

# How to install an instance of the EnGenius EzMaster server on the Amazon AWS platform.

## Introduction

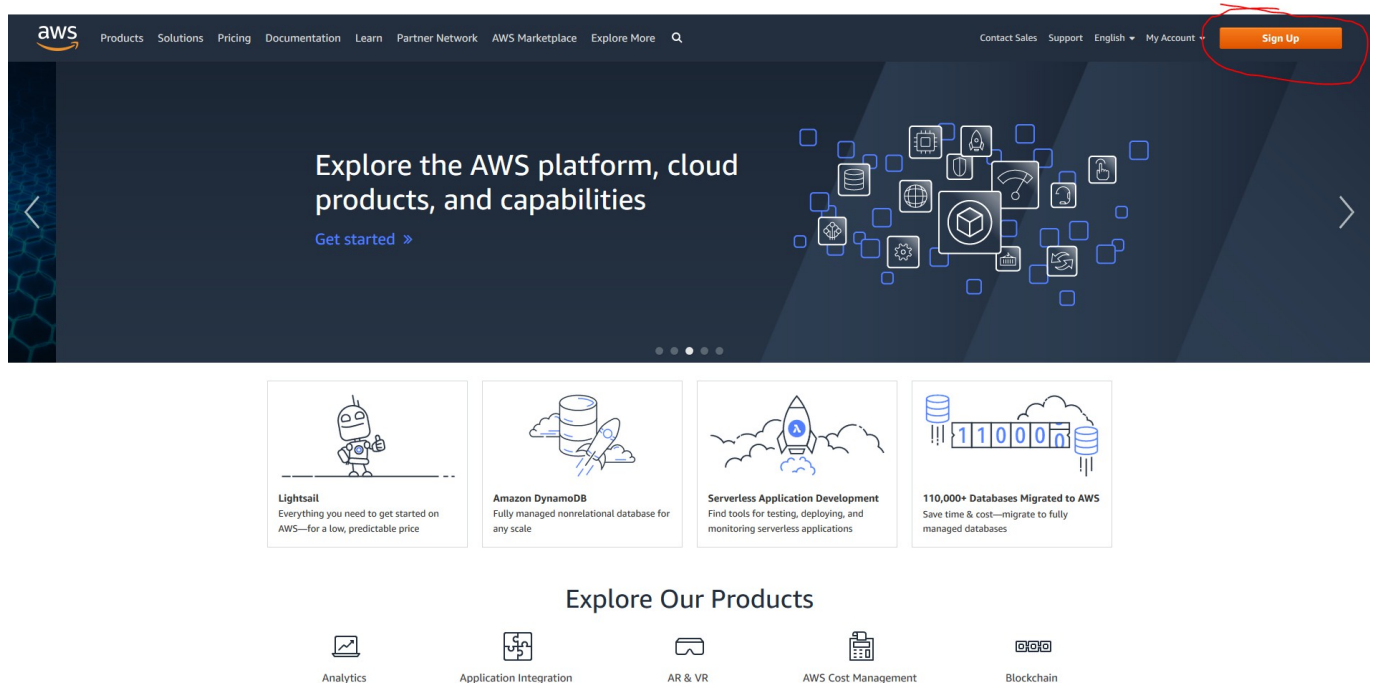
Up until recently, if you wanted to run EzMaster then you needed to do the install on your own server. The installation is trivial, quick and easy to do, and the server demands are quite low so it will run on even a quite low spec Windows PC. However some users have felt wary of running their own server package.

Anyway there is now a public image file for the EnGenius EzMaster package that allows users to run their own instance on the Amazon AWS platform. The Amazon AWS platform is probably the most popular public server platform out there and used, for example, by a number of large corporate bodies. Generally you need to pay to install and run an 'instance' on the AWS platform but Amazon do have a starter option which gives you a free service. There are limitations on the free option but it should be fine for an EzMaster instance suitable for up to 500 access points.

## Setup

First of all you need to go and create an account on the Amazon AWS. This is free...

