

[Get started](#)[Open in app](#)

## Peekaboo we see GRU

[Follow](#)[About](#)

## 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're a human to start your free trial

Verify Email

✓

Verify Phone Number

^

NUMBER

🇺🇸

▼

+1

Phone Number

?

 Why verify a phone number?

[Get started](#)[Open in app](#)

We will contact you at the number above with a verification code

© Twilio, Inc. All rights reserved.



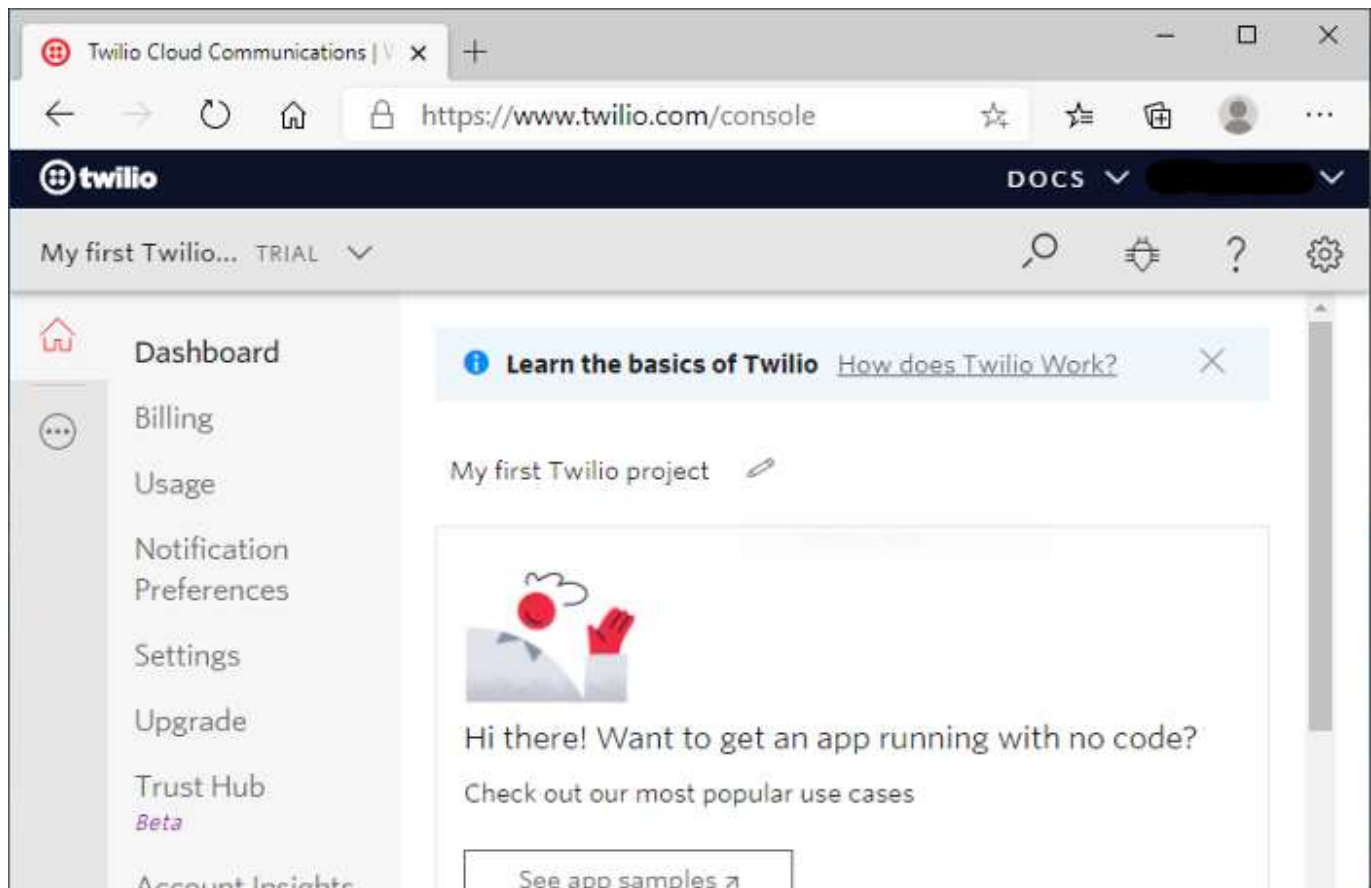
[Privacy Policy](#) | [Terms of Service](#)

