CHECK POINT

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

This integration is not remote capable.

Update Check Point

Check Point requires several initial configuration steps. For help completing the configuration, please review Check Point's documentation and contact their support team as necessary.

Prerequisites

Before starting the update, gather this information:

- Identify your Check Point version.
- Determine where the logs are being sent (Check Point Management or to a separate log server).
- Download the Check Point `opsec_pull_cert` utility. You can find this utility on the Check Point Support Center site.

TO CONFIGURE CHECK POINT (OVERVIEW)

1. Locate and read the Check Point OPSEC LEA documentation. You can find this on the Check Point Support Center site.
2. Download the `OPSEC SDK 6.1 tar.gz` file.
3. Create the OPSEC application.
    a. Use the Check Point SmartConsole or the desired CMA/Domain on the Provider.
    b. Name the new OPSEC application ***VerodinLEA***.

    You can use any name, but VerodinLEA is recommended by convention.

    The Security Validation integration with Check Point currently only supports the sslca auth method.

    c. Consult the Check Point documentation for more information.
4. Create an OPSEC application certificate in the Check Point SmartConsole using the command line.
    a. Run the following command in the Check Point `opsec_pull_cert` utility with the correct information from the customer:
    `opsec_pull_cert -h <smartcenter ip> -n <LEA Opsec Application Name> -p <activation key> -o c:\cert\opsec.p12`
    b. Capture the one-time password you enter; this will be used when you create an OPSEC LEA connection and pull the p12 authentication file.

> The password must not include any of the following special characters: exclamation (!), circumflex accent (^), tilde (~), grave accent (`), quotation ("), or apostrophe (').

c. Consult the Check Point documentation for more information.

5. After the OPSEC application initializes, note the opsec_sic_name that is generated. You will need this opsec_sic_name and the LEA server's opsec_sic_name.
   a. The Server OPSEC SIC name and the OPSEC Sic name are tied to the certificate created in step 4 above.
   b. You can also get the OPSEC SIC name and LEA Server OPSEC SIC name by running this command in Expert mode from the management server. Look for the SmartConsole SIC ID in the results to get the correct name: `cpca_client lscert -stat Valid -kind SIC`
6. Install the database.
   a. In the SmartConsole, under Policy, install the database for your Management Server.
   b. Consult the Check Point documentation for more information.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Ensure that you are running CentOS 7.0 or newer.
2. Have the OPSEC SDK Dependency file (Check_Point_OPSEC_SDK_6.1_linux50.tar.gz). See Check Point's knowledge base for more information.
3. Have an active, configured OPSEC LEA Application for use with the Validation Platform.
   a. Obtain OPSEC authentication file.
   b. Identify the LEA Server IP and Port (this defaults to 18184).
   c. Identify the OPSEC SIC and LEA Server OPSEC SIC names you noted in Step 5 above.

Configuration

TO ADD THE CHECK POINT INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Check Point**.
3. Browse for and select the OPSEC SDK 6.1 tar.gz file. When selected, the file will immediately start uploading.
4. Enter **IP**, **Port**, **OPSEC SIC Name**, and **LEA Server OPSEC SIC Name**. See **Check Point Firewall Integration (https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d8c9cba0017c2f7ddf/n/checkpoint.png)**
   - In the **OPSEC SIC Name** field, enter the OPSEC Application name you created in Step 3 in **To configure Check Point (overview)**
   - In the **LEA Server OPSEC SIC Name** field, enter the SmartConsole SID ID you noted in Step 5 in **To configure Check Point (overview)**.
5. Browse for and select the OPSEC Key (.p12 authentication) file.
6. Expand **Advanced options**.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Assign a **Name**.
9. (Optional) Choose **Yes** to save suspicious events.
10. Click **Submit**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d8c9cba0017c2f7ddf/n/checkpoint.png)

Check Point Firewall Integration

Verify connectivity

TO VERIFY CONNECTIVITY TO CHECK POINT

Click **Test** to verify that the Director can communicate with the Check Point host using the provided setup information.