SaiFlow and Check Point - Integration Guide

Products Integration Overview

About SaiFlow’s Cybersecurity Platform

SaiFlow's SaaS-based cybersecurity platform, tailored for the distributed nature of modern energy networks, combines energy telemetry streams with network and communication data for comprehensive contextual cyber incident detection, full energy network and asset observability, energy-oriented anomaly detection, configuration and vulnerability management, enabling the users to monitor, detect, and swiftly mitigate cyber incidents across the energy networks.

About Check Point and SaiFlow Integration

Check Point and SaiFlow have partnered to deliver a cutting-edge cybersecurity solution for EV charging hubs and energy networks. This integration combines contextualized security, advanced detection, enhanced observability, and proactive IoT protection to address the unique challenges of modern, distributed energy systems.
SaiFlow’s SaaS-based platform leverages energy telemetry and network data to detect cyber events and assess risks comprehensively. Its native support for industry standards and protocols ensures seamless integration into energy networks. Complementing this, Check Point’s next-generation firewalls (NGFWs) and Check Point’s IoT Protect proactive IoT security provides dedicated firewall policies, enforced authentication and encryption, enhanced network visibility, and enable dynamic protection. Together, the solution delivers unparalleled security tailored to the demands of EV charging and distributed energy infrastructures.

Integration Uses Cases

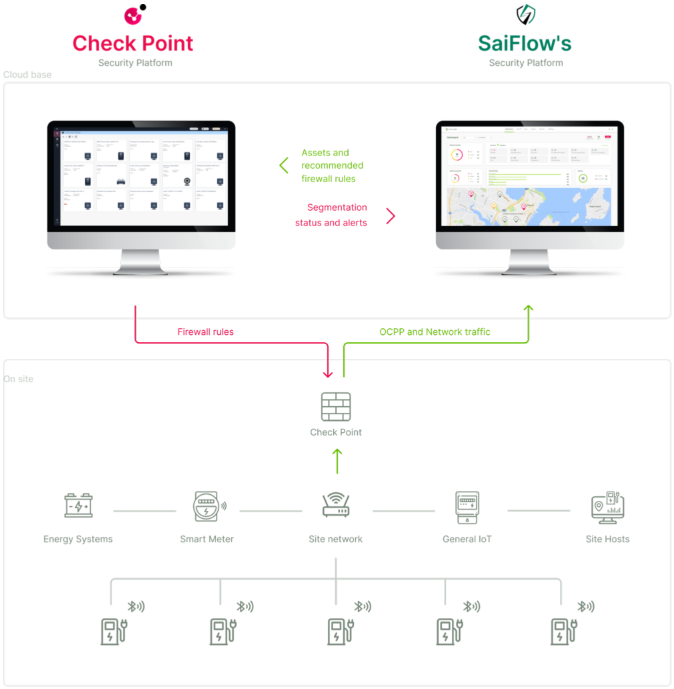
- **Full Visibility Into the EV Charging and Energy Network Structure:** SaiFlow’s platform maps and discovers all assets across the entire energy and charging network. The platform automatically pulls all Security Gateway information, parses the existing network policies, and builds a comprehensive network map the entire energy infrastructure. All energy assets discovered by SaiFlow’s platform are automatically synced with Check Point Quantum IoT Protect, supporting multi-site environments through Check Point Infinity Portal.

- **Automated Firewall Policies Tailored To Energy Networks and Charging Site:** Utilizing SaiFlow's deep know-how in EV charging and distributed energy networks, SaiFlow’s platform builds tailored firewall policies, based on known and required services for each asset in the energy network, including needed connections to the different SaaS and management platforms. The recommended policies can be automatically streamlined and enforced via Check Point's Security Gateways with Quantum IoT Protect on the different charging sites to strengthen the overall network resiliency.

