How to use Pancakeswap Sniper bot

Hello! Thank you for buying the pancakeswap sniping bot!

In this pdf you will find out how to use it.

If you encounter anything you don’t understand please dm me so I can fix this guide.

Content

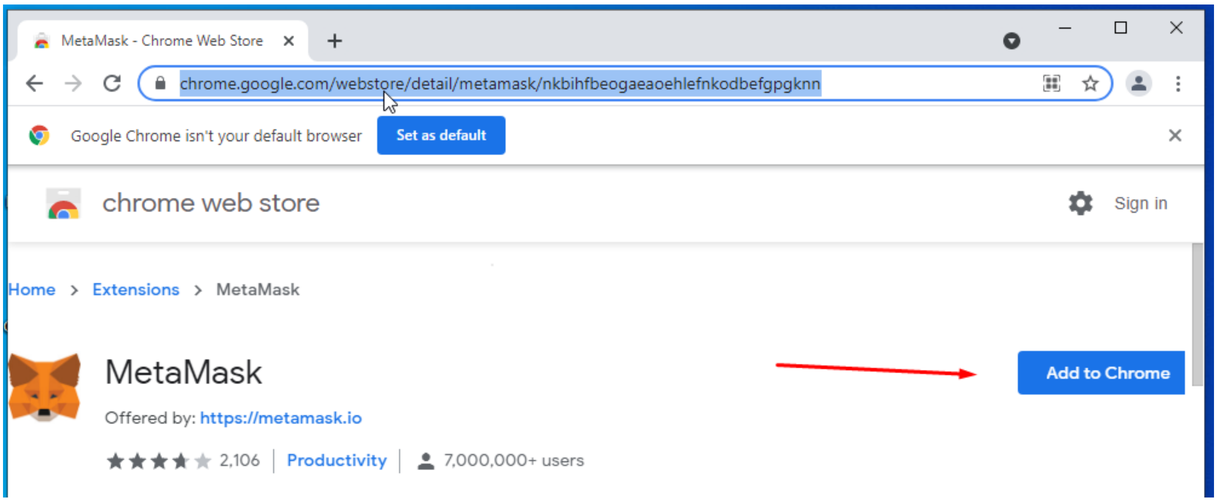
How to create a metamask wallet

To snipe a token we first need a wallet to hold all our tokens. In this case we will install metamask because it's one of the most popular wallets.

Step 1. Add metamask to chrome extenions.

To add metamask to you chrome extenions you need to go to https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn

And press the add to chrome button.



MetaMask - Chrome Web Store

chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn

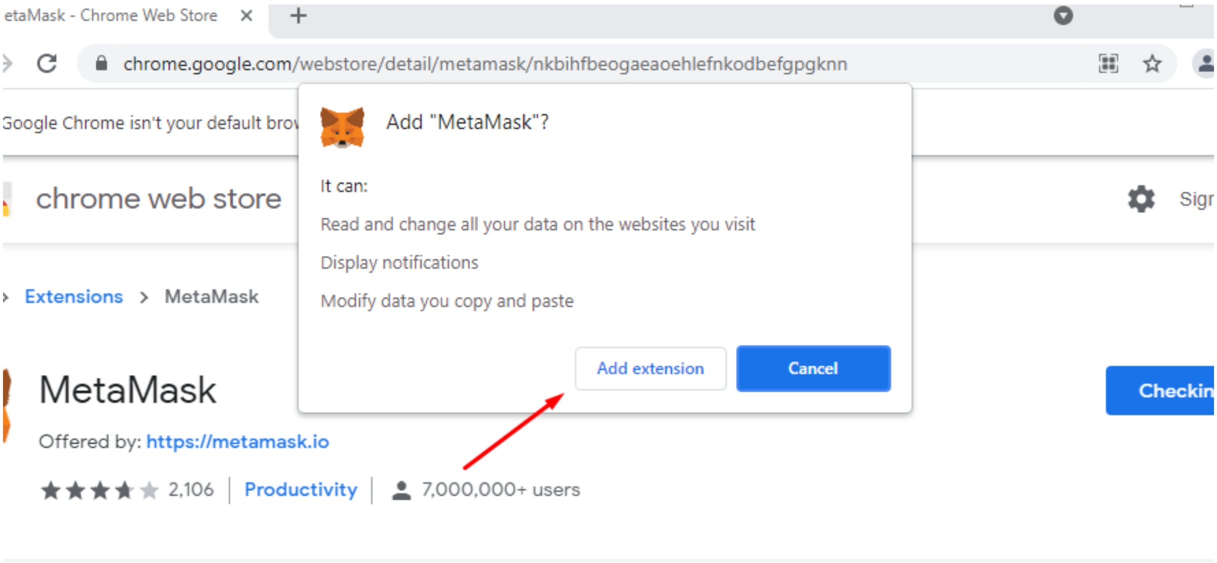
Google Chrome isn't your default browser

MetaMask

Offered by: https://metamask.io

★★★★☆ 2,106 | Productivity | 7,000,000+ users

Chrome will ask if you would like to add metamask, press "Add extension"



etaMask - Chrome Web Store

chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn

Google Chrome isn't your default brov

Add "MetaMask"?

It can:

Read and change all your data on the websites you visit

Display notifications

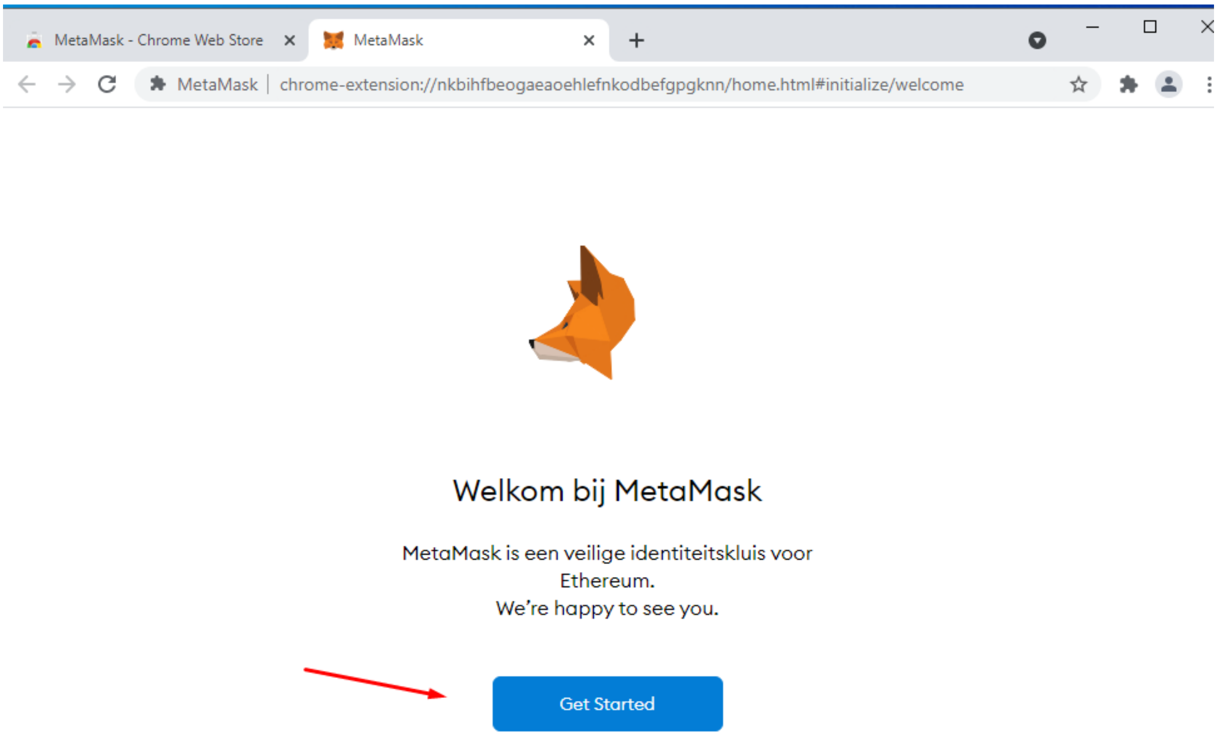
Modify data you copy and paste

MetaMask

Offered by: https://metamask.io

★★★★☆ 2,106 | Productivity | 7,000,000+ users

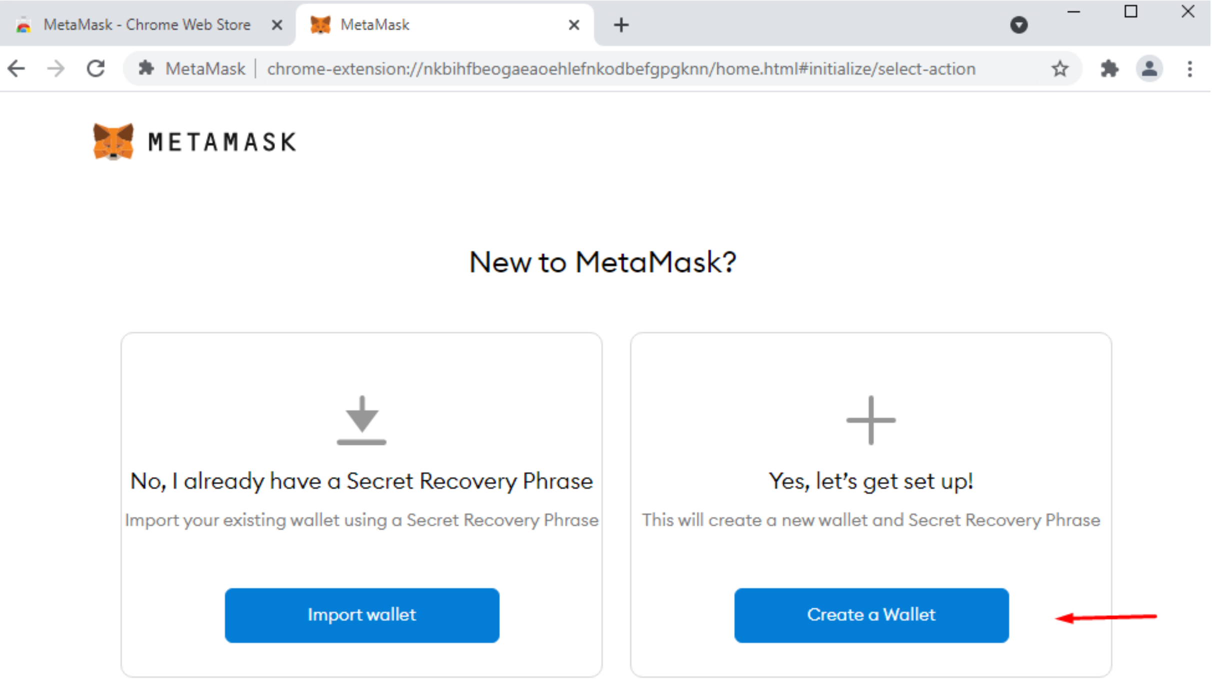
After installing metamask, it will automatically open a new webpage. Press “Get Started”


MetaMask - Chrome Web Store
MetaMask
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/welcome

Welkom bij MetaMask

MetaMask is een veilige identiteitskluis voor Ethereum.
We’re happy to see you.

Now we will press: “Create a Wallet”


MetaMask - Chrome Web Store
MetaMask
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/select-action
METAMASK

New to MetaMask?

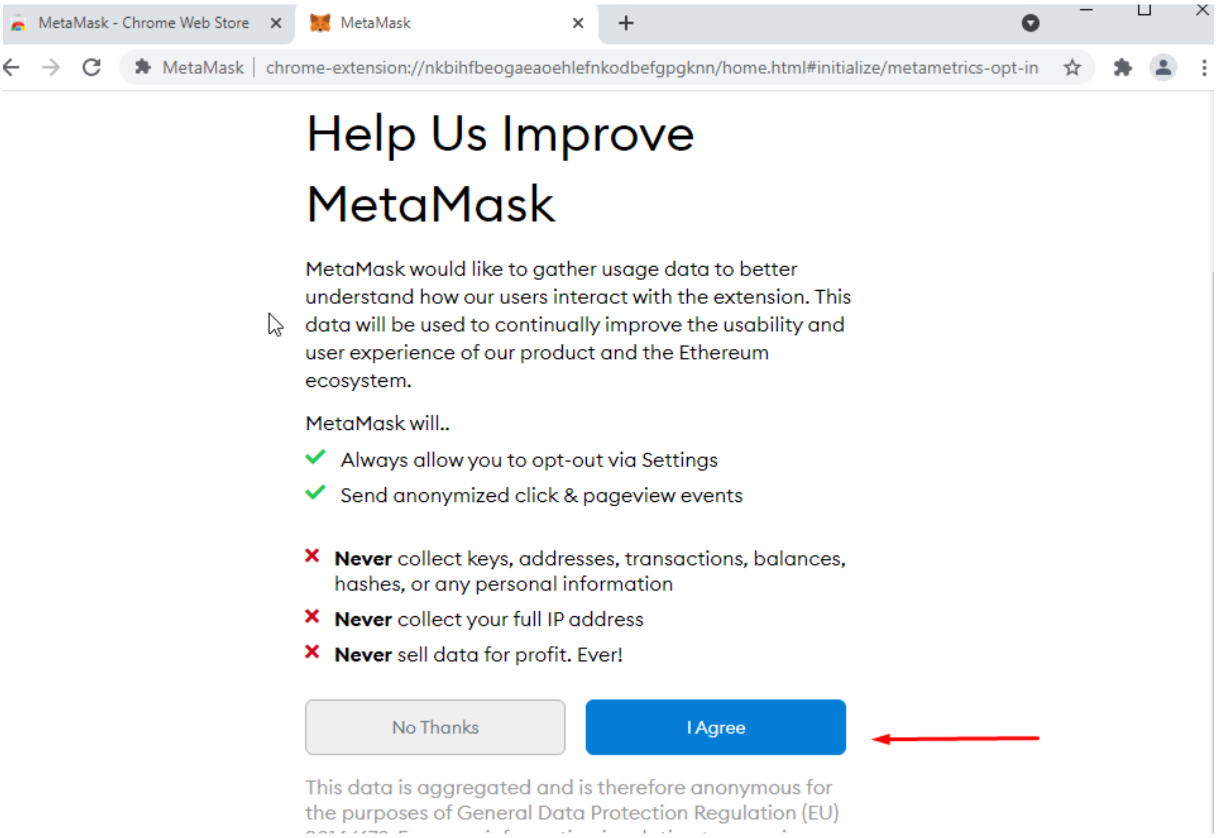
No, I already have a Secret Recovery Phrase

Import your existing wallet using a Secret Recovery Phrase

Yes, let’s get set up!

This will create a new wallet and Secret Recovery Phrase

After that we will accept there TOS by clicking: “I Agree”


MetaMask - Chrome Web Store
MetaMask
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/metametrics-opt-in
No Thanks
I Agree

Help Us Improve MetaMask

MetaMask would like to gather usage data to better understand how our users interact with the extension. This data will be used to continually improve the usability and user experience of our product and the Ethereum ecosystem.

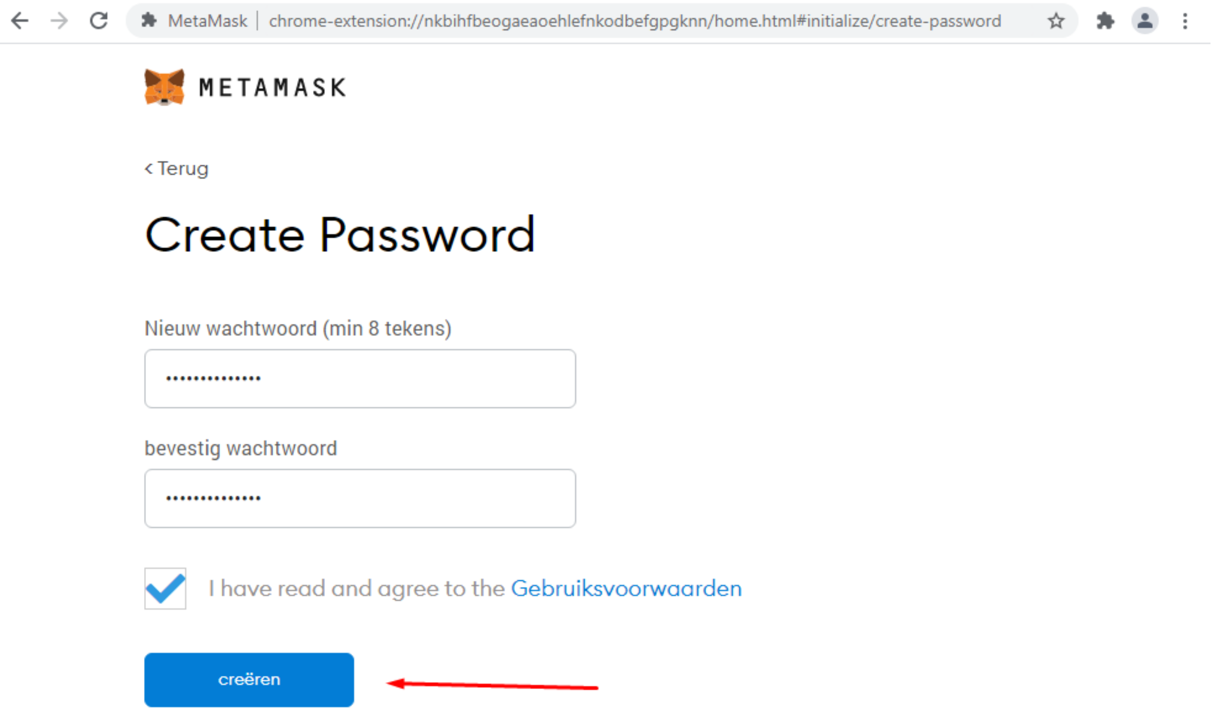
MetaMask will..

- ✓ Always allow you to opt-out via Settings
- ✓ Send anonymized click & pageview events

- ✗ **Never** collect keys, addresses, transactions, balances, hashes, or any personal information
- ✗ **Never** collect your full IP address
- ✗ **Never** sell data for profit. Ever!

This data is aggregated and is therefore anonymous for the purposes of General Data Protection Regulation (EU)

Now you need to create a password to access your wallet. When you filled in the same password 2 times then you press create.


MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/create-password
METAMASK
< Terug
creëren

Create Password

Nieuw wachtwoord (min 8 tekens)

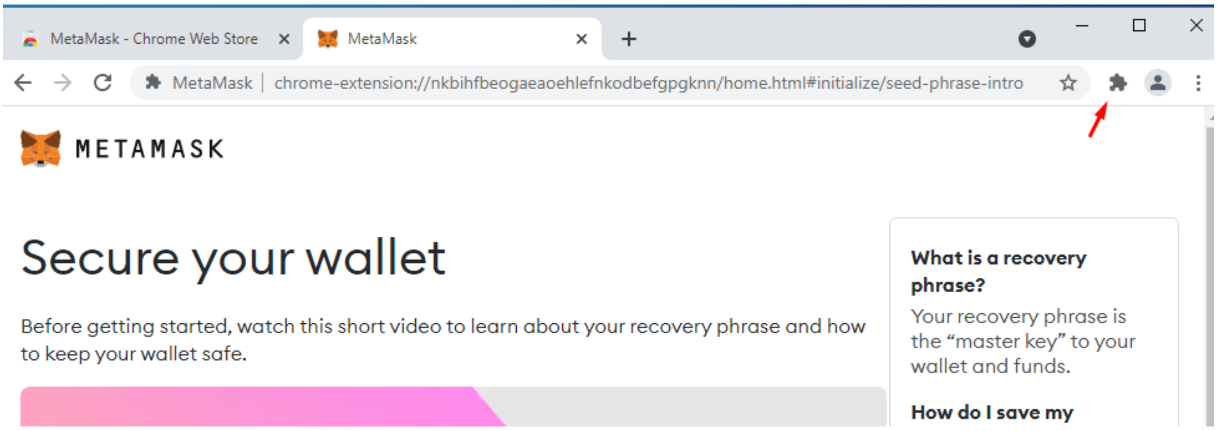
••••••••••••••

bevestig wachtwoord

••••••••••••••

☑ I have read and agree to the Gebruiksvoorwaarden

Now you can pin down metamask by pressing the little puzzle icon and then the pin icon.



