



AWS + Windows + Power BI Setup Guide

v1.0.0



Contents

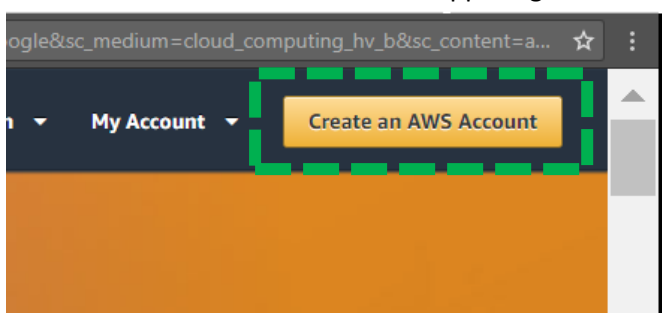
1. Create an AWS Account	1
2. Create Instance	5
2.1. Navigate to instance creation page. (2 ways to do it)	5
2.2. Create Instance	6
3. Retrieve Windows Administrator's Password in AWS	10
4. Remote Access	12
4.1. Remote Access on Windows	12
4.2. Remote Access on Mac	15
5. Install PowerBI	18
5.1. Enable File Download in IE	18
5.2. Download PowerBI	20
5.3. Install PowerBI	21
6. Create Elastic IP (Optional Step)	25



1. Create an AWS Account

1.1. Go to AWS website: <https://aws.amazon.com/>

1.2. Click **Create an AWS Account** in the upper right-hand corner



1.3. Input Email, Password, AWS account name → Click **Continue**

Create an AWS account

Email address
xxxx@gmail.com

Password
.....

Confirm password
.....

AWS account name ⓘ
xxxxxx

Continue

[Sign in to an existing AWS account](#)

© 2017 Amazon Web Services, Inc. or its affiliates.
All rights reserved.
[Privacy Policy](#) | [Terms of Use](#)



1.4. Input your personal information

Account type ⓘ

☐ Professional ☒ Personal

Full name

xxxxx

Phone number

xxxx

Country

Hong Kong ▼

Address

xxxx

xxxx

City

Hong Kong

State / Province or region

Hong Kong

Postal code

852

1.5. Input Credit Card details → Click **Secure Submit**

Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the [AWS Free Tier Limits](#). Review [frequently asked questions](#) for more information.

Credit/Debit card number

xxx xxx

Expiration date

12 ▼ 2017 ▼

Cardholder's name

xxxxxx

Billing address

☒ Use my contact address

Hong Kong
Hong Kong Hong Kong 852
HK

☐ Use a new address

Secure Submit



1.6. Input your phone number → Click **Call Me Now** → AWS will call you

AWS will call you immediately using an automated system. When prompted, enter the 4-digit number from the AWS website on your phone keypad.

Provide a telephone number

Please enter your information below and click the "Call Me Now" button.

Country code

Hong Kong (+852)

Phone number

xxxxxx

Ext

Security Check

m53xw3



m53xw3

Call Me Now

1.7. Enter the **PINS** displayed on your screen to your phone

Phone Verification

AWS will call you immediately using an automated system. When prompted, enter the 4-digit number from the AWS website on your phone keypad.

Call in progress...

Please answer the call from AWS and, when prompted, enter the 4-digit number on your phone keypad.




5 8 0 1



1.8. Select **Basic Plan**

Select a Support Plan

AWS offers a selection of support plans to meet your needs. Choose the support plan that best aligns with your AWS usage. [Learn more](#)

 Basic Plan	 Developer Plan	 Business Plan
Free	From \$29/month	From \$100/month
<ul style="list-style-type: none">• Included with all accounts• 24/7 self-service access to forums and resources• Best practice checks to help improve security and performance• Access to health status and notifications	<ul style="list-style-type: none">• For early adoption, testing and development• Email access to AWS Support during business hours• 1 primary contact can open an unlimited number of support cases• 12-hour response time for nonproduction systems	<ul style="list-style-type: none">• For production workloads & business-critical dependencies• 24/7 chat, phone, and email access to AWS Support• Unlimited contacts can open an unlimited number of support cases• 1-hour response time for production systems

1.9. Click **Sign in to the Console**

Welcome to Amazon Web Services

Thank you for creating an Amazon Web Services Account. We are activating your account, which should only take a few minutes. You will receive an email when this is complete.

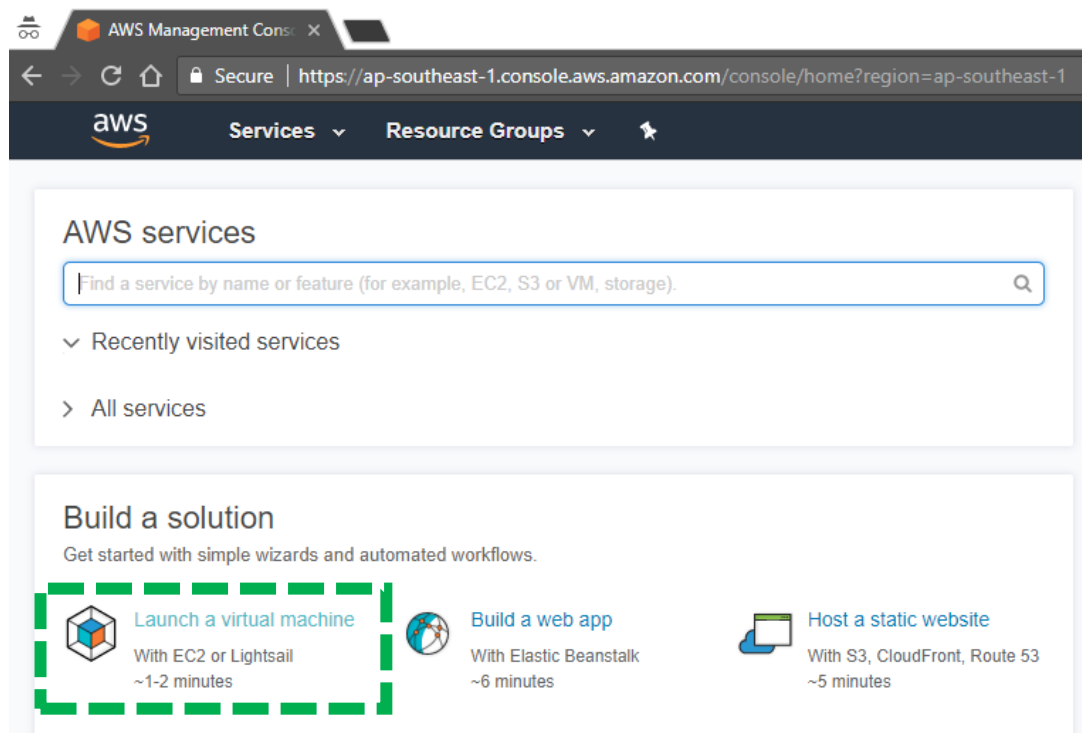
[Sign in to the Console](#)
[Contact Sales](#)



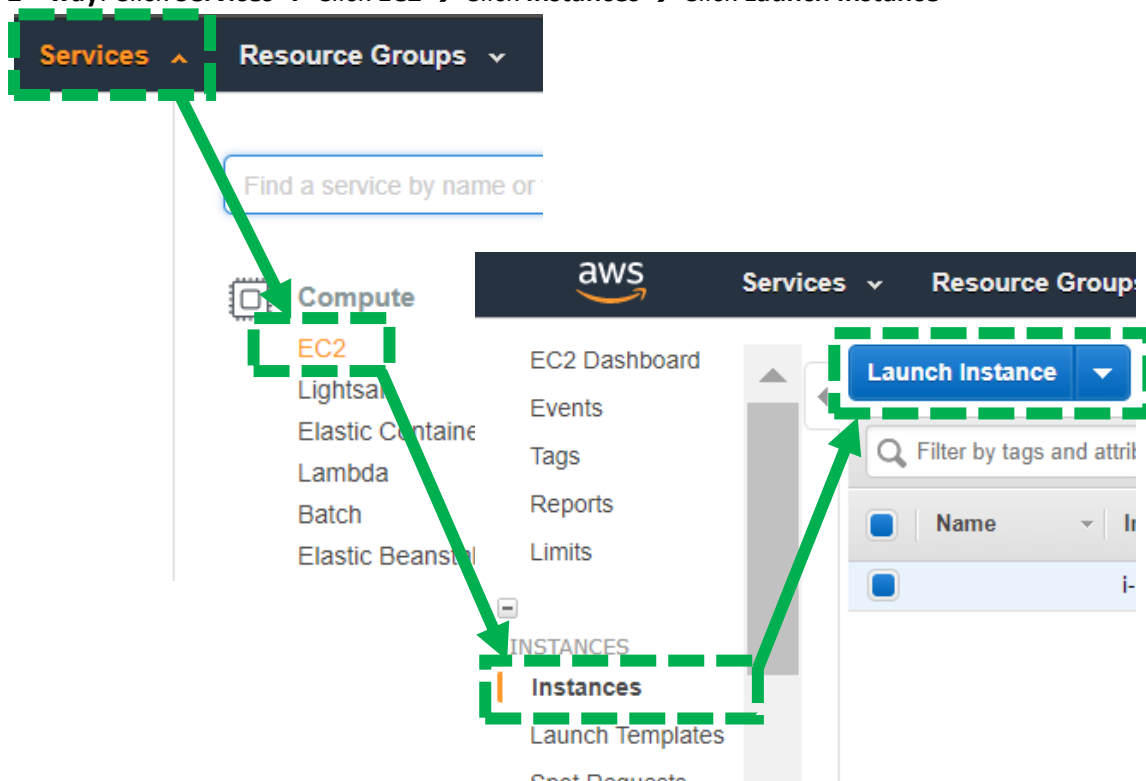
2. Create Instance

2.1. Navigate to instance creation page. (2 ways to do it)

2.1.1. 1st way: Click **Launch a virtual machine**



2.1.2. 2nd way: Click **Services** → Click **EC2** → Click **Instances** → Click **Launch Instance**

