

CHECKPOINT INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Checkpoint to test the efficacy and configuration of the security control using Security Validation jobs.

API Calls

| API | Usage |
|---------------------------------|------------------------------|
| <code>/web_api/login</code> | Authentication |
| <code>/web_api/logout</code> | End an authenticated session |
| <code>/web_api/show-logs</code> | Query events to return |

Supported Versions

Checkpoint version R80 and above

Before You Begin

To configure this integration, you need:


- The hostname of your Checkpoint instance
- One of the following:
 - A valid username and password for a user with permissions to use the API endpoints described in the previous step
 - An Api Key for an administrator account

To generate an API Key

1. Login to the **Checkpoint SmartConsole**, click **Manage & Settings > Permissions & Administrators > Administrators**.
2. Click the **New** icon in the top menu.
3. In the **New Administrator** window, give the administrator a **name** and select **API Key** as the **Authentication Method**.
4. Click **Generate API key**.
5. From the new API key window, click **Copy key to Clipboard**, and paste it to a safe location for use in the integration configuration.
6. Click **OK**.
7. Publish the SmartConsole session.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Checkpoint**.

 You can add this as either a Direct or Remote Integration.

3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (<https://docs.mandiant.com/home/msv-proxy-rules>).
5. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Https** or **Http**).
6. Enter the **Host** for the Checkpoint instance.
7. Enter a **Port** value. The default is **443**.

8. Enter the **Domain** value for the Checkpoint instance.
9. Select a **CheckpointAuthMethod** and then choose an option:
 - If you chose **Basic**, enter the Username and Password for the account with permissions to use the API endpoints.
 - If you chose **Apikey**, enter the **Api Key** that you generated.
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
12. Optional: Add any **Log Servers**, if needed.
13. Optional: Modify **Queries**, as needed. A default **IP Query** is provided.
14. Optional: Select an option from the drop-down if you want to change the **CheckpointTimeFrame**.
15. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **100**.
16. Optional: Modify the **Field Map** values, as necessary.



- Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
- When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

17. Optional: Expand **Advanced options** and update the information as necessary.
 - a. Update **Query Time** and **Delay Time**.



The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.



If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

- b. Update **Query Interval** (seconds).
- c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
- d. Modify the **Correlation Query Interval**, if necessary (minutes).
- e. Select **Discover network devices automatically**, the default and recommended option.



If unselected, reported events won't include product information for any matching network security technology.

- f. Select **Save Suspicious Events**.
- g. Modify the **Event Time Adjustment** (seconds). The default is **0**.

- h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

18. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click **:** > **Test** to verify that:
 - The Director can communicate with the integration host on the port and protocol specified.
 - The integration credentials are valid and working.

For more information on setting up queries, see [Manage Integrations \(https://docs.mandiant.com/home/msv-managing-integrations\)](https://docs.mandiant.com/home/msv-managing-integrations).