention - Hourly	33 days (default)
Accumulator Retention - Daily	1 year (default)
Payload Index Retention	30 days(default)
Offense Retention Period	30 days(default)
Attacker Retention Period	30 days(default)

- As part of the MVISION Connector app, custom log source, log source type, log source extension and custom properties will be populated which help in parsing the threat events on QRadar and display them accordingly.
- **Log Source type**: **MVISION ePO Threat Events** log source type will be created on installing this app.
- **Log Source**: **MVISION ePO Threat Events** log source with log source identifier **MVISION_ePO_event** is created by this app as shown below:



Log Sources - Google Chrome

Not secure | [redacted]onsole/do/sem/maintainSensorDevice?dispatch=ed...

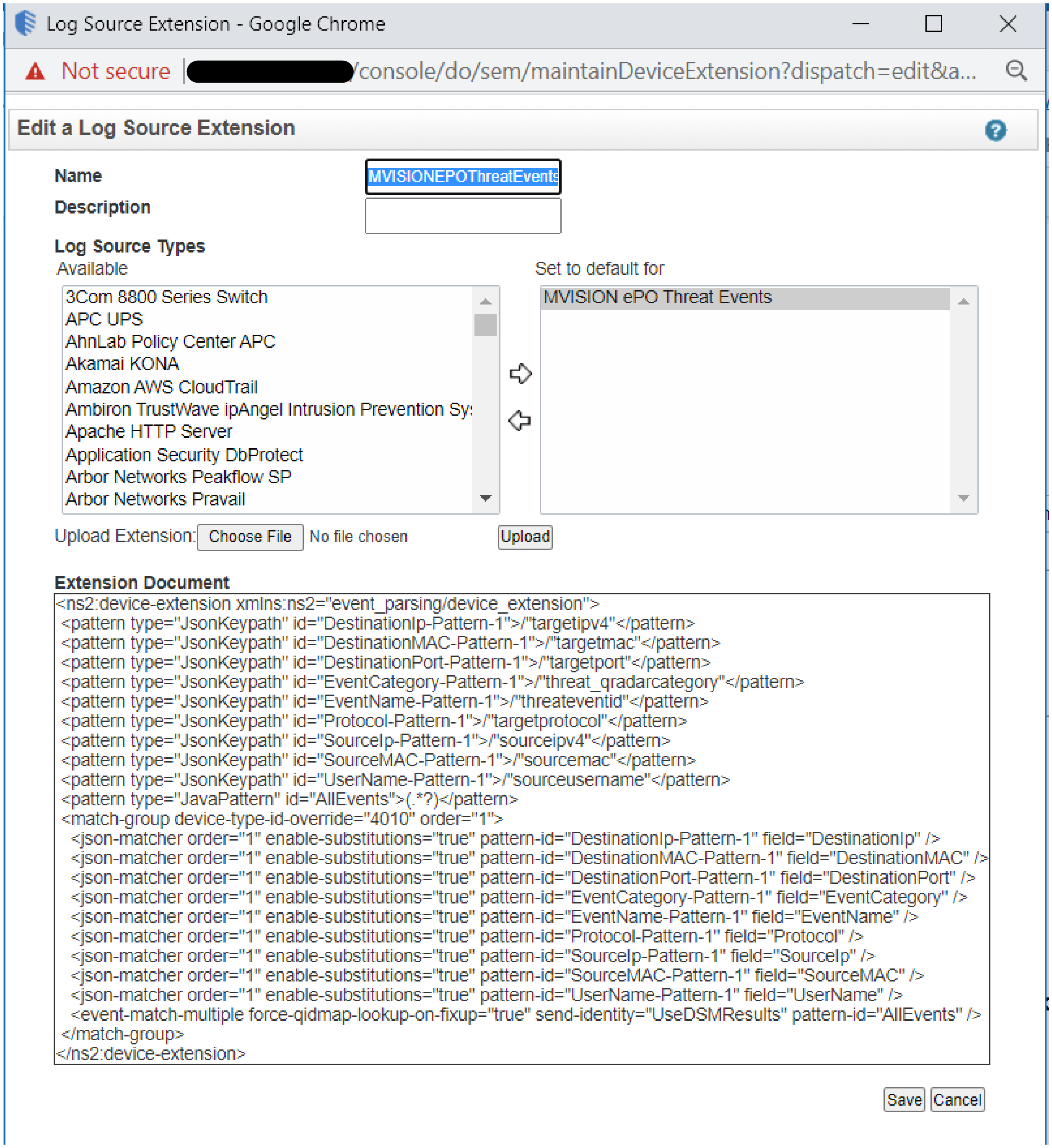
Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources.

Log Source Name	MVISION ePO Threat Even
Log Source Description	
Log Source Type	MVISION ePO Threat Events
Protocol Configuration	Syslog
Log Source Identifier	MVISION_ePO_event
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: ibmqradar
Coalescing Events	☑
Incoming Payload Encoding	UTF-8
Store Event Payload	☑
Log Source Language	
Log Source Extension	MVISIONEPOThreatEventsCustom_ext

Please select any groups you would like this log source to be a member of:

- **Log Source Extension**: **MVISIONEPOThreatEventsCustom_ext** is created by app upon installation as shown below:



[redacted]/console/do/sem/maintainDeviceExtension?dispatch=edit&a...

Edit a Log Source Extension

Name: MVISIONEPOThreatEvents

Description:

Log Source Types

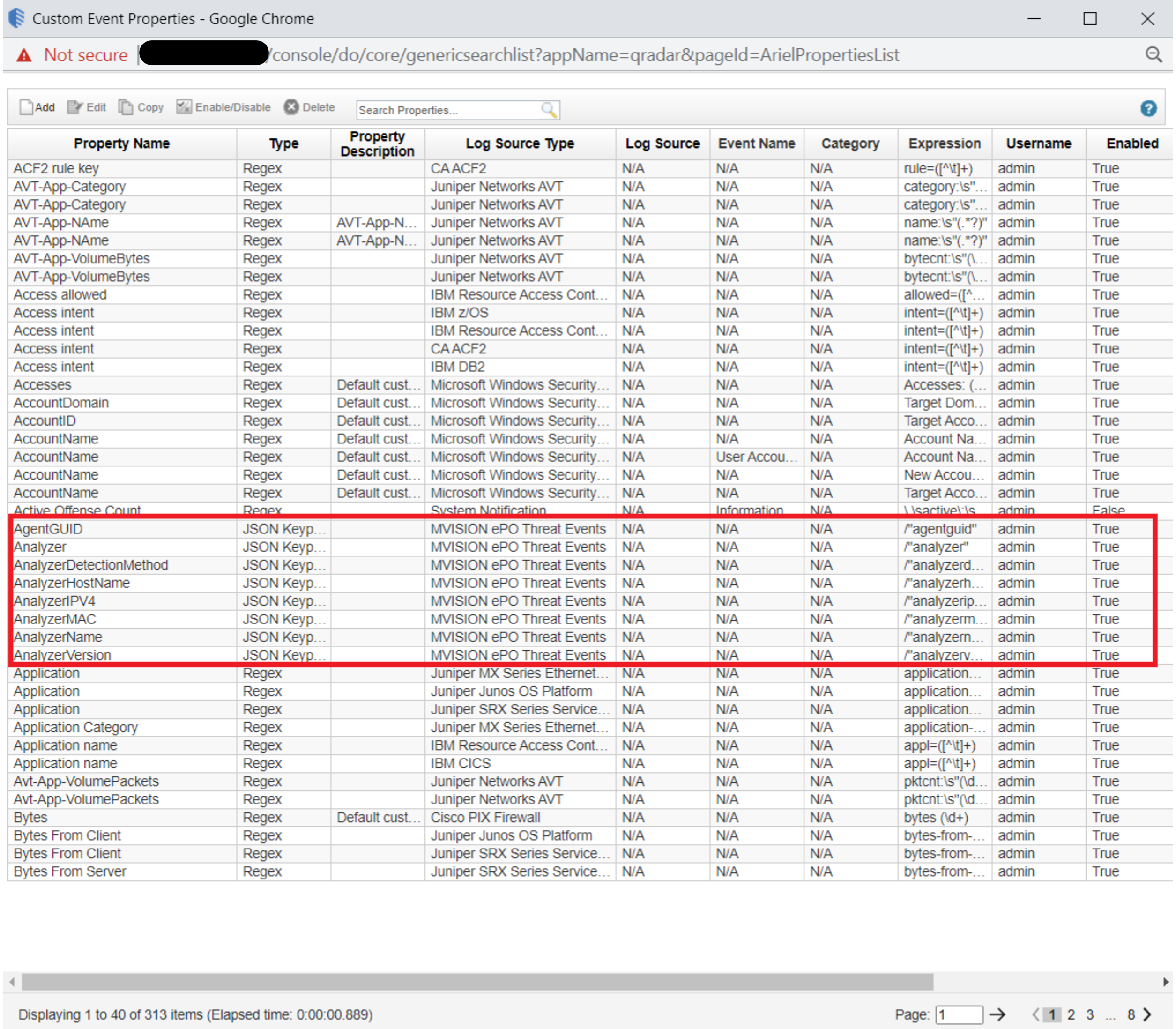
Available	Set to default for
3Com 8800 Series Switch APC UPS AhnLab Policy Center APC Akamai KONA Amazon AWS CloudTrail Ambiron TrustWave ipAngel Intrusion Prevention Sy Apache HTTP Server Application Security DbProtect Arbor Networks Peakflow SP Arbor Networks Pravail	MVISION ePO Threat Events

Upload Extension: Choose File No file chosen Upload

Extension Document

```
<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
 <pattern type="JsonKeypath" id="DestinationIp-Pattern-1">/"targetipv4"</pattern>
 <pattern type="JsonKeypath" id="DestinationMAC-Pattern-1">/"targetmac"</pattern>
 <pattern type="JsonKeypath" id="DestinationPort-Pattern-1">/"targetport"</pattern>
 <pattern type="JsonKeypath" id="EventCategory-Pattern-1">/"threat_qradarcategory"</pattern>
 <pattern type="JsonKeypath" id="EventName-Pattern-1">/"threateventid"</pattern>
 <pattern type="JsonKeypath" id="Protocol-Pattern-1">/"targetprotocol"</pattern>
 <pattern type="JsonKeypath" id="SourceIp-Pattern-1">/"sourceipv4"</pattern>
 <pattern type="JsonKeypath" id="SourceMAC-Pattern-1">/"sourcemac"</pattern>
 <pattern type="JsonKeypath" id="UserName-Pattern-1">/"sourceusername"</pattern>
 <pattern type="JavaPattern" id="AllEvents">(.*?)</pattern>
 <match-group device-type-id-override="4010" order="1">
   <json-matcher order="1" enable-substitutions="true" pattern-id="DestinationIp-Pattern-1" field="DestinationIp" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="DestinationMAC-Pattern-1" field="DestinationMAC" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="DestinationPort-Pattern-1" field="DestinationPort" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="EventCategory-Pattern-1" field="EventCategory" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="EventName-Pattern-1" field="EventName" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="Protocol-Pattern-1" field="Protocol" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="SourceIp-Pattern-1" field="SourceIp" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="SourceMAC-Pattern-1" field="SourceMAC" />
   <json-matcher order="1" enable-substitutions="true" pattern-id="UserName-Pattern-1" field="UserName" />
   <event-match-multiple force-qidmap-lookup-on-fixup="true" send-identity="UseDSMResults" pattern-id="AllEvents" />
 </match-group>
</ns2:device-extension>
```

- **Custom Properties**: Few custom properties specific to MVISION ePO will be created on app installation as shown below:



Custom Event Properties - Google Chrome

Not secure | [redacted]/console/do/core/genericsearchlist?appName=qradar&pageId=ArielPropertiesList

Property Name	Type	Property Description	Log Source Type	Log Source	Event Name	Category	Expression	Username	Enabled
ACF2 rule key	Regex		CA ACF2	N/A	N/A	N/A	rule=([^\t]+)	admin	True
AVT-App-Category	Regex		Juniper Networks AVT	N/A	N/A	N/A	category:\s"...	admin	True
AVT-App-Category	Regex		Juniper Networks AVT	N/A	N/A	N/A	category:\s"...	admin	True
AVT-App-NAme	Regex	AVT-App-N...	Juniper Networks AVT	N/A	N/A	N/A	name:\s"(.*?)"	admin	True
AVT-App-NAme	Regex	AVT-App-N...	Juniper Networks AVT	N/A	N/A	N/A	name:\s"(.*?)"	admin	True
AVT-App-VolumeBytes	Regex		Juniper Networks AVT	N/A	N/A	N/A	bytecnt:\s"(\...	admin	True
AVT-App-VolumeBytes	Regex		Juniper Networks AVT	N/A	N/A	N/A	bytecnt:\s"(\...	admin	True
Access allowed	Regex		IBM Resource Access Cont...	N/A	N/A	N/A	allowed=([^...	admin	True
Access intent	Regex		IBM z/OS	N/A	N/A	N/A	intent=([^\t]+)	admin	True
Access intent	Regex		IBM Resource Access Cont...	N/A	N/A	N/A	intent=([^\t]+)	admin	True
Access intent	Regex		CA ACF2	N/A	N/A	N/A	intent=([^\t]+)	admin	True
Access intent	Regex		IBM DB2	N/A	N/A	N/A	intent=([^\t]+)	admin	True
Accesses	Regex	Default cust...	Microsoft Windows Security...	N/A	N/A	N/A	Accesses: (...	admin	True
AccountDomain	Regex	Default cust...	Microsoft Windows Security...	N/A	N/A	N/A	Target Dom...	admin	True
AccountID	Regex	Default cust...	Microsoft Windows Security...	N/A	N/A	N/A	Target Acco...	admin	True
AccountName	Regex	Default cust...	Microsoft Windows Security...	N/A	N/A	N/A	Account Na...	admin	True
AccountName	Regex	Default cust...	Microsoft Windows Security...	N/A	User Accou...	N/A	Account Na...	admin	True
AccountName	Regex	Default cust...	Microsoft Windows Security...	N/A	N/A	N/A	New Accou...	admin	True
AccountName	Regex	Default cust...	Microsoft Windows Security...	N/A	N/A	N/A	Target Acco...	admin	True
Active Offense Count	Regex		System Notification	N/A	Information	N/A	\ \sactive\:\s	admin	False
AgentGUID	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"agentguid"	admin	True
Analyzer	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"analyzer"	admin	True
AnalyzerDetectionMethod	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"analyzerd...	admin	True
AnalyzerHostName	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"analyzerh...	admin	True
AnalyzerIPV4	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"analyzerip...	admin	True
AnalyzerMAC	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"analyzerm...	admin	True
AnalyzerName	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"analyzern...	admin	True
AnalyzerVersion	JSON Keyp...		MVISION ePO Threat Events	N/A	N/A	N/A	/"analyzerv...	admin	True
Application	Regex		Juniper MX Series Ethernet...	N/A	N/A	N/A	application...	admin	True
Application	Regex		Juniper Junos OS Platform	N/A	N/A	N/A	application...	admin	True
Application	Regex		Juniper SRX Series Service...	N/A	N/A	N/A	application...	admin	True
Application Category	Regex		Juniper MX Series Ethernet...	N/A	N/A	N/A	application-...	admin	True
Application name	Regex		IBM Resource Access Cont...	N/A	N/A	N/A	appl=([^\t]+)	admin	True
Application name	Regex		IBM CICS	N/A	N/A	N/A	appl=([^\t]+)	admin	True
Avt-App-VolumePackets	Regex		Juniper Networks AVT	N/A	N/A	N/A	pktcnt:\s"(\d...	admin	True
Avt-App-VolumePackets	Regex		Juniper Networks AVT	N/A	N/A	N/A	pktcnt:\s"(\d...	admin	True
Bytes	Regex	Default cust...	Cisco PIX Firewall	N/A	N/A	N/A	bytes (\d+)	admin	True
Bytes From Client	Regex		Juniper Junos OS Platform	N/A	N/A	N/A	bytes-from-...	admin	True
Bytes From Client	Regex		Juniper SRX Series Service...	N/A	N/A	N/A	bytes-from-...	admin	True
Bytes From Server	Regex		Juniper SRX Series Service...	N/A	N/A	N/A	bytes-from-...	admin	True

Displaying 1 to 40 of 313 items (Elapsed time: 0:00:00.889)

- Make sure UDP port 514 is enabled as QRadar Syslog server uses this port to listen to incoming messages.
- Make sure to deploy changes from QRadar Admin panel before starting poll so that Log source changes are deployed properly.