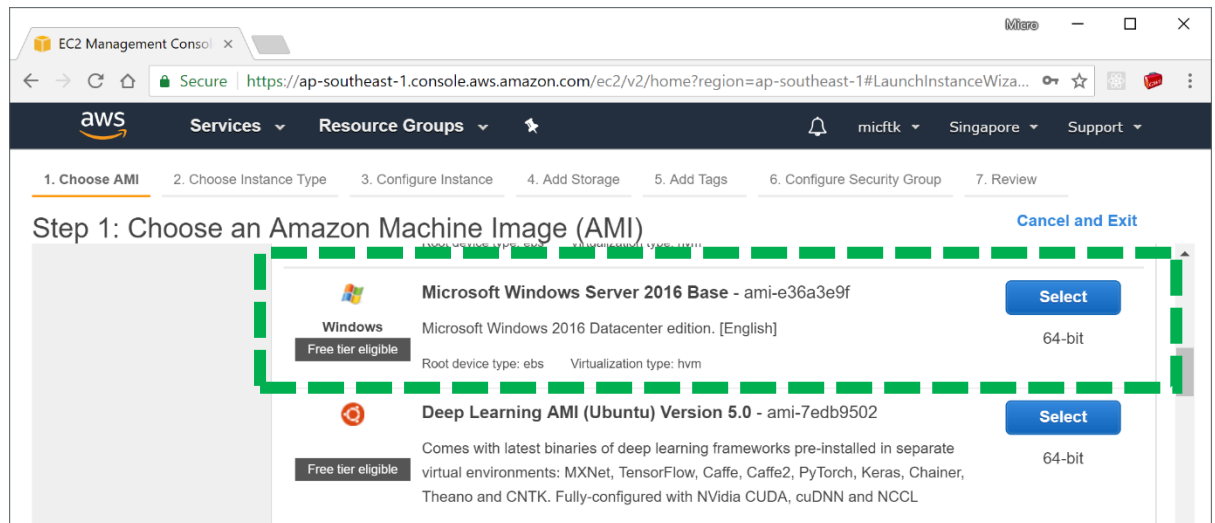




2.2. Create Instance

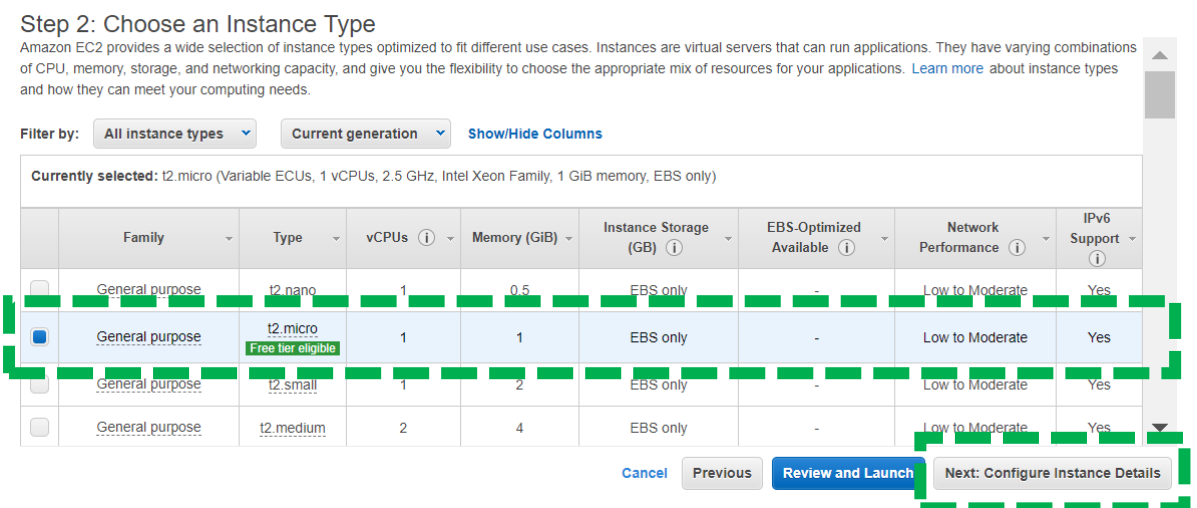
2.2.1. Choose Machine Image

Select **Microsoft Windows Server 2016 Base**



2.2.2. Choose Instance Type

Select **t2.micro** → Click **Next: Configure Instance Details**





2.2.3. Configure Instance

Tick **Protect against accidental termination** → Click **Next: Add Storage**

Shutdown behaviour: (Choose Stop as always)

**** Stop means shutdown**

**** Terminate means DESTROY!!!**

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

Domain join directory [Create new directory](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Enable termination protection ☒ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

2.2.4. Add Storage (How large should be your harddisk?)

Keep the default setting, increase it later if you want → Click **Next: Add Tags**

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/sda1	snap-0b0af4e6722ae6b23	<input type="text" value="30"/>	General Purpose <input type="text" value="SSD"/>	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.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)



2.2.5. Add Tags (Optional Step)

Add any tags you want to describe your new instance → Click **Next: Configure Security Group**

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

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	Volumes
------------------------------	--------------------------------	-----------	---------

This resource currently has no tags

Choose the Add tag button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

(Up to 50 tags maximum)

[Cancel](#)

2.2.6. Configure Security Group

It has **3389** port in default which is Microsoft Remote Display Protocol.

This specific port allows us to remote access the machine later.

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:

Description:

Type	Protocol	Port Range	Source	Description
Custom TCP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop



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](#)




2.2.7. Review Instance

Good to go, Click **Launch**

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

Step 7: Review Instance Launch

▼ AMI Details

 **Microsoft Windows Server 2016 Base - ami-e36a3e9f**

Free tier eligible

Microsoft Windows 2016 Datacenter edition. [English]
Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

Edit AMI

▼ 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

Edit instance type

▼ Security Groups

Security group name

launch-wizard-2

Description

launch-wizard-2 created 2018-03-15T15:22:13.263+08:00

Type ⓘ

Protocol ⓘ

Port Range ⓘ

Source ⓘ

Description ⓘ

Cancel

Previous

Launch

2.2.8. Create key pair

It is a key pair for you to login AWS, so **PLEASE DOWNLOAD IT** and **SAVE IT IN SECURE LOCATION**

Choose **Create a new key pair** → Type key pair name → Click **Download Key Pair** → Click **Launch Instances**

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](#)

