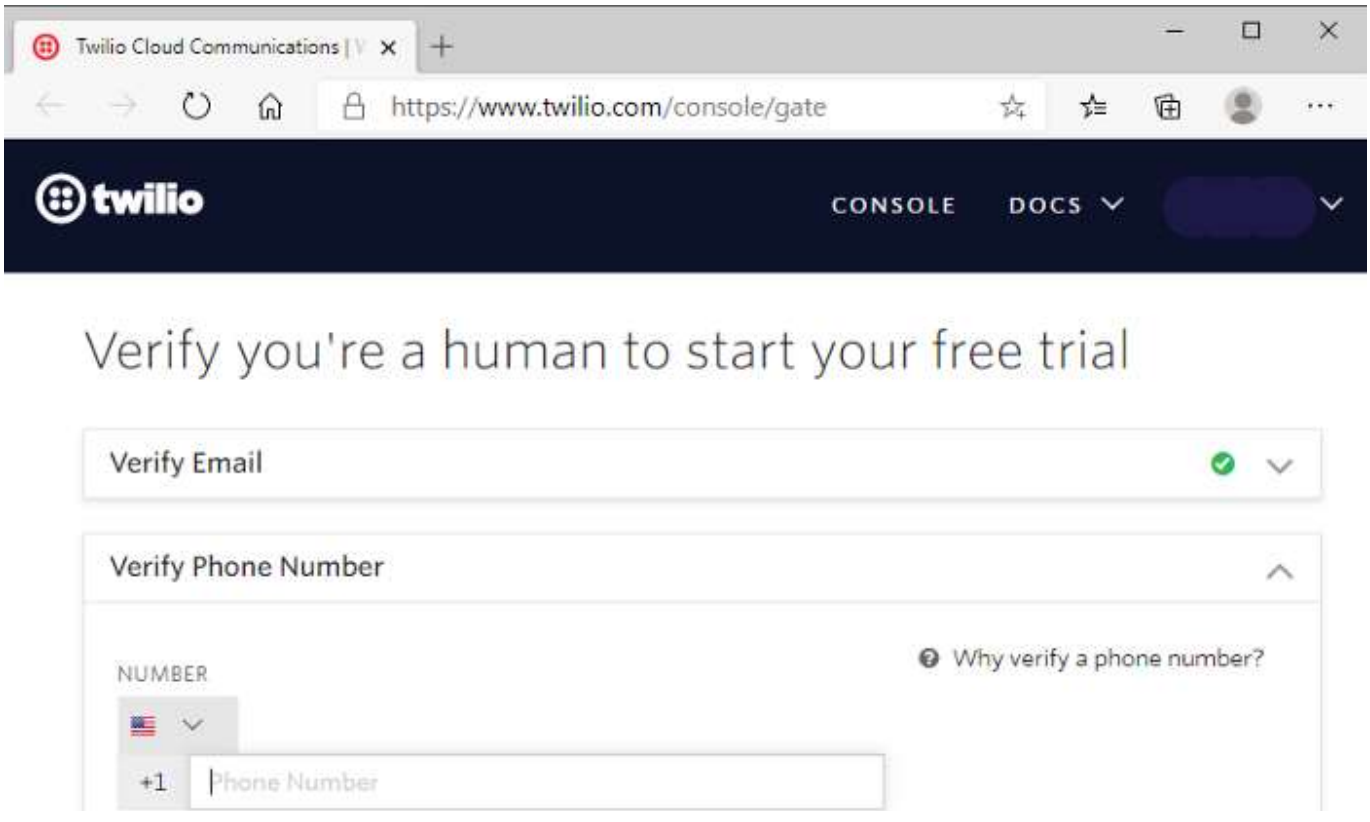
Peekaboo we see GRU

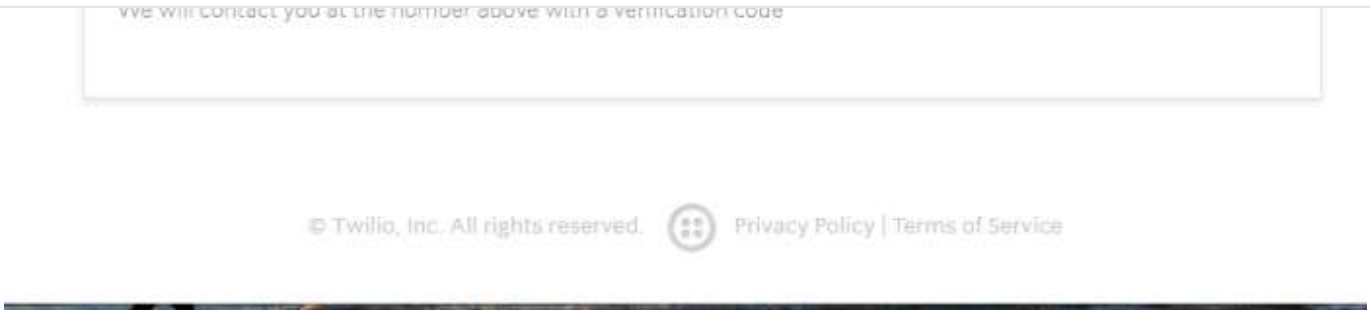
Peekaboo we see GRU (part 2)

Peekaboo we see GRU 3 days ago · 3 min read

Peekaboo we see GRU (part 2)

Now that Sysmon is installed, we will setup our development environment and get prepared for part 3 when we will code a 150 line program that sends us a text when “unauthorized” windows programs try to initiate network traffic. The basic example app is in python, the main app will be C#.