Software version and platform details

Below is the list of components that we have used to test McAfee Connector for QRadar app.

Service name	**Component version and platform details**
MVISION ePO server	As per the details mentioned in on-boarding welcome mail
MVISION EDR	As per the details mentioned in on-boarding welcome mail
IBM QRadar Server	IBM QRadar v7.3.1 Build 20171206222136 and above

Step by Step Instruction to use McAfee MVISION Connector for QRadar App

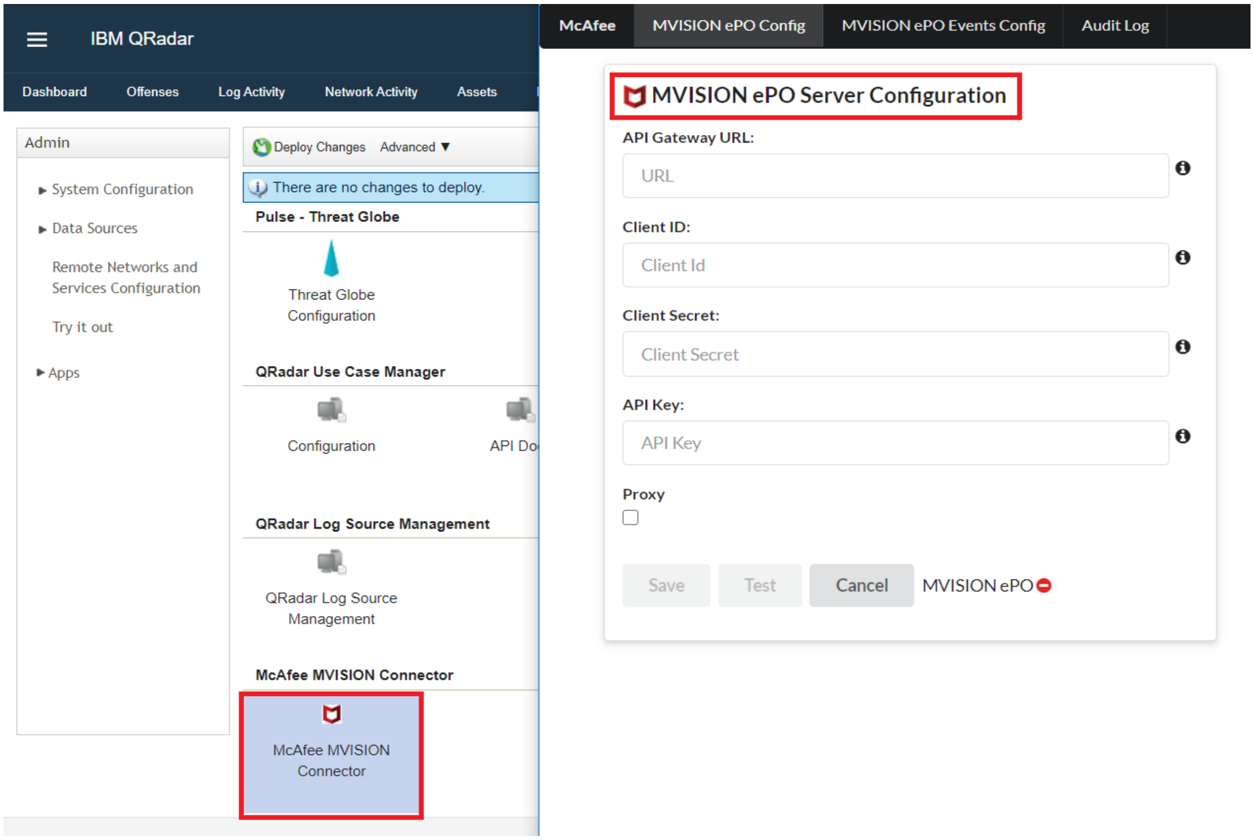
As part of this app documentation we assume that all MVISION ePO related operation and configuration will be performed only by MVISION ePO sever **tenant** users and all QRadar related operation and configuration will be done by QRadar server **admin** user.

Acquiring client credentials from McAfee Marketplace

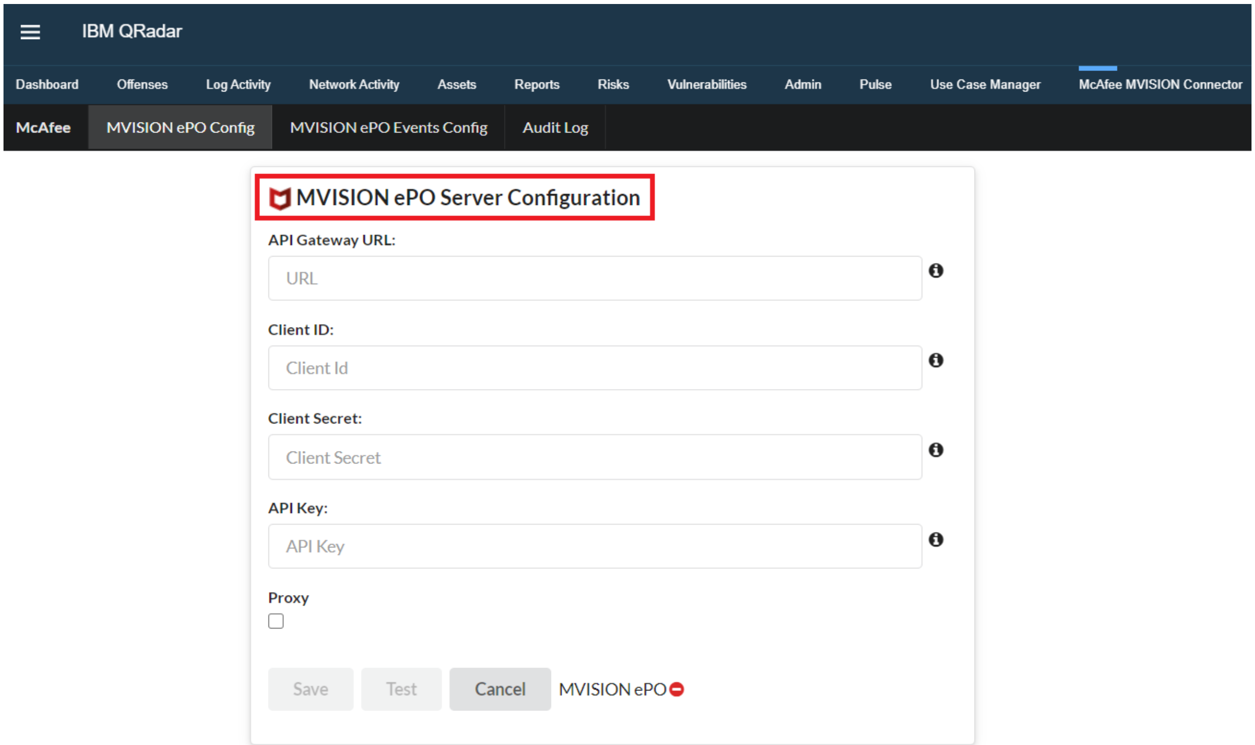
1. As part of the workflow customer/tenant should login into MVISION Marketplace using their MVISION credential.
2. Customer/tenant then should register and get IBM QRadar app from MVISION Market place. After opening the IBM QRadar app, click on "configure" button to configure actual QRadar server URL and click "Launch" button.
3. The "Launch" action will open the given QRadar Server URL in a separate browser window.
4. Now enter the QRadar server credentials to login into QRadar console.
5. Now you must install McAfee MVISION Connector app into QRadar server. In order to achieve this, you have two options
   Option #1: Go to Menu | Admin | Extension Management page in QRadar server and click "IBM Security App Exchange" button to download McAfee MVISION Connector app.
   Option #2: Go to IBM X-Force Exchange website (https://exchange.xforce.ibmcloud.com/hub?q=mcafee) to download the latest McAfee MVISION Connector app.
6. Install the downloaded "McAfee MVISION Connector" app into QRadar Server.
7. Open the "McAfee MVISION Connector" app landing page to configure MVISION ePO credentials.
   Note: Go back to IBM QRadar app in MVISION Market place to copy Client ID, Client Secret, and API Key, and provide the same in corresponding input fields.
8. If the configuration saved successfully, following task can be performed by QRadar admin user.
   a. Create Investigation in MVISION EDR for the QRadar offences based on the app scheduler/filter configuration.
   b. Right click option in QRadar console to apply a tag for an IP in MVISION ePO.
   c. Right click option in QRadar console to show additional device details from MVISION ePO.

Configure/Provision McAfee MVISION Connector for QRadar App

Before the QRadar admin takes advantage of actions that are provided by McAfee MVISION Connector for QRadar App, the QRadar admin user should configure/provision MVISION ePO server inside the McAfee MVISION Connector for QRadar app.
Refer the screenshot below-



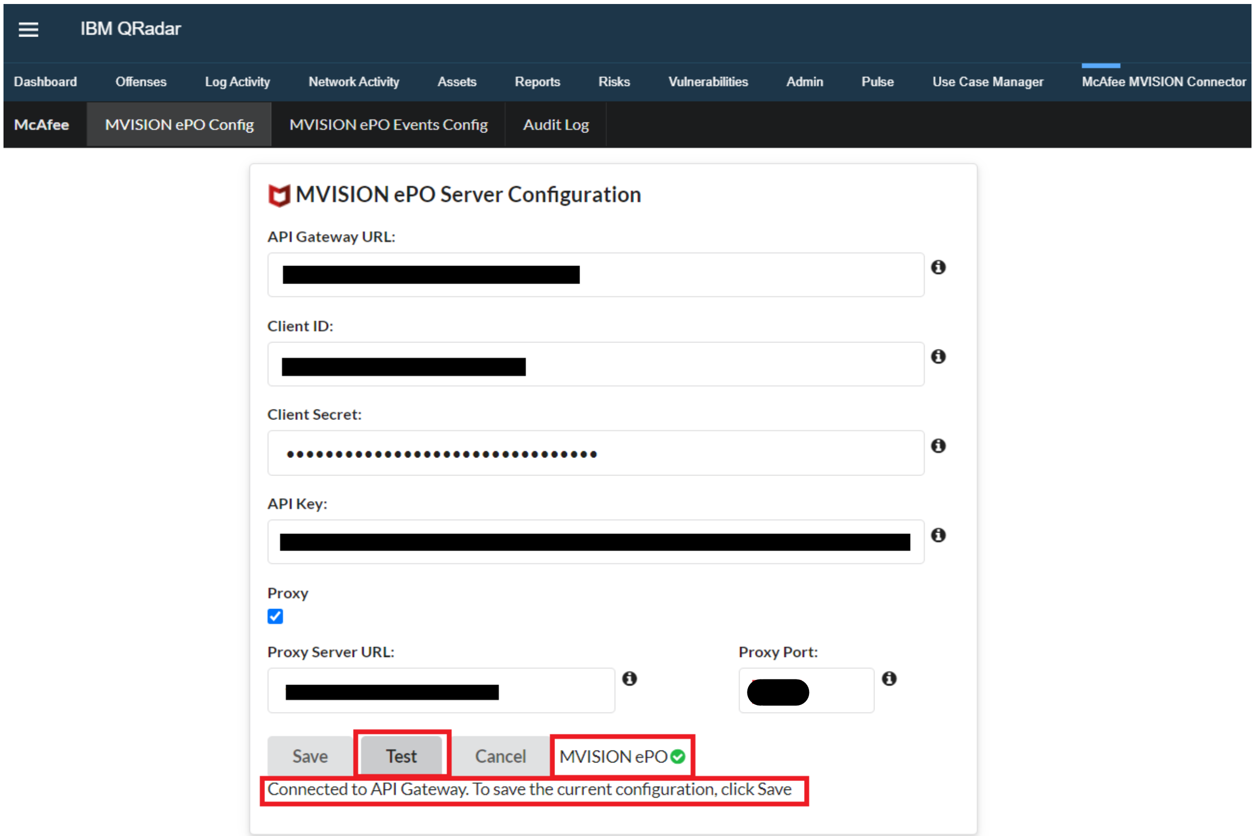
Also, the same app will be shown as part of QRadar ribbon tab. Refer the screenshot below-



Provide the values under MVISION ePO Server Configuration page like the sample data given below:

Field Name	Sample Value	Description
API Gateway URL	https://api.dev.mvision.mcafee.com	Provide URL of MVISION API Gateway (IP address or number inputs are not allowed)
Client ID	<client id from MVISION Market place>	Provide valid Client ID which is generated by the Tenant ID provided in the activation mail.
Client Secret	<client secret from MVISION Market place >	Provide valid Client Secret which is generated by the Tenant ID provided in the activation mail.
API Key	<api key from MVISION Market place>	Provide valid API Key which is provided as part of the activation mail for a Tenant ID.
Proxy	Checkbox	This checkbox should be checked if proxy is required to be configured.
Proxy Server URL	Proxy URL	Provide valid Proxy server URL. For eg. Sample.proxy.com
Proxy Port	Port Number	Provide valid proxy port number associated with the proxy URL. For e.g 9090

Once all the fields are populated, click on **Test** button to validate the given credentials.



