



# Tenable Vulnerability Management and Amazon Web Services Integration Guide

Last Revised: April 28, 2025



# Table of Contents

<b>Welcome to AWS for Tenable Vulnerability Management</b> .....	<b>3</b>
<b>Integration Requirements</b> .....	<b>4</b>
<b>Integration Configuration</b> .....	<b>5</b>
Tenable Nessus BYOL Scanner .....	5
Activate the Nessus BYOL Scanner .....	9
Activate Tenable Nessus BYOL Scanner via the Command Line .....	10
Copy or Regenerate Tenable Vulnerability Management Linking Key .....	11
Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management .....	12
Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line .....	15
Link a BYOL Scanner to Tenable Vulnerability Management with Pre-Authorized Scanner Features .....	16
Optional Configuration .....	17
Create a Scan .....	18
View Scan Results in Tenable Vulnerability Management .....	18
Audit the AWS Environment .....	18
Create a Read-Only Group in AWS .....	19
Create a Scanning User in AWS .....	21
Configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management .....	24
View Audit Details in the Scan Results .....	25
AWS Audit Troubleshooting .....	26
<b>Security Hub</b> .....	<b>29</b>
Requirements .....	29



---

## Welcome to AWS for Tenable Vulnerability Management

---

This document describes how to deploy Tenable Vulnerability Management® for integration with Amazon Web Services.

With more than one million users, Tenable Nessus® is the world's most widely deployed vulnerability, configuration, and compliance assessment product. Tenable Nessus prevents attacks by identifying the vulnerabilities, configuration issues, and malware that hackers could use to penetrate your network. It is as important to run these assessments in AWS as it is in any other IT environment. Amazon recommends that all new and existing AWS customers scan their AWS instances while in development and operations and before publishing to AWS users. The AWS Connector provides real-time visibility and inventory of EC2 assets in AWS by querying the AWS API.

**Note:** To manage existing AWS connectors, see [Manage Connectors](#) in the *Tenable Vulnerability Management User Guide*.

**Tip:** For common connector errors, see [Connectors](#) in the Tenable Developer Portal.



---

## Integration Requirements

---

The following are required in order to integrate Tenable Vulnerability Management with AWS:

- **Tenable Vulnerability Management account**

To purchase a Tenable Vulnerability Management account or set up a free evaluation, visit <http://www.tenable.com/products/tenable-io>.

- **AWS account**

To create a free account, visit <https://aws.amazon.com/start-now>.

- **Internet connection**



# Integration Configuration

To configure AWS for Tenable Vulnerability Management, see the following integration configuration topics:

1. [Tenable Nessus BYOL Scanner](#)
  - a. [Activate the Nessus BYOL Scanner](#)
    - [Activate Tenable Nessus BYOL Scanner via the Command Line](#)
  - b. [Copy or Regenerate Tenable Vulnerability Management Linking Key](#)
  - c. [Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management](#)
    - [Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line](#)
  - d. [Optional Configuration](#)
2. [Create a Scan](#)
  - [View Scan Results in Tenable Vulnerability Management](#)
3. [Audit the AWS Environment](#)
  - [AWS Audit Troubleshooting](#)

## Tenable Nessus BYOL Scanner

The following instructions describe how to configure a Tenable Nessus Bring Your Own License (BYOL) Amazon Web Services (AWS) scanner. Each section includes steps for configuring the scanner via the user interface or via the command line.

**Note:** For more information on advanced settings for Tenable Nessus (for example, security group configuration), see [Advanced Settings](#) in the *Tenable Nessus User Guide*.

Before you begin:

- Ensure that your system meets the [hardware requirements](#) described in the *Tenable Nessus User Guide*.

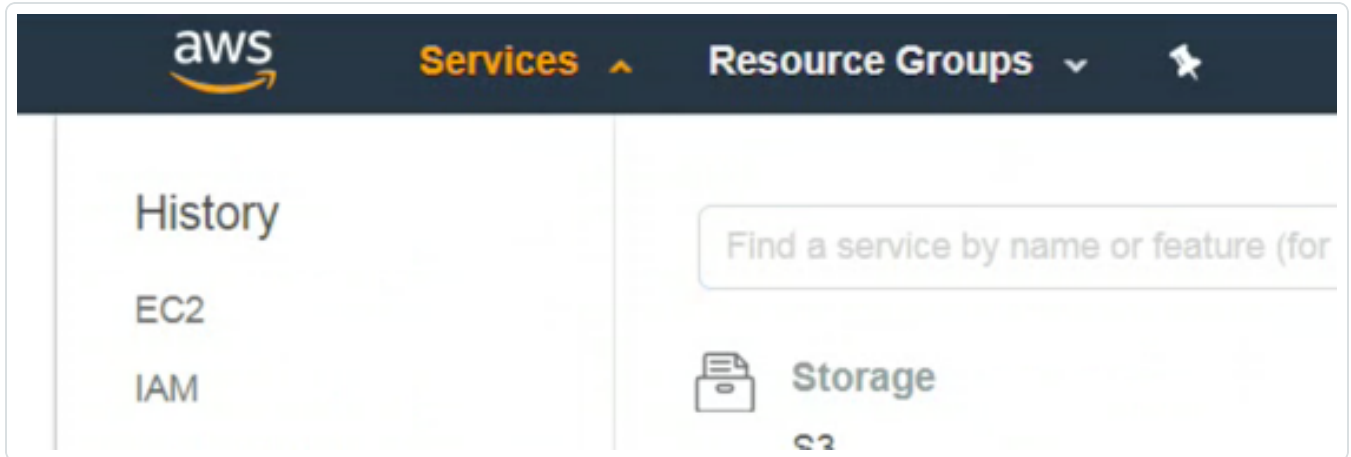
To configure the Nessus BYOL Scanner in AWS:



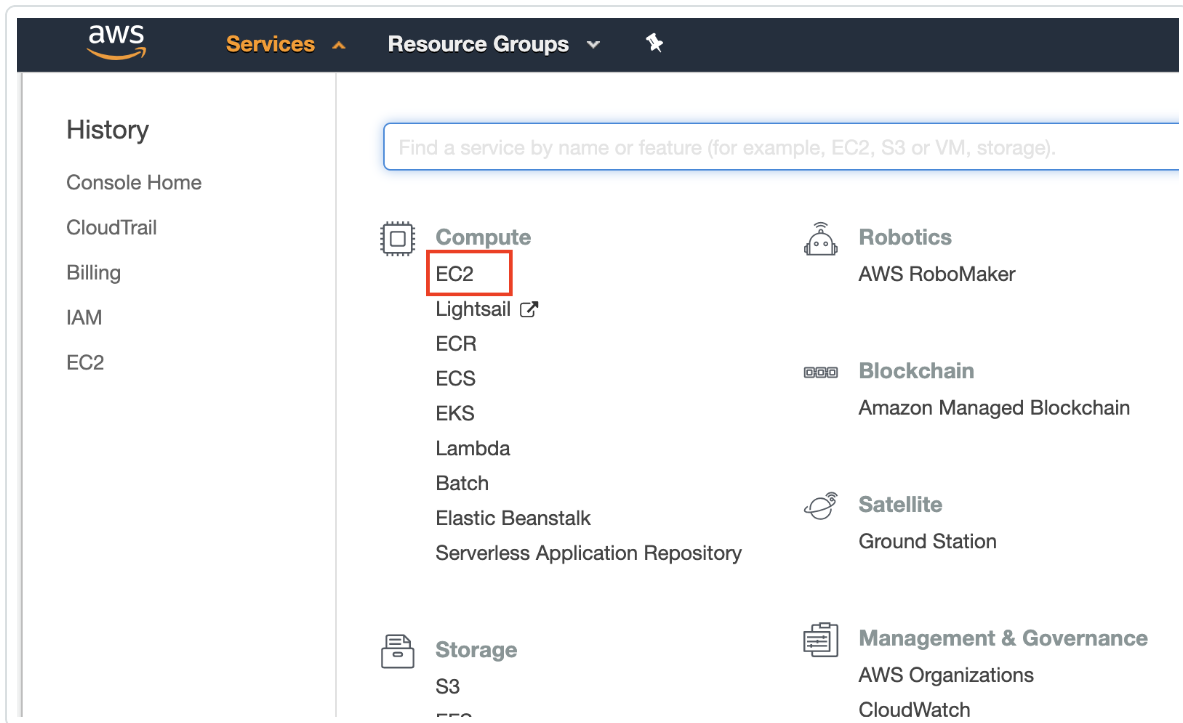
1. Log in to the AWS Management Console.
2. In the top menu bar, click **Services**.

The **Services** page appears.

**Note:** Amazon is continually updating their service, so screenshots may differ from the AWS interface you see.



3. In the **Compute** section, click **EC2**.



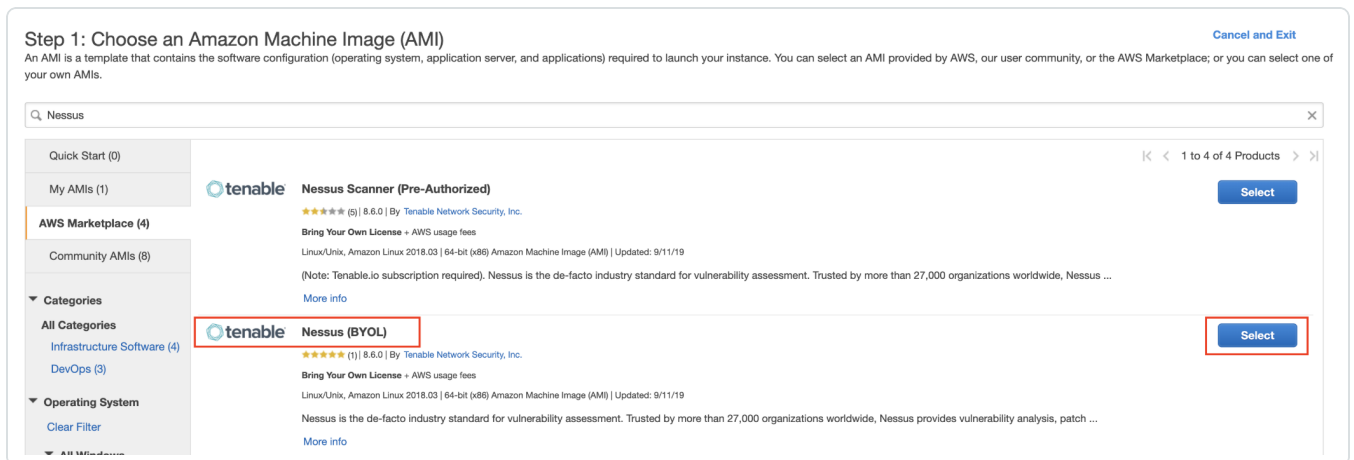


The **EC2 Dashboard** appears.

4. In the **Create Instance** section, click **Launch Instance**.

The **Choose an Amazon Machine Image (AMI)** page appears.

5. In the left panel, click **AWS Marketplace**.
6. In the search box, type **Nessus**.
7. On your keyboard, press **Enter**.
8. In the **Nessus (BYOL)** section, click **Select**.



The **Nessus (BYOL)** review window appears.

9. Review the pricing details and instance type details.
10. Click **Continue**.

The **Step 2: Choose an Instance Type** page appears.

11. Click **Next: Configure Instance Details**.

The **Step 3: Configure Instance Details** page appears.

12. Configure the instance details according to your company-specific preferences.

**Note:** Your system must also:

- Meet the [hardware requirements](#) described in the *Tenable Nessus User Guide*.
- Include an internet connection with which to access Tenable Vulnerability Management.



13. Click **Next: Add Storage**.

The **Step 4: Add Storage** page appears.

14. Configure the storage details according to your company-specific preferences.

15. Click **Next: Add Tags**.

The **Step 5: Add Tags** page appears.

16. (Optional) Configure tags according to your company-specific preferences.