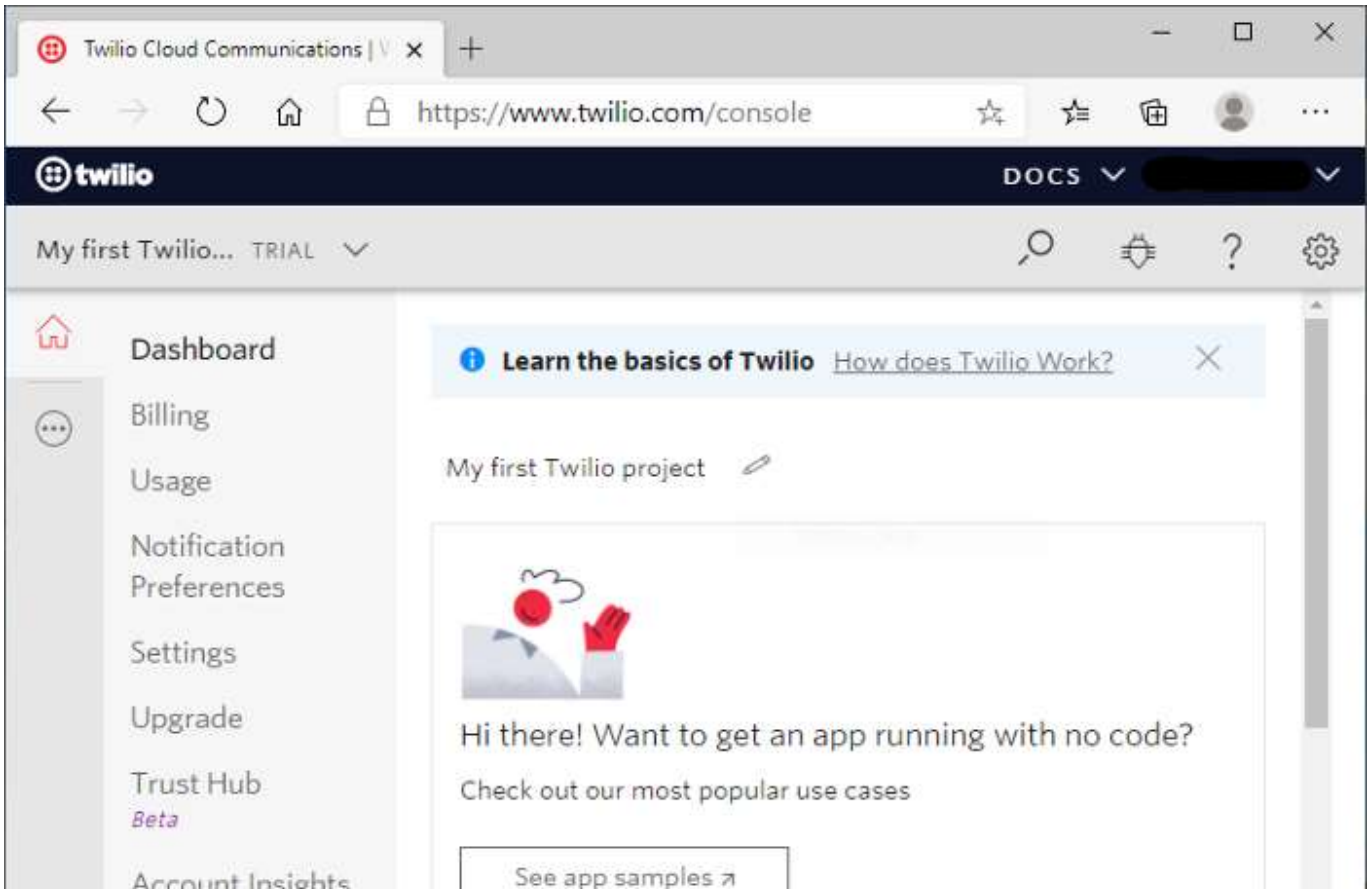


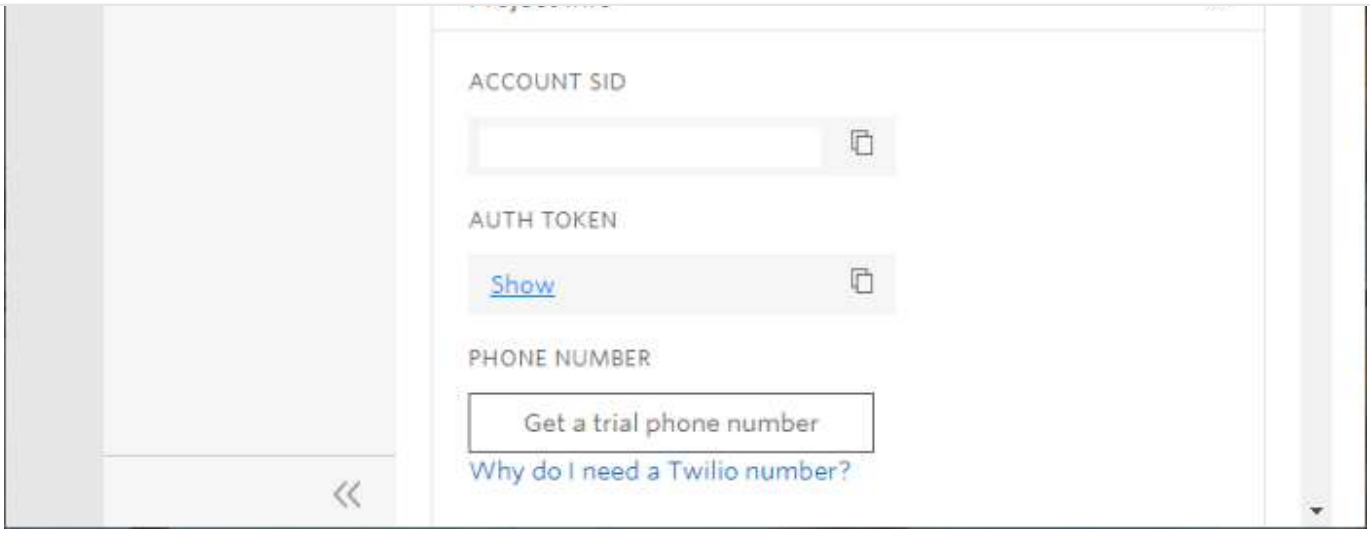
Verify you are human

Why C#? Many organizations don't allow python on user systems. C# will be a standard windows exe. Also, if your org has a way to sign binary files, that will allow you to follow security best practices.

The first step will be to create a Free Twilio account. We won't go through every step for that. Images of the key steps are above and below. If you need more help, this GeeksforGeeks link is a good guide.

