

Konfiguracja komunikacji OPC UA z AVEVA System Platform jako serwerem OPC UA

Informator Techniczny AVEVA nr 189

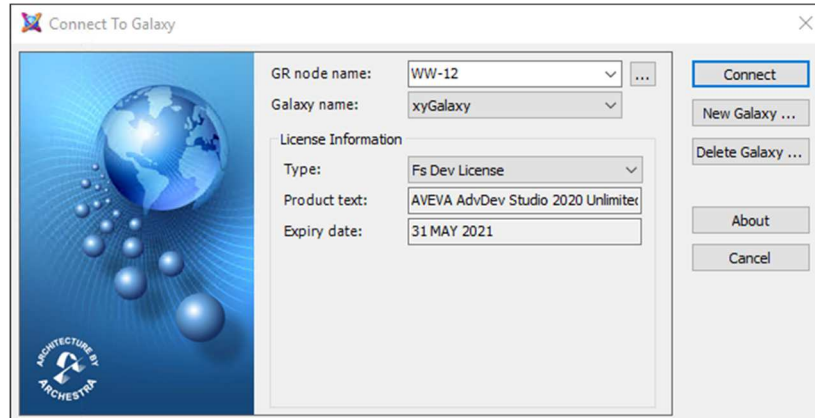
27-05-2021

Aplikacja Platformy Systemowej od wersji 2020 R2 umożliwia udostępniania danych po protokole OPC UA jako serwer OPC UA. Poniżej zostały opisane dwa sposoby konfiguracji połączenia do aplikacji Platformy Systemowej po OPC UA: bez skonfigurowanych zabezpieczeń oraz z zabezpieczeniami z wykorzystaniem certyfikatów.

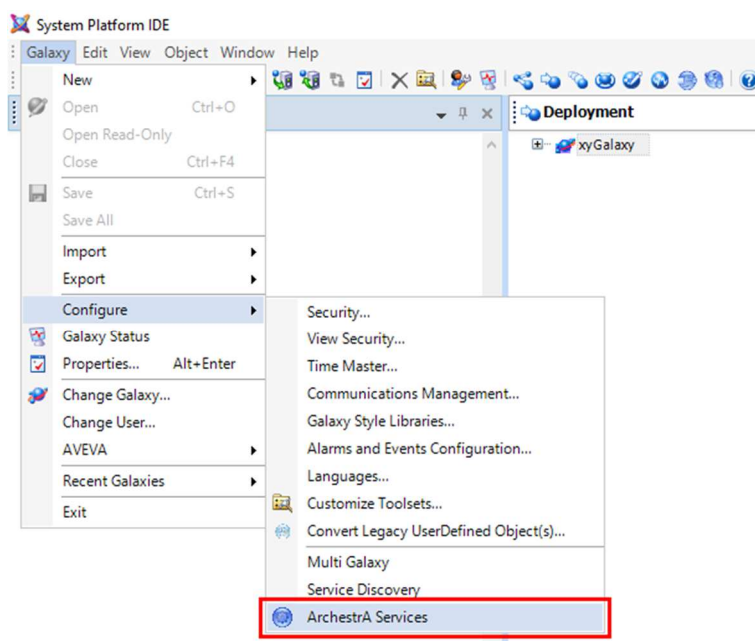
KONFIGURACJA KOMUNIKACJI KLIENTA OPC UA DO AVEVA SYSTEM PLATFORM JAKO SERWERA OPC UA BEZ SKONFIGUROWANYCH ZABEZPIECZEŃ

1. Konfiguracja i uruchamianie serwera OPC UA w programie System Platform IDE

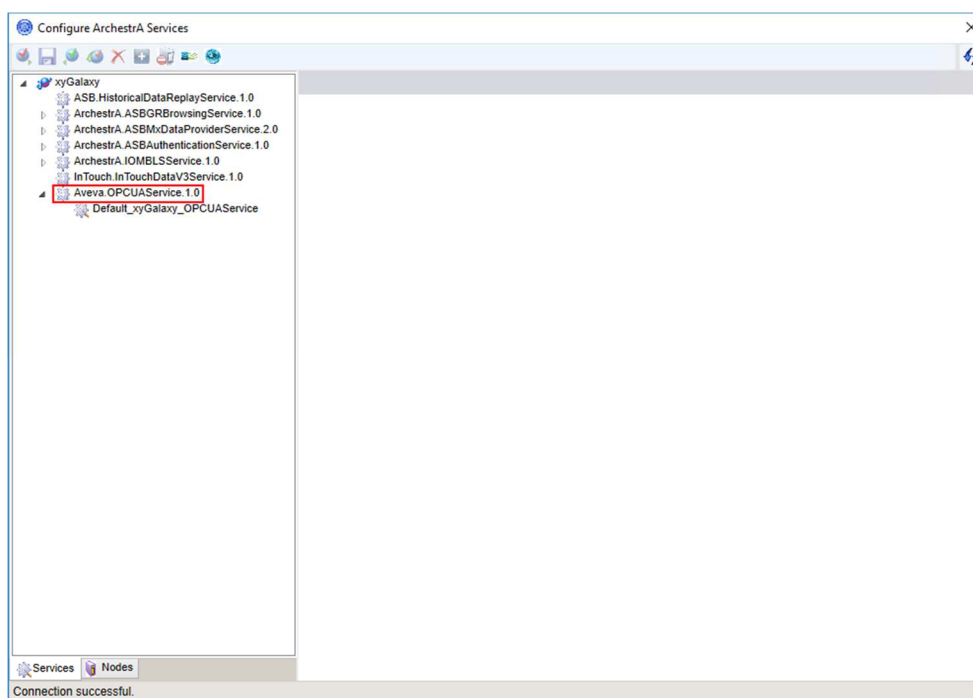
Z grupy programów **AVEVA System Platform** należy uruchomić program **System Platform IDE**.



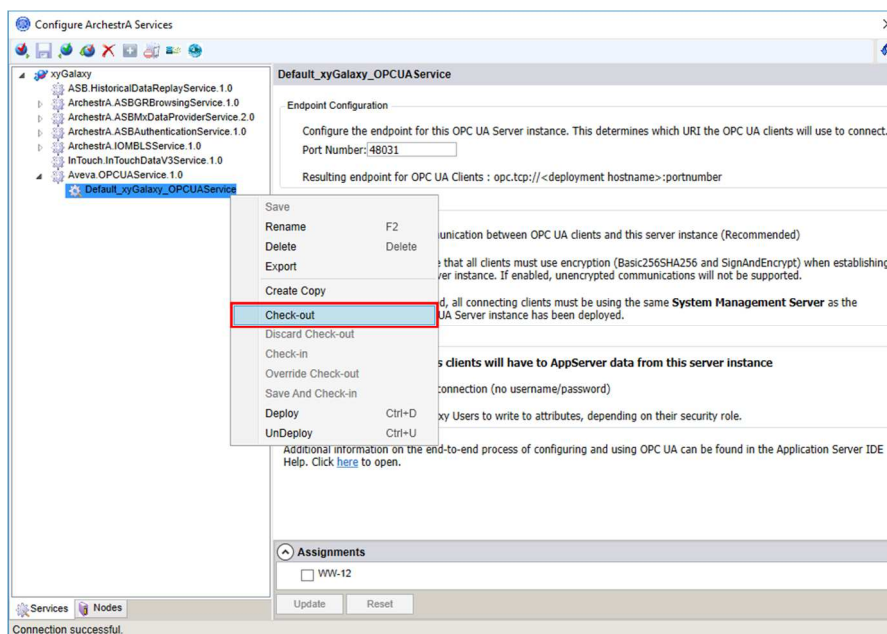
Pojawi się okno **Connect To Galaxy**, w którym należy połączyć się projektu, w którym ma zostać skonfigurowane udostępnianie danych po protokole OPC UA.



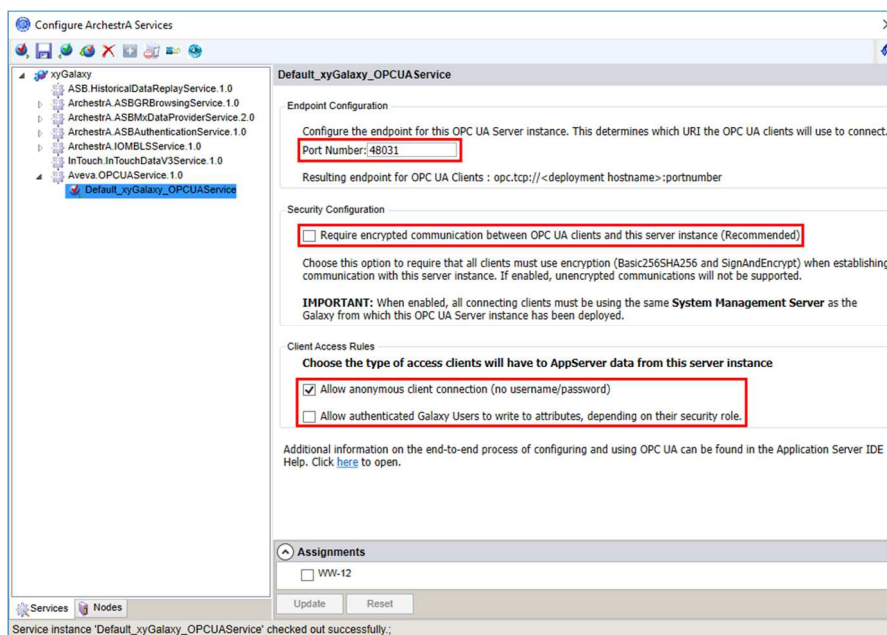
W programie **System Platform IDE** z menu należy wybrać **Galaxy**, następnie **Configure** i **Archestra Services**.



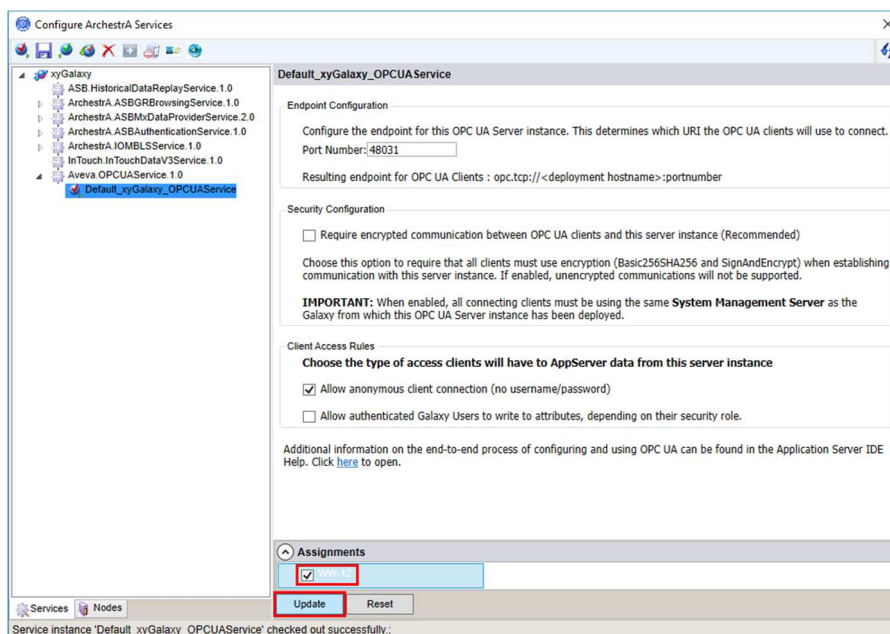
W oknie **Configure Archestra Services** należy rozwinąć listę serwisów dla wybranego projektu aplikacji, a następnie rozwinąć opcję **Aveva.OPCUAService.1.0**.