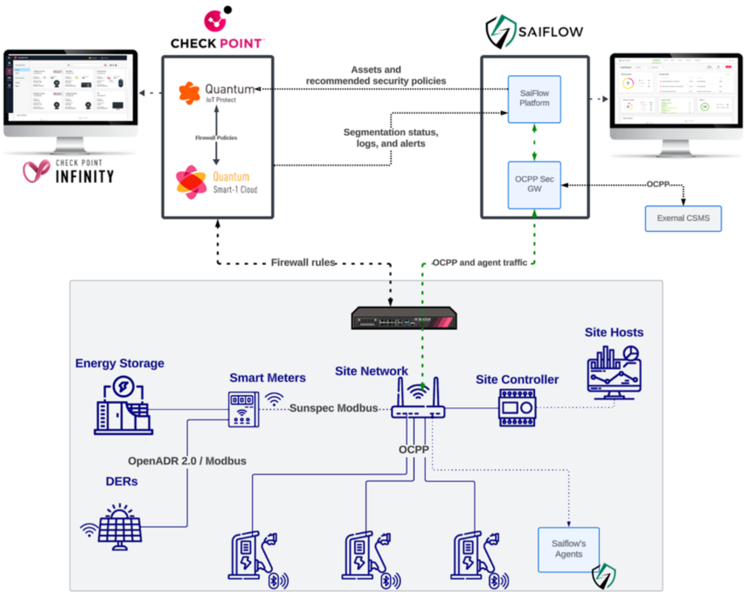
- **Comprehensive Detection & Response to Threats Under a Unified System:** SaiFlow’s platform retrieves, in real-time, all network logs and FW dropped packets and sessions from Check Point’s Security Gateways located in the EV charging sites. The platform alerts in real time on possible cyber-attacks and on any suspicious activities and unrecognized outbound traffic. All logs and alerts are visible in SaiFlow’s platform to further investigate cyber incidents. All events and alerts can be automatically streamlined from SaiFlow’s Platform to **Check Point XDR**.

Integration Diagram

General integration Diagram



Detailed Integration Diagram



* SaiFlow’s network agent is an optional component.

Requirements

SaiFlow's Platform:

- Verify that the Infinity Portal and Check Point Quantum IoT Protected are accessible to SaiFlow's cloud environment.

Check Point:

- Check Point Firewall with Quantum IoT Protect enabled.
- A user with permission to add a new event forwarding destination.

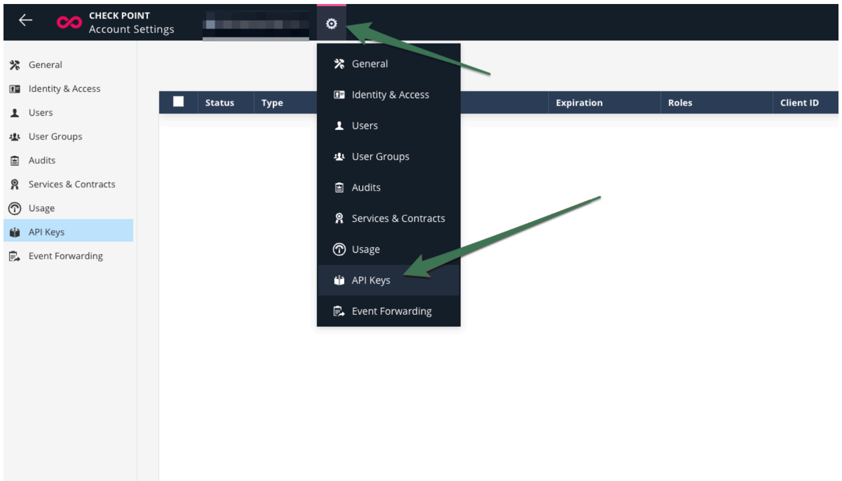
Check Point Configuration

<u>To connect with Check Point Firewalls, you first need to get API credentials, please follow the following steps:</u>

