A close up of a logo

Description automatically generated

**GuardDuty Delegated Admin Setup In AWS Control Tower**

**Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Effective Date | Summary of Changes |
| 1 | Ankit Sahai | 16-May-2022 | Setup AWS GuardDuty with Delegated Administrator in AWS Control Tower (Run Book) |
|  |  |  |  |

**Table 1: Document History**

**Purpose/Scope**

Standard operating procedure to Setup AWS GuardDuty with Delegated Administrator in AWS Control Tower

Contents

[Overview 3](#_Toc103333162)

[Pre-requisites 3](#_Toc103333163)

[Step by Step Setup of GuardDuty with Delegated Administrator 4](#_Toc103333164)

[Retrieve the Audit Account ID 4](#_Toc103333165)

[Delegate a GuardDuty Administrator 4](#_Toc103333166)

[Setup GuardDuty for the organization 6](#_Toc103333167)

[Explore GuardDuty 8](#_Toc103333168)

# **Overview**

When you use GuardDuty with an AWS Organizations organization, you can designate any account within the organization to be the GuardDuty delegated administrator. Only the organization management account can designate GuardDuty delegated administrators.

An account that is designated as a delegated administrator becomes a GuardDuty administrator account, has GuardDuty automatically enabled in the designated Region, and is granted permission to enable and manage GuardDuty for all accounts in the organization within that Region. The other accounts in the organization can be viewed and added as GuardDuty member accounts associated with the delegated administrator account.

# **Pre-requisites**

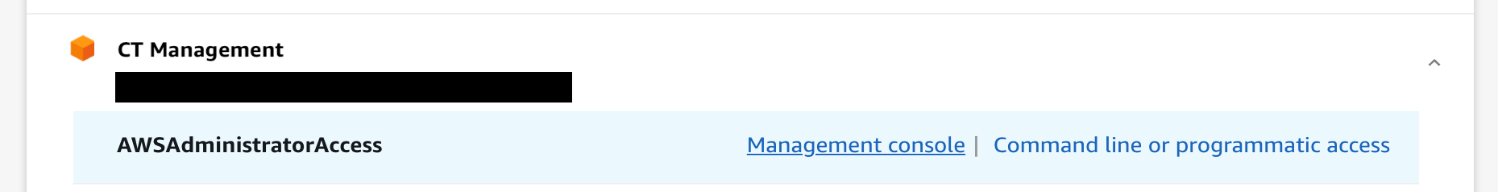
You will need administrator level access to both the AWS Control Tower Management Account and the account where you have designated for security tooling to be setup. It is recommended to use AWS Control Tower Audit Account, but if you have a separate security account you can substitute that in its place.

In this document we are going to administer and deploy AWS GuardDuty in 1 region, referred to as Home Region, and will be using N.Virginia. If you wish to deploy in different or additional regions, substitute your regions for the ones in this document where applicable.