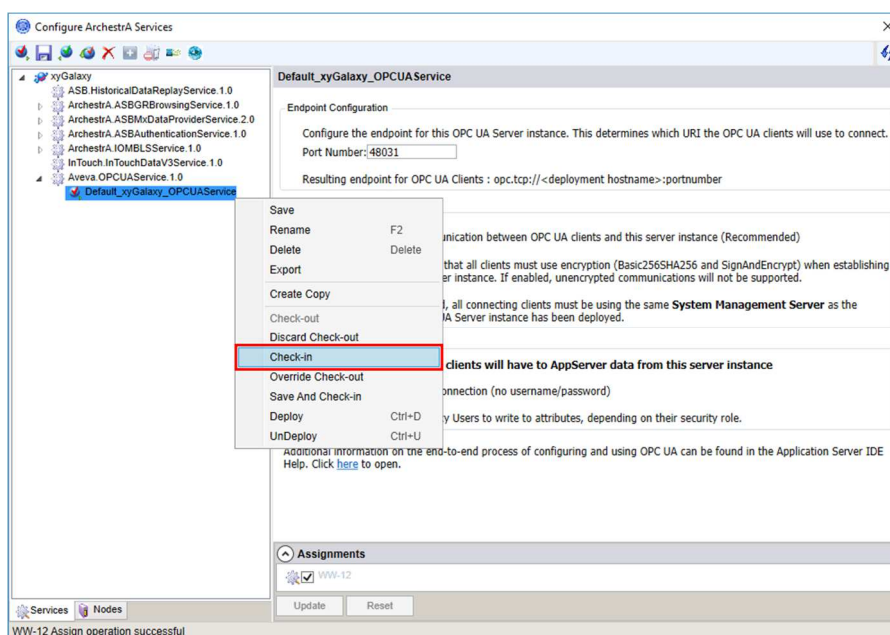
W kolejnym kroku należy kliknąć prawym przyciskiem myszy na serwis o nazwie **Default_<nazwa projektu>_OPCUAService** i wybrać opcję **Check-out**.



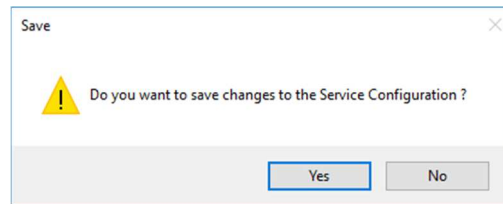
W oknie **Default_<nazwa projektu>_OPCUAService** w pierwszej kolejności należy skonfigurować **Port Number**. Domyślnie port jest ustawiony na **48031**. Następnie należy odznaczyć opcję **Require encrypted communication between OPC UA clients and this server instance (Recommended)**, zaznaczyć **Allow anonymous client connection (no username/password)** i odznaczyć **Allow authenticated Galaxy Users to write to attributes, depending on their security role**.



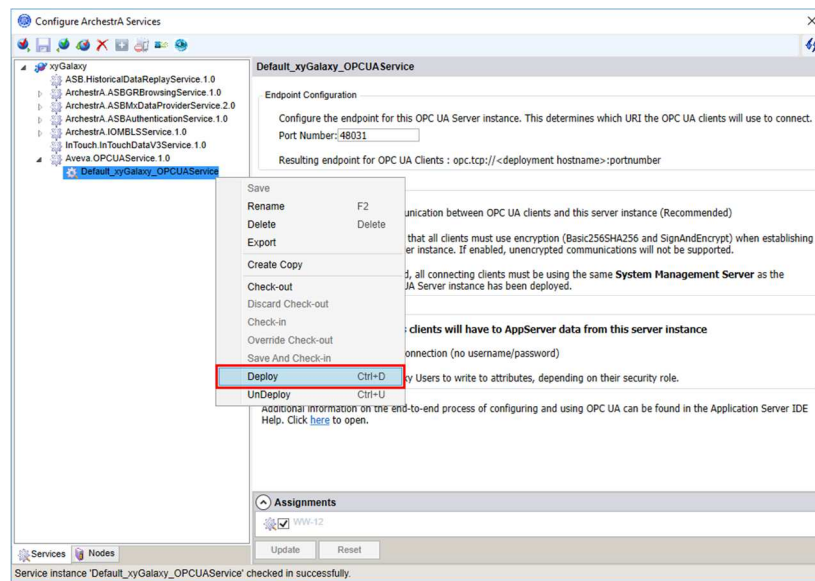
U dołu w oknie **Assignments** pokazane są komputery dostępne w platformie, na których możliwe jest uruchomienie skonfigurowanego serwisu OPC UA Service. Należy zaznaczyć komputer, na którym ma zostać uruchomiony serwis i kliknąć **Update**.



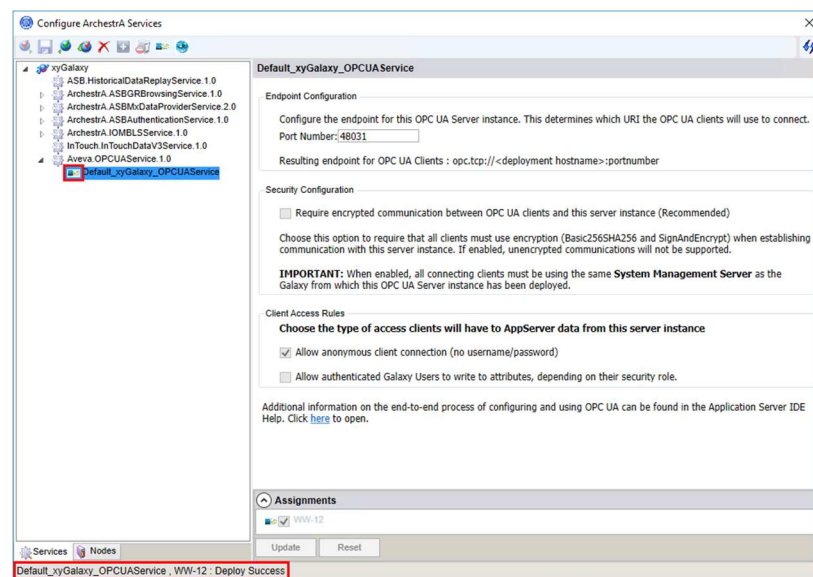
W oknie po lewej stronie należy kliknąć prawym przyciskiem myszy na serwis o nazwie **Default_<nazwa projektu>_OPCUAService** i wybrać opcję **Check-in**.



Pojawi się komunikat **Do you want to save changes to the Service Configuration?** Należy nacisnąć przycisk **Yes**.



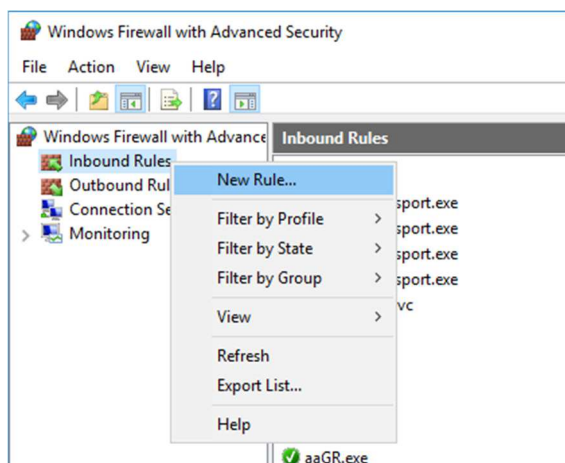
W oknie po lewej stronie należy kliknąć prawym przyciskiem myszy na serwis o nazwie **Default_<nazwa projektu>_OPCUAService** i wybrać opcję **Deploy**.



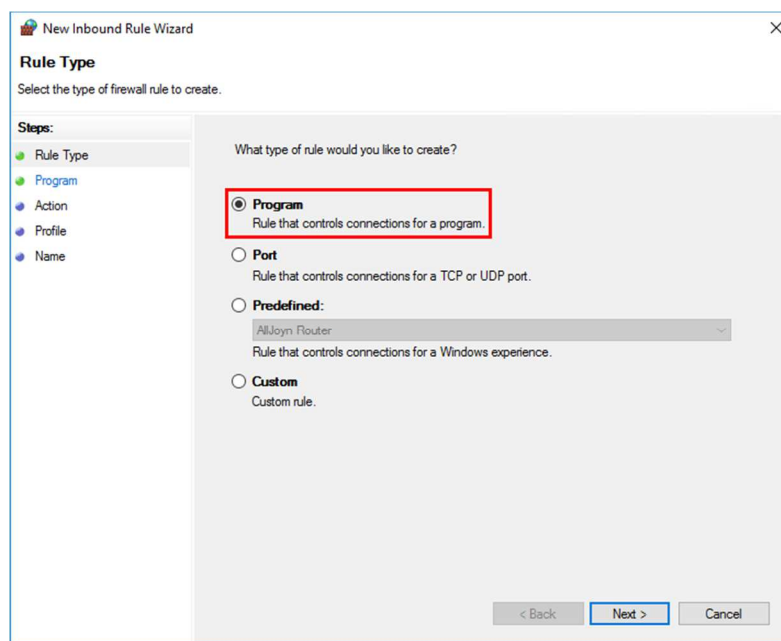
Po uruchomieniu, po lewej stronie nazwy serwisu pojawi się ikona , a u dołu okna pojawi się komunikat **Default_<nazwa projektu>_OPCUAService, <nazwa komputera>: Deploy Success**.

2. Konfiguracja reguły w zaporze Windows na komputerze z uruchomionym serwisem OPC UA Service

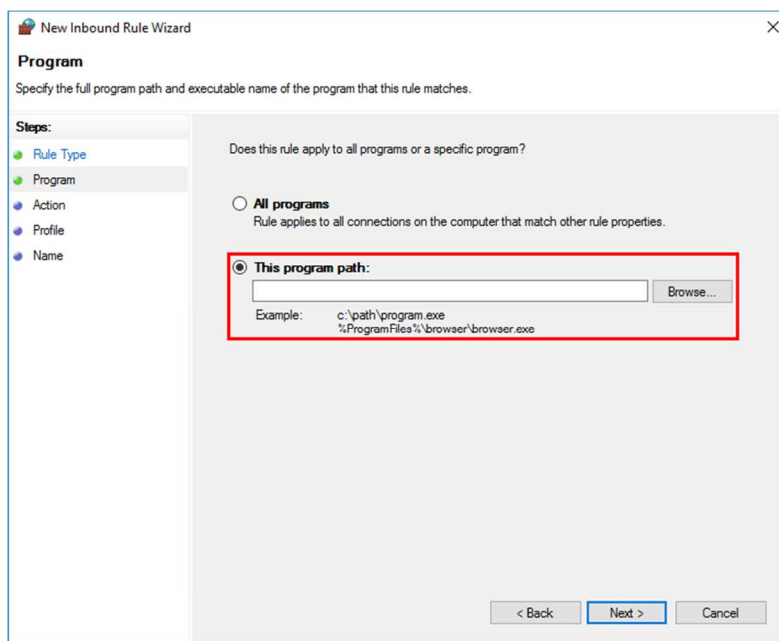
Konfigurację reguły w zaporze Windows należy wykonać na komputerze, na którym został uruchomiony serwis OPC UA Service. Jest to niezbędne, aby aplikacja kliencka OPC UA mogła nawiązać prawidłowe połączenie z serwerem OPC UA.