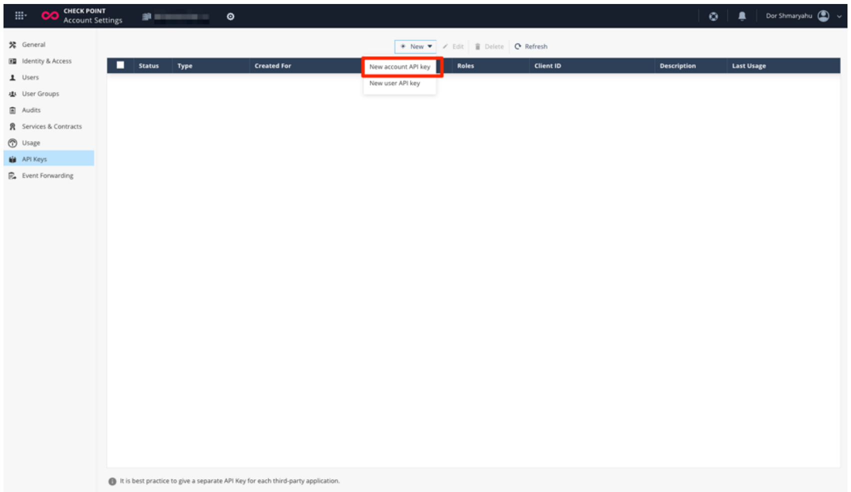
1. Go to https://portal.checkpoint.com/ and create an account if you don't have one

2. Create API Key for IoT Protect:

   a. Go to Account Settings -> API Keys

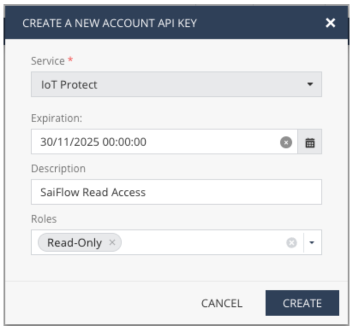


   b. Create a *New account API Key*



It is best practice to give a separate API Key for each third-party application.

c. Select the IoT Protect service with "Read Only" permissions.



CREATE A NEW ACCOUNT API KEY

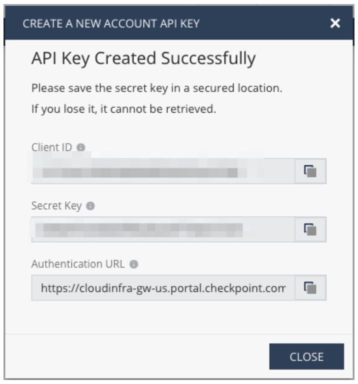
Service *: IoT Protect

Expiration: 30/11/2025 00:00:00

Description: SaiFlow Read Access

Roles: Read-Only

d. Copy the Client ID and Secret Key to a notepad to add it in SaiFlow's integration form.



CREATE A NEW ACCOUNT API KEY

API Key Created Successfully

Please save the secret key in a secured location.
If you lose it, it cannot be retrieved.

Client ID: [redacted]

Secret Key: [redacted]

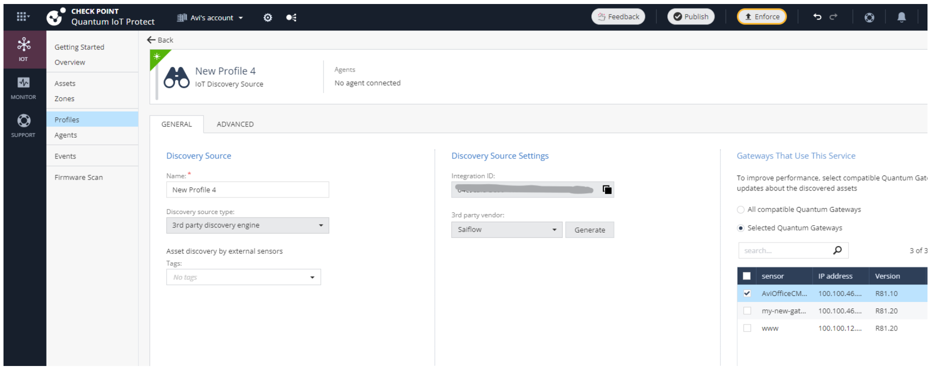
Authentication URL: https://cloudinfra-gw-us.portal.checkpoint.com

