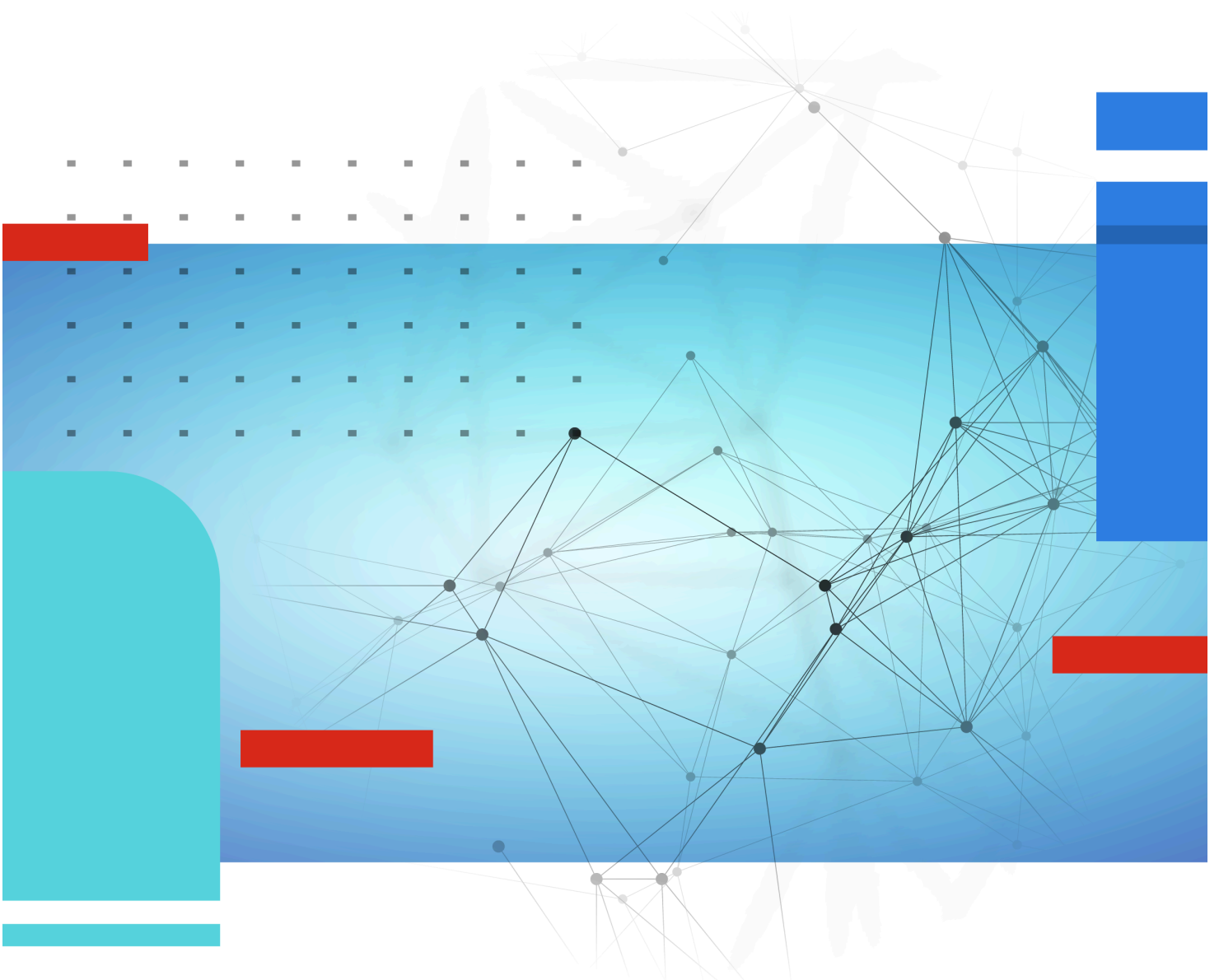




# FortiCASB-SSPM Application Connector

CrowdStrike Connector



# CrowdStrike Connector

---



## Category

---

- IT & Security

## Connection Method

---

- API Token
- Service Account

## Supported SSOs for connection

---

- Okta
- Azure
- OneLogin
- Google
