

## **Implementation Guide: Sysdig Secure – AWS Control Tower Integration**



# Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram	5
Pre-requisites	6
Deployment and Configuration Steps	6
Sysdig Secure Configuration	7
Deploying Integration	9
Verifying Integration	11
Best Practices	15
Solution Estimated Pricing	15
FAQs	15
Additional resources	16
Partner contact information	16

## Foreword

The Sysdig Secure DevOps Platform, featuring CloudVision, allows you to manage your security posture on AWS cloud. With CloudVision, you can keep track of cloud events, configurations, roles, threats, and compliance to reduce risk. The purpose of this Implementation Guide is to enable AWS users to deploy, configure, and activate the Sysdig CloudVision component in an AWS cloud environment to take full advantage of the resources and capabilities of AWS Control Tower. With this solution, you can leverage Sysdig cloud security capabilities for multiple organizations following AWS best practices.

## Solution overview and features

Sysdig Secure integration with [AWS Control Tower](#) enables customers to automatically protect existing and newly enrolled AWS accounts through ingestion of [AWS CloudTrail](#) logs. Through a series of automation steps, this solution leverages existing AWS Control Tower infrastructure to:

- Discover the centralized AWS CloudTrail logging bucket in the Log Archive account.
- Discover the centralized [AWS SNS topic for CloudTrail](#) in the Audit account.
- Deploy Sysdig Cloud Connector in the Log Archive account.
- Discover and optionally add permission for Sysdig Cloud Connector to decrypt AWS CloudTrail with the existing [AWS KMS](#) key.
- Automatically integrate AWS accounts in the Sysdig Secure portal, including a future account created by AWS Control Tower.

Sysdig Secure detects anomalous activity across AWS workloads with out-of-the-box policies based on [Falco](#). Sysdig Secure extends the open-source Falco detection engine to provide comprehensive security across AWS workloads.

Sysdig Secure allows you to:

- Block threats by extending Falco's detection capabilities with prevention and automated responses that don't impact performance.
- Ease the burden of creating and updating runtime Falco rules with ML-based profiling, a flexible Policy Editor to customize rules, and an extensive curated Rules Library.
- Reduce false positives by tuning Falco-based policies for your own environment.
- Embed security across the DevOps process with image scanning, security monitoring, forensics, incident response, and audit.
- Validate compliance using out-of-the-box checks and runtime policies that map to compliance standards like NIST and PCI.
- Continuously detect cloud threats using AWS CloudTrail (e.g., suspicious logins, file access, etc.)

## Architecture diagram

Sysdig Secure ingests AWS CloudTrail using the [Sysdig Cloud Connector](#), which runs AWS CloudTrail ingestors using an [AWS ECS Fargate](#) task with a combination of [AWS SQS](#) and [AWS SNS](#) to receive AWS CloudTrail logs. By leveraging AWS CloudTrail and [Sysdig Secure policies](#), users are able to detect unexpected and unwanted behavior in their AWS accounts.