MetaMask - Chrome Web Store

MetaMask

MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/seed-phrase-intro

METAMASK

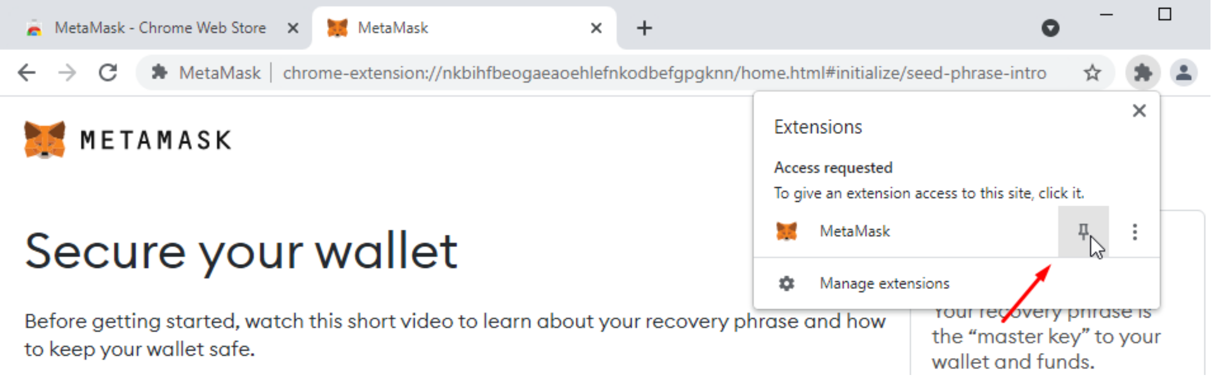
Secure your wallet

Before getting started, watch this short video to learn about your recovery phrase and how to keep your wallet safe.

What is a recovery phrase?

Your recovery phrase is the “master key” to your wallet and funds.

How do I save my



MetaMask - Chrome Web Store

MetaMask

MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/seed-phrase-intro

Extensions

Access requested

To give an extension access to this site, click it.

MetaMask

Manage extensions

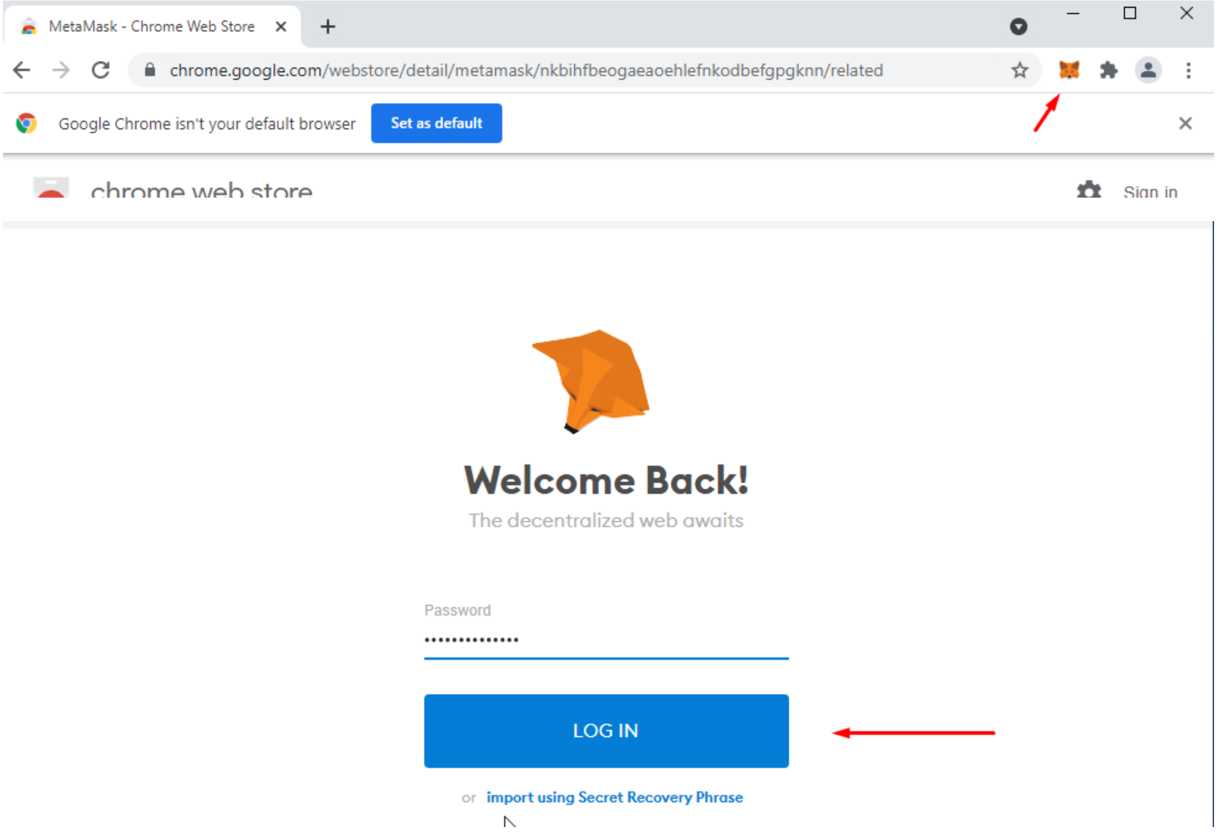
METAMASK

Secure your wallet

Before getting started, watch this short video to learn about your recovery phrase and how to keep your wallet safe.

Your recovery phrase is the “master key” to your wallet and funds.

Now we need to login into our wallet. Press the metamask icon and then login



MetaMask - Chrome Web Store

chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn/related

Google Chrome isn't your default browser   Set as default

chrome web store   Sign in

Welcome Back!

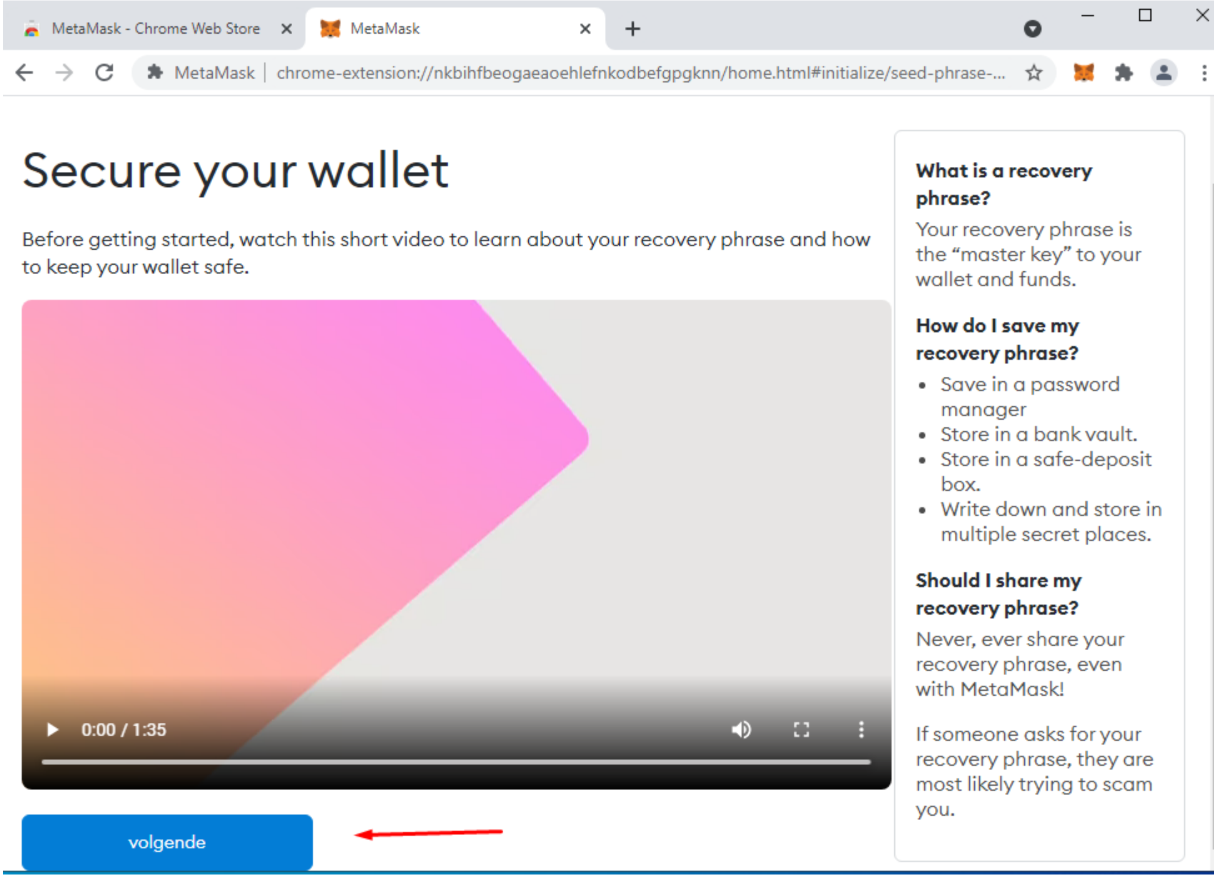
The decentralized web awaits

Password: ••••••••••••••

LOG IN

or import using Secret Recovery Phrase

Now scroll down and press next.



MetaMask - Chrome Web Store

MetaMask

MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/seed-phrase-...

Secure your wallet

Before getting started, watch this short video to learn about your recovery phrase and how to keep your wallet safe.

volgende

What is a recovery phrase?

Your recovery phrase is the "master key" to your wallet and funds.

How do I save my recovery phrase?

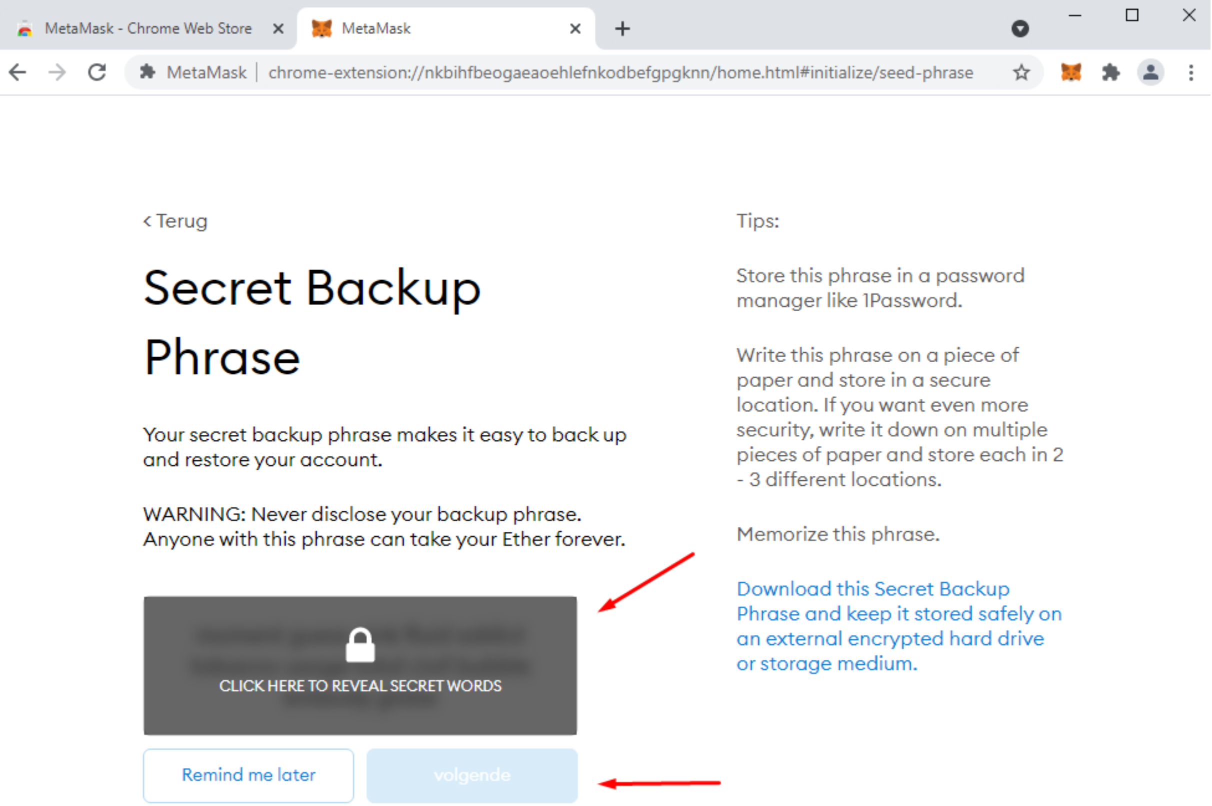
- Save in a password manager
- Store in a bank vault.
- Store in a safe-deposit box.
- Write down and store in multiple secret places.

Should I share my recovery phrase?

Never, ever share your recovery phrase, even with MetaMask!

If someone asks for your recovery phrase, they are most likely trying to scam you.

Once you have done that you need to save your secret words and click next



MetaMask - Chrome Web Store

MetaMask

MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/seed-phrase

< Terug

Secret Backup Phrase

Your secret backup phrase makes it easy to back up and restore your account.

WARNING: Never disclose your backup phrase. Anyone with this phrase can take your Ether forever.

CLICK HERE TO REVEAL SECRET WORDS

Remind me later

volgende

Tips:

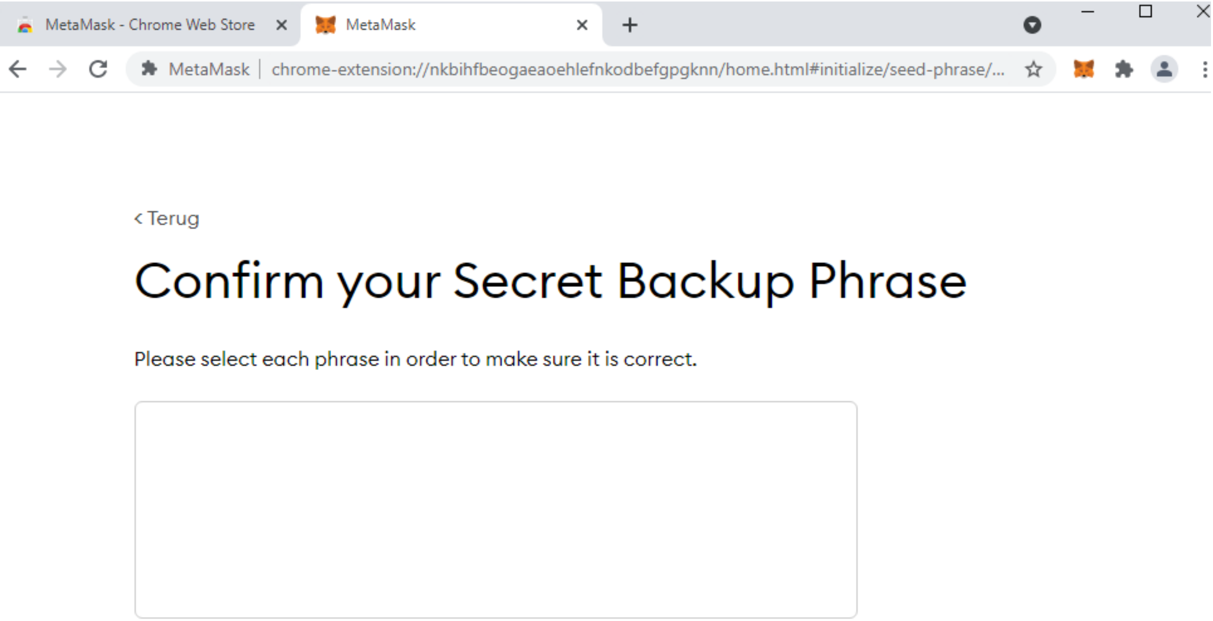
Store this phrase in a password manager like 1Password.

Write this phrase on a piece of paper and store in a secure location. If you want even more security, write it down on multiple pieces of paper and store each in 2 - 3 different locations.

Memorize this phrase.

Download this Secret Backup Phrase and keep it stored safely on an external encrypted hard drive or storage medium.

Now you need to fill in these words in the same order

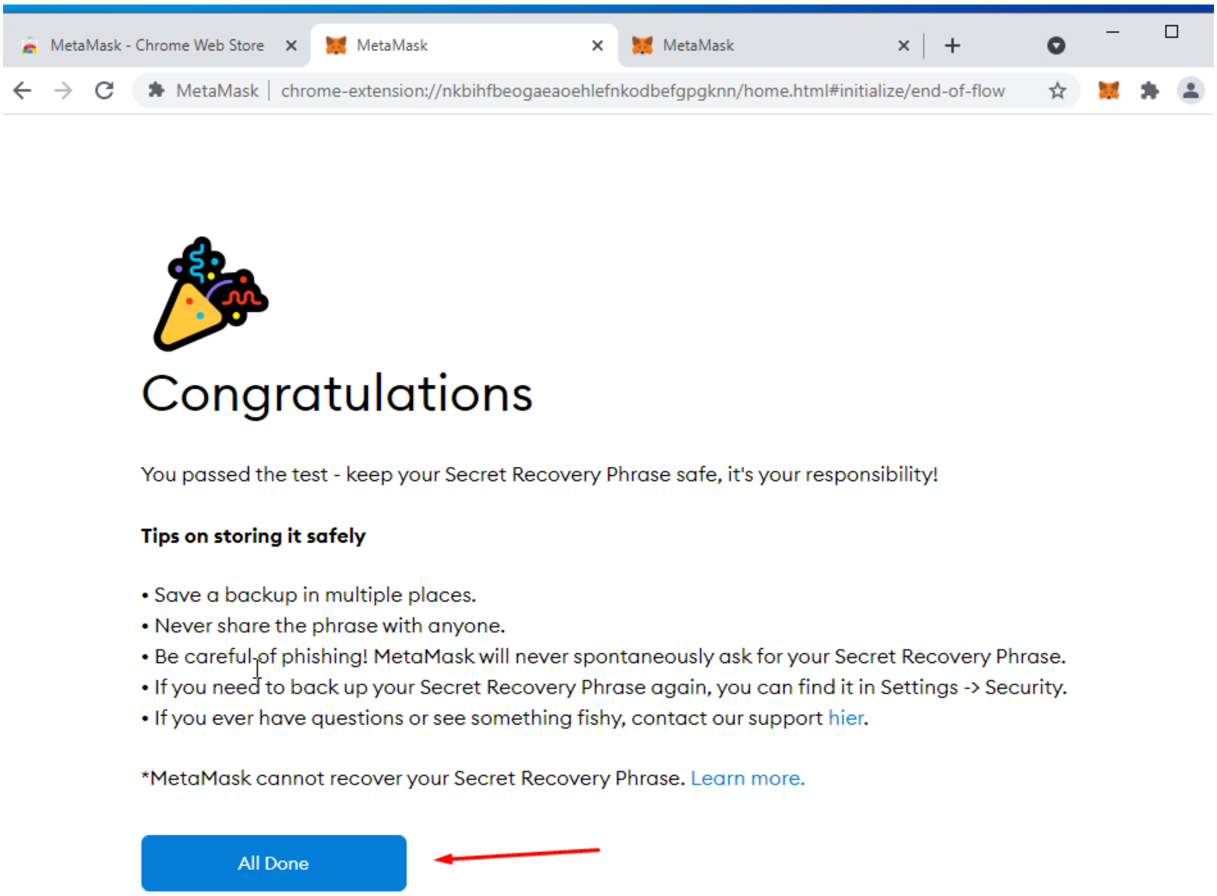

MetaMask - Chrome Web Store
MetaMask
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/seed-phrase/...