MVISION ePO Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: •••••••••••••••••••••••••••••••••

API Key: [redacted]

Proxy
☑

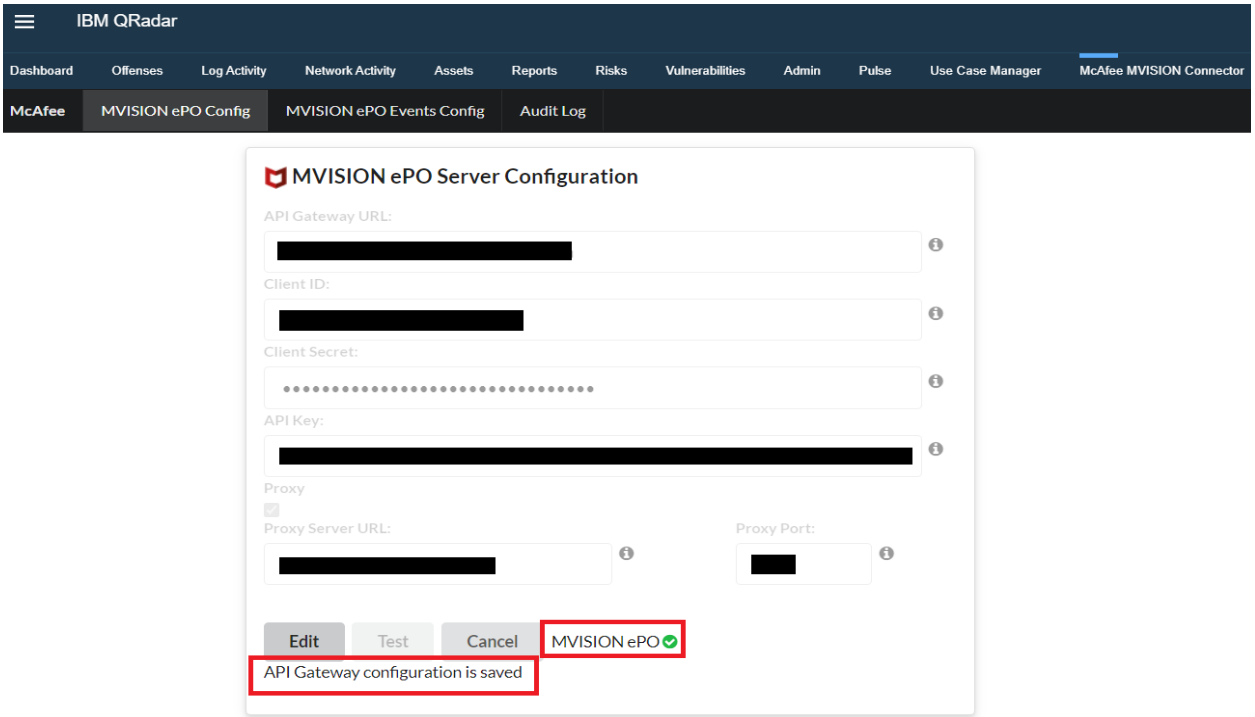
Proxy Server URL: [redacted]

Proxy Port: [redacted]

Connected to API Gateway. To save the current configuration, click Save

If the test is successful, click on **Save** button to save this configuration.

Refer the screenshot below-



MVISION ePO Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: ••••••••••••••••••••••••••••••••

API Key: [redacted]

Proxy ☑

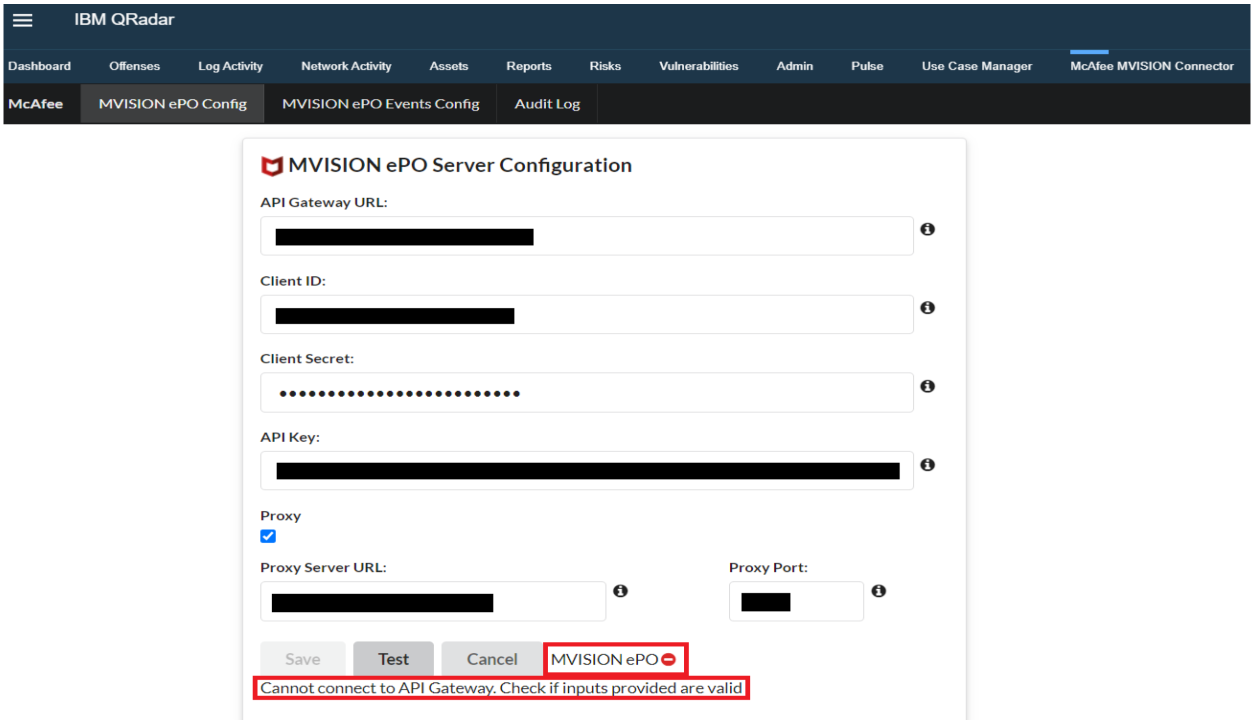
Proxy Server URL: [redacted]

Proxy Port: [redacted]

MVISION ePO ✓

API Gateway configuration is saved

If the Test fails, a failure message will be displayed. Check if valid inputs are provided and retry. Refer the screenshot below-



MVISION ePO Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: ••••••••••••••••••••••••••

API Key: [redacted]

Proxy ☑

Proxy Server URL: [redacted]

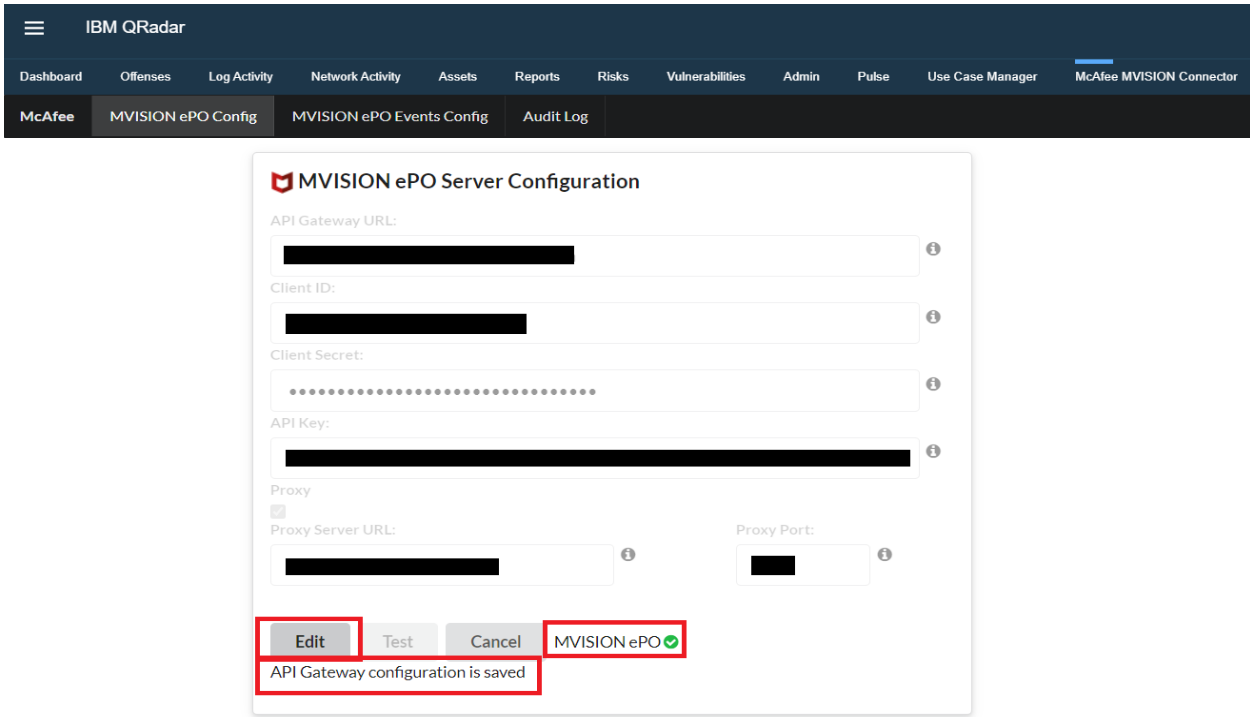
Proxy Port: [redacted]

MVISION ePO ⊖

Cannot connect to API Gateway. Check if inputs provided are valid

It is mandatory that Test should pass to Save and proceed and perform other actions.

Once the Save is completed, user can Edit the MVISION ePO server details by clicking Edit button. Refer the screenshot below-



MVISION ePO Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: ••••••••••••••••••••••••••••••••

API Key: [redacted]

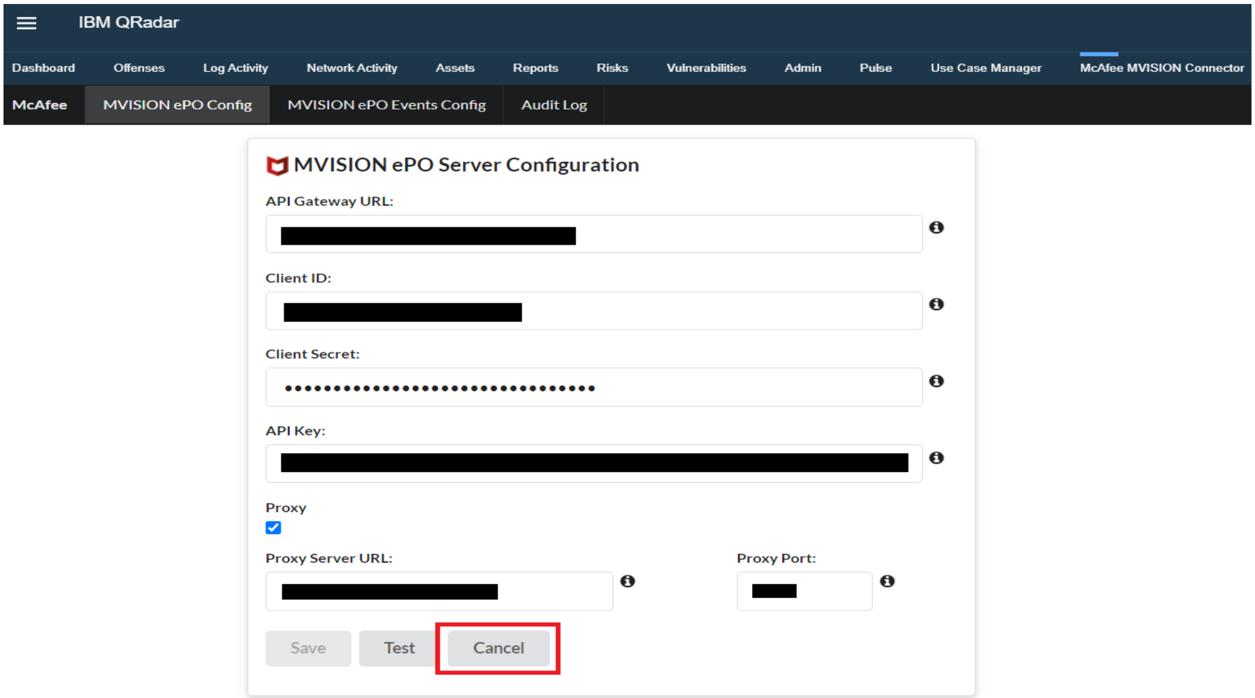
Proxy ☑

Proxy Server URL: [redacted]

Proxy Port: [redacted]

API Gateway configuration is saved

After editing server details QRadar admin can change the details and Test, then Save the MVISION ePO details. If the QRadar admin does not want to provision again then the admin must click “Cancel” button to retain old settings. Refer the screenshot below-



MVISION ePO Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: ••••••••••••••••••••••••••••••••

API Key: [redacted]

Proxy ☑

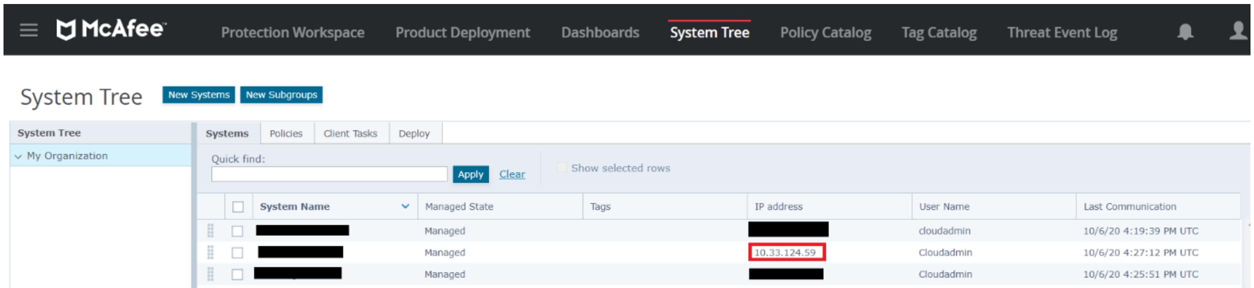
Proxy Server URL: [redacted]

Proxy Port: [redacted]

Apply MVISION ePO Tags

The “**MVISION ePO Tags**” action in QRadar console will allow the QRadar user to select an IP from “**Log Activity**” page (only if the selected IP is managed by ePO server) and apply any tag which exists in the configured ePO on a system/IP. This action from QRadar server can initiate ePO’s automatic tag-based policy/task as a remediation action.