Create a new key pair

Key pair name

powerbi.accelerating.tech

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

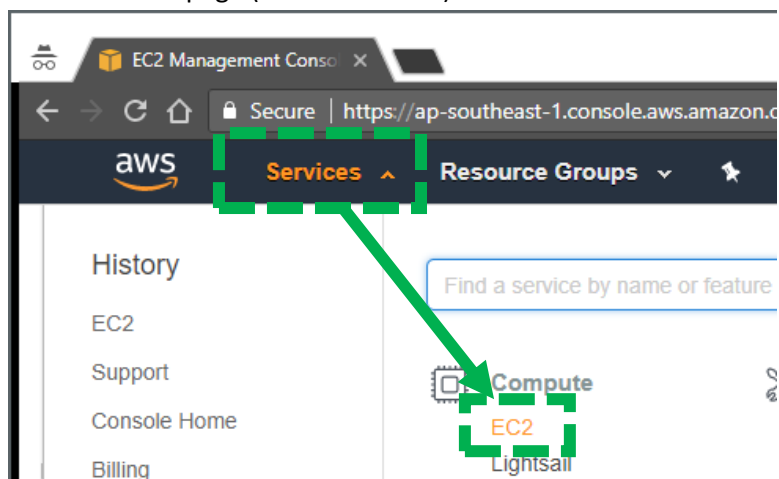
Launch Instances

9

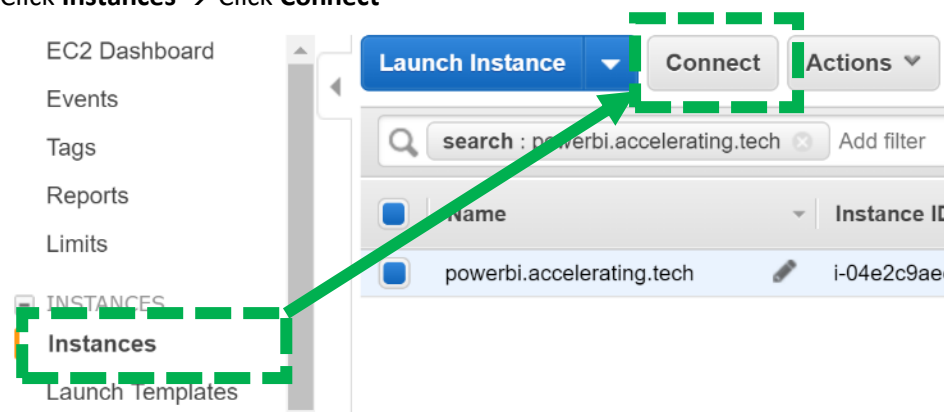


3. Retrieve Windows Administrator's Password in AWS

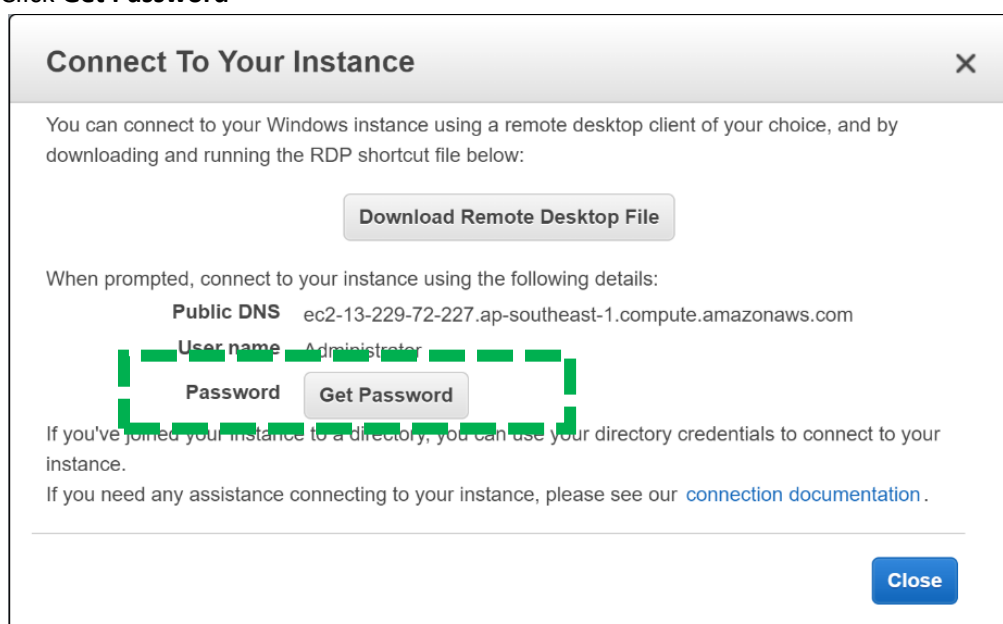
3.1. Go back to **EC2** page (Services → EC2)



3.2. Click **Instances** → Click **Connect**



3.3. Click **Get Password**





- 3.4. Click **Choose File** → Choose the **.pem** file we downloaded in [“Create Key Pair”](#) section → Click **Decrypt Password**

Connect To Your Instance > Get Password

The following Key Pair was associated with this instance when it was created.

Key Name powerbi.accelerating.tech.pem

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path **Choose File** powerbiaccel...ech (1).pem