- JumpCloud

## Data Collected

---

- Misconfigurations
- 3rd Party Applications
- Tokens
- Identities
- Activities

## Integration Guide

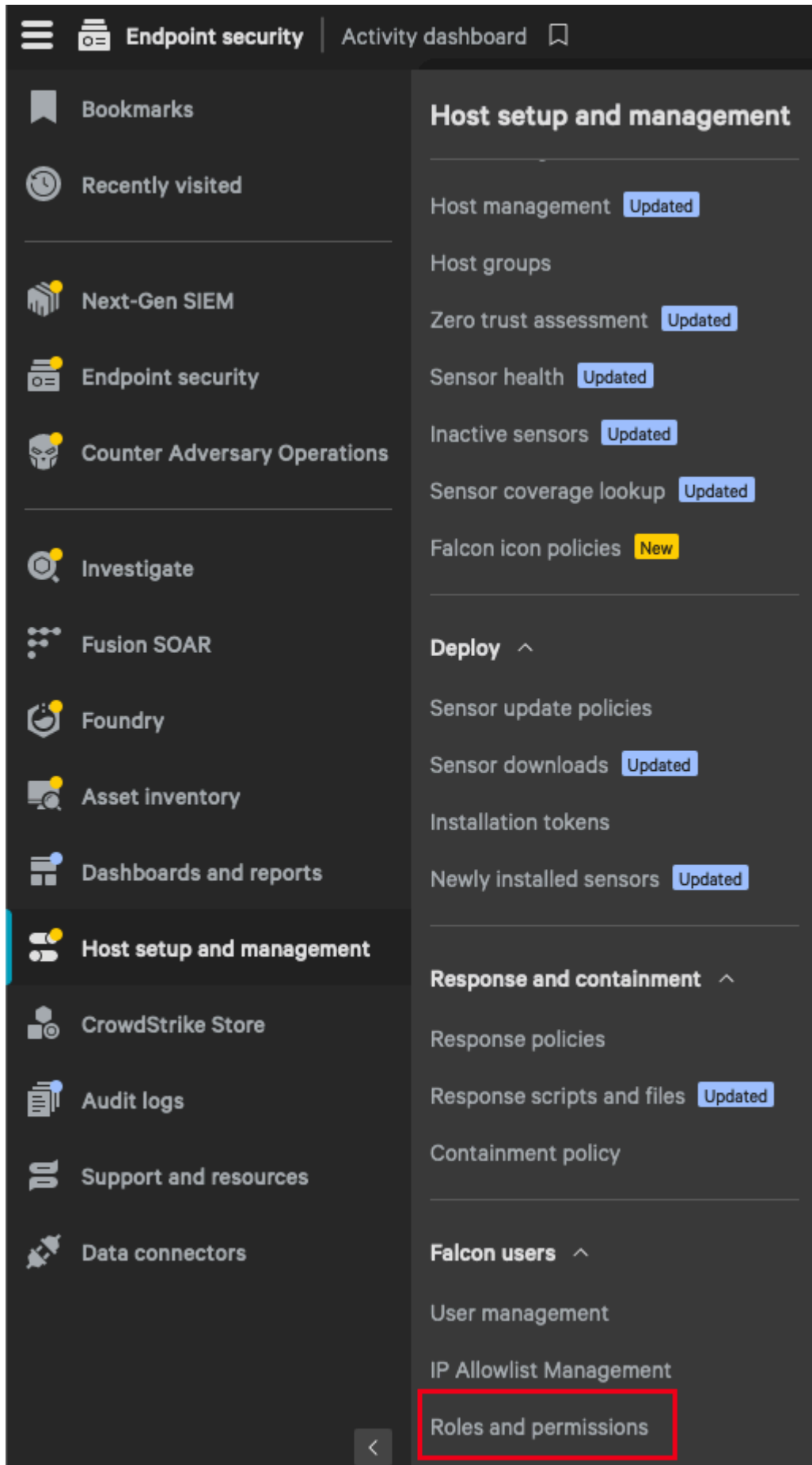
---

### Intro

Use this guide to add CrowdStrike as a secured SaaS application in FortiCASB-SSPM SaaS Security platform.

