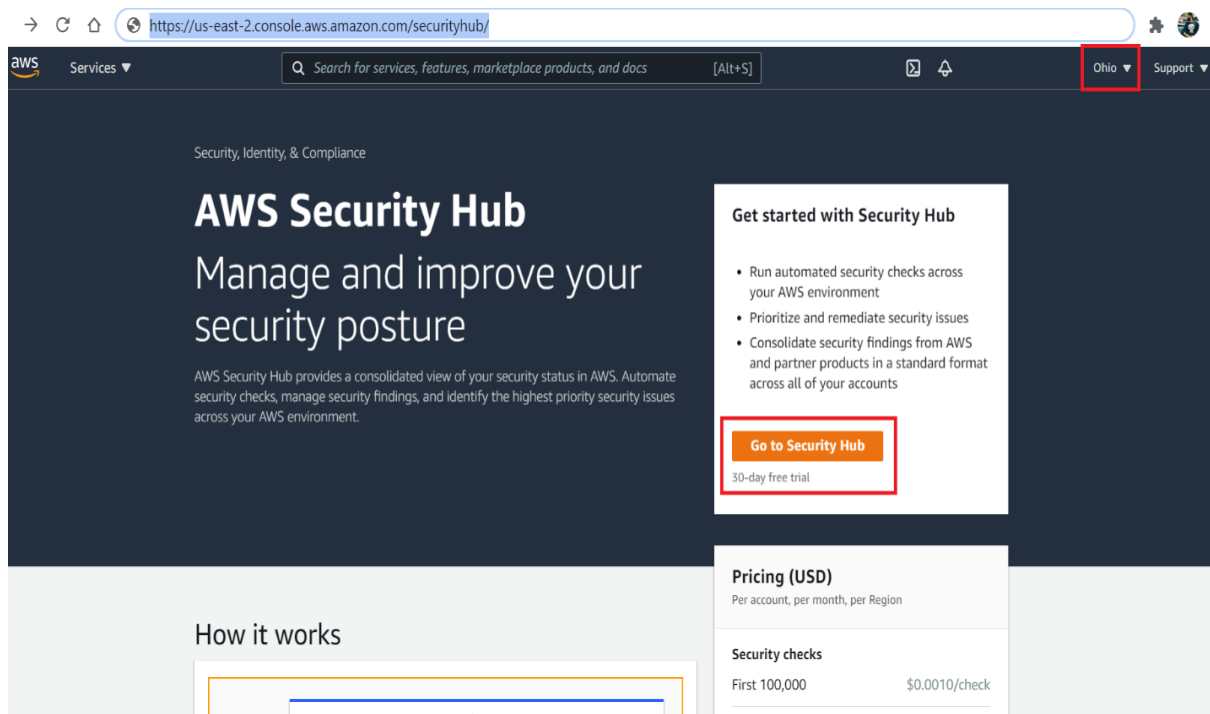


Step 1

[Click here](#) to Navigate to AWS Security Hub. Select the right region where you are planning to run the master template & click **Go to Security Hub** as shown below. **Note: Security Hub is a regional service and eligible for a 30-days free trial. If you have already exhausted the 30-day free trial, run it in a different region where you haven't availed of the 30 days free trial. If you have already activated the Security Hub earlier in the specific region, no need to take any action.**



→ ↻ ⌂ <https://us-east-2.console.aws.amazon.com/securityhub/> ⚙️ 🌐

aws Services ▾ 🔍 Search for services, features, marketplace products, and docs [Alt+S] 📄 🔔 Ohio ▾ Support ▾

Security, Identity, & Compliance

AWS Security Hub

Manage and improve your security posture

AWS Security Hub provides a consolidated view of your security status in AWS. Automate security checks, manage security findings, and identify the highest priority security issues across your AWS environment.


Get started with Security Hub

- Run automated security checks across your AWS environment
- Prioritize and remediate security issues
- Consolidate security findings from AWS and partner products in a standard format across all of your accounts

Go to Security Hub

30-day free trial

How it works



Pricing (USD)

Per account, per month, per Region


Security checks	
First 100,000	\$0.0010/check

Step 2

Once you land upon the below page, you need to click on **Enable Security Hub**, as shown below. Congratulation, you have successfully configured AWS Security Hub in your desired region. **Note:** You can ignore the below warning, you really don't need to enable AWS Config for this tutorial at least. AWS Config is an expensive service, it's better not to activate it for any demo purpose. **Follow Step 3 for Clean Up without failure.**

The screenshot shows the AWS Security Hub console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, and a search bar. Below the navigation bar, the main heading is 'Welcome to AWS Security Hub'. The page is divided into three main sections: 'Enable AWS Config', 'Security standards', and 'AWS Integrations'. The 'Enable AWS Config' section contains text explaining the need for resource recording in AWS Config and a 'Download' button. The 'Security standards' section lists three standards with checkboxes: 'Enable AWS Foundational Security Best Practices v1.0.0' (checked), 'Enable CIS AWS Foundations Benchmark v1.2.0' (checked), and 'Enable PCI DSS v3.2.1' (unchecked). The 'AWS Integrations' section contains text about importing findings and a 'Learn more' link. At the bottom right, there are two buttons: 'Cancel' and 'Enable Security Hub', with the latter being highlighted by a red rectangular box.

If you see the below warning after activating the Security Hub, kindly ignore.

 **AWS Config is not appropriately enabled on some accounts**
AWS Config is required for Security Hub's security checks. Review remediation steps for the related findings for CIS 2.5. If you recently enabled AWS Config, note that it can take up to 12 hours for Security Hub to detect the change.

Related findings

Step 3 (Clean-Up)

As Security Hub is eligible for 30 Days free trial, it is advisable to disable the service after you have completed the ongoing tutorial or else you will incur a cost. Go to Security Hub, select **Settings** in the left pane & then switch to **General Tab**. At the bottom page, you will find the option to **Disable AWS Security Hub**, as shown below.

The image shows two screenshots of the AWS Security Hub console. The top screenshot displays the 'Summary' page, which provides an overview of findings and integrations. The bottom screenshot shows the 'Settings' page, specifically the 'General' tab, where users can manage controls, permissions, and policies, and importantly, have the option to 'Disable AWS Security Hub'.

Summary Page:

- Insights:** A table showing the number of results for various security insights.
- Latest findings from AWS integrations:** A list of findings from integrated services, all showing 'No findings'.

Insights	Results
1. AWS resources with the most findings	0
2. S3 buckets with public write or read permissions	0
3. AMIs that are generating the most findings	0
4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs)	0
5. AWS principals with suspicious access key activity	0

Latest findings from AWS integrations:

- Amazon GuardDuty:** No findings
- Amazon Inspector:** No findings
- Amazon Macie:** No findings
- AWS IAM Access Analyzer:** No findings
- AWS Systems Manager Patch**

Settings Page (General Tab):

- Auto-enable new controls:** ON
- Service permissions:** View service permissions
- Resource policies:** View resource policy
- Disable AWS Security Hub:** Button to disable the service.