

## Symfonia Detal

### Rozwiązywanie problemów

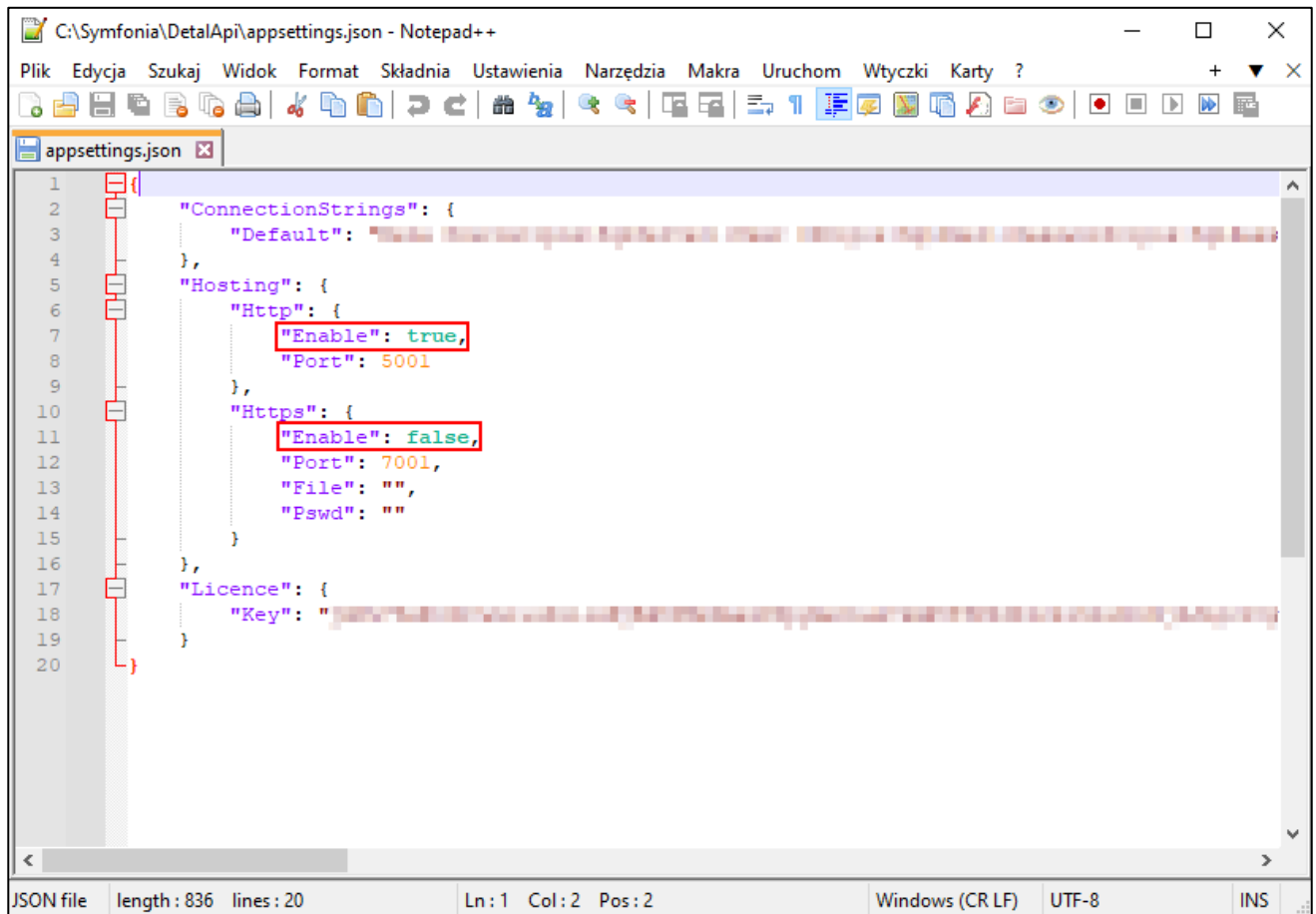
*Producent zastrzega sobie prawo dokonywania w rozwiązaniu zmian i udoskonaleń nieujętych w niniejszej dokumentacji. Wszelkie prawa zastrzeżone. Żadna część tej pracy nie może być powielana, czy rozpowszechniana w jakiegokolwiek formie i jakiegokolwiek sposób (elektroniczny, mechaniczny) włącznie z fotokopiowaniem, nagrywaniem na nośniki magnetyczne, optyczne, magneto-optyczne lub przy użyciu innych systemów, bez pisemnej zgody wydawcy.*