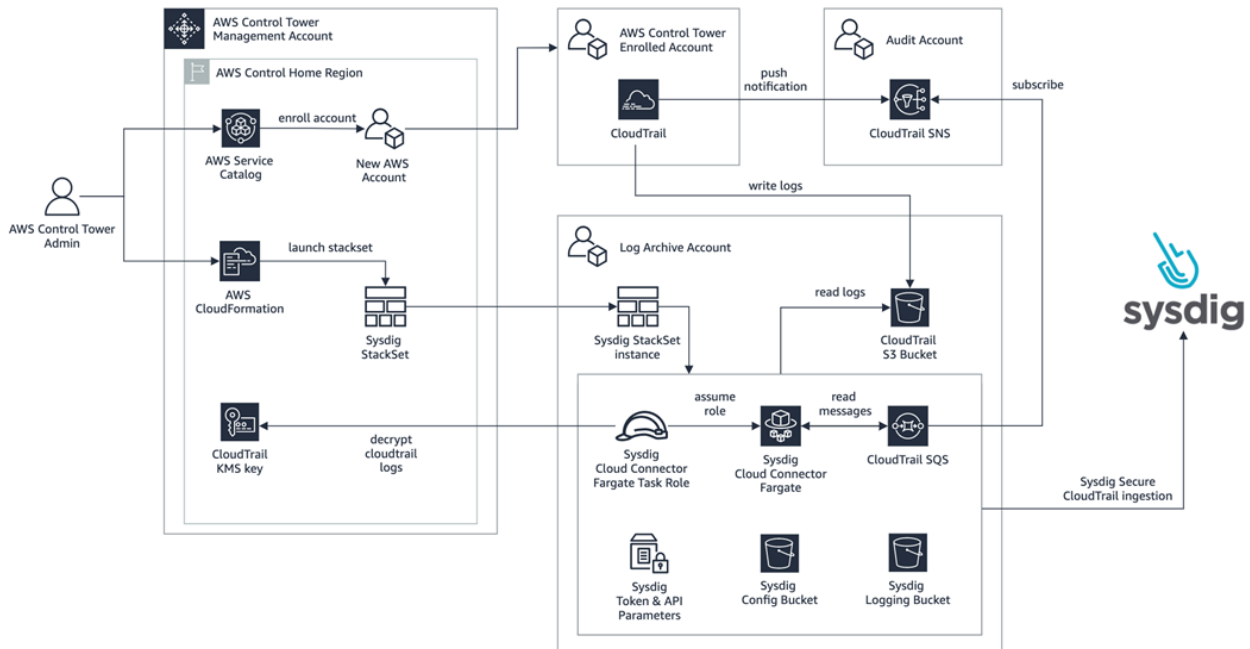


Figure 1 – Sysdig Secure AWS Control Tower Integration Architecture Diagram

This solution leverages AWS Control Tower centralized CloudTrail infrastructure and automates AWS CloudTrail ingestion. Customers can deploy the solution using [AWS CloudFormation](#) stack in the management account, which then orchestrates the following:

- Deploys the Sysdig Cloud Connector Fargate infrastructure in the Log Archive account, including:
  - Dedicated VPC, ECS cluster, ECS service, ECS task and role for CloudTrail ingestion.
  - SQS queue to subscribe to CloudTrail SNS topic.
  - [AWS SSM Parameter store](#) for token and endpoint information.
  - [Amazon S3](#) bucket for Sysdig Cloud Connector config and logs.
- Adds the SNS topic policy to aws-controltower-AllConfigNotification SNS topic located in the Audit account.
- Subscribes the SQS queue to aws-controltower-AllConfigNotification SNS topic.
- Adds permissions to the Sysdig Cloud Connector Fargate task to decrypt the KMS key used for AWS CloudTrail encryption.

## Pre-requisites

The following prerequisites are required to implement the Sysdig Secure integration with AWS Control Tower:

- Fully deployed AWS Control Tower. For information about setting up an AWS Control Tower landing zone, see [Getting Started with AWS Control Tower](#). You also need administrator privileges in the AWS Control Tower management account.
- An active Sysdig Secure or Sysdig Platform account. You can sign up for a free trial from [AWS Marketplace](#).

This solution guide assumes working knowledge with AWS management console and AWS CloudFormation. If you are new to AWS, see [Getting Started with AWS](#). For additional information about AWS Marketplace, see [AWS Marketplace Overview](#)

## Deployment and Configuration Steps

### Step 1.1: Subscribe to Sysdig Secure on AWS Marketplace.

*Optional: Skip to step 2 if you already have an active Sysdig Secure account.*

Locate **Sysdig Secure** in the [AWS Marketplace](#)

The screenshot shows the product page for Sysdig Secure DevOps Platform - Enterprise Tier on AWS Marketplace. The page features the Sysdig logo on the left, which consists of a blue hand icon pointing to a cursor. To the right of the logo, the product name is displayed in bold, followed by 'Sold by: Sysdig' and a 'Free trial' badge. Below this, a short description states: 'Confidently secure containers, Kubernetes, and cloud with the Sysdig Secure DevOps Platform. Scan images, flag misconfigurations, detect and respond to threats, validate' with a 'Show more' link. On the right side, there are three buttons: 'Continue to Subscribe' (orange), 'Try for free' (green), and 'Save to list' (blue). At the bottom of the product card, there are five tabs: 'Overview' (selected), 'Pricing', 'Usage', 'Support', and 'Reviews'. Below the product card, the 'Product Overview' section is visible, containing a paragraph about the platform's security and visibility features. To the right of the overview, there is a 'Highlights' section with a bullet point: 'BUILT ON AN OPEN-SOURCE STACK: Unify threat detection across containers and cloud using Falco'.