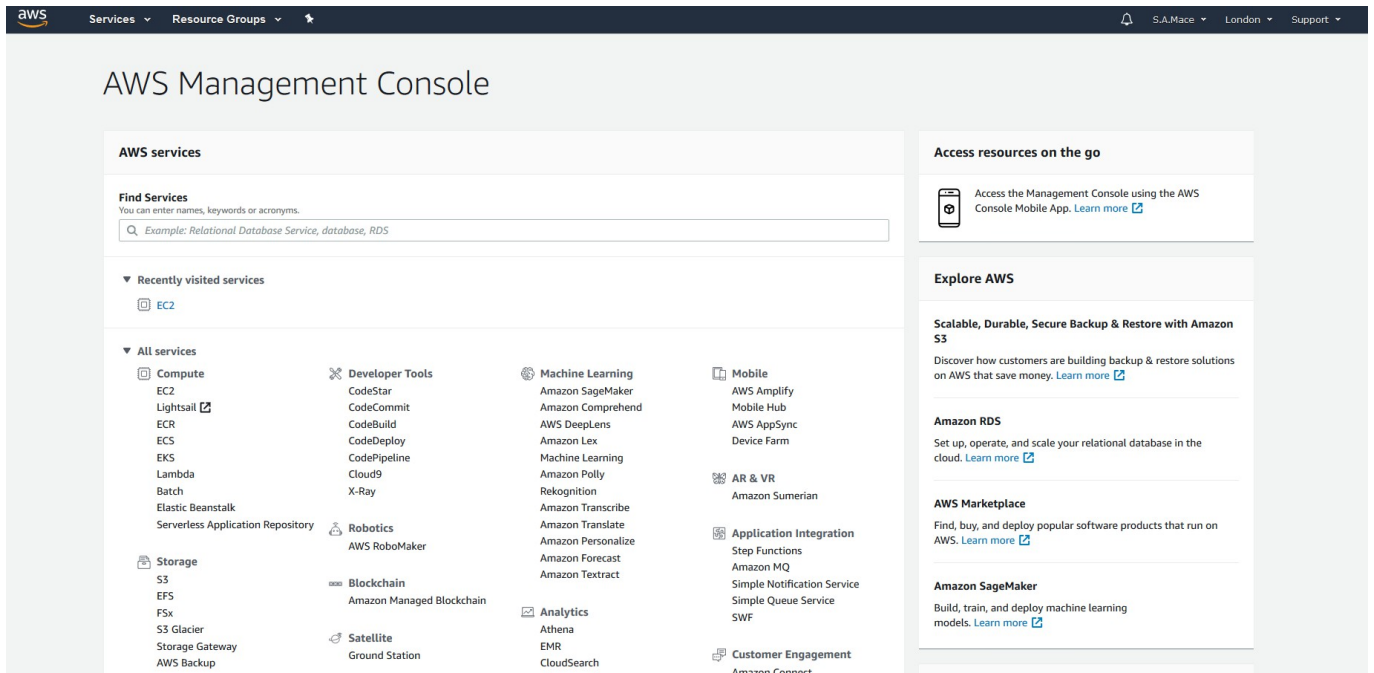
<https://aws.amazon.com/>



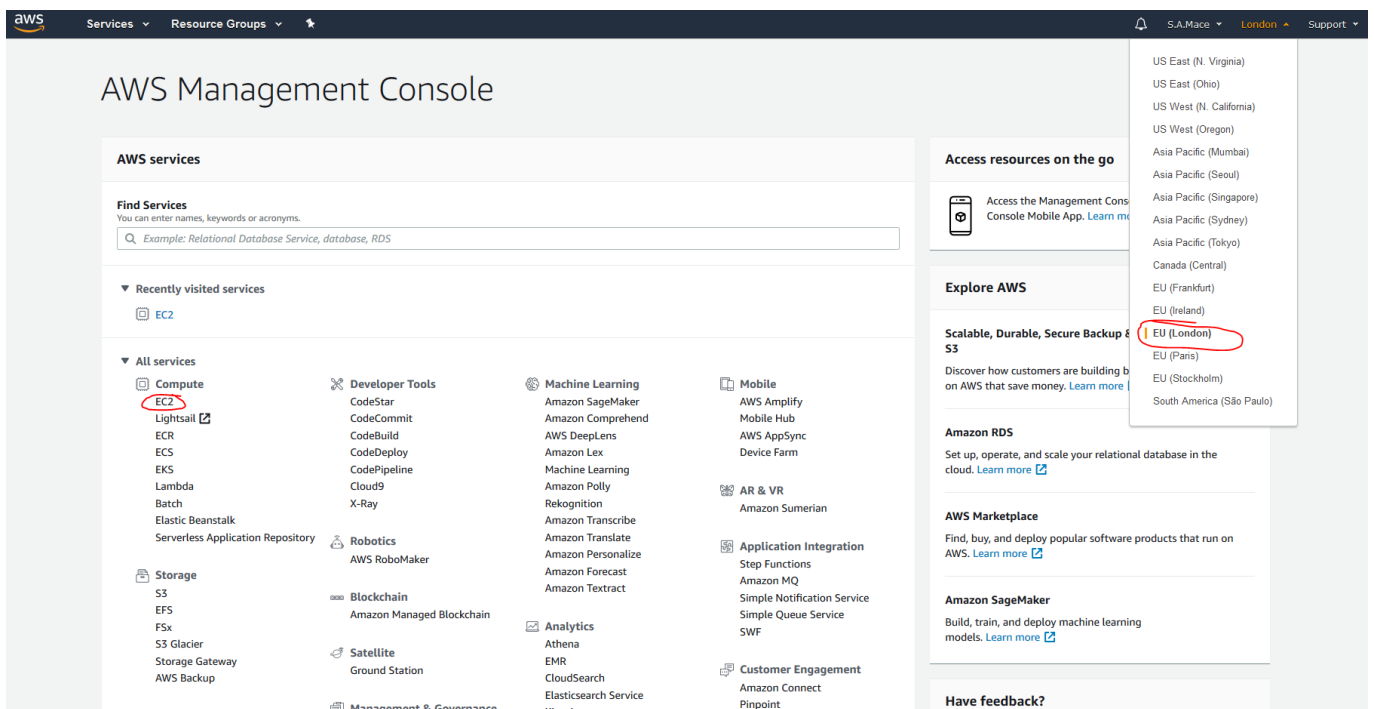
The screenshot shows the AWS website homepage. The top navigation bar includes links for Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, and Explore More. On the right, there are links for Contact Sales, Support, English, My Account, and a red-circled 'Sign Up' button. The main banner features the text 'Explore the AWS platform, cloud products, and capabilities' with a 'Get started >' link. Below the banner are four product cards: Lightsail (Everything you need to get started on AWS—for a low, predictable price), Amazon DynamoDB (Fully managed nonrelational database for any scale), Serverless Application Development (Find tools for testing, deploying, and monitoring serverless applications), and 110,000+ Databases Migrated to AWS (Save time & cost—migrate to fully managed databases). At the bottom, the 'Explore Our Products' section lists Analytics, Application Integration, AR & VR, AWS Cost Management, and Blockchain.