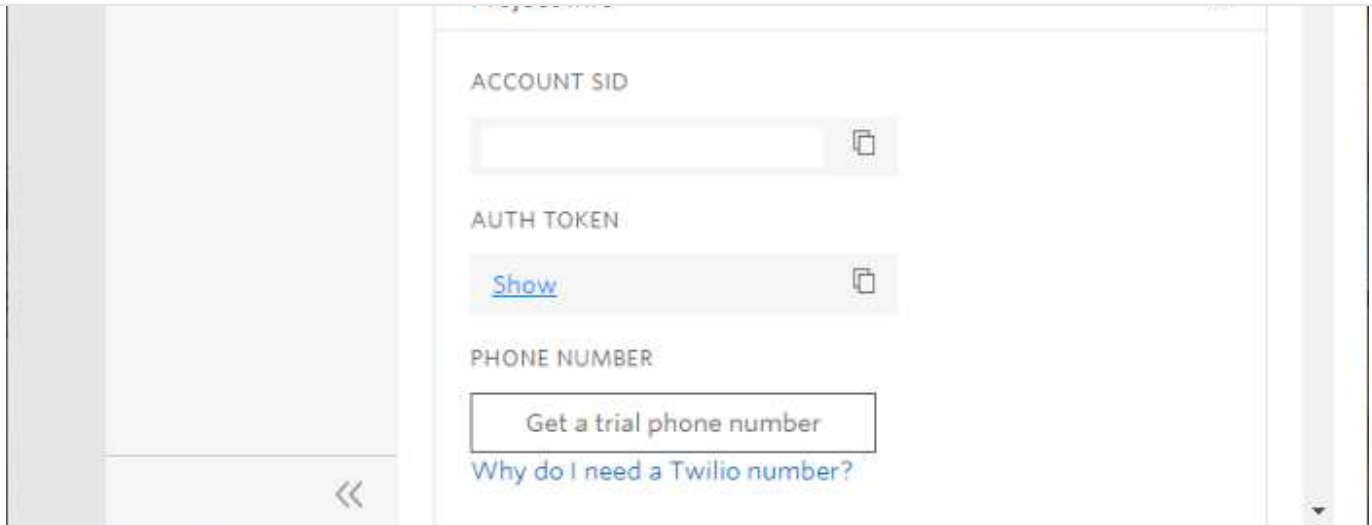
Verify you are human

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.

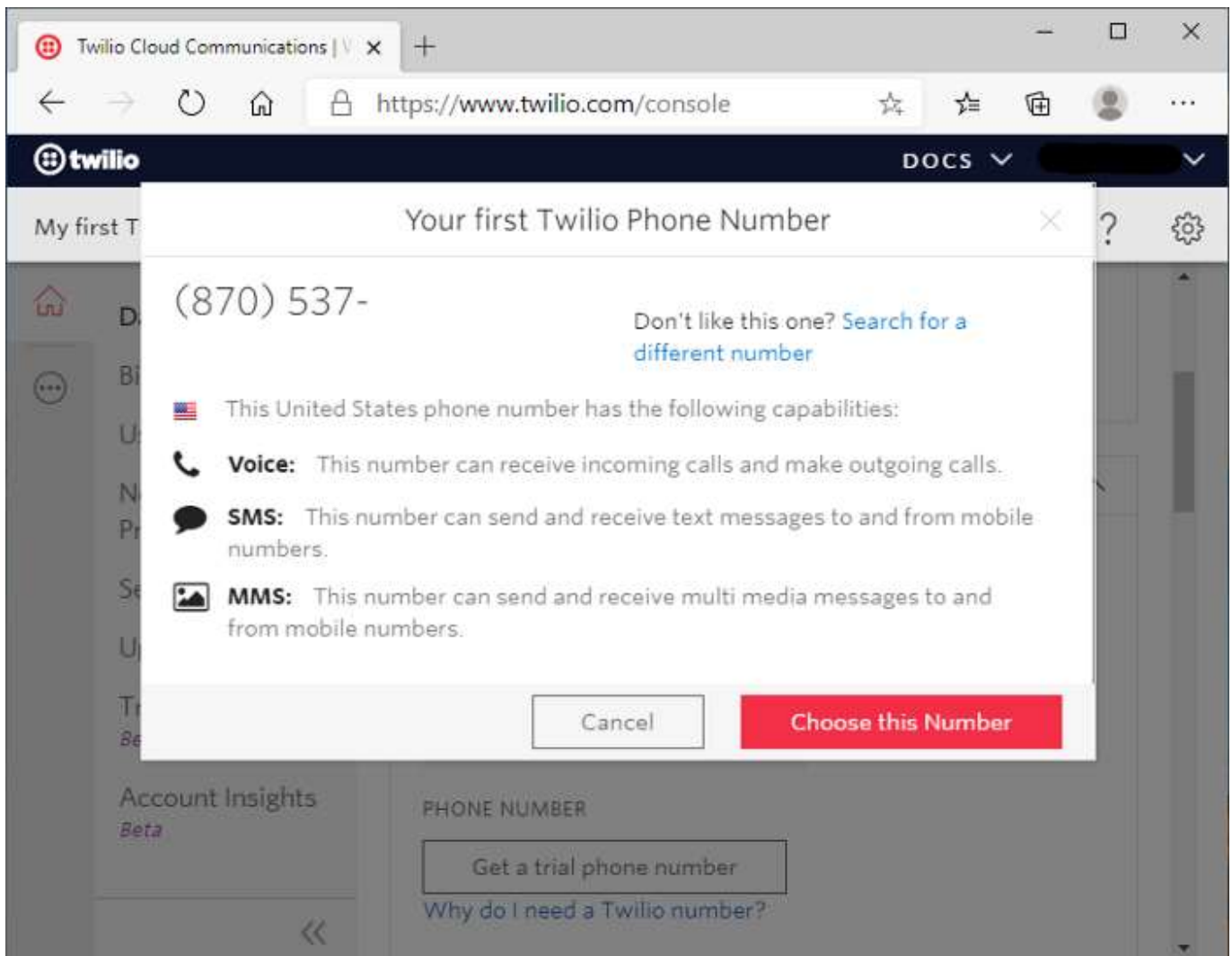
[Python | Send SMS using Twilio — GeeksforGeeks](#)



[Get started](#)[Open in app](#)

www.twilio.com/console

View of the Twilio console dashboard.



[Get started](#)[Open in app](#)

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 = 'ACXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
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.