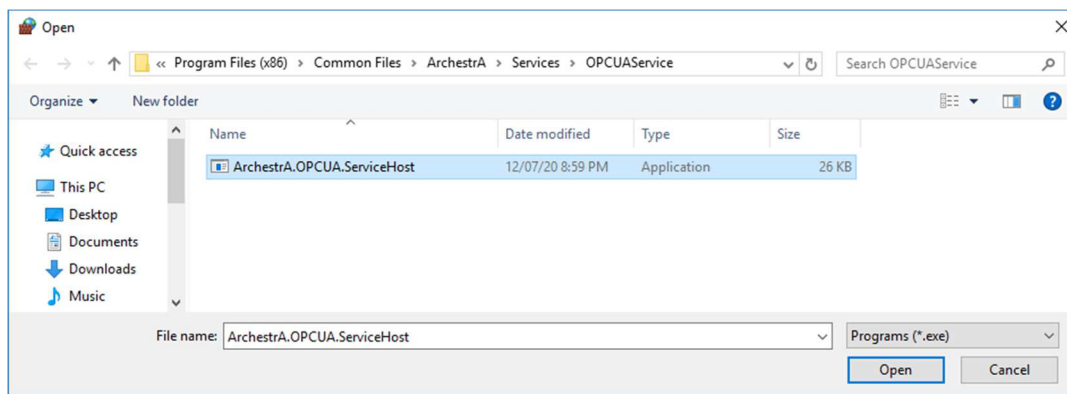
W systemie Windows należy uruchomić **Administrative Tools (Narzędzia administracyjne systemu Windows)**, a następnie program **Windows Firewall with Advanced Security (Zapora Windows Defender z narzędziami zaawansowanymi)**. Po uruchomieniu programu należy zaznaczyć **Inbound Rules (Reguły przychodzące)**, kliknąć prawym przyciskiem myszy i wybrać opcję **New Rule (Nowa reguła)**.



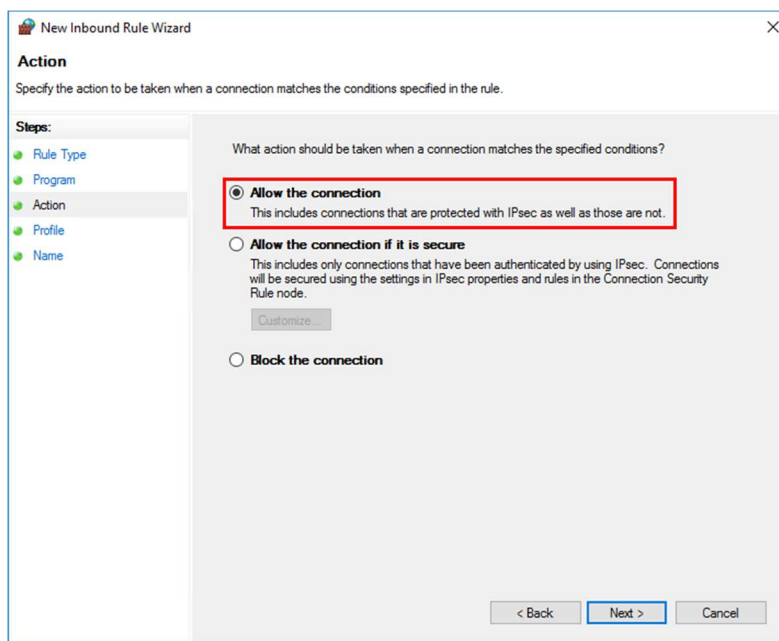
W oknie **Rule Type (Typ reguły)**, należy zaznaczyć **Program** i nacisnąć przycisk **Next**.



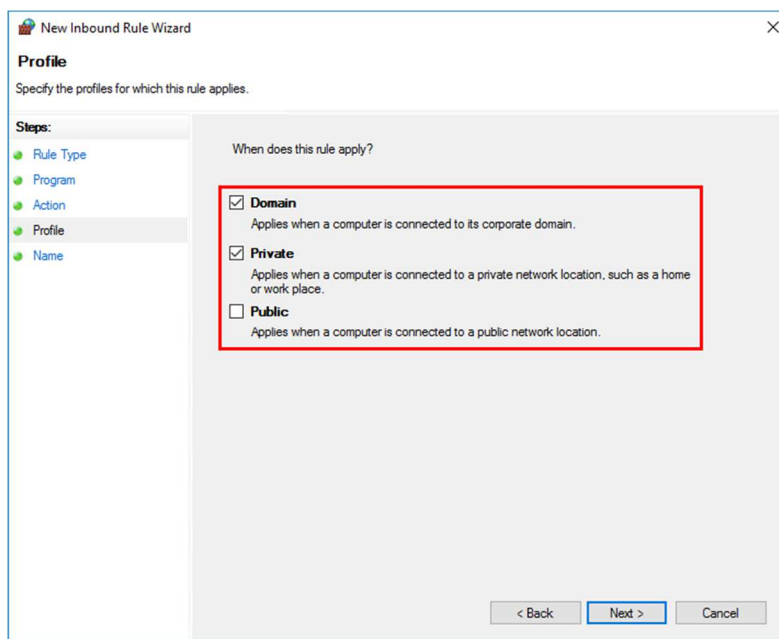
W kolejnym oknie należy zaznaczyć opcję **This program path** i wyszukać lokalizację serwisu OPC UA Server Service. W tym celu należy nacisnąć przycisk **Browse** znajdujący się po prawej stronie pola **This program path**. Jeśli Platforma Systemowa zainstalowana była w domyślnej lokalizacji, ścieżka dostępu wygląda następująco: **C:\Program Files (x86)\Common Files\Archestra\Services\OPCUAService**.



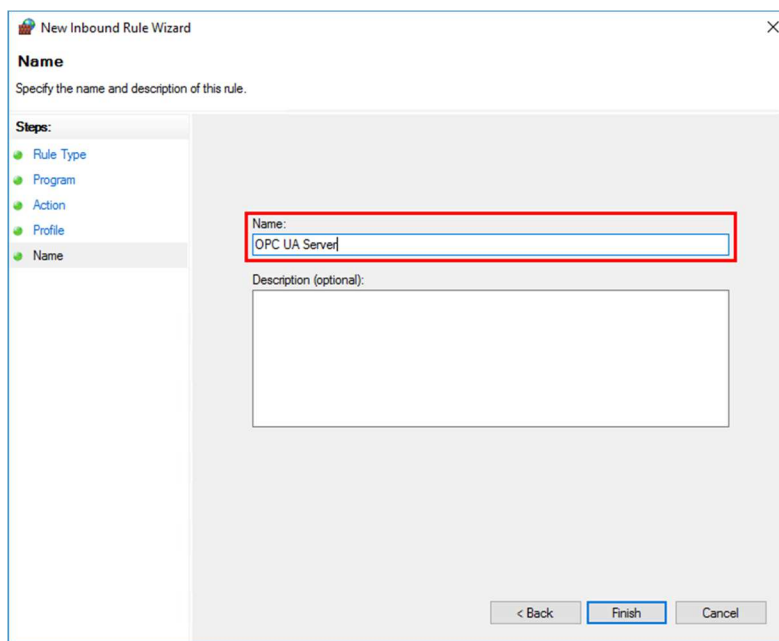
W następnym kroku należy wybrać **Archestra.OPCUA.ServiceHost.exe** i nacisnąć przycisk **Open**. Następnie należy nacisnąć przycisk **Next**, aby przejść do następnego okna.



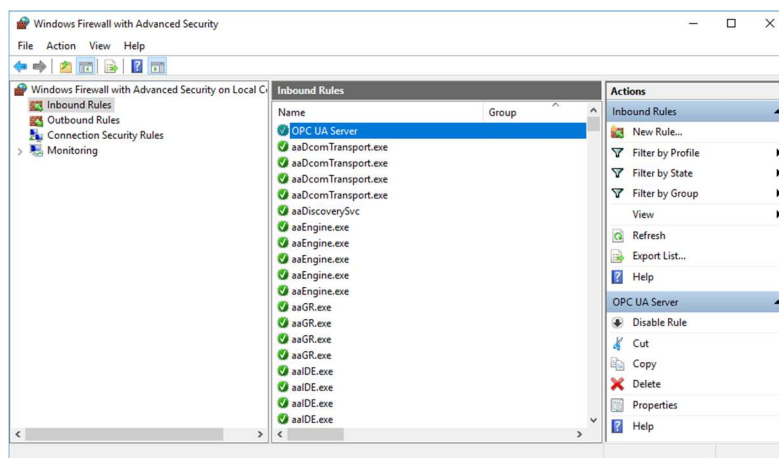
W następnym oknie należy zaznaczyć opcję **Allow the connection** i nacisnąć przycisk **Next**.



W kolejnym oknie należy zaznaczyć opcje **Domain** oraz **Private**, a odznaczyć opcję **Public** i nacisnąć przycisk **Next**.



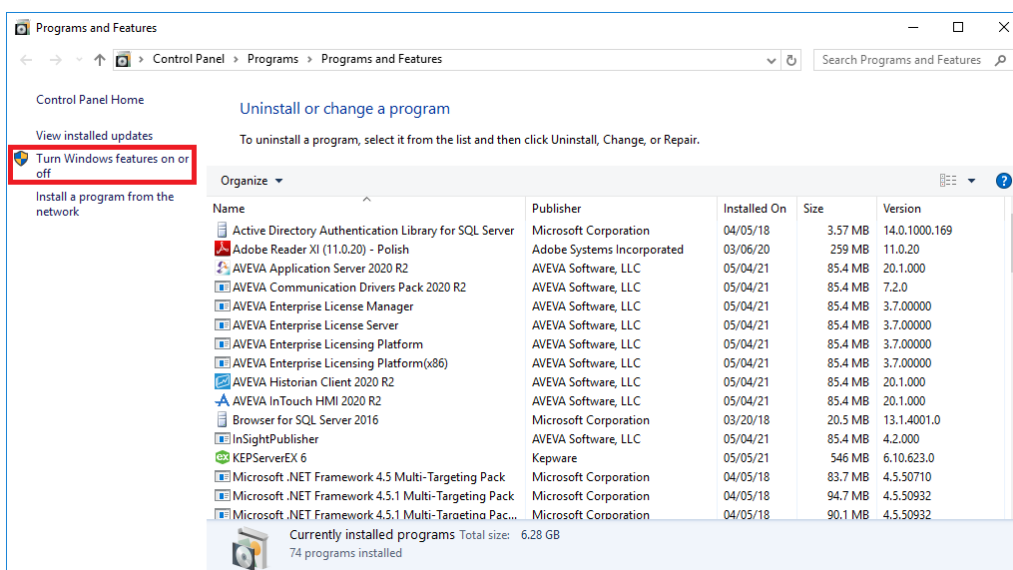
Następnie w polu **Name** należy wpisać nazwę dla zdefiniowanej reguły np. **OPC UA Server** i nacisnąć przycisk **Finish**.