If you already have an account then you can go direct to console management (you may have to confirm login before you can access this page):

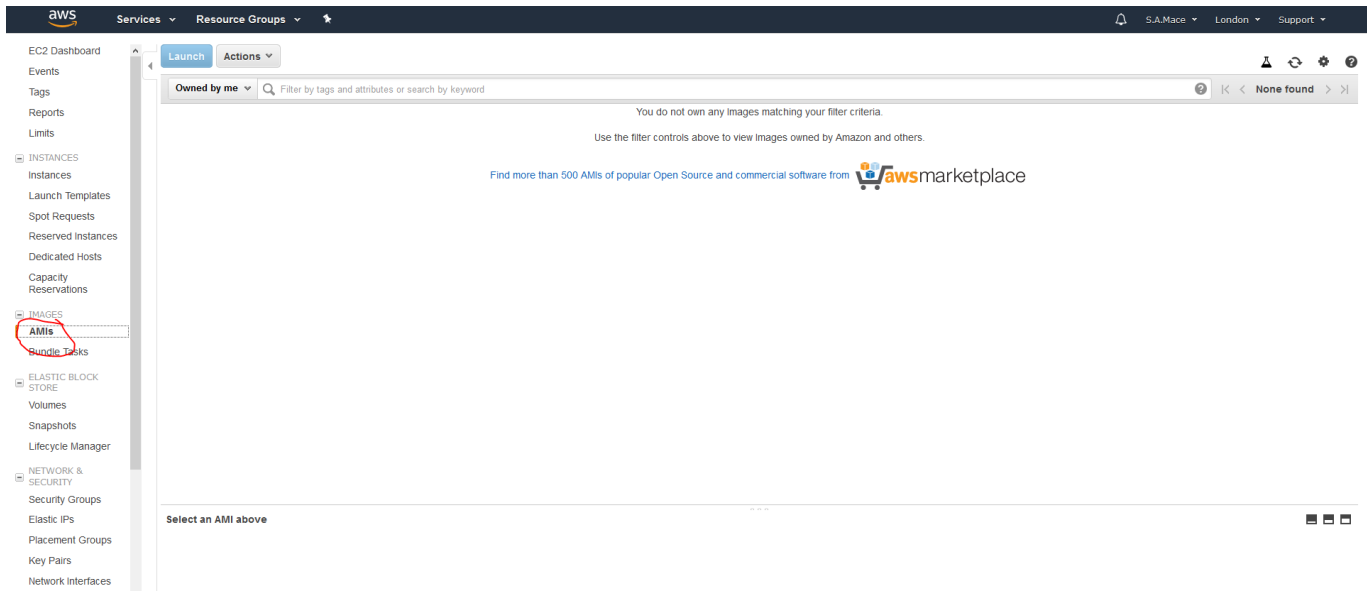
<https://eu-west-2.console.aws.amazon.com/console/home?region=eu-west-2#>



Make sure the region in the top right suites your location e.g. London. Then select **EC2**.

