

Create an Amazon AWS Account

LightSail is a very affordable (almost free depending on usage) cloud computing platform that is great for running TikiWiki for personal projects or small collaboration groups.

Another aspect of LightSail is that it is geared for easy to setup and maintenance with just the bare amount of features that you need to run a professional looking TikiWiki.

AWS Lightsail Requirements

Given the high security requirements of Amazon AWS you will need a virtual Two Factor Authentication device. Google provide a good virtual Two Factor Authentication app on the [Play store](#) and the [App Store](#)

AWS Account Creation

- Go to the AWS account setup page [here](#).
- After email verification you then use the AWS sign-in page [here](#).



Sign in

Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

happy-tikiwiki-user@tiki.org

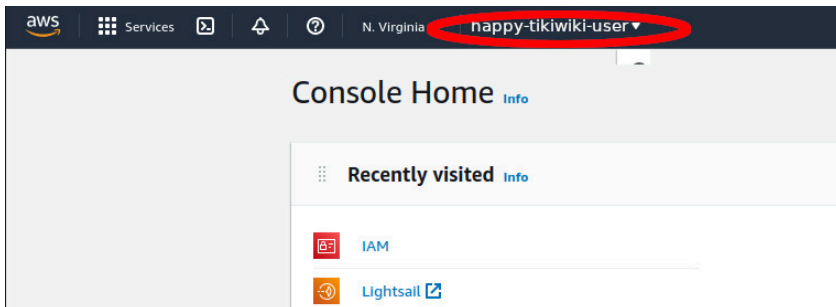
Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.



AWS Login

- When the AWS account page opens click on your account name in the top right corner.
- Next click Security Credentials.



aws security console

- Next click the Multi-factor authentication (MFA) sliding section.

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).
To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

▲ Password

▼ Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

Device type	Serial number	Actions
Virtual	██████████ root-account-mfa-device	Manage

▲ Access keys (access key ID and secret access key)

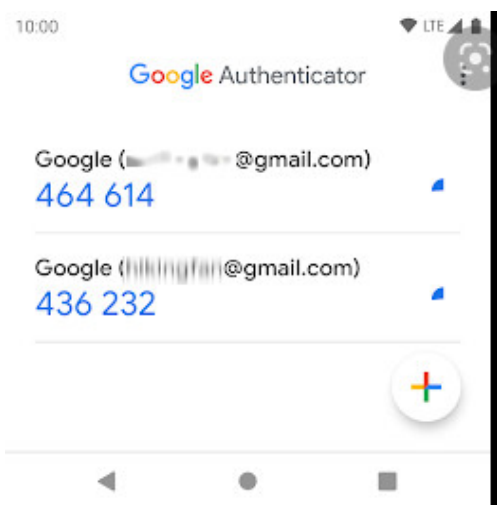
▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers

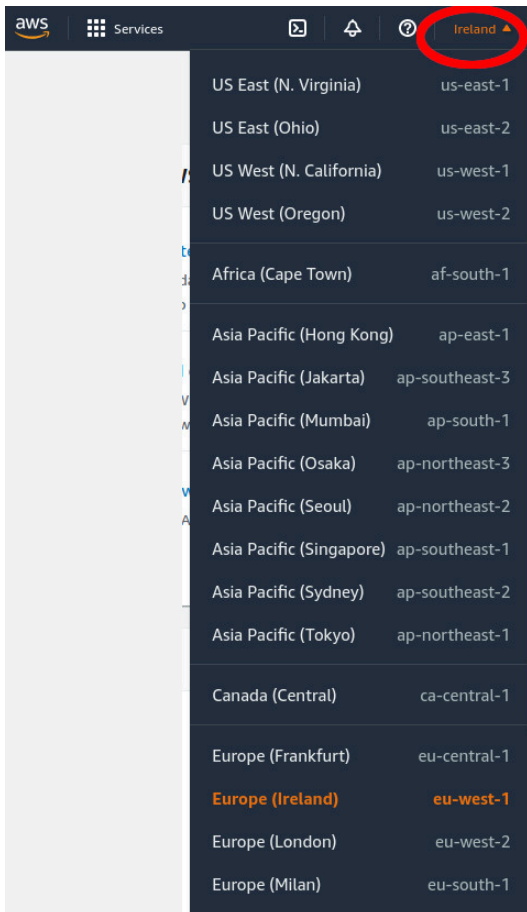
AWS MFA Setup

- Next click MANAGE to setup your virtual MFA device. Once your virtual MFA device can generate codes as shown you will be able to login with increased security.