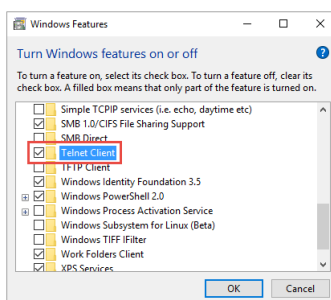
Skonfigurowana reguła pojawi się na liście reguł.

3. Sprawdzenie na komputerze z aplikacją kliencką OPC UA możliwości połączenia z serwerem OPC UA uruchomionego przez serwis OPC UA Service

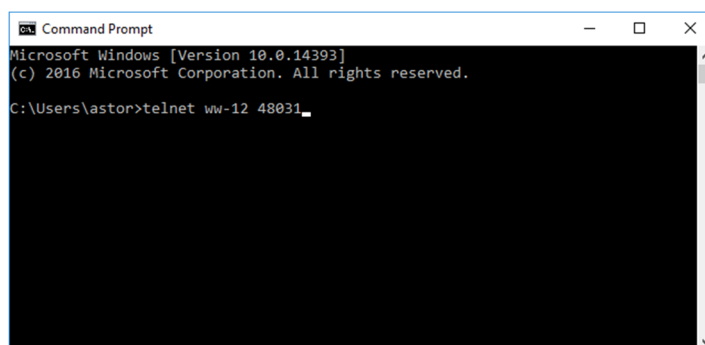
Po skonfigurowaniu reguły w zaporze Windows należy sprawdzić, czy jest możliwa komunikacja przez port, który wykorzystuje serwis OPC UA Service. Test połączenia należy wykonać na komputerze z aplikacją kliencką OPC UA, która ma zostać skonfigurowana do połączenia z serwerem OPC UA.



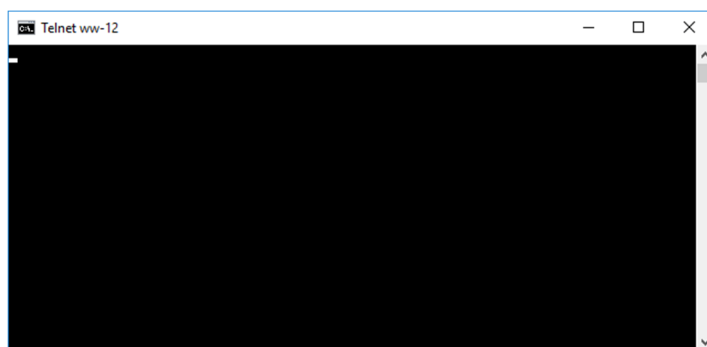
W tym celu w systemie Windows należy wejść do **Add or remove programs (Dodaj lub usuń programy)**, a następnie kliknąć **Programs and features (Programy i funkcje)** i wybrać **Turn Windows features on or off (Włącz lub wyłącz funkcje systemu Windows)**.



Spośród dostępnych funkcji należy zaznaczyć **Telnet Client (Klient Telnet)** i nacisnąć **OK**, aby zainstalować w systemie Windows tę funkcję.



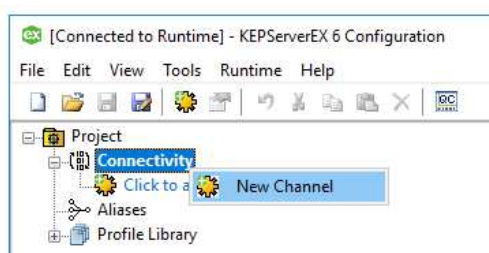
W kolejnym kroku w systemie Windows należy uruchomić linię komend i wpisać polecenie **telnet nazwa_komputera lub adres_IP nr_portu_serwera_OPC_UA** i nacisnąć Enter np. **telnet WW-12 48031**



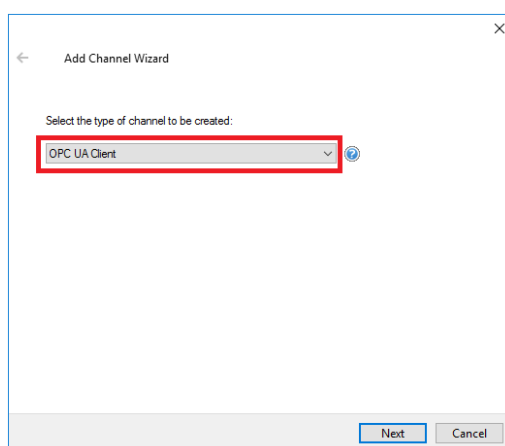
Jako wynik pojawi się kursor w lewym górnym rogu, który jest potwierdzeniem, że port jest dostępny w systemie Windows do komunikacji.

4. Konfiguracja połączenia programu klienckiego OPC UA na przykładzie programu KEPServerEX

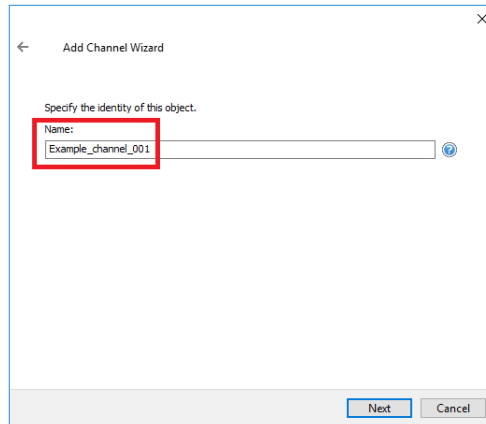
Po zainstalowaniu oprogramowania **KEPServerEX** należy uruchomić program **KEPServerEX 6 Configuration**.



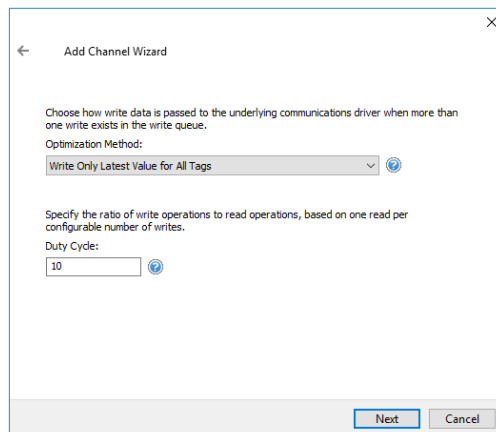
Następnie należy kliknąć prawym przyciskiem myszy na **Connectivity** i wybrać opcję **New Channel**.



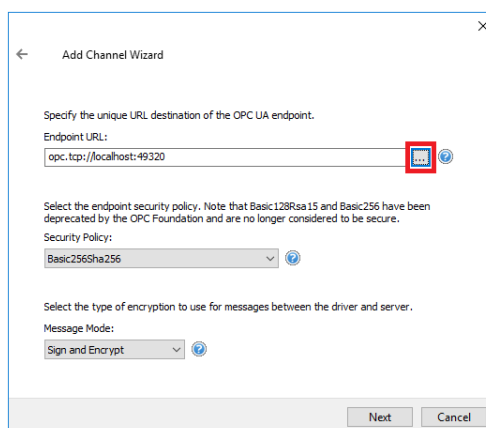
W oknie **Add Channel Wizard** z rozwijanego menu należy wybrać opcję **OPC UA Client** i nacisnąć przycisk **Next**.




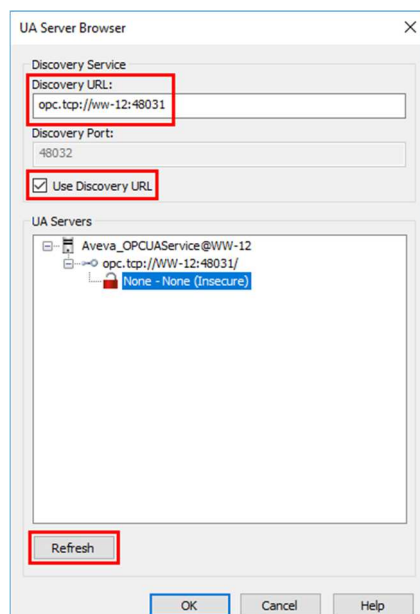
W następnym oknie w polu **Name** należy wpisać nazwę dla tworzonego kanału i nacisnąć przycisk **Next**.



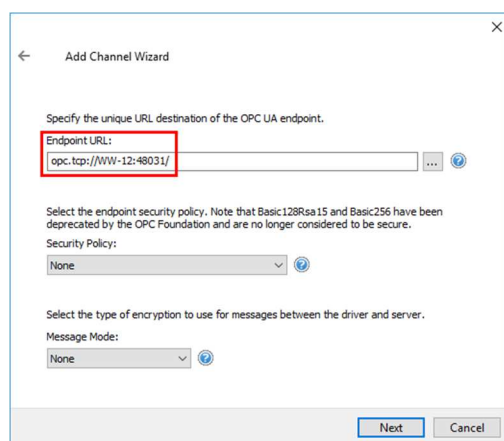
W kolejnym oknie należy nacisnąć przycisk **Next**.



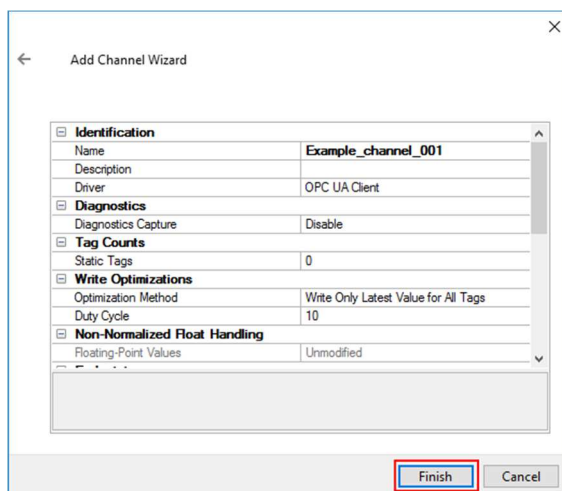
W następnym oknie należy kliknąć na ikonę  znajdującą się po prawej stronie pola **Endpoint URL**.