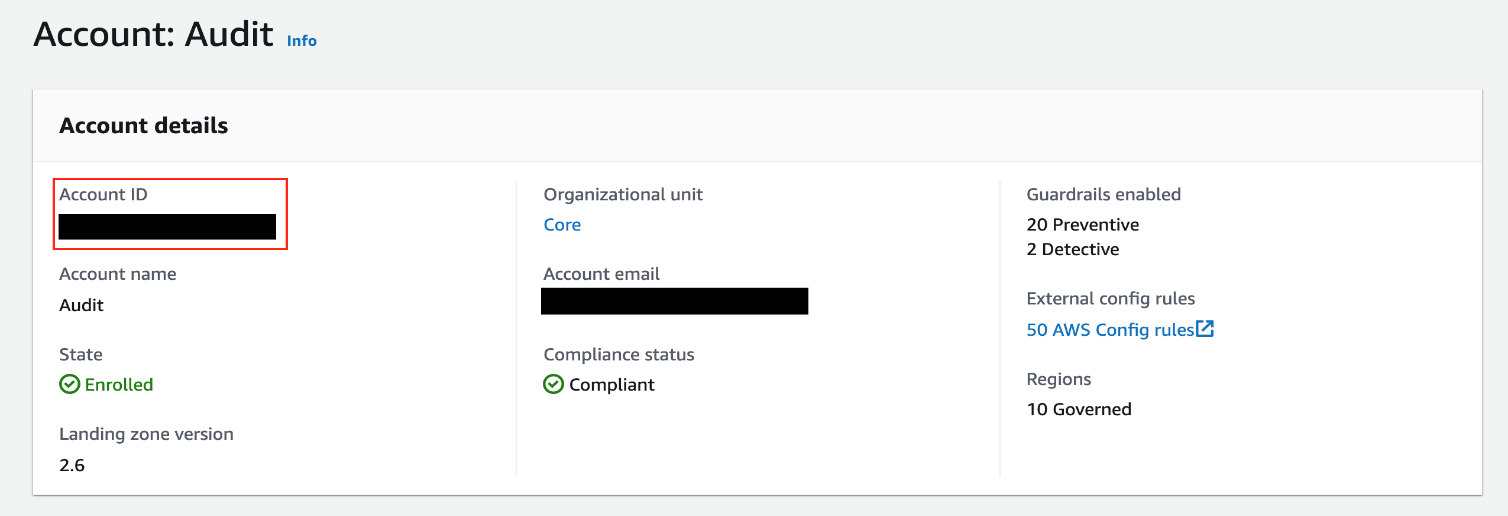
# **Step by Step Setup of Security Hub with Delegated Administrator**

## ***Retrieve the Audit Account ID***

* Login to your AWS Control Tower Management Account with Administrator Access.

****

* Go to the Control Tower Dashboard.
* In the left side-bar, click on Accounts.
* In the account list, find your Audit Account and click on it to get its details.
* In the account details, note the Audit Account’s Account ID. You will use it later.



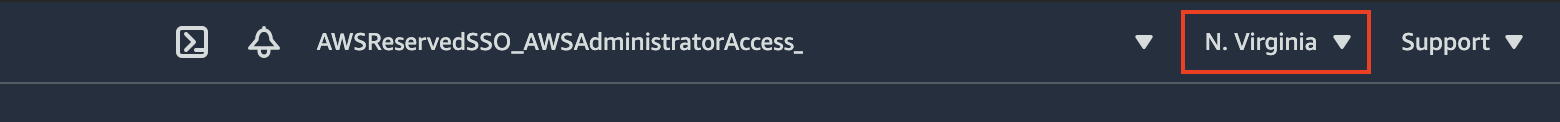
**Note:** You can use any other account also as a delegated administrator for AWS GuardDuty, which is part of your Control Tower.