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEEowlBAAKCAQEAqksbSHbsgxb4qb89rbeWE7bGG6F0Qi1+Sy2bAfb9u9fPuWmAWcGDvHI4n6wy
9sZ7b0uDoOoHor0O8WLKrT4AIKGuD3Mq7irYjyYhyZGfNKONTfVfW36Mz4o7eDzs763AQUQOJwO
etdzlQAw1fyZvmjE5172I9rzi+78z2I0O80IS+Rlmmi4IDKekqllLhpAHxXmz3kQP6JWht6dfmsn
pe5rog6+2R9TaIETUqT5zBYFU0EhJlQzaRnXmRQyu/l2o2vHhmp48fwDoRjadd2rvaT59K63yqto
oIPQSSwtc9kKXluU+XYsK1vHHV+YBoG7BCTDNHxetTncCpSE8+MTFQIDAQABoIBABiVcSHb8Tb
-----
```

Decrypt Password

Back **Close**

- 3.5. Please remember **Public DNS, User name, Password**

We are going to use it to access our remote machine.

For Windows User, please click **Download Remote Desktop File** to download a pre-configured profile to remote access your local machine

Connect To Your Instance

You can connect to your Windows instance using a remote desktop by downloading and running the RDP shortcut file below:

Download Remote Desktop File

When prompted, connect to your instance using the following details:

Public DNS	ec2-52-220-13-81.ap-southeast-1.compute.amazonaws.com
User name	Administrator
Password	123456

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Close

For Windows User, please click it



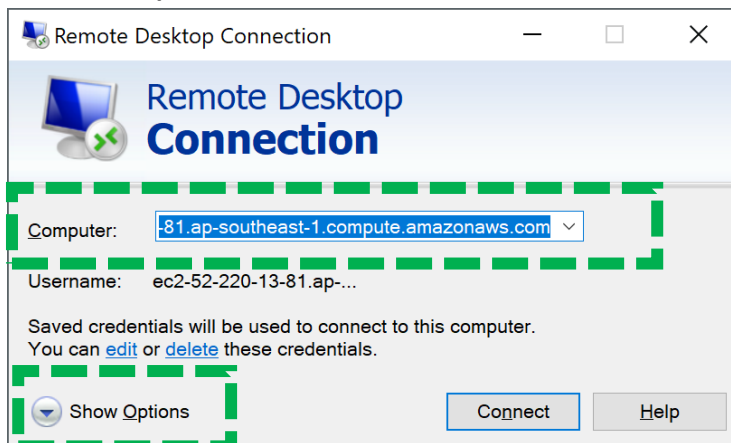
4. Remote Access

You have created a remote machine and retrieve all the necessary information from AWS.
Let's connect it from our local machine.

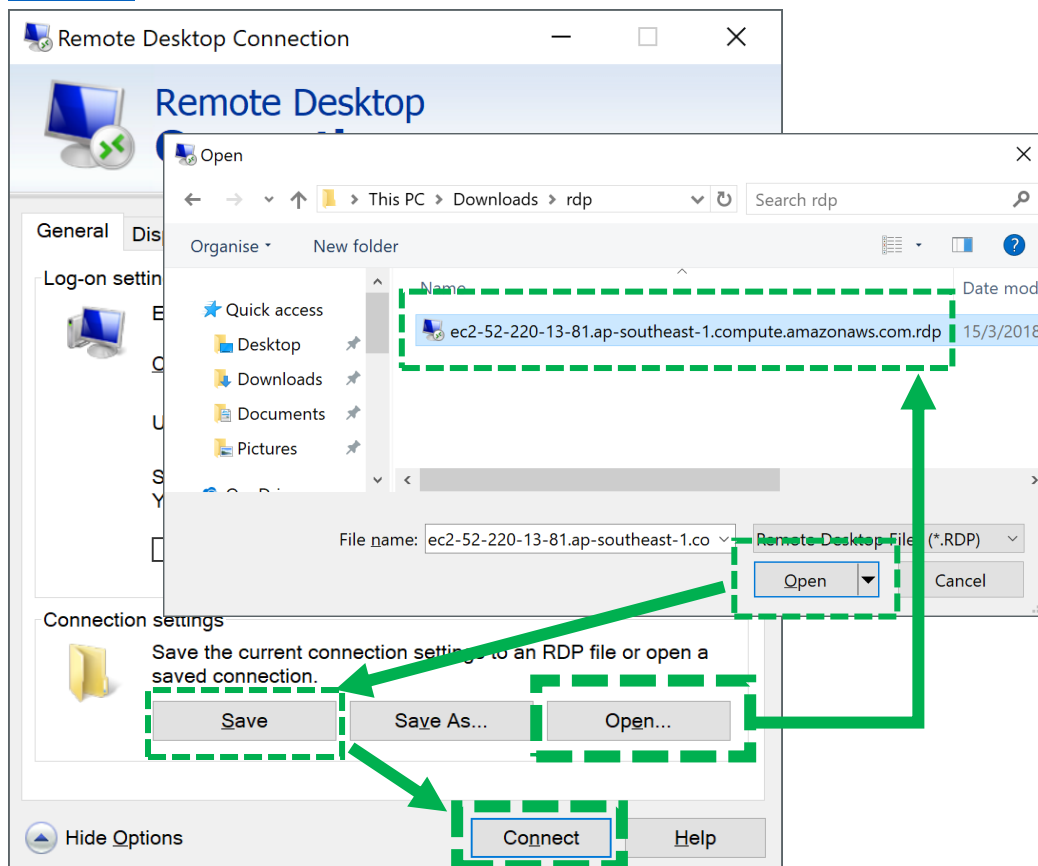
- For Windows Users, please read [4.1](#).
- For Mac Users, please read [4.2](#).
- For Linux Users, please contact our staff to help you.

4.1. Remote Access on Windows