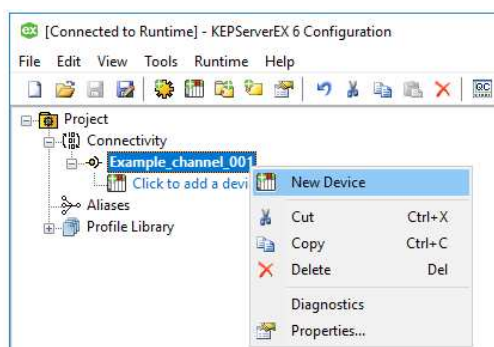
Pojawi się okno **UA Server Browser**. W oknie **UA Servers** należy zaznaczyć **Use Discovery URL** i w polu **Discovery URL**: należy wpisać adres w postaci **opc.tcp://nazwa_komputera_z_uruchomionym_serwisem_OPC_UA_Service:OPC_UA_Service_Port_Number/** i nacisnąć **Refresh**. Wtedy w oknie **UA Servers** pojawi się serwer OPC UA uruchomiony jako OPC UA Service. Należy zaznaczyć **None – None (Insecure)** i nacisnąć **OK**.



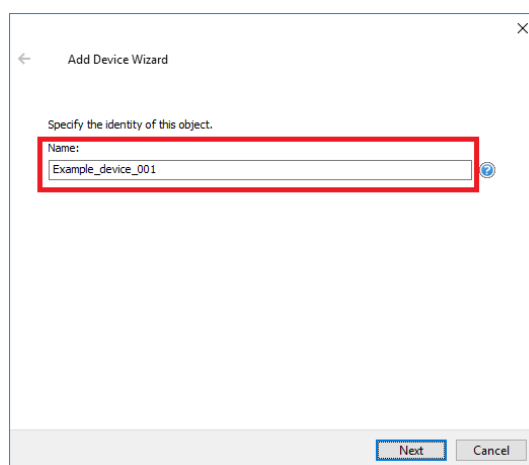
W polu **Endpoint URL** pojawi się skonfigurowany adres w postaci **opc.tcp://nazwa_komputera_z_uruchomionym_serwisem_OPC_UA_Service:OPC_UA_Service_Port_Number/**. Należy nacisnąć przycisk **Next**.



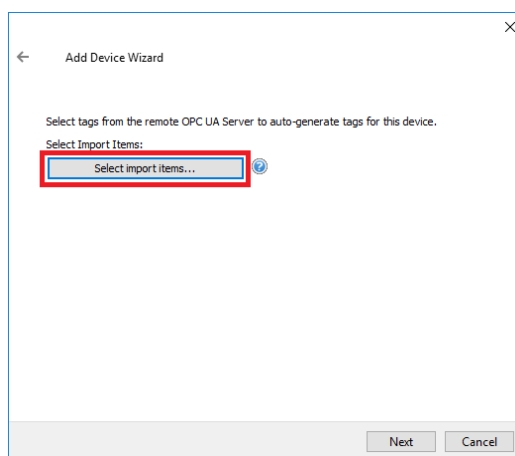
W kolejnych oknach należy pozostawić domyślne ustawienia. W ostatnim oknie należy nacisnąć przycisk **Finish**.



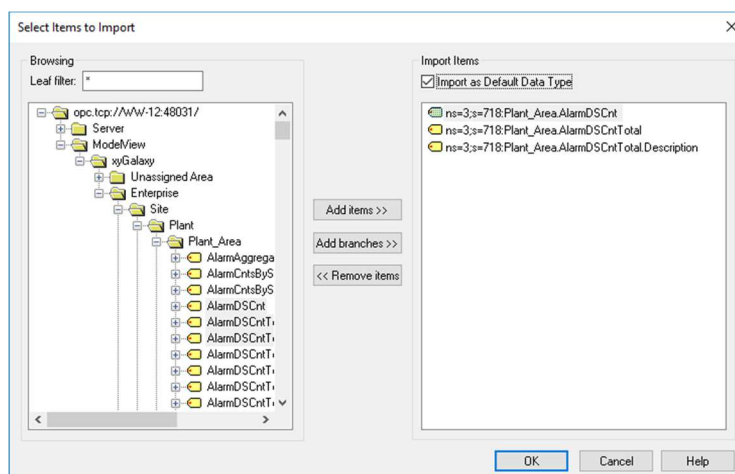
W następnym kroku w programie **KEPServerEX 6 Configuration** należy kliknąć prawym przyciskiem myszy na nowo utworzony kanał i wybrać opcję **New Device**.



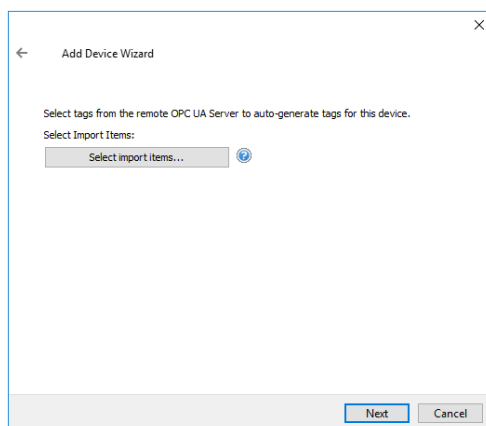
W polu **Name** należy wpisać nazwę dla tworzonego urządzenia i przejść do następnego okna klikając przycisk **Next**.



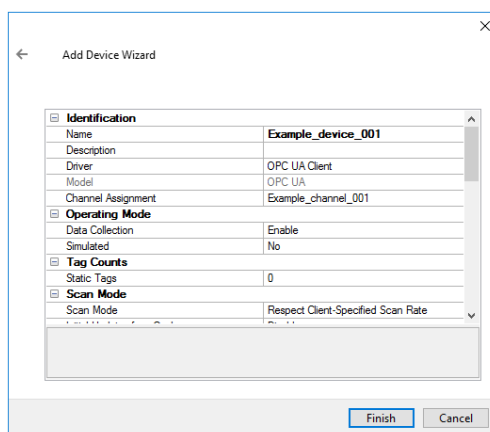
W kolejnych oknach należy pozostawić domyślne ustawienia, aż do okna z przyciskiem **Select import items**, który należy nacisnąć.



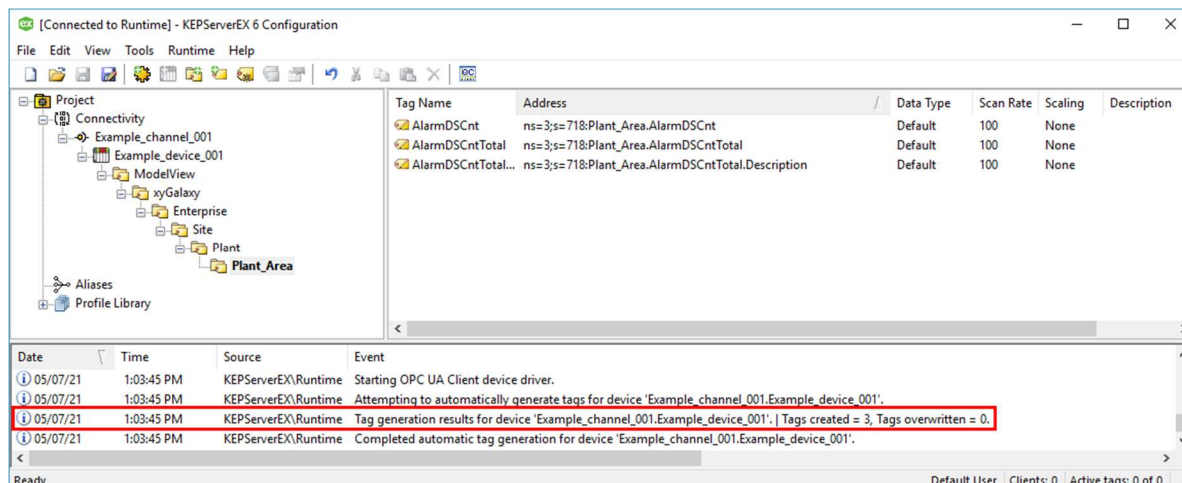
Pojawi się okno **Select Items to Import**, w którym w oknie **Browsing** należy rozwinąć **opc.tcp://nazwa_komputera_z_uruchomionym_serwisem OPC-UA_Service:OPC-UA_Service_Port_Number/** oraz **ModelView**. Wtedy zostanie pokazana struktura widoku **Model** znajdującego się w wybranym projekcie aplikacji Platformy Systemowej. Zaznaczając wybrane atrybuty obiektów należy nacisnąć przycisk **Add items >>**. Atrybuty zostaną dodane do okna **Import Items**. Należy zaznaczyć opcję **Import as Default Data Type** i nacisnąć przycisk **OK**.



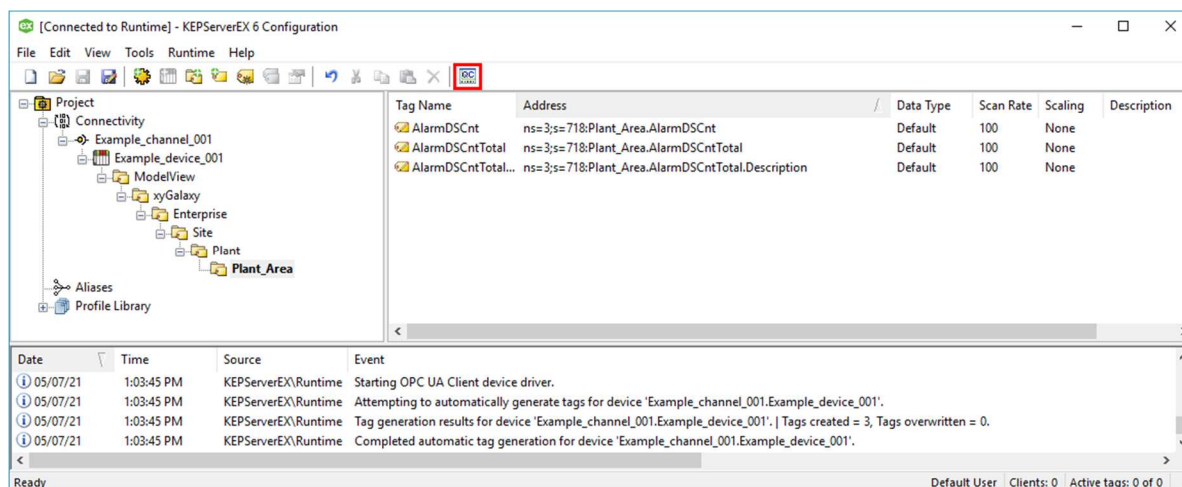
Okno **Select Items to Import** zostanie zamknięte. Należy nacisnąć przycisk **Next**.