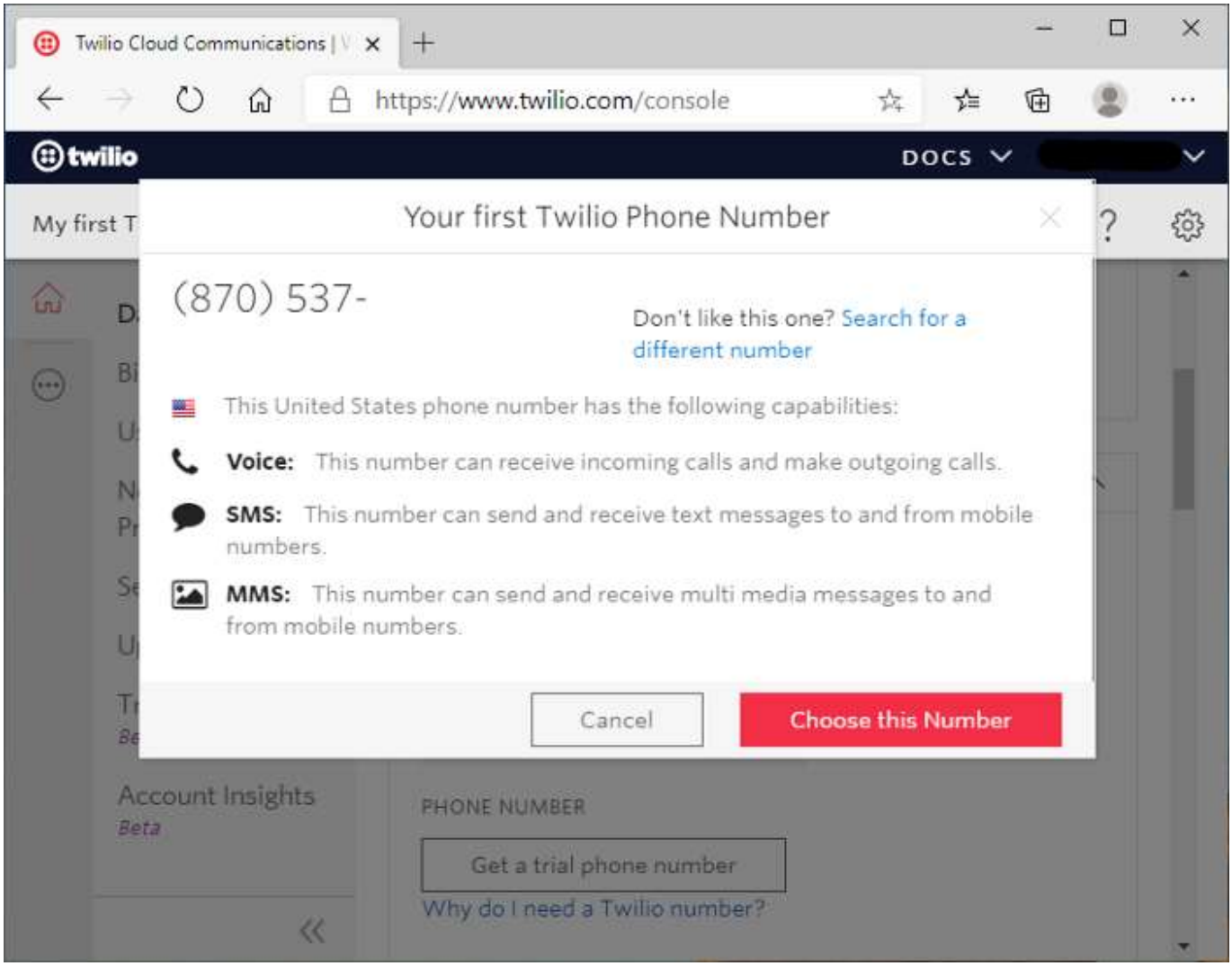
Python | Send SMS using Twilio — GeeksforGeeks





www.twilio.com/console

View of the Twilio console dashboard.



Choose your phone number. **Note Twilio starts with a $15 credit.**

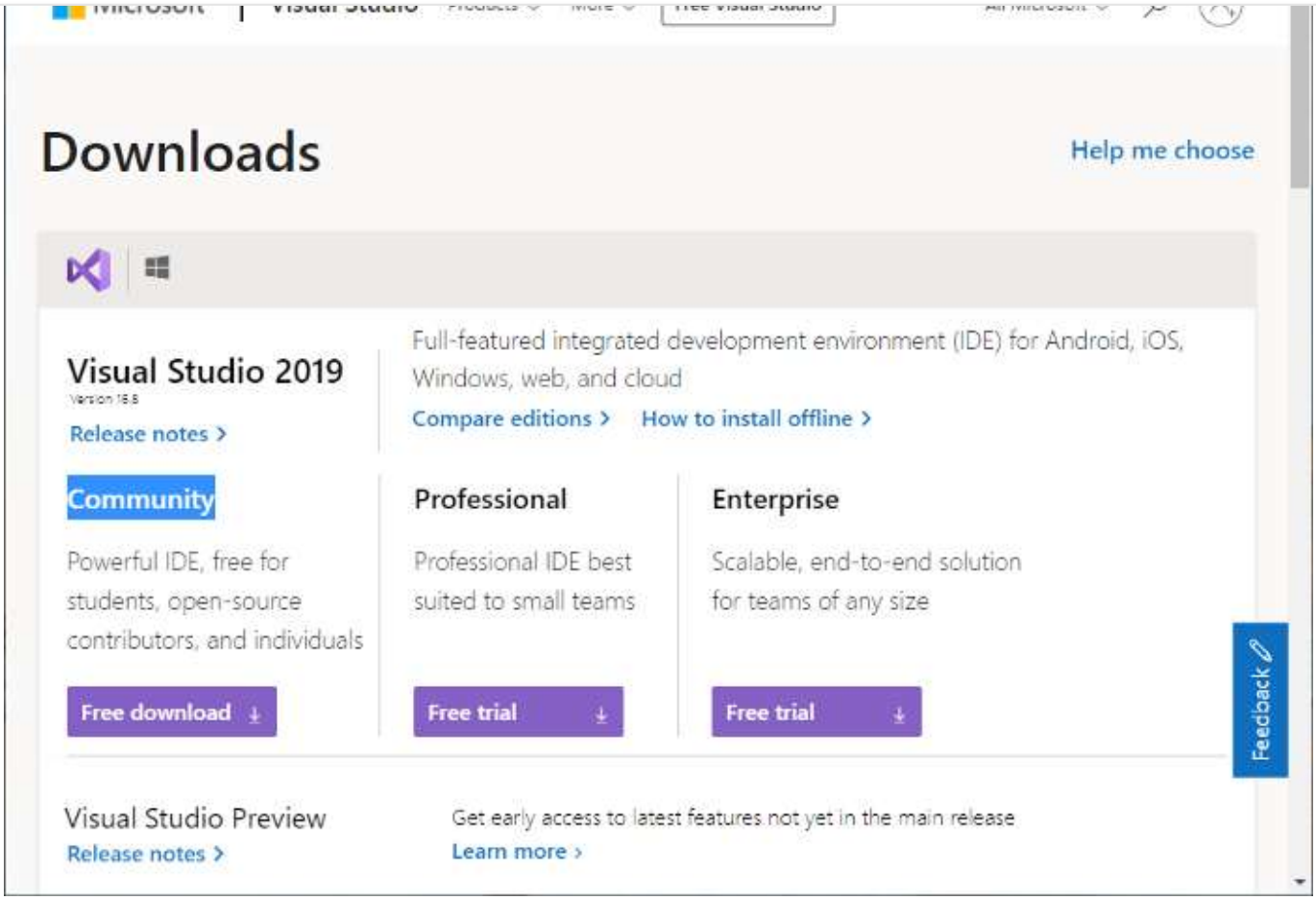
Before we jump into C#, here is the python code you can use to quickly send a text message to your phone. Best to confirm everything is working before we jump into Visual Studio.

```
# importing twilio
from twilio.rest import Client

# Your Account Sid and Auth Token from twilio.com / console
account_sid = 'ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
auth_token = 'your_auth_token'

client = Client(account_sid, auth_token)

''' Change the value of 'from' with the number
received from Twilio and the value of 'to'
with the number in which you want to send message.'''
message = client.messages.create(
                              from_='+15017122661',
                              body ='body',
                              to ='+15558675310'
                          )

print(message.sid)
```