< Terug

Confirm your Secret Backup Phrase

Please select each phrase in order to make sure it is correct.

Next press “All Done” and login


MetaMask - Chrome Web Store
MetaMask
MetaMask
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#initialize/end-of-flow

Congratulations

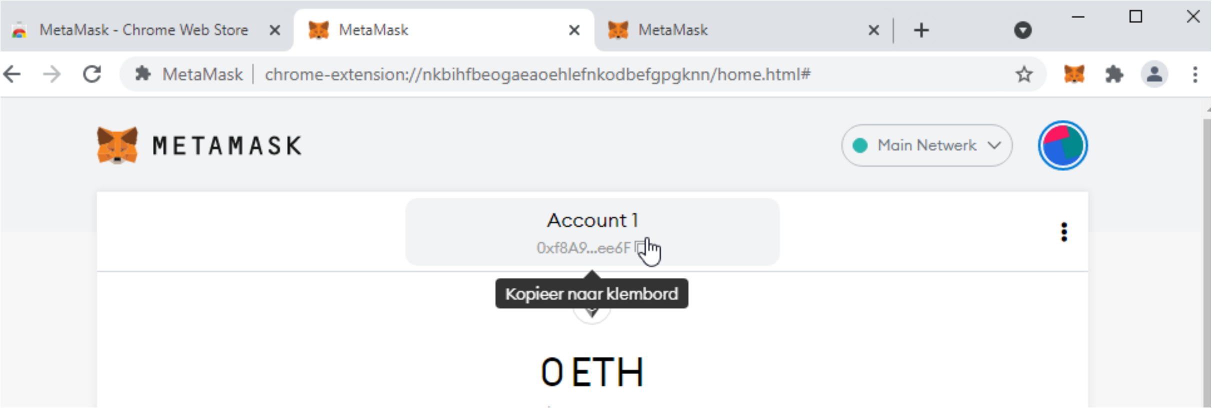
You passed the test - keep your Secret Recovery Phrase safe, it's your responsibility!

Tips on storing it safely

- Save a backup in multiple places.
- Never share the phrase with anyone.
- Be careful of phishing! MetaMask will never spontaneously ask for your Secret Recovery Phrase.
- If you need to back up your Secret Recovery Phrase again, you can find it in Settings -> Security.
- If you ever have questions or see something fishy, contact our support hier.

*MetaMask cannot recover your Secret Recovery Phrase. Learn more.

Now you need to copy your address hash, and we are done.

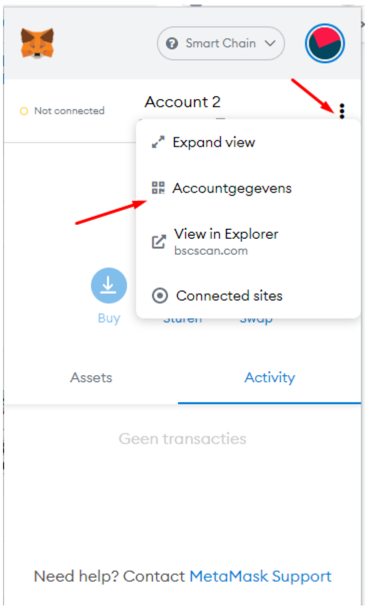


chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#

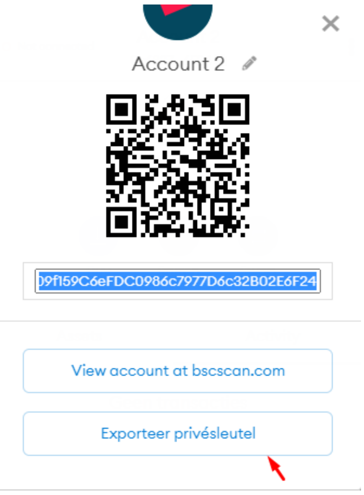
Account 1

0xf8A9...ee6F

Now you need to copy your secret key. To do this, open metamask, click on the 3 dots and click “account information”.



Now press “export private key”, then fill in your password and press confirm. Now you will see your private key



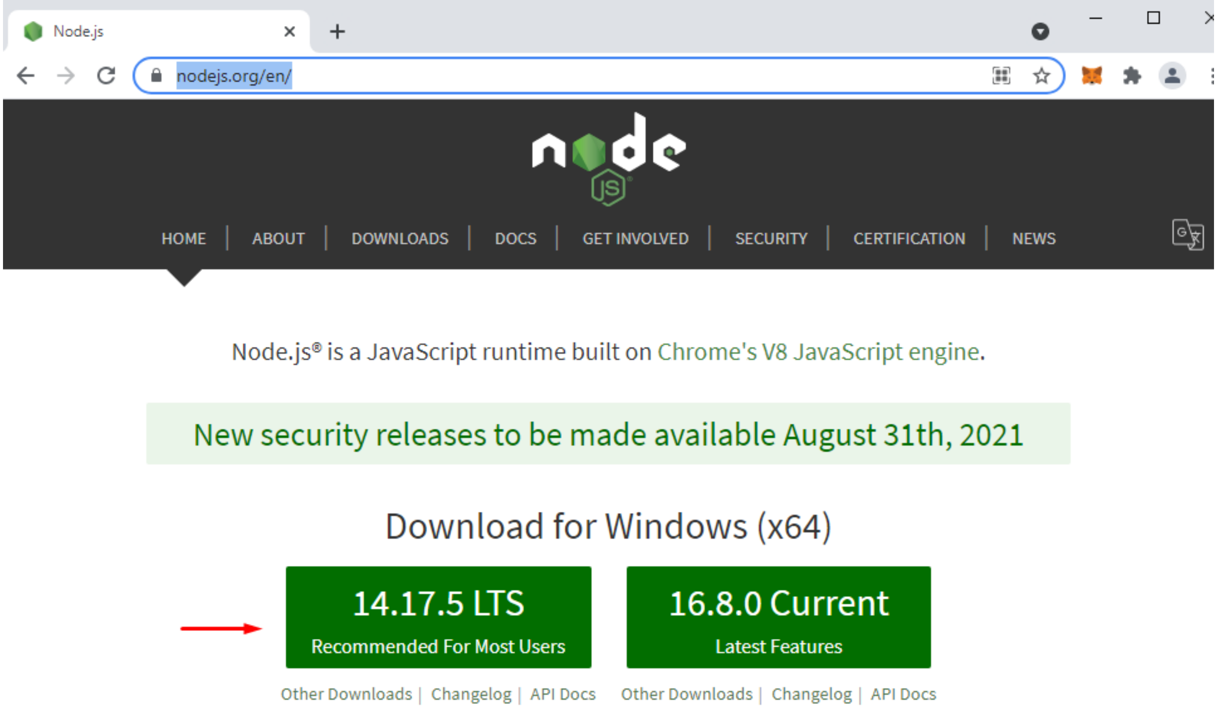
Account 2

09f159C6eFDC0986c7977D6c32B02E6F24

Setup the bot for Windows

Installing Nodejs

First of all we need install Nodejs, to do this go to https://nodejs.org/en/ And then press "Download for Windows Recommended for most users"



Node.js® is a JavaScript runtime built on Chrome's V8 JavaScript engine.

New security releases to be made available August 31th, 2021

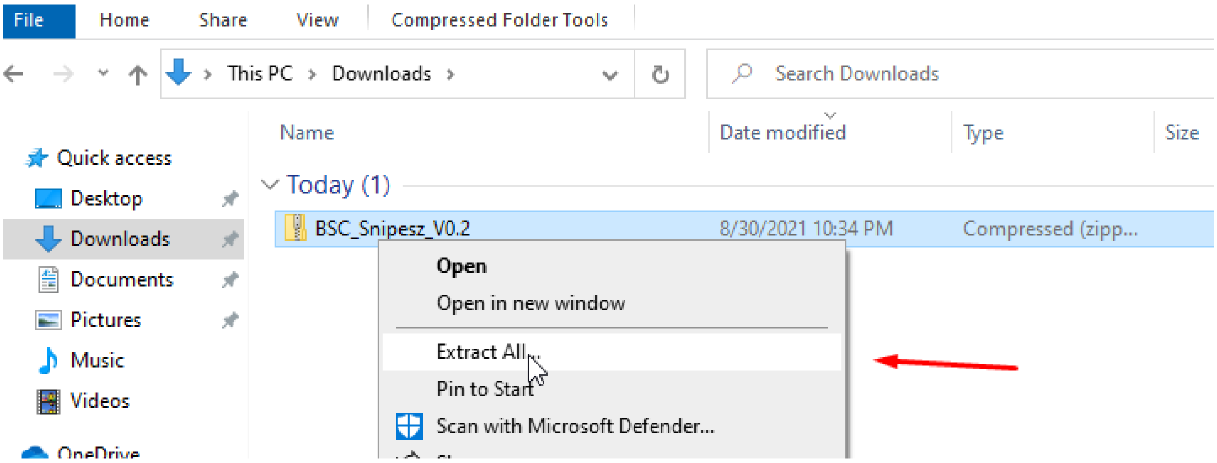
Download for Windows (x64)

14.17.5 LTS
Recommended For Most Users
16.8.0 Current
Latest Features
Other Downloads | Changelog | API Docs
Other Downloads | Changelog | API Docs

Now follow the installation wizard.

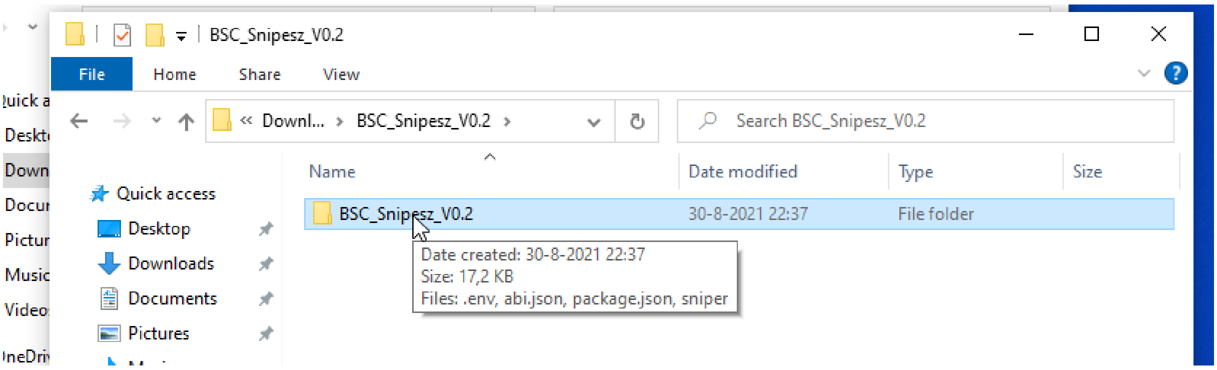
Installing the script

After you downloaded the script you need to unzip it. Go to your download folder, right click the BSC_Snipesz file and press extract file.



Name	Date modified	Type
BSC_Snipesz_V0.2	8/30/2021 10:34 PM	Compressed (zipp...

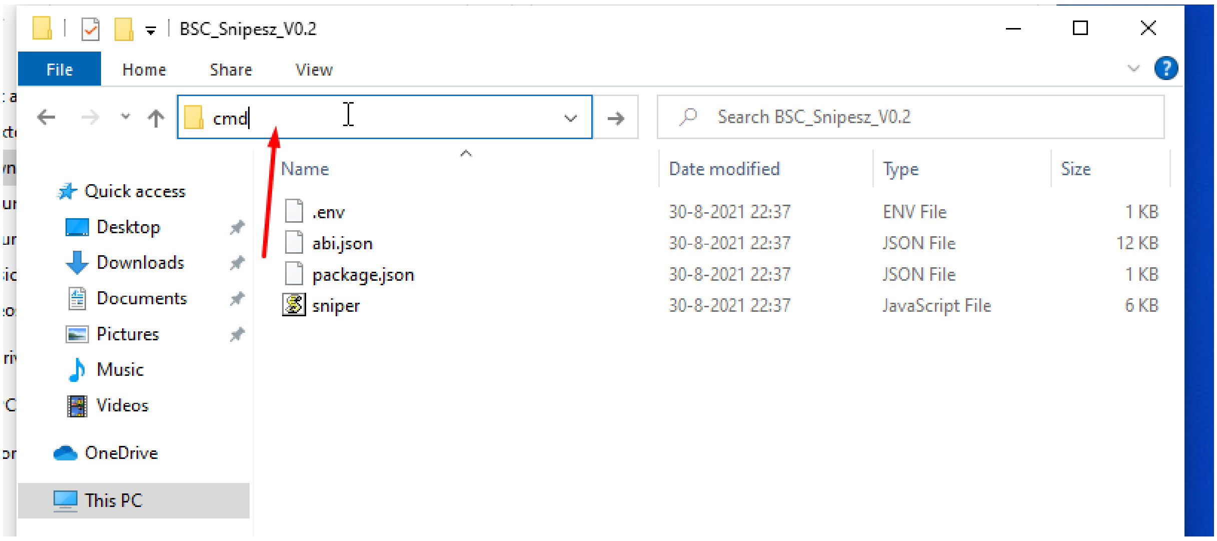
Open the next folder aswell.



Name	Date modified	Type	Size
BSC_Snipesz_V0.2	30-8-2021 22:37	File folder	

Date created: 30-8-2021 22:37
Size: 17,2 KB
Files: .env, abi.json, package.json, sniper

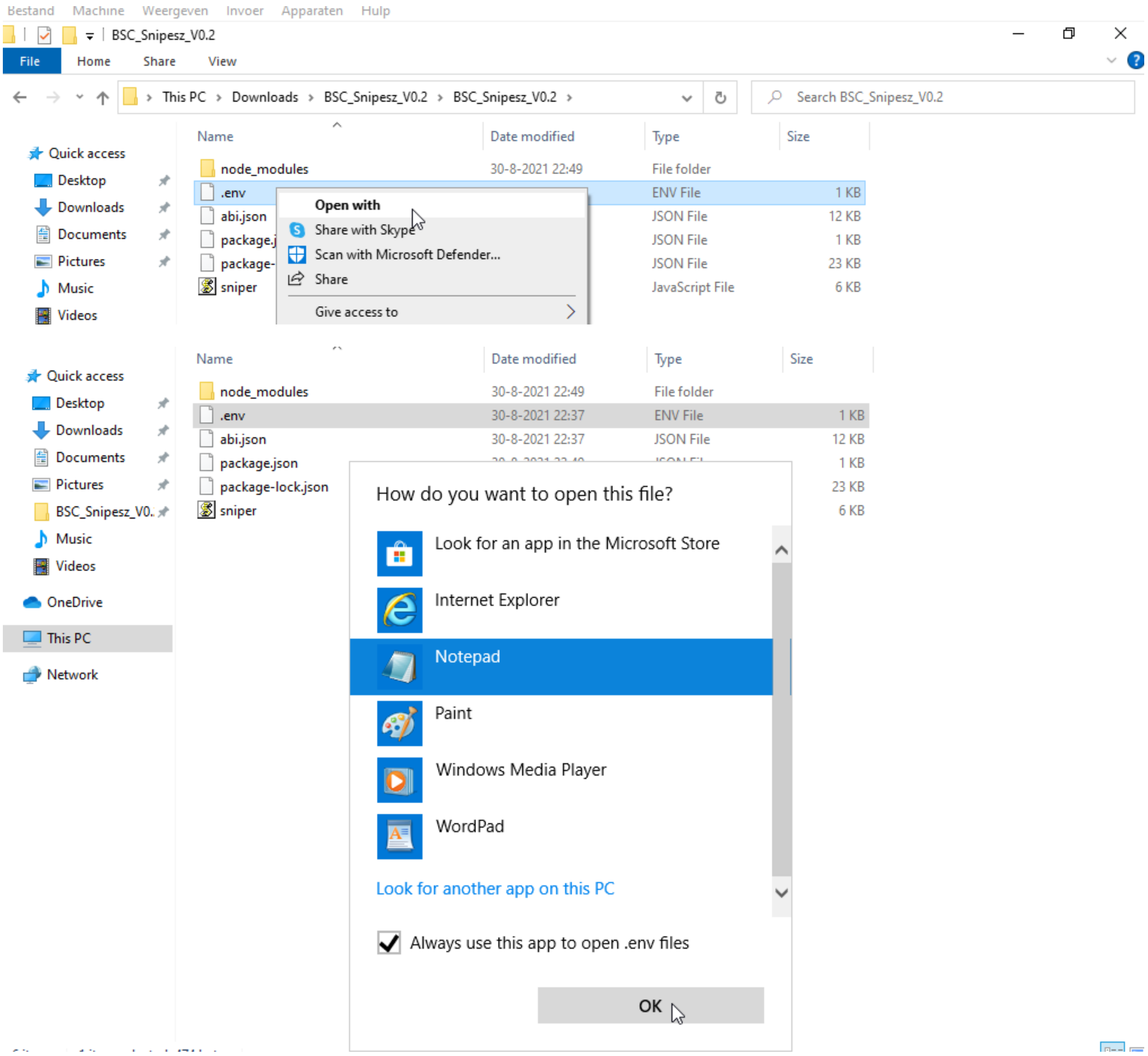
Next you will click this box, type: cmd, and press enter.