4.1.1. Press **Win + R** on keyboard → Type **mstsc** → Type the **Public DNS** in computer name → Click **Show Options**

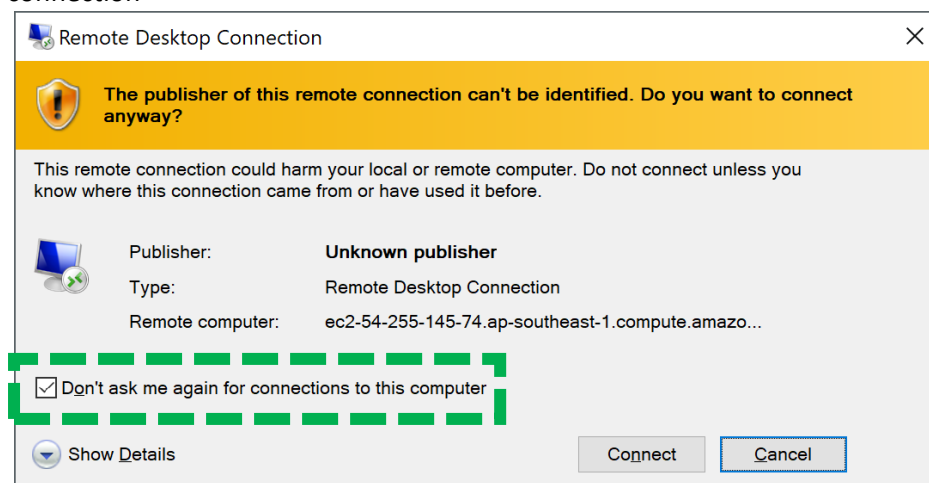


4.1.2. Click **Open...** → Choose the rdp file you downloaded in [“Markdown Username and Password”](#) section → Click **Save** → Click **Connect**

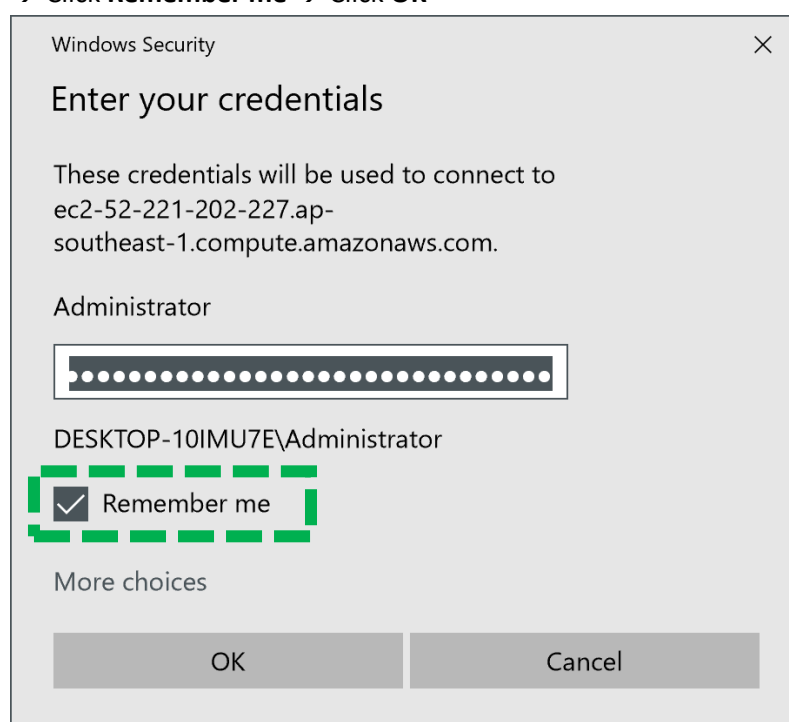




- 4.1.3. If the below image pops up, Tick the box → Click Connect to trust the remote connection



- 4.1.4. Enter Password (it should be retrieved in [“Markdown Username and Password”](#) section)
→ Click **Remember me** → Click **OK**



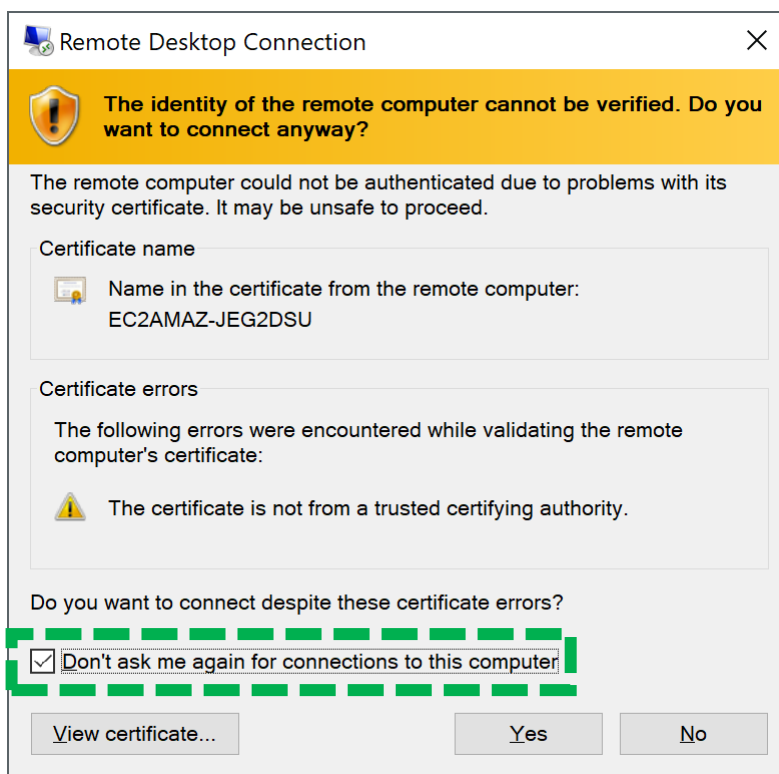
- 4.1.5. **Copy file from local PC to remote machine**

Easy to do it on Windows:

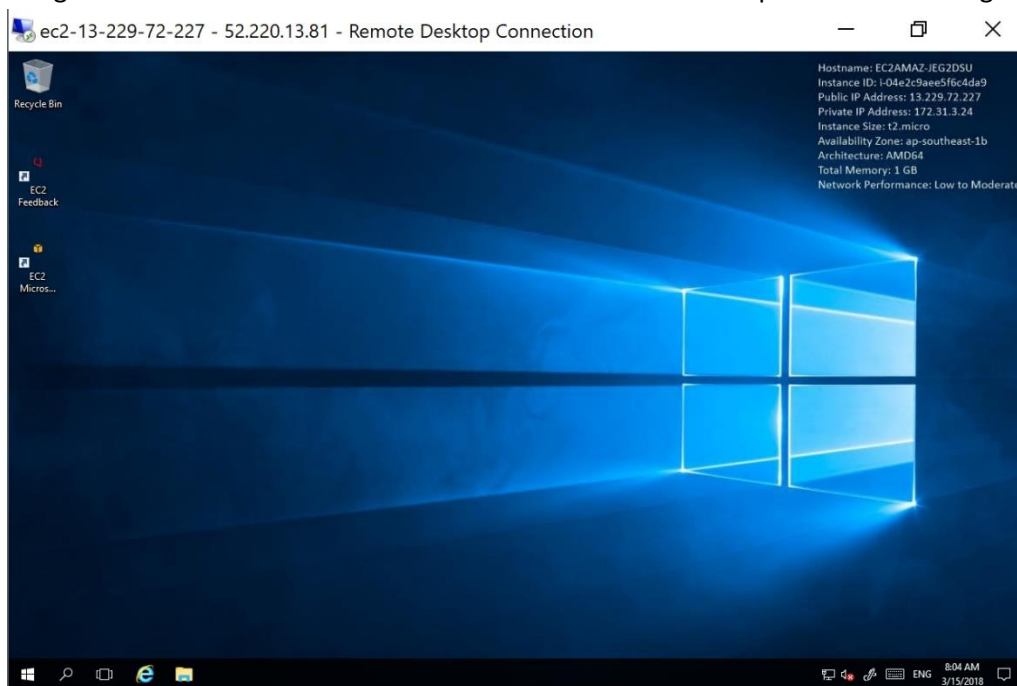
1. Select any files/folders in your local PC, press **Ctrl + c** to copy it
2. In your remote machine, press **Ctrl + v** to paste it.



4.1.6. Tick the box → Click Yes to trust the certificate from remote machine



Congratulation! You should be able to see the Windows desktop screen in this stage.

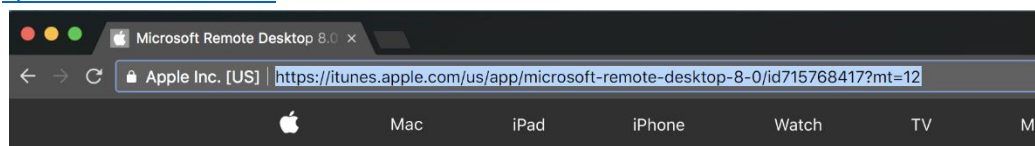




4.2. Remote Access on Mac

4.2.1. Install Microsoft Remote Desktop 8.0

Go to App Store: <https://itunes.apple.com/us/app/microsoft-remote-desktop-8-0/id715768417?mt=12>



Mac App Store Preview

Open the Mac App Store to buy and download apps.



Microsoft Remote Desktop 8.0 4+

Microsoft Corporation

★★★★☆ 126 Ratings

Free

[View in Mac App Store](#)

4.2.2. Click **Get** → Input your Apple Account Password → Click **Install App**



Microsoft Remote Desktop 8.0

With the Microsoft Remote Desktop app, you can connect to Experience the power of Windows with RemoteFX in a Remot you are.