Click on the **Continue to Subscribe** button.

### Step 1.2: Guidance on Contract Duration and Renewal

In the new screen, you can configure your contract. You can select the **Contract Duration** and set the **Renewal Settings**.

### Step 1.3: Select Contract Options

Select the Contract Options to be activated with your contract.

### Step 1.4: Create the Contract and Pay

Once you have configured your contract, you can click on the Create contract button.

You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.

### Step 1.5: Set up Account

To complete registration, choose Setup your account and follow the remaining instructions.

**Sysdig Secure DevOps Platform - Enterprise Tier** ×

✔ Congratulations! You're now subscribed.

<b>Sysdig Platform Trial</b>	<b>\$0 - Due Today</b>
30-Day Free Trial Sysdig Platform (Secure and Monitor)	
<b>Auto Renew - No</b>	

---


To complete registration and start using your software, choose Setup your account.

[Setup your account](#)

## Sysdig Secure Configuration

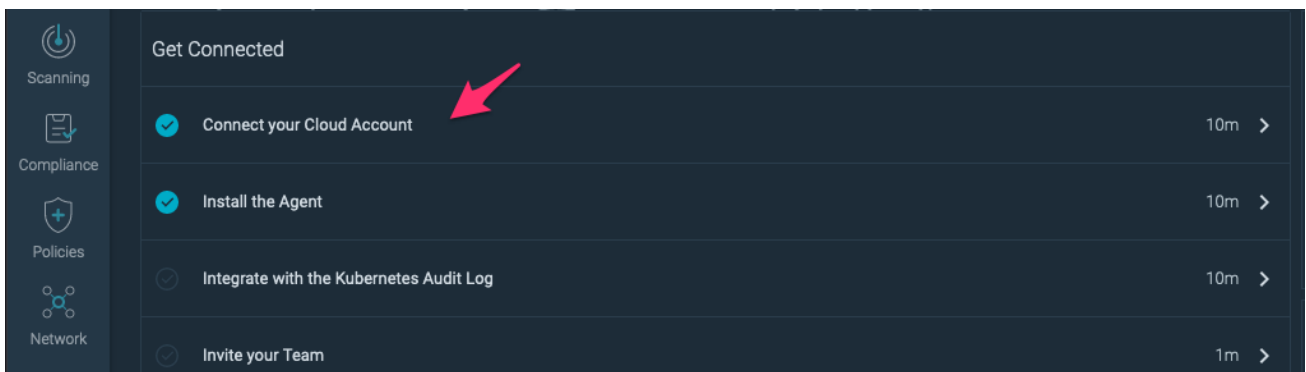
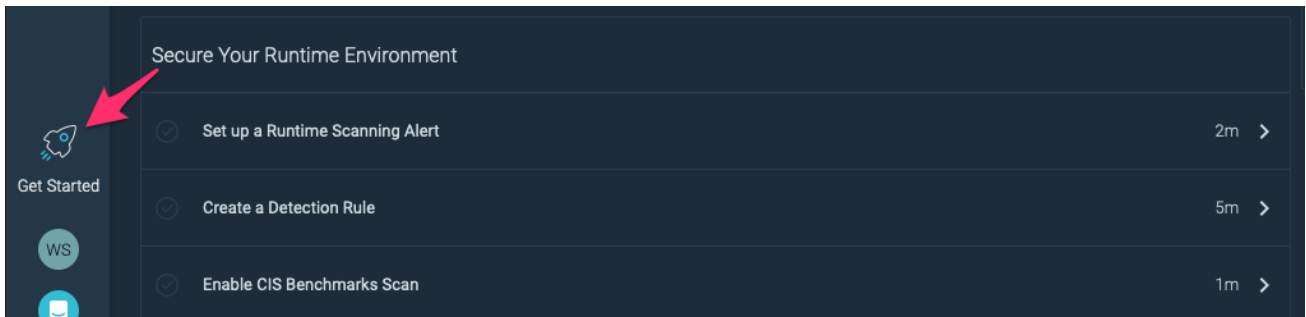
### Step 2.1: Log into the Sysdig Secure

Using the provided link and your user-name credentials, login to the Sysdig Secure portal.