Before performing “**MVISION ePO Tags**” action from QRadar console, login to MVISION ePO server and go to **Menu | Systems | System Tree** page and search for the “IP” (in our example it is “10.33.124.59”) and check the list of tags applied for this IP. Refer the screenshot below-

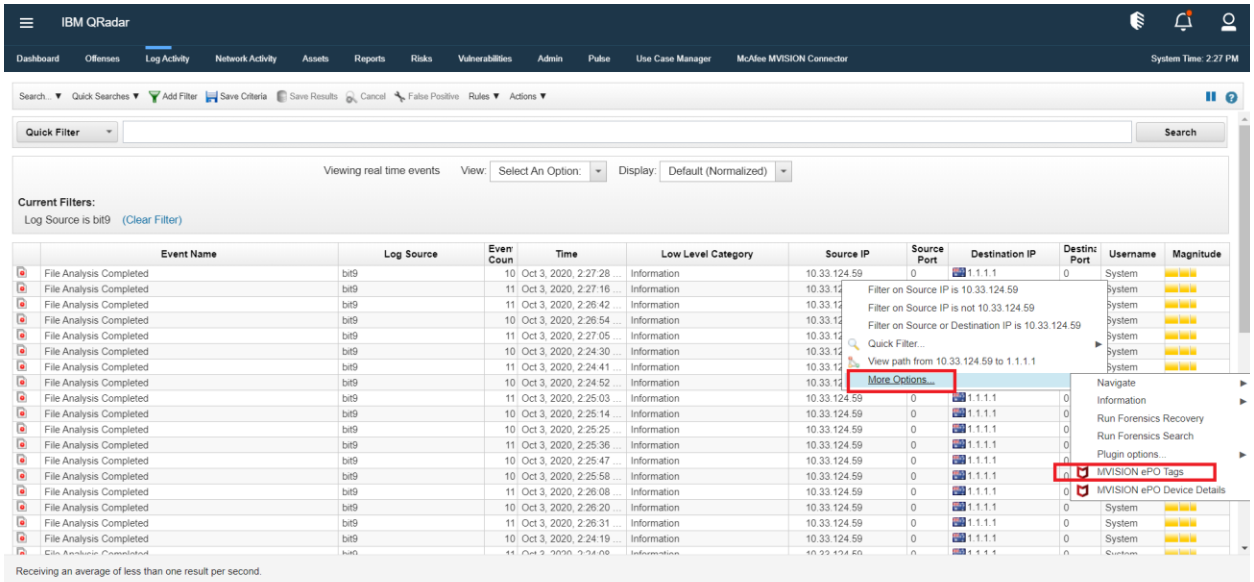


System Name	Managed State	Tags	IP address	User Name	Last Communication
[redacted]	Managed		[redacted]	cloudadmin	10/6/20 4:19:39 PM UTC
[redacted]	Managed		10.33.124.59	Cloudadmin	10/6/20 4:27:12 PM UTC
[redacted]	Managed		[redacted]	Cloudadmin	10/6/20 4:25:51 PM UTC

Note: At this stage the IP (10.33.124.59) does not have any tag applied.

Go to “Log Activity” page in QRadar console and right click on **Source IP** column and select **More Options | MVISION ePO Tags.** This action will open a new page to perform “**MVISION ePO Tags**” action.

Refer the screenshot below-



Viewing real time events View: Select An Option: Display: Default (Normalized)

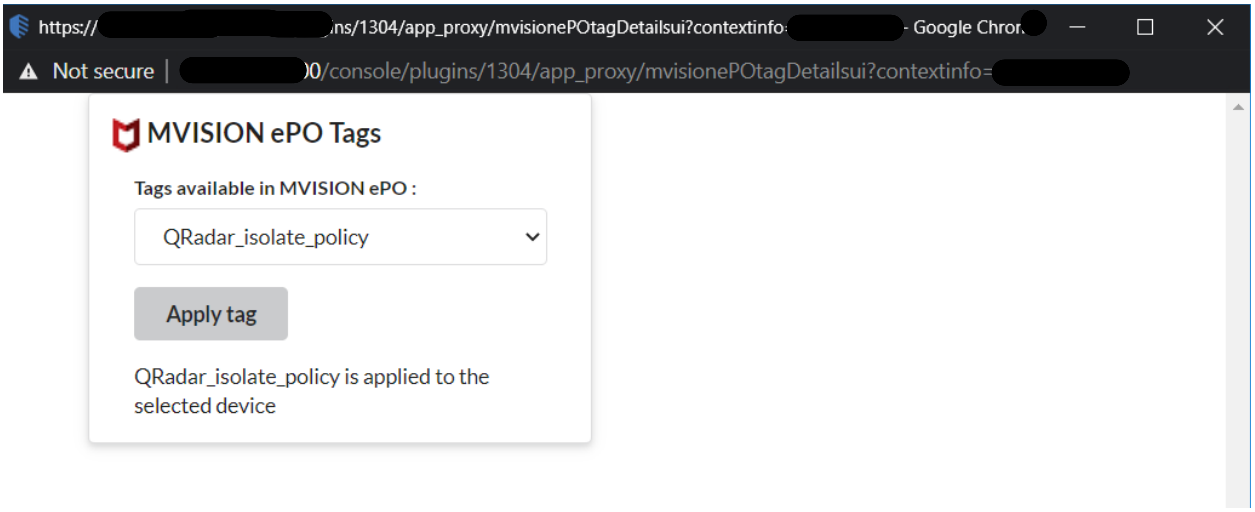
Current Filters:
Log Source is bit9 (Clear Filter)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
File Analysis Completed	bit9	10	Oct 3, 2020, 2:27:28 ...	Information	10.33.124.59	0	1.1.1.1	0	System	▬▬▬
File Analysis Completed	bit9	11	Oct 3, 2020, 2:27:16 ...	Information	10.33.12				System	▬▬▬
File Analysis Completed	bit9	11	Oct 3, 2020, 2:26:42 ...	Information	10.33.12				System	▬▬▬
File Analysis Completed	bit9	10	Oct 3, 2020, 2:26:54 ...	Information	10.33.12				System	▬▬▬
File Analysis Completed	bit9	11	Oct 3, 2020, 2:27:05 ...	Information	10.33.12				System	▬▬▬
File Analysis Completed	bit9	10	Oct 3, 2020, 2:24:30 ...	Information	10.33.12				System	▬▬▬
File Analysis Completed	bit9	11	Oct 3, 2020, 2:24:41 ...	Information	10.33.12				System	▬▬▬
File Analysis Completed	bit9	10	Oct 3, 2020, 2:24:52 ...	Information	10.33.12					
File Analysis Completed	bit9	11	Oct 3, 2020, 2:25:03 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:25:14 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:25:25 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	11	Oct 3, 2020, 2:25:36 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:25:47 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:25:58 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	11	Oct 3, 2020, 2:26:08 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:26:20 ...	Information	10.33.124.59	0	1.1.1.1	0	System	▬▬▬
File Analysis Completed	bit9	11	Oct 3, 2020, 2:26:31 ...	Information	10.33.124.59	0	1.1.1.1	0	System	▬▬▬
File Analysis Completed	bit9	10	Oct 3, 2020, 2:24:19 ...	Information	10.33.124.59	0	1.1.1.1	0	System	▬▬▬
File Analysis Completed	bit9	11	Oct 3, 2020, 2:24:08 ...	Information	10.33.124.59	0	1.1.1.1	0	System	▬▬▬

Filter on Source IP is 10.33.124.59
Filter on Source IP is not 10.33.124.59
Filter on Source or Destination IP is 10.33.124.59
Quick Filter...
View path from 10.33.124.59 to 1.1.1.1
More Options...
Navigate
Information
Run Forensics Recovery
Run Forensics Search
Plugin options...
MVISION ePO Tags
MVISION ePO Device Details

Receiving an average of less than one result per second.

If the selected **Source IP** address is managed by ePO server, the new page will allow the user to select a tag from the list and click “Apply”. If the tag is applied successfully in ePO server, you will get **“<tagname> tag applied successfully to the selected system.**” Message as shown in the screenshot below-



https://[redacted]ns/1304/app_proxy/mvisionePOtagDetailsui?contextinfo[redacted]- Google Chrom[redacted]

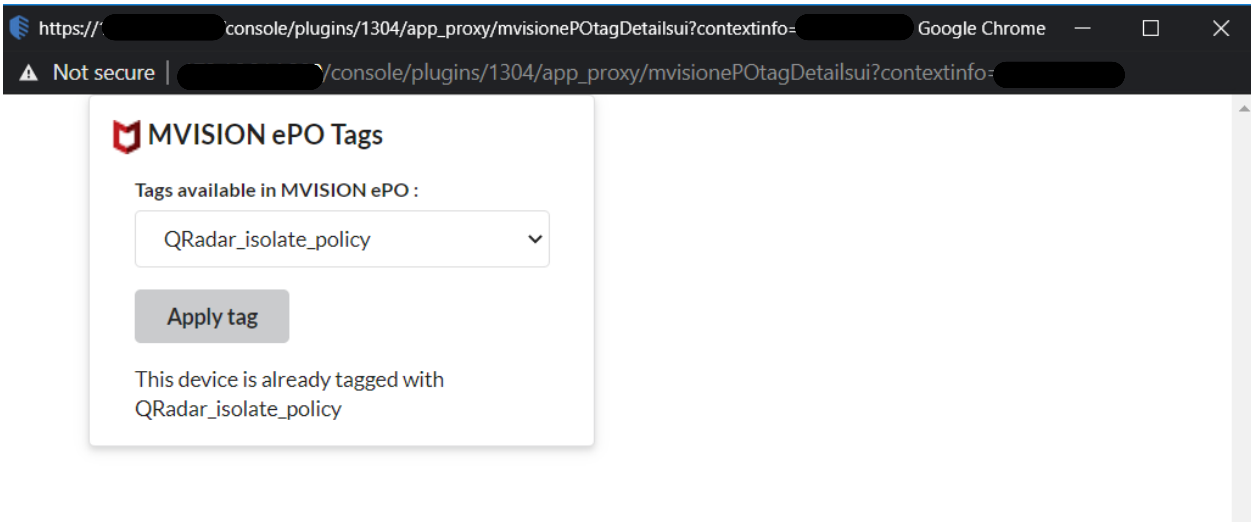
Not secure | [redacted]0/console/plugins/1304/app_proxy/mvisionePOtagDetailsui?contextinfo=[redacted]

MVISION ePO Tags

Tags available in MVISION ePO : QRadar_isolate_policy

QRadar_isolate_policy is applied to the selected device

Note: If the selected tag is already applied for the system IP in the ePO, you will receive “**<tagname> tag is already applied to the selected system.”** as a response message.
Refer the screenshot below-



https://[redacted]console/plugins/1304/app_proxy/mvisionePOtagDetailsui?contextinfo=[redacted] Google Chrome

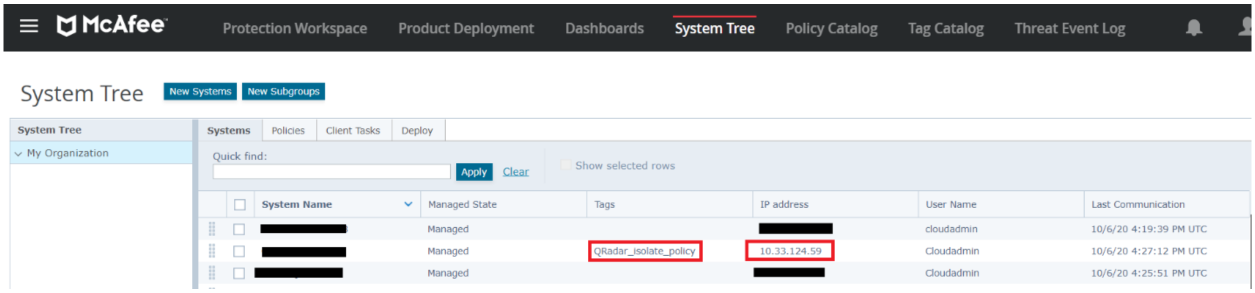
Not secure | [redacted]/console/plugins/1304/app_proxy/mvisionePOtagDetailsui?contextinfo=[redacted]

MVISION ePO Tags

Tags available in MVISION ePO : QRadar_isolate_policy

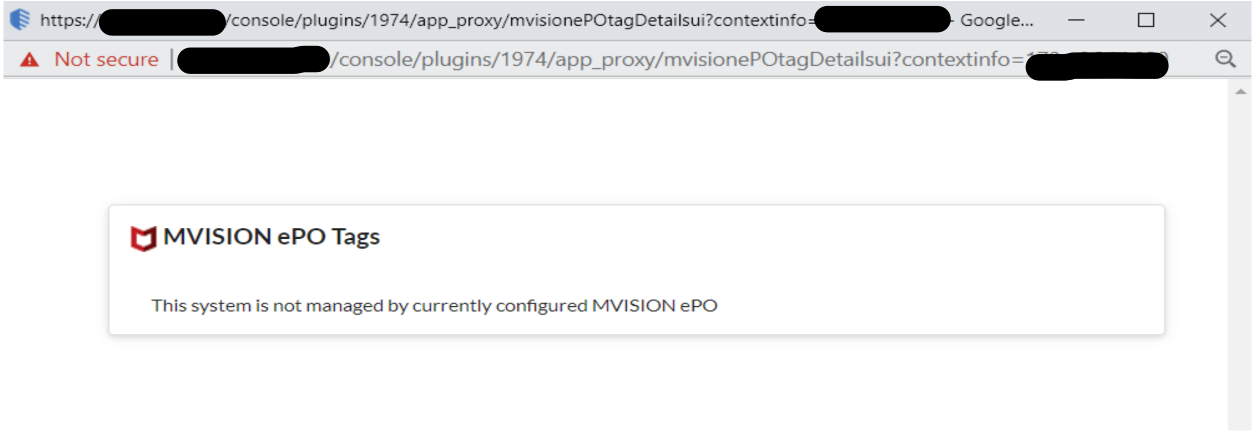
This device is already tagged with QRadar_isolate_policy

Once the “**MVISION ePO Tags**” action in QRadar server is successful you can see the same in the MVISIONS ePO’s system tree page next to the selected system.
Refer the screenshot below-



□	System Name	Managed State	Tags	IP address	User Name	Last Communication
□	[redacted]	Managed		[redacted]	cloudadmin	10/6/20 4:19:39 PM UTC
□	[redacted]	Managed	QRadar_isolate_policy	10.33.124.59	Cloudadmin	10/6/20 4:27:12 PM UTC
□	[redacted]	Managed		[redacted]	Cloudadmin	10/6/20 4:25:51 PM UTC

Note: In case the selected IP is not managed by the MVISION ePO configured in the QRadar-Right click on **Source IP** column and select **More Options | MVISION ePO Tags** will display a message indicating "This system does not belong to the configured ePO". Refer the screenshot below-

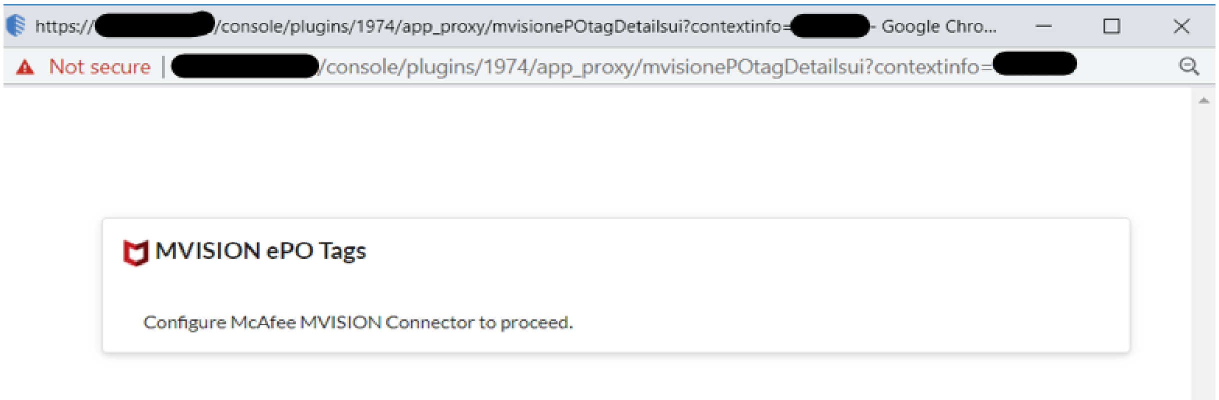

https://[redacted]/console/plugins/1974/app_proxy/mvisionePOtagDetailsui?contextinfo=[redacted]- Google...