Python | Send SMS using Twilio — GeeksforGeeks

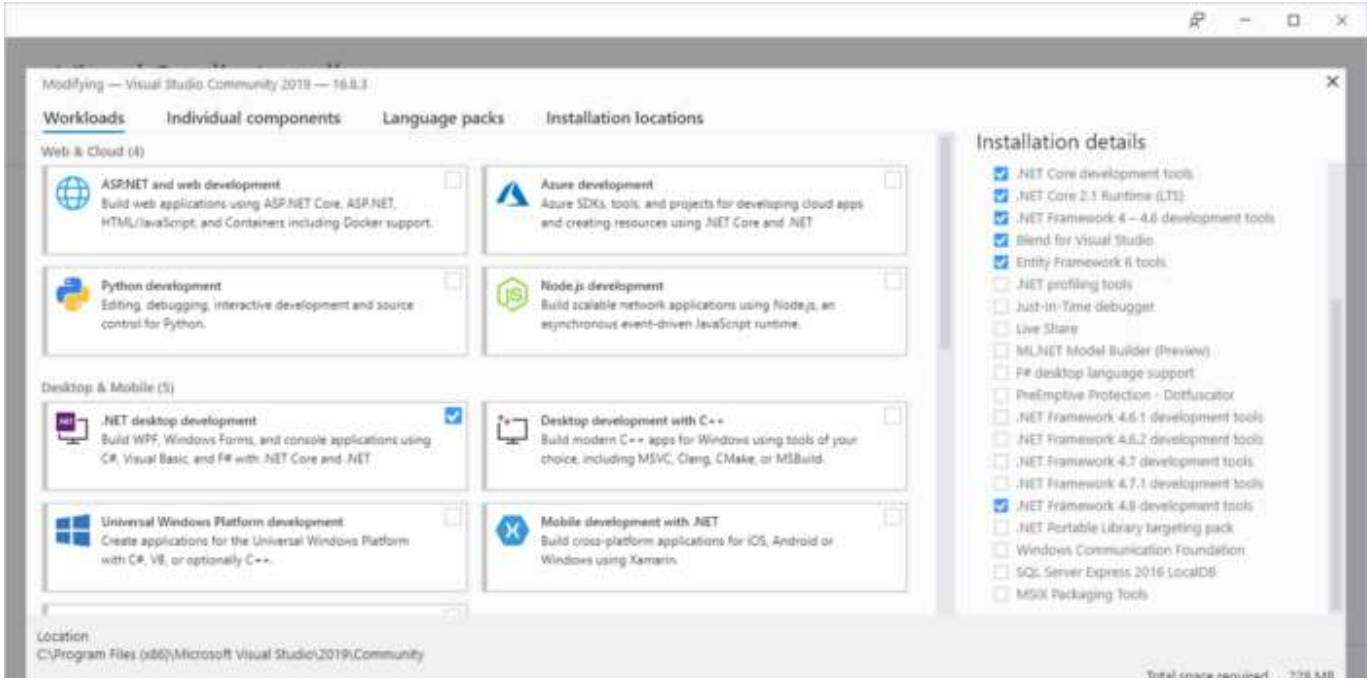
This python example is from here.. Python | Send SMS using Twilio — GeeksforGeeks

Now we are ready to create our C# project. Easier to show the next steps, skip these steps if you already have Visual Studio installed.