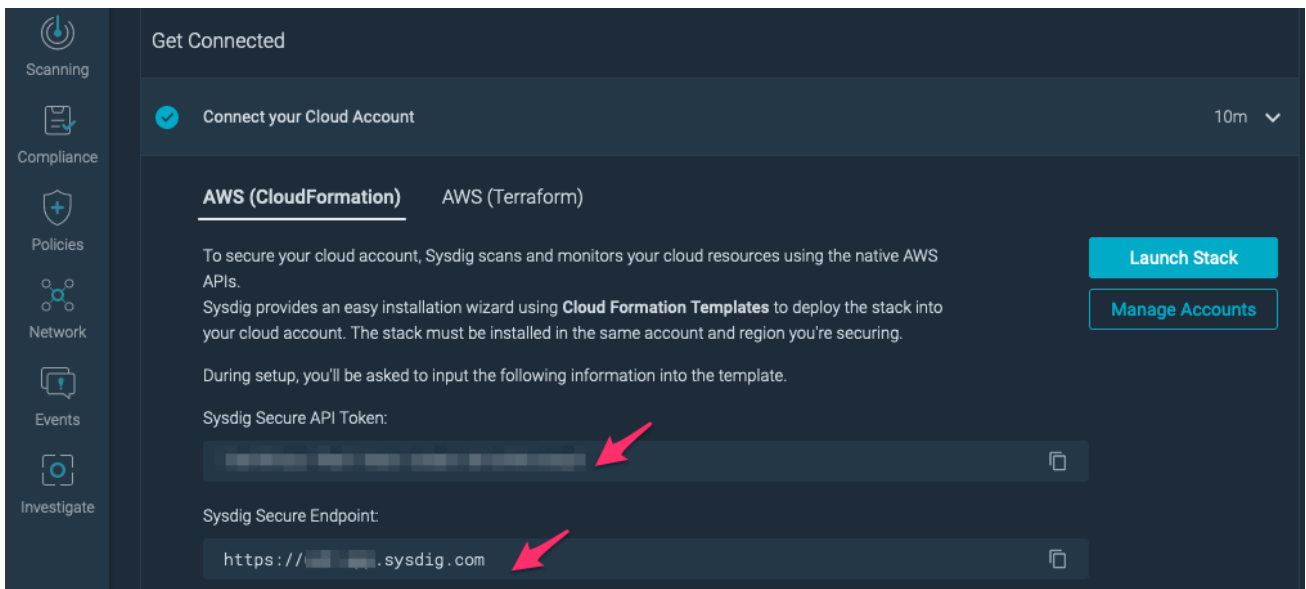
  
  
  
  
[Forgot your password?](#)

## Step 2.2: Sysdig Secure API and Endpoint

From the navigation side-bar, select **Get Started** and choose **Connect your Cloud account**.



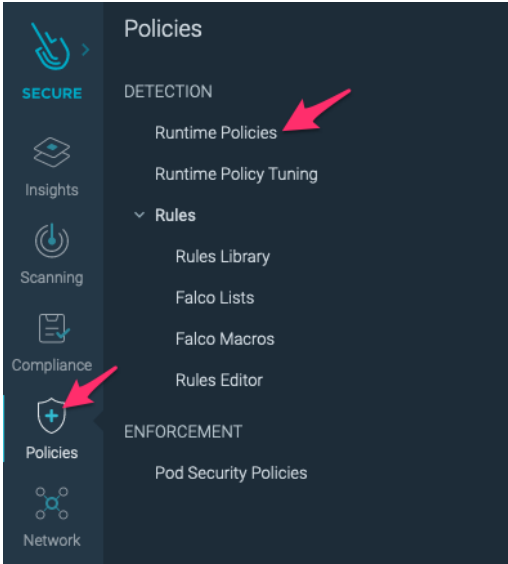
Copy the **Sysdig Secure API Token** and **Sysdig Secure Endpoint** URL.



