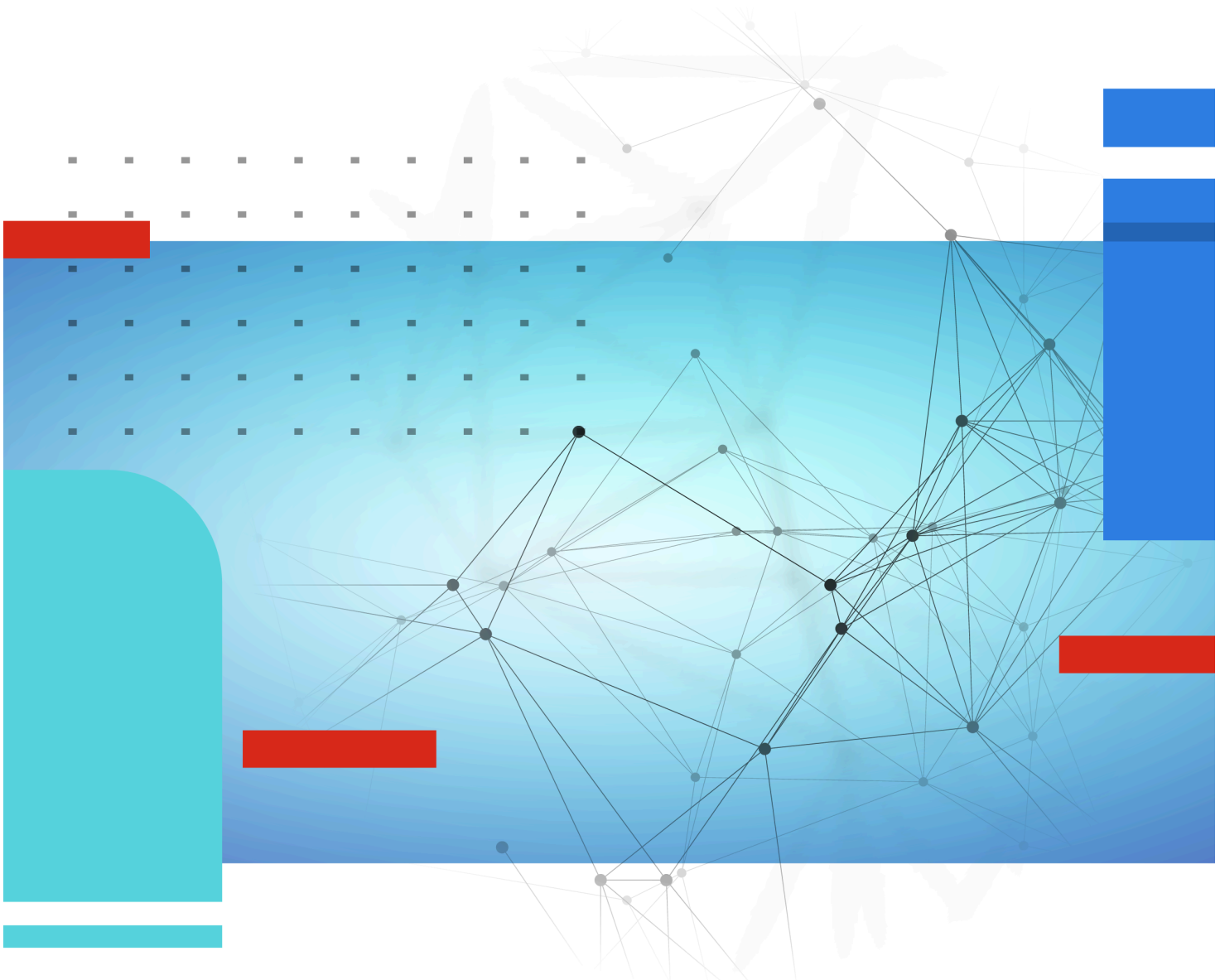
FortiCASB-SSPM Application Connector

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

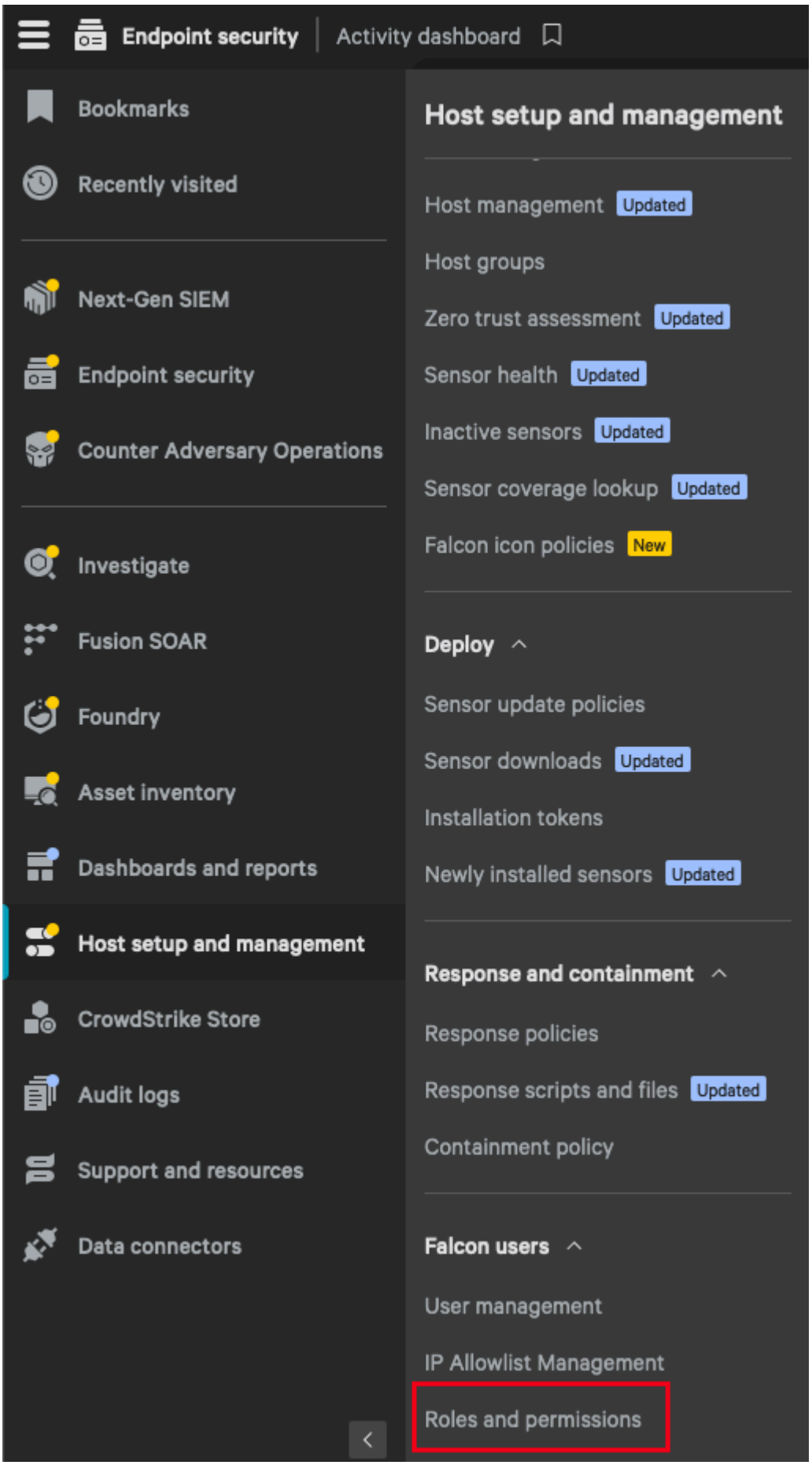
Integration Guide

Intro

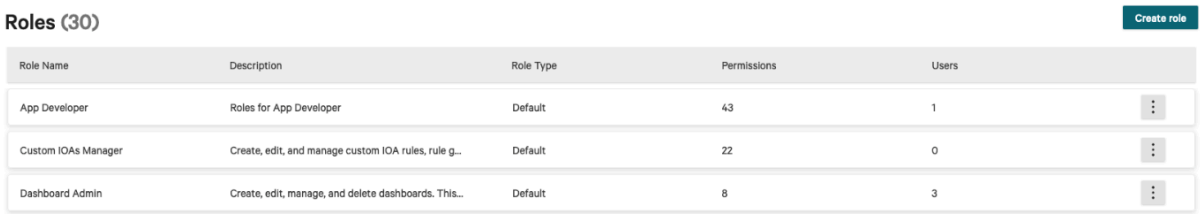
Use this guide to add Crowdstrike as a secured SaaS application in FortiCASB-SSPM SaaS Security platform.