...



Get



Microsoft Remote Desktop 8.0 4+

With the Microsoft Remote Desktop app, you can connect to Experience the power of Windows with RemoteFX in a Remot you are.

...

What's New in Version 8.0.43

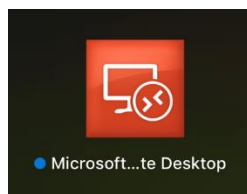
General bug fixes.



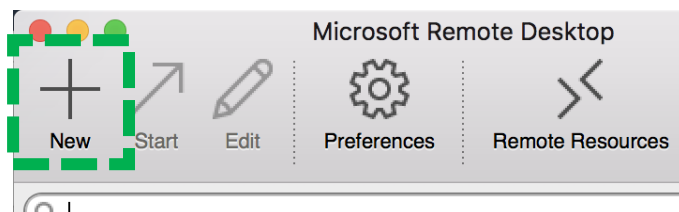
Install App



4.2.3. Microsoft Remote Desktop App is installed → Click the Icon to start the app



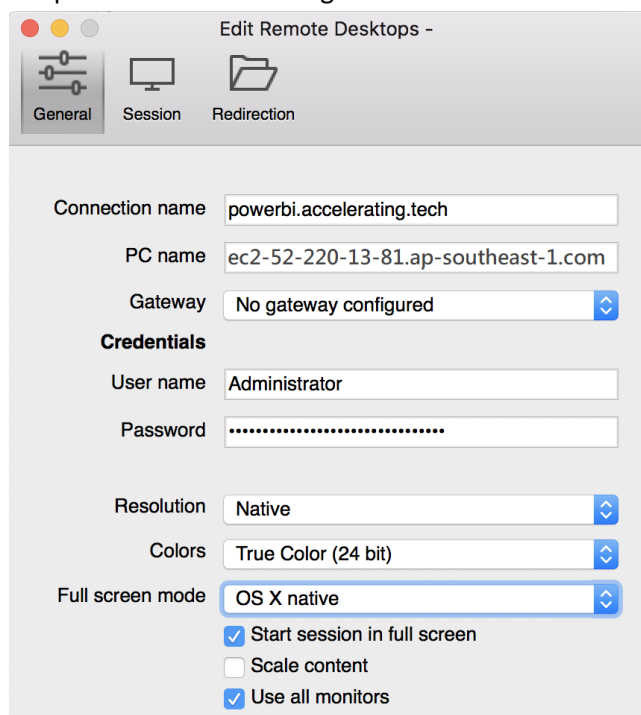
4.2.4. Click New to create connection



4.2.5. Fill in information

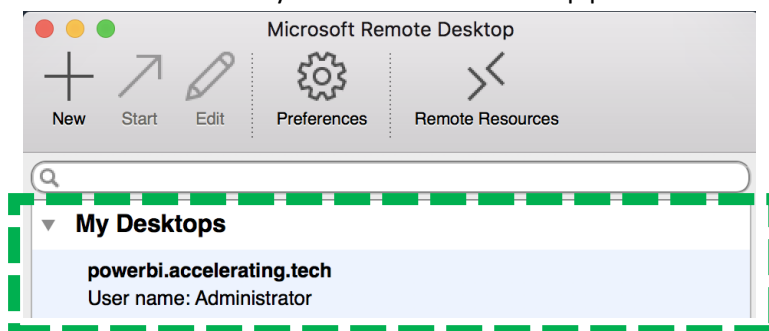
Connection name	<Type any Name you want>
PC name	<Public DNS>
Gateway	No gateway configured
User name	Administrator
Password	<The password you copied in Key Pair>

Keep the rest of the settings as default → Close the setting page





4.2.6. Double Click the newly created remote desktop profile to connect your remote machine.



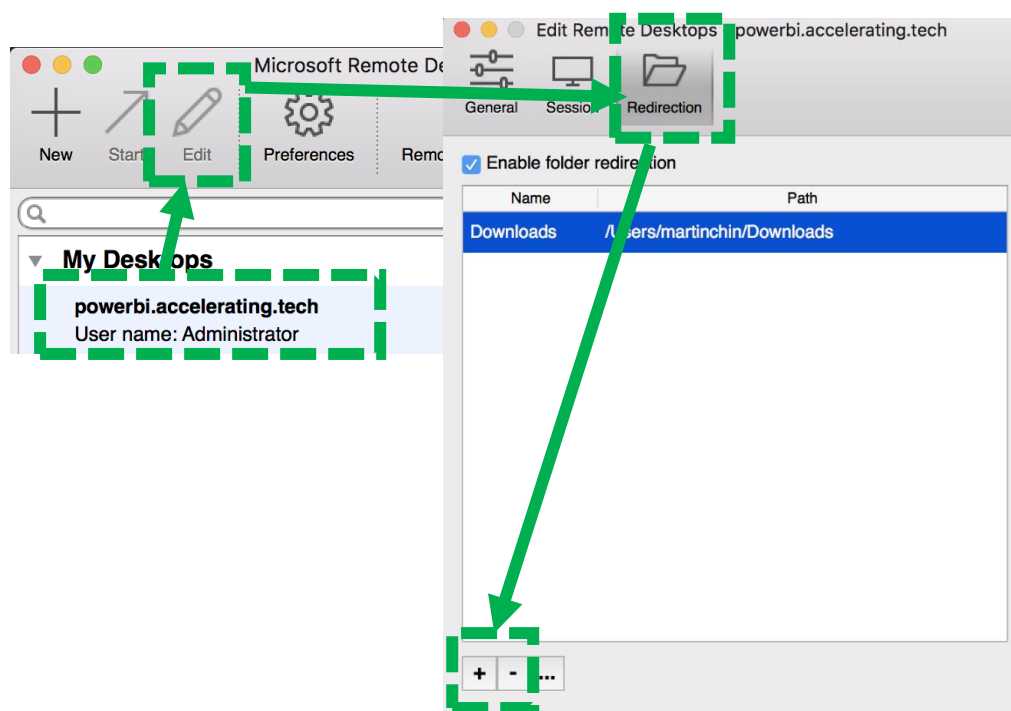
Congratulation! You should be able to see the windows desktop screen in this stage.

4.2.7. Add Share Folder b/w Mac and Remote Machine (Optional)

If you do not want to download file through remote server, you may add a share folder in remote settings.

Select the profile → Click **Edit** → Choose **Redirection** → Click + → Choose your desired folders you want to share with your remote machine →

Close the setting page and login to remote machine again





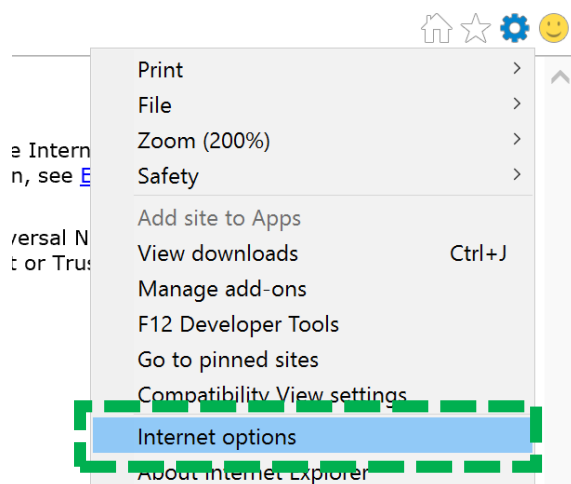
5. Install PowerBI

5.1. Enable File Download in IE

5.1.1. In your remote machine, Open Internet Explorer on the Taskbar