Not secure | [redacted]/console/plugins/1974/app_proxy/mvisionePOtagDetailsui?contextinfo=[redacted]

MVISION ePO Tags

This system is not managed by currently configured MVISION ePO

When the McAfee MVISION Connector has not been configured at all, -Following failure message will be displayed-


https://[redacted]/console/plugins/1974/app_proxy/mvisionePOtagDetailsui?contextinfo=[redacted]- Google Chro...

Not secure | [redacted]/console/plugins/1974/app_proxy/mvisionePOtagDetailsui?contextinfo=[redacted]

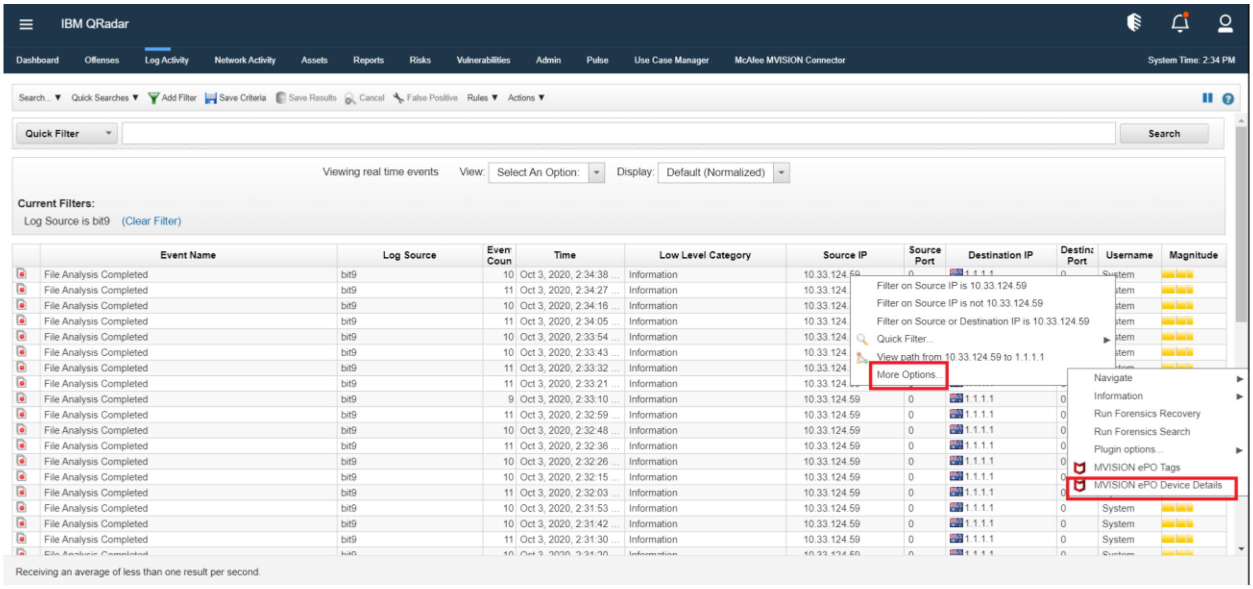
MVISION ePO Tags

Configure McAfee MVISION Connector to proceed.

MVISION ePO Device Details

The “**MVISION ePO Device Details**” action in QRadar console will allow the QRadar user to select an IP from “**Log Activity**” page (only if the selected IP is managed by ePO server).

Refer the screenshot below-



Viewing real time events View: Select An Option: Display: Default (Normalized)

Current Filters:
Log Source is bit9 (Clear Filter)

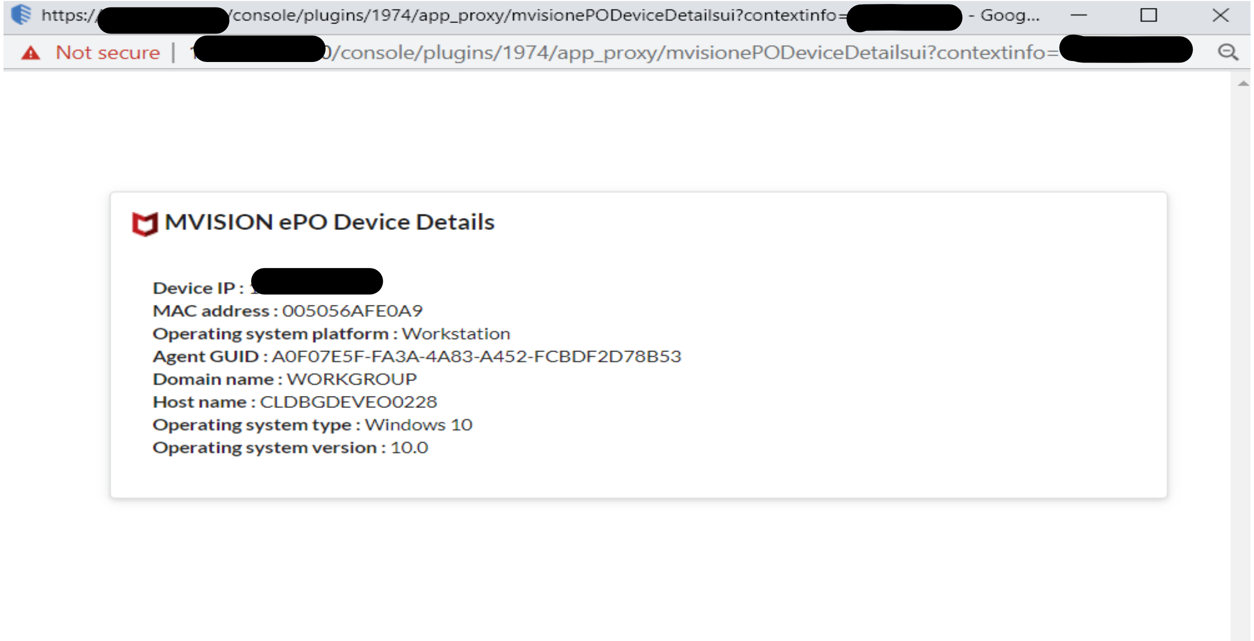
Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destin: Port	Username	Magnitude
File Analysis Completed	bit9	10	Oct 3, 2020, 2:34:38 ...	Information	10.33.124.59	0	1.1.1.1	0	System	
File Analysis Completed	bit9	11	Oct 3, 2020, 2:34:27 ...	Information	10.33.124.				stem	
File Analysis Completed	bit9	10	Oct 3, 2020, 2:34:16 ...	Information	10.33.124.				stem	
File Analysis Completed	bit9	11	Oct 3, 2020, 2:34:05 ...	Information	10.33.124.				stem	
File Analysis Completed	bit9	10	Oct 3, 2020, 2:33:54 ...	Information	10.33.124.				stem	
File Analysis Completed	bit9	10	Oct 3, 2020, 2:33:43 ...	Information	10.33.124.				stem	
File Analysis Completed	bit9	11	Oct 3, 2020, 2:33:32 ...	Information	10.33.124.					
File Analysis Completed	bit9	11	Oct 3, 2020, 2:33:21 ...	Information	10.33.124.					
File Analysis Completed	bit9	9	Oct 3, 2020, 2:33:10 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	11	Oct 3, 2020, 2:32:59 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:32:48 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	11	Oct 3, 2020, 2:32:36 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:32:26 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:32:15 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	11	Oct 3, 2020, 2:32:03 ...	Information	10.33.124.59	0	1.1.1.1	0		
File Analysis Completed	bit9	10	Oct 3, 2020, 2:31:53 ...	Information	10.33.124.59	0	1.1.1.1	0	System	
File Analysis Completed	bit9	10	Oct 3, 2020, 2:31:42 ...	Information	10.33.124.59	0	1.1.1.1	0	System	
File Analysis Completed	bit9	11	Oct 3, 2020, 2:31:30 ...	Information	10.33.124.59	0	1.1.1.1	0	System	
File Analysis Completed	bit9	10	Oct 3, 2020, 2:31:20 ...	Information	10.33.124.59	0	1.1.1.1	0	System	

Filter on Source IP is 10.33.124.59
Filter on Source IP is not 10.33.124.59
Filter on Source or Destination IP is 10.33.124.59
Quick Filter...
View path from 10.33.124.59 to 1.1.1.1
More Options...
Navigate
Information
Run Forensics Recovery
Run Forensics Search
Plugin options...
MVISION ePO Tags
MVISION ePO Device Details

Receiving an average of less than one result per second.

This action will open a new popup page to show system details from MVISION ePO server.

Considering the system 10.33.124.59 . Refer the screenshot below-

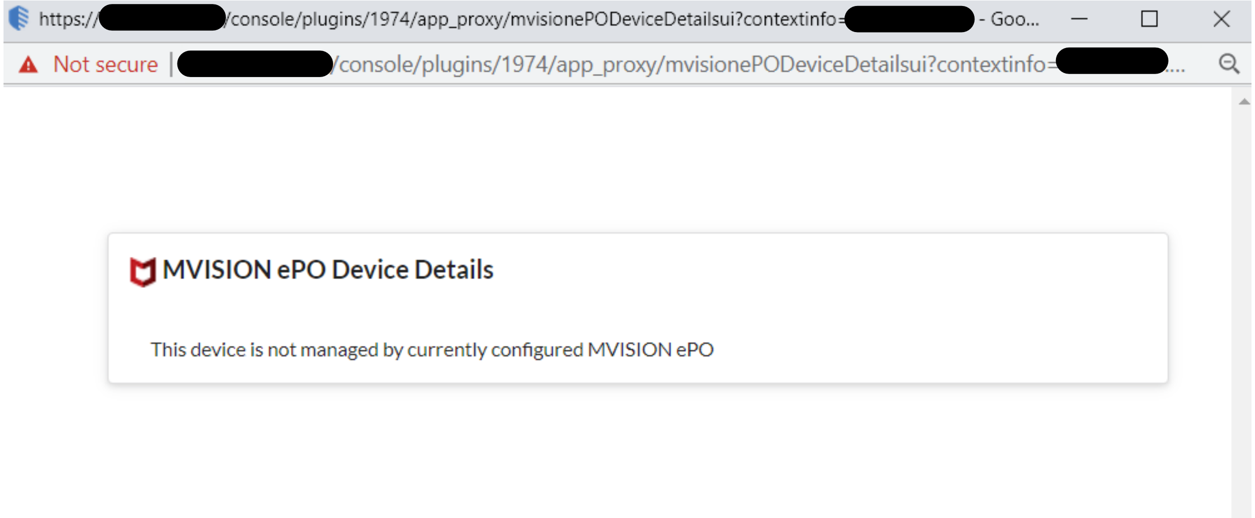


https://[redacted]/console/plugins/1974/app_proxy/mvisionePODeviceDetailsui?contextinfo=[redacted] - Goog...
Not secure | [redacted]/console/plugins/1974/app_proxy/mvisionePODeviceDetailsui?contextinfo=[redacted]

MVISION ePO Device Details

Device IP : [redacted]
MAC address : 005056AFE0A9
Operating system platform : Workstation
Agent GUID : A0F07E5F-FA3A-4A83-A452-FCBDF2D78B53
Domain name : WORKGROUP
Host name : CLDBGDEVEO0228
Operating system type : Windows 10
Operating system version : 10.0

In case the selected IP is not managed by the MVISION ePO configured in the QRadar-
Right click on **Source IP** column and select **More Options | MVISION ePO Device Details** will display a message indicating "This system does not belong to the configured ePO". Refer the screenshot below-



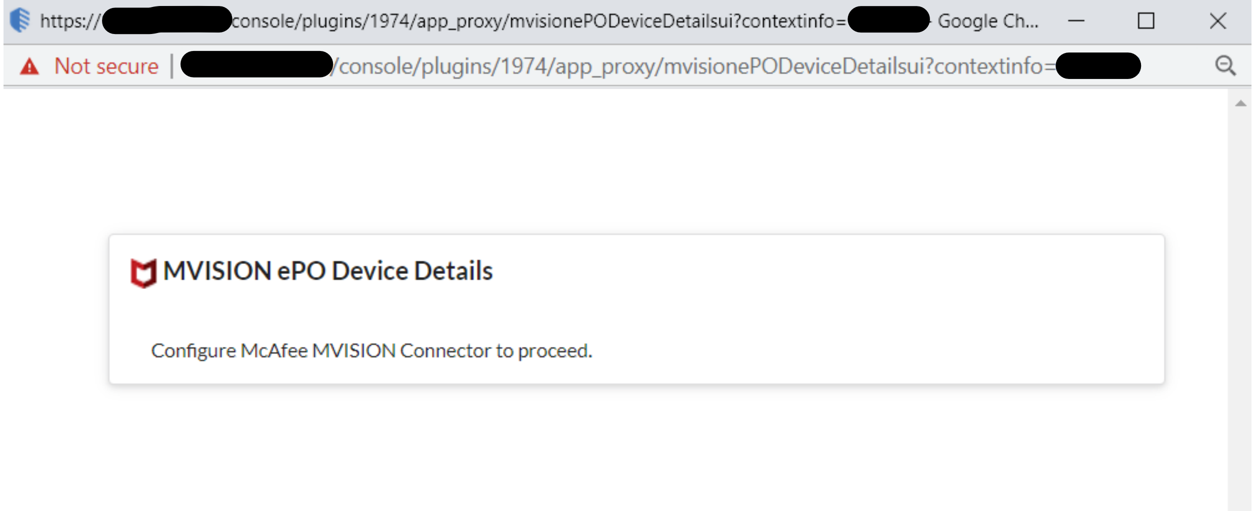
https://[redacted]/console/plugins/1974/app_proxy/mvisionePODeviceDetailsui?contextinfo=[redacted] - Goo...

Not secure | [redacted]/console/plugins/1974/app_proxy/mvisionePODeviceDetailsui?contextinfo=[redacted]...

MVISION ePO Device Details

This device is not managed by currently configured MVISION ePO

When the McAfee MVISION ePO config is not present and admin tried to take an action then following failure message will be displayed:



https://[redacted]console/plugins/1974/app_proxy/mvisionePODeviceDetailsui?contextinfo=[redacted] Google Ch...