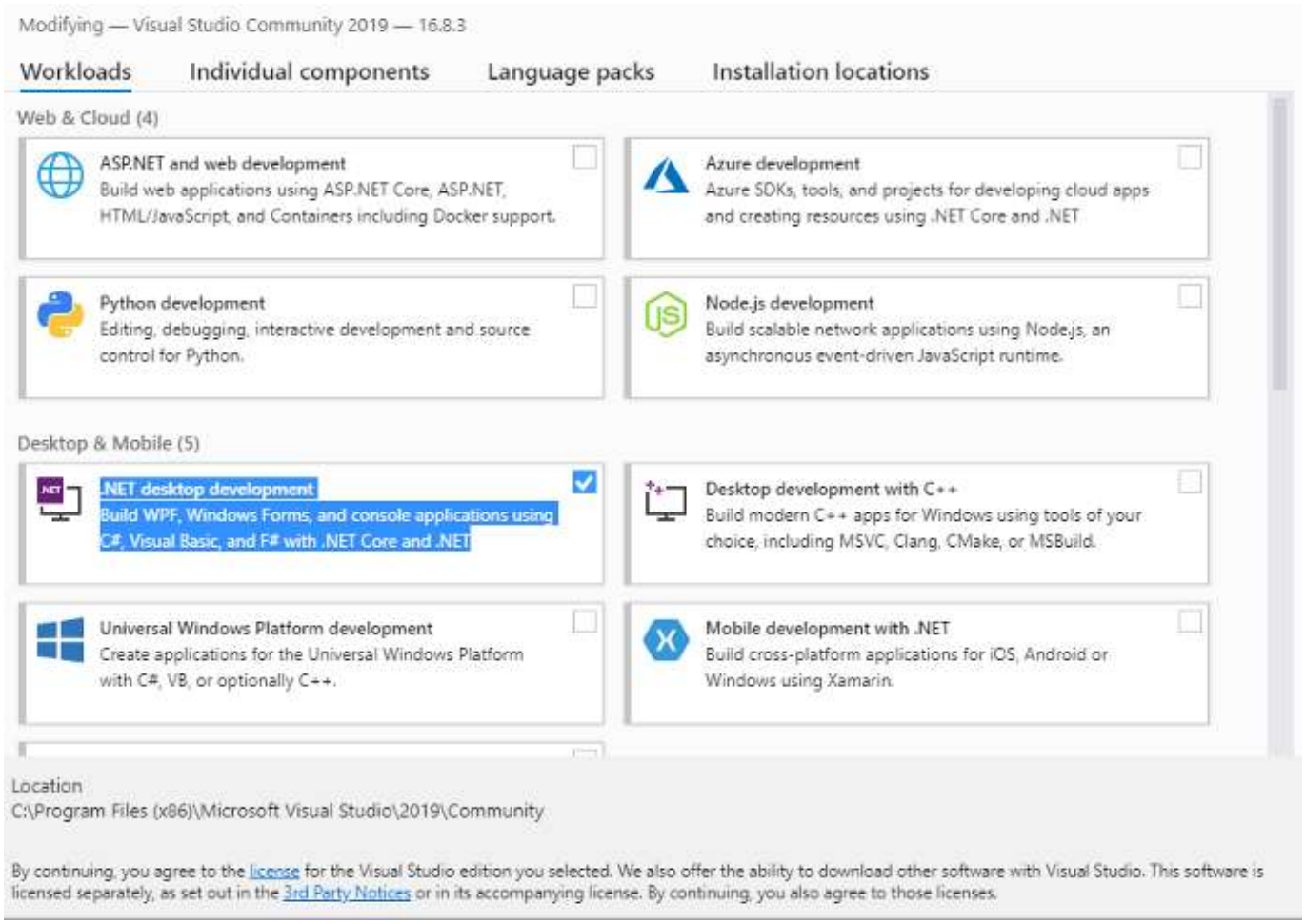


Download Visual Studio Community

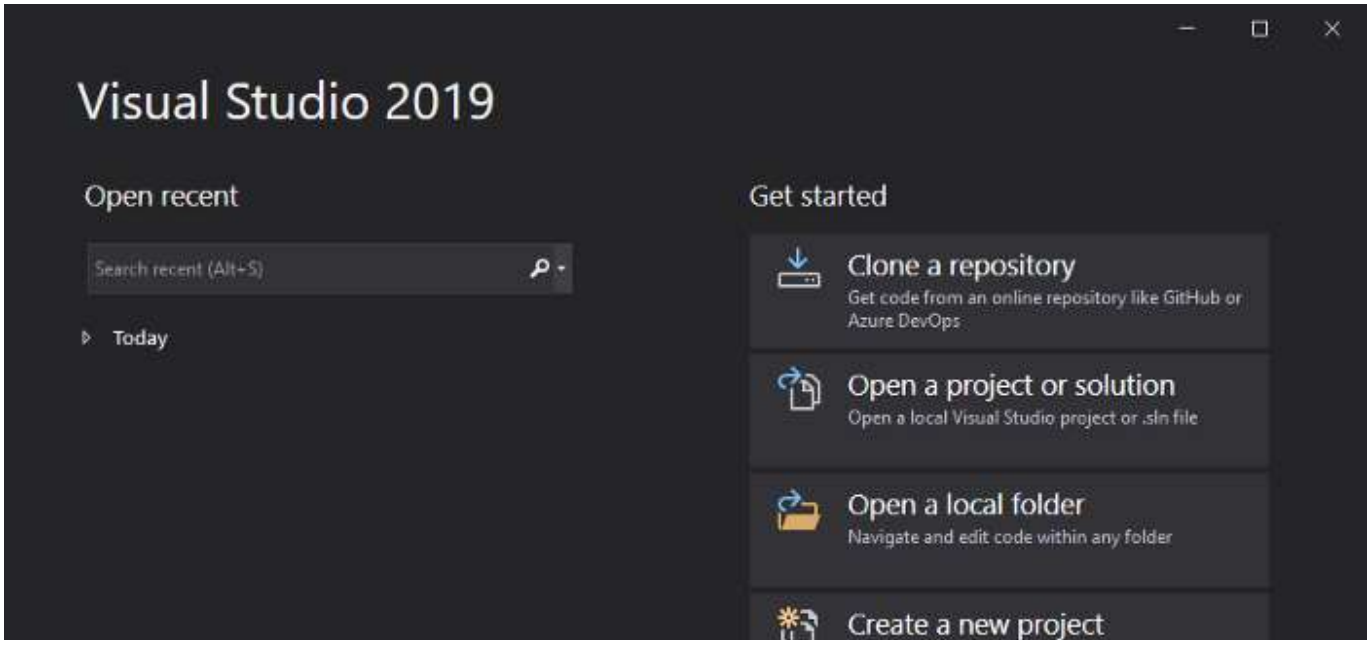
Download Visual Studio Community.