[Get started](#)[Open in app](#)

**Downloads** [Help me choose](#)

**Visual Studio 2019**  
Version 16.8  
[Release notes >](#)

**Community**  
Powerful IDE, free for students, open-source contributors, and individuals  
[Free download](#)

**Professional**  
Professional IDE best suited to small teams  
[Free trial](#)

**Enterprise**  
Scalable, end-to-end solution for teams of any size  
[Free trial](#)

**Visual Studio Preview**  
[Release notes >](#)

Get early access to latest features not yet in the main release  
[Learn more >](#)

[Feedback](#)

Download Visual Studio Community

Download Visual Studio Community.

Modifying — Visual Studio Community 2019 — 16.8.3

**Workloads** Individual components Language packs Installation locations

Web & Cloud (4)

- ☐ ASP.NET and web development  
Build web applications using ASP.NET Core, ASP.NET, HTML/JavaScript, and Containers including Docker support.
- ☐ Azure development  
Azure SDKs, tools, and projects for developing cloud apps and creating resources using .NET Core and .NET
- ☐ Python development  
Editing, debugging, interactive development and source control for Python.
- ☐ Node.js development  
Build scalable network applications using Node.js, an asynchronous event-driven JavaScript runtime.

Desktop & Mobile (5)

- ☒ .NET desktop development  
Build WPF, Windows Forms, and console applications using C#, Visual Basic, and F# with .NET Core and .NET
- ☐ Desktop development with C++  
Build modern C++ apps for Windows using tools of your choice, including MSVC, Clang, CMake, or MSBuild.
- ☐ Universal Windows Platform development  
Create applications for the Universal Windows Platform with C#, VB, or optionally C++.
- ☐ Mobile development with .NET  
Build cross-platform applications for iOS, Android or Windows using Xamarin.

Location  
C:\Program Files (x86)\Microsoft Visual Studio\2019\Community

**Installation details**

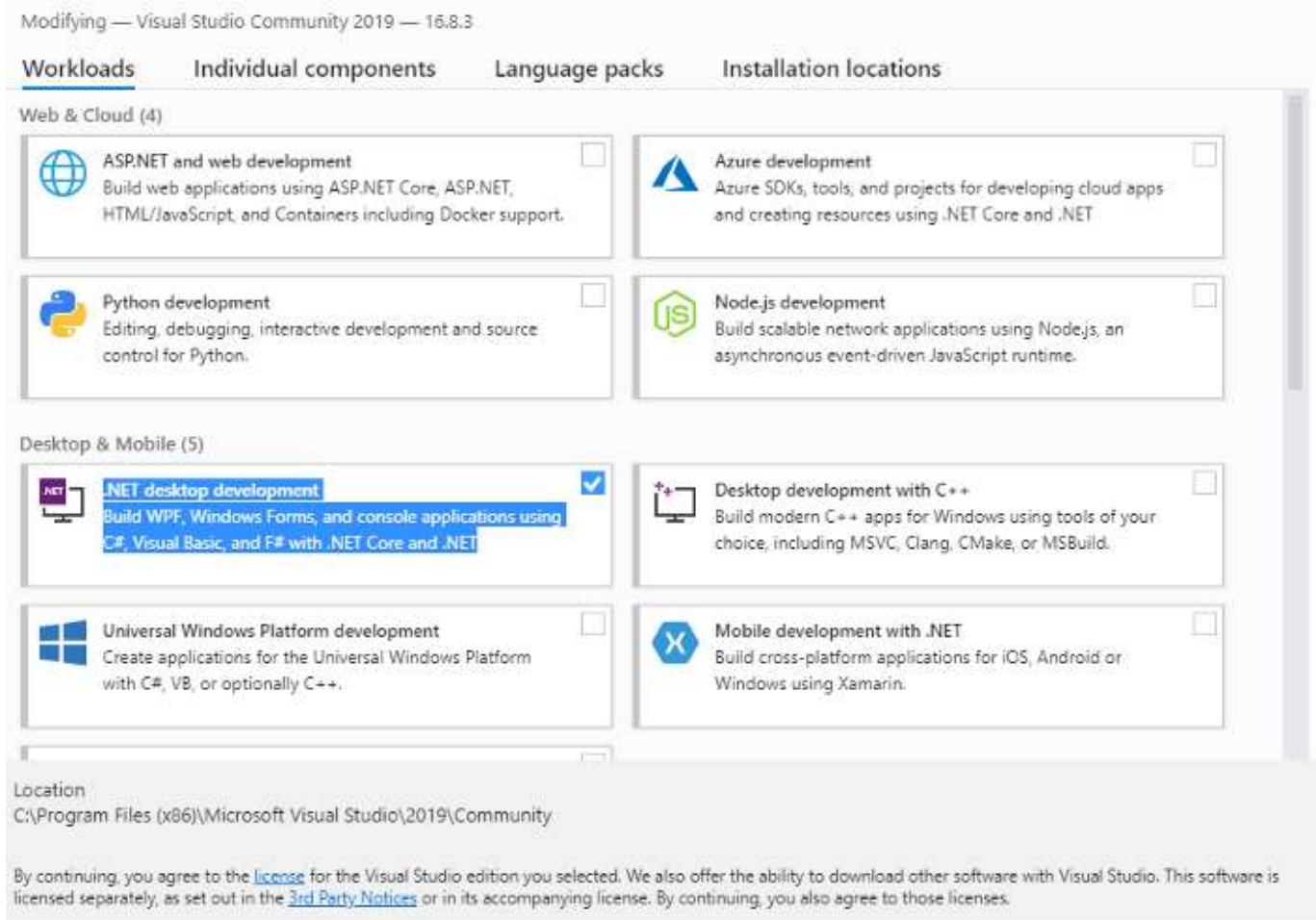
- ☒ .NET Core development tools
- ☒ .NET Core 2.1 Runtime (LTS)
- ☒ .NET Framework 4 - 4.6 development tools
- ☒ Blend for Visual Studio
- ☒ Entity Framework 6 tools
- ☐ .NET profiling tools
- ☐ Just-In-Time debugger
- ☐ Live Share
- ☐ ML.NET Model Builder (Preview)
- ☐ F# desktop language support
- ☐ PreEmptive Protection - Dotfuscator
- ☐ .NET Framework 4.6.1 development tools
- ☐ .NET Framework 4.6.2 development tools
- ☐ .NET Framework 4.7 development tools
- ☐ .NET Framework 4.7.1 development tools
- ☒ .NET Framework 4.8 development tools
- ☐ .NET Portable Library targeting pack
- ☐ Windows Communication Foundation
- ☐ SQL Server Express 2016 LocalDB
- ☐ MSIX Packaging Tools