3. Click the application drawer icon (▦) and select IoT Protect

4. Click IoT topic on the right side, and then 'Profiles' tab

5. Click on the new icon (✳ ▾) to add a new profile

6. Select:
   a. Discovery source type: 3rd party discovery
   b. 3rd Party vendor: Saiflow
   c. Select the gateways on the right side, on which you wish to enforce IoT policies



New Profile 4
IoT Discovery Source

Agents: No agent connected

Discovery Source

Name: * New Profile 4

Discovery source type: 3rd party discovery engine

Asset discovery by external sensors

Tags: No tags

Discovery Source Settings

Integration ID: [redacted]

3rd party vendor: Saiflow

Generate

Gateways That Use This Service

To improve performance, select compatible Quantum Gat
updates about the discovered assets

○ All compatible Quantum Gateways

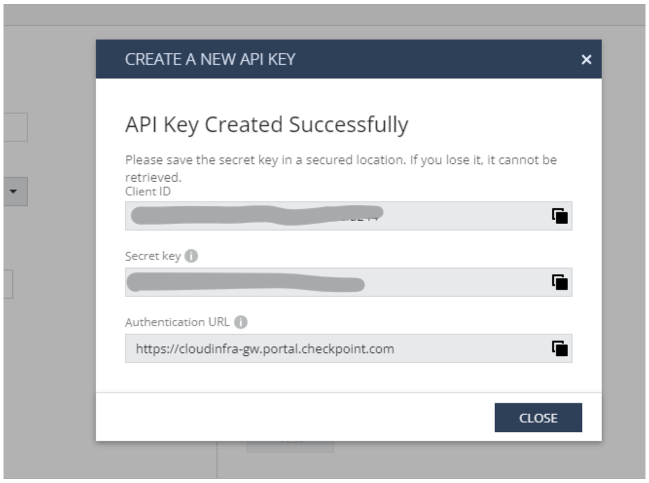
● Selected Quantum Gateways

search... 3 of 3

☐	sensor	IP address	Version
☑	AviOfficeCM...	100.100.46....	R81.10
☐	my-new-gat...	100.100.46....	R81.20
☐	www	100.100.12....	R81.20

7. Click **Generate**

8. Copy the Client ID, Secret Key and URL to a notepad to add it in SaiFlow's integration form.



CREATE A NEW API KEY ×

API Key Created Successfully

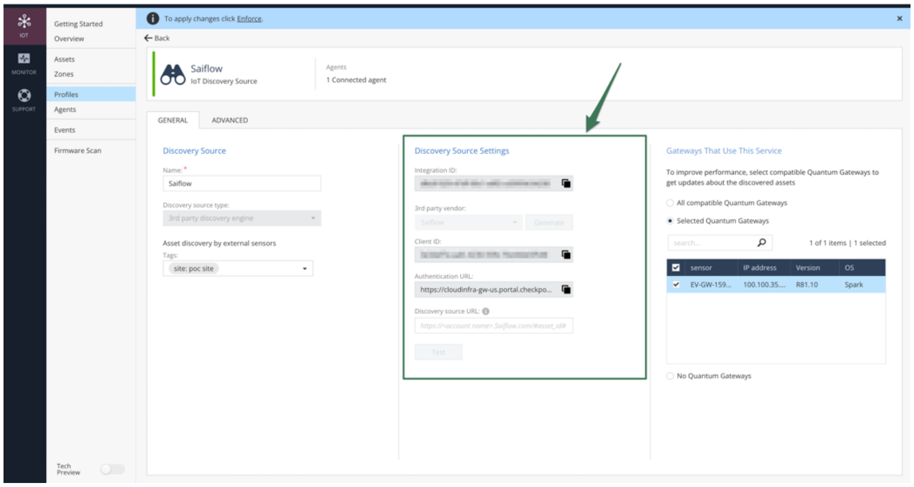
Please save the secret key in a secured location. If you lose it, it cannot be retrieved.