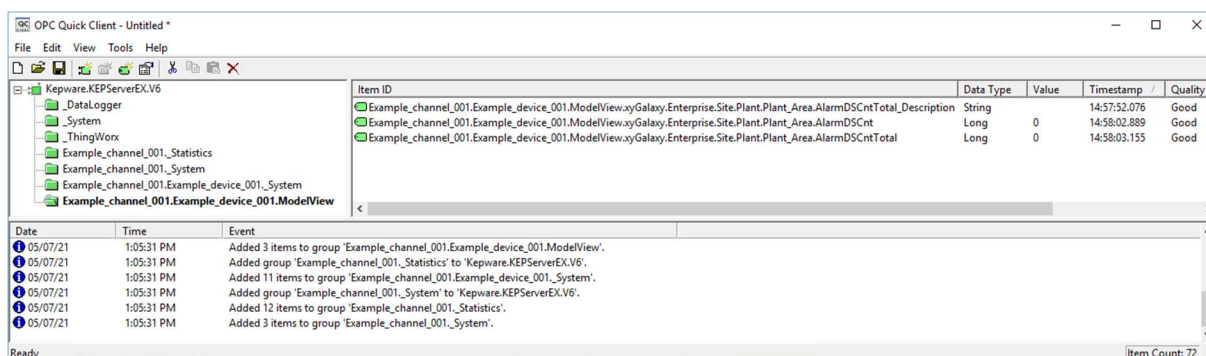
W kolejnym oknie należy nacisnąć przycisk **Finish**.



W konfiguracji programu **KEPServerEX 6 Configuration** pojawi się wybrana lista zmiennych, a w oknie u dołu komunikat o utworzeniu zmiennych.



W kolejnym kroku należy sprawdzić możliwość odczytania wartości zmiennych. W tym celu należy uruchomić program **OPC Quick Client** naciskając ikonę .

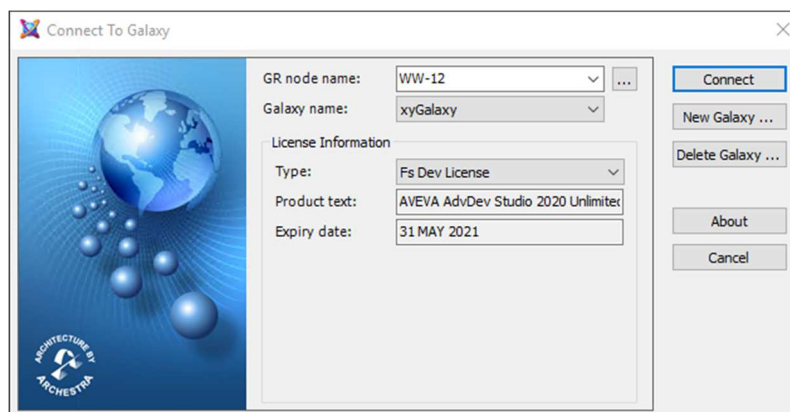


W oknie znajdującym się po lewej stronie należy zaznaczyć element o nazwie **<nazwa kanału>.<nazwa urządzenia>.ModelView**. Wtedy w oknie po prawej stronie pojawią się zmienne, a w kolumnie **Value** ich bieżące wartości.

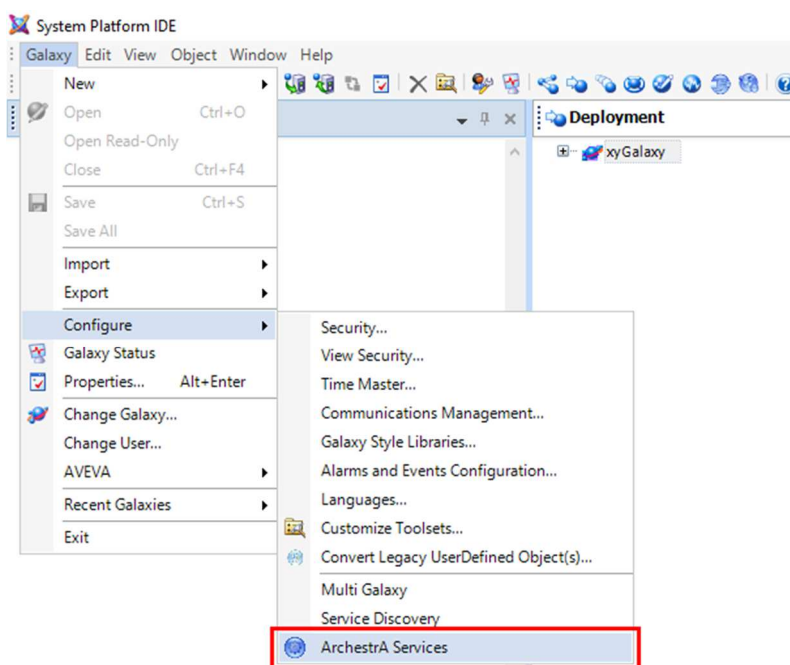
KONFIGURACJA KOMUNIKACJI KLIENTA OPC UA DO AVEVA SYSTEM PLATFORM JAKO SERWERA OPC UA ZE SKONFIGUROWANYMI ZABEZPIECZENIAMI (ENCRYPTED COMMUNICATION)

1. Konfiguracja i uruchamianie serwera OPC UA w programie System Platform IDE

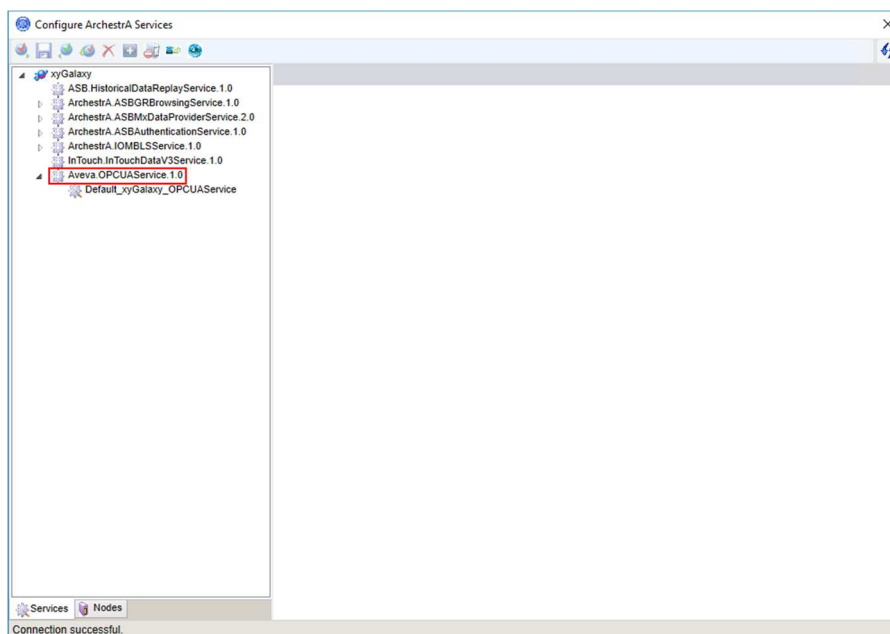
Z grupy programów **AVEVA System Platform** należy uruchomić program **System Platform IDE**.



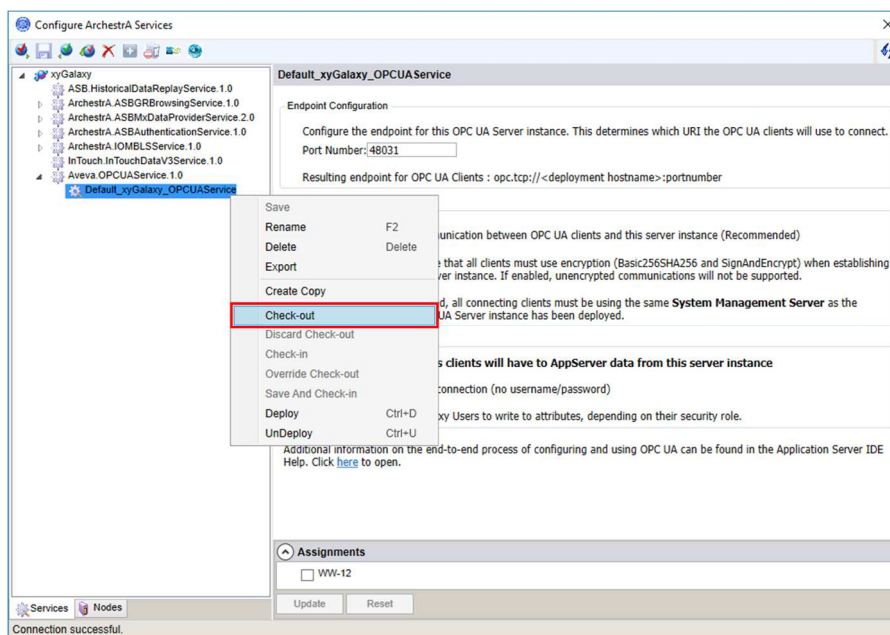
Pojawi się okno **Connect To Galaxy**, w którym należy połączyć się projektu, w którym ma zostać skonfigurowane udostępnianie danych po protokole OPC UA.



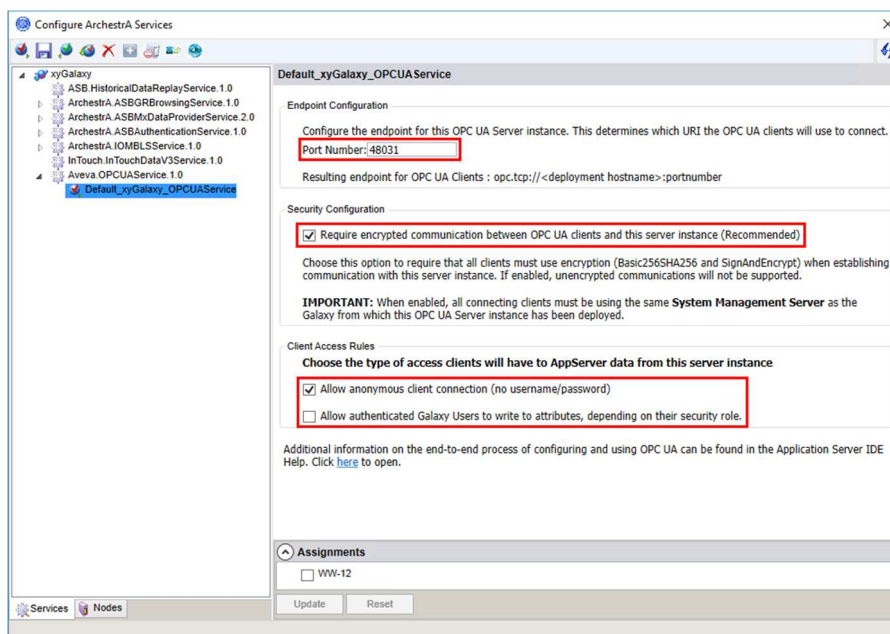
W programie **System Platform IDE** z menu należy wybrać **Galaxy**, następnie **Configure** i **Archestra Services**.