Total space required: 3.98 GB

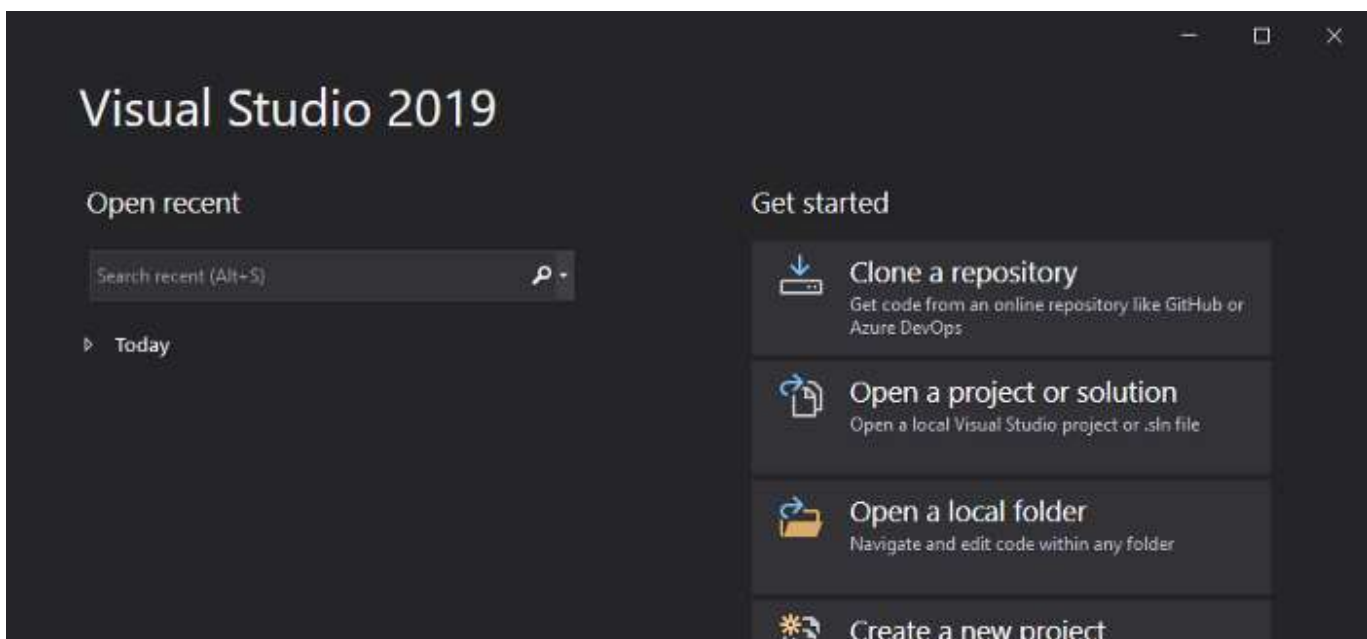


[Get started](#)[Open in app](#)