Not secure | [redacted]/console/plugins/1974/app_proxy/mvisionePODeviceDetailsui?contextinfo=[redacted]

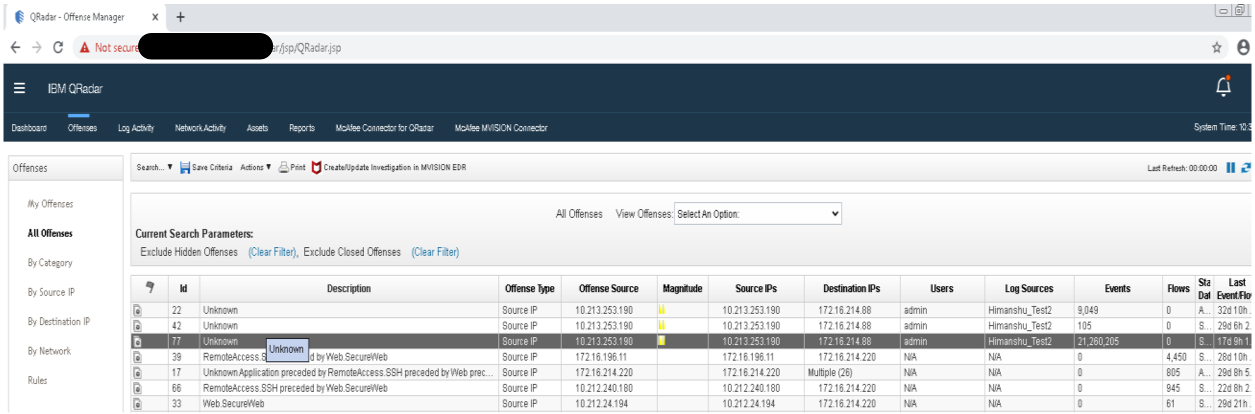
MVISION ePO Device Details

Configure McAfee MVISION Connector to proceed.

Create/Update EDR Investigation for an offense in QRadar

QRadar Admins can create an Investigation for any offense to have additional insight about the offense in MVISION EDR. Admins will have the option to either create a new Investigation or update an existing Investigation for an offense in MVISION EDR.
Note: Only Offense types with IP and Hostname are supported to create EDR Investigation. And EDR supports creation/update of 20 investigations in a single day.

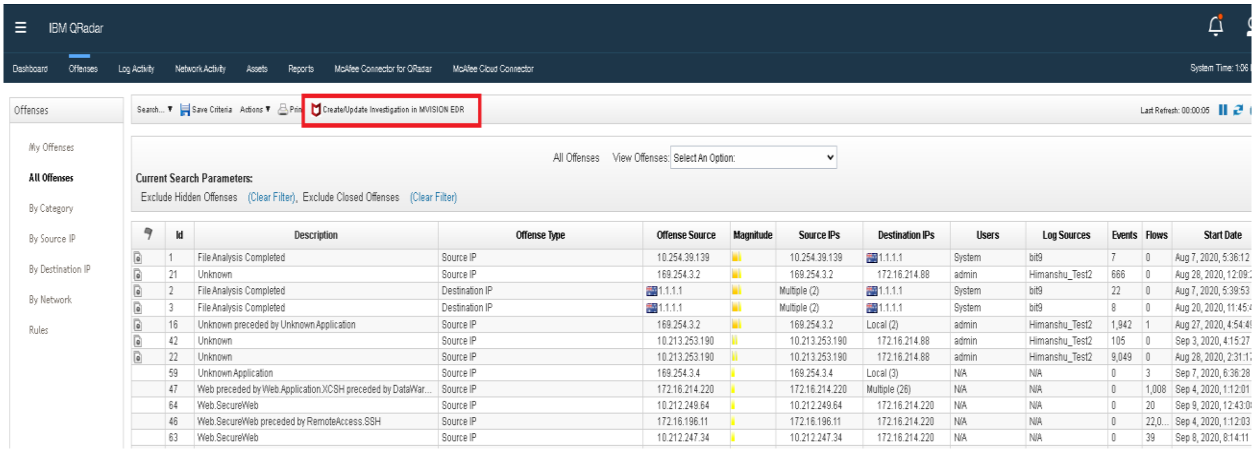
- Go to **Offense** page in QRadar console
- Before taking any action, select any offense for which EDR Investigation to be created as shown below:



Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Sta Dat	Last Event/Flo
22	Unknown	Source IP	10.213.253.190		10.213.253.190	172.16.214.88	admin	Himanshu_Test2	9,049	0	A...	32d 10h ...
42	Unknown	Source IP	10.213.253.190		10.213.253.190	172.16.214.88	admin	Himanshu_Test2	105	0	S...	29d 6h 2...
77	Unknown	Source IP	10.213.253.190		10.213.253.190	172.16.214.88	admin	Himanshu_Test2	21,260,205	0	S...	17d 9h 1...
39	RemoteAccess.S Unknown d by Web.SecureWeb	Source IP	172.16.196.11		172.16.196.11	172.16.214.220	N/A	N/A	0	4,450	S...	28d 10h ...
17	Unknown.Application preceded by RemoteAccess.SSH preceded by Web prec...	Source IP	172.16.214.220		172.16.214.220	Multiple (26)	N/A	N/A	0	805	A...	29d 8h 5...
66	RemoteAccess.SSH preceded by Web.SecureWeb	Source IP	10.212.240.180		10.212.240.180	172.16.214.220	N/A	N/A	0	945	S...	22d 8h 2...
33	Web.SecureWeb	Source IP	10.212.24.194		10.212.24.194	172.16.214.220	N/A	N/A	0	61	S...	29d 21h ...

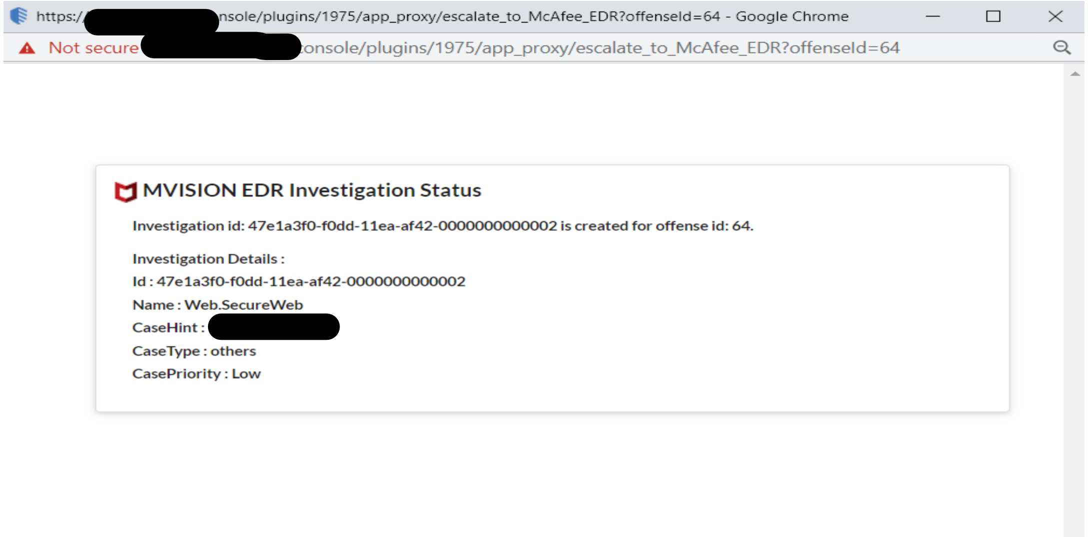
- Click on **Create/Update Investigation in MVISION EDR** button available on offense toolbar as shown below:



Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start Date
1	File.Analysis Completed	Source IP	10.254.39.139		10.254.39.139	1.1.1.1	System	bit9	7	0	Aug 7, 2020, 5:36:12
21	Unknown	Source IP	169.254.3.2		169.254.3.2	172.16.214.88	admin	Himanshu_Test2	666	0	Aug 28, 2020, 12:09:
2	File.Analysis Completed	Destination IP	1.1.1.1		Multiple (2)	1.1.1.1	System	bit9	22	0	Aug 7, 2020, 5:39:53
3	File.Analysis Completed	Destination IP	1.1.1.1		Multiple (2)	1.1.1.1	System	bit9	8	0	Aug 20, 2020, 11:45:
16	Unknown preceded by Unknown.Application	Source IP	169.254.3.2		169.254.3.2	Local (2)	admin	Himanshu_Test2	1,942	1	Aug 27, 2020, 4:54:4
42	Unknown	Source IP	10.213.253.190		10.213.253.190	172.16.214.88	admin	Himanshu_Test2	105	0	Sep 3, 2020, 4:15:27
22	Unknown	Source IP	10.213.253.190		10.213.253.190	172.16.214.88	admin	Himanshu_Test2	9,049	0	Aug 28, 2020, 2:31:1
59	Unknown.Application	Source IP	169.254.3.4		169.254.3.4	Local (3)	N/A	N/A	0	3	Sep 7, 2020, 6:36:28
47	Web preceded by Web.Application.XCSH preceded by DataWar...	Source IP	172.16.214.220		172.16.214.220	Multiple (26)	N/A	N/A	0	1,008	Sep 4, 2020, 1:12:01
64	Web.SecureWeb	Source IP	10.212.249.64		10.212.249.64	172.16.214.220	N/A	N/A	0	20	Sep 9, 2020, 12:43:0
46	Web.SecureWeb preceded by RemoteAccess.SSH	Source IP	172.16.196.11		172.16.196.11	172.16.214.220	N/A	N/A	0	22,0...	Sep 4, 2020, 1:12:03
63	Web.SecureWeb	Source IP	10.212.247.34		10.212.247.34	172.16.214.220	N/A	N/A	0	39	Sep 8, 2020, 8:14:11

- If the existing Investigation doesn't exist, then Admin will see a window where details of newly created EDR Investigation will be shown as depicted below:



https:/[redacted]nsole/plugins/1975/app_proxy/escalate_to_McAfee_EDR?offenseId=64 - Google Chrome

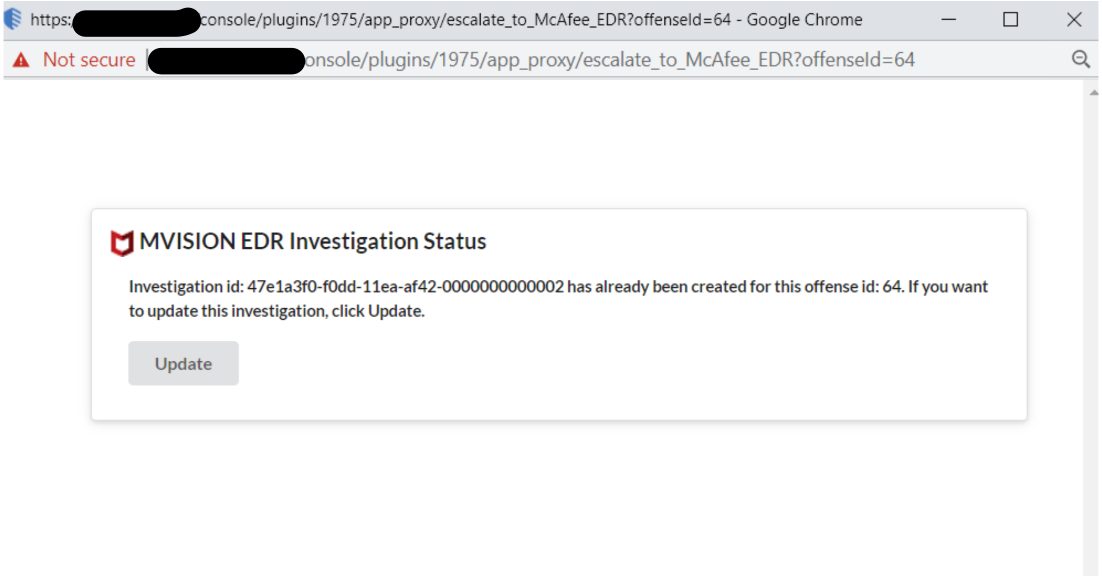
Not secure [redacted]onsole/plugins/1975/app_proxy/escalate_to_McAfee_EDR?offenseId=64

MVISION EDR Investigation Status

Investigation id: 47e1a3f0-f0dd-11ea-af42-0000000000002 is created for offense id: 64.

Investigation Details :
Id : 47e1a3f0-f0dd-11ea-af42-0000000000002
Name : Web.SecureWeb
CaseHint : [redacted]
CaseType : others
CasePriority : Low

- If the investigation already exists in MVISION EDR then Admin will be presented with a window with Investigation id detail as shown below:



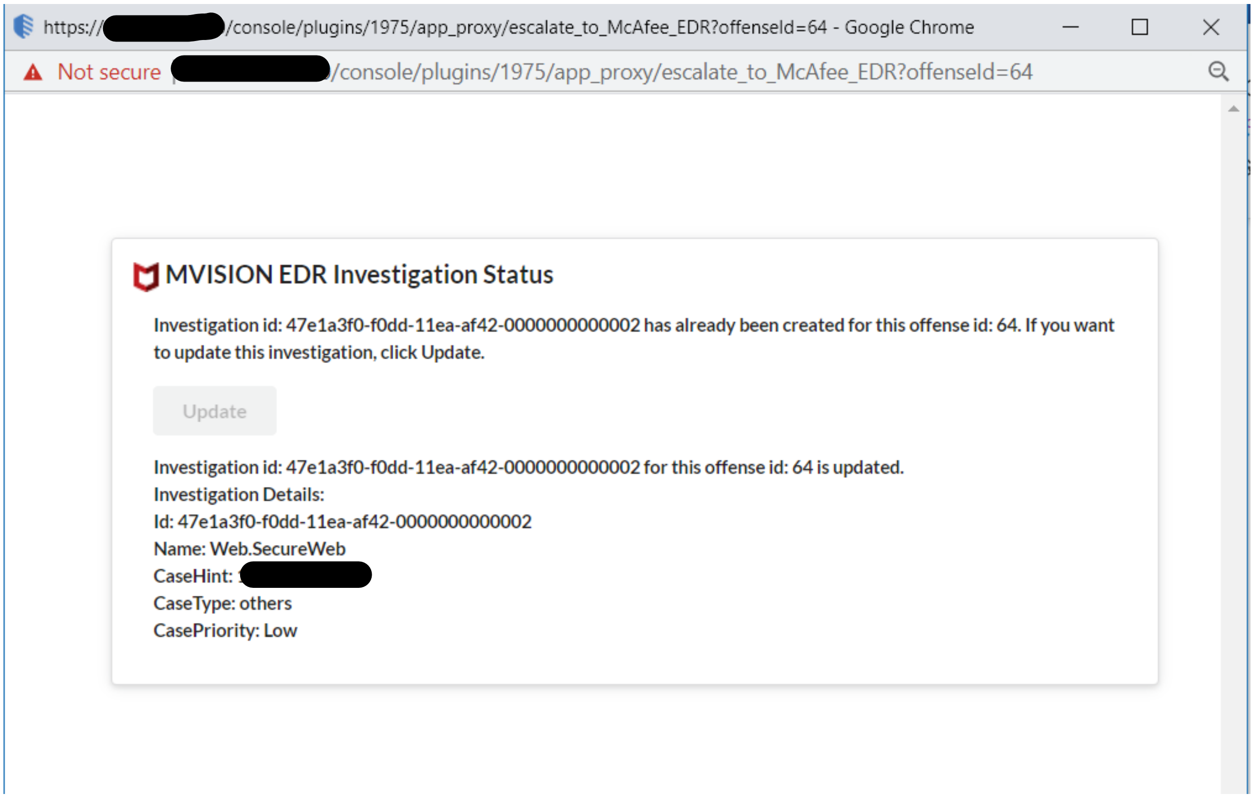
https:[redacted]console/plugins/1975/app_proxy/escalate_to_McAfee_EDR?offenseId=64 - Google Chrome

Not secure [redacted]onsole/plugins/1975/app_proxy/escalate_to_McAfee_EDR?offenseId=64

MVISION EDR Investigation Status

Investigation id: 47e1a3f0-f0dd-11ea-af42-0000000000002 has already been created for this offense id: 64. If you want to update this investigation, click Update.

