

AWS Test Environment and CRWD integration process

Purpose: Document the steps taken to integrate AWS and CRWD and note down that specific configurations we selected

Prerequisites:

1. AWS account with permission (ask Paul for specifics)
2. Organizational Account ID (o-)
3. Delegated admin account ID ()
4. Organizational unit

Step 1:

- Entered Organizational Account
- Delegated Admin Account used instead of Organizational Management account

1. **Note:** Delegated Admin Account cannot monitor activities within the organization management account itself. This means that the organizational management account will not be monitored and you won't be able to see any resources or activity from the management account in Falcon Cloud Security.

- **AWS organizational account will show as inactive.**

2. **Additional Note:** Using delegated admin account is AWS best practice

The screenshot shows the 'Select account structure' configuration page. It has a dark background with white text and input fields. At the top, there's a radio button for 'AWS Organization' which is selected and highlighted with a yellow 'Recommended' badge. Below it, there's a note: 'For help locating this information, refer to AWS documentation on [Organization Settings](#) and [OUs](#)'. There are two input fields: 'Organization ID' containing '0123456789' and 'Organization management account ID' containing '51'. A checked checkbox labeled 'This is a delegated admin account' has a note below it: 'We recommend using the organization management account. The delegated admin account cannot monitor activities within the organization management account itself. This means that the organization management account will not be monitored and you won't be able to see any resources or activity from the management account in Falcon Cloud Security.' There's also a section for 'Organizational unit(s) to register' with a placeholder 'r-' and a radio button for 'Single AWS account' which is selected.

Select account structure

AWS Organization Recommended

For help locating this information, refer to AWS documentation on [Organization Settings](#) and [OUs](#)

Organization ID
0123456789

Organization management account ID
51

This is a delegated admin account

We recommend using the organization management account. The delegated admin account cannot monitor activities within the organization management account itself. This means that the organization management account will not be monitored and you won't be able to see any resources or activity from the management account in Falcon Cloud Security.

Organizational unit(s) to register ⓘ
r-

Single AWS account

Select deployment method

CloudFormation template

Terraform

Step 2:

Select deployment method:

1. CloudFormation template

Step 3:

1. Real time visibility and detections (IOAs)

 **Register an AWS account**

← [Return to cloud accounts registration](#)

Select features ?

CrowdStrike offers a variety of ways to protect your AWS account. Click products to view available features, then select options for this registration.

 **Cloud security**  **IDP**

Cloud security posture management

Included

- Asset inventory
- Indicators of misconfiguration (IOMs)

Optional

- Real-time visibility and detection ?**
Stream CloudTrail logs to Falcon Cloud Security, which enables indicators of attack, real-time asset inventory, and IDP monitoring of AWS Identity Center
- 1-click sensor deployment ?**
Add the Falcon Sensor to any unmanaged EC2 instance with a single click
- Data security posture management (DSPM) ?**
Discover sensitive data in AWS and identify related attack paths

Step 4:

1. We didn't select anything and continued with default settings

The screenshot shows the 'Register an AWS account' configuration page. At the top, there's a link to 'Return to cloud accounts registration'. Below that, a section titled 'Configure advanced settings (optional) ?' is shown. It includes a note: 'Define additional settings for your AWS registration'. There are three tabs at the top of this section: 'Feature settings' (which is selected), 'Customize resource names', and 'Add tags'. Under 'Feature settings', there's a 'Asset inventory' section with a note: 'CrowdStrike automatically creates an IAM role for asset inventory collection. If you wish to customize the permissions you grant to CrowdStrike, you can specify an existing role instead.' A checkbox labeled 'Specify a role name for asset inventory' is present. Below this is a 'Real-time visibility and detection' section with a note: 'By default, CrowdStrike will deploy resources to support Real-time visibility and detection to all available AWS regions. If you only want to deploy these resources to specific regions, select them below.' A dropdown menu labeled 'Regions to deploy to' contains a 'Search options...' button. The entire configuration section has a dark background.

Step 5:

1. Selected "Open CloudFormation Template"
2. Entered CrowdStrike API key's client Secret ID and client Secret value
Note: API key is stored in key vault name "zhe2-cloudsec-kv-prod-01"
 - <https://zhe2-cloudsec-kv-prod-01.vault.azure.net/>

CrowdStrike Falcon API Key

Falcon API Client ID

Your CrowdStrike Falcon OAuth2 API Client ID

4b

Falcon API Client Secret

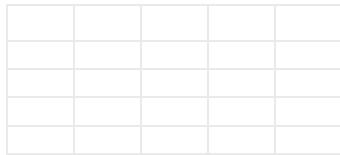
Your CrowdStrike Falcon OAuth2 API Secret

Step 6:

1. Select "Create Stack"

Note: You will notice multiple Stacks created. Registering AWS Organizations using CloudFormation, the registration process creates both stacks and StackSets that contain the resources required for the features that we're enabling:

- StackSets contain the resources for the Organization's member accounts and/or resources that need to be deployed to more than one region in an account
- Stacks contain the resources for the Organization's management account
- CrowdStrike-Integration stack - CrowdStrike Registration Template
- StackSet-crowdstrike-RealtimeVisibility-StackSet
- StackSet-crowdstrike-AssetInventory
- StackSet-AWS-QuickSetup-SSM-TA



Stacks (5)				
	Stack name	Status	Created time	Description
<input type="radio"/>	StackSet-crowdstrike-RealtimeVisibility-EB-Stackset-4ec50014-e713-43e7-80e5-03d364b1b988	CREATE_COMPLETE	2025-06-06 13:46:25 UTC-0400	Setup script to enable CrowdStrike Falcon Realtime Visibility and Detection EventBus Rules.
<input type="radio"/>	StackSet-crowdstrike-RealtimeVisibility-StackSet-504a3339-cbef-4d33-a874-f47af940f42	CREATE_COMPLETE	2025-06-06 13:45:42 UTC-0400	Setup script to enable CrowdStrike FCS Realtime Visibility and Detection IAM resources.
<input type="radio"/>	StackSet-crowdstrike-AssetInventory-5ac31bd0-c9b5-45db-a7ee-0deb3320ba36	CREATE_COMPLETE	2025-06-06 13:45:35 UTC-0400	Setup script to enable CrowdStrike FCS Asset Inventory.
<input type="radio"/>	CrowdStrike-Integration	CREATE_COMPLETE	2025-06-06 13:45:20 UTC-0400	CrowdStrike Registration Template
<input type="radio"/>	StackSet-AWS-QuickSetup-SSM-TA-40rt-f8e40b52-bd72-428c-ac74-4b338efb2b52	CREATE_COMPLETE	2024-12-12 13:29:29 UTC-0500	-