Name	Date modified	Type	Size
.env	30-8-2021 22:37	ENV File	1 KB
abi.json	30-8-2021 22:37	JSON File	12 KB
package.json	30-8-2021 22:37	JSON File	1 KB
sniper	30-8-2021 22:37	JavaScript File	6 KB

Open bot settings

You can find the bot settings in the .env file, to open the settings right click on the .env file, press open with and then press "notepad"



Name	Date modified	Type	Size
node_modules	30-8-2021 22:49	File folder	
.env	30-8-2021 22:37	ENV File	1 KB
abi.json	30-8-2021 22:37	JSON File	12 KB
package.json		JSON File	1 KB
package-lock.json		JSON File	23 KB
sniper		JavaScript File	6 KB

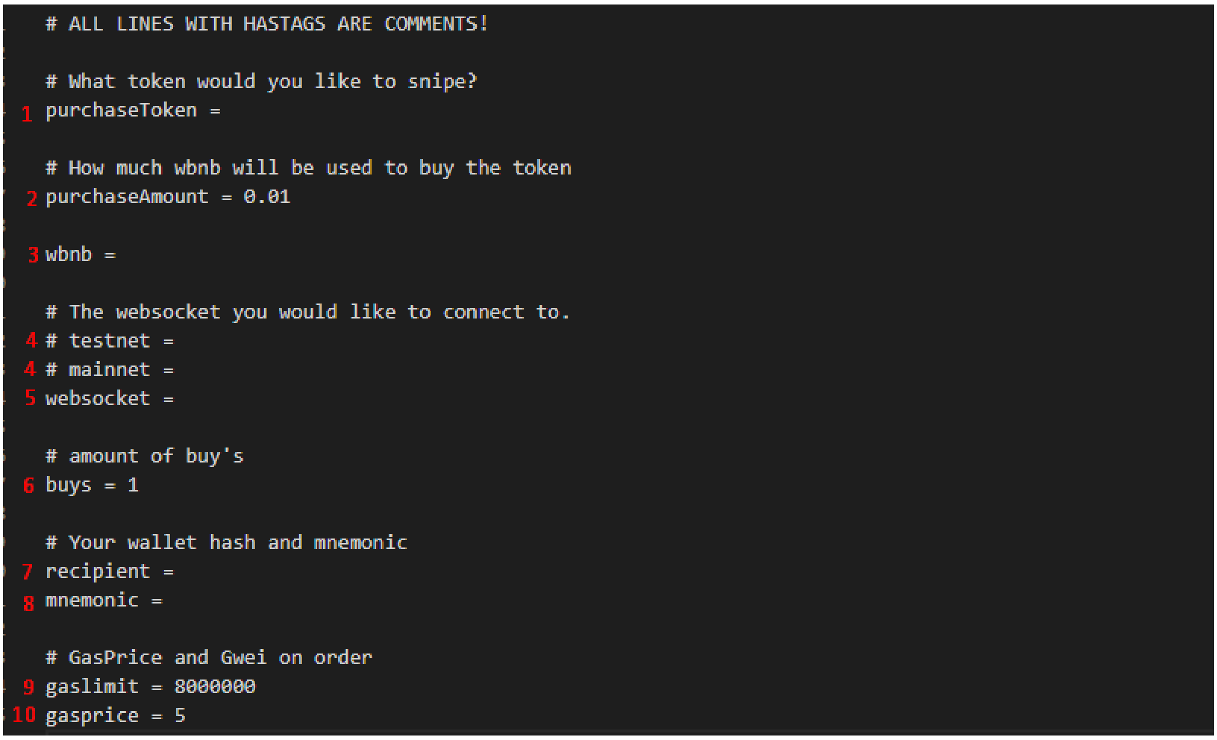
How do you want to open this file?

- Look for an app in the Microsoft Store
- Internet Explorer
- Notepad
- Paint
- Windows Media Player
- WordPad

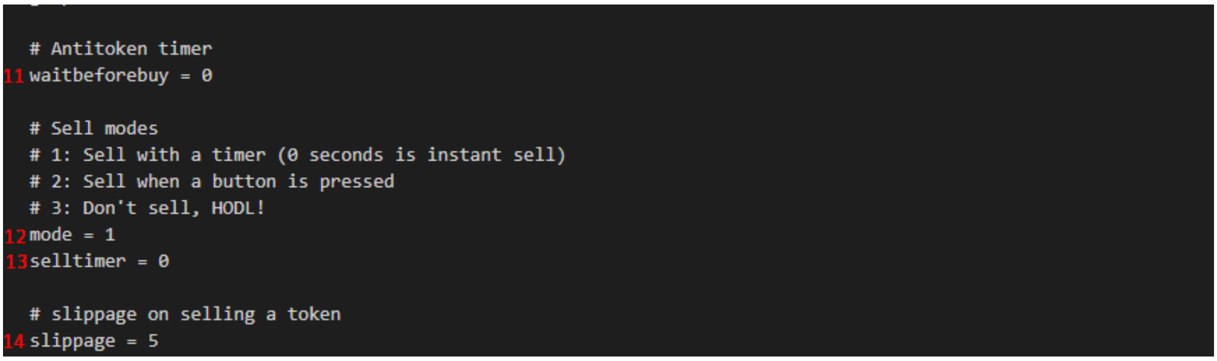
Look for another app on this PC

☑ Always use this app to open .env files

Edit bot settings



```
   # ALL LINES WITH HASTAGS ARE COMMENTS!

   # What token would you like to snipe?
1  purchaseToken =

   # How much wbnb will be used to buy the token
2  purchaseAmount = 0.01

3  wbnb =

   # The websocket you would like to connect to.
4  # testnet =
4  # mainnet =
5  websocket =

   # amount of buy's
6  buys = 1

   # Your wallet hash and mnemonic
7  recipient =
8  mnemonic =

   # GasPrice and Gwei on order
9  gaslimit = 8000000
10 gasprice = 5
```



```
   # Antitoken timer
11 waitbeforebuy = 0

   # Sell modes
   # 1: Sell with a timer (0 seconds is instant sell)
   # 2: Sell when a button is pressed
   # 3: Don't sell, HODL!
12 mode = 1
13 selltimer = 0

   # slippage on selling a token
14 slippage = 5
```

1. purchaseToken: Fill in the contract address for the token you would like to snipe
2. purchaseAmount: How much would you like to buy of this token in wbnb (The bot is using wbnb because the event to trade with is faster than paying with bnb. so make sure you have enough wbnb)
3. wbnb: Here you fill in the contract address for wbnb, it can depend if you are sniping on the mainnet or testnet for which one you need. But here are both contracts:
   a. Mainnet: 0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c
   b. Testnet: 0xae13d989daC2f0dEbFf460aC112a837C89BAa7cd
4. # testnet / mainnet: these are my place holders to save my websocket url's
5. websocket: Fill in your websocket url, more about this on page 14.
6. buys: fill in how many buy orders you would like to perform, by default this is 1. For example if you filling in 5, the bot will do 5 buy orders
7. recipient: Fill in your wallet hash, I have explained how to get this on page 8.
8. Mnemonic (now privatekey): Fill in your wallet privatekey, I have explained how to get this on page 8.

9. gaslimit: Fill in the amount of gaslimit, I recommend using 8.000.000 to 22.000.000 for a big launch, however in my videos I use 800.000 and this works fine aswell. If you fill in less, you can end up skipping a block.
10. gasprice: This is how much gwei you want to use, I always recommend using 5 over here.
11. Waitbeforebuy: here you fill in seconds how long you want to wait before buying. This is the antibot function.
12. Mode: this is what you would like to do after you have sniped a token.
13. selltimer: this only works for mode one. Fill in the time in seconds you want to wait before selling.
14. Slippage: this is the slippage set for selling a token, simple buy and simple approve.

How to use a websocket?

A websocket is the type of connection to interact with a fullnode. A fullnode is a server in the blockchain that receives all data of what is happening. So with a websocket we can have access to this data.

Create a mainnet websocket

For the mainnet I always recommend hosting your own fullnode. But this can be expensive, so you can hire a websocket url aswell. When using free websocket url's I noticed they aren't that fast.

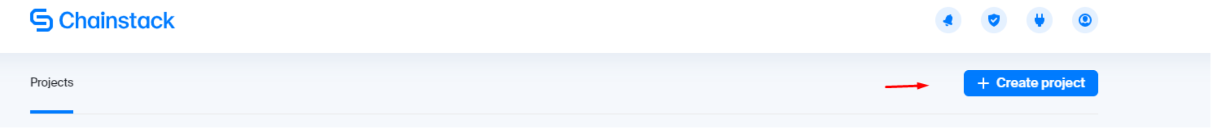
I Personally use chainstack. They are fast and provide you with 3.000.000 free requests every month. After that you will pay 10$ for 1.000.000 requests. They are also hosted on aws, so you can run the bot on aws aswell and it gets close to hosting your own fullnode.

The bot does around 200k requests every 10 min

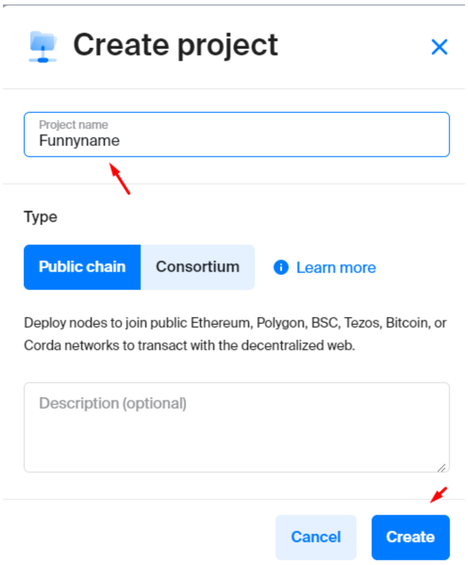
https://chainstack.com/

After creating a chainstack, login and go to https://console.chainstack.com/projects

Now you want to press "Create project"

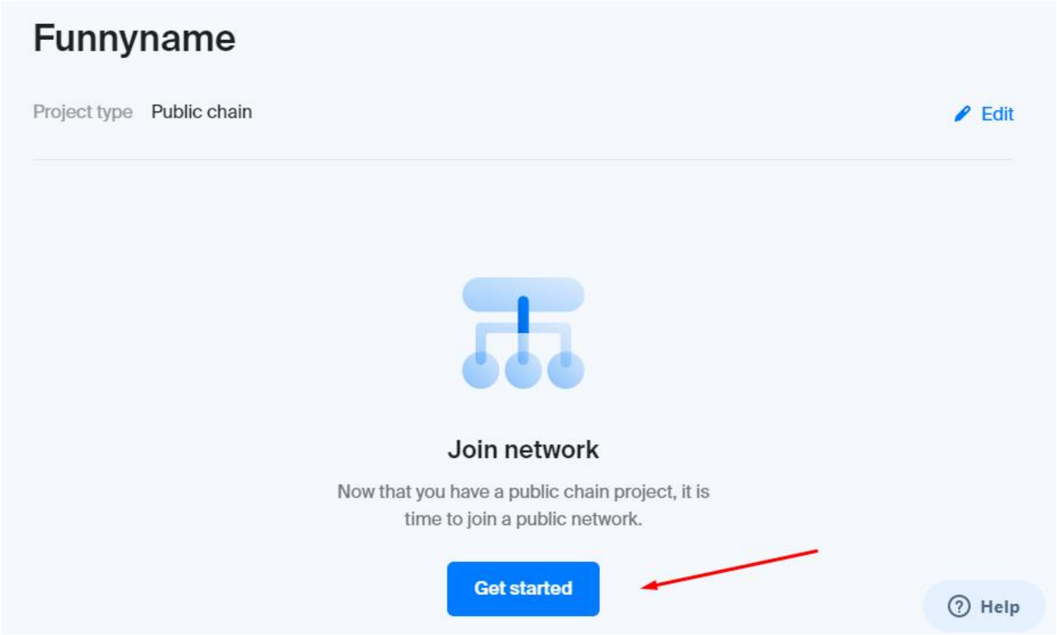


Give it an name an press "Create".



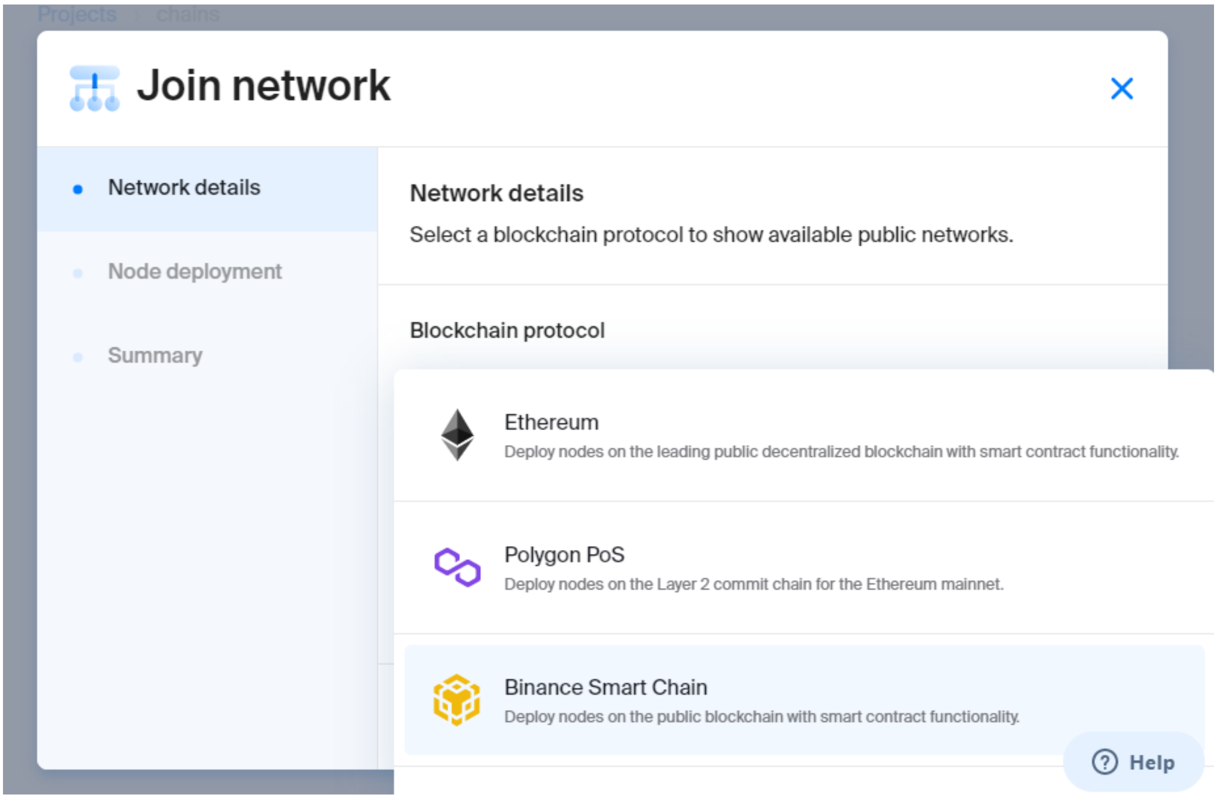
Deploy nodes to join public Ethereum, Polygon, BSC, Tezos, Bitcoin, or Corda networks to transact with the decentralized web.

Click on your project and after that press “Get Started”



Now that you have a public chain project, it is time to join a public network.

Now you want to click on “Select blockchain protocol” and then press Binance Smart Chain.



Join network

- Network details
- Node deployment
- Summary

Network details

Select a blockchain protocol to show available public networks.

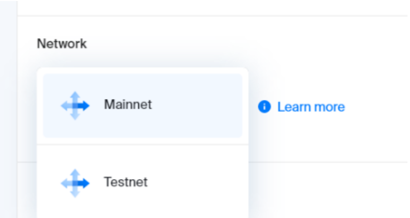
Blockchain protocol

Ethereum
Deploy nodes on the leading public decentralized blockchain with smart contract functionality.

Polygon PoS
Deploy nodes on the Layer 2 commit chain for the Ethereum mainnet.

Binance Smart Chain
Deploy nodes on the public blockchain with smart contract functionality.

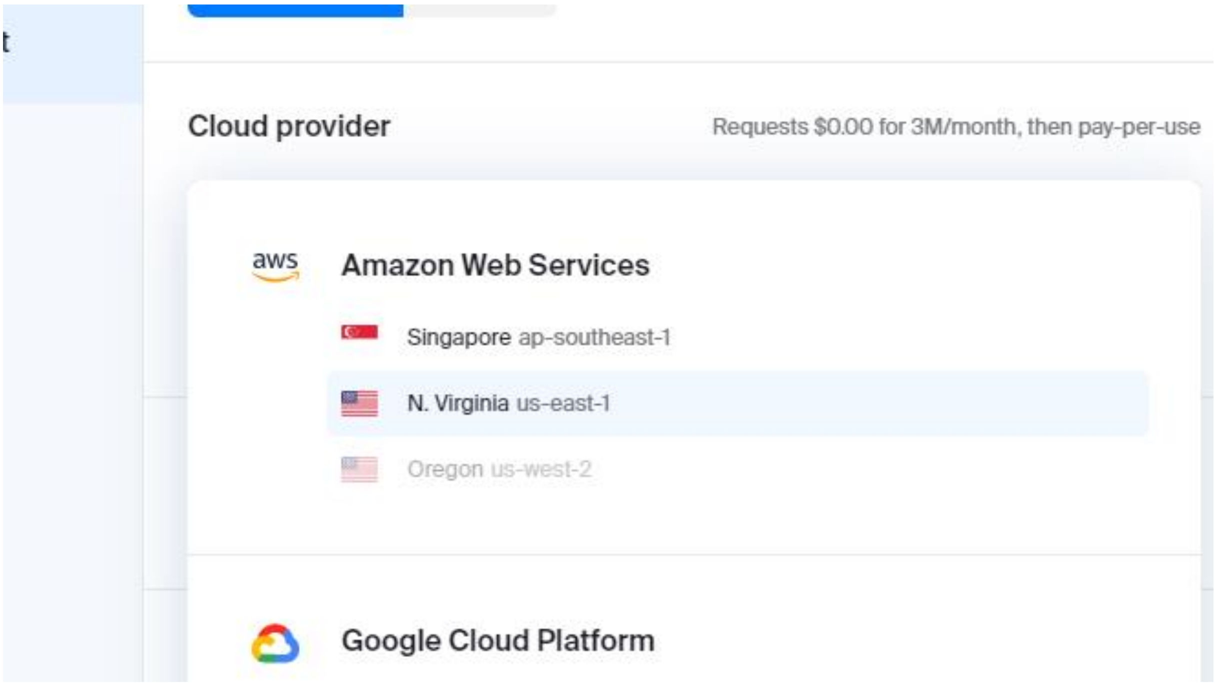
After that we select the “Mainnet” and then press “Next”


Network

Mainnet

Testnet

At node deployment press “Select Cloud Provider”. In this case I selected N. Virginia. And as you can see the node is hosted at AWS so later in this guide I will show you how to get a server over there.