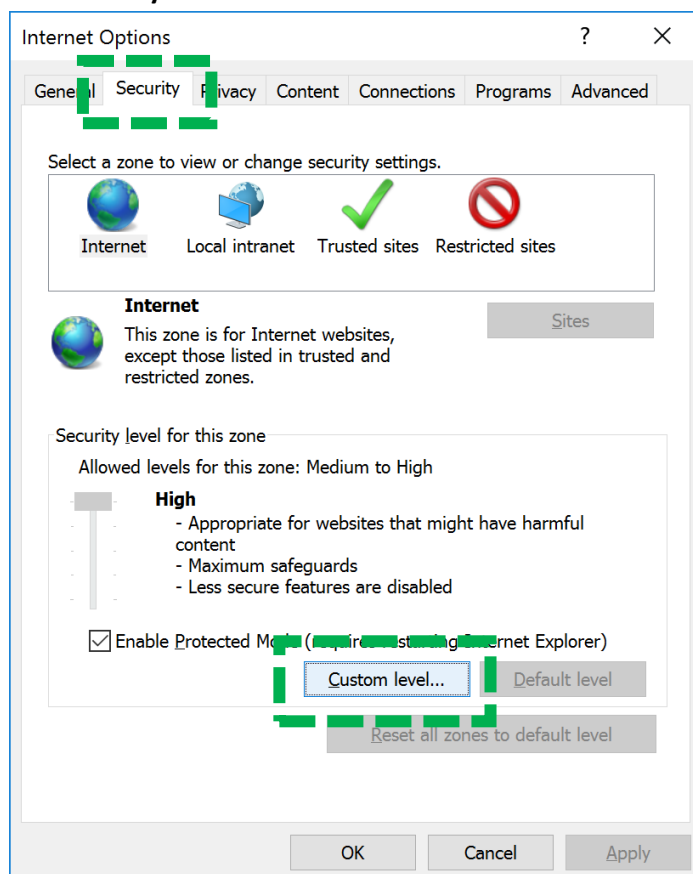


5.1.2. Click the Gear  → Click **Internet Options**

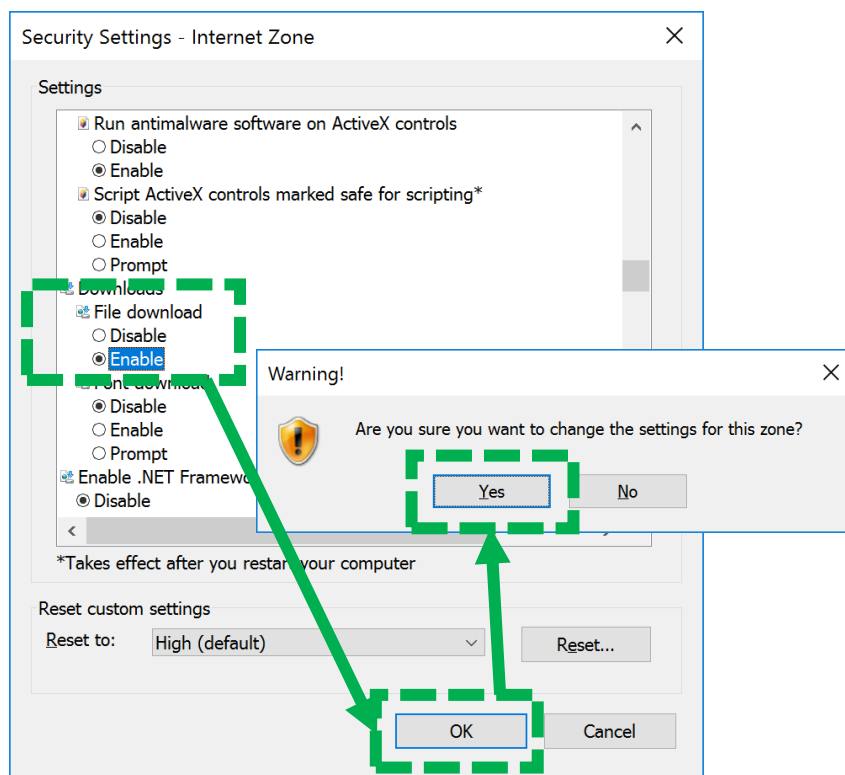




5.1.3. Click Security → Custom level....



5.1.4. File download → Click Enable → Click OK → Click Yes to save the settings.

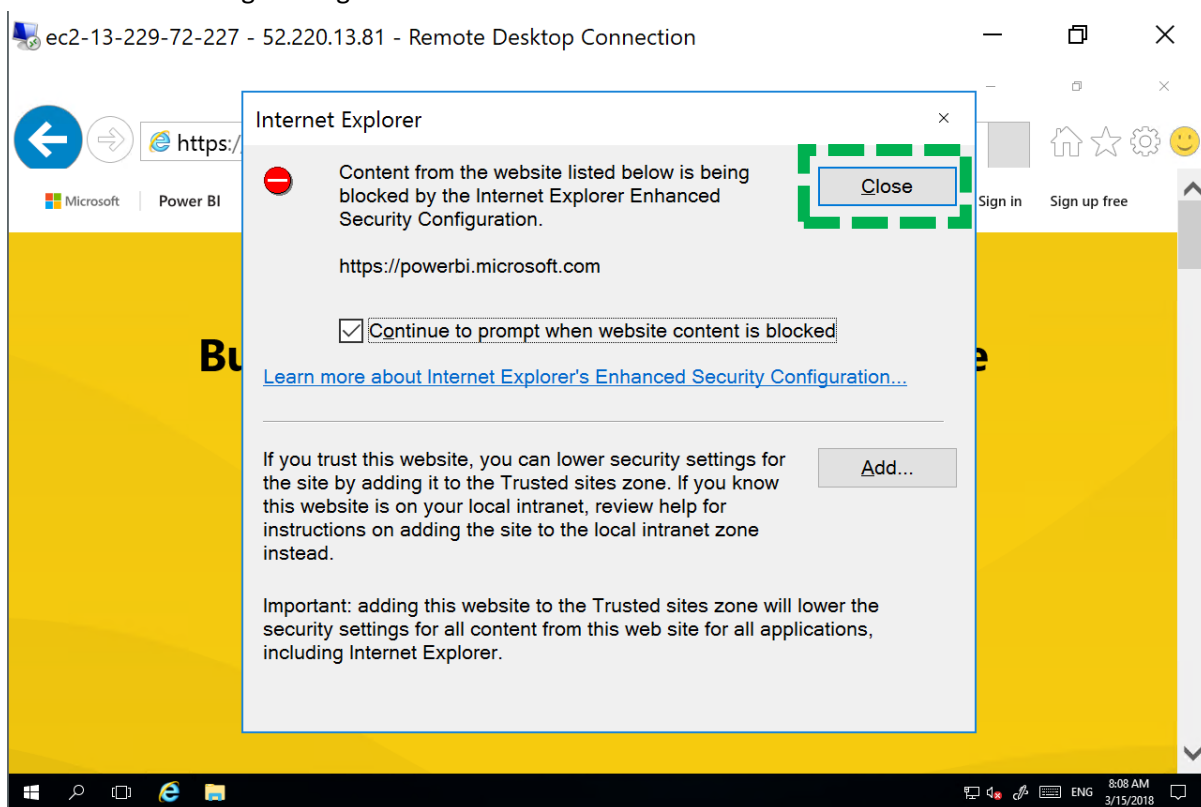




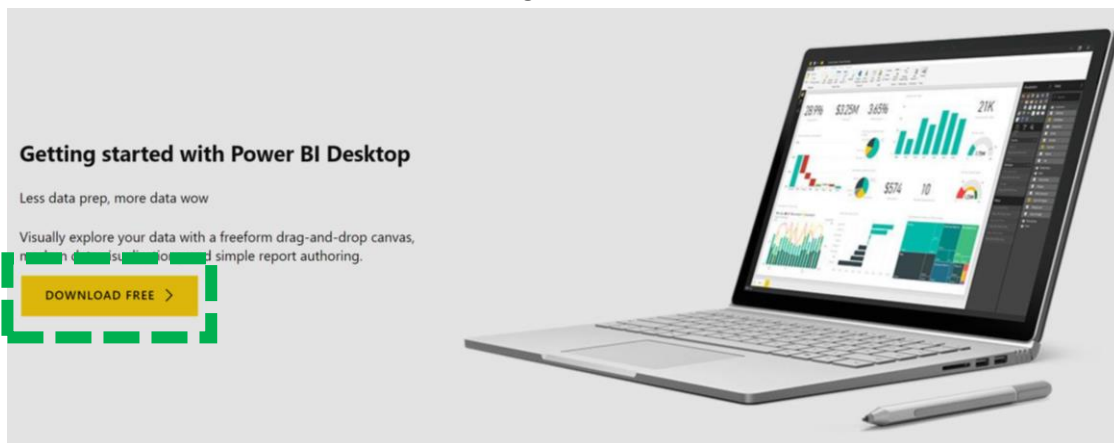
5.2. Download PowerBI

5.2.1. Go to PowerBI webpage: <https://powerbi.microsoft.com/en-us/get-started/> →

Click **Close** if blocking message shows



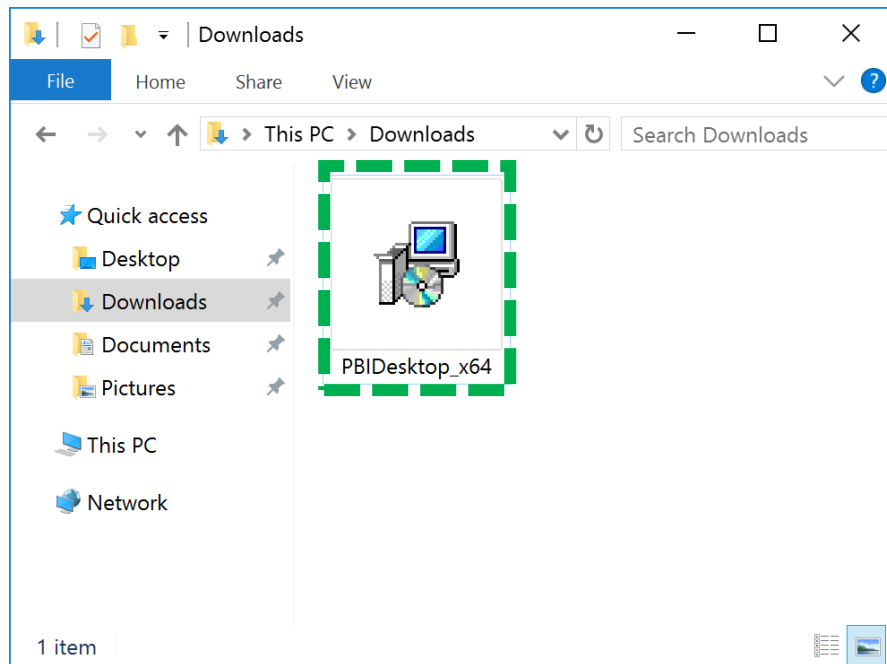
5.2.2. Click **DOWNLOAD FREE** to start downloading it



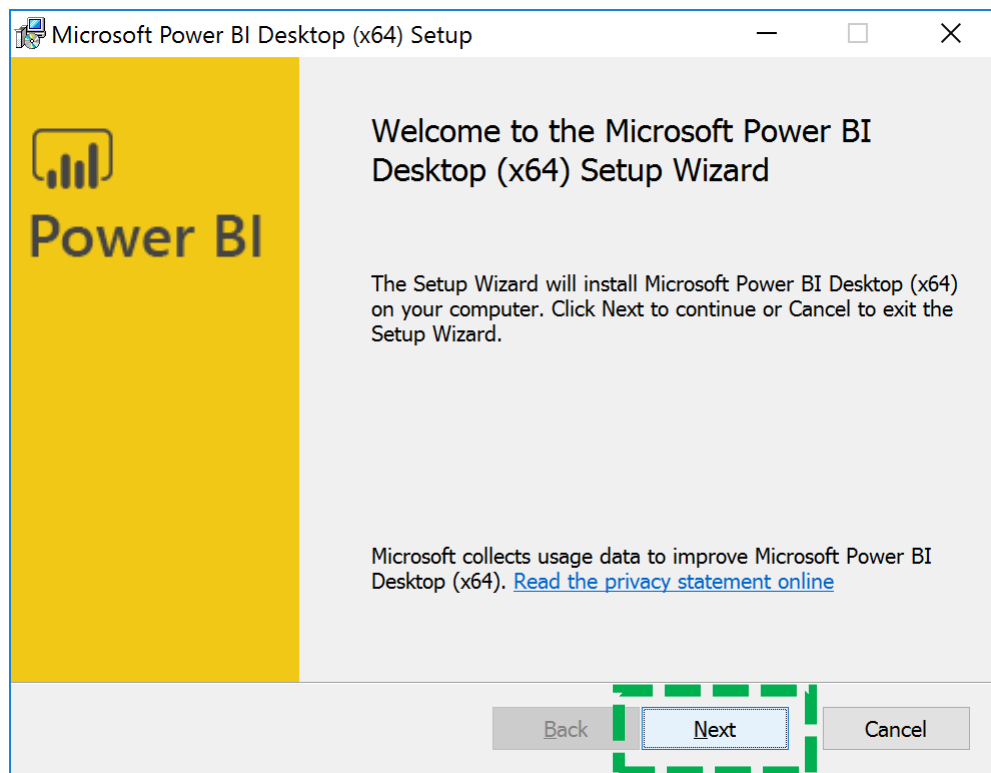


5.3. Install PowerBI

5.3.1. Open Windows Explore → C:\Users\Administrator\Download → Double Click **PBIDesktop_x64.msi**

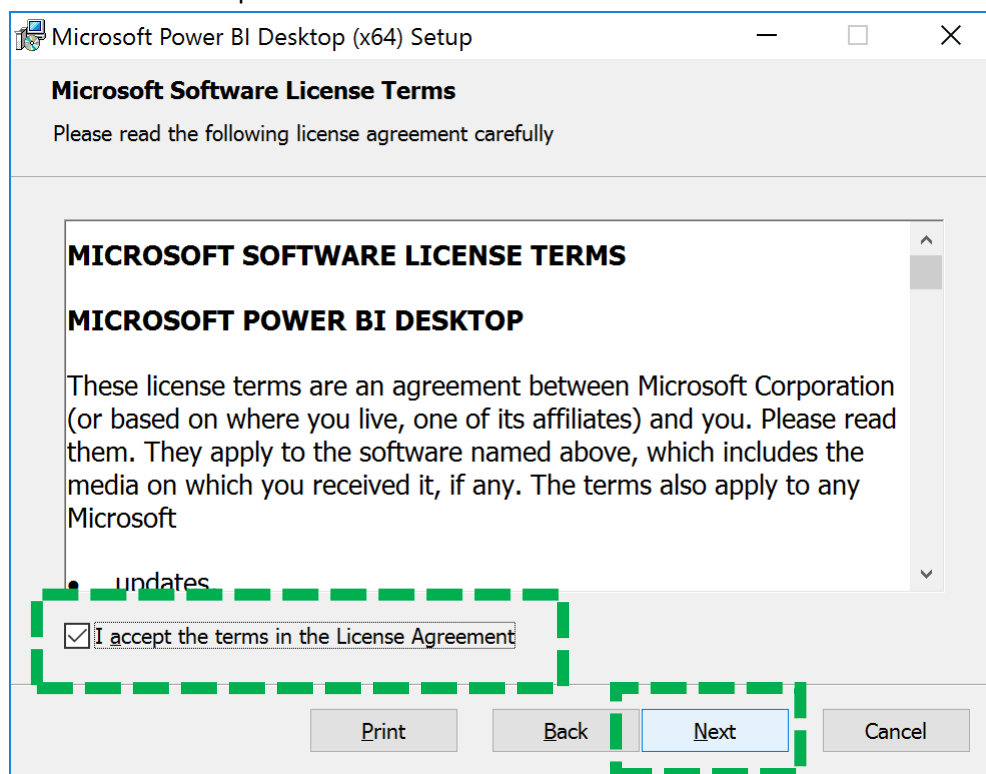


5.3.2. Click **Next**

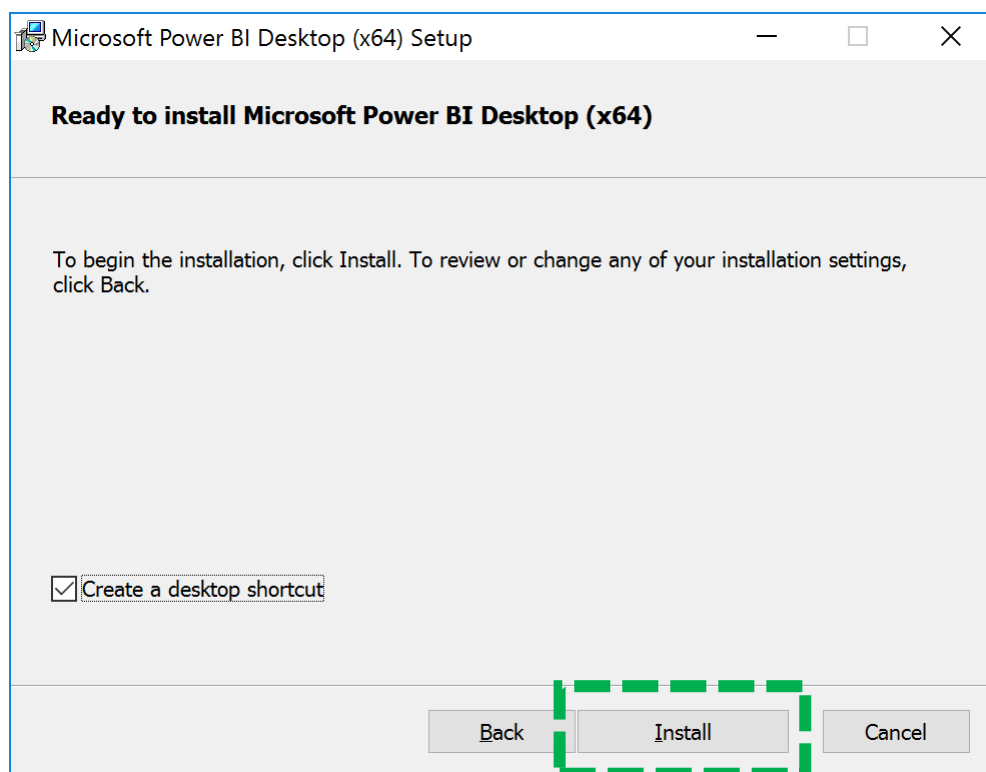




5.3.3. Tick the box to accept the term → Click **Next**

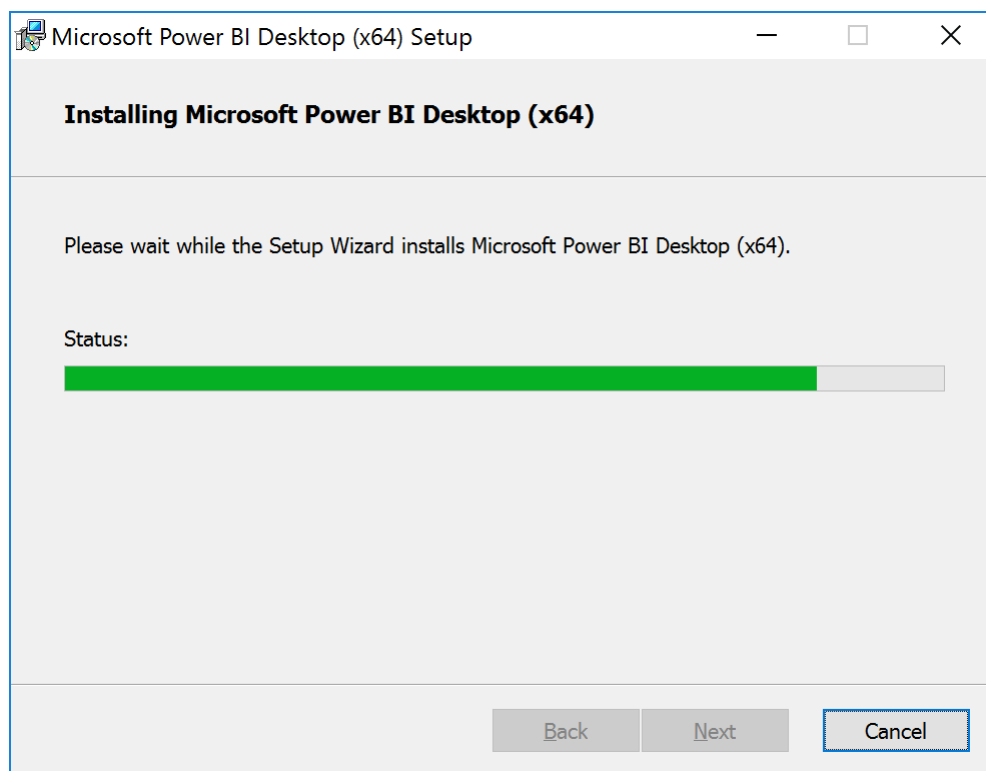


5.3.4. Click **Install**

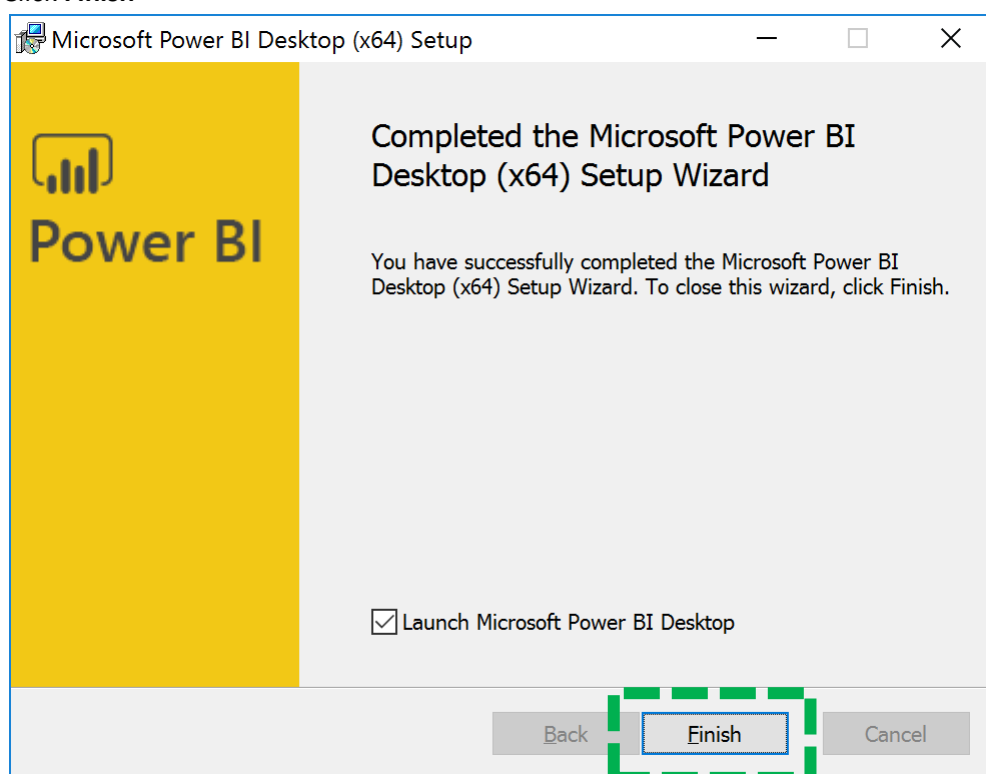




5.3.5. Wait for it to finish



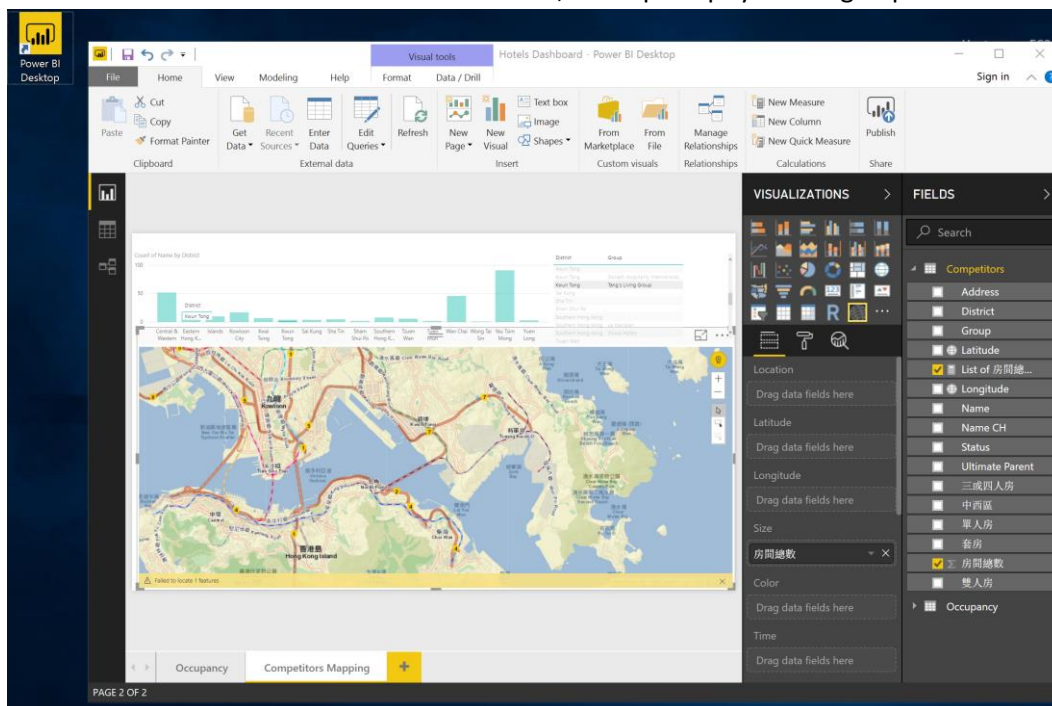
5.3.6. Click Finish





From here, you are good to go. Enjoy it.

After the PowerBI is launched for the first time, it will prompt you to sign up the service.



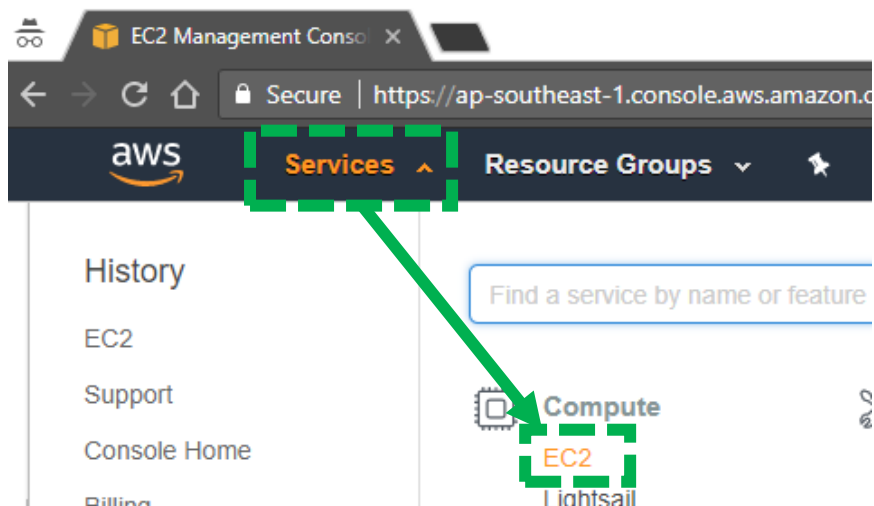


6. Create Elastic IP (Optional Step)

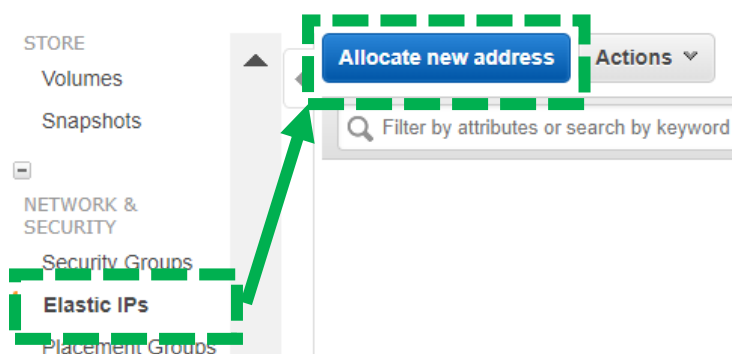
You may find that after you stop and start your remote machine, you cannot access it anymore. Why? Oh GOD! the IP has changed.

Elastic IP is here to save us to provide a dedicated IP for our remote machine.