## ***Delegate a GuardDuty Administrator***

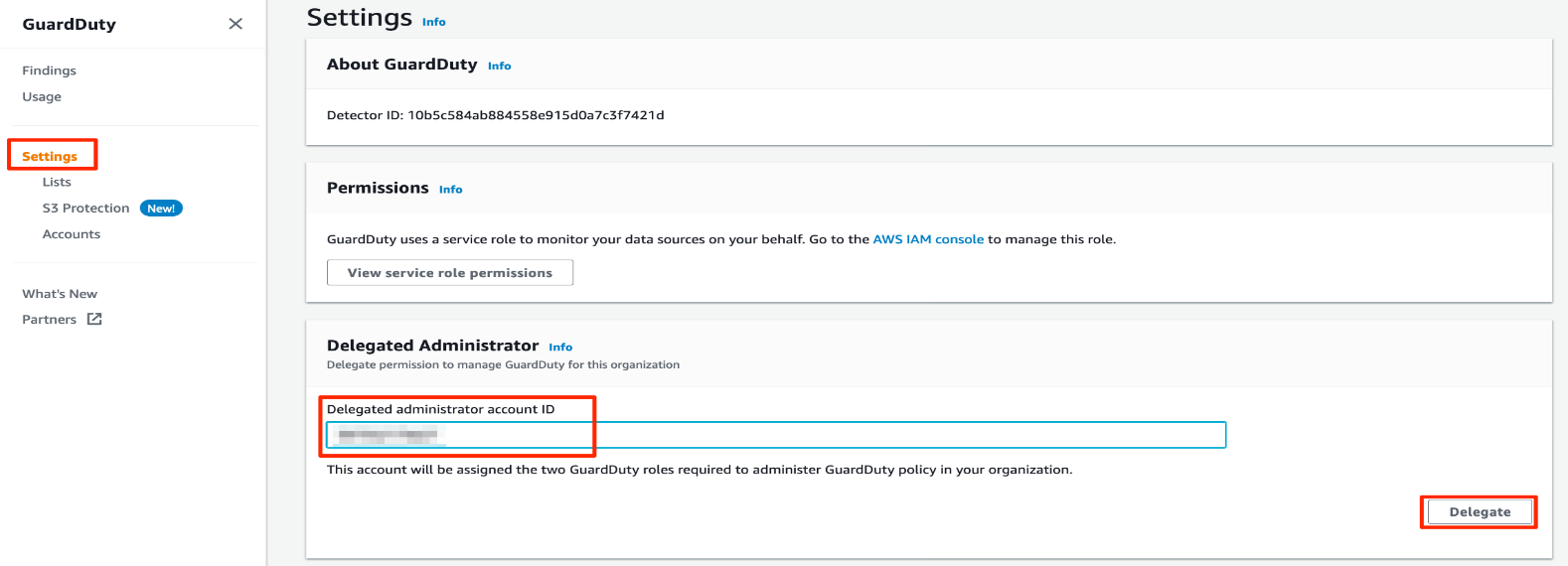
Now you will set up our GuardDuty Delegated Administrator. This process will move the administration of GuardDuty out of the Management Account and into the Audit account, so your security teams can access and manage it.

**Note:** GuardDuty is a region-based service. You will need to make sure you complete the following steps in each region to delegate GuardDuty administration in all the regions that you wish to run it. In this document we want to run GuardDuty in a Home region of N.Virginia (us-east-1), and will complete the steps in this region only. If you wish to deploy in different or additional regions, substitute your regions for the ones in the document where applicable.

* This step is performed in your AWS Control Tower Management Account.
* Go to the GuardDuty Console
* In the region selector in the top bar, check that the region is set to your **Home** region.



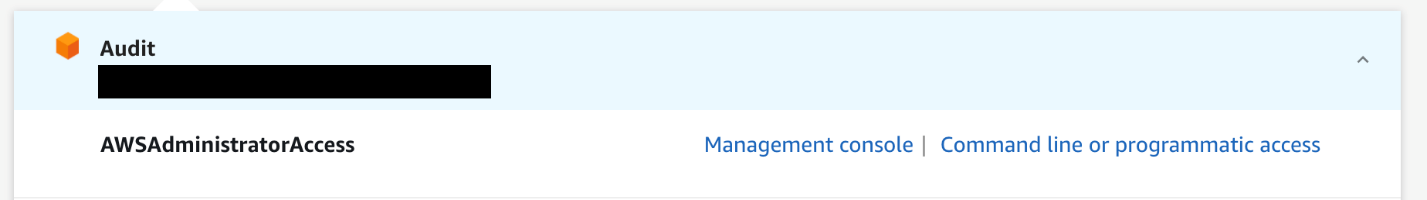
* Click Settings from the sidebar.
* On **Delegated Administrator** section
* **Delegated administrator account ID** : enter the Audit account id
* Click **Delegate**