17. Click **Next: Configure Security Group**.

The **Step 6: Configure Security Group** page appears.

18. (Optional) Configure the security group details according to your company-specific preferences.

19. Click **Review and Launch**.

The **Review Instance** page appears.

20. Click **Launch**.

A key pair page appears.

### Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair ▾

**Key pair name**  
myNessusKey

**Download Key Pair**

**You have to download the private key file (\*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.**

**Cancel** **Launch Instances**





21. Do one of the following:

- If you have access to an existing key pair, select **Choose an existing key pair**.
  - a. In the **Select a key pair** section, select the key pair you want to use.
  - b. Select the acknowledge checkbox.
- If you do not have access to an existing key pair, select **Create a new key pair**.
  - a. In the **Key pair name** box, type a name for the key pair.
  - b. Click **Download Key Pair**.

**Tip:** You need this key pair to access the Nessus Professional BYOL scanner from the command line for activation/registration. For more information, see [Activate Tenable Nessus BYOL Scanner via the Command Line](#).

22. Click **Launch Instances**.

The **Launch Status** page appears. AWS begins a validation process for the new Nessus BYOL EC2 Instance and proceeds to pass health checks.

23. Click **View Instances** to confirm the instance appears successfully.

**Note:** When the status checks are complete, take note of the public IP (if applicable) of the Nessus BYOL instance. Otherwise, you need a Bastion host to access the command line to continue configuration of the Nessus BYOL Scanner.

## Activate the Nessus BYOL Scanner

Before you begin:

- View the login and instance-type information in the [Nessus BYOL Scanner](#) documentation.

To activate the Tenable Nessus BYOL Scanner (Tenable Nessus Expert or Tenable Nessus Professional):

1. Navigate to the Tenable Nessus user interface on Port 8834, for example, `https://<NessusBYOL-IP>:8834`, where `<BYOLpublicIP>` is the IP address of your Tenable Nessus Expert or Tenable Nessus Professional instance.



The **Welcome to Tenable Nessus** page appears.

2. Select Tenable Nessus Expert or Tenable Nessus Professional.
3. Click **Continue**.

The **Register Tenable Nessus** page appears.

4. In the **Activation Code** box, type your Tenable Nessus Expert or Tenable Nessus Professional activation code.
5. Click **Continue**.

Activation begins and plugins download. For more information, see the [Nessus User Guide](#).

## Activate Tenable Nessus BYOL Scanner via the Command Line

To activate the Tenable Nessus Professional BYOL scanner via the command line:

1. Adjust the permissions for your downloaded SSH Key using the following command:

```
chmod 400 myNessusKey.pem
```

2. SSH into the Nessus BYOL scanner using the following command:

```
ssh -i myNessusKey.pem ec2-user@<BYOLpublicIP>
```

Where *<BYOLpublicIP>* is the IP address of your Tenable Nessus Professional instance.

3. Elevate privileges using the following command:

```
sudo su
```

4. Update the AMI using the following command:

```
yum update -y
```

5. Stop Tenable Nessus using the following command:

```
service nessusd stop
```

6. Register the scanner with your Tenable Nessus Professional activation code using the following command:

```
/opt/nessus/sbin/nessuscli fetch --register <ACTIVATION CODE>
```



Where <ACTIVATION CODE> is the activation code for your instance.

7. Start Tenable Nessus using the following command:

```
service nessusd start
```

## Copy or Regenerate Tenable Vulnerability Management Linking Key

**Required User Role:** Administrator

Under certain circumstances, you may need to regenerate the linking key for your Tenable Vulnerability Management instance. For example, you may regenerate the key for security reasons if an employee with knowledge of the linking key leaves your organization.

Regenerating a linking key does not affect sensors that are currently linked to Tenable Vulnerability Management, because the linking key is only used to establish the initial link. After you link a sensor, the sensor connects to Tenable Vulnerability Management using unique credentials.

If your organization has hard-coded a linking key into implementation scripts, keep in mind the following:

- Be sure to replace the original key with the regenerated key to prevent script failure.
- Each Tenable Vulnerability Management instance uses a single linking key for all sensor types. If you regenerate the linking key while working with one type of sensor (for example, Tenable Nessus scanners), you also regenerate the linking key for the other sensor types. If you regenerate the linking key, be sure to update the implementation for scripts involving all types of sensors.

**Note:** To learn more about linking keys, see [Sensor Security](#) in the *Tenable Vulnerability Management User Guide*.

**Note:** These steps only apply if registering the Nessus BYOL scanner to be linked to and managed by Tenable Vulnerability Management.

To copy or regenerate the Tenable Vulnerability Management linking key:

1. Log in to <https://cloud.tenable.com>.
2. In the left navigation pane, click **Sensors**.



The **Sensors** page appears.

3. Click any sensor type tab (for example, **Nessus Scanner**).

The appropriate sensor page appears.

4. Click the **+** **Add [Sensor Type]** button (for example, **Add Nessus Scanner**).

The appropriate sensor plane appears (for example, **Add Nessus Scanner**).

5. In the **Add [Sensor Type]** plane, click the **Copy** or the **Regenerate** button.

A confirmation window appears.

6. If regenerating the linking key, in the confirmation window, click **Regenerate**.

The **Regenerated Linking Key** message appears, and the new linking key replaces the original linking key in the **Add [Sensor Type]** plane.