Cloud provider

Requests $0.00 for 3M/month, then pay-per-use

Amazon Web Services

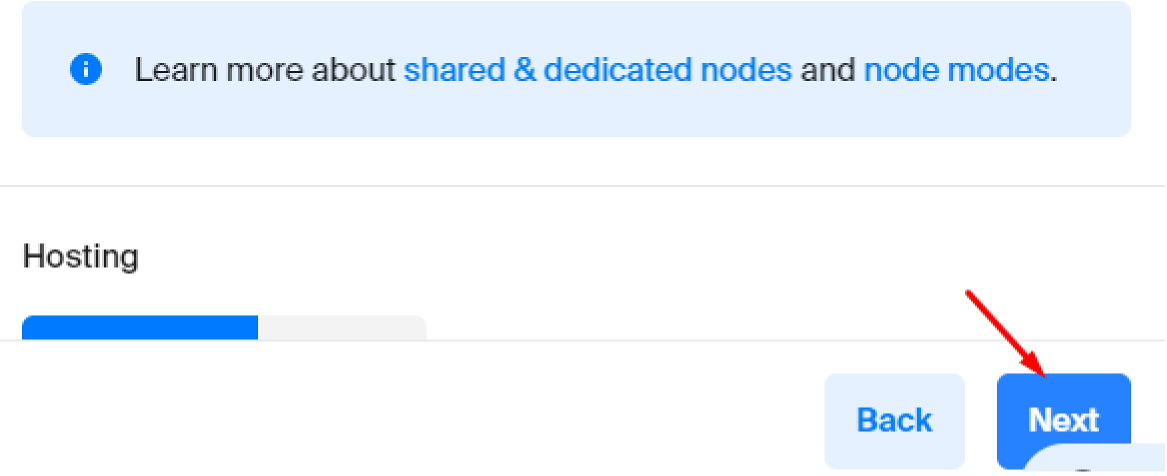
Singapore ap-southeast-1

N. Virginia us-east-1

Oregon us-west-2

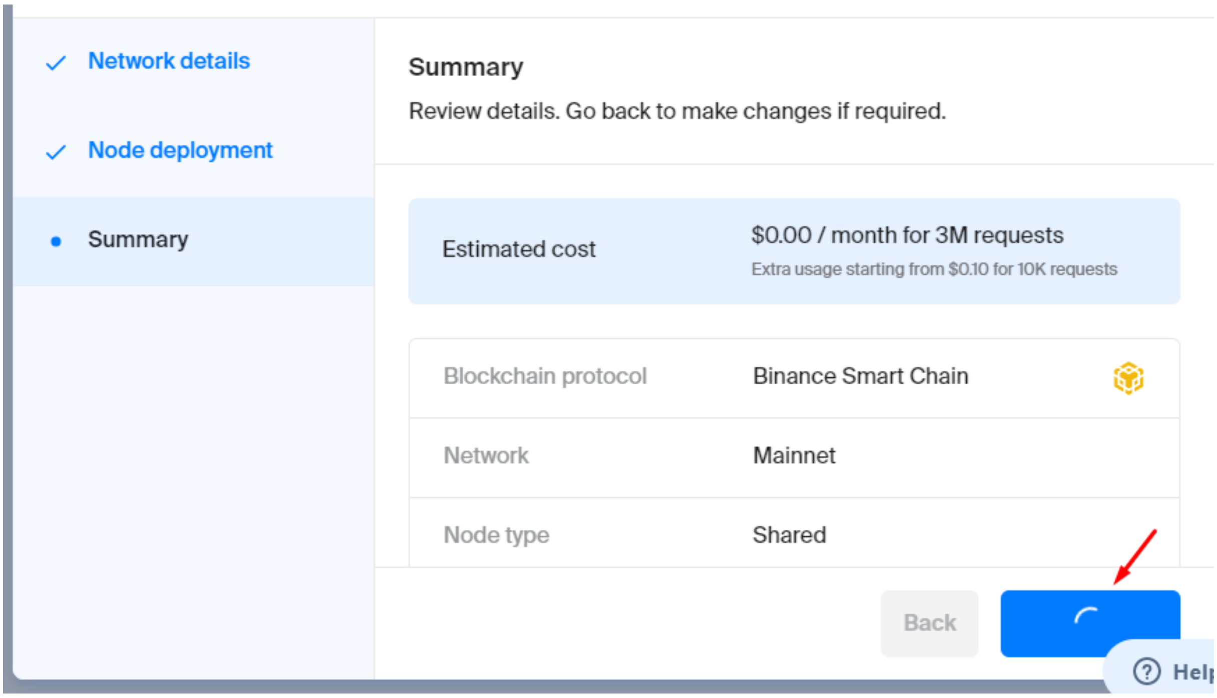
Google Cloud Platform

Now press “Next” and then “Join Network”.



Learn more about shared & dedicated nodes and node modes.

Hosting



✓ Network details

✓ Node deployment

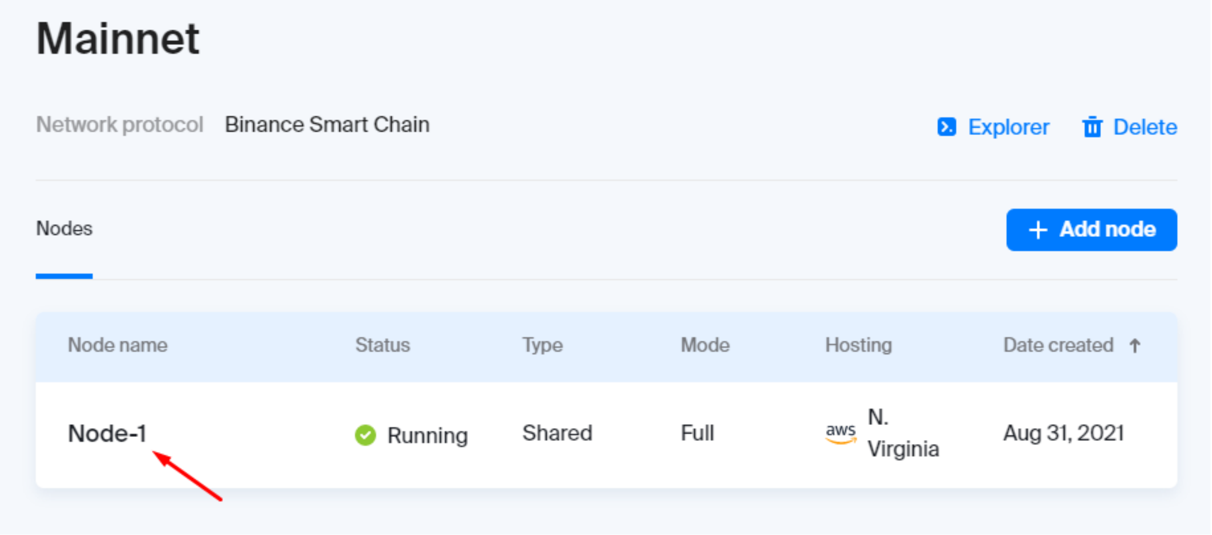
● Summary

Summary

Review details. Go back to make changes if required.

Estimated cost	$0.00 / month for 3M requests Extra usage starting from $0.10 for 10K requests
Blockchain protocol	Binance Smart Chain
Network	Mainnet
Node type	Shared

Now you need to wait some time before it gets activated. When it is activated you click on you node.

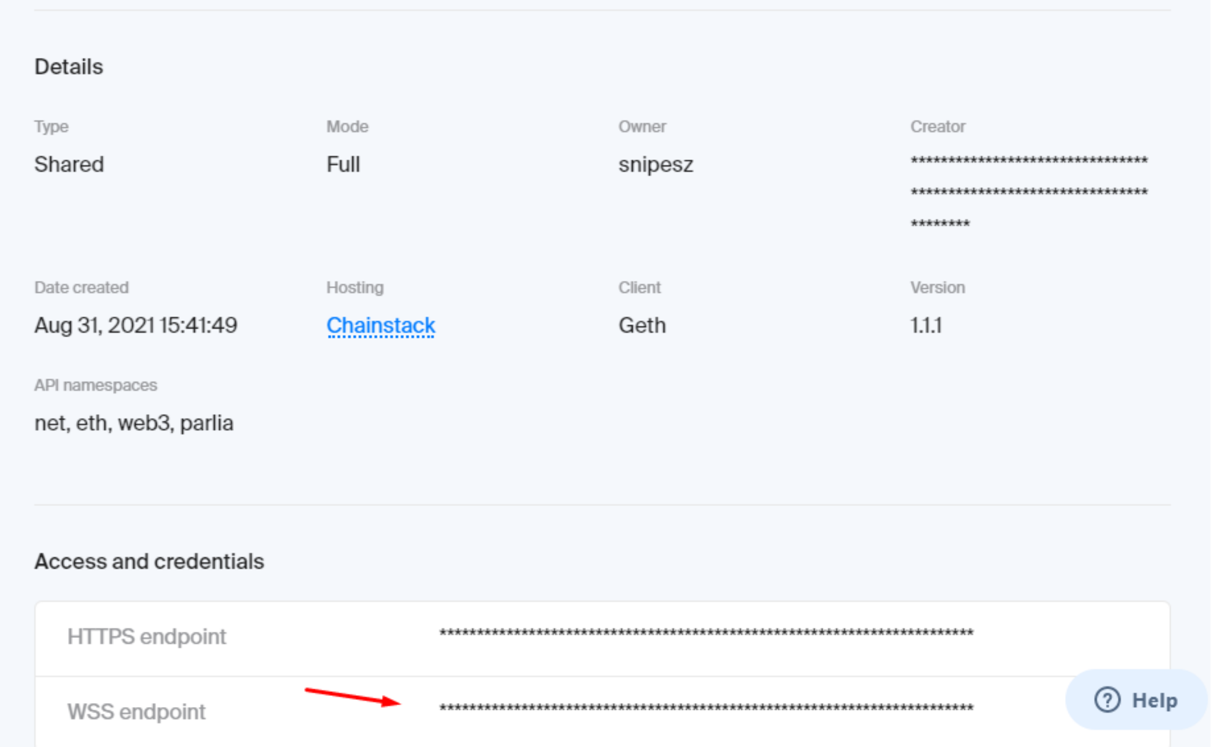


Mainnet

Network protocol Binance Smart Chain

Node name	Status	Type	Mode	Hosting	Date created ↑
Node-1	✓ Running	Shared	Full	aws N. Virginia	Aug 31, 2021

Now we can see our Websocket url. You can copy this and past it in your .env file.



Details

Type	Mode	Owner	Creator
Shared	Full	snipesz	******************************** ******************************** ********
Date created	**Hosting**	**Client**	**Version**
Aug 31, 2021 15:41:49	Chainstack	Geth	1.1.1

API namespaces

net, eth, web3, parlia

Access and credentials

HTTPS endpoint	**
WSS endpoint	**

To see how many requests you have done checkout: https://console.chainstack.com/user/settings/billing

Create a testnet websocket

For the testnet I personaly use moralis. They are fast and free to use.

https://moralis.io/

Setup the bot for AWS/Linux

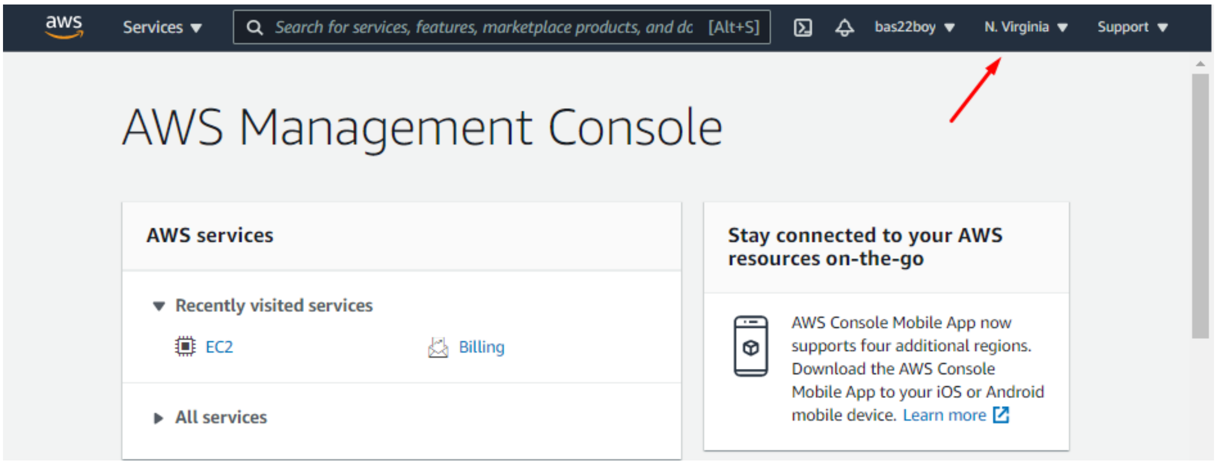
The best way to connect your bot is by using your own fullnode, but if you can't afford it I recommend running the bot on a AWS server. This can be a pain in the ass to set it up, but it is definitely worth it.

You first need to create a aws account. To do this you need to go to https://portal.aws.amazon.com/billing/signup#/start

After you created you AWS account you need to go to:

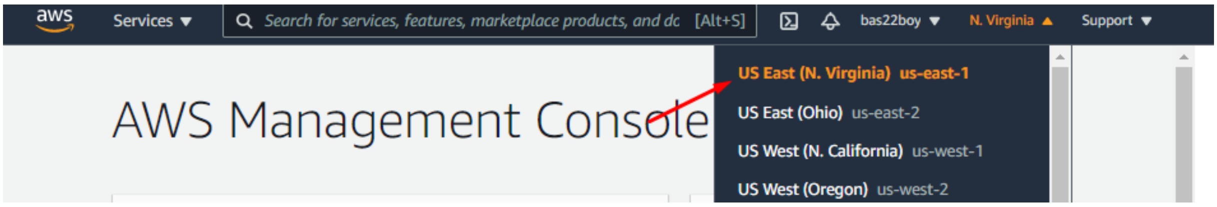
https://console.aws.amazon.com/console/home

Press the region option to the right of your name,

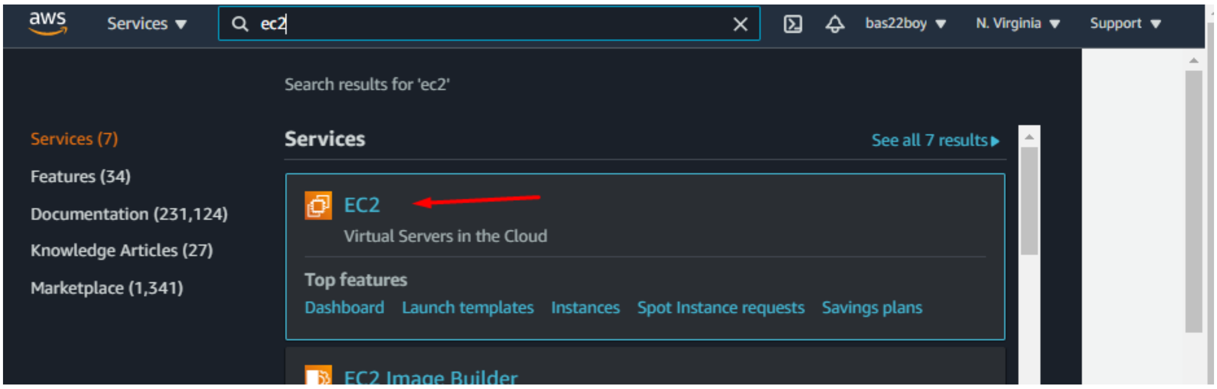

aws
Services ▼
Search for services, features, marketplace products, and dc [Alt+S]
bas22boy ▼
N. Virginia ▼
Support ▼
AWS Management Console
AWS services
▼ Recently visited services
EC2
Billing
▶ All services
Stay connected to your AWS resources on-the-go

AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

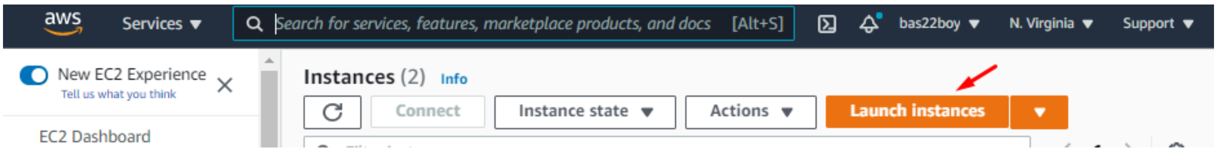
Then select "N. Virginia"


aws
Services ▼
Search for services, features, marketplace products, and dc [Alt+S]
bas22boy ▼
N. Virginia ▲
Support ▼
AWS Management Console
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2

Now we are going to create a vps. At the top of your screen press the search bar and type "ec2". Click on the first option.

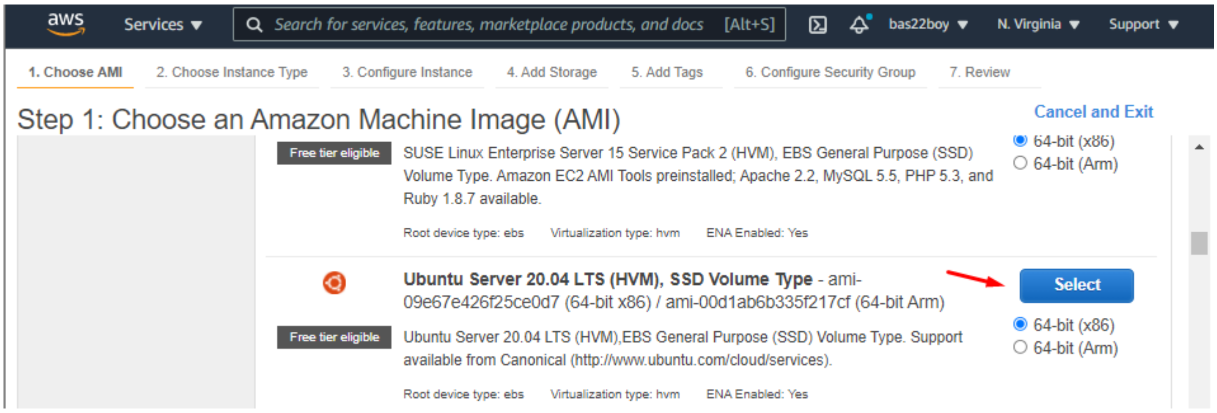


After that you press the orange “Launch instances” button.



Configure VPS

Then you scroll down a bit and select the ubuntu server option.