Client ID: [redacted]

Secret key: [redacted]

Authentication URL: https://cloudinfra-gw.portal.checkpoint.com

9. Copy the Integration ID to a notepad.



To apply changes click Enforce.

Saiflow
IoT Discovery Source

Agents: 1 Connected agent

Discovery Source

Name: * Saiflow

Discovery source type: 3rd party discovery engine

Asset discovery by external sensors

Tags: site: poc site

Discovery Source Settings

Integration ID: [redacted]

3rd party vendor: Saiflow

Client ID: [redacted]

Authentication URL: https://cloudinfra-gw-us.portal.checkpo...

Discovery source URL: https://<account name>.Saiflow.com/#asset_id#

Gateways That Use This Service

To improve performance, select compatible Quantum Gateways to get updates about the discovered assets

○ All compatible Quantum Gateways

● Selected Quantum Gateways

search... 1 of 1 items | 1 selected

☑	sensor	IP address	Version	OS
✓	EV-GW-159...	100.100.35....	R81.10	Spark

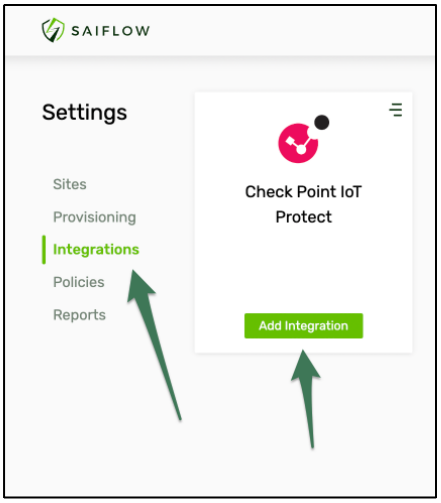
○ No Quantum Gateways

10. Follow the "event forwarder admin guide" to add a new Syslog forwarding destination to SaiFlow.
    a. Host: lf.saiflow.com
    b. Port: 514
    c. Client Certificate: upload the downloaded certificate from SaiFlow (*sf-client-certificate-for-secure-syslog.pem)*.
    d. Certificate Authority (CA) Certificate: upload the downloaded certificate from SaiFlow (*sf-sub-ca-certificate.pem)*.

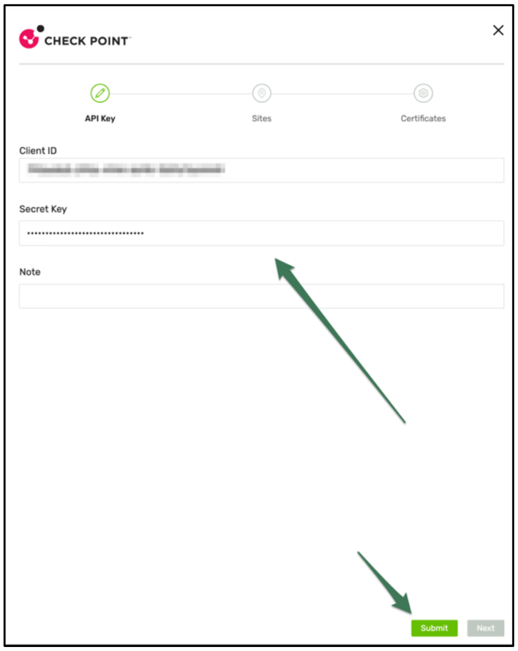
SaiFlow Platform Configuration

To connect with Check Point Firewalls and Quantum IoT Protect, please follow the following steps:

1. On the SaiFlow Platform - Go to Settings -> Integrations -> Check Point IoT Protect and click Add Integration.



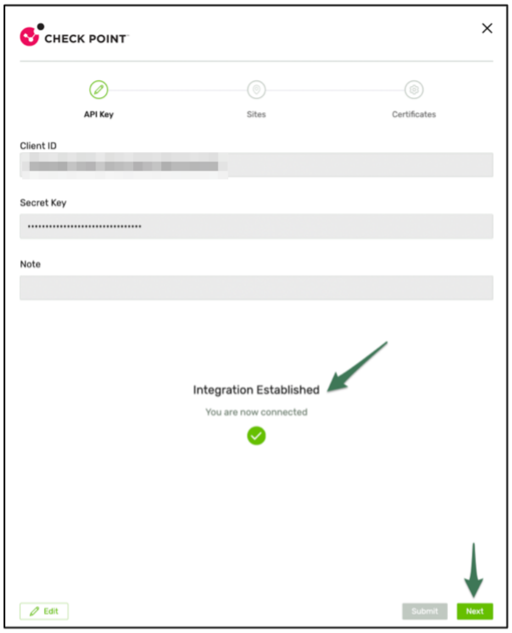
2. In the integration form, fill in the API Key details generated by Check Point.
   a. Add the API Client ID.
   b. Add the API Secret.
   c. Click Submit.



Client ID
[redacted]

Secret Key
••••••••••••••••••••••••••••••••••

Note



Client ID
[redacted]

Secret Key
••••••••••••••••••••••••••••••••••

Note

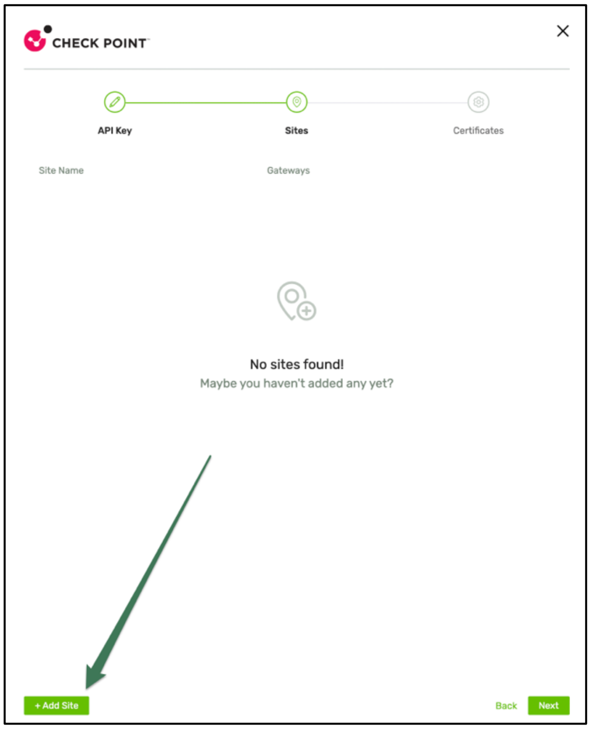
Integration Established

You are now connected

   d. Once the connection established, click ***Next***.

3. Add the relevant charging sites that contain the Check Point Firewalls configured with the IoT Protect and fill in the relevant API keys.