7. Copy and save the **Linking Key**.

## Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management

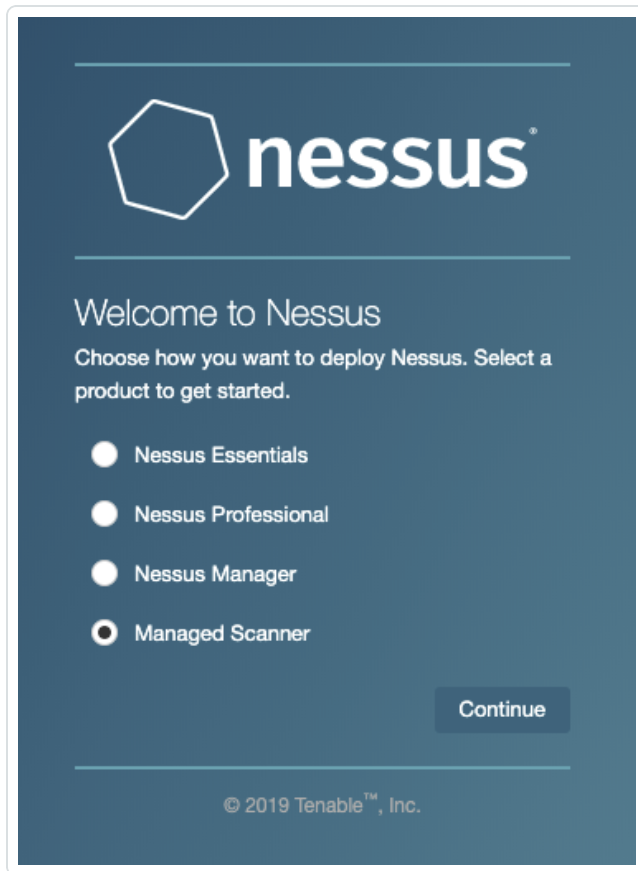
To activate the Tenable Nessus BYOL Scanner linked to and managed by Tenable Vulnerability Management:

1. Navigate to the Tenable Nessus user interface on Port 8834, for example, <https://<NessusBYOL-IP>:8834>.

The **Welcome to Tenable Nessus** page appears.

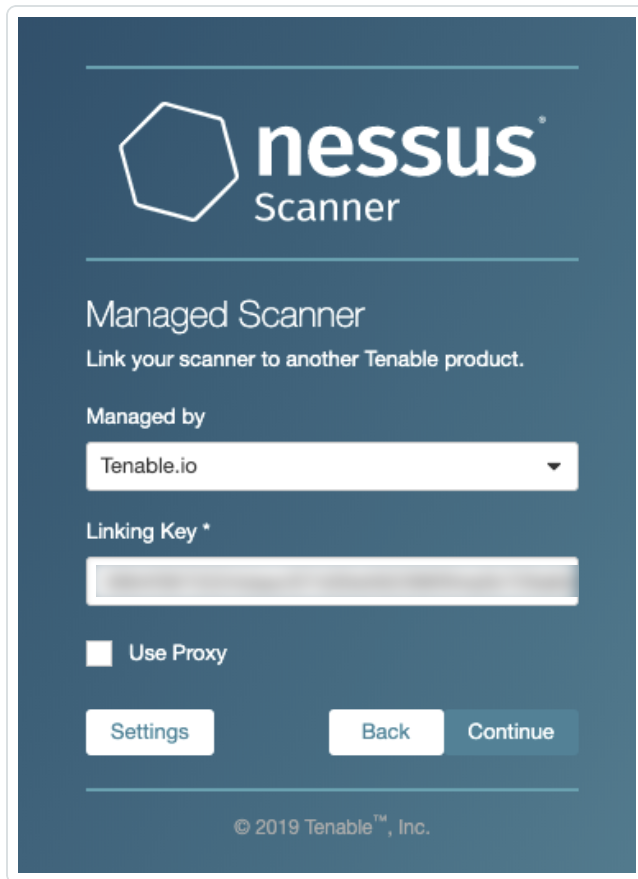
---

2. Select **Managed Scanner**.



3. Click **Continue**.

The **Managed Scanner** page appears.



4. From the **Managed by** drop-down box, select **Tenable Vulnerability Management**.
5. In the **Linking Key** box, paste the linking key copied in the [Copy or Regenerate Tenable Vulnerability Management Linking Key](#) section.
6. Click **Continue**.

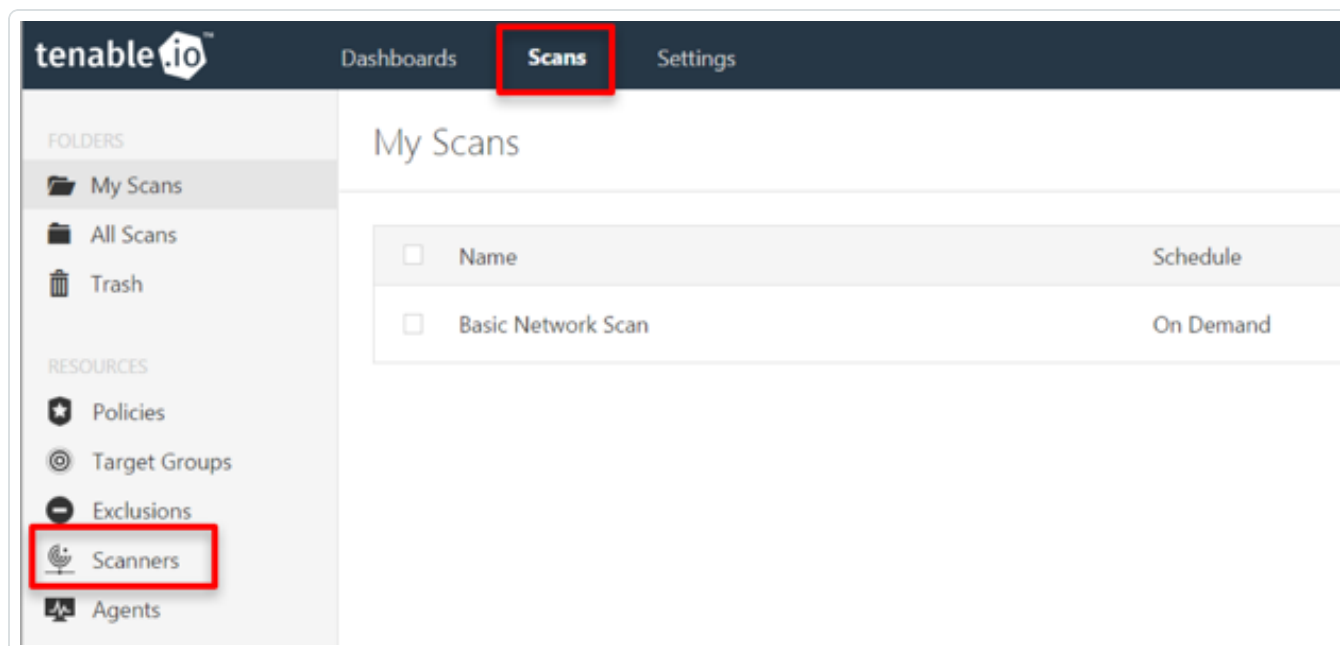
Tenable Vulnerability Management begins managing Tenable Nessus and plugins begin downloading. For more information, see the [Nessus User Guide](#).