### Part A: Service Account Creation

1. Navigate to "Roles and Permissions"



2. Create Role:

Roles (30)

Create role

Role Name	Description	Role Type	Permissions	Users	
App Developer	Roles for App Developer	Default	43	1	⋮
Custom IOAs Manager	Create, edit, and manage custom IOA rules, rule g...	Default	22	0	⋮
Dashboard Admin	Create, edit, manage, and delete dashboards. This...	Default	8	3	⋮

3. See the following example:

## Create role ✕

Role name

Suridata SSPM Access

Description (optional)

Set of minimal permissions for Suridata's service account

Cancel
Create role

4. Click on Edit permissions under each group name, mark the relevant permissions and click "Save".

Example:

**API Client Management** (0/6) ^ Collapse

Manage API Clients

Permissions Cancel Save

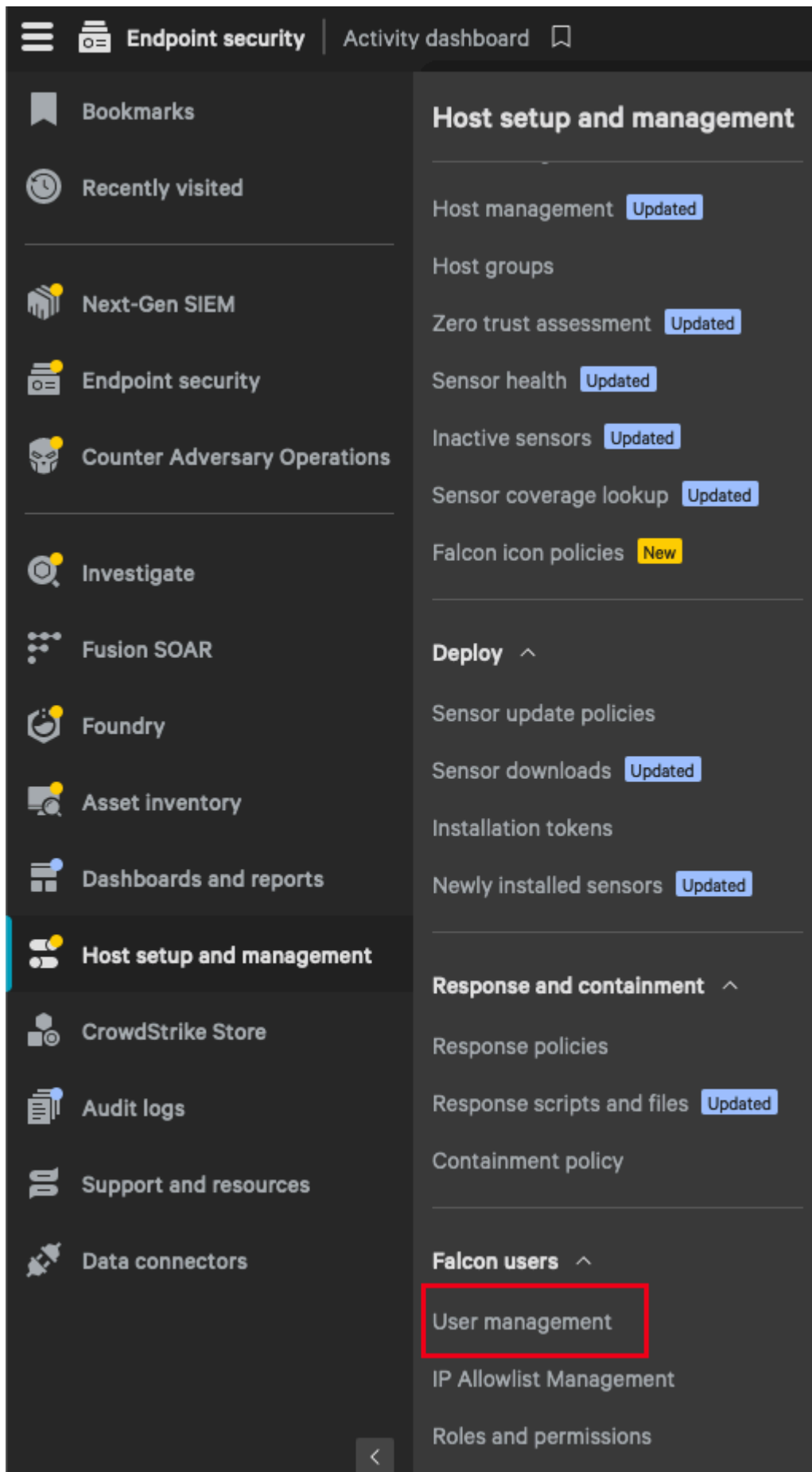
Name	Description	Status
<input type="checkbox"/> Create API client	Create an API client	● Disabled
<input type="checkbox"/> Delete API client	Delete an API client	● Disabled
<input type="checkbox"/> Reset API client secret	Reset an API Clients secret. WARNING! this action is very powerful. (Note - ...	● Disabled
<input type="checkbox"/> Update API client	Update an existing API client (except the client secret)	● Disabled
<input checked="" type="checkbox"/> View API client IDs	View the list of all API client IDs	● Disabled
<input checked="" type="checkbox"/> View API client details	View details for all API clients	● Disabled