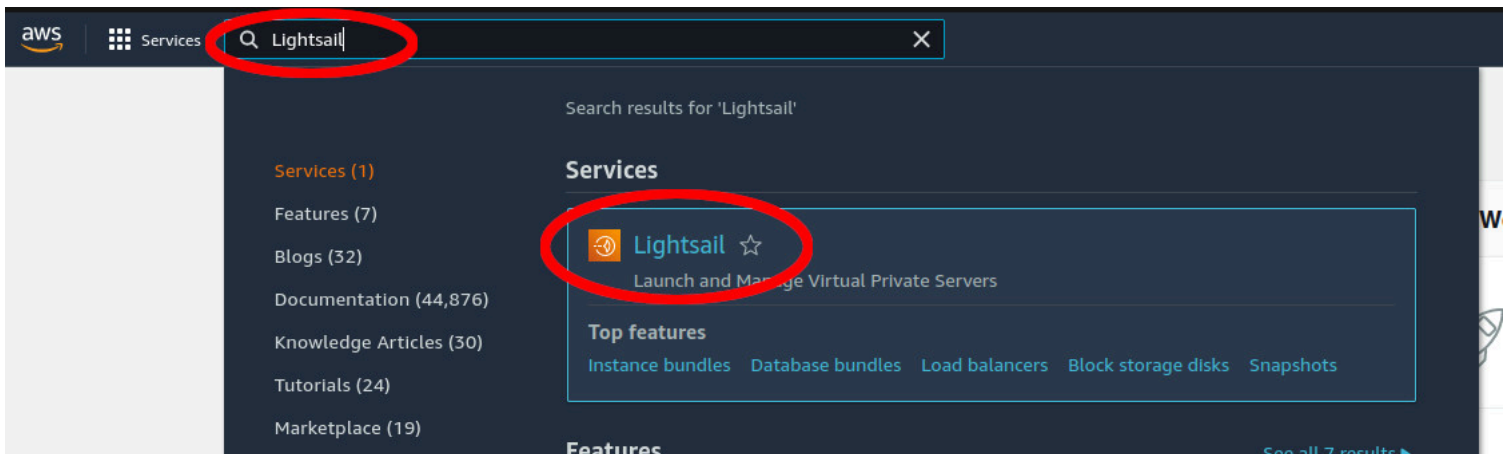
Google virtual MFA device

- Back in the AWS Management Console select your preferred local data-center.



AWS Lightsail data-center

- Now do a service search and type in "Lightsail", when the Lightsail icon appears click it to start the setup of the next stage.



AWS Lightsail Service Search

- You are then presented with instance creation page, click "Create Instance".

Good morning!

Filter by name, location, tag, or type

Instances Containers Databases Networking Storage Snapshots

You have no instances right now.

Create an instance and get started with Lightsail!

Create instance

Learn more about instances



Lightsail instance creation

- From this point forward its up to you to go with your preferred configuration.

You can setup a linux instance by following one of the many great tutorials on the AWS Lightsail website.

- [Setup Linux Instance](#)
- [Setup Debian Linux instance with MariaDB and Virtualmin control panel](#)
- Due to the lower compute power of the Lightsail instances your TikiWiki database will have to be placed in a separate database instance that is easy to configure when following the AWS Lightsail tutorials.
 - [Setup database instance](#)
- To secure TikiWiki you should configure your web-server to use SSL encryption when serving content to clients.

MySQL SSL

- Given that the TikiWiki web-server and database server are not on the same virtual machine the contents of the TikiWiki database will be traversing Amazon's AWS data-center in the clear so you need to encrypt this web-server to database connection with SSL.
- Get your preferred AWS Lightsail certificate from [here](#).

Note

The certificates available for download are labeled for Amazon Relational Database Service (Amazon RDS), but also work for managed databases in Lightsail.

To get a certificate bundle that contains both the intermediate and root certificates, download from <https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem>.

To get a root certificate that works for all AWS Regions, download from one of these locations:

- <https://s3.amazonaws.com/rds-downloads/rds-ca-2019-root.pem>
- <https://s3.amazonaws.com/rds-downloads/rds-ca-2015-root.pem>

AWS LightSail root certificate

- When you have everything configured to your satisfaction in TikiWiki and all seems to be working, you should then encrypt the web-server to database connection by placing the certificate file "rds-ca-2019-root.pem" you downloaded from [here](#) into the cert sub-folder on your web-server.

```
root@webserver1:~$ ls -l /var/www/html/ssl/openssl.com/tiki-24.0/db/cert/
-rwxr-xr-x 1 www-data www-data 1172 May  6 01:11 rds-ca-2019-root.pem
root@webserver1:~$
```

Lightsail root CA file location on your web-server instance.

- END