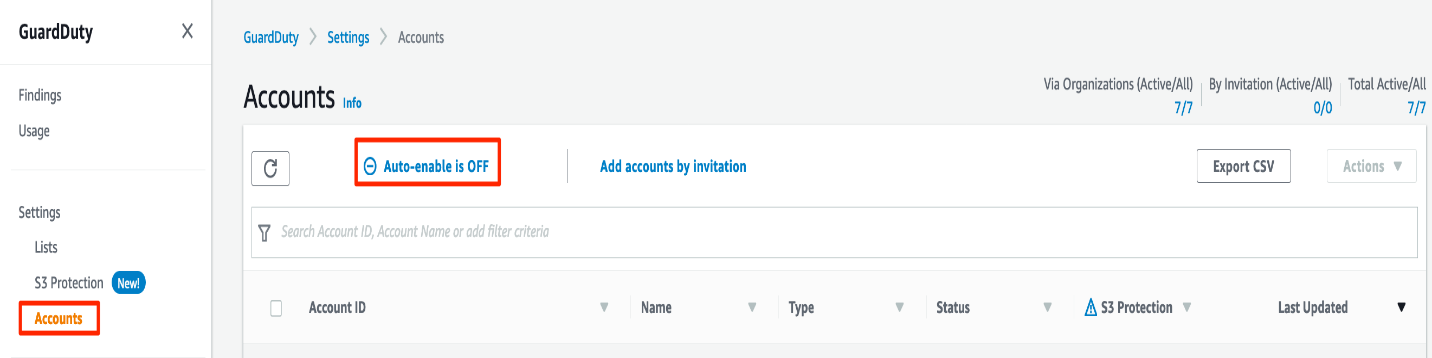
## ***Setup GuardDuty for the organization***

In this step you will enable GuardDuty in the accounts that you already have provisioned, and then enable the Organizations integration with GuardDuty to allow newly vended accounts to automatically be enrolled in GuardDuty.

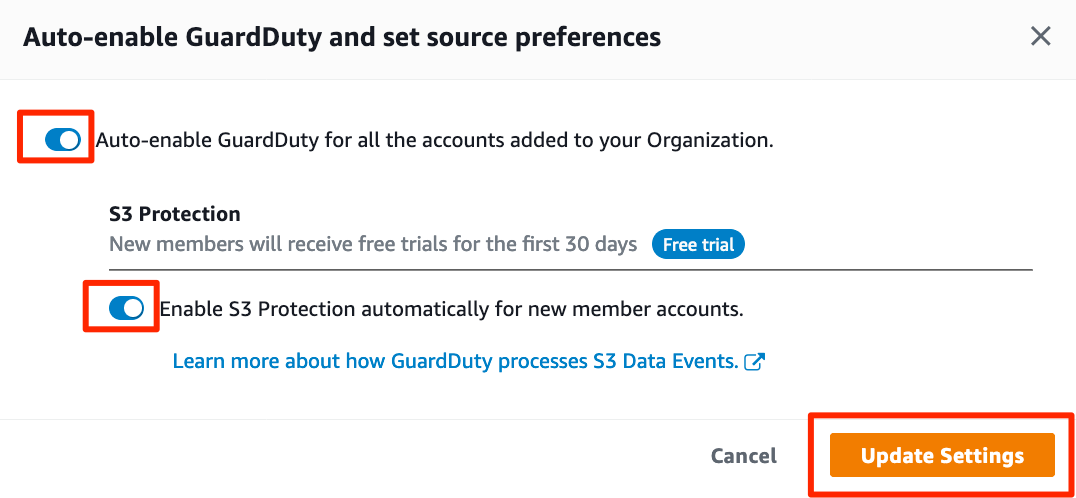
* Switch to your Audit Account with AdministratorAccess.