5. Do the same for the flowing groups:

Group	Scope
API Client Management	View API client IDs
API Client Management	View API client details
Manage All Users	List assignable roles
Manage All Users	List host group assignments
Manage All Users	List user roles
Manage All Users	View host group assignments

Group	Scope
Manage All Users	View user activity metadata
Manage All Users	View user details
Manage All Users	View user details (identities)
Manage All Users	View users
Manage Current Customer	Read customer access control settings
Response Policies and Settings	View Response policies
Role Management	Permission - List
Role Management	Permission - View
Role Management	Permission Group - List
Role Management	Permission Group - View
Role Management	Role Details
Role Management	Role Permission - List

6. Navigate to User management:



7. Click on Create User

8. Fill in the details and in the role, select the one you just created:

The email should be an email that is associated with the Crowdstrike interface

## Create user



User email

EmailAccount@client.com

First name

Suridata

Last name

SSPM service account

Roles

Suridata SSPM Access ⓘ × Type to search

Host groups

All hosts ×

If left blank, this user won't have access to any hosts

Cancel

Save

9. You will get an activation link from CrowdStrike. Click on it and continue the account registration:

## Activation Link

---

### Hello!

Use this one-time link to activate your Falcon account and set your password. Next, you'll set up **two-factor authentication**. Use Chrome, the supported browser.