Choose these options

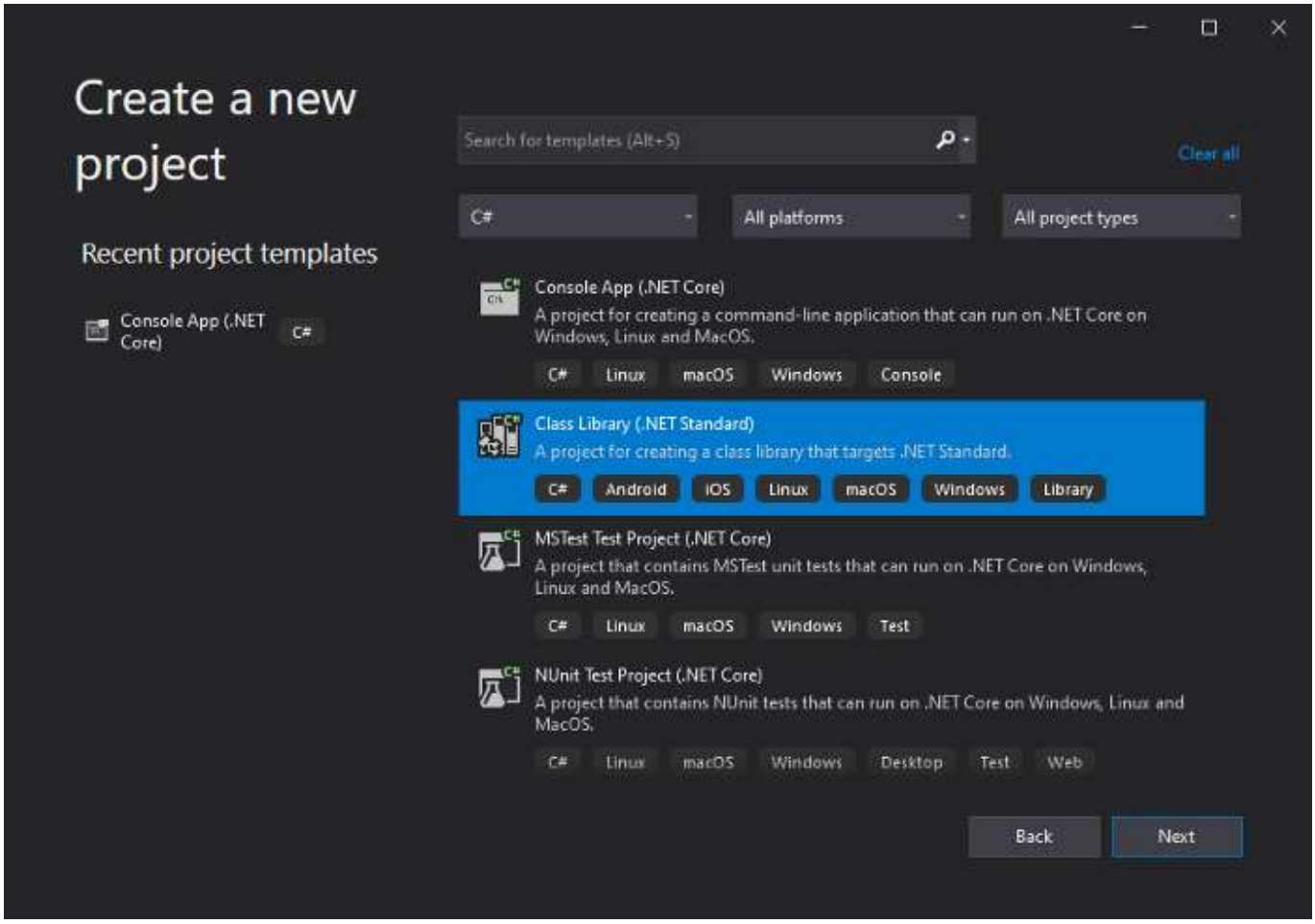


Select .NET desktop development



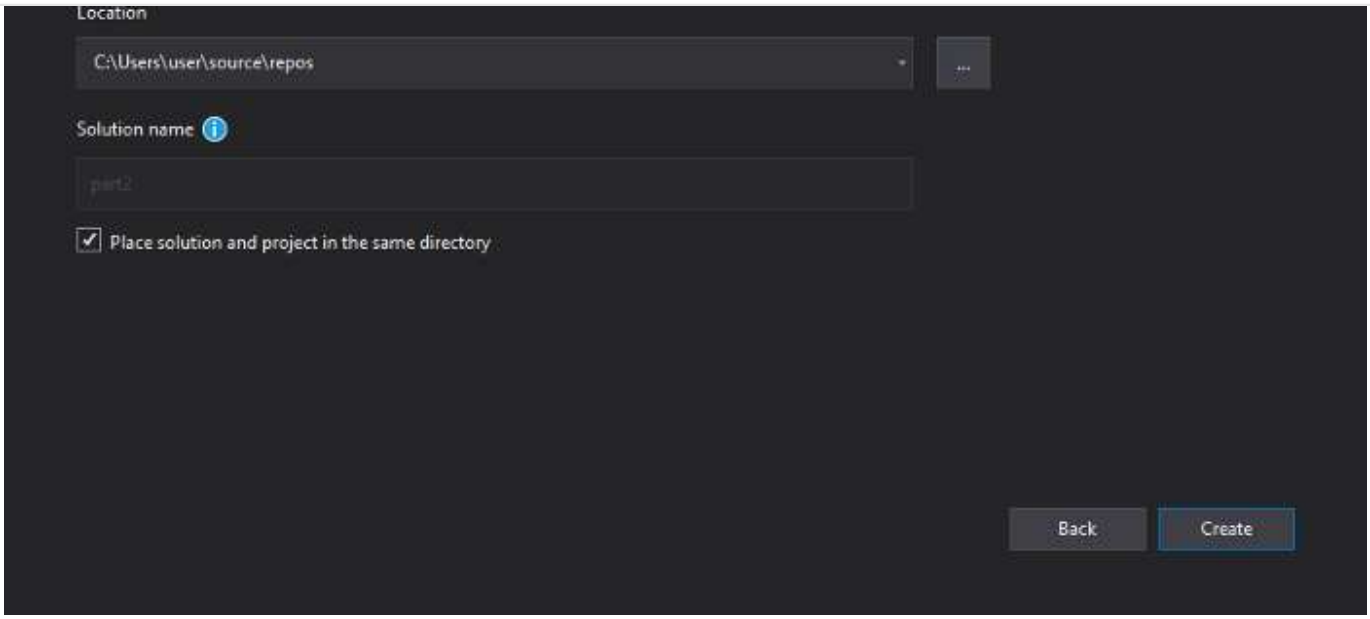
Create a new project

Select create a new project.



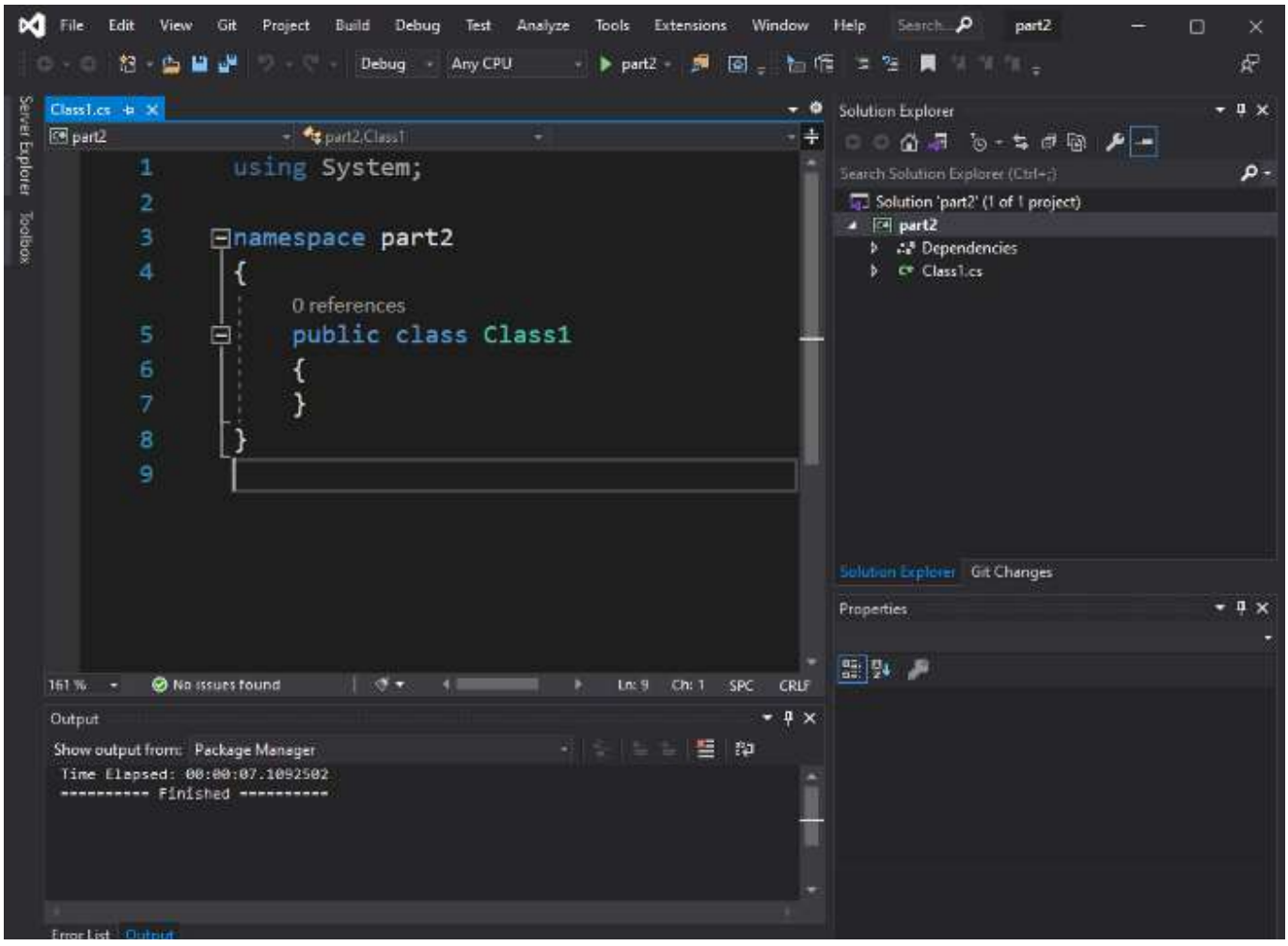
C# Class (.NET Standard)