6.1. Go back to **EC2** page (Services → EC2)



6.2. Click **Elastic IPs** → **Allocate new address**



6.3. Click **Allocate**

[Addresses](#) > Allocate new address

Allocate new address

Allocate a new Elastic IP address by selecting the scope in which it will be used

* Required

Cancel

Allocate

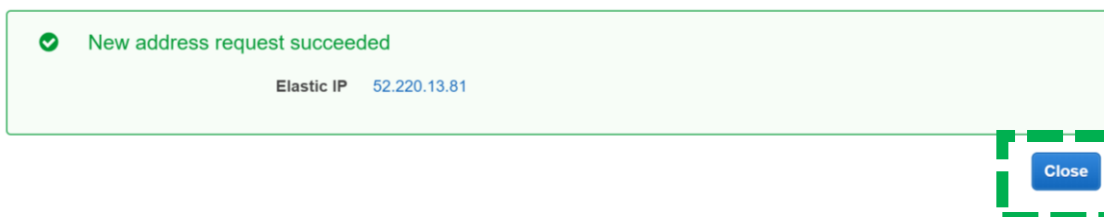


6.4. A new IP is allocated, Click **Close**

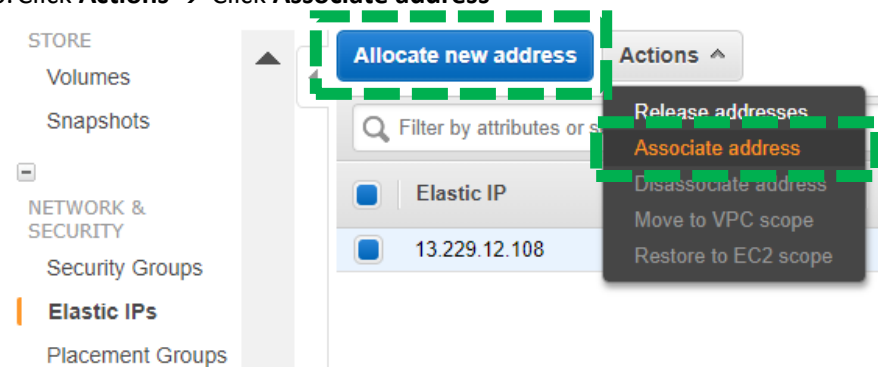
It allocated 52.220.13.81 for me. Your IP **MUST** be different from mine.

[Addresses](#) > Allocate new address

Allocate new address



6.5. Click **Actions** → Click **Associate address**



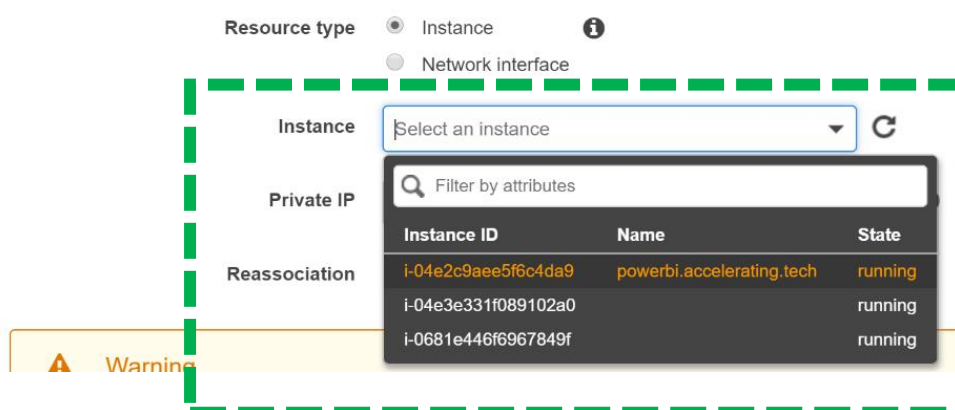
6.6. Associate address

- Choose the instance you created
- Choose the **Private IP**
- Click **Associate**

[Addresses](#) > Associate address

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (52.220.13.81)





[Addresses](#) > Associate address

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (52.220.13.81)

Resource type ☒ Instance ⓘ ☐ Network interface

Instance ⓘ

Private IP ⓘ

Reassociation ☐ Allow Elastic IP to be reassociated if already attached ⓘ



Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. [Learn more](#).

Cancel

Associate

**** Private IP – 172.31.3.24 is an Intranet IP and the IP – 52.220.13.81 which is allocated by Elastic IP is Public IP/Internet IP. Read the following post to know what internet and intranet is:**

https://www.tutorialspoint.com/computer_fundamentals/computer_internet_intranet.htm

6.7. Click **Close**

[Addresses](#) > Associate address

Associate address



Associate address request succeeded

Close