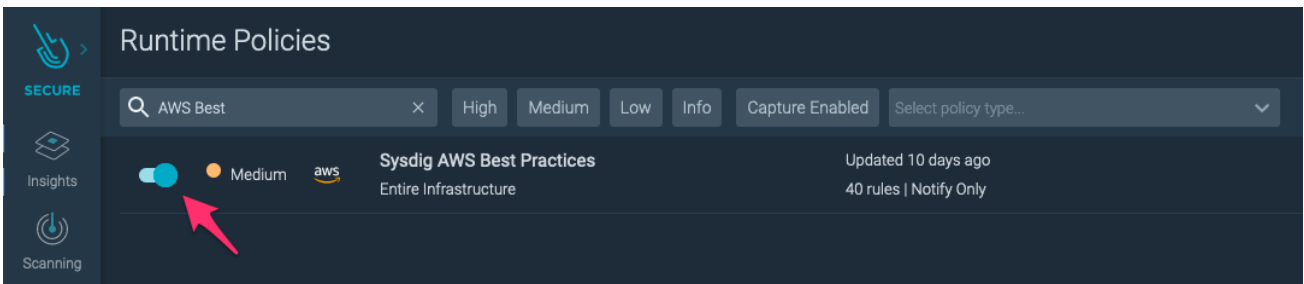


### Step 2.3: Enable Runtime Policies

Returning back to the main menu, from the side-bar navigation, select **Policies** and then select **Runtime Policies**.



Search for **Sysdig AWS Best Practices** and select the toggle to enable the runtime policies.



## Deploying Integration

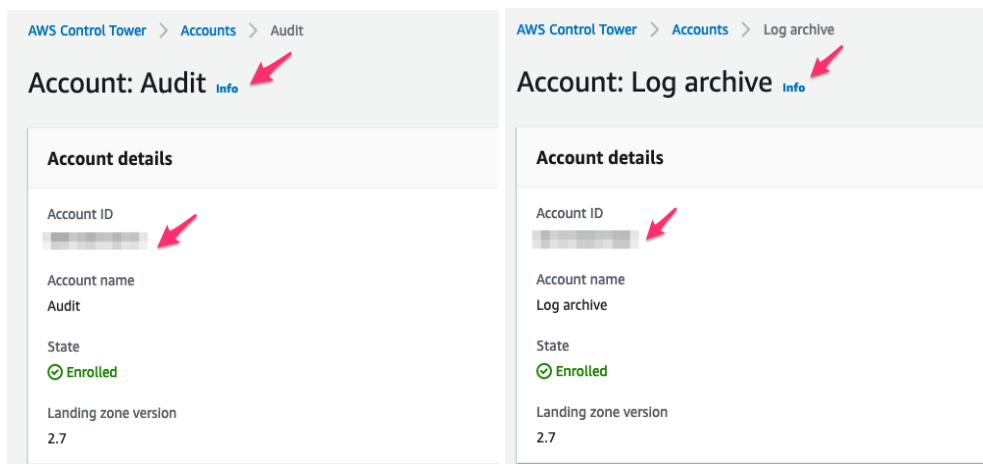
### Step 3.1: Solution repository

The complete solution (Cloud Formation templates and Lambda functions) can be found in the following [GitHub repository](#). The deployment steps below use direct reference from the Sysdig owned S3 bucket originated from this repository.

### Step 3.2: AWS Control Tower Parameters

Login into the Management account in AWS Control Tower as Admin role. Navigate to [AWS Control Tower console](#) and select Accounts from the side navigation bar. Ensure you are selecting the home region where your AWS Control Tower is deployed.

Locate the Audit account and Log Archive account from the list and take note of both account IDs.



### Step 3.3: Launch AWS CloudFormation Template

From the AWS Control Tower management account, launch the CloudFormation template using the following [Quick-Crete link](#).

Enter the required parameters and leave the default parameters value as is.

- Sysdig Secure Endpoint = use value from step 2.2
- Sysdig Secure API Token = use value from step 2.2
- AWS Control Tower Audit Account id = use value from step 3.2
- AWS Control Tower Log Archive Account id = use value from step 3.2
- StackSet name = required, change this only if you have any other StackSet with the same name.
- Stack name = required, change this if you have Stack with the same name.