Choose these options



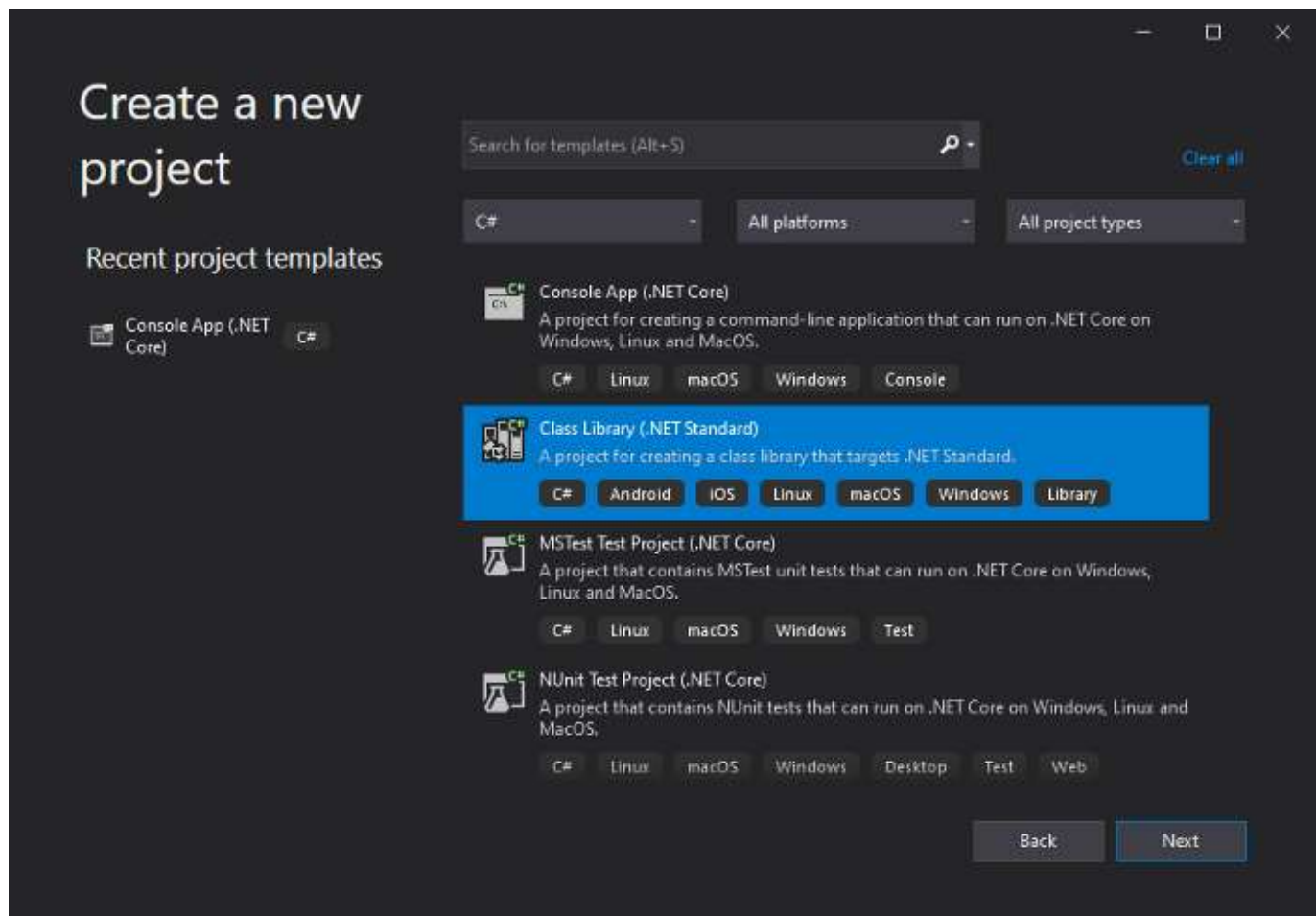
Select .NET desktop development



[Get started](#)[Open in app](#)

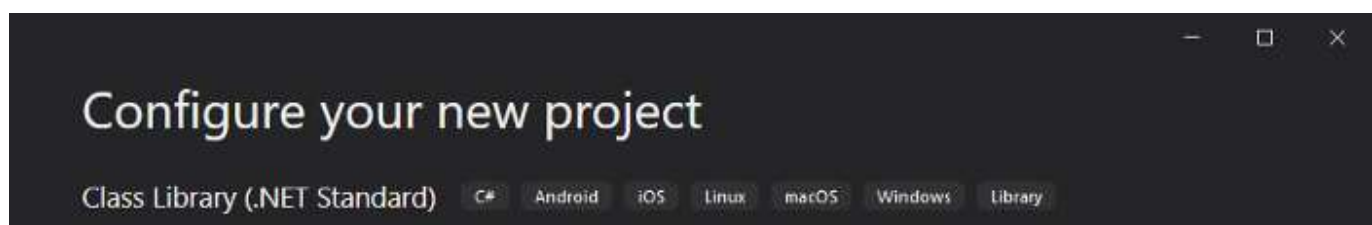
Create a new project

Select create a new project.



C# Class (.NET Standard)

Select C# Class Library (.NET Standard)



[Get started](#)[Open in app](#)