Part A: Service Account Creation

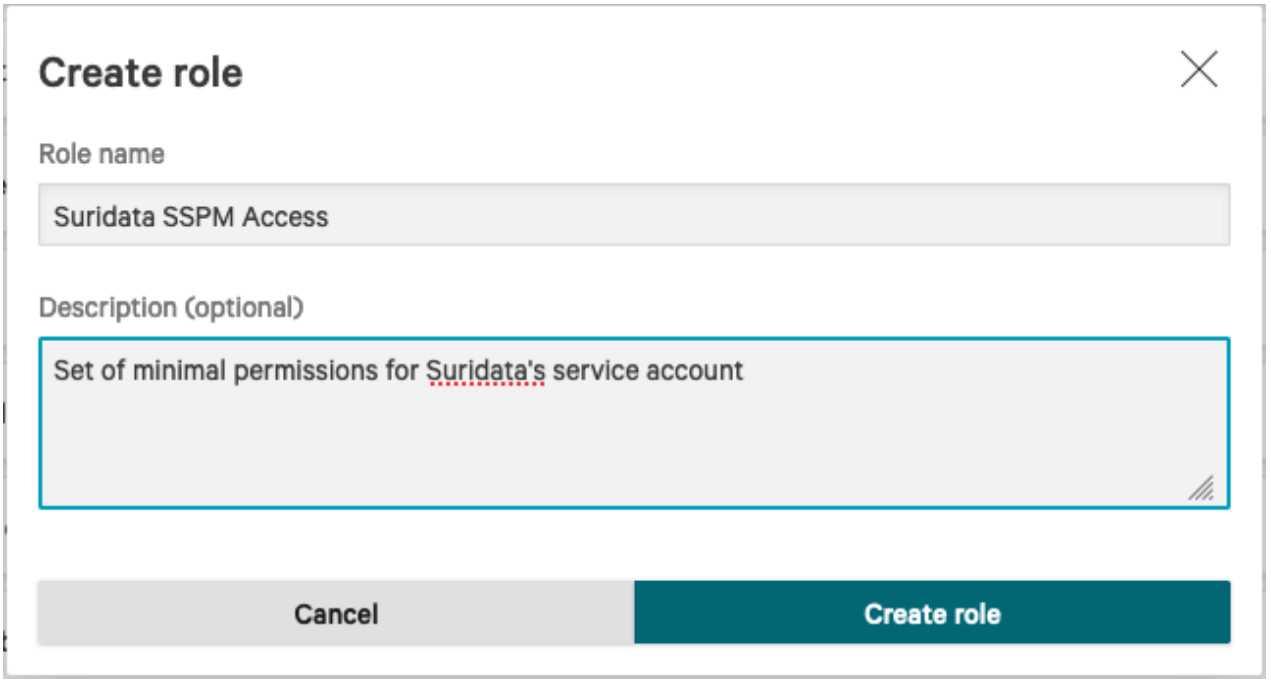
1. Navigate to "Roles and Permissions"



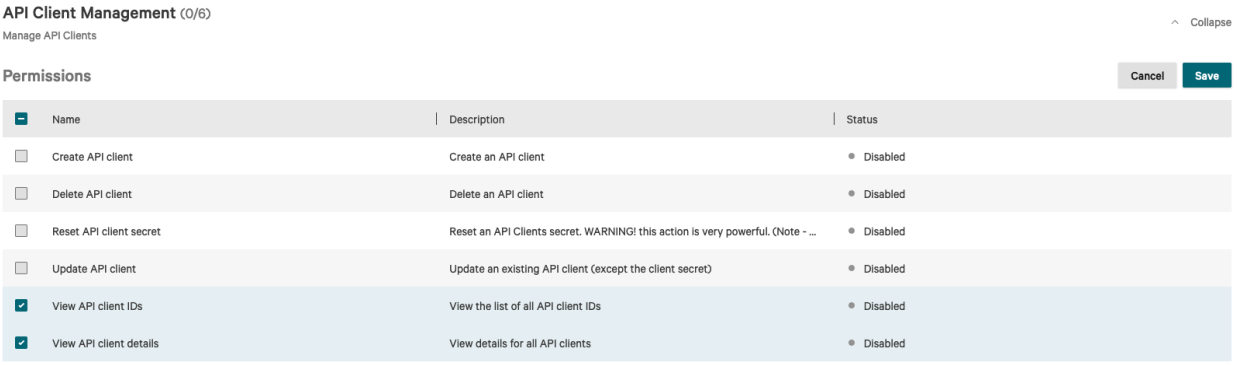
2. Create Role:



3. See the following example:



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

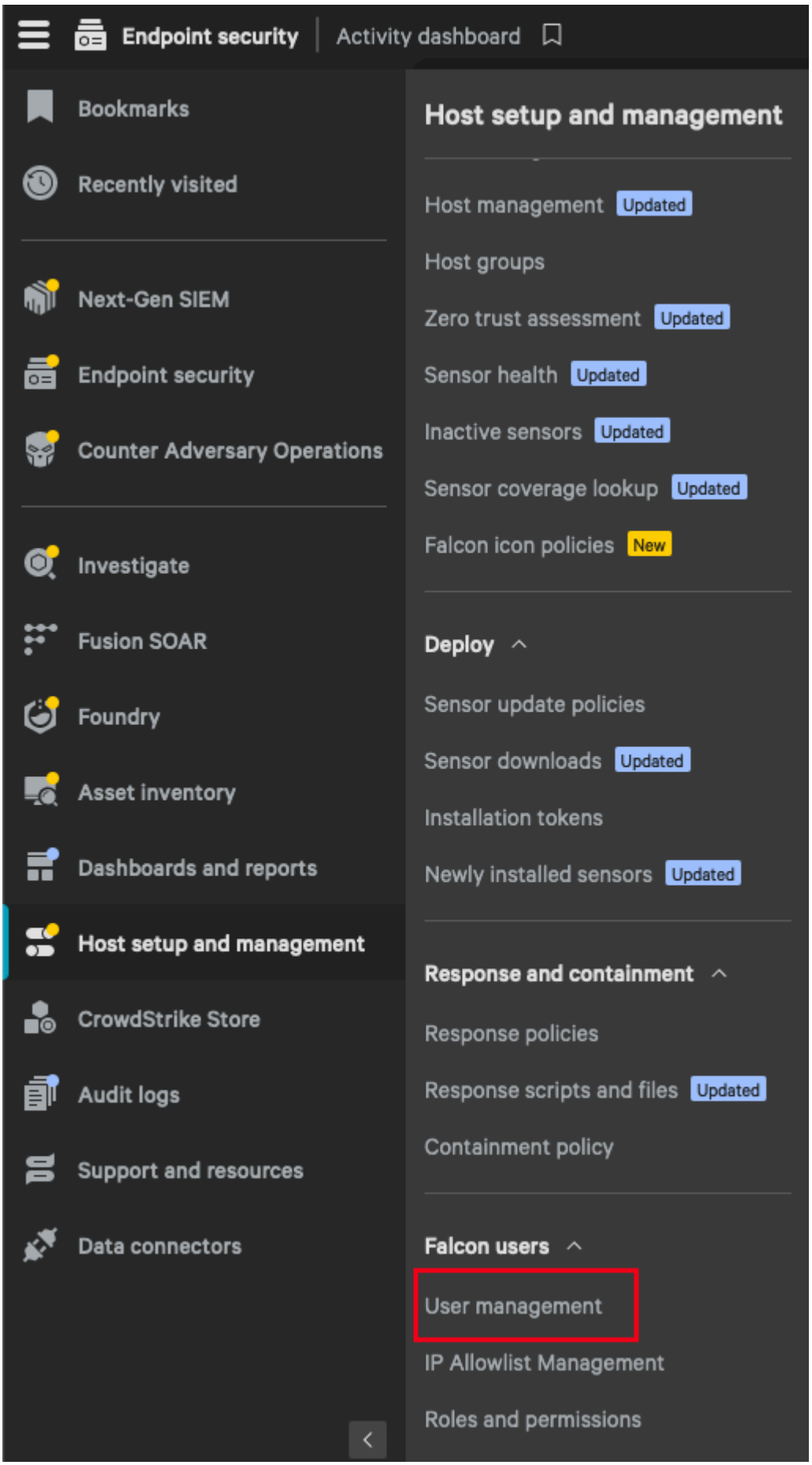


5. Do the same for the flowing groups:

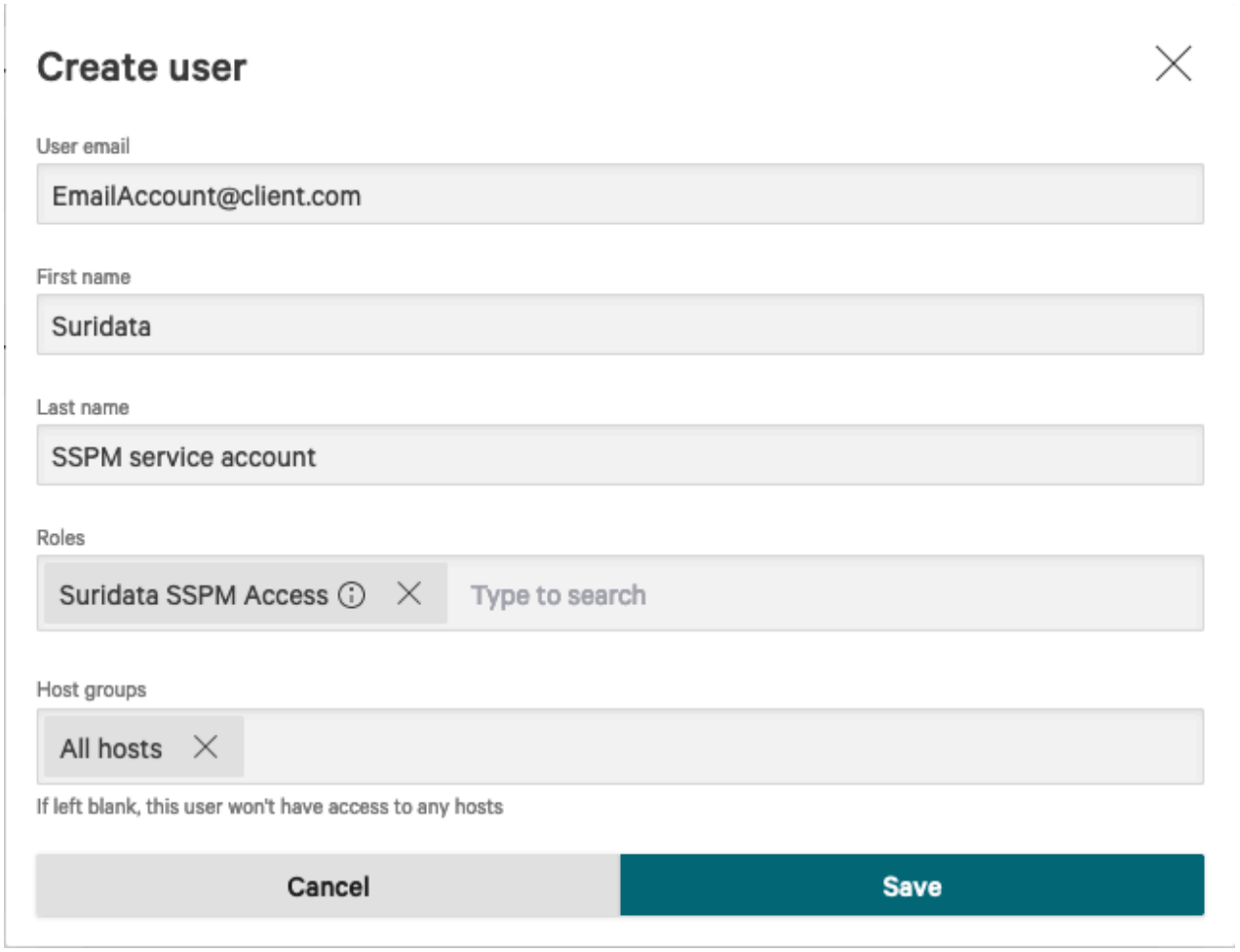
Group	Scope
API Client Management	View API client IDs
API Client Management	View API client details
Manage All Users	List assignable roles
Manage All Users	List host group assignments
Manage All Users	List user roles
Manage All Users	View host group assignments

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



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.

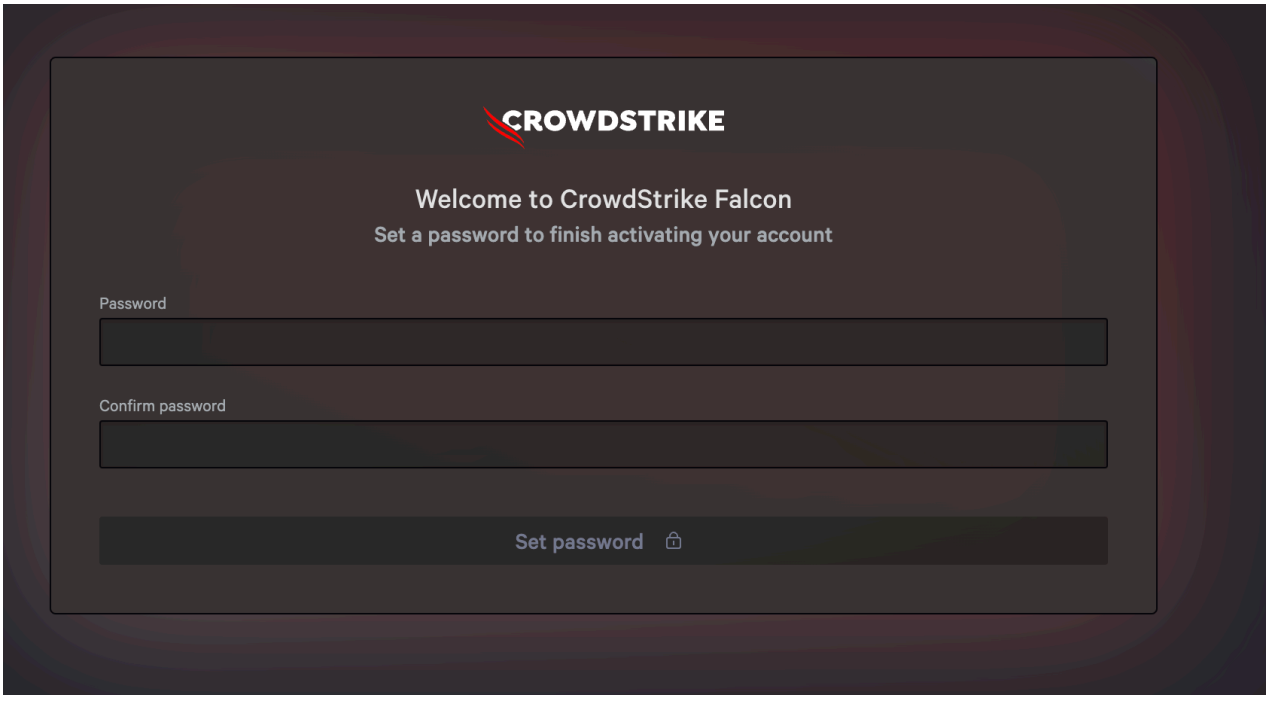
Activate My Falcon Account

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.