   a. Click the ***+ Add Site***

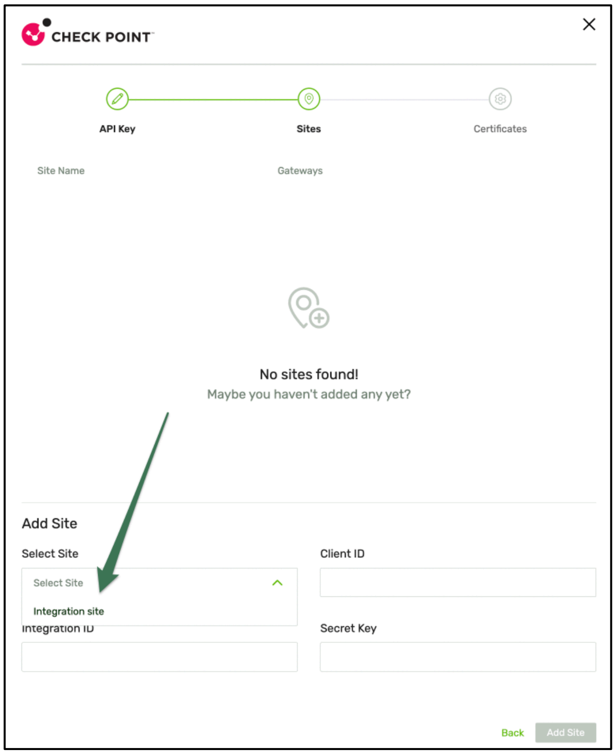


CHECK POINT

No sites found!

Maybe you haven't added any yet?

   b. Select the relevant site from the sites list



CHECK POINT

No sites found!

Maybe you haven't added any yet?

Add Site

Select Site: Select Site

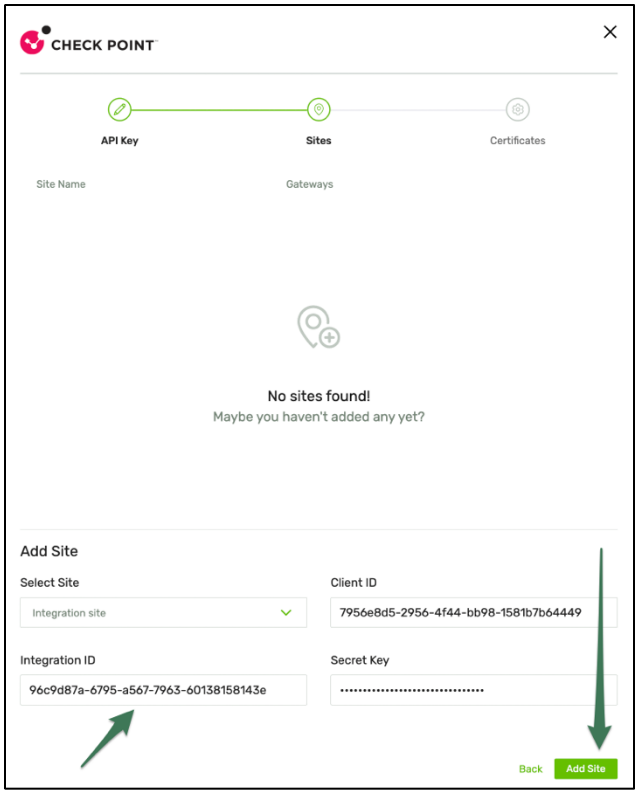
Integration site

Integration ID

Client ID

Secret Key

c. Add the Client ID, Integration ID, and Secret Key generated by Check Point, and click the ***Add Site*** button.



No sites found!
Maybe you haven't added any yet?

Add Site

Select Site: Integration site

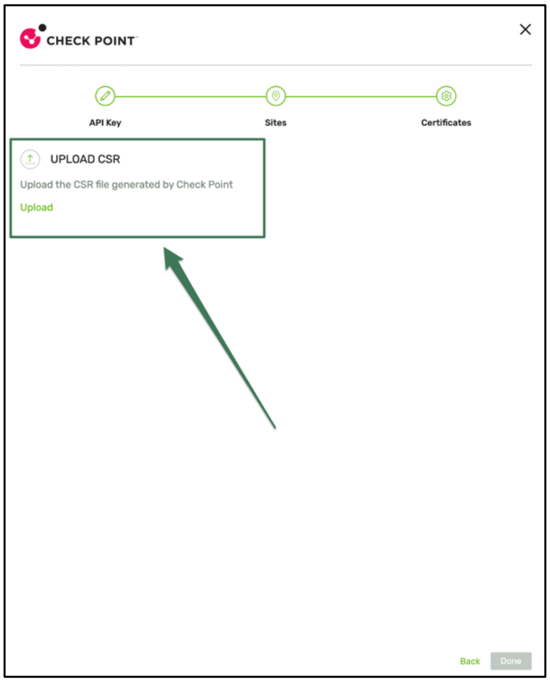
Client ID: 7956e8d5-2956-4f44-bb98-1581b7b64449