****

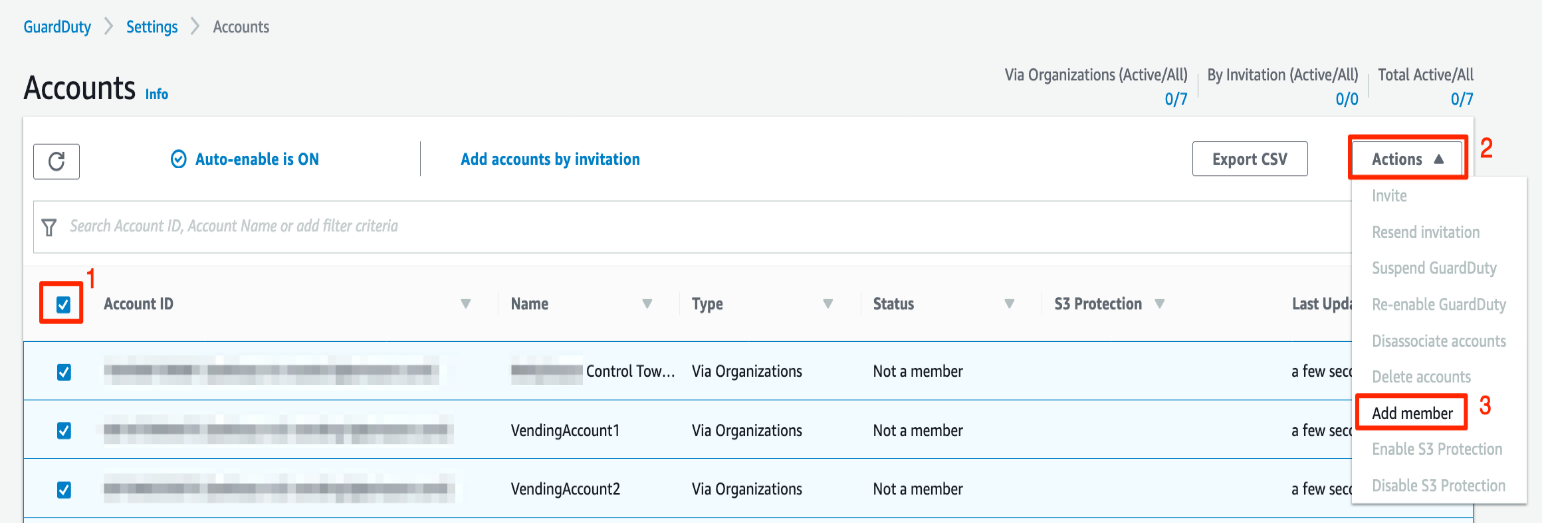
* Go to the GuardDuty Console.
* Click Accounts from the sidebar.
* Select the toggle Auto-enable

****

* Select \*\*Auto-enable GuardDuty for all the accounts added to your Organization
* Optional select \*\*Enable S3 Protection automatically for new member accounts
* Click **Update Settings**

****

* Still on the **Accounts** section.
* Click the checkbox on the table header to select all accounts
* Select Action from the drop-down menu
* Select Add member
* Click **Add member** to confirm



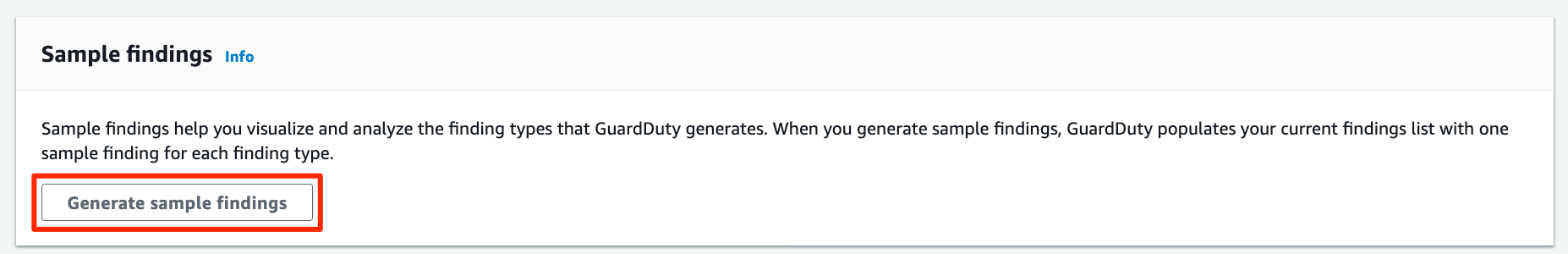
* It will take a few seconds to activate GuardDuty, click on the refresh button to confirm GuardDuty enabled on all accounts.

**Note:** All existing accounts now has GuardDuty enabled and will send the findings into Audit account. Newly vended accounts from AWS Control Tower will have GuardDuty enabled automatically.

## ***Explore GuardDuty***

In this section, we will generate sample GuardDuty findings and explore it in GuardDuty console.

* Continue from the GuardDuty dashboard on the Audit account.
* Click on **Settings** from the sidebar.
* On the **Sample findings** section, Click on **Generate sample findings**.

****

* Click on **Findings** from the sidebar.
* You will now see a variety of sample findings listed in the table, the sample ones you generated above will be prefixed with **[SAMPLE]**.