10. Set a complex password:

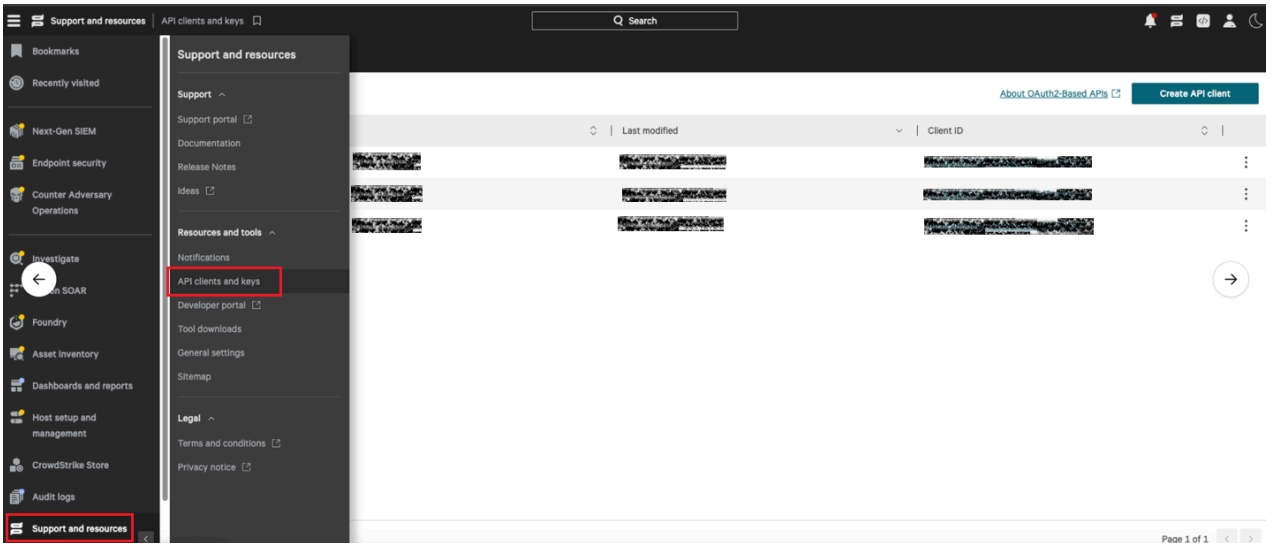


11. When setting the MFA, first copy and save the activation key (this is the TOTP secret)

12. Complete the MFA registration

Part B: Create an Access Token

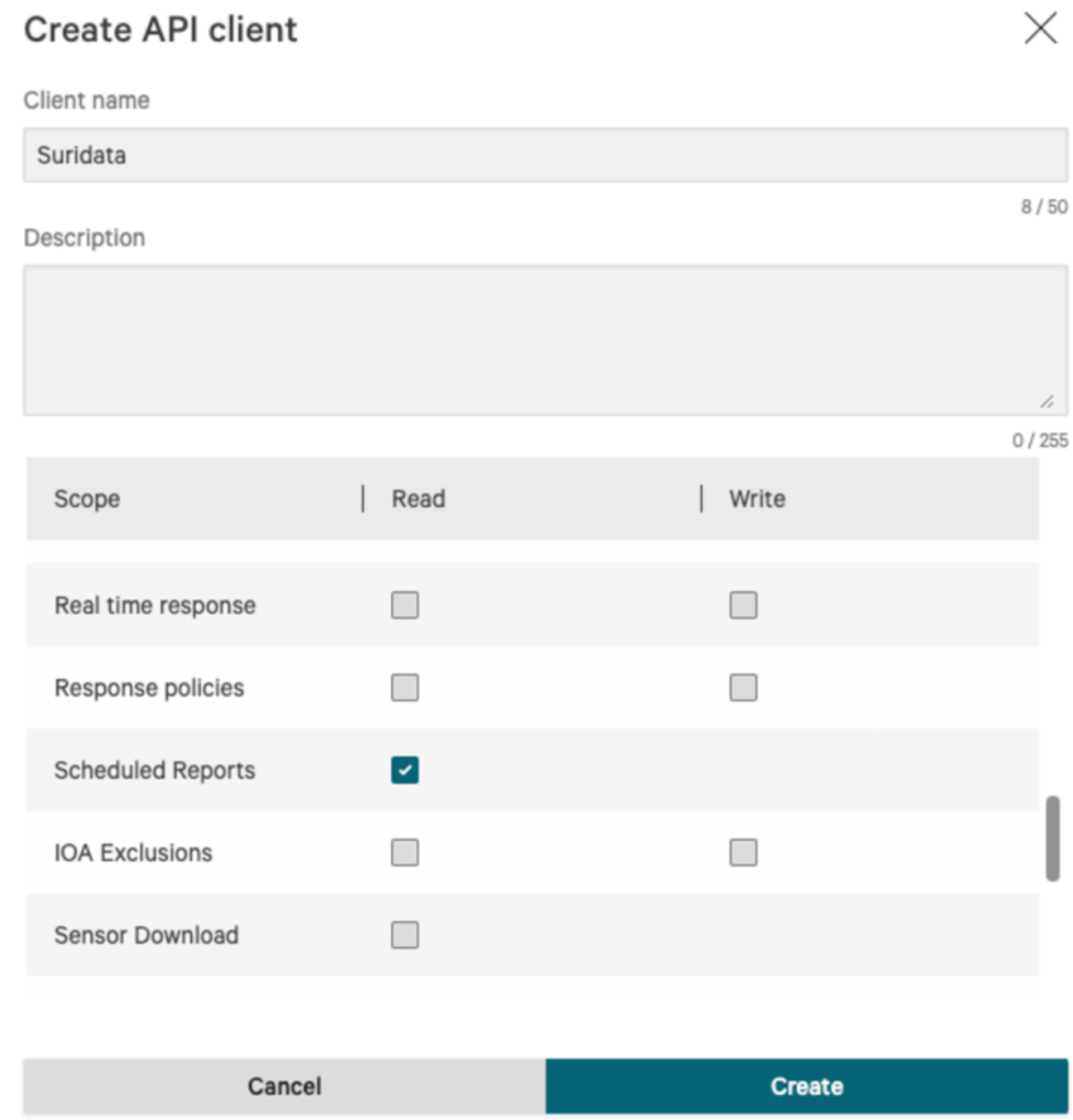
1. Sign in to your CrowdStrike account.
2. Navigate to Support.
3. Navigate to API Clients and Keys:



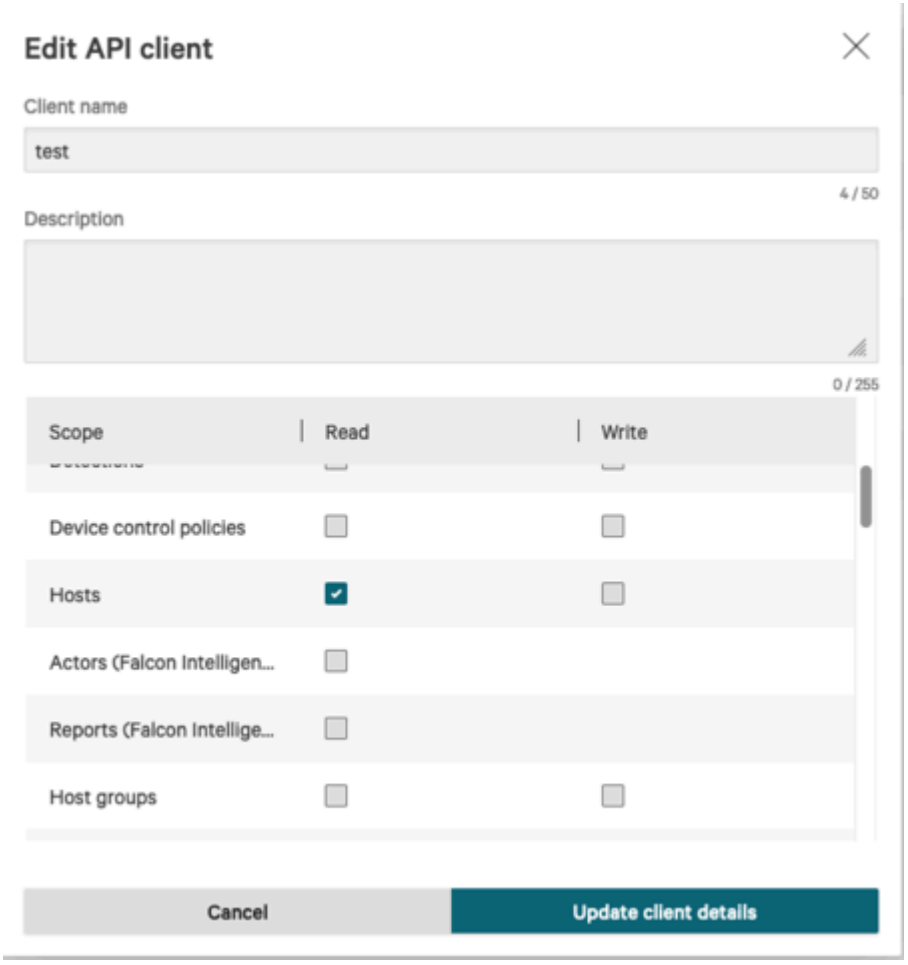
4. Click on: "Create API client"

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

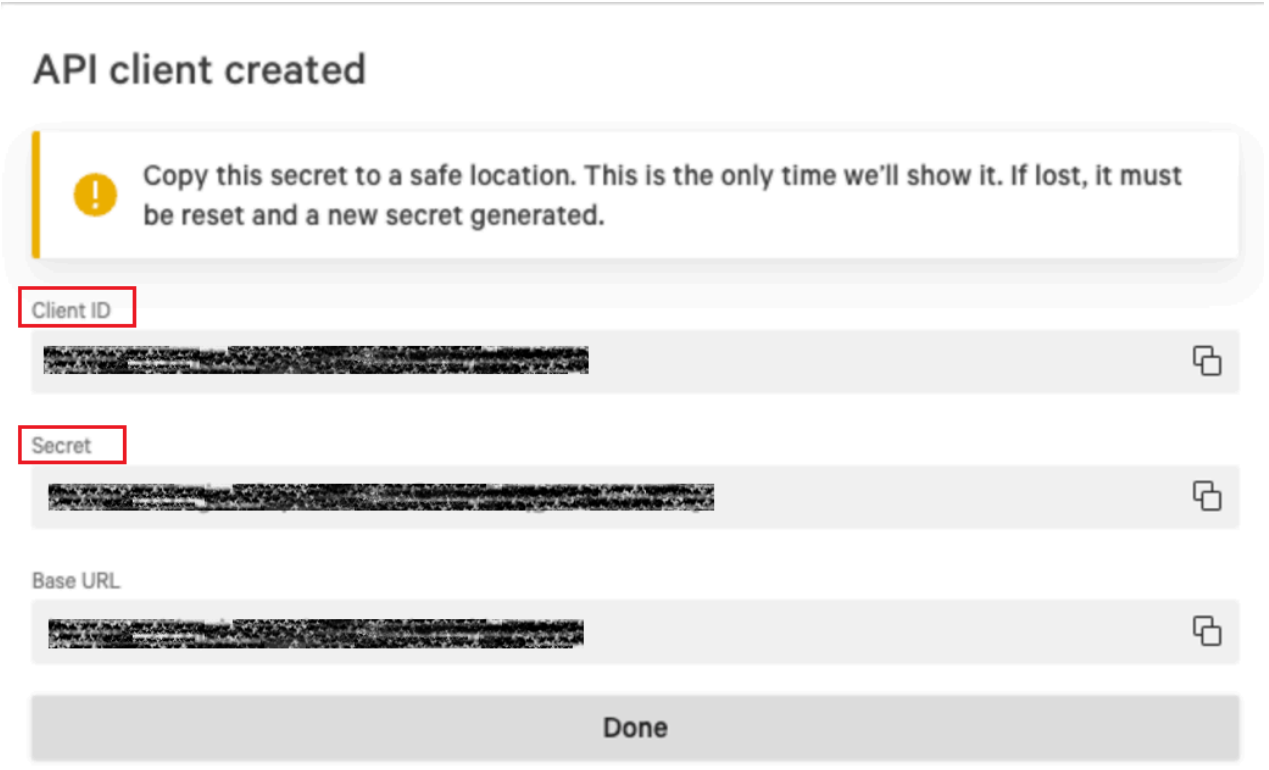
   Example 1:


Create API client
Client name
Suridata
8 / 50
Description
0 / 255
Scope
Read
Write
Real time response
Response policies
Scheduled Reports
IOA Exclusions
Sensor Download
Cancel
Create

Example 2:

