

Odblokowanie portów zapory systemu Windows dla poprawnego działania programu Comotel:

1. Wchodzimy do folderu (* w zależności od systemu, folder może wyglądać inaczej):

C:\Program Files\Microsoft SQL Server\MSSQL\$CALISIA\LOG
C:\Program Files (x86)\Microsoft SQL Server\MSSQL\$CALISIA\LOG

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG
C:\Program Files (x86)\Microsoft SQL Server\MSSQL.1\MSSQL\LOG

2. Za pomocą edytora tekstu, np. notatnika, otwieramy plik o nazwie „errorlog” i szukamy wiersza:

```
2016-04-25 08:09:10.51 Server Server is listening on [ 'any' <ipv4> 53199].
```

Jeśli nie znajdziemy tej linijki w pliku może to oznaczać, że protokół TCP/IP jest wyłączony. Należy wejść w narzędzie SQL Configuration Manager i dla naszej instancji ustawić ten protokół na 'Enabled'

3. Zapisujemy numer portu (w tym przypadku **53199**).
4. Przechodzimy do panelu sterowania, otwieramy „Zapora systemu Windows”

← → ▾ ↑ 🏠 > Panel sterowania > Wszystkie elementy Panelu sterowania > Zapora Windows Defender

Chroń swój komputer za pomocą Zapory Windows Defender

Zapora Windows Defender utrudnia hakerom lub złośliwemu oprogramowaniu uzyskanie dostępu do tego komputera za pośrednictwem Internetu lub sieci.

Sieci prywatne Połączono	
Sieci w domu lub w miejscu pracy, w których użytkownik zna ludzi i urządzenia, a także im ufa	
Stan Zapory Windows Defender:	Wł.
Połączenia przychodzące:	Blokuj wszystkie połączenia z aplikacjami, których nie ma na liście dozwolonych aplikacji
Aktywne sieci prywatne:	Sieć
Stan powiadamiania:	Powiadamij mnie, gdy Zapora Windows Defender zablokuje nową aplikację

Sieci publiczne Brak połączenia	
---	--

Wybieramy 'Ustawienia zaawansowane' i dodajemy nowe reguły przychodzące/wychodzące, np.

TCP:

139, 445, 1433

+ zapisany wcześniej numer

UDP:

137, 138, 1434