Select the checkbox **“I acknowledge that AWS CloudFormation might create IAM resources”** and select **Create Stack**.

Wait until the stack creation is complete. This deployment will asynchronously deploy the Sysdig StackSet. Navigate to [AWS CloudFormation StackSet console](#), and search for the Sysdig StackSet according to the parameter you entered earlier. Select **Operations** and wait until the operation is completed. The operation will take 5-10 minutes to complete.

CloudFormation > StackSets > Sysdig-Secure-CT: StackSet details

## Sysdig-Secure-CT

StackSet Info | Stack Instances | **Operations** | Parameters | Template

Operations (1) View drift details Stop operation

Q Search

Operation ID	Type	Status	Created time
301fc476-571f-4aae-a4fc-fcd5ec5c45e6	CREATE	<span>ⓘ</span> <b>RUNNING</b>	2021-10-09 08:34:55 UTC-0700

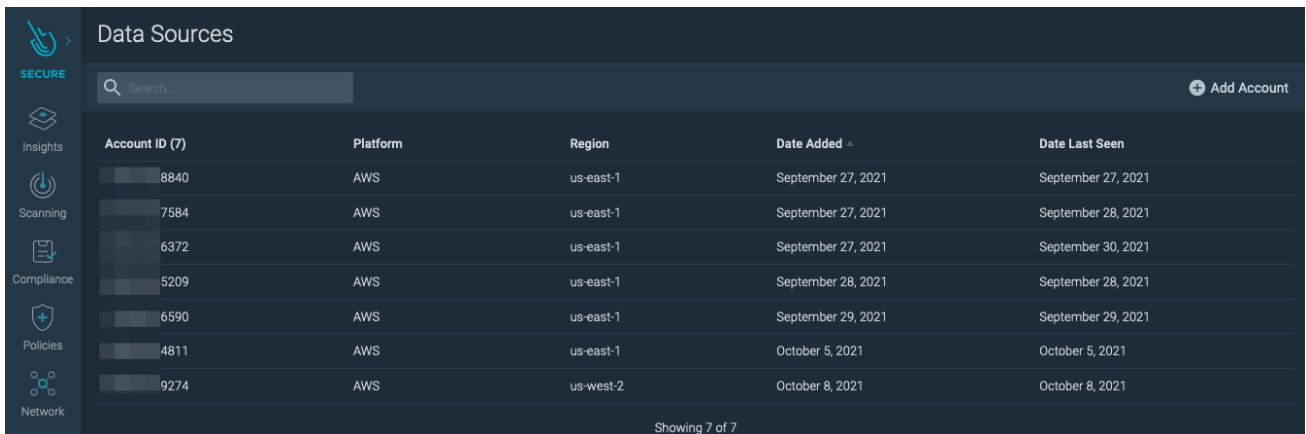
## Verifying Integration

### Step 4.1: Data Source Cloud Account Validation

Navigate back to Sysdig Secure console. From the side-bar navigation, select your username and choose **Data Sources**.

The screenshot shows the Sysdig Secure console sidebar navigation menu. The menu items are: Events, Investigate, Get Started, WS (user profile), Data Sources, Settings, and Logout. The 'Data Sources' option is highlighted with a red arrow, and the 'WS' user profile icon is also highlighted with a red arrow.

The Log Archive account id should be automatically registered in the list as the data source. Other AWS account ids will automatically be listed here once the CloudTrail logs are ingested, and events are triggered.