To confirm the Nessus BYOL Scanner in Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
2. In the top menu bar, click **Scans**.

The **My Scans** page appears.

3. In the left-hand menu, click **Scanners**.



The **Scanners** page appears. Confirm the BYOL Scanner appears in the **Linked Scanners** list.

## Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line

To link the Tenable Nessus BYOL scanner to Tenable Vulnerability Management via the command line:

1. Adjust the permissions for your downloaded SSH Key using the following command:

```
chmod 400 myNessusKey.pem
```

2. SSH into the Nessus BYOL scanner using the following command:

```
ssh -i myNessusKey.pem ec2-user@<BYOLpublicIP>
```

Where <BYOLpublicIP> is the IP address of your Tenable Nessus BYOL instance.

3. Elevate privileges using the following command:

```
sudo su
```

4. Update the AMI using the following command:

```
yum update -y
```



5. Stop Tenable Nessus using the following command:

```
service nessusd stop
```

6. Link the Nessus BYOL scanner to Tenable Vulnerability Management for management using the following command:

```
/opt/nessus/sbin/nessuscli managed link --key=<key> --cloud
```

Where <key> is the linking key associated with your Tenable Vulnerability Management instance.

**Note:** FedRAMP customers must use the following command:

```
/opt/nessus/sbin/nessuscli managed link --key=<key> -  
host=fedcloud.tenable.com --port=443
```

7. Start Tenable Nessus using the following command:

```
service nessusd start
```

## Link a BYOL Scanner to Tenable Vulnerability Management with Pre-Authorized Scanner Features

You can retain your pre-authorized AMI installation features when linking BYOL scanners to Tenable Vulnerability Management by using the following procedure.

**Note:** This feature is only available for Nessus versions 10.2.0 and later.

**Caution:** If you plan to downgrade a 10.2 Nessus scanner that was linked with the AWS scanner flag (see the following steps) to version 10.1.x or earlier, you need to manually unlink and relink the scanner after downgrading. Otherwise, Tenable Vulnerability Management does not recognize the scanner.

Before you begin:

Assign an IAM role to the Tenable Nessus instance you are deploying.

To link a BYOL scanner to Tenable Vulnerability Management with pre-authorized scanner features:





When you link the scanner to Tenable Vulnerability Management using the command line, as described in the [Link to Tenable Vulnerability Management](#) topic in the *Tenable Nessus User Guide*, use the optional `--aws-scanner` flag. For example:

```
> nessuscli managed link --key=<LINKING KEY> --cloud --aws-scanner
```

**Note:** The scanner must already be running on an AWS instance for the flag to take effect.

## Optional Configuration

In addition to manual configuration, you can use a bootstrap script to configure the Tenable Nessus BYOL scanner. The following screenshot shows an example of using a bootstrap Script during Nessus BYOL Configuration:

### Step 3: Configure Instance Details

<b>IAM role</b> ⓘ	None	<a href="#">Create new IAM role</a>
<b>Shutdown behavior</b> ⓘ	Stop	
<b>Enable termination protection</b> ⓘ	<input type="checkbox"/> Protect against accidental termination	
<b>Monitoring</b> ⓘ	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	
<b>Tenancy</b> ⓘ	Shared - Run a shared hardware instance	<a href="#">Additional charges will apply for dedicated tenancy.</a>
<b>Elastic Inference</b> ⓘ	<input type="checkbox"/> Add an Elastic Inference accelerator <a href="#">Additional charges apply.</a>	
<b>T2/T3 Unlimited</b> ⓘ	<input type="checkbox"/> Enable <a href="#">Additional charges may apply</a>	
<b>Advanced Details</b>		
<b>User data</b> ⓘ	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded	
	<pre>#!/bin/bash yum update -y service nessusd stop /opt/nessus/sbin/nessuscli managed link --key=&lt;insert-key-here&gt; --cloud service nessusd start</pre>	

Copy the following bootstrap script:



```
#!/bin/bash
yum update -y
service nessusd stop
/opt/nessus/sbin/nessuscli managed link --key=<insert-key-here> --cloud
service nessusd start
```

## Create a Scan

Follow the [Create a Scan](#) steps in the Tenable Vulnerability Management User Guide.

## View Scan Results in Tenable Vulnerability Management

Do one of the following:

- To view scan results, click on the completed scan.
- To view more details about the scan results, click the **Vulnerabilities** tab.

The screenshot displays the 'AWS Basic Network Scan' interface. At the top right, there are buttons for 'Configure', 'Launch', 'Audit Trail', and 'Export' (highlighted with a red box). Below these are tabs for 'Hosts' (1), 'Vulnerabilities' (23), and 'History' (1). The 'Vulnerabilities' tab is selected and highlighted with a red box. A table shows a host with ID 'i-0534147da4783aa88' and a progress bar indicating 1 high vulnerability and 24 low vulnerabilities. To the right, 'Scan Details' are listed: Name: AWS Basic Network Scan, Status: Completed, Policy: Basic Network Scan, Scanner: AWS\_Scanner\_Test, Start: Today at 3:10 PM, End: Today at 3:14 PM, Elapsed: 4 minutes. At the bottom right, a 'Vulnerabilities' donut chart shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

- To export the results in Nessus, PDF, HTML, CSV, or Nessus DB formats, click the **Export** button in the top-right corner.