- Admin can decide whether they want to update the EDR Investigation details. In case if they choose to update, they will be presented with updated EDR Investigation details as shown below:



https://[redacted]/console/plugins/1975/app_proxy/escalate_to_McAfee_EDR?offenseId=64 - Google Chrome

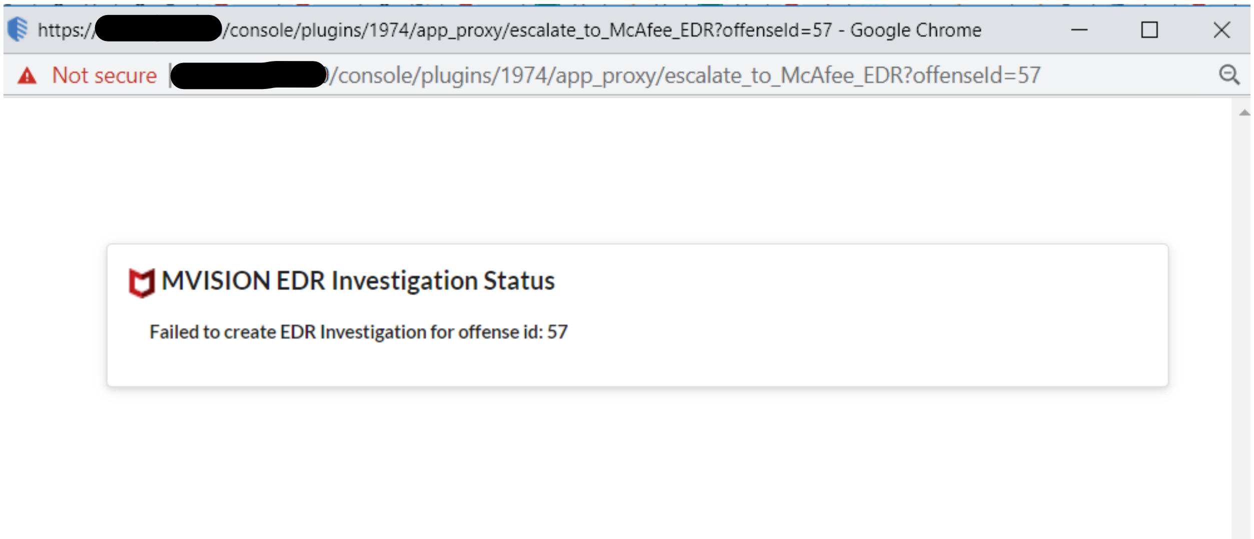
Not secure [redacted]/console/plugins/1975/app_proxy/escalate_to_McAfee_EDR?offenseId=64

MVISION EDR Investigation Status

Investigation id: 47e1a3f0-f0dd-11ea-af42-0000000000002 has already been created for this offense id: 64. If you want to update this investigation, click Update.

Investigation id: 47e1a3f0-f0dd-11ea-af42-0000000000002 for this offense id: 64 is updated.
Investigation Details:
Id: 47e1a3f0-f0dd-11ea-af42-0000000000002
Name: Web.SecureWeb
CaseHint: [redacted]
CaseType: others
CasePriority: Low

- In case where EDR investigation creation fails, below mentioned failure message will be displayed:



https://[redacted]/console/plugins/1974/app_proxy/escalate_to_McAfee_EDR?offenseId=57 - Google Chrome

Not secure [redacted]/console/plugins/1974/app_proxy/escalate_to_McAfee_EDR?offenseId=57

MVISION EDR Investigation Status

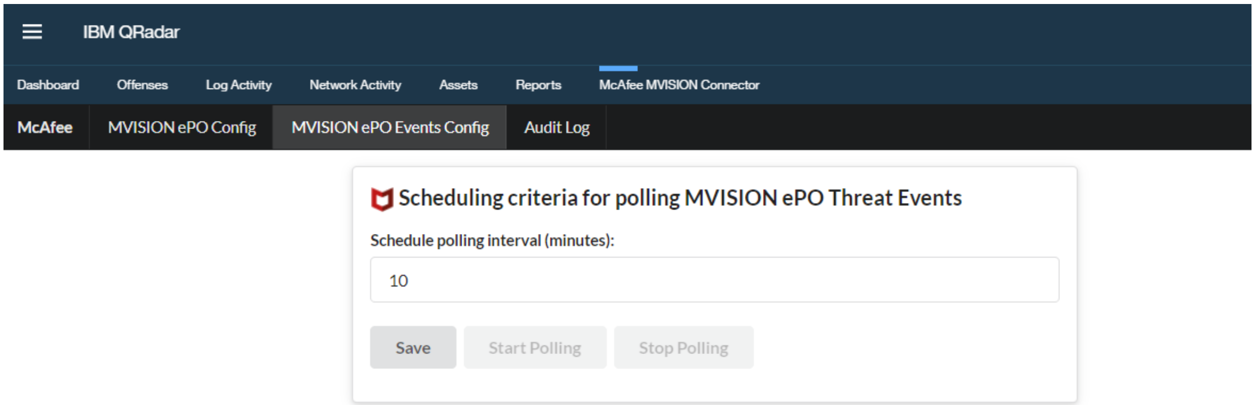
Failed to create EDR Investigation for offense id: 57

Poll Threat Events from MVISION ePO to Log Activity on QRadar

This feature enables QRadar Admins to fetch threat events from MVISION ePO and show on Log Activity page. Admins must configure scheduling criteria for polling the events by providing how frequently polling must be done.

Poll Configuration

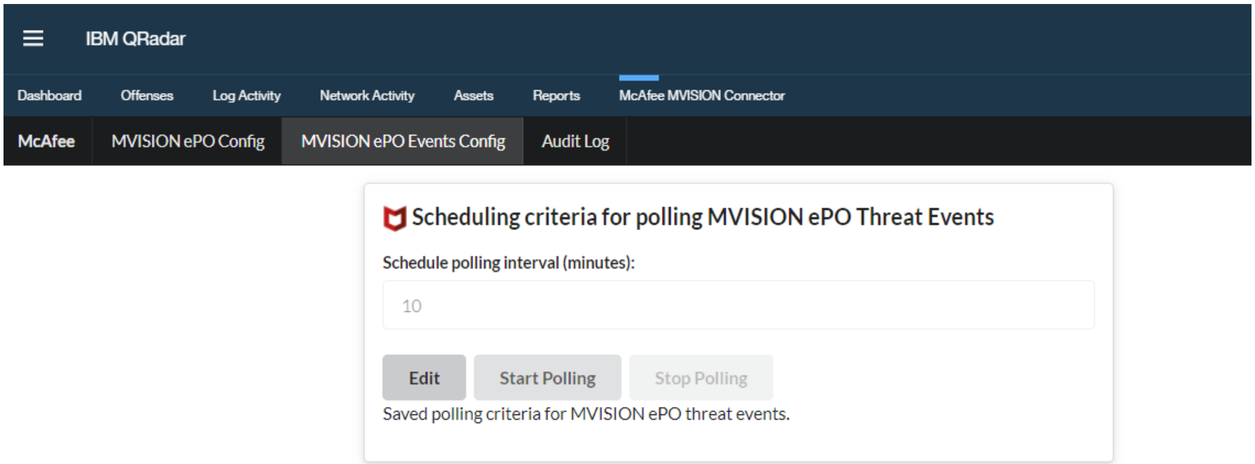
To configure this, navigate to **McAfee MVISION Connector** App > click **on MVISION ePO Events Config** tab as shown below:



Scheduling criteria for polling MVISION ePO Threat Events

Schedule polling interval (minutes): 10

Admin can specify polling interval in minutes. Range of the interval is :10 minutes to 2880 minutes



Scheduling criteria for polling MVISION ePO Threat Events

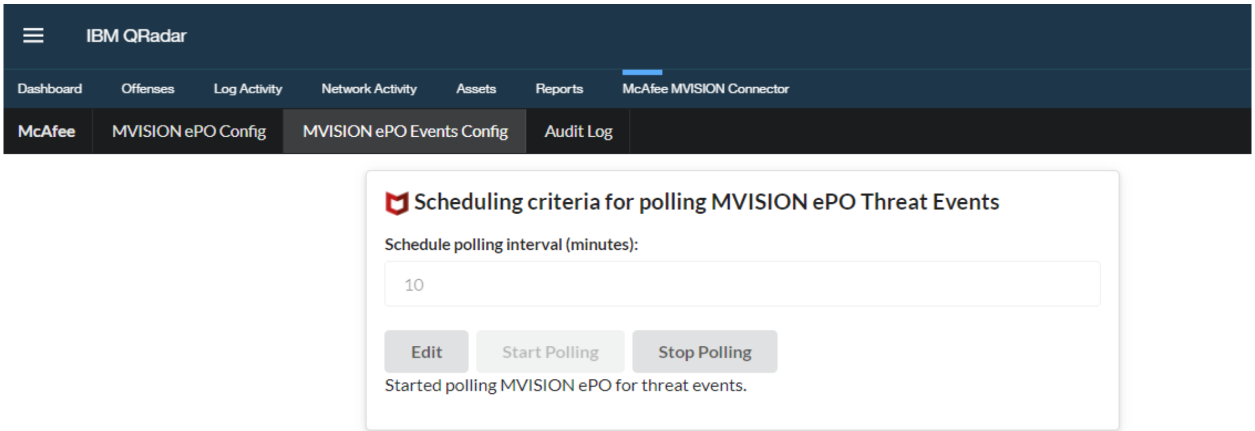
Schedule polling interval (minutes): 10

Saved polling criteria for MVISION ePO threat events.

Once the interval is saved, Admins will be able to start the poll for threat events. Once the poll is started, background process will fetch the events generated between the poll start time and interval specified. For example: if poll started at 2:00 PM and interval specified is 10 minutes then it will pull all events received on MVISION ePO between 2:00 PM and 2:10 PM in the first go. In next poll, background process will pull all events received on ePO from 2:10 PM to 2:20 PM and so on.

Note: UTC time is considered for performing polling operation. Make sure QRadar server and MVISION ePO are time-synced.

To start polling, click on **Start Polling** button once polling interval is saved as shown below:

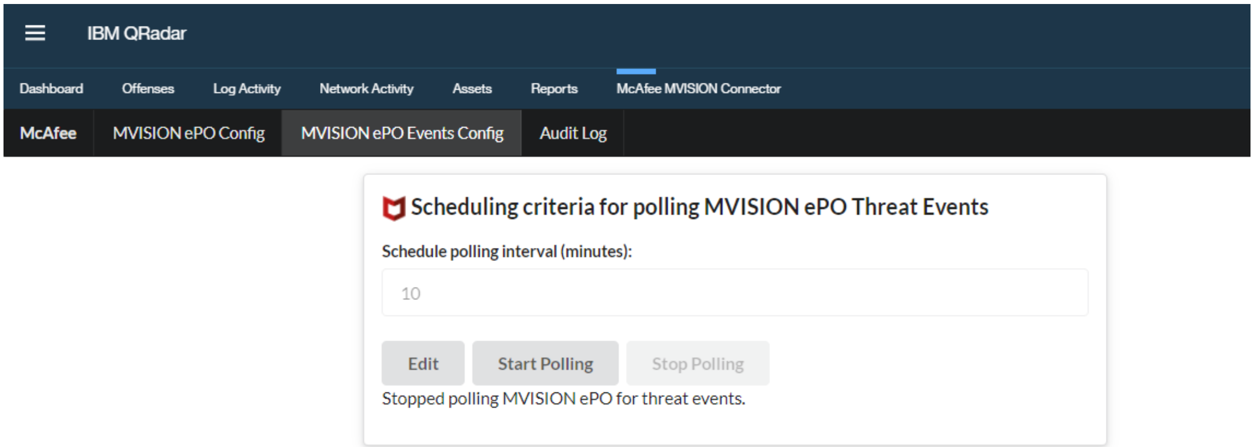


Scheduling criteria for polling MVISION ePO Threat Events

Schedule polling interval (minutes): 10

Started polling MVISION ePO for threat events.

To stop polling, click on **Stop Polling** button as shown below:



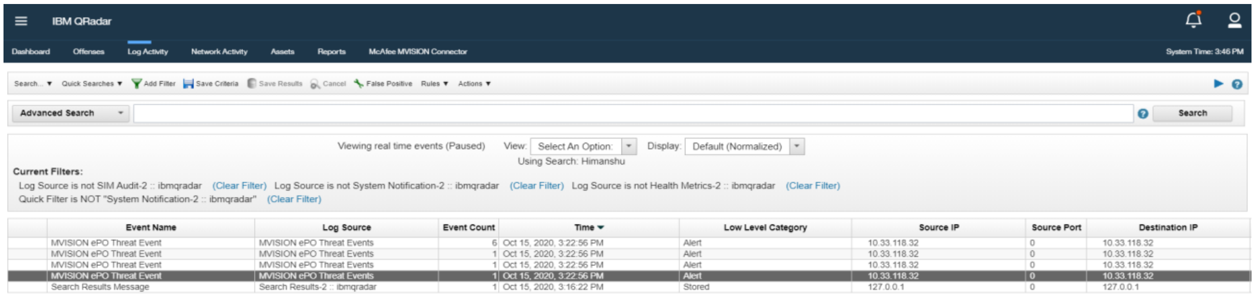
Scheduling criteria for polling MVISION ePO Threat Events

Schedule polling interval (minutes): 10

Stopped polling MVISION ePO for threat events.

Note: Threat events will be fetched only for the time duration when polling is active. Any events generated before start of event poll or after the poll has been stopped will not be fetched on QRadar.