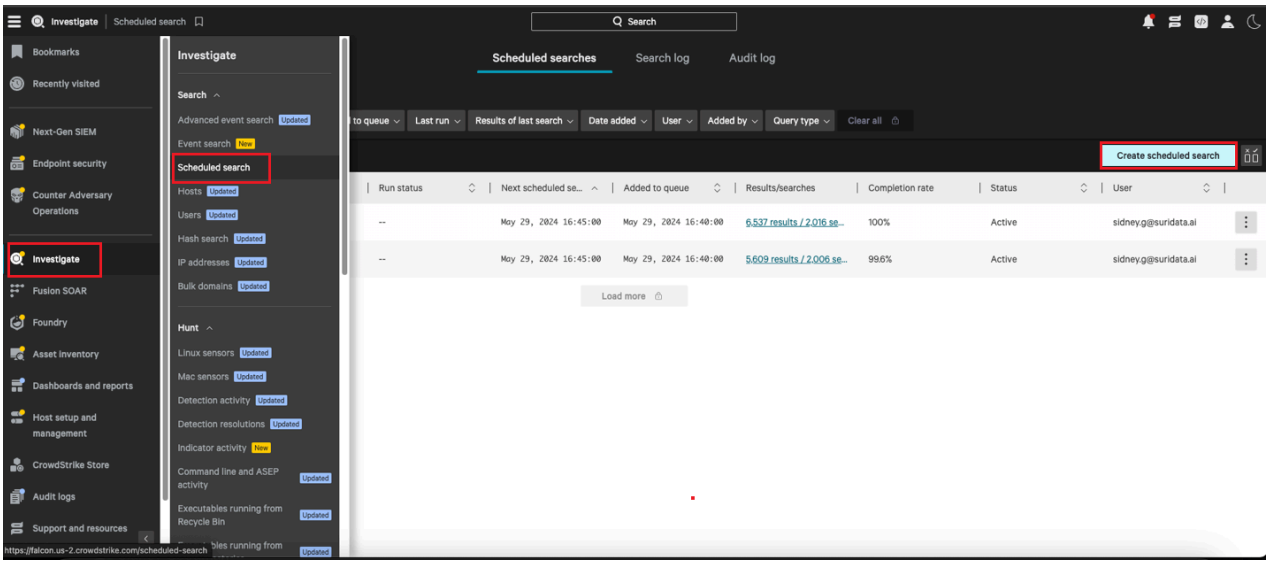


6. Click 'Create'.
7. **Copy the Client ID and Secret** (you will need it for the connection to FortiCASB-SSPM).

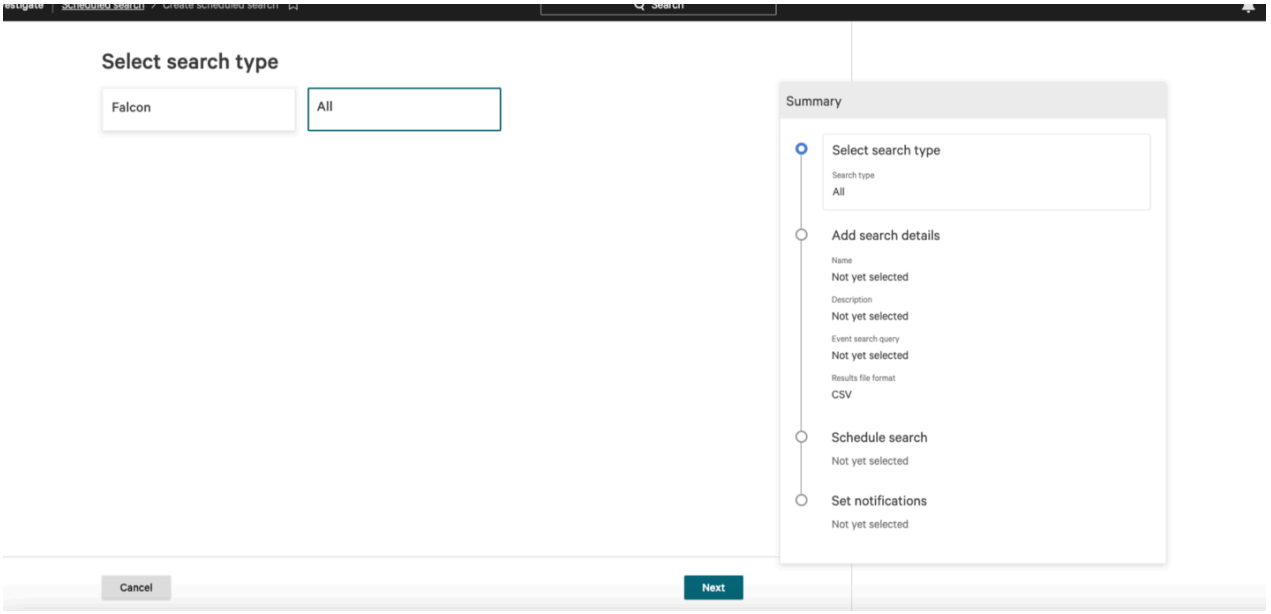


Part C: Setting Up a Scheduled Search

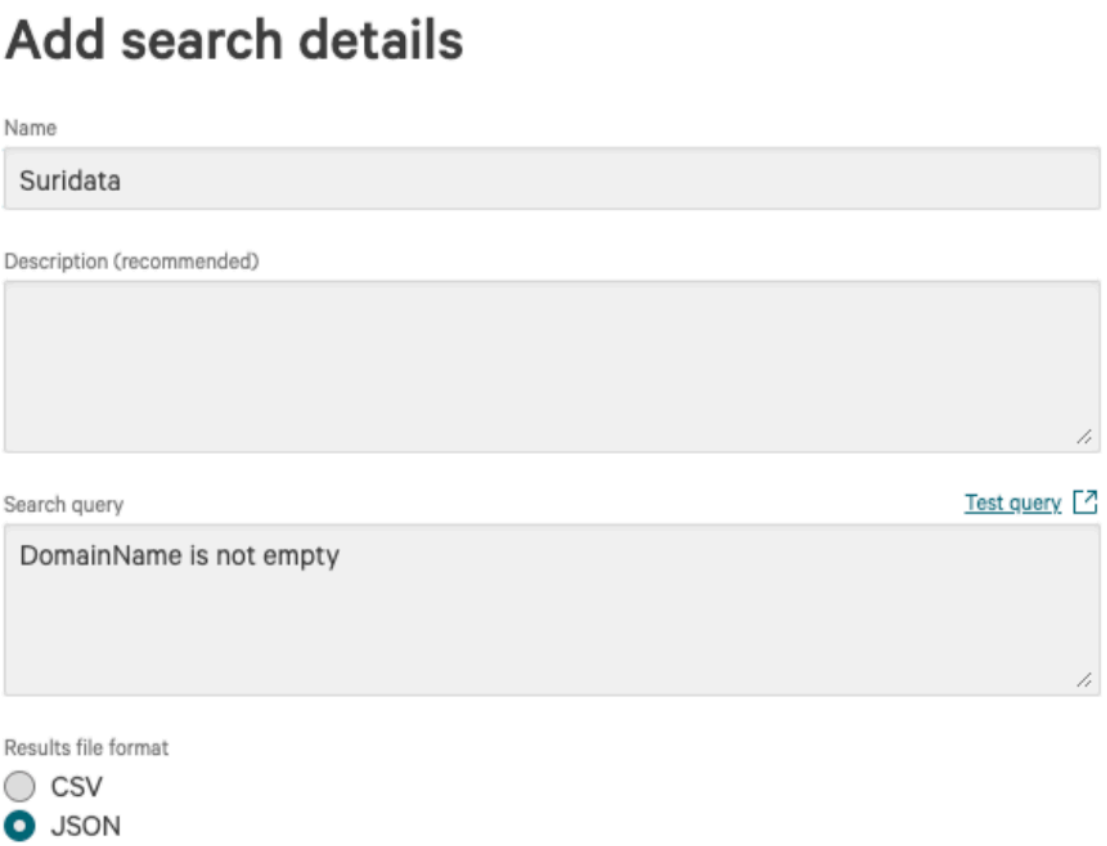
1. Go to 'Investigate'.
2. Go to 'Schedule search'.
3. Click on "Create Scheduled Search".



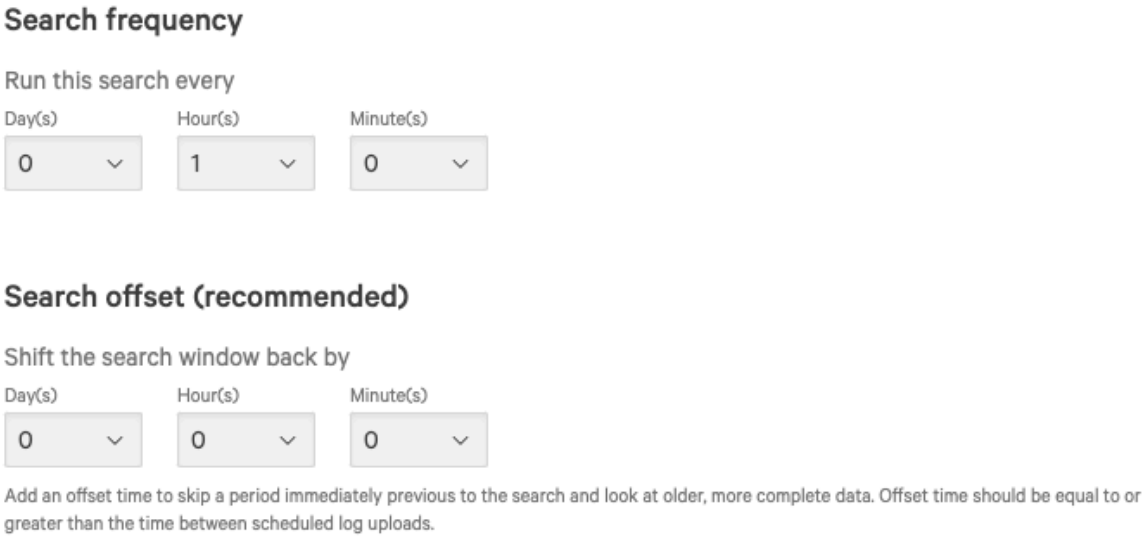
4. Choose All and click "Next".



