McAfee ePolicy Orchestrator

The McAfee ePolicy Orchestrator (ePO) DSM for IBM Security QRadar accepts events using Java Database Connectivity (JDBC) or Simple Network Management Protocol (SNMPv2, and SNMPv3).

QRadar records all relevant ePO anti-virus events from JDBC or SNMP. You can configure McAfee ePolicy Orchestrator to integrate with QRadar using one of the following methods:

- **Configuring a log source using the JDBC protocol**
- **Configuring ePO to Forward SNMP Events**

Configuring a log source using the JDBC protocol

To configure QRadar to access the ePO database using the JDBC protocol:

Procedure

Step 1 Click the **Admin** tab.

Step 2 Click the **Log Sources** icon.

Step 3 Click **Add**.

Step 4 In the **Log Source Name** field, type a name for your McAfee ePolicy Orchestrator log source.

Step 5 From the **Log Source Type** list, select **McAfee ePolicy Orchestrator**.

Step 6 Using the **Protocol Configuration** list, select **JDBC**.

You must refer to the Configure Database Settings on your ePO Management Console to configure the McAfee ePolicy Orchestrator with JDBC.

Step 7 Configure the following log source parameters:

Table 59-6 McAfee ePO JDBC protocol parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. The log source identifier must be added in the following format: **`<McAfee ePO Database>@<McAfee ePO Database Server IP or Host Name>`** Where: **`<McAfee ePO Database>`** is the database name, as entered in the Database Name parameter. **`<McAfee ePO Database Server IP or Host Name>`** is the hostname or IP address for this log source, as entered in the IP or Hostname parameter. When defining a name for your log source identifier, you must use the values of the McAfee ePO Database and Database Server IP address or hostname from the ePO Management Console.
Database Type	From the list, select **MSDE**.

Table 59-6 McAfee ePO JDBC protocol parameters (continued)

Parameter	Description
Database Name	Type the exact name of the McAfee ePolicy Orchestrator database.
IP or Hostname	Type the IP address or host name of the McAfee ePolicy Orchestrator SQL Server.
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the McAfee ePolicy Orchestrator database. The McAfee ePolicy Orchestrator database must have incoming TCP connections enabled to communicate with QRadar. ***Note:*** *If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.*
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this parameter blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. ***Note:*** *If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.*
Table Name	Type a table or view that includes the event records as follows: • For ePO 3.x - Type **Events**. • For ePO 4.x - Type **EPOEvents**.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. Also, the list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type **AutoID** in the compare field. The compare field is used to identify new events added between queries to the table.

Table 59-6 McAfee ePO JDBC protocol parameters (continued)

Parameter	Description
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allow the JDBC protocol source to setup the SQL statement once, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

Note: Selecting a value for the Credibility parameter greater than 5 will weight your McAfee ePolicy Orchestrator log source with a higher importance compared to other log sources in QRadar.

Step 8 Click **Save**.

Step 9 On the **Admin** tab, click **Deploy Changes**.

Configuring ePO to Forward SNMP Events

To configure ePO to forward events using SNMP, you must complete the following configuration steps on your McAfee ePolicy Orchestrator device:

1. Add a registered server. For more information, see **Adding a Registered Server to McAfee ePO**.
2. Configure the SNMP trap notifications on your ePO device. For more information, see **Configuring SNMP Notifications**.
3. Configure the log source and protocol in QRadar. For more information, see **Configuring the Log Source in QRadar**.
4. Optional. Install the Java Cryptography Extension for high level SNMP decryption algorithms. For more information, see **Installing the Java Cryptography Extension**.

Adding a Registered Server to McAfee ePO

Step 1 Log in to your McAfee ePolicy Orchestrator console.

Step 2 Select **Menu > Configuration > Registered Servers**.

Step 3 Click **New Server**.

Step 4 From the **Server Type** menu, select **SNMP Server**.

Step 5 Type the name and any additional notes about the SNMP server, click **Next**.

Step 6 From the **Address** list, select the type of server address you are using:

- a **DNS Name** - Type the DNS name of QRadar.
- b **IPv4** - Type the IPv4 address of QRadar.
- c **IPv6** - Type the IPv6 address of QRadar.

Step 7 From the **SNMP Version** list, select the SNMP version to use with QRadar.

- a If you are using SNMPv2c, you must provide the **Community** name.
- b If you are using SNMPv3, you must provide the **SNMPv3 Security** details.

Step 8 Click **Send Test Trap** to verify the SNMP configuration.

Step 9 Click **Save**.

The SNMP server you configured is added to the Registered Server page.

You are now ready to configure the SNMP notifications in McAfee ePolicy Orchestrator.

Configuring SNMP Notifications

To configure the event type to generate SNMP trap notifications:

Step 1 Select **Menu > Automation > Automatic Responses**.

Step 2 Click **New Responses**.

Step 3 Configure the following values:

- a **Name** - Type a name for the response.

b **Description** - Type a description for the response.

c **Event group** - From the **Event group** list, select **ePO Notification Events**.

d **Event type** - From the **Event type** list, select **Threats**.

e **Status** - Select **Enabled**.

Step 4 Click **Next**.

The Response Builder Filter is displayed.

Step 5 From the **Value** column, type a value to use for system selection, or click the ellipsis button.

Step 6 Optional. From the **Available Properties** list, select any additional filters to narrow the response results.

Step 7 Click **Next**.

The Response Builder Aggregation window is displayed.

Step 8 Select **Trigger this response for every event** and click **Next**.

Note: We recommend that when you configure aggregation for your McAfee ePO responses that you do not enable throttling.

Step 9 From the **Actions** list, select **Send SNMP Trap**.