## Audit the AWS Environment

You can use Tenable Vulnerability Management to audit the Amazon Web Services environment to detect misconfigurations in your cloud environment and account settings using Tenable



Vulnerability Management. Complete the following steps to configure AWS for successful Audit Cloud Infrastructure assessments with Tenable Vulnerability Management.

**Note:** Tenable recommends that you create a new read-only access AWS account just for Tenable Vulnerability Management. If you experience issues, see [AWS Audit Troubleshooting](#).

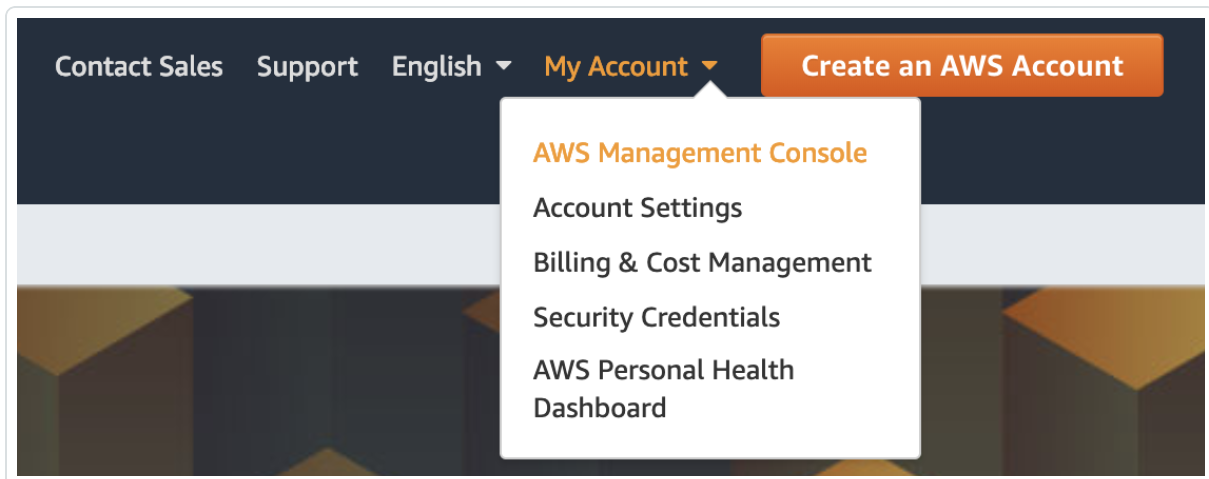
To audit the AWS environment, you must complete the following tasks:

- [Create a Read-Only Group in AWS](#)
- [Create a Scanning User in AWS](#)
- [Configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management](#)
- [View Audit Details in the Scan Results](#)

## Create a Read-Only Group in AWS

To create a read-only group in AWS:

1. Log in to your AWS account.
2. Click **My Account** > **AWS Management Console**.



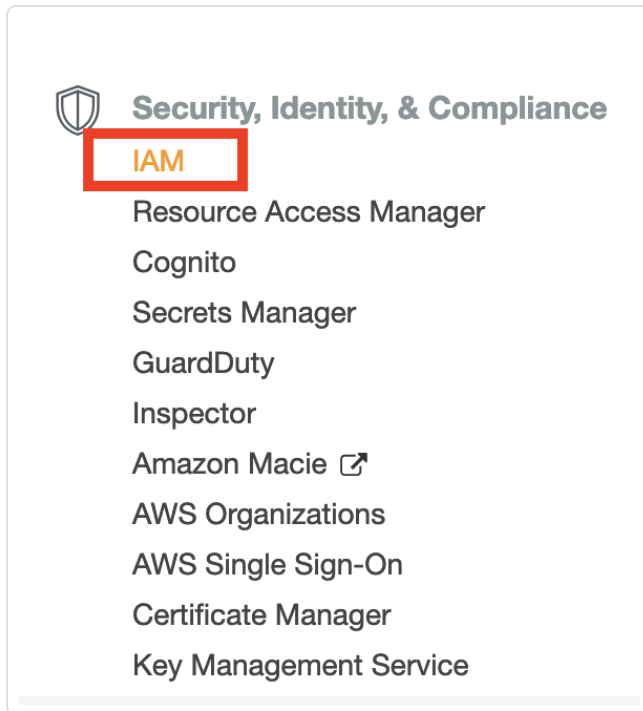
The **AWS Management Console** appears.

3. Click **Services**.

The **Services** page appears.



- In the **Security, Identity, and Compliance** section, click **IAM**.



The **IAM** control panel appears.

- In the left panel, click **Groups**.

The **Groups** page appears.

- Click **Create New Group**.

The **Create New Group Wizard** appears.

- In the **Group Name** box, type a name for the read-only group.

## Set Group Name

Specify a group name. Group names can be edited any time.

**Group Name:**

Example: Developers or ProjectAlpha  
Maximum 128 characters



8. Click **Next Step**.

The **Attach Policy** screen appears.

9. Select the **ReadOnlyAccess** AWS-managed policy.

**Attach Policy**

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ readonly Showing 105 results

	Policy Name ↕	Attached Entities ↕	Creation Time ↕	Edited Time ↕
<input checked="" type="checkbox"/>	ReadOnlyAccess	1	2015-02-06 13:39 EST	2019-02-05 13:19 EST

10. (Optional) On the **Attach Policy** screen, select the **SecurityAudit** AWS-managed policy.

11. Click **Next Step**.

The **Review** page appears.

12. Review the group information.

13. Click **Create Group**.

AWS creates the read-only group.

## Create a Scanning User in AWS

To create a scanning user in AWS:

1. Log in to your AWS account.

2. Click **Users > Add Users**.

The **Add User** page appears.

3. In the **Set user details** section, in the **User name** text box, type a name for the user.



4. In the **Select AWS access type** section, select the **Programmatic access** checkbox.

### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

**User name\***

[+ Add another user](#)

### Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

**Access type\***  **Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

**AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

5. Click **Next: Permissions**.

The **Set permissions** page appears.

