# Table of Contents

**Welcome to AWS for Tenable Vulnerability Management** .................................................. 4  
**Integration Requirements** ................................................................................................. 5  
**Integration Configuration** ................................................................................................ 6  
  Tenable Nessus BYOL Scanner .............................................................................................. 6  
  Activate the Nessus BYOL Scanner ...................................................................................... 11  
  Activate Tenable Nessus BYOL Scanner via the Command Line ........................................ 12  
  Obtain Tenable Vulnerability Management Linking Key ..................................................... 12  
  Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management ........ 14  
  Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line ........................................................................................................... 17  
  Link a BYOL Scanner to Tenable Vulnerability Management with Pre-Authorized Scanner Features ......................................................................................................................... 18  
  Optional Configuration ......................................................................................................... 19  
  AWS Multi-Account Multi-VPC Scanning ............................................................................. 20  
  Create a Scan ............................................................................................................................. 24  
  View Scan Results in Tenable Vulnerability Management .................................................... 24  
  Audit the AWS Environment .................................................................................................. 25  
  Create a Read-Only Group in AWS ..................................................................................... 25  
  Create a Scanning User in AWS ............................................................................................ 28  
  Configure AWS Audit Cloud Infrastructure in Tenable Vulnerability Management ............ 31  
  View Audit Details in the Scan Results ................................................................................ 32  
  AWS Audit Troubleshooting ................................................................................................. 33  
**Security Hub** ...................................................................................................................... 36
Requirements
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.

A pre-authorized Tenable Nessus scanner is available in the Amazon Marketplace. The Tenable Nessus scanner links to and is managed by Tenable Vulnerability Management, and allows pre-authorized scanning of AWS EC2 environments and instances. The AWS Connector provides real-time visibility and inventory of EC2 assets in AWS by querying the AWS API. Customers interested in leveraging the pre-authorized Tenable Nessus scanner to secure their AWS environments and instances must have active Tenable Vulnerability Management and Amazon Web Services accounts.

To configure an AWS connector with Frictionless Assessment, see Frictionless Assessment for AWS in the Tenable Vulnerability Management User Guide.

To configure an AWS connector without Frictionless Assessment, see AWS Cloud Connector (without Frictionless Assessment) in the Tenable Vulnerability Management User Guide.

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:

- AWS Connector
- Tenable Nessus BYOL Scanner
  - Activate the Nessus BYOL Scanner
    - Activate Tenable Nessus BYOL Scanner via the Command Line
  - Obtain Tenable Vulnerability Management Linking Key
  - Activate Tenable Nessus BYOL Scanner Linked to Tenable Vulnerability Management
    - Link Tenable Nessus BYOL Scanner to Tenable Vulnerability Management via the Command Line
  - Optional Configuration
- Create a Scan
  - View Scan Results in Tenable Vulnerability Management
- Create an Agent Scan
- 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**.

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.

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
   ```

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

To obtain the Tenable Vulnerability Management linking key:

1. Log in to [https://cloud.tenable.com](https://cloud.tenable.com).
2. In the top menu bar, click **Scans**.
3. In the left-hand menu, click **Scanners**.

   The **Scanners** page appears.

4. Click the **Linked Scanners** tab.
5. Copy and save the **Linking Key**.

![Tenable Nessus BYOL Scanner](image)

**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 [Obtain 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**.

![Screenshot of the Scanners page in Tenable Nessus](image)

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:

   ```bash
   chmod 400 myNessusKey.pem
   ```

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

   ```bash
   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:

   ```bash
   sudo su
   ```

4. Update the AMI using the following command:

   ```bash
   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**

- **IAM role**: None
- **Shutdown behavior**: Stop
- **Enable termination protection**: None
- **Monitoring**: Enable CloudWatch detailed monitoring
  **Additional charges apply.**
- **Tenancy**: Shared - Run a shared hardware instance
  **Additional charges will apply for dedicated tenancy.**
- **Elastic Inference**: Add an Elastic Inference accelerator
  **Additional charges apply.**
- **T2/T3 Unlimited**: Enable
  **Additional charges may apply**

**Advanced Details**

- **User data**: As text, As file, Input is already base64 encoded

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

AWS Multi-Account Multi-VPC Scanning

You can use your Tenable Nessus BYOL scanner to perform scans across multiple accounts and Virtual Private Clouds (VPCs). The BYOL scanner does not require AWS IAM roles or permissions to scan.

If you want your Tenable Nessus BYOL scanner in AWS to scan across multiple VPCs belonging to different accounts, you must configure your VPCs to allow traffic to flow between them. To do this, you can use VPC peering or Transit Gateway.

VPC peering is the more secure option, but you should decide which approach is best for your VPC configuration. As with on-premises firewalls, if you don't want to facilitate communication between VPCs, you must either install a scan engine in each VPC or embed the agent on all Elastic Compute Cloud (EC2) instances.

AWS Transit Gateway does not support routing between Amazon VPCs with identical classless inter-domain routing (CIDR) IP addresses. If you attach a new Amazon VPC with an identical CIDR address to an already-attached Amazon VPC, AWS Transit Gateway does not propagate the route of the new Amazon VPC into the AWS Transit Gateway route table. See the AWS documentation for more information.

You can only scan by IPs, DNS, or dynamic tags. You cannot scan by ID instances.

**Note:** These steps have been tested with 4 accounts containing 8 VPCs and 16 EC2s.

Before you begin:

- To automate tag-based discovery and scanning, set up the [AWS Connector](#) with Tenable Vulnerability Management.

To configure your Tenable Nessus BYOL scanner to scan across multiple accounts and VPCs:
1. In Tenable Vulnerability Management, **Deploy the BYOL scanner** in one of your VPCs.

   You can use the Tenable Vulnerability Management wizard or CFT using the BYOL scanner Ami Id.

   **Tip:** You can find the Ami Id here, after you select a region for the scanner.

2. Link the Tenable Nessus BYOL scanner to Tenable Vulnerability Management in one of two ways:

   - [Link the Tenable Nessus BYOL scanner in Tenable Vulnerability Management](#).
   - [Use a bootstrap script to configure the Tenable Nessus BYOL scanner](#).

3. Perform the VPC peering or Transit Gateway configurations and allow the scanner to access all ports in the security groups.

   The following is an example transit gateway and the scanner authorization in the inbound rules of the security groups:
4. After the communication at your transit gateway is verified, in Tenable Vulnerability Management, select the assets you want to scan.

5. Create a tag for the assets. You can create this tag based on the account IDs, VPCs, instance types, or the AWS discovery source.
6. Create a scan, and select the tag you created in Step 5 in the Basic settings.

7. Launch the scan.

The scan displays results from across all the scanned VPCs.

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.

[Image of AWS Basic Network Scan]

• 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**.

   ![AWS Management Console](image)

   The **AWS Management Console** appears.

3. Click **Services**.

   The **Services** page appears.
4. In the **Security, Identity, and Compliance** section, click **IAM**.

![IAM control panel](image1)

The **IAM** control panel appears.

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

The **Groups** page appears.

6. Click **Create New Group**.

The **Create New Group Wizard** appears.

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

![Set Group Name](image2)

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

**Group Name:** `ReadOnly`

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 Screen](image)

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.

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.

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.
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.

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

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 **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]
```

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-account-id AWS_ACCOUNT_ID  
--aws-access-id AWS_ACCESS_ID  
--aws-secret-key AWS_SECRET_KEY  
--log-level LOG_LEVEL  
info, warn,  
--since OBSERVED_SINCE  
--run-every RUN_EVERY  

AWS region for Security Hub  
AWS Account ID  
AWS Access ID  
AWS Secret Key  
Log level: available levels are debug, error, crit  
The unix timestamp of the age threshold  
How many hours between recurring imports  

To run the import once, run the following script:

```bash
./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:

```bash
./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