# API SERVICE INSTALLATION DOCUMENT

The following is a description of how to deploy the restful API service in a productive environment:

**Requirements**

* You must have the Internet Information Service installed, if it is not installed it is recommended to read the documentation on the official Microsoft website. <https://learn.microsoft.com/en-us/iis/>
* The restful API service uses the .Net Framework 9.0.1 version so you must have installed the components SDK 9.0.102 for windows x64, ASP.NET Core Runtime 9.0.1 for Windows x64 and Hosting Bundle. <https://dotnet.microsoft.com/en-us/download/dotnet/9.0>

**Configure the Application Pool**

1. Open IIS Manager (inetmgr from Run Win + R).
2. In the left pane, click Application Pools.
3. In the right pane, click Add Application Pool...
4. Assign a name to your pool, for example: HealthcareAPI.
5. Under .NET CLR version, select Unmanaged.
6. Under Managed Pipeline Mode, select Integrated.
7. Click OK.
8. Optional: If you want to change the pool identity, right-click the pool, select Advanced Settings, and under Identity, change to a user with appropriate permissions.

**Adding the Web Site**

1. Copy the “HealthcareAPI IIS Release” folder provided on GitHub into the “[Healthcare\_API](https://github.com/larcila/Healthcare_API/tree/main)/Production/” path and paste it into the physical path C:\inetpub\wwwroot\.
2. Rename folder “HealthcareAPI IIS Release” to “HealthcareAPI”
3. In the left pane of IIS, right click on Sites and select Add Web Site.....
4. Site Name: Type HealthcareAPI.
5. Physical path: Select the folder where you published the API (C:\inetpub\wwwroot\HealthcareAPI).
6. Application Group: Select the HealthcareAPI you created earlier.
7. Host: If you will use a domain, enter it here. For local tests, leave it empty.
8. Port: Use an available port, for example 8084.
9. Protocol: Select http (or https if you have a certificate configured).
10. Click OK.

**Configuring Security on the Publishing Folder**

1. Navigate to the folder where you published the API (C:\inetpub\wwwroot\HealthcareAPI).
2. Right click on the folder and select Properties.
3. Go to the Security tab and click Edit → Add.
4. Type IUSR and press Check Names.
5. Give it Read and Execute permissions.
6. Also add the user IIS\_IUSRS and give it the same permissions.
7. Apply and accept the changes.

**Configure the Firewall to Allow Port**

1. Open Windows Defender Firewall with advanced security.
2. In the left pane, click Inbound Rules.
3. Click New rule... (in the right pane).
4. Select Port and click Next.
5. Select TCP and enter the port number (example: 8084). Make sure it is the same port selected in the pool configuration.
6. Click Next, select Allow connection and finish the configuration.

**Enable CORS if necessary**

1. navigate to the physical path (C:\inetpub\wwwroot\HealthcarecareAPI\appsettings.json)
2. Open the appsettings.json file with your favorite text editor
3. In line 20 you will find “Cors”, and in the option “AllowedOrigins” add the domains to authorize the use of the API.
4. Save changes and close the file.

**Configure the error log path**

1. create a folder with the name “Log” in the path C:
2. navigate to the physical path (C:\inetpub\wwwroot\HealthcarecareAPI\appsettings.json)
3. Open the appsettings.json file with your favorite text editor.
4. In line 9 you will find the “LogFilePath” configuration, verify that you have the path where you created the “Log” folder, if not, change the path where you are going to store the service error capture log.
5. Save changes and close the file.

**Configure the database connection**

1. create a folder with the name “Log” in the path C:
2. navigate to the physical path (C:\inetpub\wwwroot\HealthcarecareAPI\appsettings.json)
3. Open the appsettings.json file with your favorite text editor.
4. In line 13 you will find the “HealthcareConnection” configuration, where the connection string for the database is located.
5. Modify what is highlighted in yellow in the appsetting.json file with the connection data of your environment.

"Server=(localhost);Database=Healthcare;User ID=XXXXX;Password=XXXXX;MultipleActiveResultSets=true;Trust Server Certificate=true"

**IIS: Additional Configuration**

Enable CORS in IIS

1. Open IIS Manager
2. Select the API site
3. In the “Headers” section, add

|  |
| --- |
| Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS  Access-Control-Allow-Headers: Content-Type, Authorization |