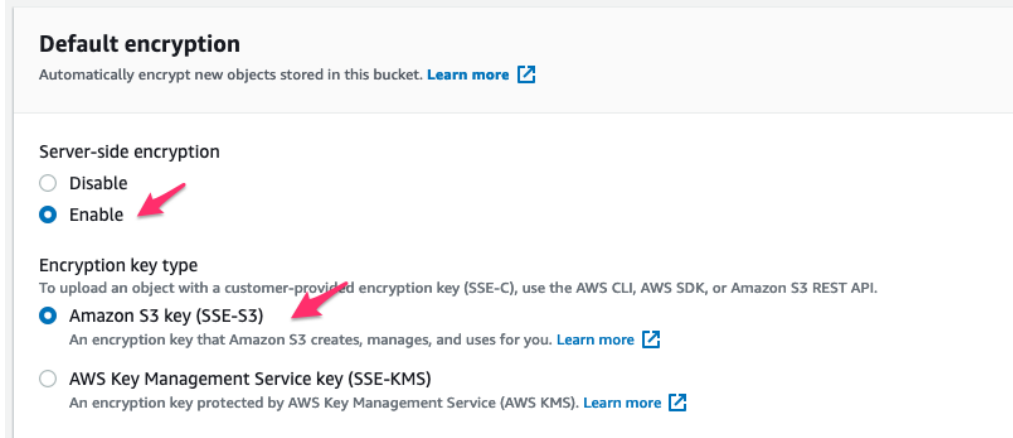
The screenshot shows the 'Data Sources' page in Sysdig Secure. It features a search bar at the top and a table with columns for Account ID, Platform, Region, Date Added, and Date Last Seen. There are 7 accounts listed, all of which are AWS accounts in the us-east-1 region, except for one in us-west-2. The table is paginated to show 7 of 7 items.

Account ID (7)	Platform	Region	Date Added ^	Date Last Seen
8840	AWS	us-east-1	September 27, 2021	September 27, 2021
7584	AWS	us-east-1	September 27, 2021	September 28, 2021
6372	AWS	us-east-1	September 27, 2021	September 30, 2021
5209	AWS	us-east-1	September 28, 2021	September 28, 2021
6590	AWS	us-east-1	September 29, 2021	September 29, 2021
4811	AWS	us-east-1	October 5, 2021	October 5, 2021
9274	AWS	us-west-2	October 8, 2021	October 8, 2021

#### Step 4.2: Testing Runtime Policies

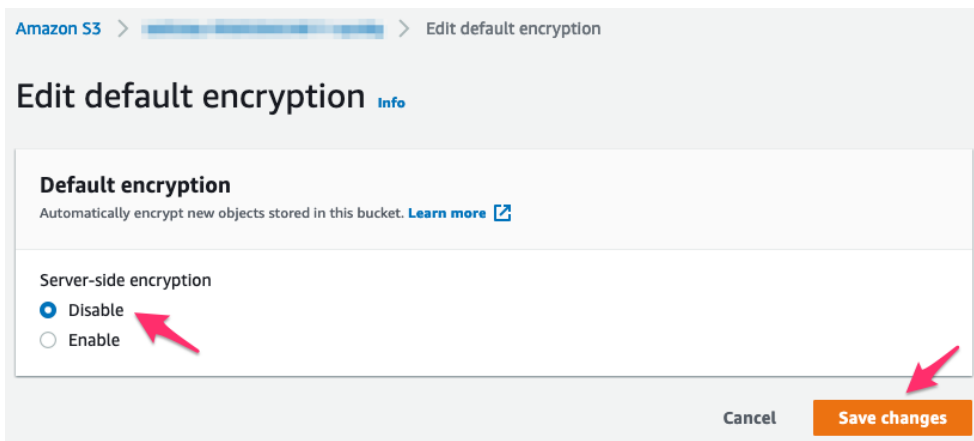
The following steps are optional but are intended to test and validate the integration by simulating suspicious activity that will trigger Sysdig Secure Runtime Policies.

Login to one of the AWS Control Tower managed accounts using a role with Admin privileges. Navigate to [S3 console](#) and create a new S3 bucket with default Server-side encryption enabled.



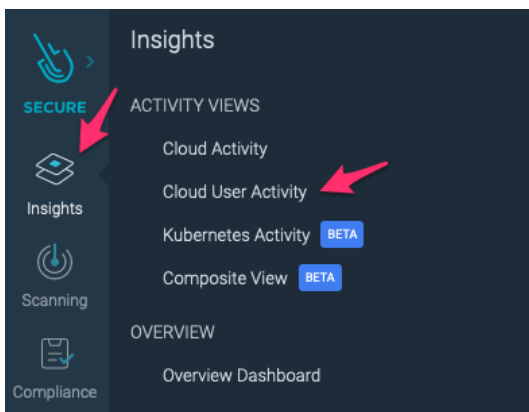
After the S3 bucket has been created, select the bucket, and select the **Properties**. Locate the **Default encryption** section and select **Edit**.