<b>1</b>	<b>Jak zainstalować/odinstalować usługę Symfonia Detal API .....</b>	<b>3</b>
<b>2</b>	<b>Jak zmienić port, na którym działa usługa Symfonia Detal API.....</b>	<b>3</b>
<b>3</b>	<b>Jak zmienić protokół z wykorzystaniem którego uruchamiana jest usługa Symfonia Detal API .....</b>	<b>4</b>
<b>4</b>	<b>Jak dodać porty do reguł zapory sieciowej.....</b>	<b>6</b>
<b>5</b>	<b>Jak utworzyć drugą instancję usługi Symfonia Detal API.....</b>	<b>13</b>



### 3 Jak zmienić protokół z wykorzystaniem którego uruchamiana jest usługa Symfonia Detal API

W celu zmiany protokołu należy otworzyć plik *appsettings.json*, a następnie wpisać „true” przy protokole, z wykorzystaniem którego ma być uruchamiana usługa. Konieczne jest także uzupełnienie numeru portu.



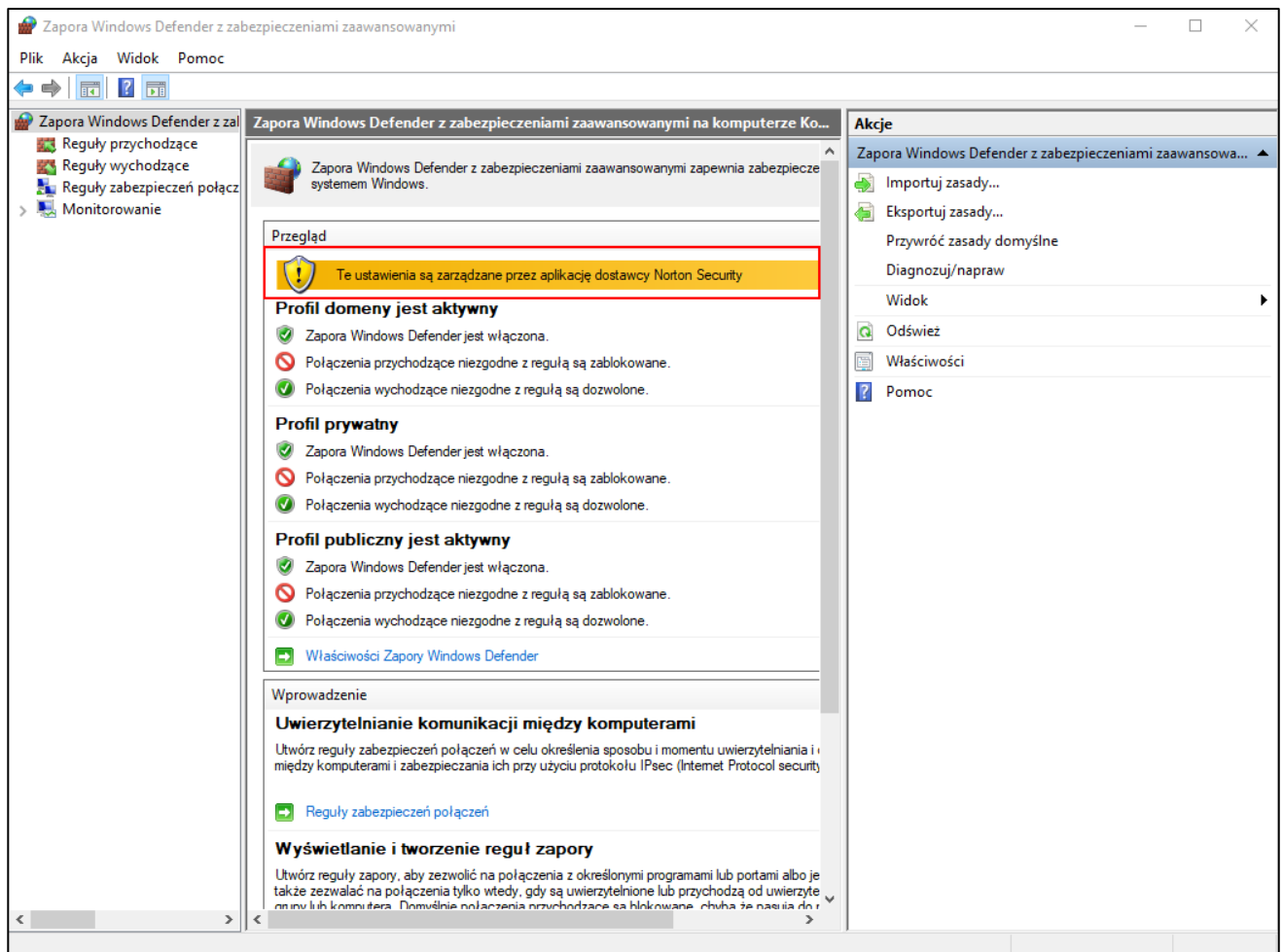
```
1  {
2      "ConnectionStrings": {
3          "Default": "..."
4      },
5      "Hosting": {
6          "Http": {
7              "Enable": true,
8              "Port": 5001
9          },
10         "Https": {
11             "Enable": false,
12             "Port": 7001,
13             "File": "",
14             "Pswd": ""
15         }
16     },
17     "Licence": {
18         "Key": "..."
19     }
20 }
```