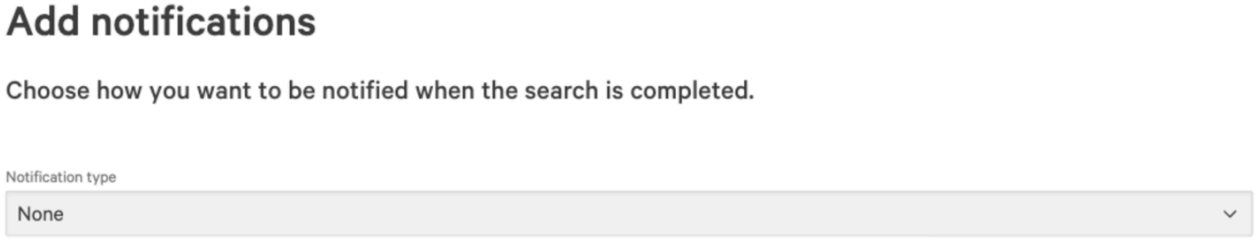
5. In the search query, write: "DomainName is not empty".
6. Results file format: JSON and click "Next".



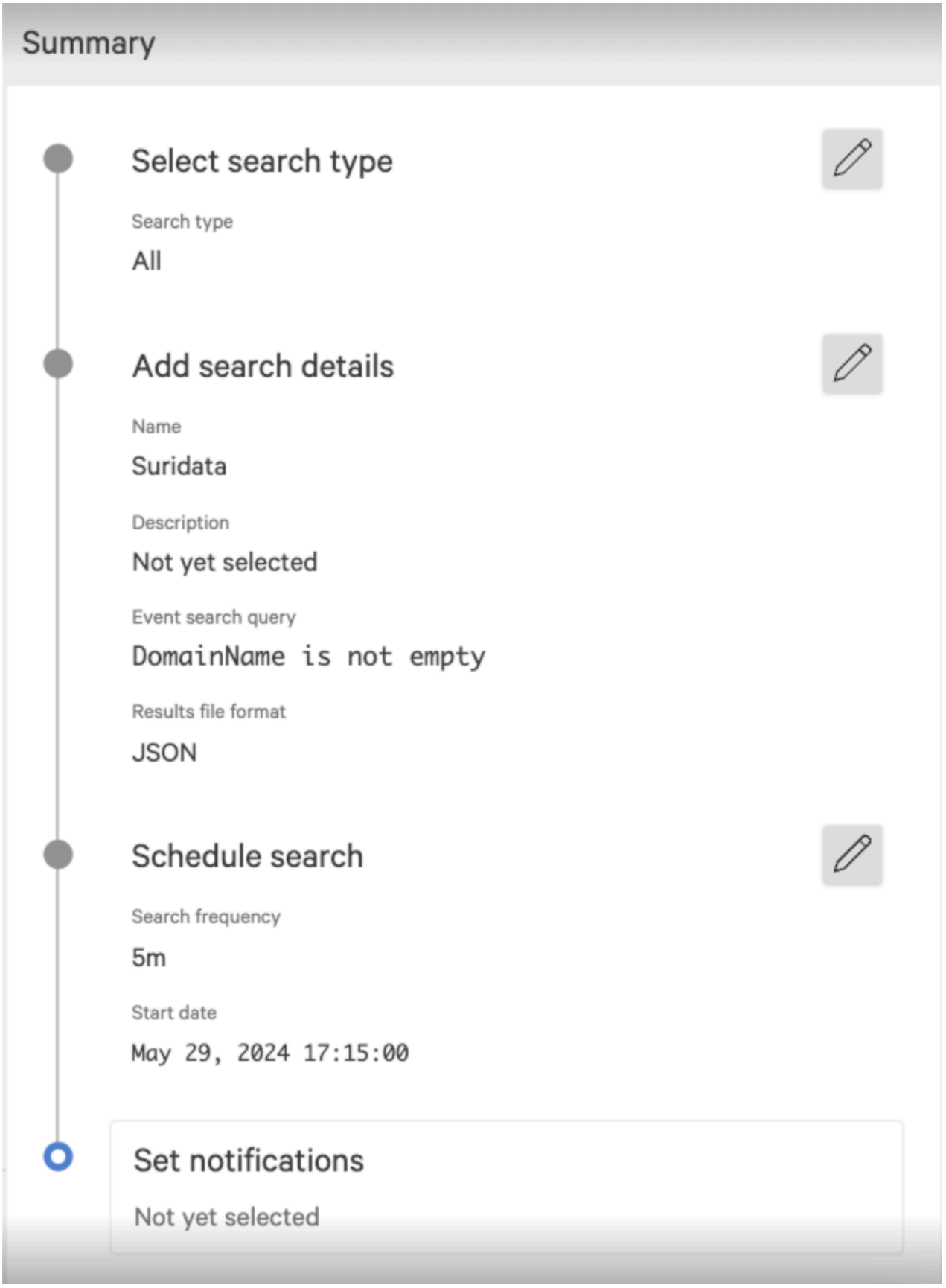
7. Set the search frequency to 1 Hour and the Search offset to 0 Hours, and click "Next".



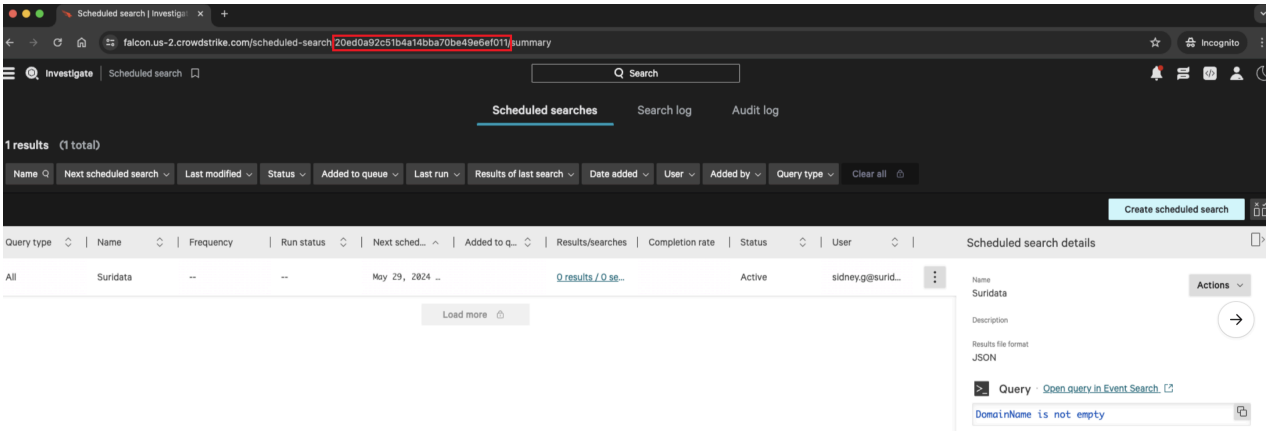
8. Chose 'None' in the Notification type



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



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.