Location

CAUsers\user\source\repos

Solution name ⓘ

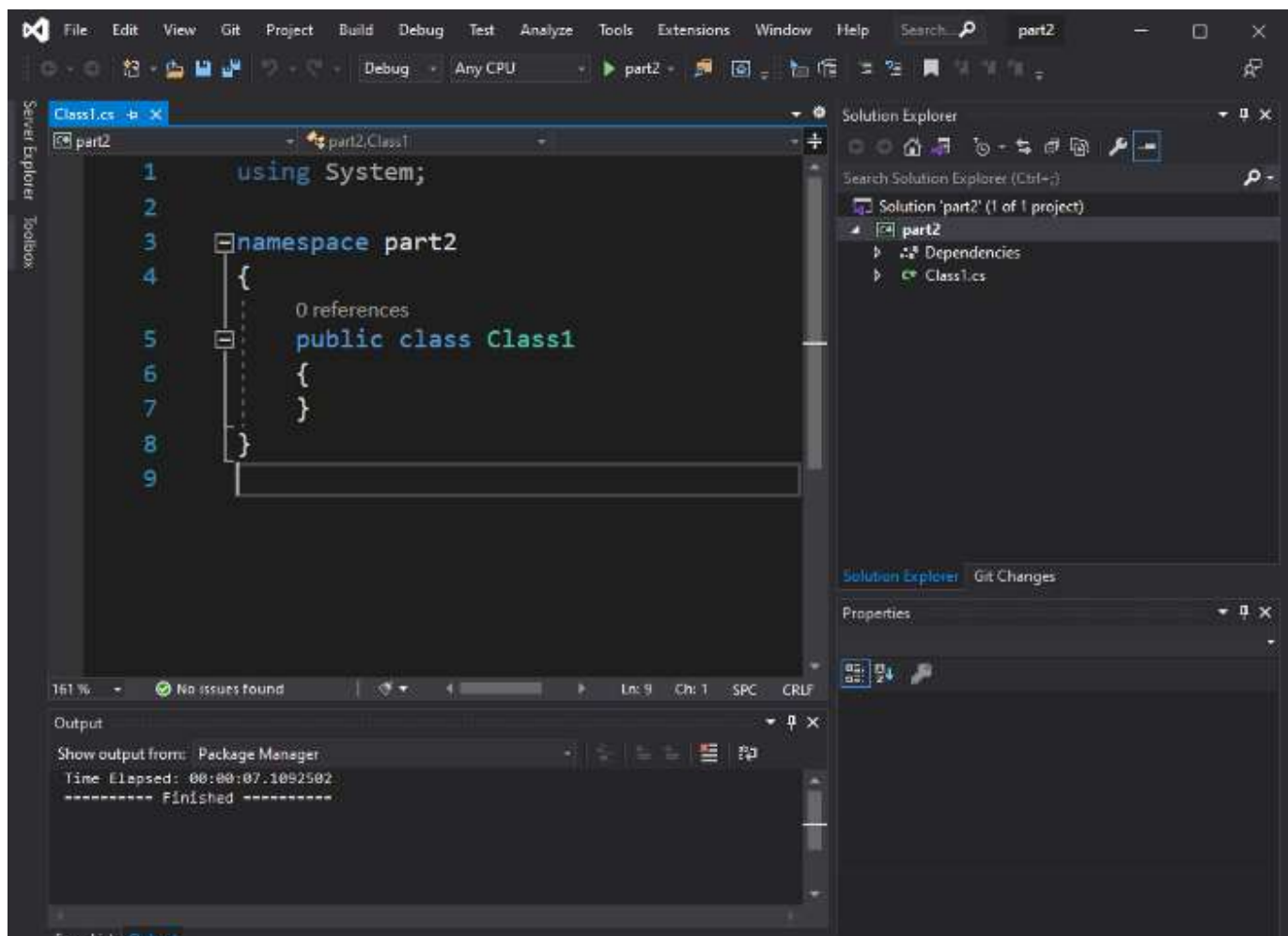
part2

☒ Place solution and project in the same directory

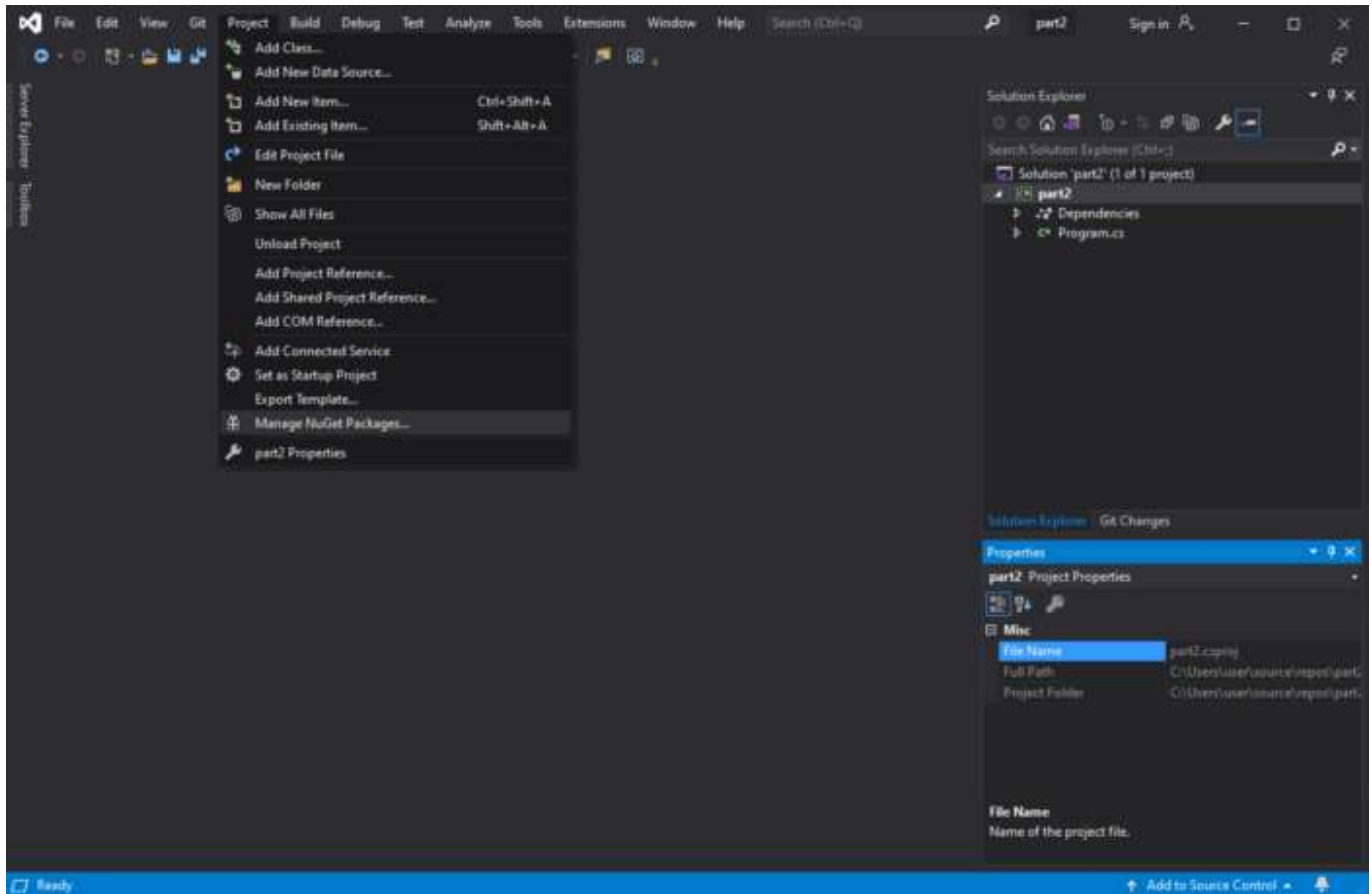
Back Create

Name your project

We are using “part2” as the project name.