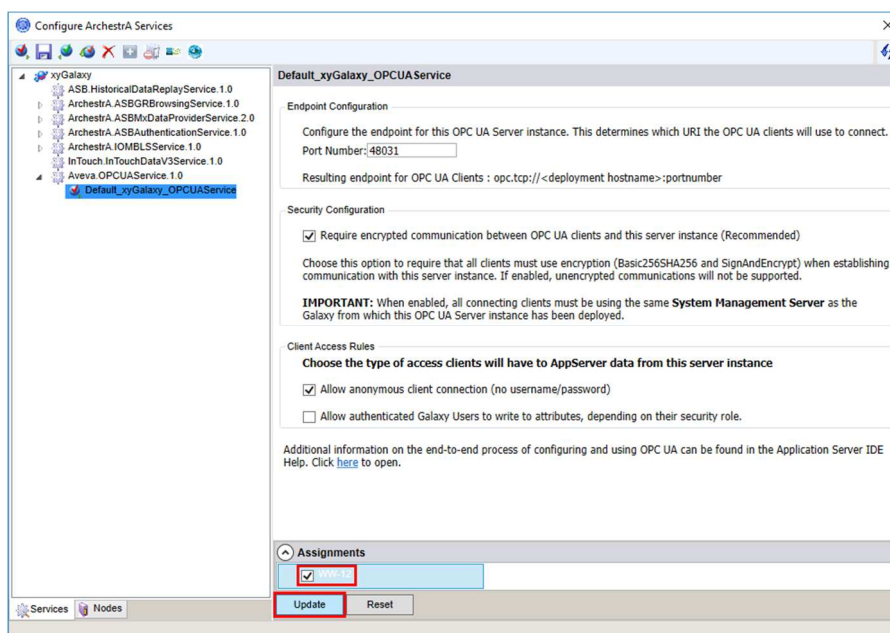
W oknie **Configure ArchestrA Services** należy rozwinąć listę serwisów dla wybranego projektu aplikacji, a następnie rozwinąć opcję **Aveva.OPCUAService.1.0**.



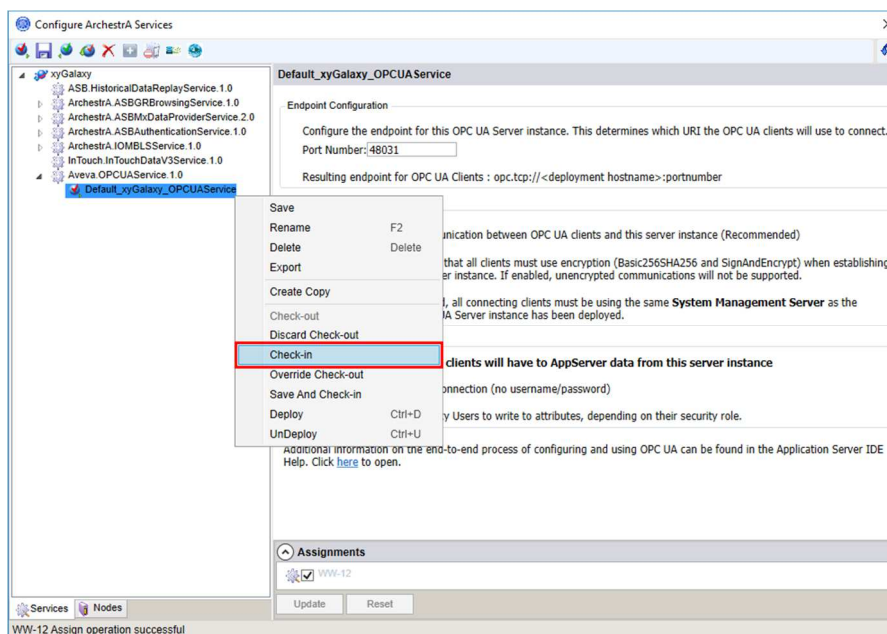
W kolejnym kroku należy kliknąć prawym przyciskiem myszy na serwis o nazwie **Default_<nazwa projektu>_OPCUAService** i wybrać opcję **Check-out**.



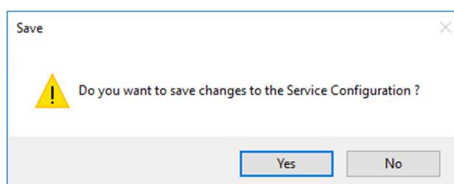
W oknie **Default_<nazwa projektu>_OPCUAService** w pierwszej kolejności należy skonfigurować **Port Number**. Domyślnie port jest ustawiony na **48031**. Następnie należy zaznaczyć opcję **Require encrypted communication between OPC UA clients and this server instance (Recommended)**, zaznaczyć **Allow anonymous client connection (no username/password)**, odznaczyć **Allow authenticated Galaxy Users to write to attributes, depending on their security role**.



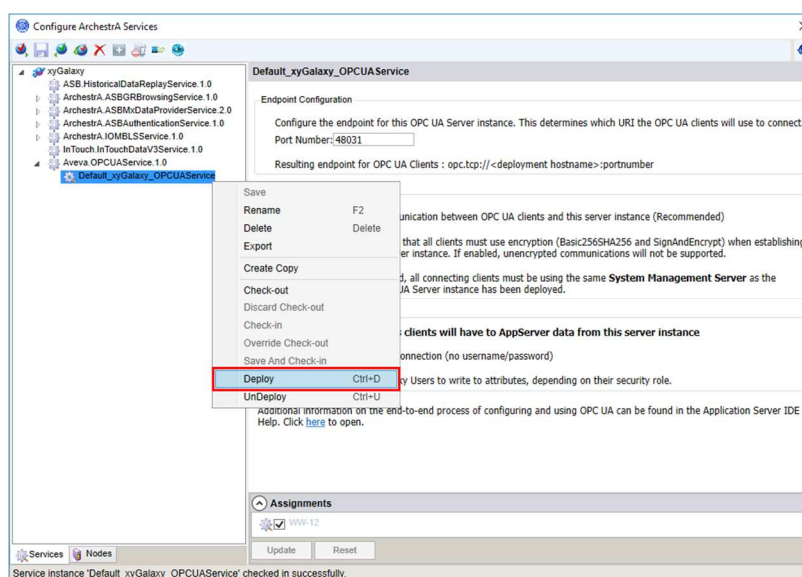
U dołu w oknie **Assignments** pokazane są komputery dostępne w platformie, na których możliwe jest uruchomienie skonfigurowanego serwisu OPC UA Service. Należy zaznaczyć komputer, na którym ma zostać uruchomiony serwis i kliknąć **Update**.



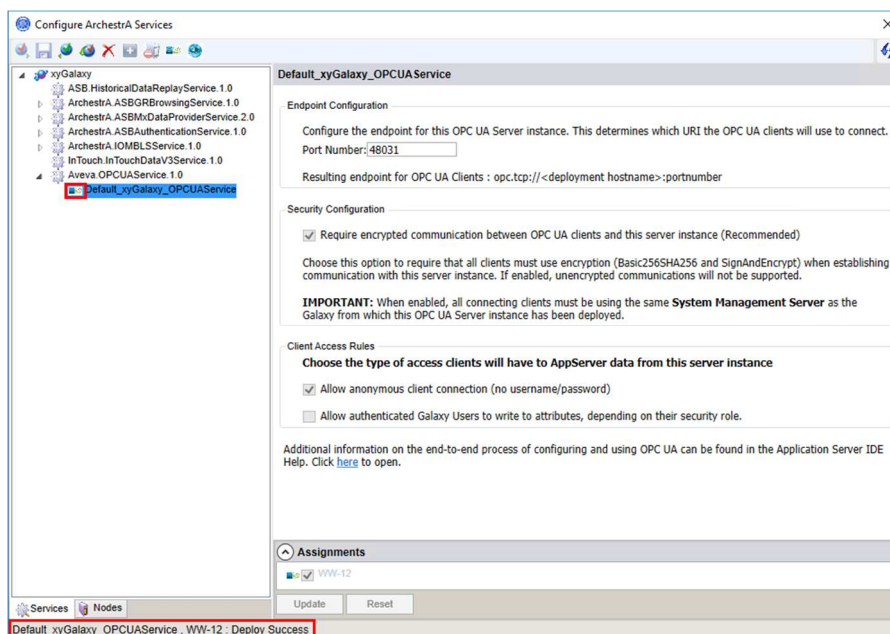
Następnie w oknie po lewej stronie należy kliknąć prawym przyciskiem myszy na serwis o nazwie **Default_<nazwa projektu>_OPCUAService** i wybrać opcję **Check-in**.



Pojawi się komunikat **Do you want to save changes to the Service Configuration?** Należy nacisnąć przycisk **Yes**.



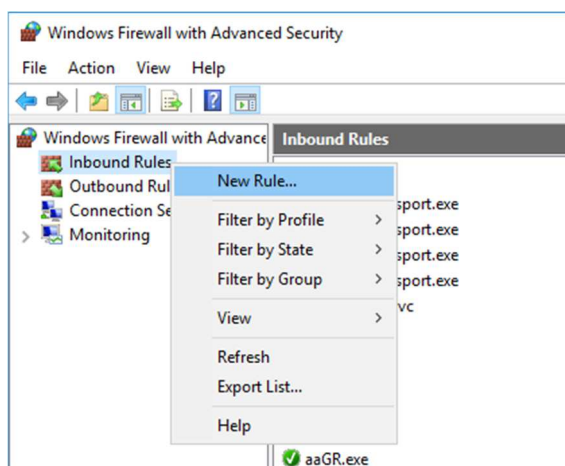
W oknie po lewej stronie należy kliknąć prawym przyciskiem myszy na serwis o nazwie **Default_<nazwa projektu>_OPCUAService** i wybrać opcję **Deploy**.



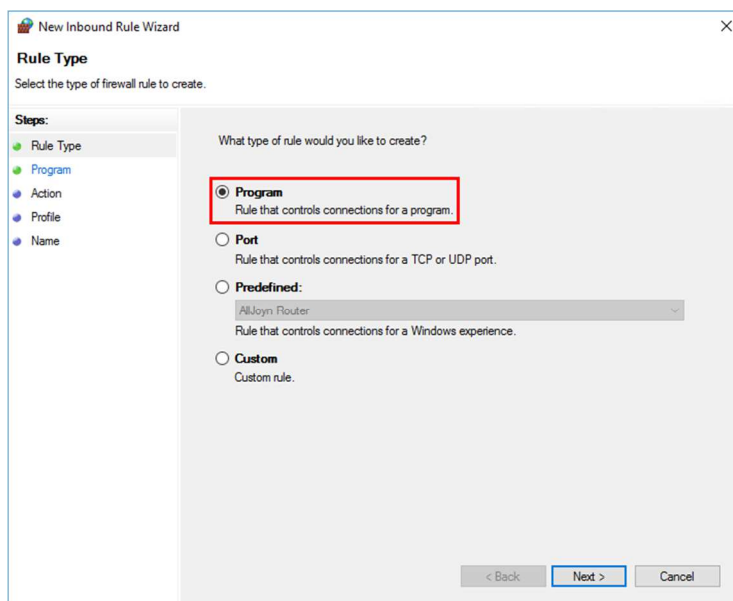
Po uruchomieniu, po lewej stronie nazwy serwisu pojawi się ikona , a u dołu okna pojawi się komunikat **Default_<nazwa projektu>_OPUCAService, <nazwa komputera>: Deploy Success.**

2. Konfiguracja reguły w zaporze Windows na komputerze z uruchomionym serwisem OPC UA Service

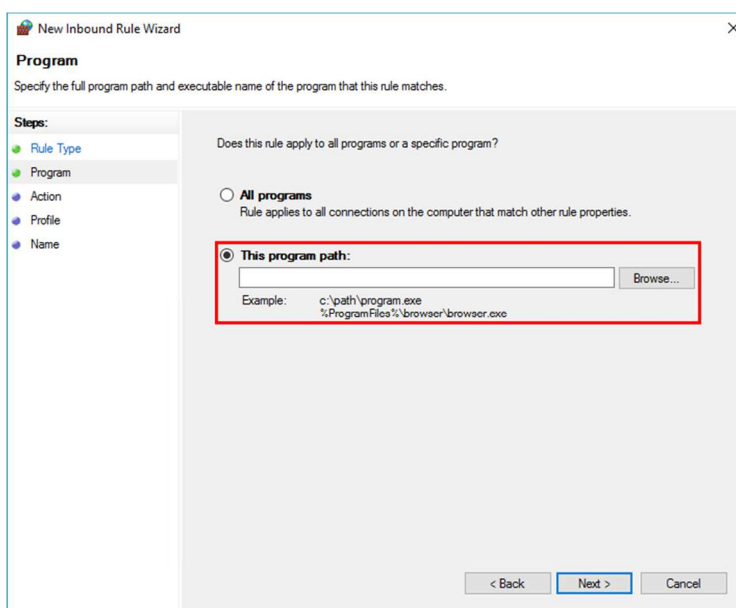
Konfigurację reguły w zaporze Windows należy wykonać na komputerze, na którym został uruchomiony serwis OPC UA Service. Jest to niezbędne, aby aplikacja kliencka OPC UA mogła nawiązać prawidłowe połączenie z serwerem OPC UA.