#### Activate My Falcon Account

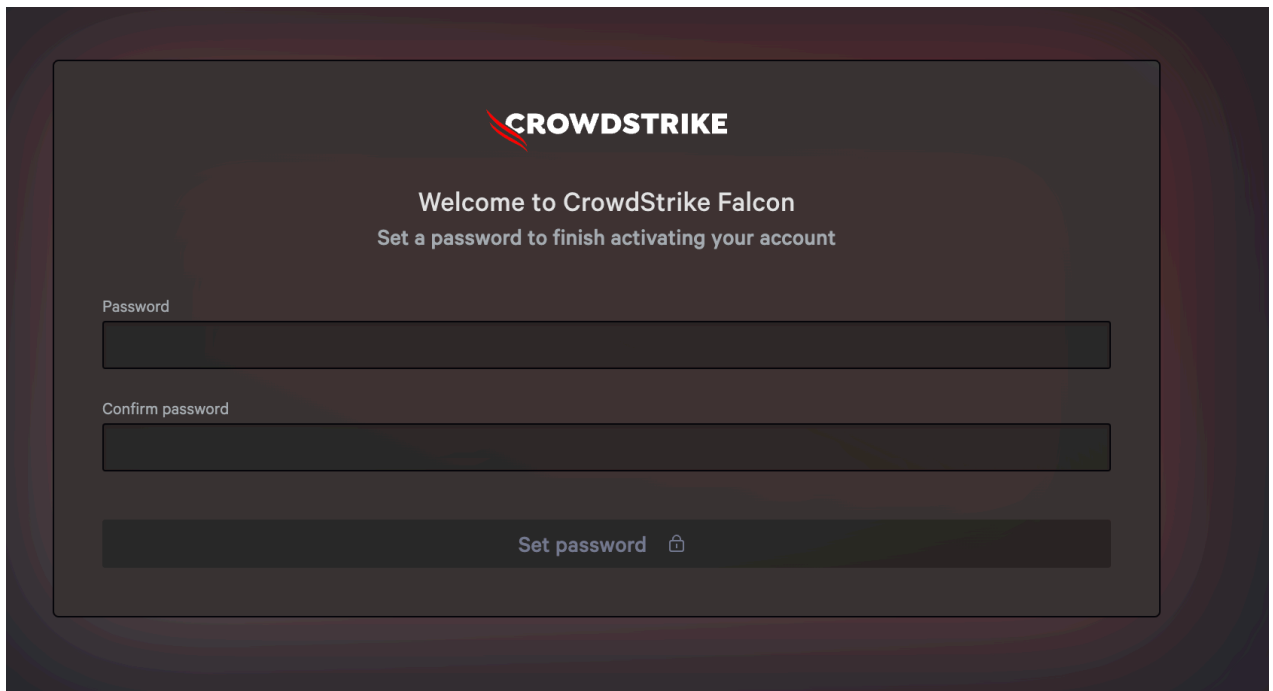


Please note, the activation link expires in 24 hours.

If the activation link has expired, click the activate account link, then click **Resend Link** and enter the email address for your account. You'll be sent a link to reset your password, which will activate your account.

If you have questions, contact [support@crowdstrike.com](mailto:support@crowdstrike.com).

### 10. Set a complex password:

The screenshot shows a dark-themed web interface for setting a password. At the top, the CrowdStrike logo is displayed. Below it, the text reads "Welcome to CrowdStrike Falcon" and "Set a password to finish activating your account". There are two input fields: "Password" and "Confirm password". At the bottom, there is a "Set password" button with a lock icon.

### 11. When setting the MFA, first copy and save the activation key (this is the TOTP secret)

## Falcon 2FA set up

### 1. Download authentication app

Download an authentication app that supports time-based one time passwords (TOTP)

### 2. Add account

Using your authentication app, scan the QR code or enter the manual activation key:



You have 5 minutes to complete Falcon MFA set up after entering your manual activation key or scanning the QR code in your authentication app