6. Click **Add user to group**.



7. In the **Add user to group** section, select the read-only group you previously created.

**Add user** 1 2 3 4 5

▼ Set permissions

**Add user to group** Copy permissions from existing user Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Add user to group**

Create group Refresh

Q Search Showing 1 result

Group ▼	Attached policies
<input checked="" type="checkbox"/> ReadOnly	ReadOnlyAccess and 1 more

8. Click **Next: Tags**.

The **Tags** page appears.

9. (Optional) Configure any tags you want to add to the user profile.

10. Click **Next: Review**.

The **Review** page appears.

11. Review the user profile.

12. Click **Create User**.

An **Access key ID** and **Secret access key** appear.

**Add user**

1 2 3 4 5

✓ **Success**  
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: [https://console.aws.amazon.com/iam/home?#/users](#)

Download .csv

User	Access key ID	Secret access key
▶ ✓ NessusAuditor	A[REDACTED]	***** Show

13. Copy the **Access key ID** and **Secret access key** to use to configure the Audit Cloud Infrastructure in Tenable Vulnerability Management.

## Configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management

To configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the ☰ button.

The left navigation plane appears.

3. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.

The **Scans** page appears.

4. In the upper-right corner of the page, click **+ Create a Scan**.

The **Select a Scan Template** page appears.

5. Click **Audit Cloud Infrastructure**.

The **New Scan** page appears.

6. On the **Settings** tab, type a name for the scan.

7. Set **Scanner Type** to **Tenable Cloud Sensor**.





8. Click the **Compliance** tab.  
The **Compliance** options appear.
9. Click **AMAZON AWS**.
10. Select the appropriate audit files for the scan.  
When you select an audit file, Tenable Vulnerability Management adds the file to the list.
11. Click the **Credentials** tab.  
The **Credentials** options appear.
12. In the **ADD CREDENTIALS** section, select **Amazon AWS**.
13. In the **AWS Access Key ID** text box, type the key you copied in the [Create a Scanning User in AWS](#) section.
14. In the **AWS Secret Key** text box, type the key you copied in the [Create a Scanning User in AWS](#) section.
15. From the **Regions to Access** drop-down box, select the region to which you want to apply the scan.
16. Do one of the following:
  - To save without launching the scan click **Save**.
  - To save and launch the scan immediately, click the drop-down arrow next to **Save** and select **Launch**.

**Tip:** If you experience aborted scans or are unable to find a matching scanner route, you may need to specify a dedicated scanner, and re-scan. For troubleshooting help, see [AWS Audit Troubleshooting](#). For more information on Tenable Vulnerability Management scans, refer to the [Tenable Vulnerability Management User Guide](#).

## View Audit Details in the Scan Results

After the scan completes, you can analyze the results in Tenable Vulnerability Management.

To view audit details in the scan results:



1. Log in to Tenable Vulnerability Management.
2. In the top navigation bar, click **Scans**.
3. Click the AWS Cloud Infrastructure scan you previously created.
4. Click the **Audits** tab.

The screenshot shows the AWS Audit dashboard. At the top, there are tabs for 'Assets', 'Vulnerabilities', 'Audits', and 'History'. The 'Audits' tab is selected and highlighted with a red box, showing a count of 94. Below the tabs, there are three summary cards: 'FAILED' with a count of 65, 'WARNING' with a count of 15, and 'PASSED' with a count of 14. Below these cards is a table of failed audits.

Name	Family	Count
1.10 Ensure IAM password policy prevents password reuse	Amazon AWS Compliance Checks	1
1.11 Ensure IAM password policy expires passwords within 90 days or less	Amazon AWS Compliance Checks	1
1.13 Ensure MFA is enabled for the 'root' account	Amazon AWS Compliance Checks	1
1.14 Ensure hardware MFA is enabled for the 'root' account	Amazon AWS Compliance Checks	1
1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password 'AccountMFAEnabled'	Amazon AWS Compliance Checks	1

5. Click an audit in the table to view audit details, including the **Description**, **Reference Information**, and **Solution**.

The screenshot shows the details page for the audit '1.10 Ensure IAM password policy prevents password reuse'. The page is divided into three main sections: 'Description', 'Solution', and 'Reference Information'. The 'Description' section explains that IAM password policies can prevent password reuse and that preventing reuse increases account resiliency. The 'Solution' section provides instructions on how to set the password policy via the AWS Console and CLI. The 'Reference Information' section lists various standards and frameworks that this audit is based on.

**Description**

IAM password policies can prevent the reuse of a given password by the same user. It is recommended that the password policy prevent the reuse of passwords.

Preventing password reuse increases account resiliency against brute force login attempts.

**Solution**

Perform the following to set the password policy as prescribed:

Via AWS Console

1. Login to AWS Console (with appropriate permissions to View Identity Access Management Account Settings)
2. Go to IAM Service on the AWS Console
3. Click on Account Settings on the Left Pane
4. Check 'Prevent password reuse'
5. Set 'Number of passwords to remember' is set to '24'

Via CLI

```
aws iam update-account-password-policy --password-reuse-prevention 24
```

Note: All commands starting with 'aws iam update-account-password-policy' can be combined into a single command.

**Reference Information**

- 800-171: 3.5.8
- 800-53: IA-5
- CCE: CCE-78908-1
- CSCV6: 4.4
- CSF: PR.AC-1
- ISO/IEC-27001: A.9.4.3
- ITSG-33: IA-5
- LEVEL: 1S
- NESA: T5.2.3
- NIAV2: AM22c
- SWIFT-CSCV1: 4.1
- TBA-FIISB: 26.2.3

## AWS Audit Troubleshooting

If you encounter issues while running the Audit Cloud Infrastructure scan, first, check the following:



- User configuration or permissions issues with the AWS account.
- AWS networking mechanisms that potentially block Tenable Vulnerability Management scan attempts.

If necessary, enable debug logging and contact Tenable Support for troubleshooting assistance.