Step 1: Choose an Amazon Machine Image (AMI)

SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

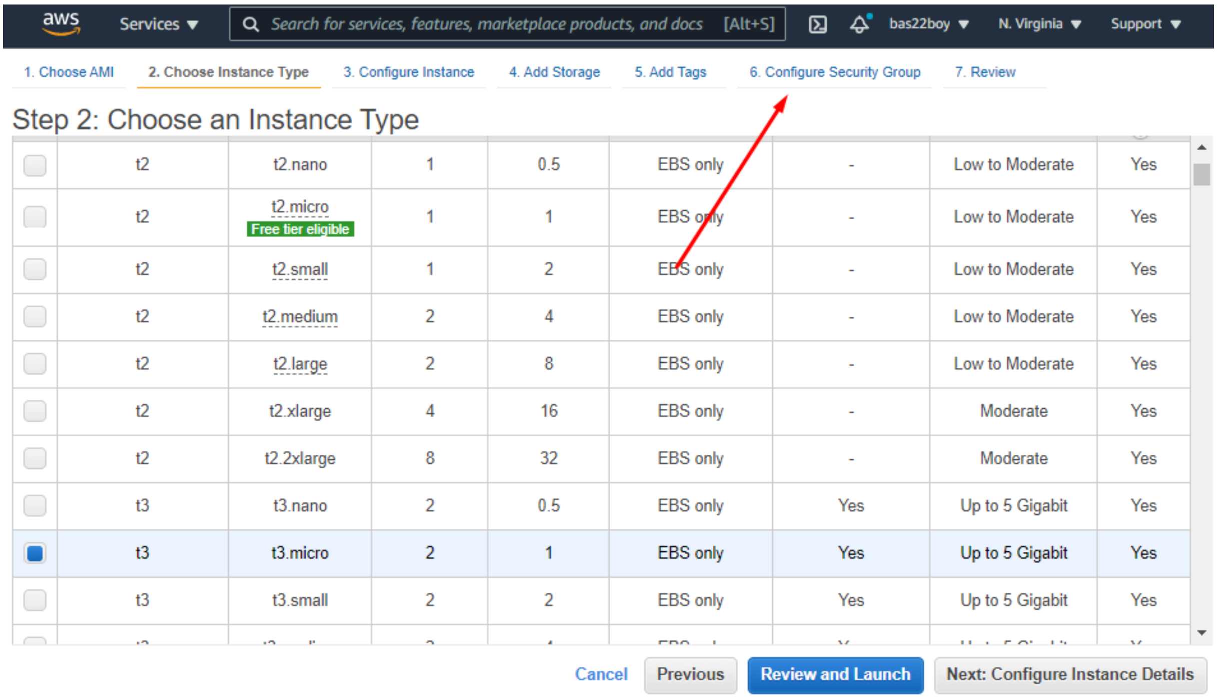
Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-09e67e426f25ce0d7 (64-bit x86) / ami-00d1ab6b335f217cf (64-bit Arm)

Ubuntu Server 20.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

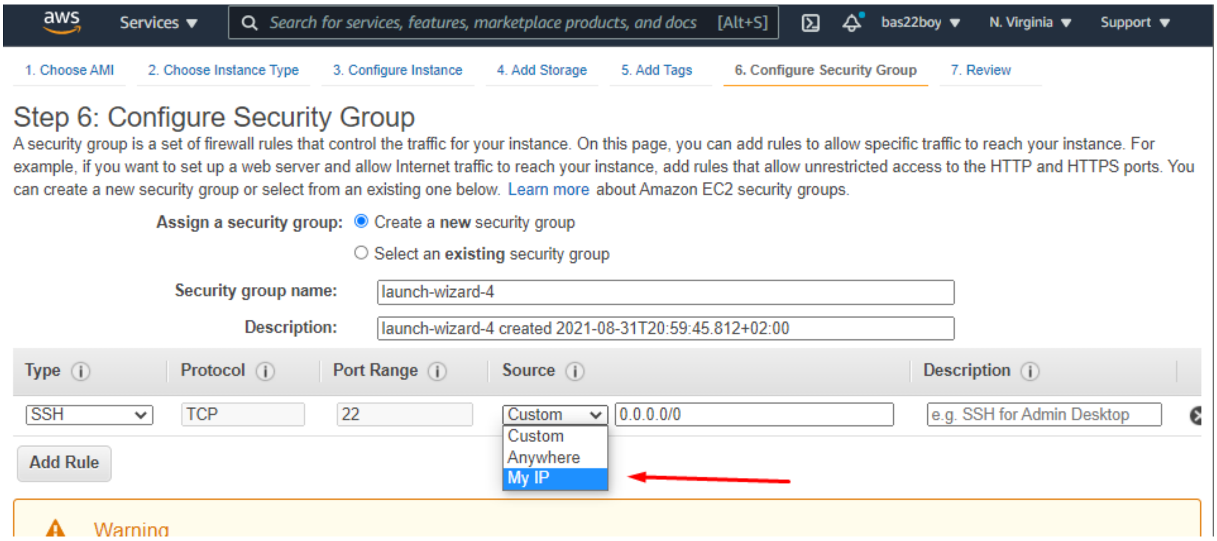
Now you can choose what type of server hardware you want. I selected t3.micro, but you can choose whatever you want, and press “Configure Security Group”.



Step 2: Choose an Instance Type

☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☐	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
☐	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
☐	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
☐	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
☑	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes

Then you need to press “custom” and then select “My ip”.



aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
bas22boy ▼
N. Virginia ▼
Support ▼

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

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.

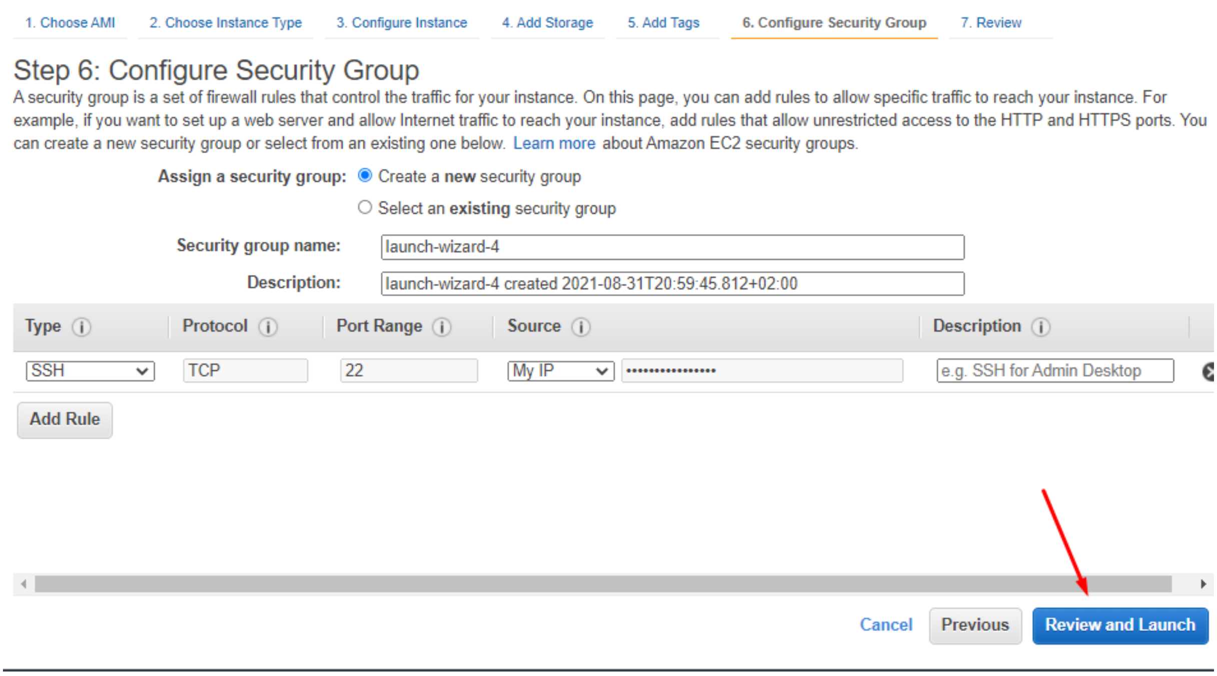
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: launch-wizard-4

Description: launch-wizard-4 created 2021-08-31T20:59:45.812+02:00

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

The next step is pressing “Review and Launch”.



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

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.

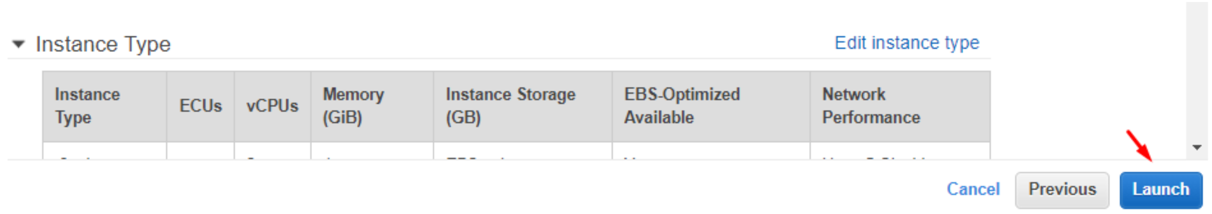
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: launch-wizard-4

Description: launch-wizard-4 created 2021-08-31T20:59:45.812+02:00

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	My IP	•••••••••••••••••	e.g. SSH for Admin Desktop

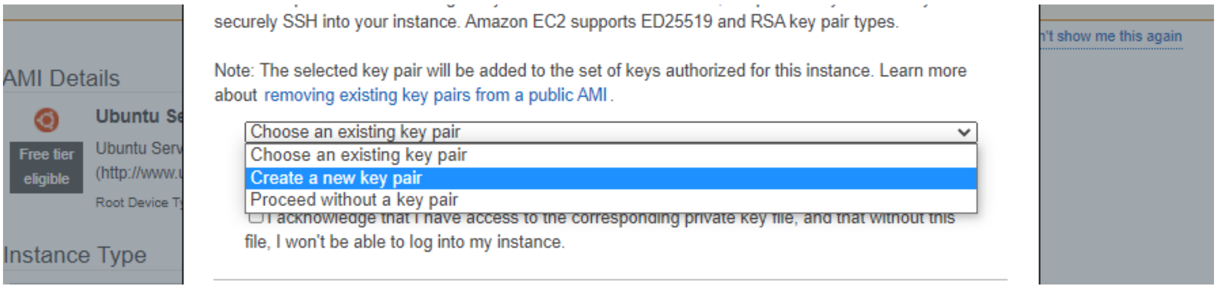
Then press “Launch”.



▼ Instance Type Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance

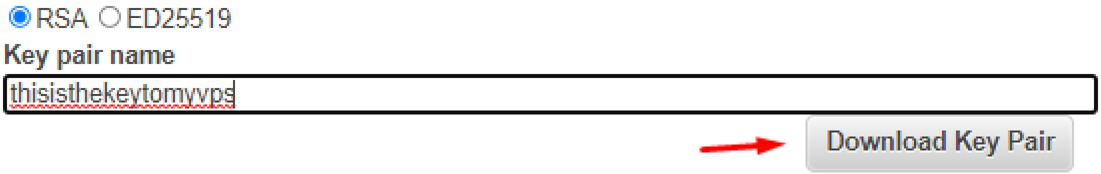
AWS will now ask you to create a key. Hit the option “Create new key pair”. Now you need to create a key pair name. Call it whatever you like and press “Download key pair”.



securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

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 .

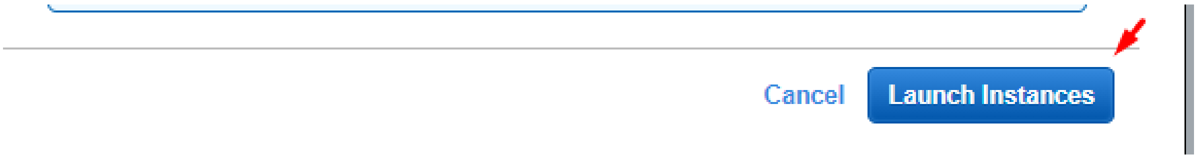
□ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.



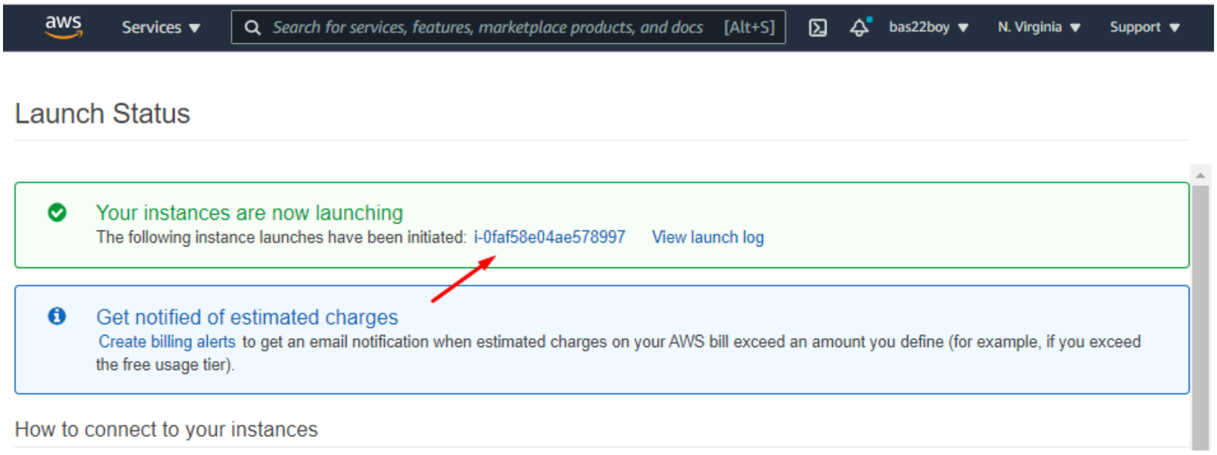
● RSA ○ ED25519

Key pair name: thisisthekeytomyvps

After downloading press “Launch Instances”.



Then press you’re instance.



aws
Services ▾
Search for services, features, marketplace products, and docs [Alt+S]
bas22boy ▾
N. Virginia ▾
Support ▾

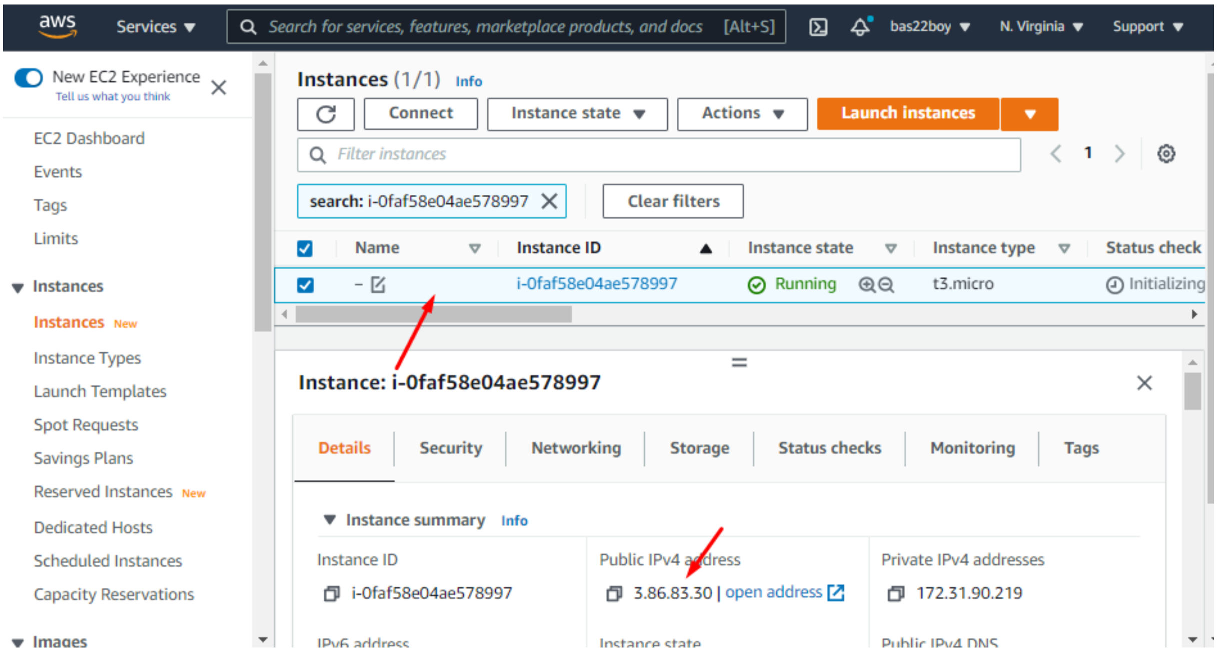
Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0faf58e04ae578997 View launch log

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

Now you want to click on your instance again and copy your ip for later.



Instances (1/1) Info

search: i-0faf58e04ae578997

☑	Name	Instance ID	Instance state	Instance type	Status check
☑	–	i-0faf58e04ae578997	Running	t3.micro	Initializing

Instance: i-0faf58e04ae578997

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0faf58e04ae578997	3.86.83.30 | open address	172.31.90.219
IPv6 address	Instance state	Public IPv4 DNS

Change permissions of the pem file

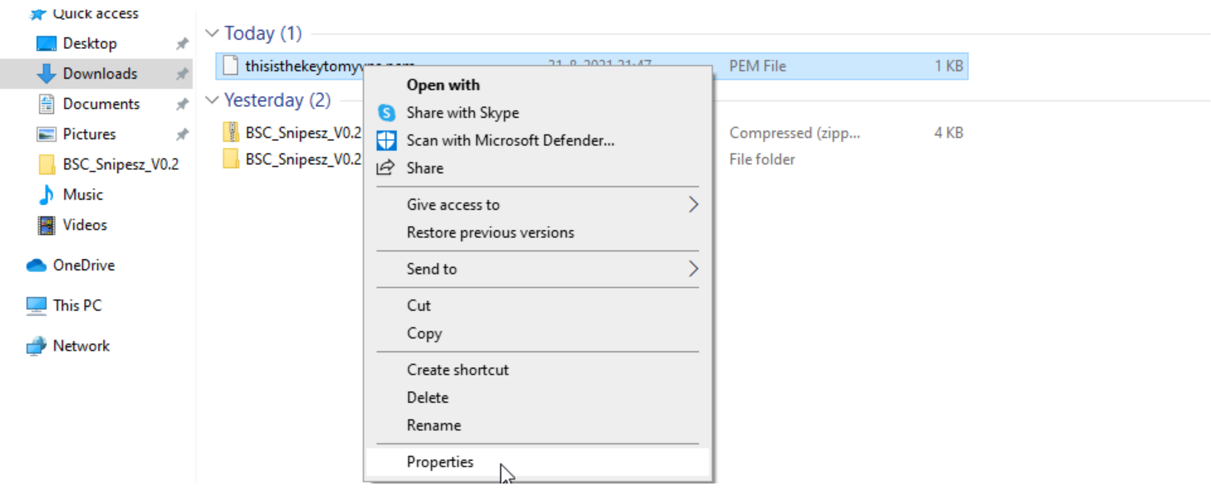
To connect to our vps we first need to change the permission of our pem file. If you are using a linux machine this is quite easy on windows its more difficult.

Change pem permissions linux

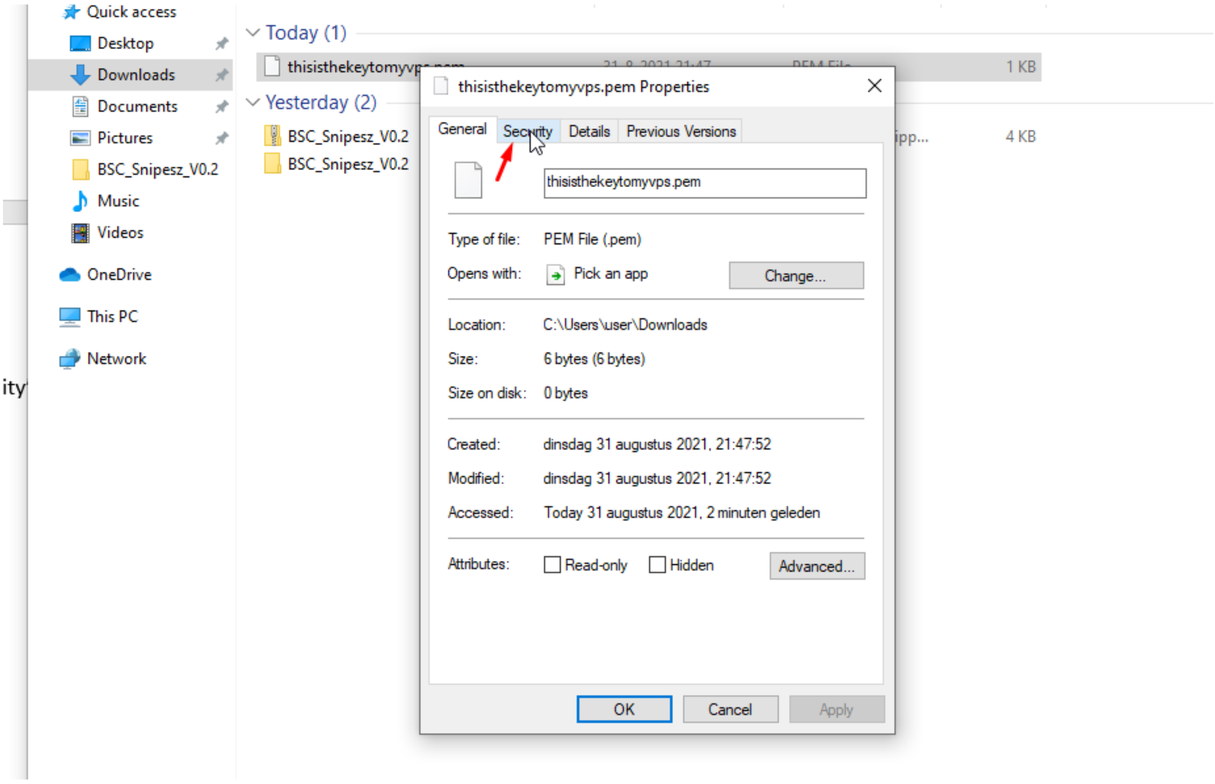
In your console cd to your pem file and then type “chmod 400 pemkeyfilename.pem”

Change pem permissions Windows

First you want to go to your downloads folder and right click your pem file. Then you press “properties” at the bottom.