### 3. Enter verification code

Enter 6-digit verification code from the app

 - 

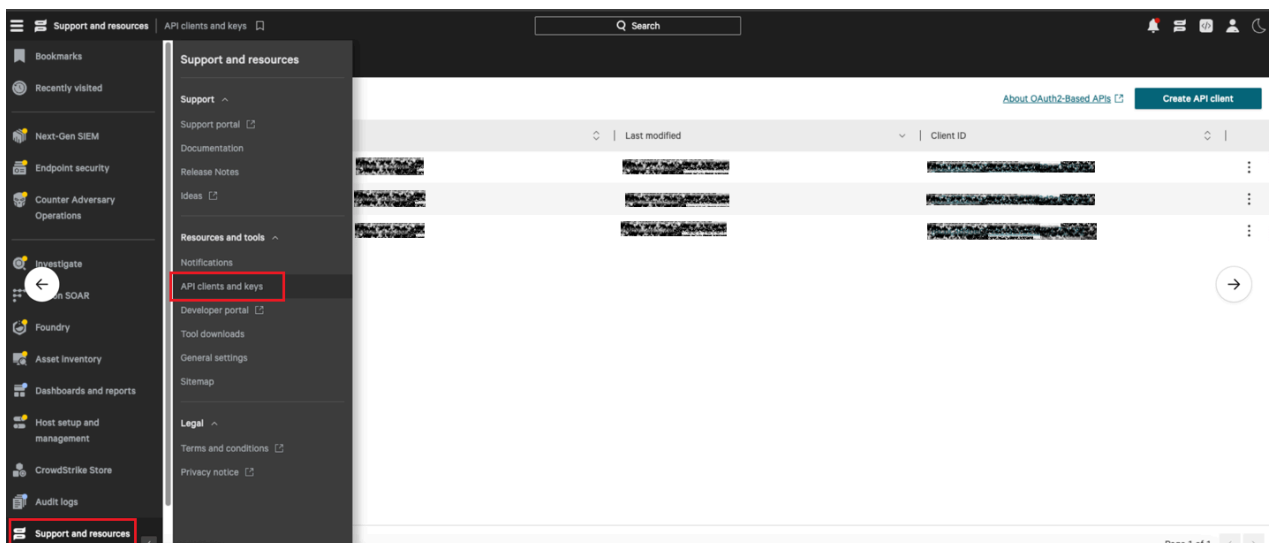
Cancel

Set up 2FA

12. Complete the MFA registration

## Part B: Create an Access Token

1. Sign in to your CrowdStrike account.
2. Navigate to Support.
3. Navigate to API Clients and Keys:



4. Click on: "Create API client"

---



**Create API client**

5. A window will open.

Fill in the Client Name, Description and grant the following scopes (Read):

- Scheduled Reports
- User Management
- Firewall Management
- Installation tokens
- Hosts

Example 1:

# Create API client



Client name

Suridata

8 / 50

Description

[Empty text area for description]

0 / 255

Scope	Read	Write
Real time response	<input type="checkbox"/>	<input type="checkbox"/>
Response policies	<input type="checkbox"/>	<input type="checkbox"/>
Scheduled Reports	<input checked="" type="checkbox"/>	
IOA Exclusions	<input type="checkbox"/>	<input type="checkbox"/>
Sensor Download	<input type="checkbox"/>	

**Cancel** **Create**

Example 2:

### Edit API client ✕

Client name  
 4 / 50

Description  
0 / 255

Scope	Read	Write
Device control policies	<input type="checkbox"/>	<input type="checkbox"/>
Hosts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Actors (Falcon Intelligen...	<input type="checkbox"/>	
Reports (Falcon Intellige...	<input type="checkbox"/>	
Host groups	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Update client details

6. Click 'Create'.

7. **Copy the Client ID and Secret** (you will need it for the connection to FortiCASB-SSPM).

## API client created



Copy this secret to a safe location. This is the only time we'll show it. If lost, it must be reset and a new secret generated.

Client ID

[Redacted]



Secret

[Redacted]



Base URL

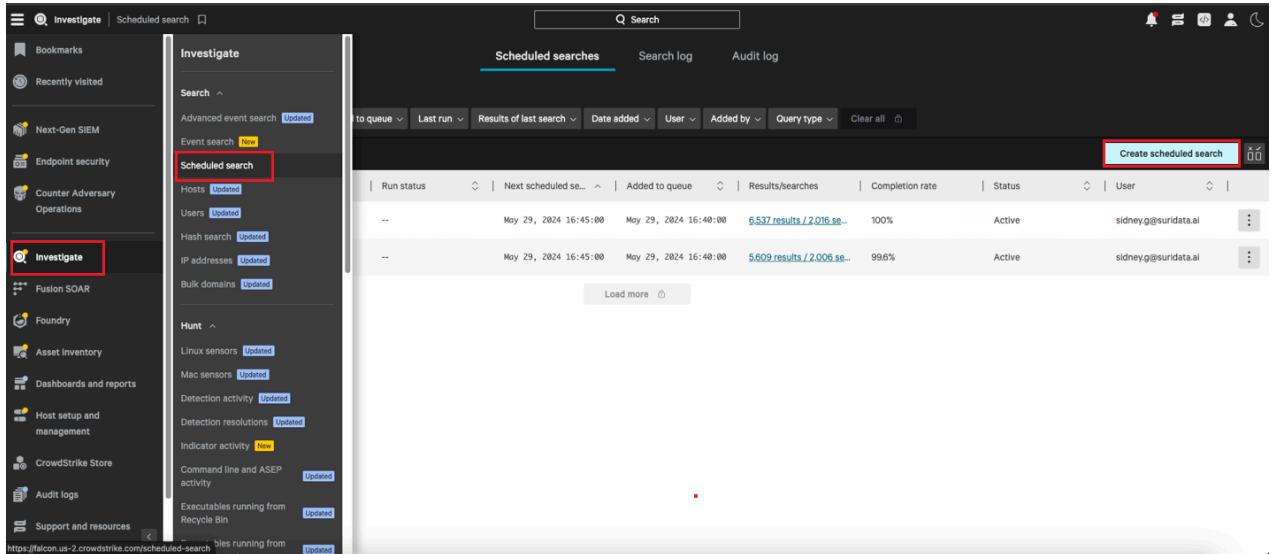
[Redacted]



