# McAfee Enterprise Security Manager

# Data Source Configuration Guide

Data Source: *Check Point*

August 21, 2014

**Important Note:**

The information contained in this document is confidential and proprietary.

Please do not redistribute without permission.

# Table of Contents

# 1 Introduction

This guide details how to configure Check Point to allow the Receiver to pull events from the OPSEC LEA client.

# 2 Prerequisites

McAfee Enterprise Security Manager Version 9.2.0 and above.

In order to configure Check Point, appropriate administrative level access is required to perform the necessary changes documented below.

# 3 Specific Data Source Configuration Details

## 3.1 Check Point Configuration

### 3.1.1 Enable LEA service on the Check Point management server

1. SSH to the Check Point management server
2. Enter expert mode
3. Open $FWDIR/conf/fwopsec.conf and edit the file according to the type of authentication you want to use.  Recommend is Authenticated and encrypted.
   For Authenticated and encrypted connection, specify:
   ```
   lea_server auth_port 18184
   lea_server auth_type sslca (or other supported method )
   ```
   For Authenticated Connection only, specify:
   ```
   lea_server auth_port 18184
   ```
   For no authentication or encryption, specify:
   ```
   lea_server port 18184
   ```
4. Run “cprestart”

### 3.1.2 Create an OPSEC Application

1. Log in to the Check Point user interface.
2. Expand the OPSEC Applications tree node and right-click on the OPSEC Application category
3. Select “New OPSEC Application”
4. Enter a name for the OPSEC Application (Will be used later on when creating the data source in the SIEM.)
5. Select a host from the “Host” field and select the network object that represents the McAfee Event Receiver. If the object does not exist, create one by clicking the “New” button and entering the IP of the Receiver.
6. Leave the “Vendor” field as the default selection “User Defined”.
7. Select the “LEA” checkbox in the “Client Entries” section

Steps 7-10 only needed if using authentication

8. Click on the “Communication” button, located near the bottom of the dialog.
9. Enter and confirm your one-time password.
10. Click the “Initialize” button. This will initialize the certificate and you will see the message “Initialized but trust not established.”
11. Close the “Communication” dialog
12. Click “OK” on the OPSEC Application Process dialog.
13. Perform an Install DB on the check Point server

### 3.1.3 Additional Information (required when adding a Check Point CLM or Secondary CMA)

Typically, the DN is not required for anything other than adding the Check Point CLM as a data source. The configuration steps below are needed when firewall logs are sent to a CLM instead of the CMA.

1. SSH to the CMA
2. Enter expert mode
3. Run “grep sic_name $FWDIR/conf/objects_5_0.C”
   This will show all DNs. Find the correct one for the CLM.

## 3.2 McAfee Receiver Configuration

### 3.2.1 Best Practices

Create your Check Point Data sources in a parent child relationship. Create your Primary CMA as the Parent data source, and then add your CLMs, Secondary CMAs and Firewalls as children to the Primary CMA data source

### 3.2.2 Data Source Creation

After successfully logging into the McAfee ESM console the data source will need to be added to a McAfee Receiver in the ESM hierarchy.

1. Select the Receiver you are applying the data source setting to.
2. Select Receiver properties.
3. From the Receiver Properties listing, select “Data Sources”.
4. Select “Add Data Source”.
   OR
1. Select the Receiver you are applying the data source setting to.
2. After selecting the Receiver, select the “Add Data Source” icon.

Parent Data Source Screen Settings

1. Data Source Vendor – Check Point
2. Data Source Model – Check Point (ASP)
3. Data Format – Default
4. Data Retrieval – Default
5. Name – user-defined name of the CMA
6. IP Address – The IP address of the CMA
7. Event Collection Type – Select Audit and Log events.
8. Port – 18184 (Default)

   Steps 9-12 are only needed if authentication and or encryption are being used.

9. Use Authentication – Select depending on the setup in 3.1.1
10. Application Name – Name of OPSEC Application create in Step 3 of 3.1.2
11. Activation Key – One-time password created in Step 8 of 3.1.2
12. Use Encryption – Select if using encryption.
13. Options – Advanced settings leave default unless having connection issues.
14. Connect – Tests the connection to the OPSEC LEA service and pulls the certificate.

After Parent is successfully added create the child data sources CLMs, Firewalls, and Secondary CMAs.

1. Select the parent data source from the Receiver Properties Data Sources screen
2. Select “Add Child Data Source”.
   OR
3. Select the Parent data source from the device Tree.
4. Select the “Add Data Source” icon.

Child Data Source Screen Settings Log server / CLM and Secondary SMS / CMA

1. Name – user-defined name of the CLM
2. IP Address – IP address of the CLM
3. Device Type – Log Server / CLM or Secondary SMS / CMA
4. Event Collection Type – Select Audit and Log events.
5. Parent Report Console – The user-defined name of the CMA that the CLM is managed by. (Pre selected if creating a child data source.)
6. Distinguished Name – DN of CLM from step 3 of 3.1.3

Child Data Source Screen Settings Security Device (Firewall)

1. Name – user-defined name of the Security Device
2. IP Address – IP address of the Security Device
3. Device Type – Security Device
4. Parent Report Console – The user-defined name of the CMA that the CLM is managed by. (Pre selected if creating a child data source.)

# 4 Appendix A - Troubleshooting

- If a data source is not receiving events, verify that the data source settings have been written out and that policy has been rolled out to the Receiver.
- If connection test fails verify CMA IP address.
- If connection test fails verify application name and one-time password are correct
- If using encryption and connection test fails change encryption from the options button until connection succeeds.
- If connection test fails Re-initialize trust in the Check Point user interface