Step 10 Configure the following values:

a From the list of SNMP servers, select the SNMP server you registered in **Adding a Registered Server to McAfee ePO**, **Step 5**.

b From the **Available Types** list, select **List of All Values.**

c Click **>>** to add to the following Select Types window from **Table 59-7** based on your McAfee ePolicy Orchestrator version.

Table 59-7 Supported Parameters for Event Detection

Available Types	Selected Types	ePO Version
Detected UTC	{listOfDetectedUTC}	4.5
Received UTC	{listOfReceivedUTC}	4.5
Detecting Product IPv4 Address	{listOfAnalyzerIPV4}	4.5
Detecting Product IPv6 Address	{listOfAnalyzerIPV6}	4.5
Detecting Product MAC Address	{listOfAnalyzerMAC}	4.5
Source IPv4 Address	{listOfSourceIPV4}	4.5
Source IPv6 Address	{listOfSourceIPV6}	4.5
Source MAC Address	{listOfSourceMAC}	4.5
Source User Name	{listOfSourceUserName}	4.5
Target IPv4 Address	{listOfTargetIPV4}	4.5
Target IPv6 Address	{listOfTargetIPV6}	4.5
Target MAC	{listOfTargetMAC}	4.5
Target Port	{listOfTargetPort}	4.5

Table 59-7 Supported Parameters for Event Detection

Available Types	Selected Types	ePO Version
Threat Event ID	{listOfThreatEventID}	4.5
Threat Severity	{listOfThreatSeverity}	4.5
SourceComputers		4.0
AffectedComputerIPs		4.0
EventIDs		4.0
TimeNotificationSent		4.0

Step 11 Click **Next**.

Step 12 Click **Save**.

Configuring the Log Source in QRadar

To configure QRadar to receive event logs from McAfee ePolicy Orchestrator using SNMP:

Step 1 Click the **Admin** tab.

Step 2 Click the **Log Sources** icon.

Step 3 Click **Add**.

Step 4 In the **Log Source Name** field, type a name for your McAfee ePolicy Orchestrator log source.

Step 5 From the **Log Source Type** list, select **McAfee ePolicy Orchestrator**.

Step 6 From the **Protocol Configuration** list, select either **SNMPv2**, or **SNMPv3**.

Note: SNMPv1 is listed as an option in the Protocol Configuration list, but SNMPv1 is not a recommended protocol when using McAfee ePolicy Orchestrator with QRadar.

Step 7 Configure the following values based on the protocol you selected in **Step 6**:

a To configure the SNMPv2 protocol:

Table 59-8 SNMPv2 Configuration Parameters

Parameter	Description
Log Source Identifier	Type the IP address for the log source. The log source identifier must be unique for the log source type.
Community	Type the SNMP community string for the SNMPv2 protocol, such as Public. The default community string is Public.

Table 59-8 SNMPv2 Configuration Parameters (continued)

Parameter	Description
Include OIDs in Event Payload	Select this check box. This options allows the McAfee ePO event payloads to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events for McAfee ePO. ***Note:*** *This option is not supported for SNMPv1 configurations of McAfee ePO.*

b To configure the SNMPv3 protocol:

Table 59-9 SNMPv3 Configuration Parameters

Parameter	Description
Log Source Identifier	Type the IP address for the log source. The log source identifier must be unique for the log source type.
Authentication Protocol	From the list, select the algorithm you want to use to authenticate SNMP traps. This parameter is required if you are using SNMPv3. The options include: • **SHA** - Select this option to use Secure Hash Algorithm (SHA) as your authentication protocol. • **MD5** - Select this option to use Message Digest 5 (MD5) as your authentication protocol. The default is MD5.
Authentication Password	Type the password you want to use to authenticate SNMP. This parameter is required if you are using SNMPv3. ***Note:*** *Your authentication password must include a minimum of 8 characters.*
Decryption Protocol	From the list, select the algorithm you want to use to decrypt the SNMP traps. This parameter is required if you are using SNMPv3. The decryption algorithms include: • DES • AES128 • AES192 • AES256 The default is AES256. ***Note:*** *If you select AES192 or AES256 as your decryption algorithm, you must install additional software for QRadar. For more information, see* **Installing the Java Cryptography Extension***.*

Table 59-9 SNMPv3 Configuration Parameters (continued)

Parameter	Description
Decryption Password	Type the password used to decrypt SNMP traps. This parameter is required if you are using SNMPv3. ***Note:*** *Your decryption password must include a minimum of 8 characters.*
User	Type the user access for this protocol. The default is AdminUser. The username can be up to 255 characters in length.
Include OIDs in Event Payload	Select this check box. This options allows the McAfee ePO event payloads to be constructed using a name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events for McAfee ePO. ***Note:*** *This option is not supported for SNMPv1 configurations of McAfee ePO.*

For more information on configuring SNMP on your ePO device, see the McAfee website at *http://www.mcafee.com*.

Installing the Java Cryptography Extension

The Java™ Cryptography Extension (JCE) is a Java framework that is required for QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE with QRadar and on your McAfee ePO appliance.

To allow AES192 or AES256 decryption on QRadar, you must:

1 **Install the JCE on McAfee ePolicy Orchestrator**

2 **Install the JCE on QRadar**

Install the JCE on McAfee ePolicy Orchestrator

To install the Unrestricted JCE Policy Files on QRadar.

Step 1 Download the latest version of the JavaTM Cryptography Extension:

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

There may be several versions of the JCE available for download. The version you download should match the version of the Java™ installed on your McAfee ePO appliance.

Step 2 Copy the JCE zip file to the following directory on your McAfee ePO appliance:

`<McAfee ePO>/jre/lib/security`

Where `<McAfee ePO>` is the installation path for ePolicy Orchestrator.

The installation is complete.