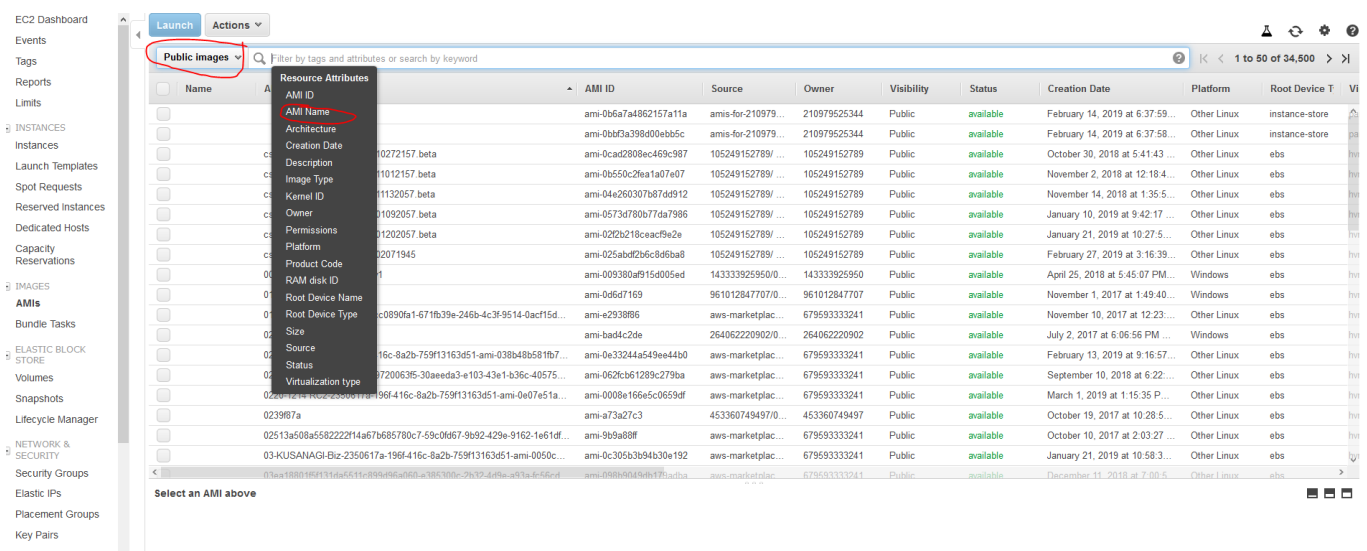


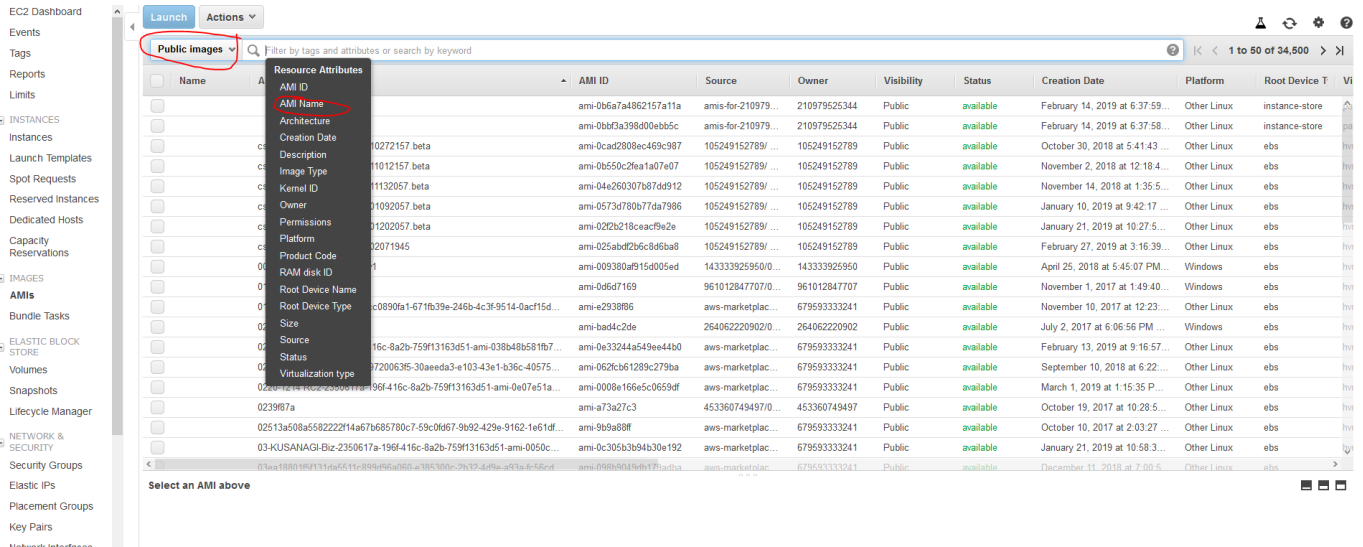
On the next page select **AMIs** on the left menu:



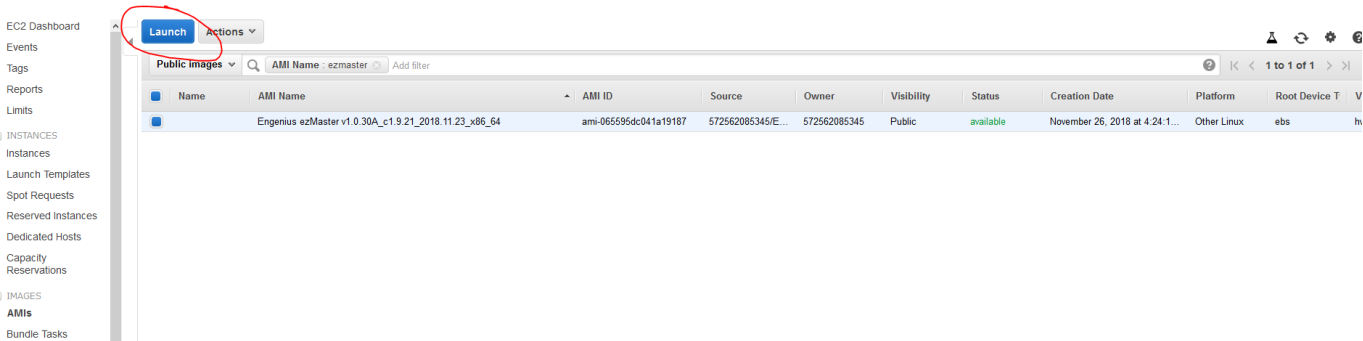
EnGenius have already uploaded a public accessible copy of the EzMaster server which you can copy onto your own platform.

Change **Owned by me** to **Public Images** and then select **AMI Name**:

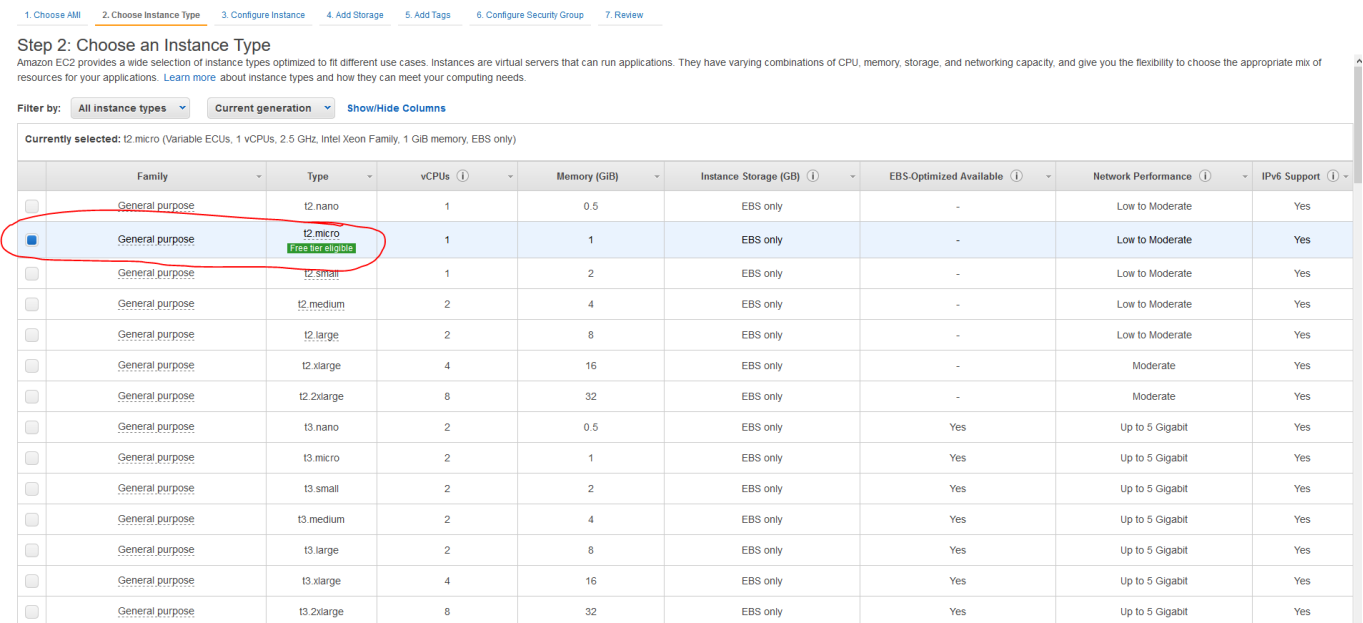




type ezmaste and then press enter. The ezmaste public image should then show, click on Launch:

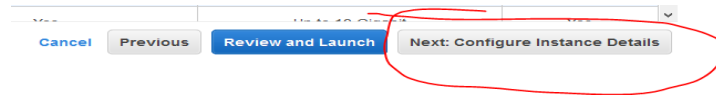


The next screen is for you to choose an Instance Type:



Select the type you need. For applications up to 500 APs then the free t2.micro is suitable. For larger numbers of APs then you will need to select a more powerful type. e.g. for the full 10000 APs then you need to go for t3.xlarge!