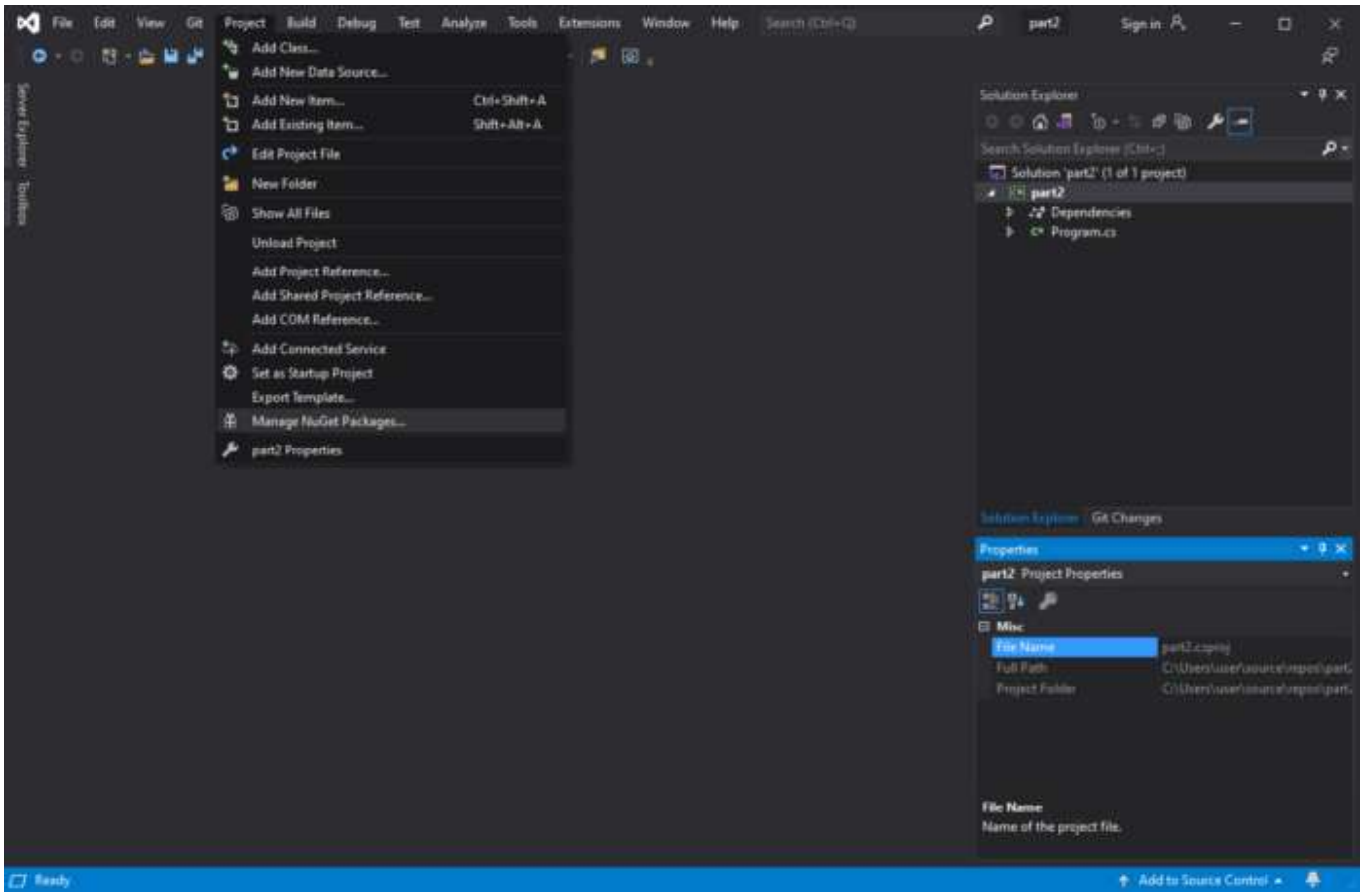
Select C# Class Library (.NET Standard)



Name your project

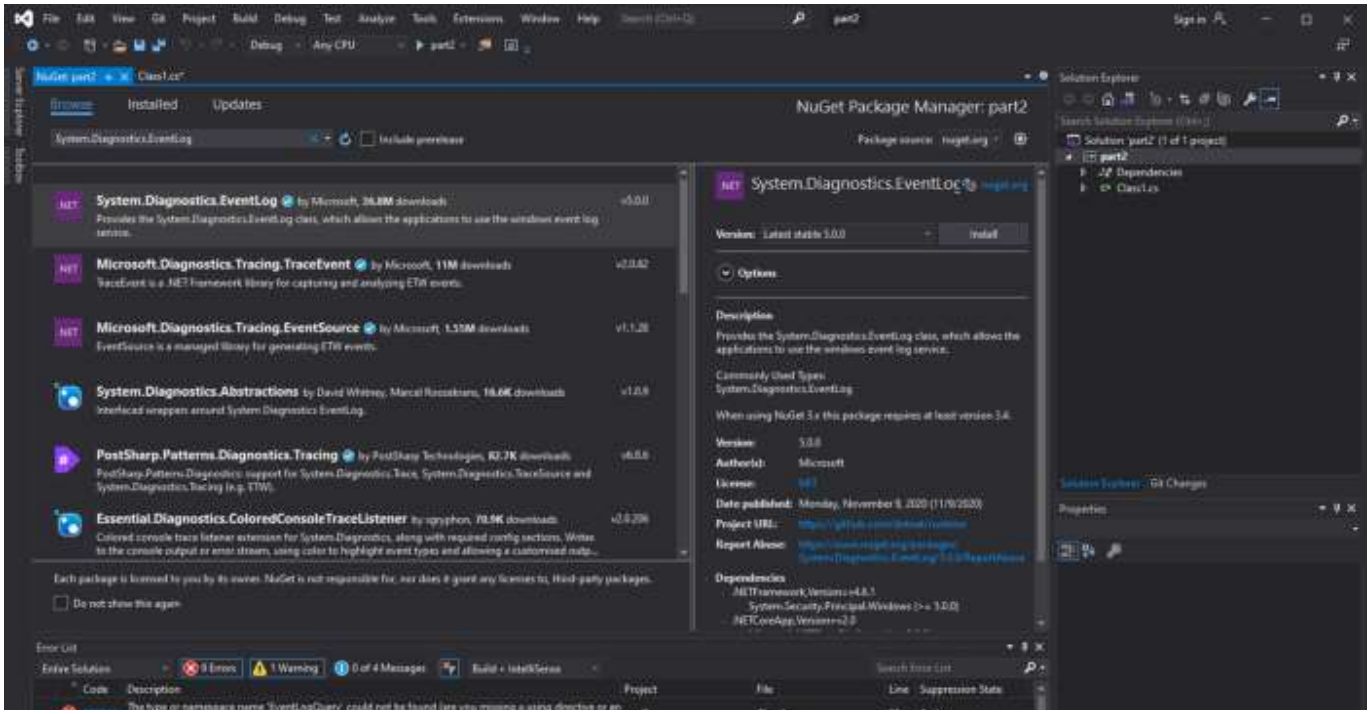
We are using “part2" as the project name.