To enable debug logging for the Audit Cloud Infrastructure scan:

1. Navigate to the **Audit Cloud Infrastructure** scan you created in [Audit the AWS Environment](#).
2. On the **Settings** tab, click **Advanced**.
3. In the **Debug Settings** section, select the **Enable plugin debugging** checkbox.
4. Do one of the following:
  - To save without launching the scan click **Save**.
  - To save and launch the scan immediately, click the drop-down arrow next to **Save** and select **Launch**.
5. In the top navigation bar, click **Scans**.
6. Click the row for the Audit Cloud Infrastructure scan you created.
7. Click the **Assets** tab.

The **Assets** information appears.

8. Click the AWS Account asset.

**Note:** This asset always has a loopback address of 127.0.0.1.

9. In the **Asset Details** section, next to **Scan DB**, click **Download**.

The screenshot shows the 'Vulnerabilities' section with a table of scan results. The table has columns for Severity, Name, Family, and Count. A single entry is shown: 'Debugging Log Report' with a count of 1. To the right of the table is the 'Asset Details' section, which includes fields for IP (127.0.0.1), Start (February 28 at 9:52 PM), End (February 28 at 9:54 PM), Elapsed (2 minutes), and KB (Download). The 'Scan DB' section has a 'Download' button highlighted with a red box.

Severity	Name	Family	Count
	<a href="#">New</a> Debugging Log Report	Settings	1

**Asset Details**

IP: 127.0.0.1  
Start: February 28 at 9:52 PM  
End: February 28 at 9:54 PM  
Elapsed: 2 minutes  
KB: [Download](#)

Scan DB: [Download](#)

The **Export** window appears.



10. In the **Password** box, type the password you want to use to encrypt the **Scan DB** file.
11. Contact Tenable Support and provide the .db log file and the encryption password.



## Security Hub

Through the use and configuration of the Tenable Vulnerability Management to AWS Security Hub Transformer, Tenable Vulnerability Management can send vulnerabilities to AWS Security Hub. This tool consumes Tenable Vulnerability Management asset and vulnerability data, transforms that data into the AWS Security Hub Finding format, and then uploads the resulting data into AWS Security Hub.

**Note:** The script does not need to be run in AWS.

The tool can be run either as a one-shot docker container or as a command line tool:

- To run as a docker image, you must build the image and then pass the necessary secrets on to the container.
- To run as a command line tool, you must install the required python modules and then run the tool using either environment variables or by passing the required parameters as run-time parameters.

## Requirements

- Tenable Vulnerability Management account
- Tenable Vulnerability Management AWS connector enabled and configured
- AWS Security Hub
- Tenable Vulnerability Management Provider enabled and configured in Security Hub

### Download Tenable + AWS Security Hub Transformer

In order to consume Tenable Vulnerability Management asset and vulnerability data, transform that data into the AWS Security Hub Finding format, and then upload the resulting data into AWS Security Hub, you need the transformer tool. Download the tool [here](#).

### Installation

To build the Docker image, run the following script:

```
docker build -t tio2sechub:latest .
```



To install python requirements, run the following script:

```
pip install -r requirements.txt
```

### Enable Script in Security Hub

1. Log in to Security Hub.
2. If you have not yet enabled Security Hub, click **Enable Security Hub**.
3. Navigate to **Settings > Providers**.
4. In the **Search** box, type *Tenable*.
5. Click **Configure**.

Your account subscribes to accept events from the script.

### Configuration

The following lists the command line arguments as well as the equivalent environment variables:

```
usage: sechubingest.py [-h] [--tio-access-key TIO_ACCESS_KEY]
                        [--tio-secret-key TIO_SECRET_KEY]
                        [--batch-size BATCH_SIZE] [--aws-region
AWS_REGION]
                        [--aws-account-id AWS_ACCOUNT_ID]
                        [--aws-access-id AWS_ACCESS_ID]
                        [--aws-secret-key AWS_SECRET_KEY]
                        [--log-level LOG_LEVEL] [--since OBSERVED_
SINCE]
                        [--run-every RUN_EVERY]

optional arguments:
-h, --help            show this help message and exit
--tio-access-key TIO_ACCESS_KEY
                        Tenable.io Access Key
--tio-secret-key TIO_SECRET_KEY
                        Tenable.io Secret Key
--batch-size BATCH_SIZE
                        Size of the batches to populate into
Security Hub
```



```
--aws-region AWS_REGION                AWS region for Security Hub
--aws-account-id AWS_ACCOUNT_ID        AWS Account ID
--aws-access-id AWS_ACCESS_ID          AWS Access ID
--aws-secret-key AWS_SECRET_KEY        AWS Secret Key
--log-level LOG_LEVEL                 Log level: available levels are debug,
info, warn,
--since OBSERVED_SINCE                The unix timestamp of the age threshold
--run-every RUN_EVERY                 How many hours between recurring imports
```

To run the import once, run the following script:

```
./sechubingest.py \
--tio-access-key {TIO_ACCESS_KEY} \
--tio-secret-key {TIO_SECRET_KEY} \
--aws-region us-east-1 \
--aws-account-id {AWS_ACCOUNT_ID} \
--aws-access-id {AWS_ACCESS_ID} \
--aws-secret-key {AWS_SECRET_KEY} \
```

To run the import once an hour, run the following script:

```
./sechubingest.py \
--tio-access-key {TIO_ACCESS_KEY} \
--tio-secret-key {TIO_SECRET_KEY} \
--aws-region us-east-1 \
--aws-account-id {AWS_ACCOUNT_ID} \
--aws-access-id {AWS_ACCESS_ID} \
--aws-secret-key {AWS_SECRET_KEY} \
--run-every 1
```

To run the same import using environment vars, run the following script:



```
export TIO_ACCESS_KEY="{TIO_ACCESS_KEY}"
export TIO_SECRET_KEY="{TIO_SECRET_KEY}"
export AWS_REGION="us-east-1"
export AWS_ACCOUNT_ID="{AWS_ACCOUNT_ID}"
export AWS_ACCESS_ID="{AWS_ACCESS_ID}"
export AWS_SECRET_KEY="{AWS_SECRET_KEY}"
export RUN_EVERY=1
./sechubingest.py
```