JSON file length: 836 lines: 20 Ln: 1 Col: 2 Pos: 2 Windows (CR LF) UTF-8 INS



## 4 Jak dodać porty do reguł zapory sieciowej

W celu dodania portów do reguł należy uruchomić aplikację **Zapora Windows Defender z zabezpieczeniami zaawansowanymi**. W przypadku, gdy na urządzeniu zainstalowane jest oprogramowanie antywirusowe firmy trzeciej wyświetli się odpowiednia informacja, wtedy nowe porty powinny zostać dodane w sposób odpowiedni dla używanego oprogramowania antywirusowego.





Wyświetli się okno kreatora, należy wybrać opcję **Port** i przejść **Dalej**.



W kolejnym kroku należy wybrać protokół TCP oraz określony numer portu.

Kreator nowej reguły ruchu przychodzącego

### Protokół i porty

Określ protokoły i porty, których dotyczy ta reguła.

**Kroki:**

- Typ reguły
- Protokół i porty**
- Akcja
- Profil
- Nazwa

Czy ta reguła dotyczy protokołu TCP, czy UDP?

TCP  
 UDP

Czy ta reguła dotyczy wszystkich portów lokalnych, czy określonych portów lokalnych?

Wszystkie porty lokalne  
 Określone porty lokalne:

Przykład: 80, 443, 5000-5010

< Wstecz **Dalej >** Anuluj

W następnym oknie należy zezwolić na połączenie.

Kreator nowej reguły ruchu przychodzącego

### Akcja

Określ akcję do wykonania w przypadku, gdy połączenie spełnia warunki określone w regule.

**Kroki:**

- Typ reguły
- Protokół i porty
- Akcja**
- Profil
- Nazwa

Jaką akcję należy wykonać, gdy połączenie spełnia określone warunki?

- Zezwalaj na połączenie**  
Obejmuje połączenia chronione za pomocą protokołu IPsec, jak i połączenia niechronione.
- Zezwalaj na połączenie, jeśli jest bezpieczne**  
Obejmuje tylko połączenia uwierzytelnione przy użyciu protokołu IPsec. Połączenia będą zabezpieczone przy użyciu ustawień określonych we właściwościach protokołu IPsec i reguł zawartych w węźle Reguła zabezpieczeń połączenia.
- Zablokuj połączenie**

< Wstecz   **Dalej >**   Anuluj

Następnie konieczne jest określenie, kiedy reguła ma mieć zastosowanie.

Kreator nowej reguły ruchu przychodzącego

### Profil

Określ profile, których dotyczy ta reguła.

**Kroki:**

- Typ reguły
- Protokół i porty
- Akcja
- Profil**
- Nazwa

Kiedy ma zastosowanie ta reguła?

- Domena**  
Ma zastosowanie, gdy komputer jest połączony ze swoją domeną firmową.
- Prywatny**  
Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci prywatnej, na przykład w domu lub w miejscu pracy.
- Publiczny**  
Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci publicznej.

< Wstecz   **Dalej >**   Anuluj

W ostatnim kroku należy nadać nazwę nowej regule i zatwierdzić przyciskiem **Zakończ**.

Kreator nowej reguły ruchu przychodzącego

### Nazwa

Określ nazwę i opis tej reguły.

**Kroki:**

- Typ reguły
- Protokół i porty
- Akcja
- Profil
- Nazwa**

Nazwa:

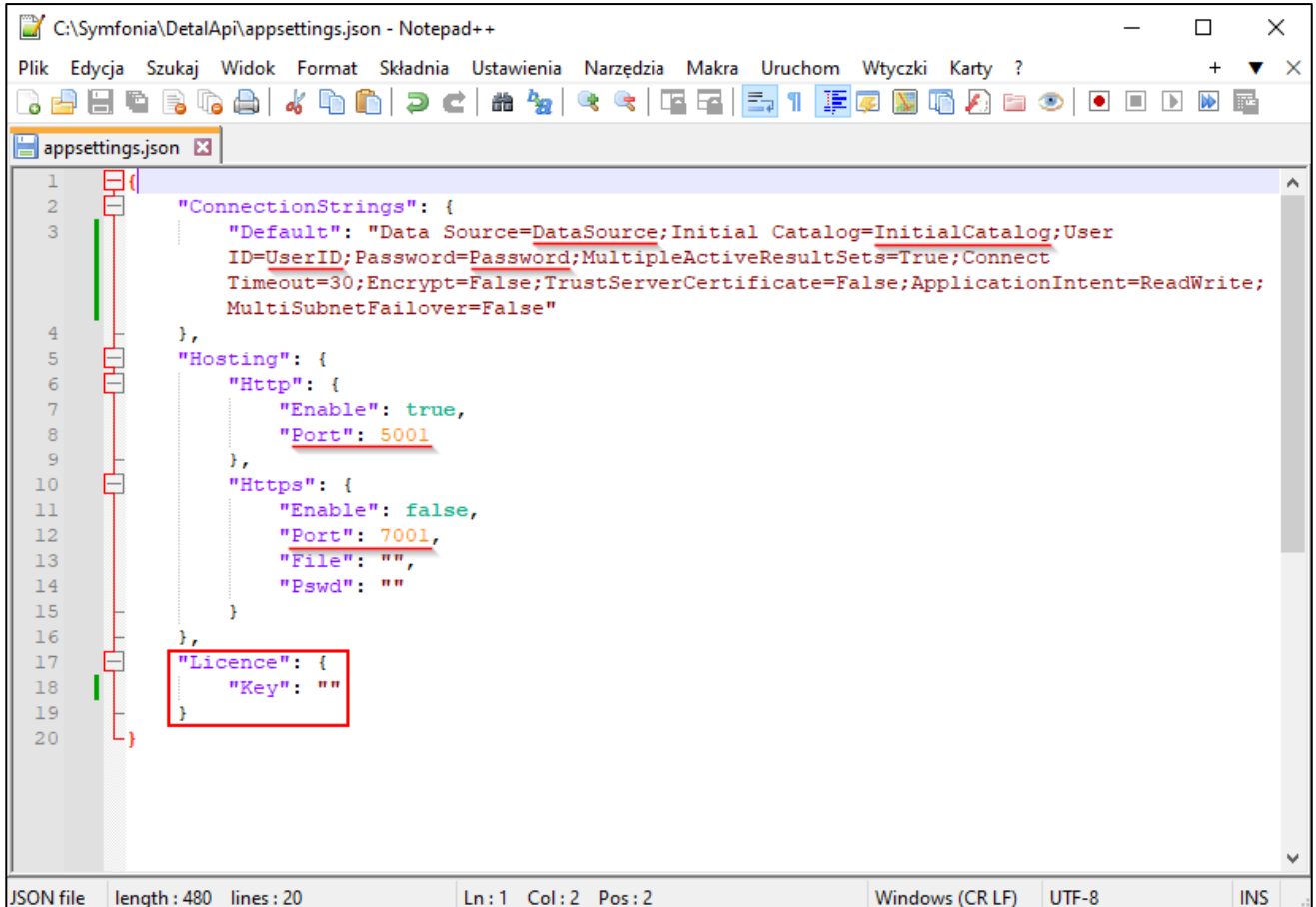
Opis (opcjonalnie):

< Wstecz **Zakończ** Anuluj

## 5 Jak utworzyć drugą instancję usługi Symfonia Detal API

Aby utworzyć drugą instancję usługi, gdzie podpięta będzie inna baza, należy w pierwszej kolejności skopiować folder z plikami WebAPI oraz Symfonia Detal API.

Następnie należy otworzyć plik *appsettings.json* i zmienić konfigurację dotyczącą bazy (nazwa serwera, nazwa bazy danych, użytkownik i hasło), numery portów oraz klucz licencji.



```
1 {
2   "ConnectionStrings": {
3     "Default": "Data Source=DataSource;Initial Catalog=InitialCatalog;User
4     ID=UserID;Password=Password;MultipleActiveResultSets=True;Connect
5     Timeout=30;Encrypt=False;TrustServerCertificate=False;ApplicationIntent=ReadWrite;
6     MultiSubnetFailover=False"
7   },
8   "Hosting": {
9     "Http": {
10      "Enable": true,
11      "Port": 5001
12    },
13    "Https": {
14      "Enable": false,
15      "Port": 7001,
16      "File": "",
17      "Pswd": ""
18    }
19  },
20  "Licence": {
21    "Key": ""
22  }
23 }
```

Kolejnym krokiem jest instalacja usługi za pomocą skryptu dostępnego w rozdziale 1 *Jak zainstalować/odinstalować usługę Symfonia Detal API*.

Na koniec konieczne jest dodanie nowych portów do reguł zapory sieciowej. W tym celu należy postępować zgodnie z instrukcją opisaną w rozdziale 4 *Jak dodać porty do reguł zapory sieciowej*.



W celu przeprowadzenia aktualizacji Symfonia Detal API należy pamiętać o konieczności ponownego wykonania powyższych kroków.