Modify the Server-side encryption to **Disable** and select **Save changes**.



CloudTrail typically delivers logs within an average of about 15 minutes of an API call. For more details check AWS documentation on [how CloudTrail works](#). To verify the effectiveness of the rule, wait for 10-15 minutes before proceeding to the next step.

In the Sysdig Secure console, from the side-bar navigation, select **Insight** and then select **Cloud User Activity**.



Locate the recently generated events and find the event with label **Delete Bucket Encryption**.

The screenshot shows the AWS Cloud Activity console. On the left, there is a bubble chart representing activity across different regions and resource types. On the right, the 'All Activity' section is visible, showing a list of events. The event 'Delete Bucket Encryption' is highlighted with a red arrow, indicating it is the event of interest.

Count	Event Name
6	Root User Executing AWS Command
3	CloudTrail Logging Disabled
2	Create Lambda Function Not Using Latest Runtime
2	Create Security Group Rule Allowing SSH Ingress
1	Delete Bucket Encryption
1	Create IAM Policy that Allows All
1	Console Login Without MFA
1	Console Root Login Without MFA

Select the event tab to dive deeper and review the details.

The screenshot shows the details of the 'Delete Bucket Encryption' event. The event was triggered on Saturday, October 9, 2021, at 9:05:54 AM. The event details include the policy name, rule type, and triggered rules.

**Policy & Triggered Rules**

- name: Delete Bucket Encryption - Sysdig AWS Best Practices
- ruleType: AWS CloudTrail
- ruleName: Delete Bucket Encryption

A encryption configuration for a bucket has been deleted (requesting user=..., requesting IP=..., AWS region=us-west-2, bucket=...-4811-sysdig)

**aws**

- aws\_s3
- mitre\_TA0005-defense-evasion
- mitre\_T1070-indicator-removal-on-host
- cloud

**Scope**

- resourceType: AWS Simple Storage Service
- resourceCategory: Storage
- aws.user: ...@... .com
- aws.sourceIP: ... 180
- aws.s3.bucket: ...-4811-sysdig

## Best Practices

- Visit the [Sysdig documentation portal](#) to learn more about Sysdig Secure installation, administrative and features.
- Visit [Sysdig blog page](#) for collection of best practice and recommended settings.
- Visit [Sysdig learn portal](#) for guided training materials.

## Solution Estimated Pricing

Please visit [sysdig.com/pricing](https://sysdig.com/pricing) for an updated price list and to calculate costs using the Sysdig SaaS price calculator. Alternatively, you can evaluate the solution by registering the free tier with no costs and upgrade to other plans in the future.

## FAQs

**I need to add a new AWS account using AWS Control Tower, are there additional steps to integrate with Sysdig?**

This solution will automatically integrate the Sysdig Secure Cloud Connector to ingest CloudTrail logs from existing and newly added AWS accounts.

**I want to integrate other Sysdig Secure capabilities such as ECR Image Registry scanning and Fargate Image scanning.**

To deploy additional Sysdig Secure and Sysdig Monitor features, follow the instructions from the [Sysdig support page](#). When selecting modules to deploy, ensure to select No for CloudTrail ingestion.

### Modules to Deploy

Do you want to deploy Cloud Security Posture Management / Compliance?

Do you want to deploy Real-Time Threat Investigation based on CloudTrail?

Do you want to deploy ECR Image Registry Scanning?

Do you want to deploy Fargate Image Scanning?

### **Why is my AWS Control Tower linked account not visible in the Sysdig portal data source?**

This solution integrates and centralizes the AWS CloudTrail log collection into the AWS Control Tower Log Archive account. The Log Archive account id will be registered first in the list as the data source. Other AWS account ids will automatically be listed once the CloudTrail logs are ingested, and events are triggered.

### **I still have more questions, where can I get help?**

Visit the [Sysdig support page](#) for additional help. You can also open issues on the [GitHub repository](#) for a specific problem with the integration with AWS Control Tower.

### Additional resources

- [Sysdig Secure product page](#)
- [Continuous Cloud Security Posture Management with Sysdig](#)
- [Cloud Workload Protection with Sysdig](#)

### Partner contact information

For further information about this solution, [Contact Sysdig](#).