

AWS Production Environment Integration with CSPM

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
3. Delegated admin account |
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 ALWAYS show as inactive.**

Additional Note: Using delegated admin account is AWS best practice

AWS (189) Azure (267) Updated GCP OCI Kubernetes

selections and complete the required information, then choose either Quick setup ⓘ or Standard setup ⓘ to continue.

Select account structure

AWS Organization Recommended

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

Organization ID

Organization management account ID

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 ⓘ

Single AWS account

Select deployment method

CloudFormation template

Terraform

Alternative methods

[Open-source deployment methods](#)

[Deploy via API](#)

Cancel **Continue with quick setup** **Continue with standard setup**

Step 2:

Select deployment method:

1. CloudFormation template

Step 3:

1. Real time visibility and detections (IOAs)

The screenshot shows the CrowdStrike registration interface for AWS accounts. At the top, there are tabs for AWS (189), Azure (267) [Updated], GCP, OCI, and Kubernetes. The AWS tab is selected. Below the tabs, the title "Register an AWS account" is displayed with the AWS logo. A link "← Return to cloud accounts registration" is present. The main section is titled "Select features" with a help icon. A note states: "CrowdStrike offers a variety of ways to protect your AWS account. Click products to view available features, then select options for this registration." Two categories are shown: "Cloud security" (selected) and "IDP". Under "Cloud security posture management", two items are listed as "Included": "Asset inventory" and "Indicators of misconfiguration (IOMs)". Under "Optional", three items are listed: "Real-time visibility and detection" (selected with a checked checkbox), "1-click sensor deployment" (unchecked), and "Data security posture management (DSPM)" (unchecked). Descriptions for each optional item provide details about their functionality.

AWS (189) Azure (267) Updated GCP OCI Kubernetes

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

aws Register an AWS account

← [Return to cloud accounts registration](#)

Configure advanced settings (optional) ①

Define additional settings for your AWS registration

Feature settings

Customize resource names

Add tags

CloudFormation template source region

By default, the CloudFormation templates for this registration are pulled from an S3 bucket in the us-east-1 region. However, if your AWS environment restricts access to us-east-1 (e.g. due to Service Control Policies or Control Tower settings in place), you can specify an alternative enabled region. The templates will then be sourced from an S3 bucket in your selected region.

Template source region

us-east-1

Asset inventory

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.

Specify a role name for asset inventory

Real-time visibility and detection

By default, CrowdStrike will deploy resources to support Real-time visibility and detection to all available AWS regions. If you only want to deploy resources to specific regions, select them below.

Exit

Previous

Next

Step 5:

1. Selected "Open CloudFormation Template"

2. CrowdStrike informed us we did not have to enter API key and that it is optional.

The screenshot shows the 'CloudFormation > Stacks > Quick create stack' interface. It includes sections for enabling various CrowdStrike features and providing API keys, along with fields for permissions and organization provisioning.

- Enable Asset Inventory:** true
- Enable 1-Click Sensor Management:** false
- Enable Realtime Visibility and Detection:** true
- Enable DSPM:** false
- CrowdStrike Falcon API Key:**
 - Falcon API Client ID:** Your CrowdStrike Falcon OAuth2 API Client ID
Enter String
 - Falcon API Client Secret:** Your CrowdStrike Falcon OAuth2 API Secret
Enter String
- Permissions Boundary:**
 - Permissions Boundary Policy Name:** If you would like a permission boundary applied to the IAM roles that CrowdStrike uses, provide the name of the policy to use here.
Enter String
- Provision entire AWS organization or specific Organization Units (OUs):**
 - Organization ID:** Provide the ID of your AWS Organization if you are registering all accounts in your Org or accounts in certain OUs within your Org
Enter String
 - Organizational Unit (OU) IDs to Provision:** (This field is empty)

At the bottom, there are links for CloudShell and Feedback.

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

After Stacks have been created, go to CrowdStrike-Integration Stack > Outputs > Copy value of ReaderRoleArn and RootStackArn

CrowdStrike-Integration

Outputs (2)

Key	Value	Description
ReaderRoleArn	arn:aws:iam::767900165210:role/CrowdStrikeCSPMReader-qirqda6g4zsm	ARN of the reader role for CrowdStrike Falcon CSPM
RootStackArn	arn:aws:cLOUDFORMATION:us-east-1:767900165210:stack/CrowdStrike-Integration/df63ef00-a53a-11f0-b9a9-0affca194541	ARN of this root stack

Step 7:

1. Copy and paste values from ReaderRoleArn and RootStackArn

2. Validate and Complete

Note: You will need to wait 2-4 hours for accounts to be registered.

Register an AWS account

[← Return to cloud accounts registration](#)

Enter ARN details ?

To complete registration, provide the required ARN information

IAM role ARN

CloudFormation stack ARN