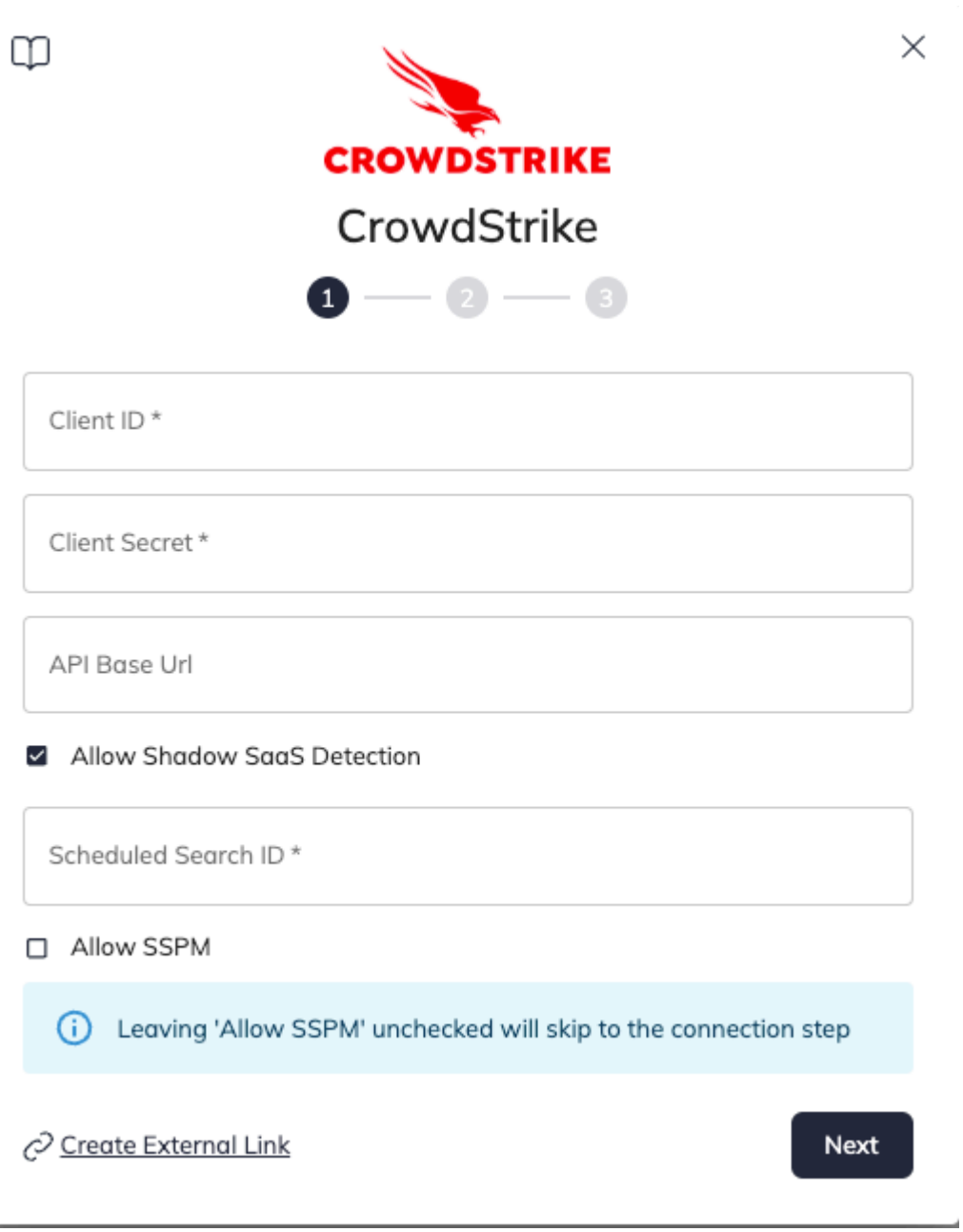
12. If your Base URL is not supported by Auto discovery (for example USGOV1), Copy your Base URL (if it is auto discovered do not enter the base-url field)

    See example:

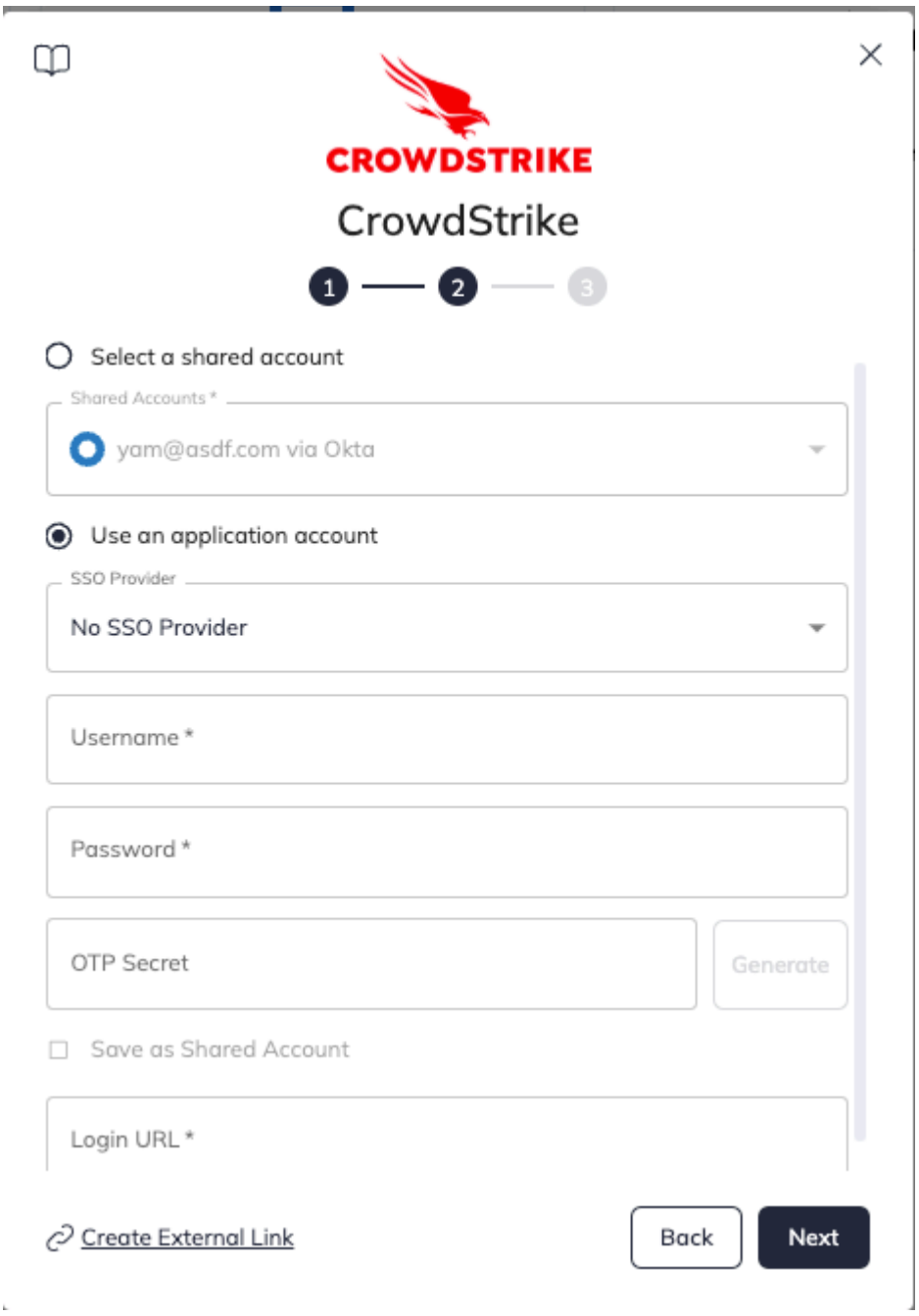
Short name	Base URL	Auto discovery support?
US1	https://api.crowdstrike.com	YES
US2	https://api.us-2.crowdstrike.com	YES
EU1	https://api.eu-1.crowdstrike.com	YES
USGOV1	https://api.laggar.gcw.crowdstrike.com	NO

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)



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)



> **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