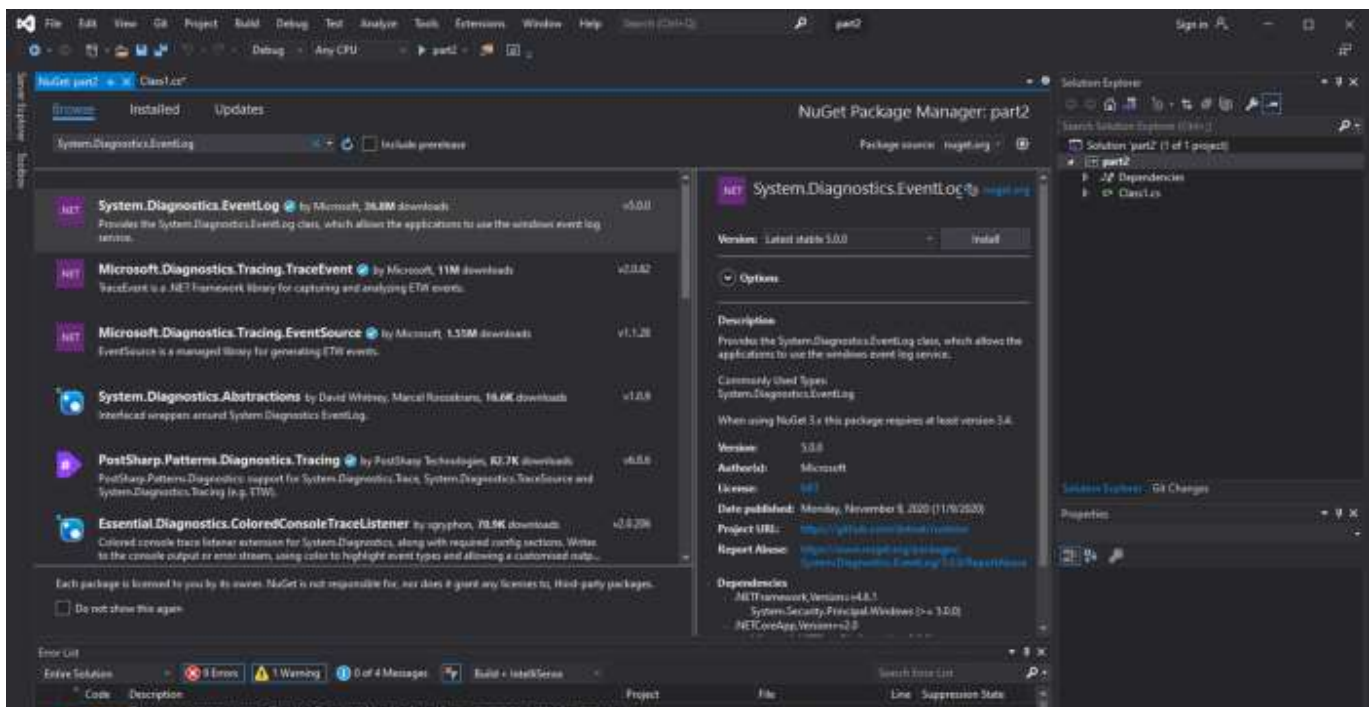




[Get started](#)[Open in app](#)

Install required NuGet Package.

