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.

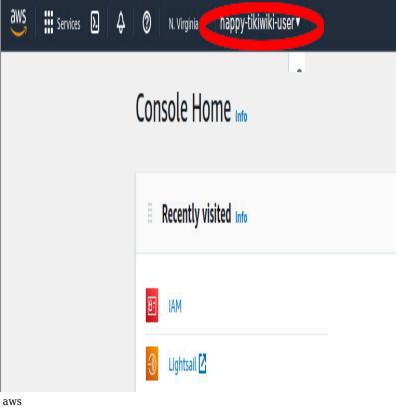


Sign in



AWS Login

- $\bullet\,$ 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.

intity and Access inagement (IAM)		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.				
angeneri (rin)						
Dashboard		To learn more about the	types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.			
Access management		 Password 				
User groups		-	and only APPA			
Users		• Multi-factor autr	enticator (MFA)			
Roles		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.				
Policies						
Identity providers		Device type	Serial number	Actions		
Account settings		Virtual	tot-account-rifa device	Manage		
Access reports Access analyzer		Access keys (access key ID and secret access key)				
Archive rules		CloudFront key pairs				
Analyzers		 X 509 certificate 				
Settings		 Account identifiers 				
AWS MFA	L					

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.

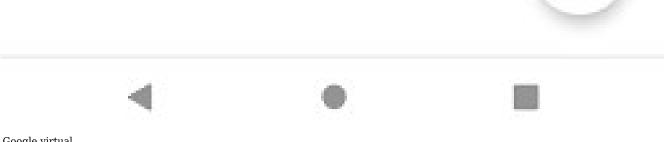


Google Authenticator

LTE:

Google (© @gmail.com) 464 614

Google (IIIIIIIIIII@gmail.com) 436 232



Google virtual MFA device

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

aws Services	D ¢	Ireland
	US East (N. Virginia)	us-east-1
	US East (Ohio)	us-east-2
<i>r</i> .	US West (N. California)	us-west-1
	US West (Oregon)	us-west-2
Ee da	Africa (Cape Town)	af-south-1
	Asia Pacific (Hong Kong)	ap-east-1
le l	Asia Pacific (Jakarta)	ap-southeast-3
~	Asia Pacific (Mumbai)	ap-south-1
	Asia Pacific (Osaka)	ap-northeast-3
A	Asia Pacific (Seoul)	ap-northeast-2
	Asia Pacific (Singapore)	ap-southeast-1
_	Asia Pacific (Sydney)	ap-southeast-2
	Asia Pacific (Tokyo)	ap-northeast-1
	Canada (Central)	ca-central-1
	Europe (Frankfurt)	eu-central-1
	Europe (Ireland)	eu-west-1
	Europe (London)	eu-west-2
	Europe (Milan)	eu-south-1
AWS		

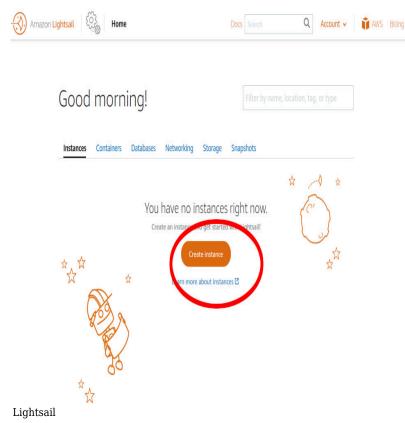
AWS LightSail datacenter

• 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

 $\bullet\,$ You are then presented with instance creation page, click "Create Instance".



• 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
- 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/rdsdownloads/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.



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

• END