Then press “security” at the top.



thisisthekeytomyvps.pem

Type of file: PEM File (.pem)

Opens with: Pick an app

Location: C:\Users\user\Downloads

Size: 6 bytes (6 bytes)

Size on disk: 0 bytes

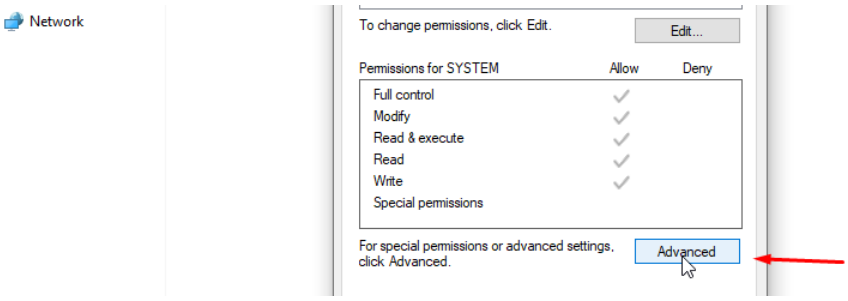
Created: dinsdag 31 augustus 2021, 21:47:52

Modified: dinsdag 31 augustus 2021, 21:47:52

Accessed: Today 31 augustus 2021, 2 minuten geleden

Attributes: ☐ Read-only ☐ Hidden

Now you need to select the “advanced option”.

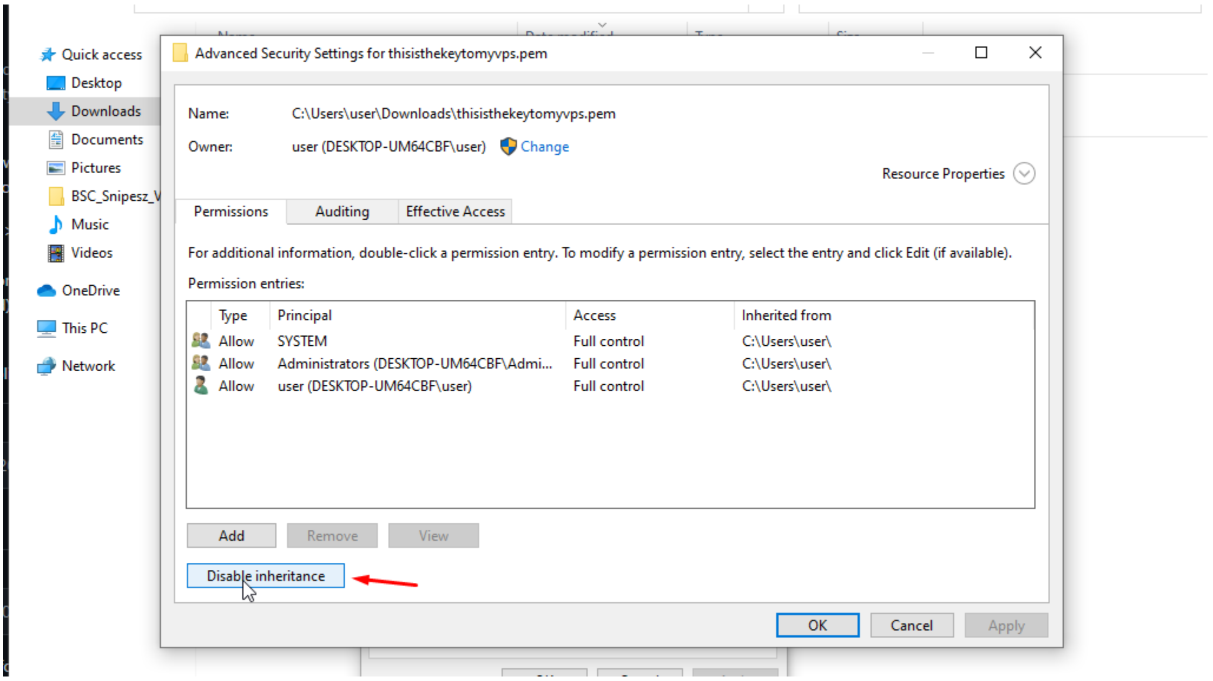


To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

When you have done that press “Disable inheritance”



Advanced Security Settings for thisisthekeytomyvps.pem

Name: C:\Users\user\Downloads\thisisthekeytomyvps.pem

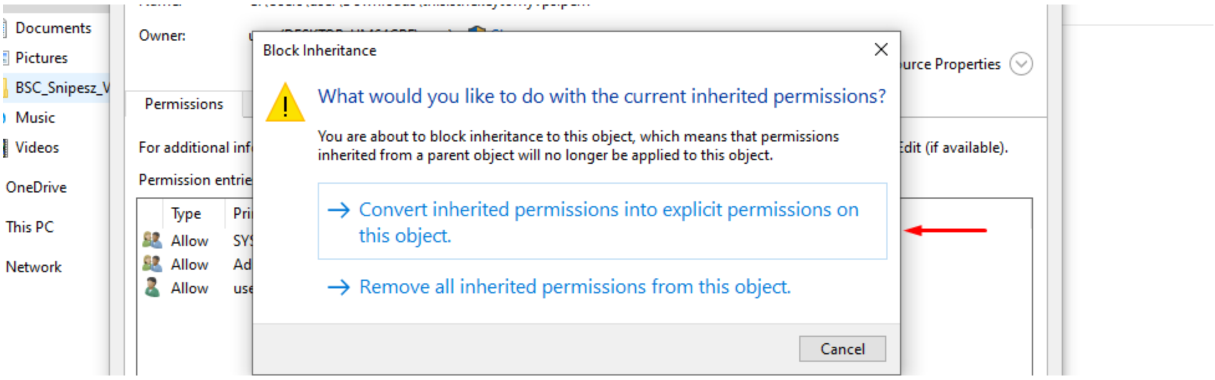
Owner: user (DESKTOP-UM64CBF\user) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	SYSTEM	Full control	C:\Users\user\
Allow	Administrators (DESKTOP-UM64CBF\Admi...	Full control	C:\Users\user\
Allow	user (DESKTOP-UM64CBF\user)	Full control	C:\Users\user\

Press “Convert inherited permissions into explicit permissions on this object”.



Block Inheritance

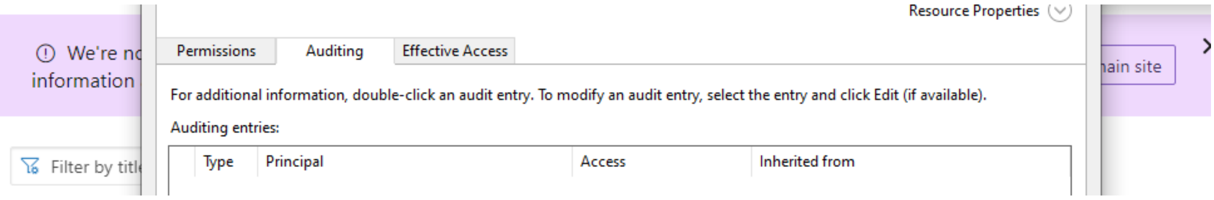
What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

→ Convert inherited permissions into explicit permissions on this object.

→ Remove all inherited permissions from this object.

Then you press “Auditing”.

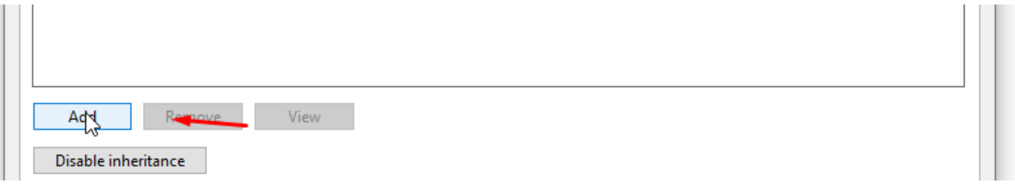


For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

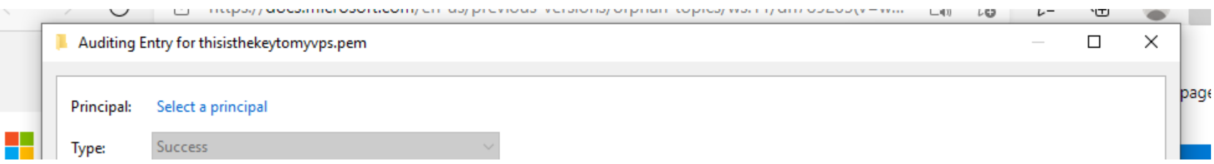
Auditing entries:

Type	Principal	Access	Inherited from

Click on “add”



Now you Select a principal.

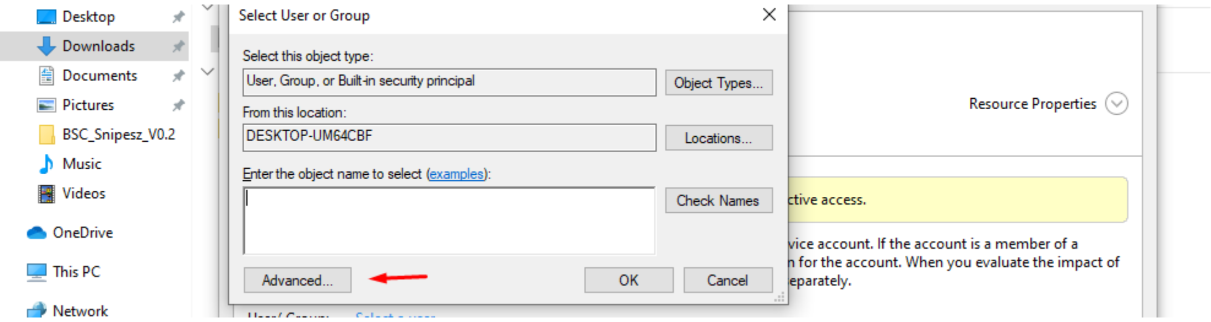


Auditing Entry for thisisthekeytomyvps.pem

Principal: Select a principal

Type: Success

Press “Advanced”.



Select User or Group

Select this object type:
User, Group, or Built-in security principal

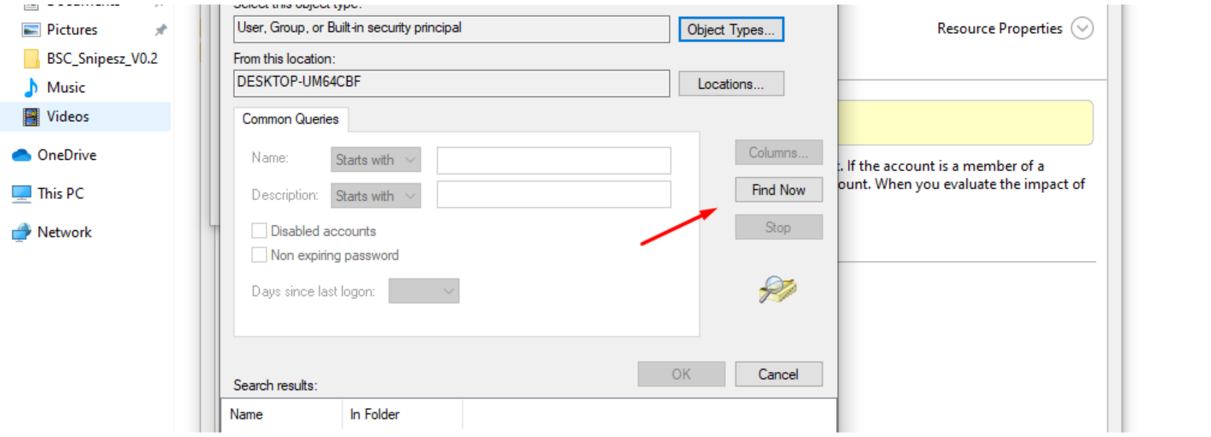
From this location:
DESKTOP-UM64CBF

Enter the object name to select (examples):

ctive access.

vice account. If the account is a member of a
n for the account. When you evaluate the impact of
eparately.

Press “Find Now”



User, Group, or Built-in security principal

From this location:
DESKTOP-UM64CBF

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

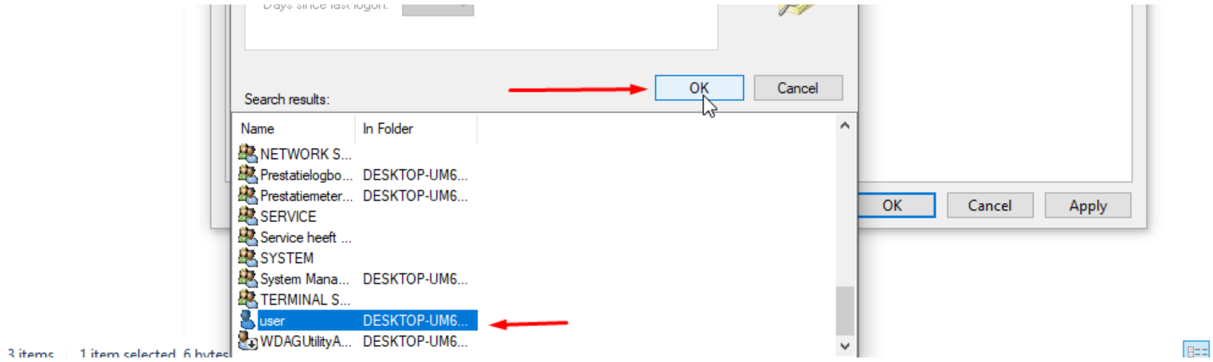
Days since last logon:

Search results:

Name	In Folder

. If the account is a member of a
ount. When you evaluate the impact of

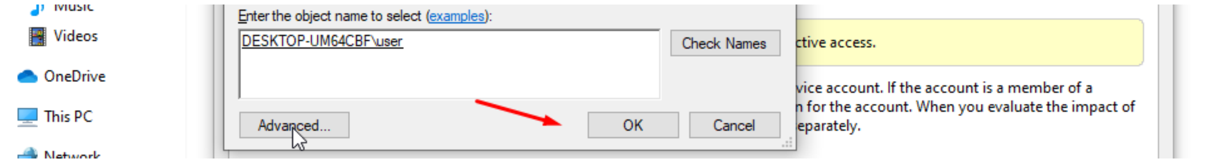
Then search for your own username and select it, and press “ok”.



Search results:

Name	In Folder
NETWORK S...	
Prestatielogbo...	DESKTOP-UM6...
Prestatiemeter...	DESKTOP-UM6...
SERVICE	
Service heeft ...	
SYSTEM	
System Mana...	DESKTOP-UM6...
TERMINAL S...	
user	DESKTOP-UM6...
WDAGUtilityA...	DESKTOP-UM6...

Press “ok” again

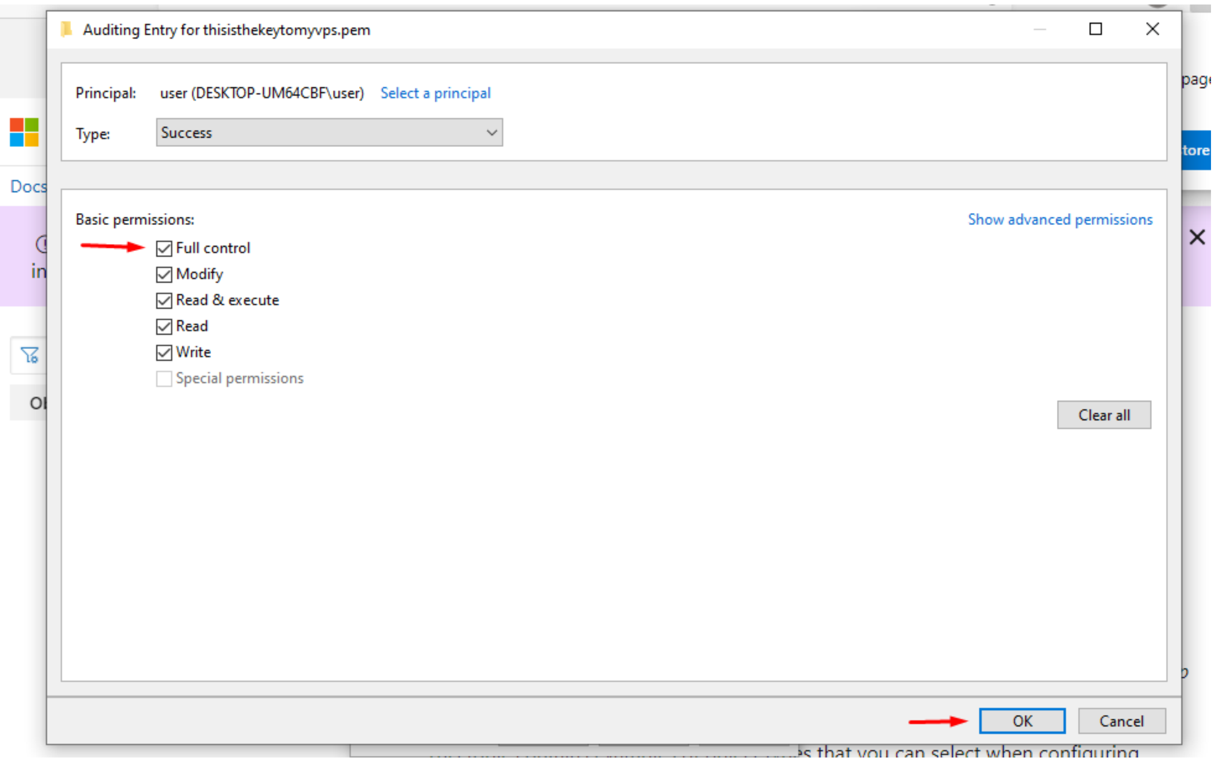


Enter the object name to select (examples):
DESKTOP-UM64CBF\user

ctive access.

vice account. If the account is a member of a
n for the account. When you evaluate the impact of
eparately.