Click on **Configure Instance Details** in the bottom right of the page:



1. Choose AMI 2. Choose Instance Type 3. **Configure Instance** 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

**Number of instances**  [Launch into Auto Scaling Group](#)

**Purchasing option**  Request Spot instances

**Network**  [Create new VPC](#)

**Subnet**  [Create new subnet](#)

**Auto-assign Public IP**

**Placement group**  Add instance to placement group

**Capacity Reservation**  [Create new Capacity Reservation](#)

**IAM role**  [Create new IAM role](#)

**Shutdown behavior**

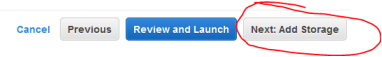
**Enable termination protection**  Protect against accidental termination

**Monitoring**  Enable CloudWatch detailed monitoring  
Additional charges apply

**Tenancy**   
Additional charges will apply for dedicated tenancy.

**T2/T3 Unlimited**  Enable  
Additional charges may apply

▶ **Advanced Details**



Nothing needs to be set on the next page so go direct to **Add Storage...**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. **Add Storage** 5. Add Tags 6. Configure Security Group 7. Review

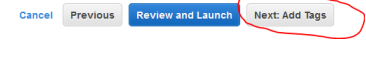
### Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0a3bc58a73dce20e7	<input type="text" value="20"/>	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.



The default 20GB storage is normally okay but you can use up to 30GB on the free platform. Click on **Add Tags...**

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances 1	Volumes 1
<i>This resource currently has no tags</i>			
Choose the <b>Add tag</b> button or <a href="#">click to add a Name tag</a> . Make sure your <a href="#">IAM policy</a> includes permissions to create tags.			

**Add Tag** (Up to 50 tags maximum)

Cancel Previous **Review and Launch** Next: Configure Security Group

You don't need to add any tags so you can go direct to **Configure Security Group**:

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:  Create a new security group

Select an existing security group

Security group name:

Description:

Type 1	Protocol 1	Port Range 1	Source 1	Description 1
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

**Add Rule**

**Warning**  
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous **Review and Launch**

Go direct to **Review and Launch**....

### Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**Improve your instances' security. Your security group, launch-wizard-2, is open to the world.**  
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)

**Engenius ezMaster v1.0.30A\_c1.9.21\_2018.11.23\_x86\_64 - ami-065595dc041a19187**  
Engenius ezMaster v1.0.30A\_c1.9.21\_2018.11.23\_x86\_64  
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name: launch-wizard-2  
Description: launch-wizard-2 created 2019-03-07T10:02:13.512+00:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Tags [Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

Then go to **Launch**....

AWS will now ask you to set up a security key:

**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](#).

Choose an existing key pair

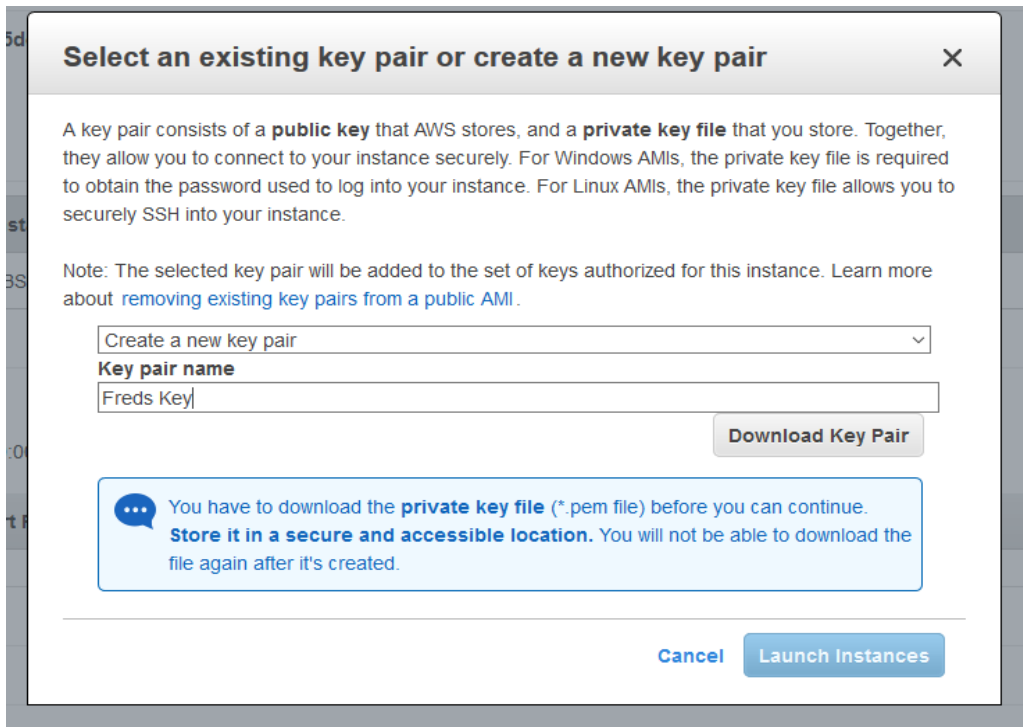
**Select a key pair**

Solwise Key

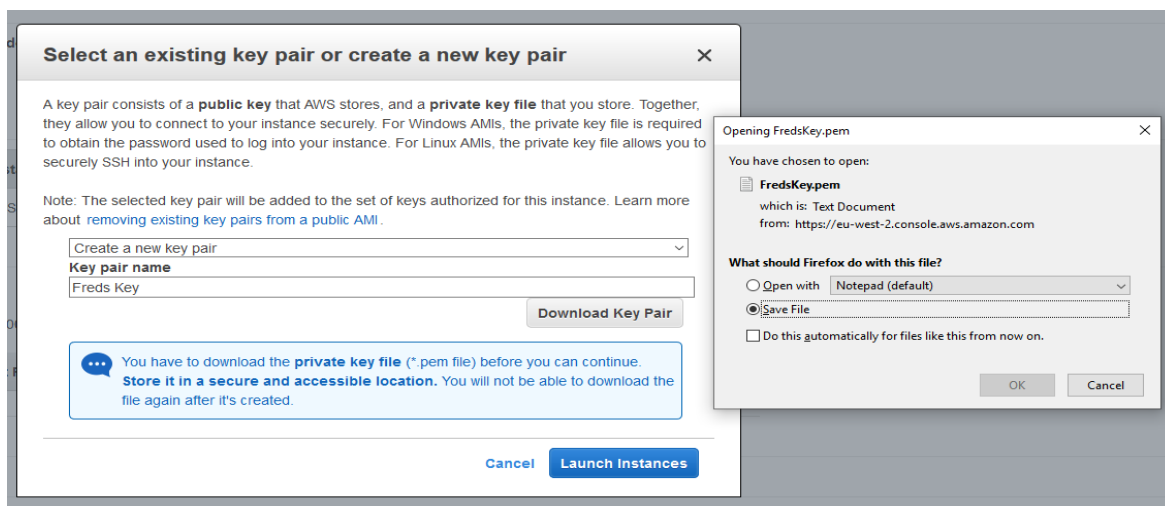
I acknowledge that I have access to the selected private key file (Solwise Key.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

Select **Create a new Key Pair** and then enter a key pair name....



Next you should download and save the key pair file...



and then you goto **Launch Instances**.

#### Launch Status

**✔ Your instances are now launching**  
The following instance launches have been initiated: **+0337d72cb04515bc3** [View launch log](#)

**ℹ Get notified of estimated charges**  
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

#### How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click **View instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the instances screen. [Find out](#) how to connect to your instances.

#### Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View instances](#)



Click on the link for the new instance....

Instance: **i-0337d72cb04515bc3** Public DNS: [ec2-18-130-106-231.eu-west-2.compute.amazonaws.com](#)

Property	Value
Instance ID	i-0337d72cb04515bc3
Instance state	running
Instance type	t2.micro
Elastic IPs	-
Availability zone	eu-west-2a
Security groups	<a href="#">launch-wizard-2</a> <a href="#">view inbound rules</a> <a href="#">view outbound rules</a>
Scheduled events	No scheduled events
AMI ID	Engenius ezMaster v1.0.30A_c1.9.21_2018.11.23_x86_64 (ami-065595dc041a19187)
Public DNS (IPv4)	ec2-18-130-106-231.eu-west-2.compute.amazonaws.com
IPv4 Public IP	18.130.106.231
IPv6 IPs	-
Private DNS	ip-172-31-21-32.eu-west-2.compute.internal
Private IPs	172.31.21.32
Secondary private IPs	-
VPC ID	vpc-e445de8c
Subnet ID	subnet-5b9e3721

Then click on the launch..... link.