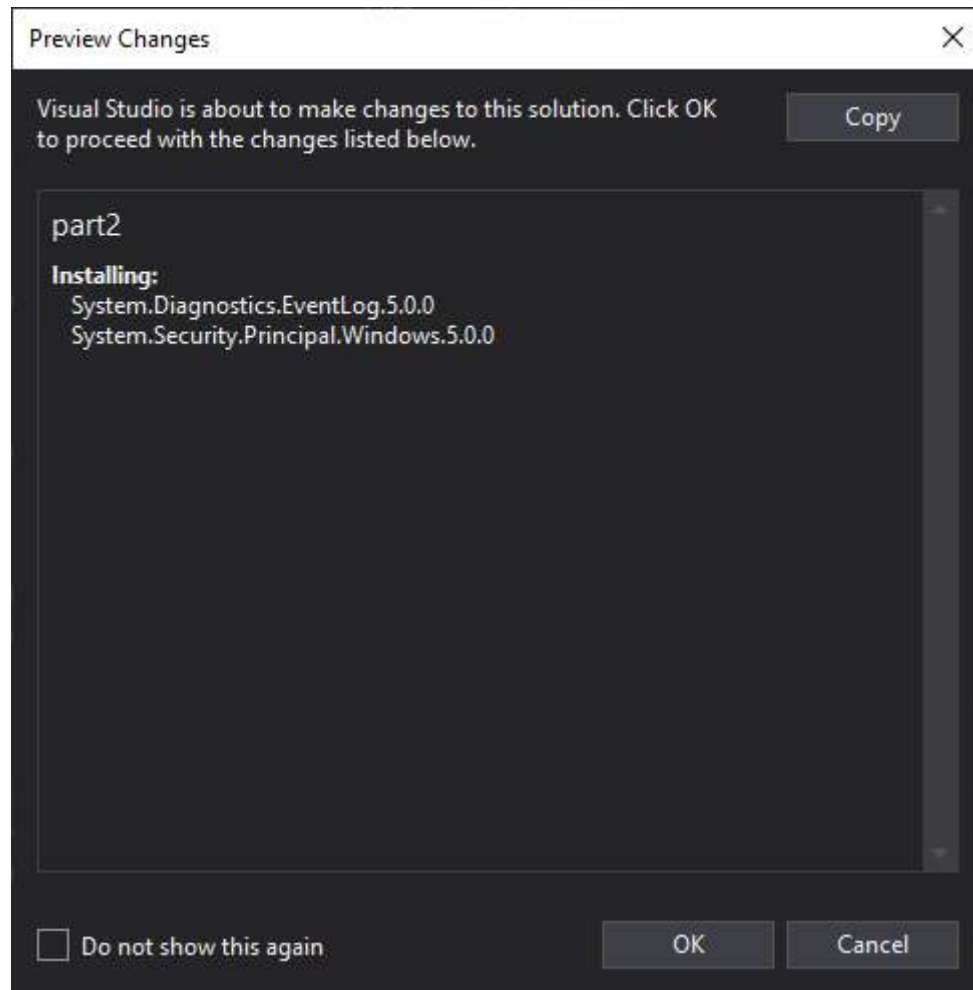
Select “Manage NuGet Packages”.



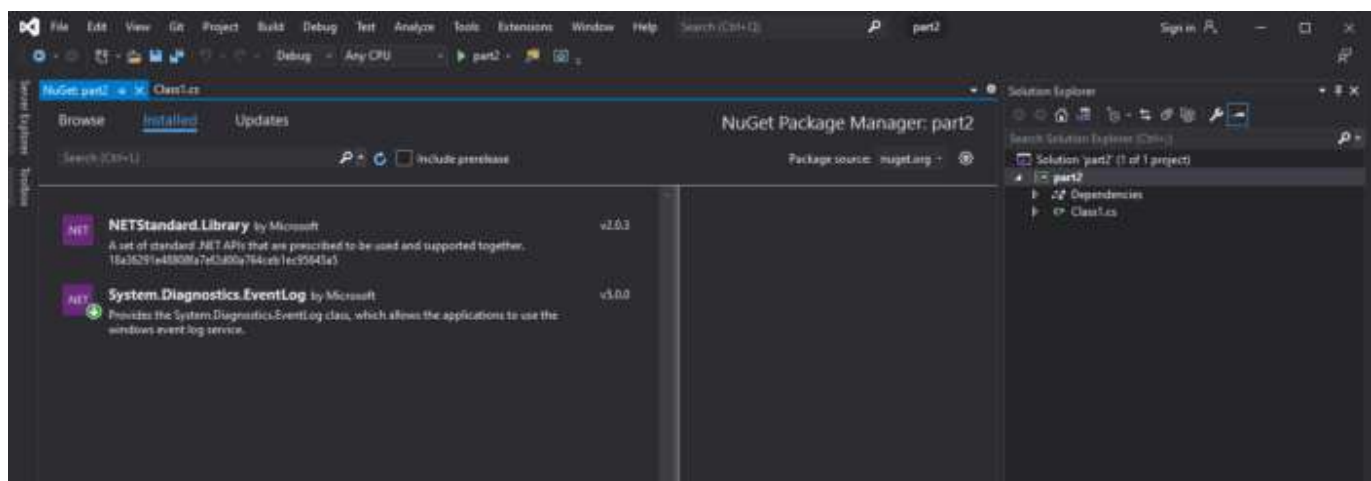
[Get started](#)[Open in app](#)

## Install System.Diagnostics.EventLog

### Install the System.Diagnostics.EventLog NuGet Package

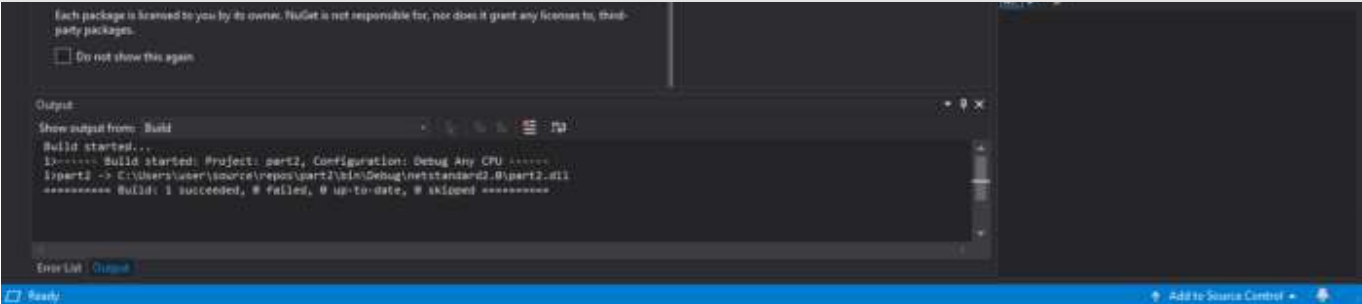


Click OK to install



Get started

Open in app



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

About

Help

Legal

Get the Medium app