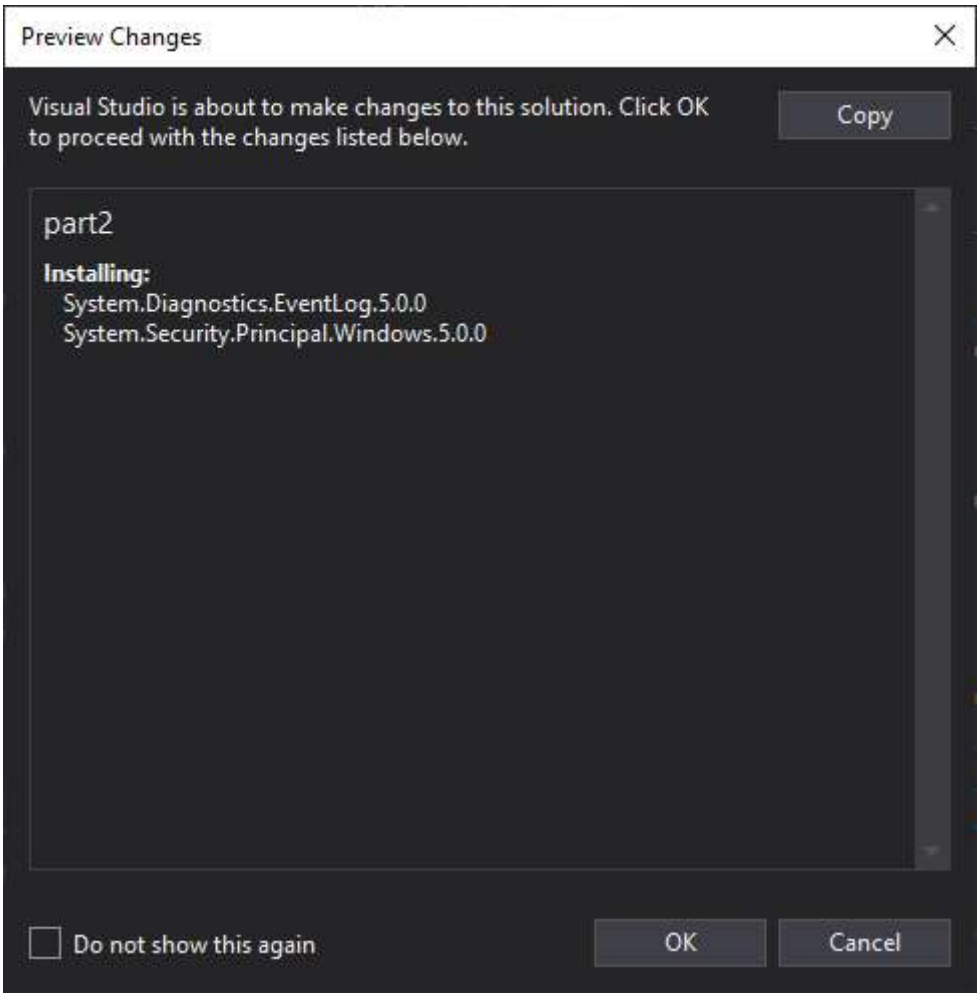
Install required NuGet Package.

Select “Manage NuGet Packages”.

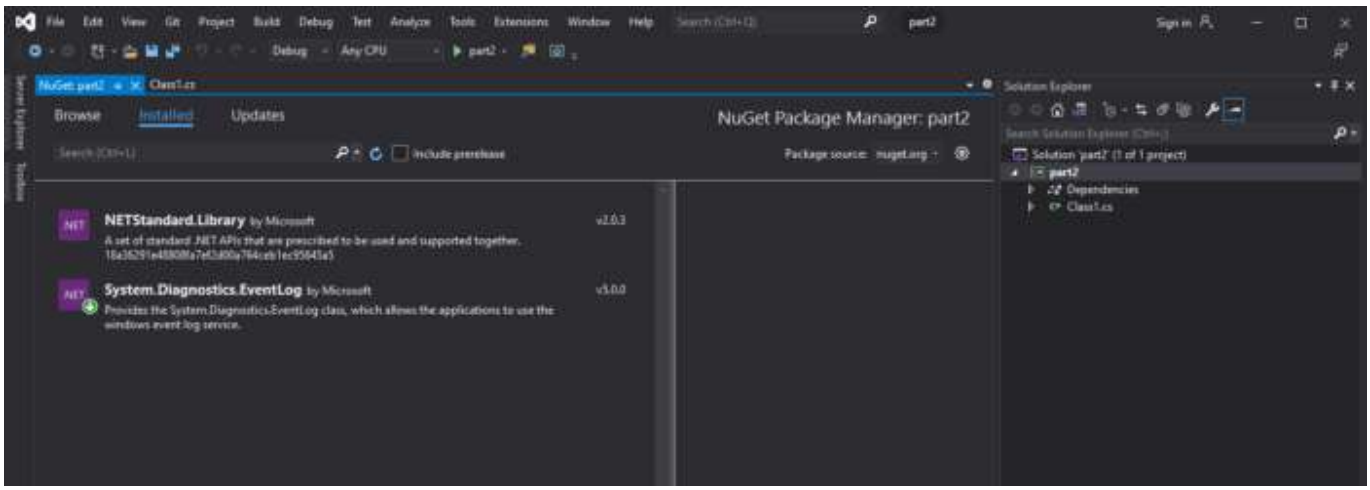


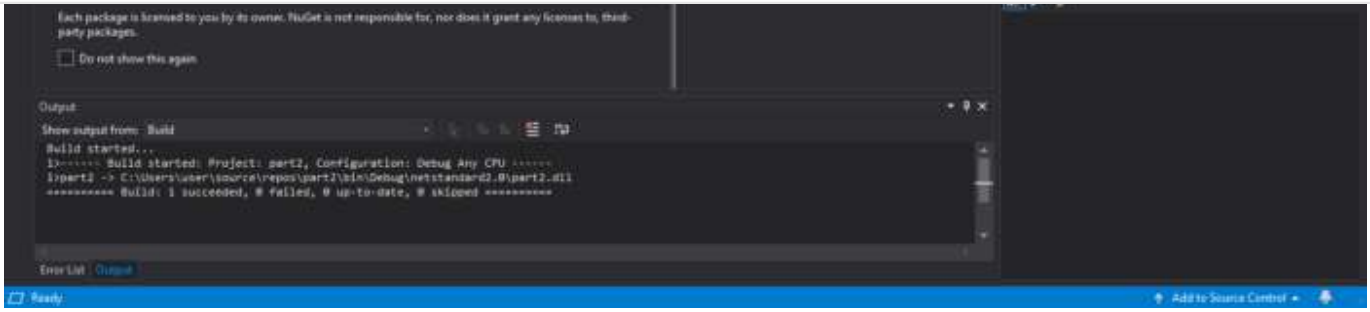
Install System.Diagnostics.EventLog

Install the System.Diagnostics.EventLog NuGet Package



Click OK to install





Installed packages

Verify your installed Packages.

OK, that was a lot of work with no real coding yet. Tomorrow we will post part 3 in our series.

Sysmon Twilio Infosec Windows10