Security Group: **sg-0d363e5296c81d61b**

**Inbound** | Outbound | Tags

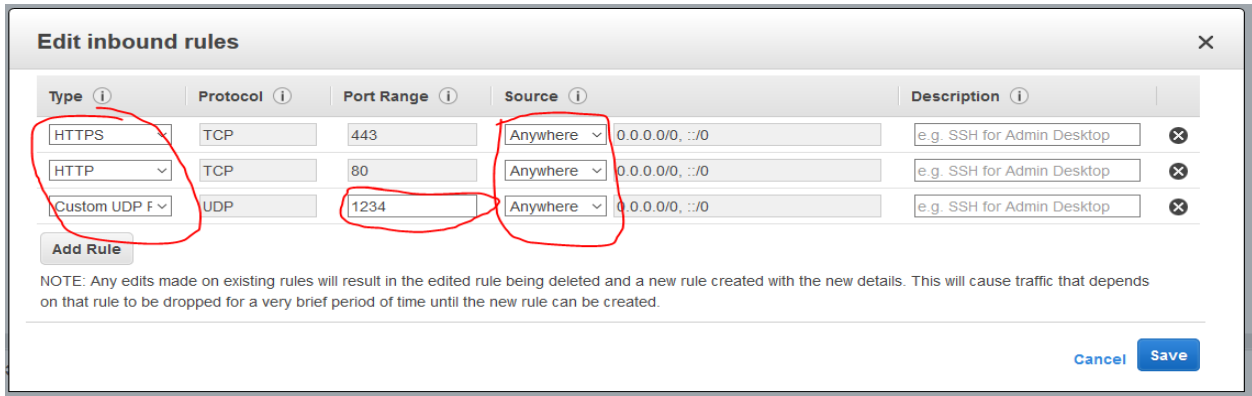
[Edit](#)

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

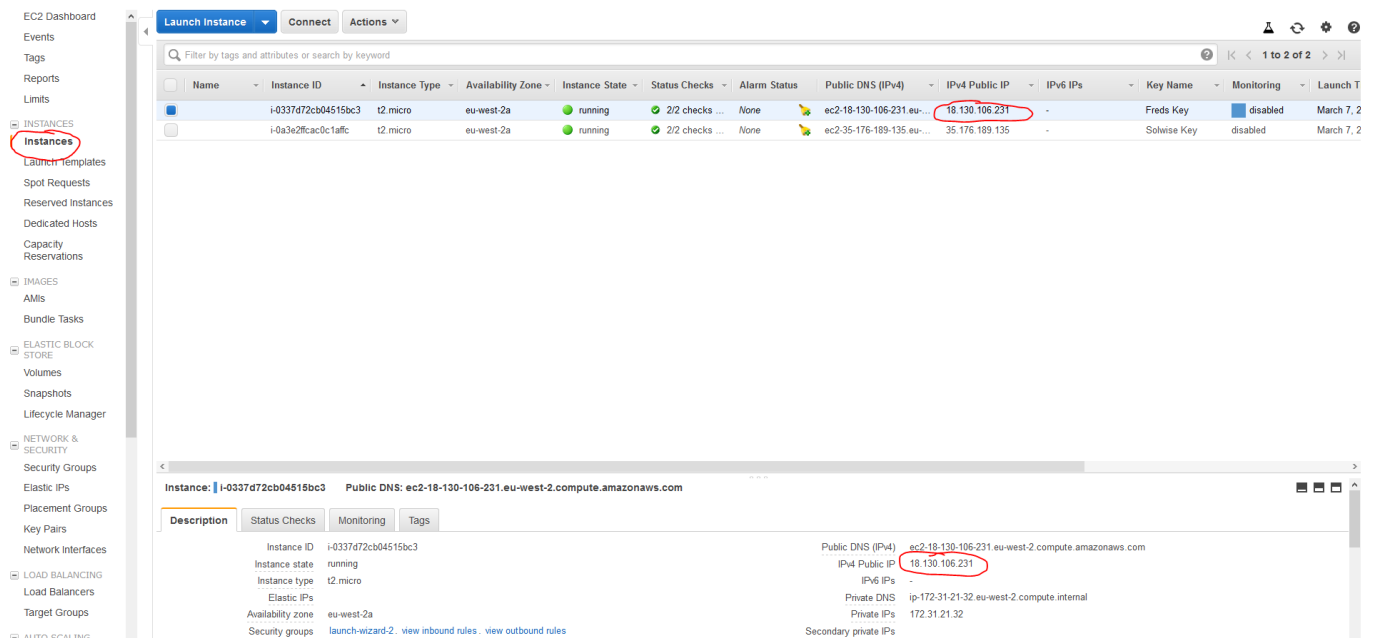
Goto the **Inbound** security tab and then **Edit**....



Delete the default SSH entry and then **Add Rule**. Add rules for HTTP and HTTPS and a Custom UDP for 1234:



Change the **Source** to **Anywhere** to allow clients from any external location to connect. Then click on **Save**.



Click on **Instances** on the left menu. Then you can see the public IP address that you can use to log into the EzMaster instance.

18.130.106.231/login.html

Phillips RCS IR

EnGenius®

### ezMaster Login

Distributed Network Management Solution

username

This connection is not secure. Logins entered here could be compromised. [Learn More](#)

password

Log in

© EnGenius 2018. All rights reserved.

Done!! :-)