Select “Full control” and hit “ok”



Auditing Entry for thisisthekeytomyvps.pem

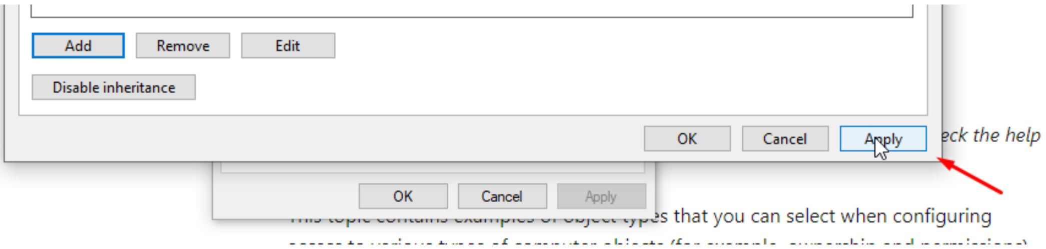
Principal: user (DESKTOP-UM64CBF\user)

Type: Success

Basic permissions:

☑ Full control
☑ Modify
☑ Read & execute
☑ Read
☑ Write
☐ Special permissions

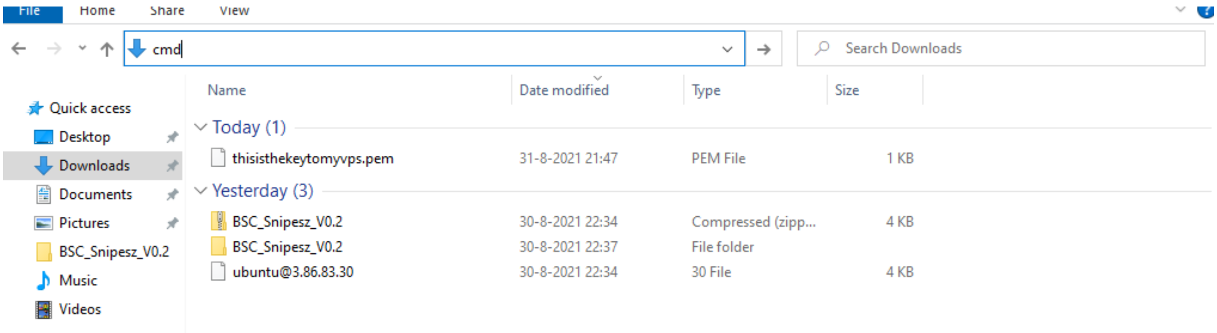
Now you hit “apply”and then ok, ok.



Okay so that was how to change permissions for the pem key on windows. As you can see doing it on linux is way more easy.

How to connect to our vps

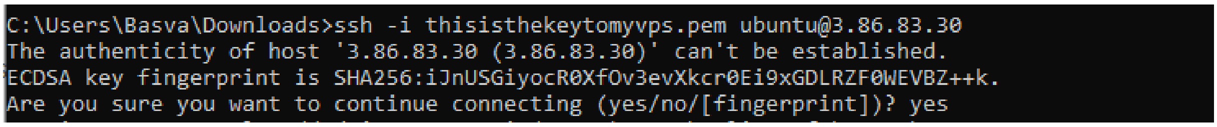
Before we connect to our vps we will first send the sniperbot to do this open cmd in the folder with the bot zip file. Type in cmd in the top search bar and hit enter.



cmd

Name	Date modified	Type	Size
Today (1)			
thisisthekeytomyvps.pem	31-8-2021 21:47	PEM File	1 KB
Yesterday (3)			
BSC_Snipesz_V0.2	30-8-2021 22:34	Compressed (zipp...	4 KB
BSC_Snipesz_V0.2	30-8-2021 22:37	File folder	
ubuntu@3.86.83.30	30-8-2021 22:34	30 File	4 KB

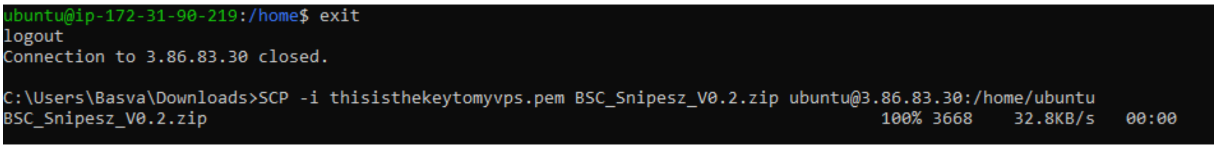
Make sure you copied your server ip (See page 23) . Now you want to connect to your vps yourself type: “ssh -i thisisthekeytomyvps.pem ubuntu@yourseverip”. It will ask you to continue, type yes and hit enter.



```
C:\Users\Basva\Downloads>ssh -i thisisthekeytomyvps.pem ubuntu@3.86.83.30
The authenticity of host '3.86.83.30 (3.86.83.30)' can't be established.
ECDSA key fingerprint is SHA256:iJnUSGiyocR0XfOv3evXkcr0Ei9xGDLRZF0WEVBZ++k.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Once you are logged in you need to exit to send our bot aswell. To do this type “exit” after that you should be back at your own pc. Now we will send our bot using this command.

“SCP -i thisisthekeytomyvps.pem BSC_Snipesz_V0.2.zip ubuntu@yourserverip:/home/ubuntu”



```
ubuntu@ip-172-31-90-219:/home$ exit
logout
Connection to 3.86.83.30 closed.

C:\Users\Basva\Downloads>SCP -i thisisthekeytomyvps.pem BSC_Snipesz_V0.2.zip ubuntu@3.86.83.30:/home/ubuntu
BSC_Snipesz_V0.2.zip                                                                100% 3668    32.8KB/s   00:00
```

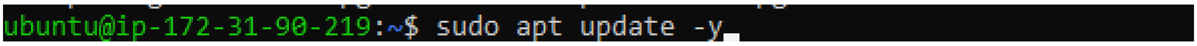
Now we can make a SSH connection to our server again by using the command.

“ssh -i thisisthekeytomyvps.pem ubuntu@yourseverip”

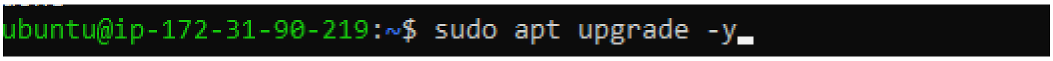
You will see now that you are instantly logged in.

Updating the VPS and installing the packages we need

Now you need to upgrade and update your system. To do this type “sudo apt update -y” and after that type “sudo apt upgrade -y”. This can take some time.



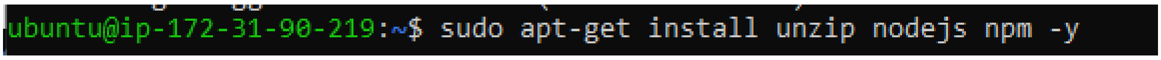
```
ubuntu@ip-172-31-90-219:~$ sudo apt update -y
```



```
ubuntu@ip-172-31-90-219:~$ sudo apt upgrade -y
```

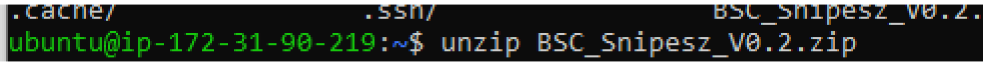
Now you need to install the nodejs and the unzip package. Type:

“sudo apt-get install unzip nodejs npm -y” in the console.



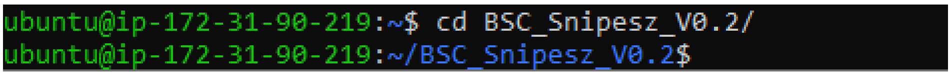
```
ubuntu@ip-172-31-90-219:~$ sudo apt-get install unzip nodejs npm -y
```

After that you need to onzip the bot by typing: “unzip BSC_Snipesz_V0.2.zip”



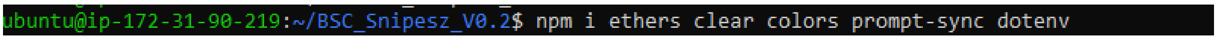
```
.cache/                 .ssh/                   BSC_Snipesz_V0.2.
ubuntu@ip-172-31-90-219:~$ unzip BSC_Snipesz_V0.2.zip
```

Then we go into the bot directory by using “cd BSC_Snipesz_V0.2”



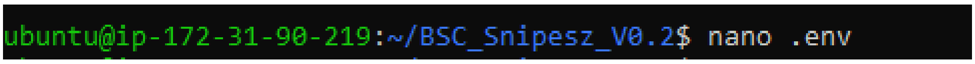
```
ubuntu@ip-172-31-90-219:~$ cd BSC_Snipesz_V0.2/
ubuntu@ip-172-31-90-219:~/BSC_Snipesz_V0.2$
```

Now you need to type: “npm i ethers clear colors prompt-sync dotenv” and press enter. This will install the required library’s.



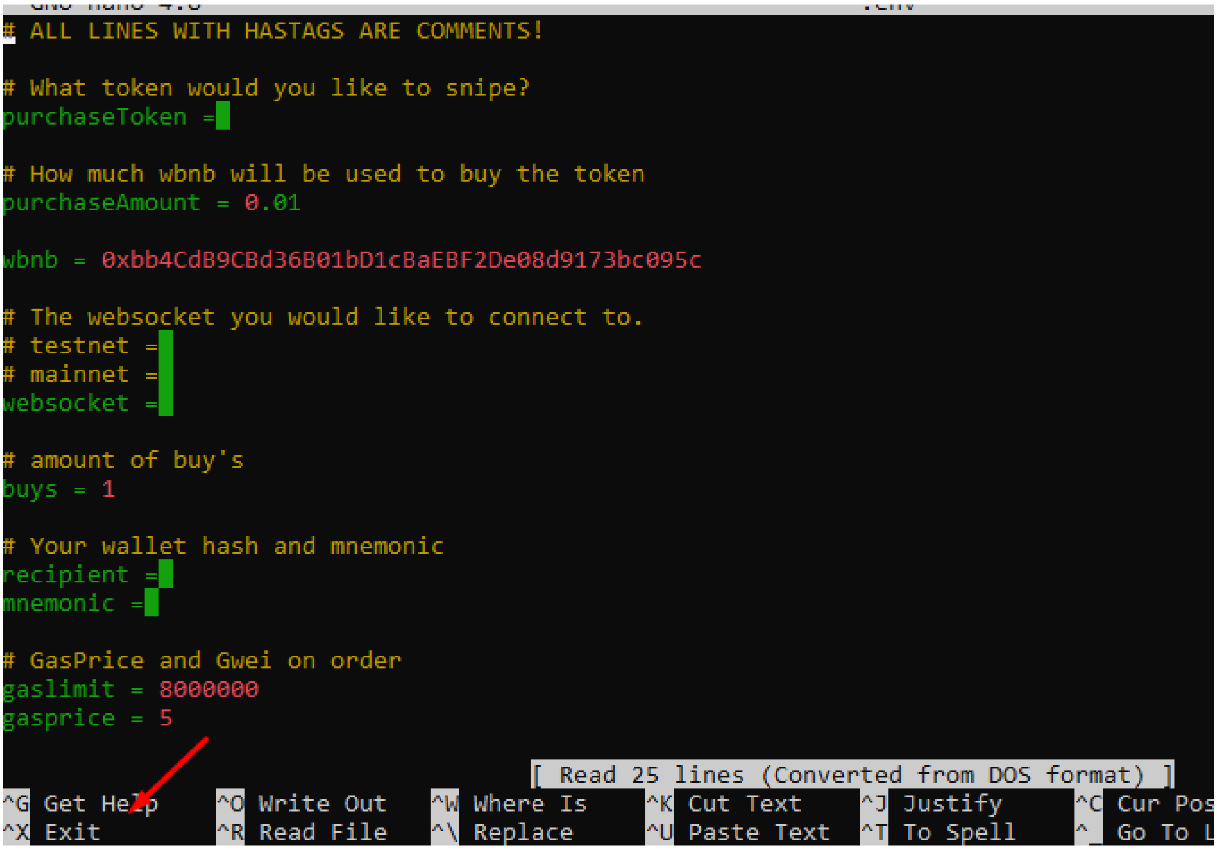
```
ubuntu@ip-172-31-90-219:~/BSC_Snipesz_V0.2$ npm i ethers clear colors prompt-sync dotenv
```

If you want to edit the bot settings, type: “nano .env”

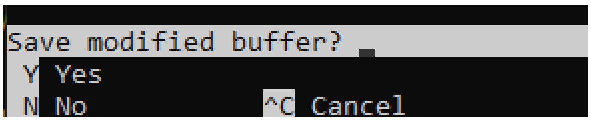


```
ubuntu@ip-172-31-90-219:~/BSC_Snipesz_V0.2$ nano .env
```

After editing your preferred bot settings you can exit by hitting “ctrl + x” on your keybord. Nano will ask of you are sure to save hit the “y” key and press enter



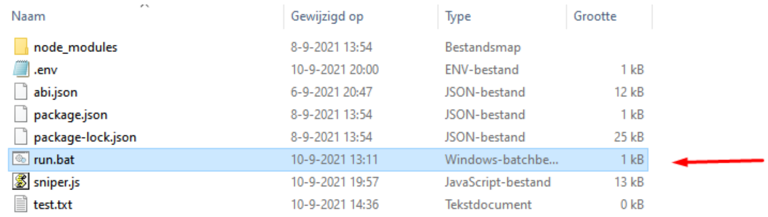
```
  GNU nano 4.8                                                   .env
# ALL LINES WITH HASTAGS ARE COMMENTS!

# What token would you like to snipe?
purchaseToken =[redacted]

# How much wbnb will be used to buy the token
purchaseAmount = 0.01

wbnb = 0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c

# The websocket you would like to connect to.
# testnet =[redacted]
# mainnet =
websocket =

# amount of buy's
buys = 1

# Your wallet hash and mnemonic
recipient =[redacted]
mnemonic =[redacted]

# GasPrice and Gwei on order
gaslimit = 8000000
gasprice = 5

                                     [ Read 25 lines (Converted from DOS format) ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To L
```



```
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

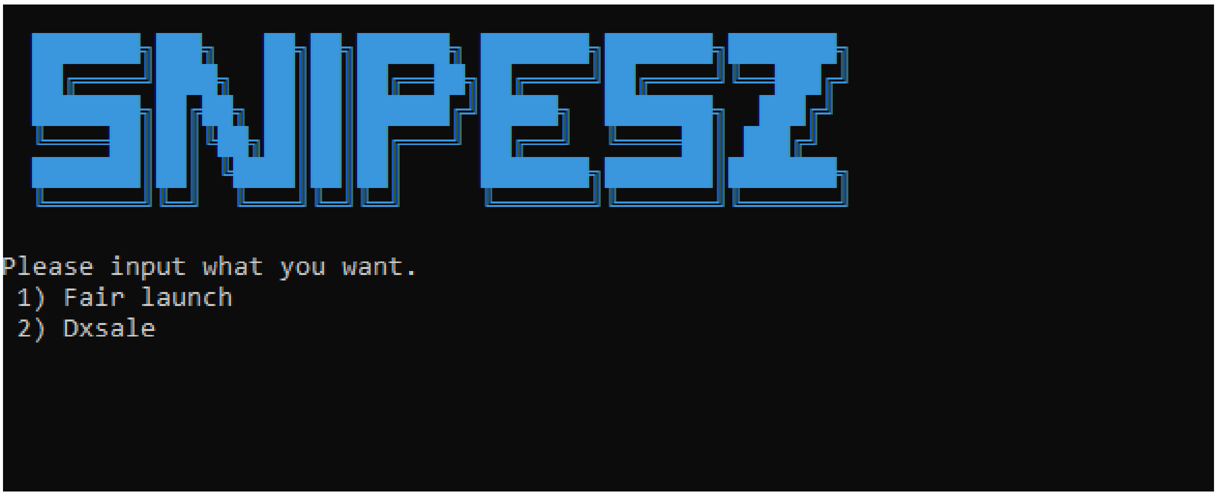
Running the Bot

Finally we are ready to run the bot. To run the bot double click run.bat again in the same folder.



Naam	Gewijzigd op	Type	Grootte
node_modules	8-9-2021 13:54	Bestandsmap	
.env	10-9-2021 20:00	ENV-bestand	1 kB
abi.json	6-9-2021 20:47	JSON-bestand	12 kB
package.json	8-9-2021 13:54	JSON-bestand	1 kB
package-lock.json	8-9-2021 13:54	JSON-bestand	25 kB
run.bat	10-9-2021 13:11	Windows-batchbe...	1 kB
sniper.js	10-9-2021 19:57	JavaScript-bestand	13 kB
test.txt	10-9-2021 14:36	Tekstdocument	0 kB

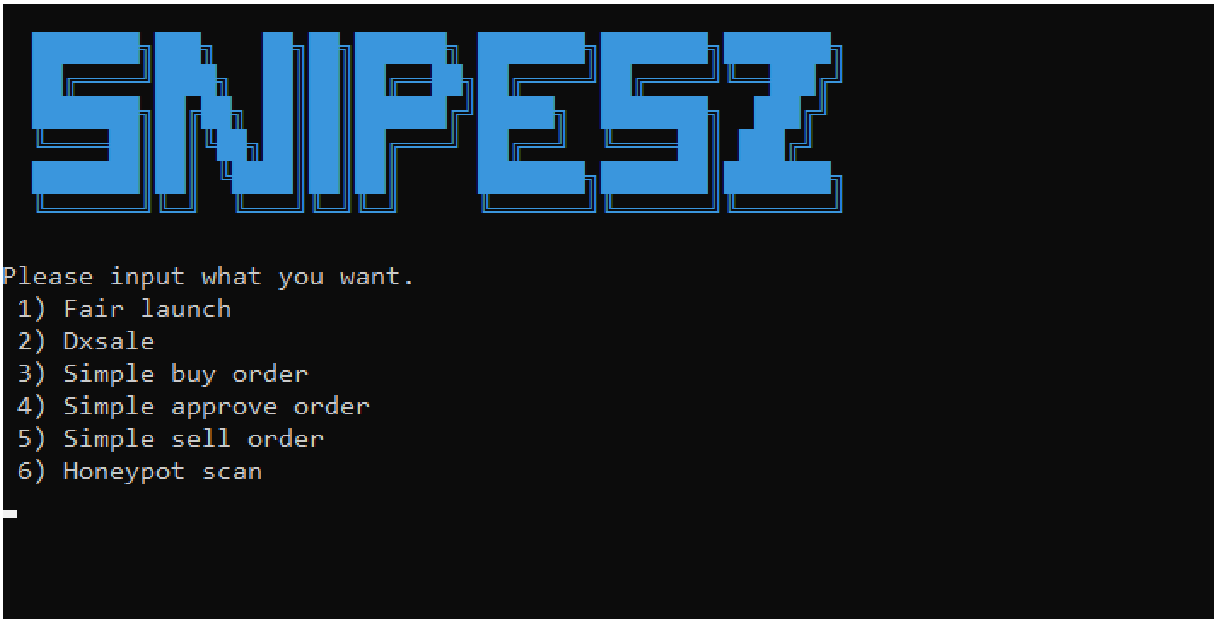
The bot will now start



```
Please input what you want.
 1) Fair launch
 2) Dxsale
```

How to use the bot

In the bot menu there are 6 options, sniping a fair launch or sniping a dxsale launch. Hit the key of what you would like to choose and press enter. The bot will now start scanning the mempool and make a transaction



```
Please input what you want.
 1) Fair launch
 2) Dxsale
 3) Simple buy order
 4) Simple approve order
 5) Simple sell order
 6) Honeypot scan
```