On successful poll of threat events, Admins can see events on **Log Activity** page as shown below:



Viewing real time events (Paused) View: Select An Option: Display: Default (Normalized)

Using Search: Himanshu

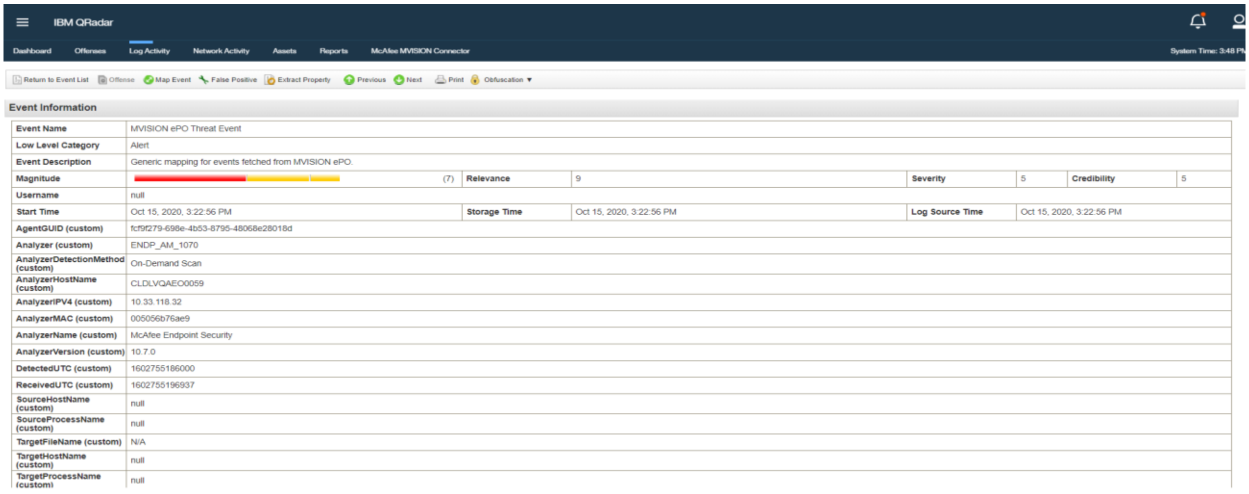
Current Filters:

Log Source is not SIM Audit-2 :: ibmqradar (Clear Filter) Log Source is not System Notification-2 :: ibmqradar (Clear Filter) Log Source is not Health Metrics-2 :: ibmqradar (Clear Filter)

Quick Filter is NOT "System Notification-2 :: ibmqradar" (Clear Filter)

Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP
MVISION ePO Threat Event	MVISION ePO Threat Events	6	Oct 15, 2020, 3:22:56 PM	Alert	10.33.118.32	0	10.33.118.32
MVISION ePO Threat Event	MVISION ePO Threat Events	1	Oct 15, 2020, 3:22:56 PM	Alert	10.33.118.32	0	10.33.118.32
MVISION ePO Threat Event	MVISION ePO Threat Events	1	Oct 15, 2020, 3:22:56 PM	Alert	10.33.118.32	0	10.33.118.32
MVISION ePO Threat Event	MVISION ePO Threat Events	1	Oct 15, 2020, 3:22:56 PM	Alert	10.33.118.32	0	10.33.118.32
Search Results Message	Search Results-2 :: ibmqradar	1	Oct 15, 2020, 3:16:22 PM	Stored	127.0.0.1	0	127.0.0.1

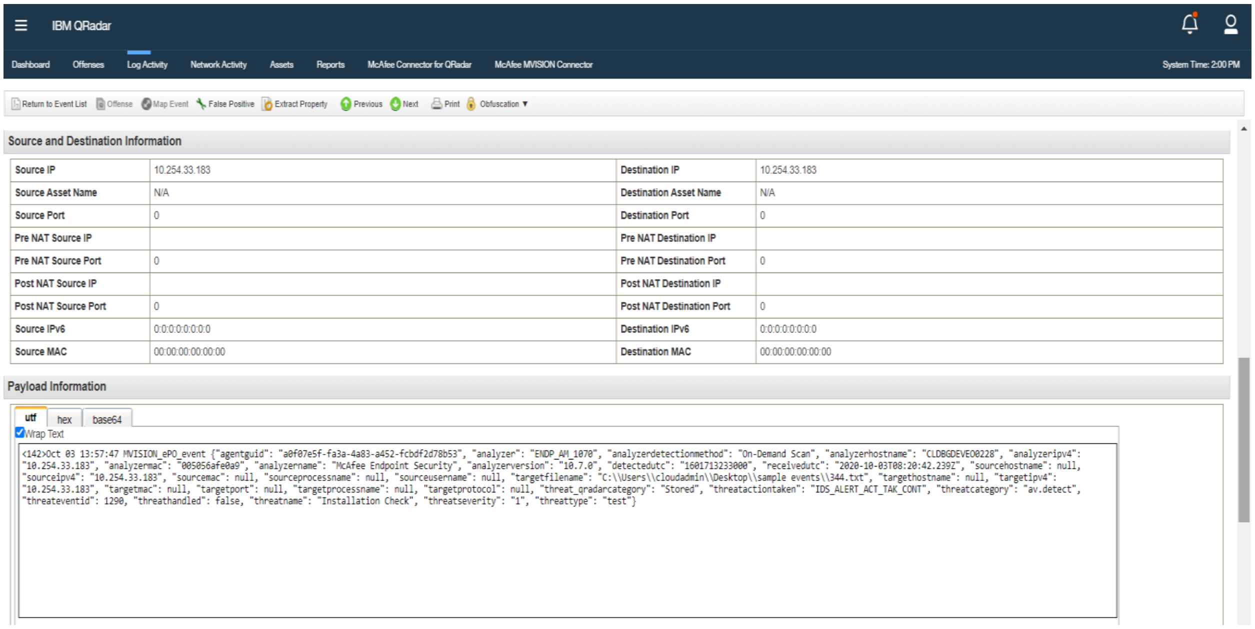
Event is parsed using the custom properties and DSM parser which is defined for MVISION ePO Threat events as shown below:



Event Information

Event Name	MVISION ePO Threat Event						
Low Level Category	Alert						
Event Description	Generic mapping for events fetched from MVISION ePO.						
Magnitude	(7)	Relevance	9	Severity	5	Credibility	5
Username	null						
Start Time	Oct 15, 2020, 3:22:56 PM	Storage Time	Oct 15, 2020, 3:22:56 PM	Log Source Time	Oct 15, 2020, 3:22:56 PM		
AgentGUID (custom)	fcf9f279-698e-4b53-8795-48068e28018d						
Analyzer (custom)	ENDP_AM_1070						
AnalyzerDetectionMethod (custom)	On-Demand Scan						
AnalyzerHostName (custom)	CLDLVQAEO0059						
AnalyzerIPV4 (custom)	10.33.118.32						
AnalyzerMAC (custom)	005056b76ae9						
AnalyzerName (custom)	McAfee Endpoint Security						
AnalyzerVersion (custom)	10.7.0						
DetectedUTC (custom)	1602755186000						
ReceivedUTC (custom)	1602755196937						
SourceHostName (custom)	null						
SourceProcessName (custom)	null						
TargetFileName (custom)	N/A						
TargetHostName (custom)	null						
TargetProcessName (custom)	null						

Threat Event in JSON format fetched from MVISION ePO



Source and Destination Information

Source IP	10.254.33.183	Destination IP	10.254.33.183
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

☑ Wrap Text

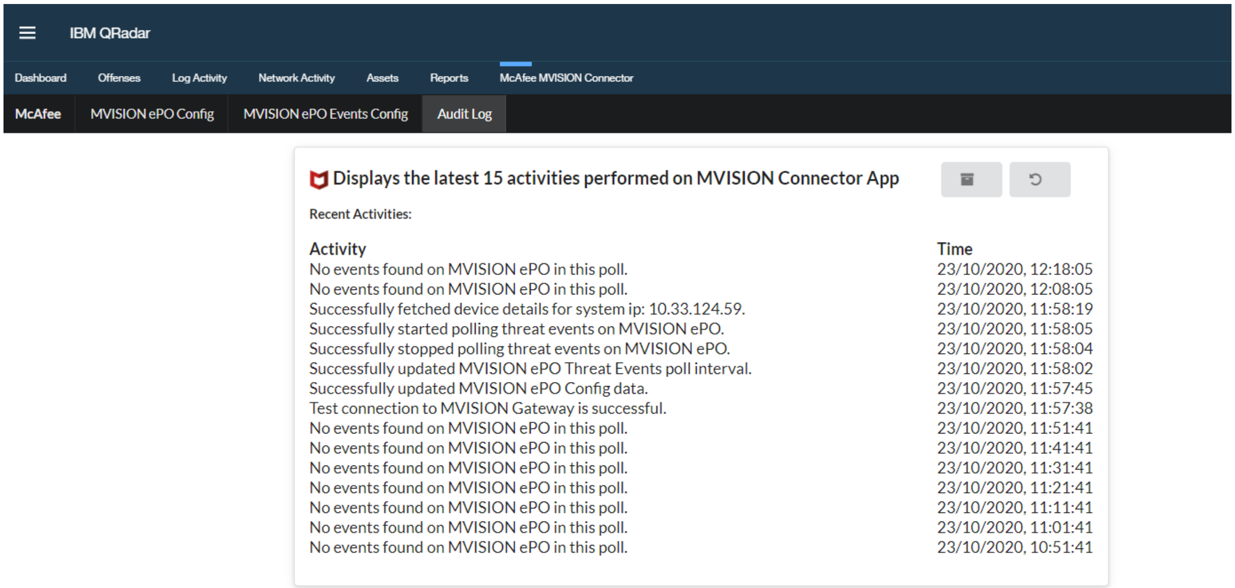
```
<142>Oct 03 13:57:47 MVISION_ePO_event {"agentguid": "a0f07e5f-fa3a-4a83-a452-fcbdf2d78b53", "analyzer": "ENDP_AM_1070", "analyzerdetectionmethod": "On-Demand Scan", "analyzerhostname": "CLDBGDEVEO0228", "analyzeripv4":
"10.254.33.183", "analyzermac": "005056afe0a9", "analyzername": "McAfee Endpoint Security", "analyzerversion": "10.7.0", "detectedutc": "1601713233000", "receivedutc": "2020-10-03T08:20:42.239Z", "sourcehostname": null,
"sourceipv4": "10.254.33.183", "sourcemac": null, "sourceprocessname": null, "sourceusername": null, "targetfilename": "C:\\Users\\cloudadmin\\Desktop\\sample events\\344.txt", "targethostname": null, "targetipv4":
"10.254.33.183", "targetmac": null, "targetport": null, "targetprocessname": null, "targetprotocol": null, "threat_qradarcategory": "Stored", "threatactiontaken": "IDS_ALERT_ACT_TAK_CONT", "threatcategory": "av.detect",
"threateventid": 1290, "threathandled": false, "threatname": "Installation Check", "threatseverity": "1", "threattype": "test"}
```

Note: All MVISION ePO Threat events will have the following mapping:

Event Name	MVISION ePO Threat Event
Low Level Category	Alert

Audit Log

This feature is provided to the Admins to see actions performed on McAfee MVISION Connector for QRadar App. This page will hold list of most recent 15 activities performed on the App for example saving ePO config etc. as shown below:



Displays the latest 15 activities performed on MVISION Connector App

Recent Activities:

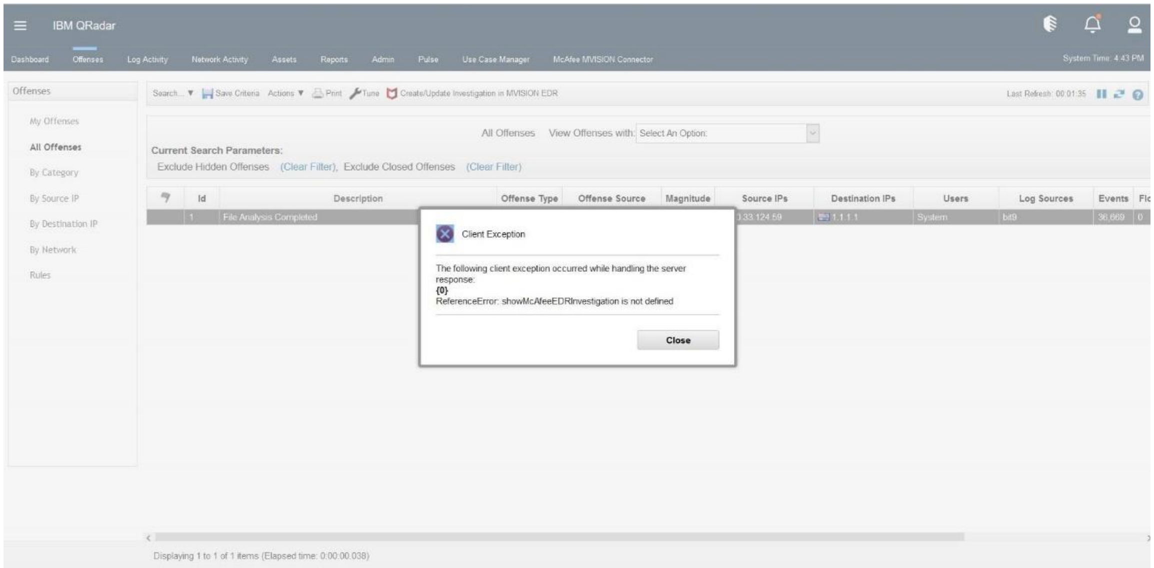
```
Activity                                                          Time
No events found on MVISION ePO in this poll.                      23/10/2020, 12:18:05
No events found on MVISION ePO in this poll.                      23/10/2020, 12:08:05
Successfully fetched device details for system ip: 10.33.124.59.  23/10/2020, 11:58:19
Successfully started polling threat events on MVISION ePO.        23/10/2020, 11:58:05
Successfully stopped polling threat events on MVISION ePO.        23/10/2020, 11:58:04
Successfully updated MVISION ePO Threat Events poll interval.     23/10/2020, 11:58:02
Successfully updated MVISION ePO Config data.                     23/10/2020, 11:57:45
Test connection to MVISION Gateway is successful.                 23/10/2020, 11:57:38
No events found on MVISION ePO in this poll.                      23/10/2020, 11:51:41
No events found on MVISION ePO in this poll.                      23/10/2020, 11:41:41
No events found on MVISION ePO in this poll.                      23/10/2020, 11:31:41
No events found on MVISION ePO in this poll.                      23/10/2020, 11:21:41
No events found on MVISION ePO in this poll.                      23/10/2020, 11:11:41
No events found on MVISION ePO in this poll.                      23/10/2020, 11:01:41
No events found on MVISION ePO in this poll.                      23/10/2020, 10:51:41
```

- To see the most recent logs, Admin must click on “**Refresh**” icon available on the top-right corner.
- To delete the logs, Admin can click on “**Delete**” icon. This action will delete all the audit logs captured for the app.

Important things to know

Steps to follow if exception is displayed while clicking on Create/Update EDR Investigation button

In case if Admin encounters an exception while executing EDR Create/Update action, try reloading the page by doing a refresh, or re-login to QRadar console or try on a different browser like chrome.



All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flo
	1	File Analysis Completed				0.33.124.59	1.1.1.1	System	bit9	36,669	0

Client Exception

The following client exception occurred while handling the server response:
{0}
ReferenceError: showMcAfeeEDRInvestigation is not defined

Displaying 1 to 1 of 1 items (Elapsed time: 0:00:00.038)

Steps to follow if ‘SSL: CERTIFICATE_VERIFY_FAILED’ message appears in app log

There might be two reasons if you see SSL: CERTIFICATE_VERIFY_FAILED in the container app log:

Reason #1: Since McAfee MVISION connector app is accessing McAfee’s API which is hosted in AWS gateway, it is required that the QRadar server should have the latest AWS cert chain in the QRadar cert bundle. Hence, make sure that the QRadar server has the required AWS cert chain the QRadar server certificate bundle.

Reason #2: If the McAfee MVISION connector app is configured with the proxy server and if the proxy server requires the certificate for any outbound request/communication, then you must have the corresponding proxy server certificate in the QRadar server certificate bundle.