Integration ID: 96c9d87a-6795-a567-7963-60138158143e

Secret Key: ••••••••••••••••••••••••••••••••

4. After the addition of all relevant sites, click ***Next.***

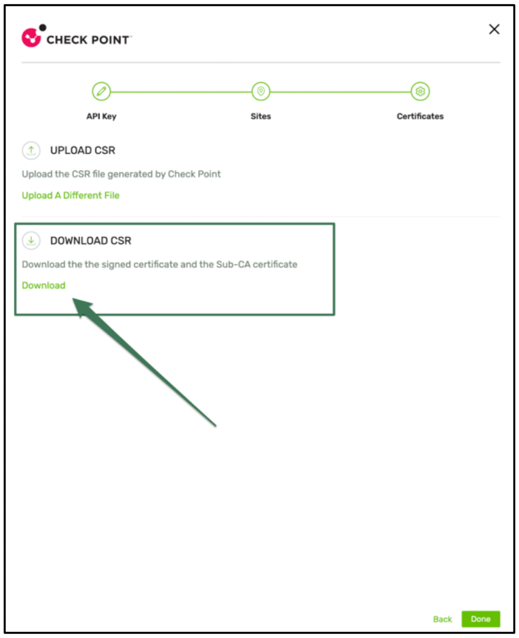
5. Upload the cp_client.csr Certificate Signing Request file to SaiFlow's platform.



UPLOAD CSR

Upload the CSR file generated by Check Point

6. Click ***Download*** to download the required certificates (file name: *certificates.zip*)
   a. After downloading the certificates, open the zip file and upload the certificates to Check Point.
   b. CA Authority Certificate - *sf-sub-ca-certificate.pem*
   c. Client Certificate - *sf-client-certificate-for-secure-syslog.pem*



UPLOAD CSR

Upload the CSR file generated by Check Point

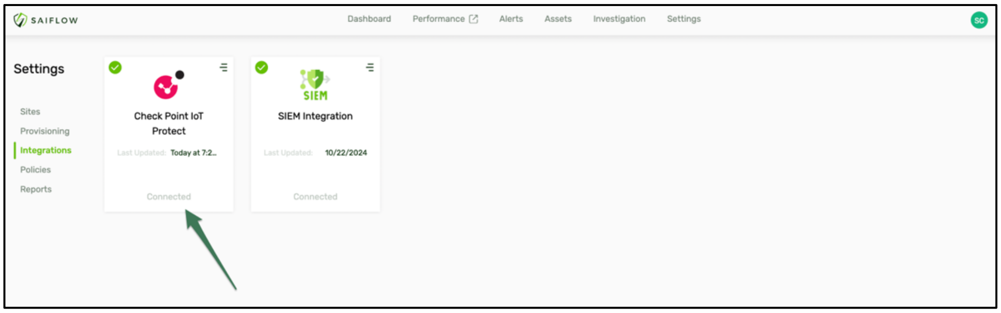
Upload A Different File

DOWNLOAD CSR

Download the the signed certificate and the Sub-CA certificate

Download

7. Click ***Done*** to finish the setting.



Check Point IoT Protect

Last Updated: Today at 7:2...

Connected

SIEM Integration

Last Updated: 10/22/2024

Connected