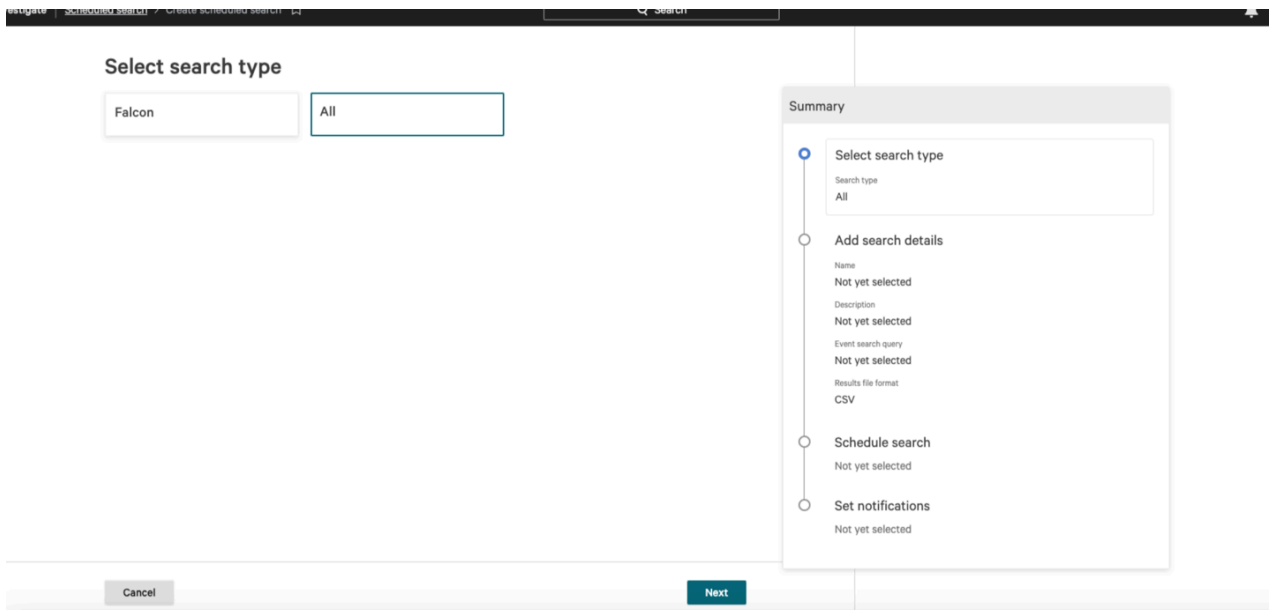
Done

## Part C: Setting Up a Scheduled Search

1. Go to 'Investigate'.
2. Go to 'Schedule search'.
3. Click on "Create Scheduled Search".



4. Choose All and click "Next".



5. In the search query, write: "DomainName is not empty".
6. Results file format: JSON and click "Next".

# Add search details

Name

Suridata

Description (recommended)

Search query

[Test query](#) 

DomainName is not empty

Results file format

- CSV
- JSON

7. Set the search frequency to 1 Hour and the Search offset to 0 Hours, and click "Next".

## Search frequency

Run this search every

Day(s)	Hour(s)	Minute(s)
<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>

## Search offset (recommended)

Shift the search window back by

Day(s)	Hour(s)	Minute(s)
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Add an offset time to skip a period immediately previous to the search and look at older, more complete data. Offset time should be equal to or greater than the time between scheduled log uploads.

8. Chose 'None' in the Notification type

## Add notifications

Choose how you want to be notified when the search is completed.

Notification type

None

9. Click on "Schedule search" -your summary should look like this:

## Summary



### Select search type



Search type

All



### Add search details



Name

Suridata

Description

Not yet selected

Event search query

DomainName is not empty

Results file format

JSON



### Schedule search



Search frequency

5m

Start date

May 29, 2024 17:15:00

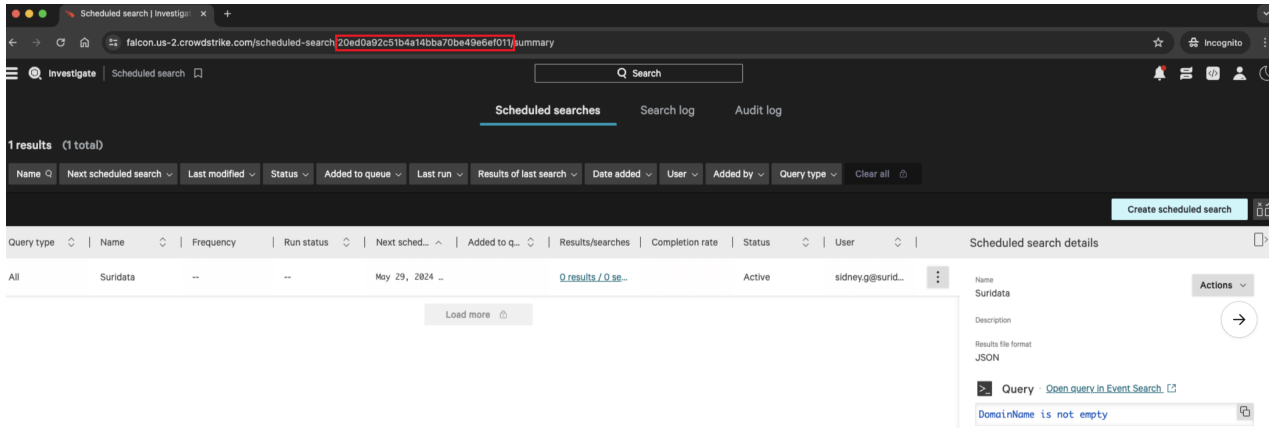


### Set notifications

Not yet selected

10. Click on "Created Search".

11. Copy both the URL itself and the ID (will be referred to as "Scheduled Search ID") from the URL (marked in red), they will also be required in the CrowdStrike settings configuration.



12. If your Base URL is not supported by Auto discovery (for example USGOV1), Copy your Base URL (if it is auto discovered do not enter the base-url field)

See example:

Short name	Base URL	Auto discovery support?
US1	https://api.crowdstrike.com	✔ YES
US2	https://api.us-2.crowdstrike.com	✔ YES
EU1	https://api.eu-1.crowdstrike.com	✔ YES
USGOV1	https://api.laggar.gcw.crowdstrike.com	✘ NO

## Part D: Connect CrowdStrike to the FortiCASB-SSPM Platform

1. Login to FortiCASB-SSPM and navigate to the App Store > Click on CrowdStrike
2. Start by inserting the Client ID and Client Secret (which are mandatory). Insert the API Base Url if necessary
3. For Shadow-SaaS detection, check the box and fill in the "Scheduled Search ID" (please note that to receive user emails, a device management application must also be connected to FortiCASB-SSPM. Examples include Microsoft Intune or JumpCloud)



CrowdStrike



Client ID \*

Client Secret \*

API Base Url

Allow Shadow SaaS Detection

Scheduled Search ID \*


Allow SSPM

Leaving 'Allow SSPM' unchecked will skip to the connection step

[Create External Link](#)

Next


4. For SSPM capabilities (misconfigurations, users and 3rd parties) check the box and fill in the relevant fields in the next step (Username, Password and Login URL are mandatory)

  
**CrowdStrike**

1 — 2 — 3

Select a shared account

Shared Accounts \*

 yam@asdf.com via Okta

Use an application account

SSO Provider

No SSO Provider

Username \*

Password \*

OTP Secret Generate

Save as Shared Account

Login URL \*

[Create External Link](#) Back Next

**Note**

Pay attention - Login URL should be without http:// or https:// and without /login

Example: **falcon.crowdstrike.com**

5. Click "Next" and proceed for the connection phase.

That's it! You're all set.

Your SaaS security is our priority!

The FortiCASB-SSPM Team

**FORTINET**