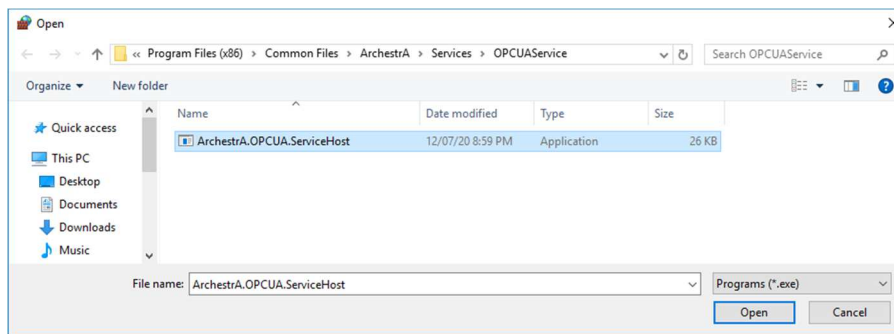
W systemie Windows należy uruchomić **Administrative Tools (Narzędzia administracyjne systemu Windows)**, a następnie program **Windows Firewall with Advanced Security (Zapora Windows Defender z narzędziami zaawansowanymi)**. Po uruchomieniu programu należy zaznaczyć **Inbound Rules (Reguły przychodzące)**, kliknąć prawym przyciskiem myszy i wybrać opcję **New Rule (Nowa reguła)**.



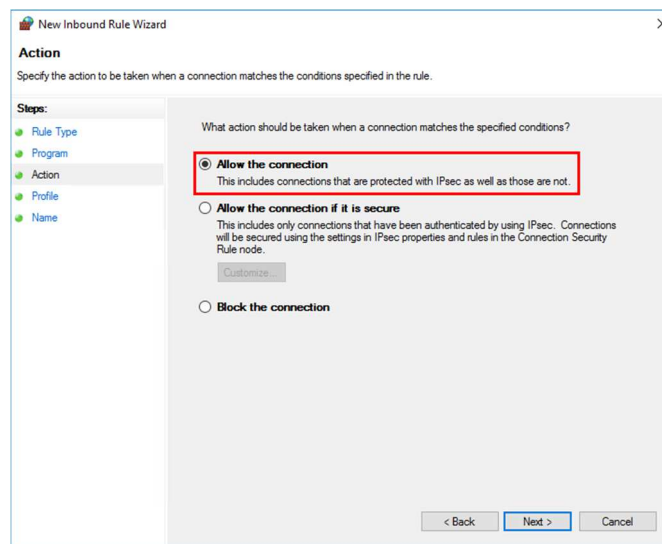
W oknie **Rule Type (Typ reguły)**, należy zaznaczyć **Program** i nacisnąć przycisk **Next**.



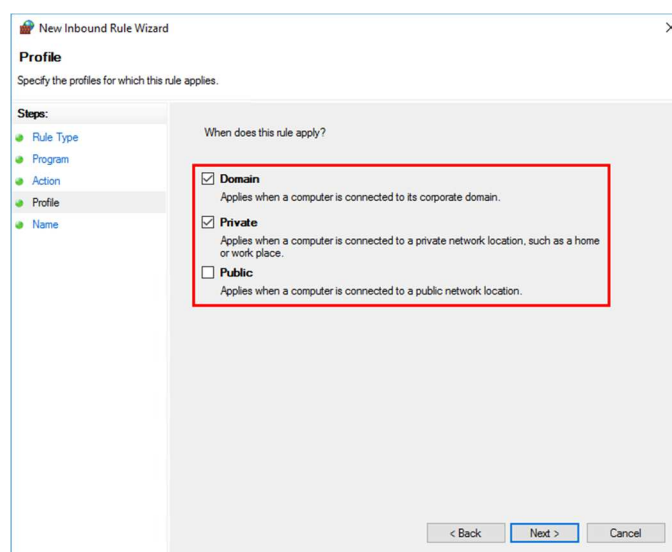
W kolejnym oknie należy zaznaczyć opcję **This program path** i wyszukać lokalizację serwisu OPC UA Server Service. W tym celu należy nacisnąć przycisk **Browse** znajdujący się po prawej stronie pola **This program path**. Jeśli Platforma Systemowa zainstalowana była w domyślnej lokalizacji, ścieżka dostępu wygląda następująco: **C:\Program Files (x86)\Common Files\ArchestrA\Services\OPCUAService**.



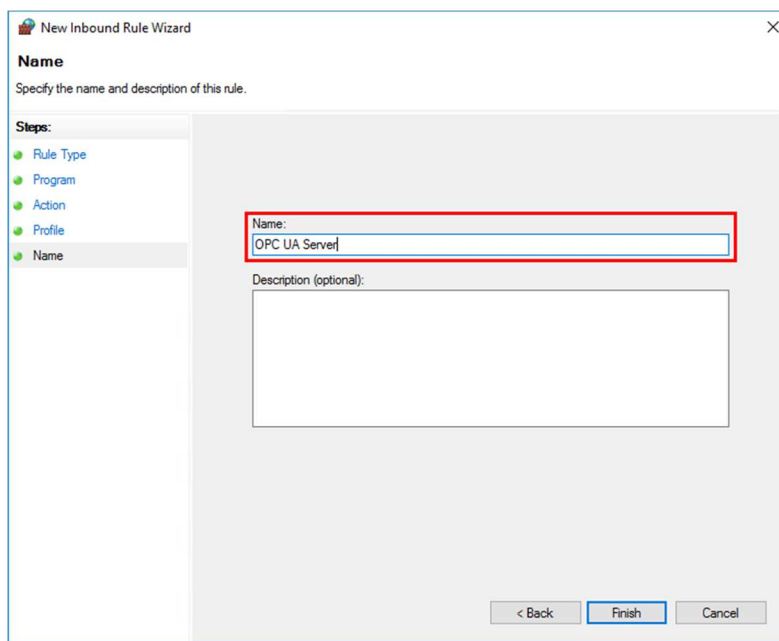
W następnym kroku należy wybrać **Arcestra.OPCUA.ServiceHost.exe** i nacisnąć przycisk **Open**. Następnie należy nacisnąć przycisk **Next**, aby przejść do następnego okna.



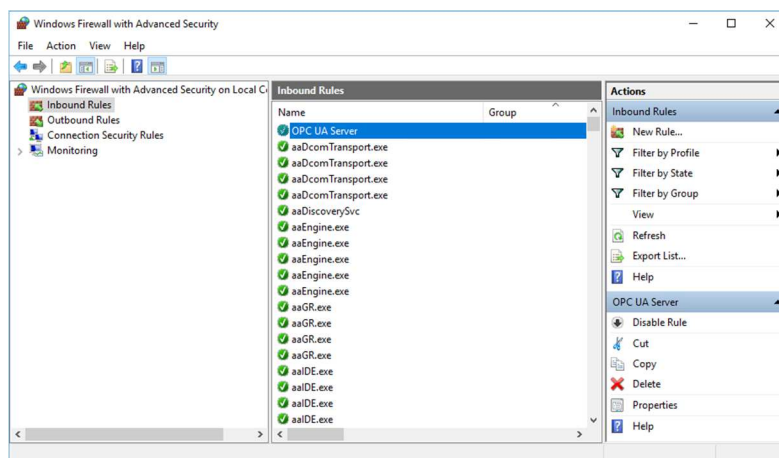
W następnym oknie należy zaznaczyć opcję **Allow the connection** i nacisnąć przycisk **Next**.



W kolejnym oknie należy zaznaczyć opcje **Domain** oraz **Private**, a odznaczyć opcję **Public** i nacisnąć przycisk **Next**.



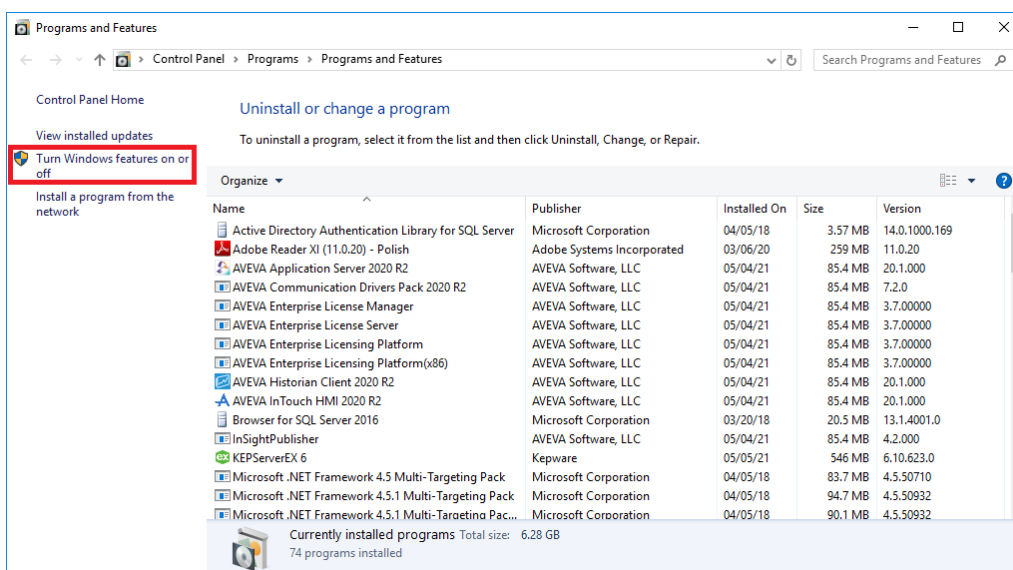
Następnie w polu **Name** należy wpisać nazwę dla zdefiniowanej reguły np. **OPC UA Server** i nacisnąć przycisk **Finish**.



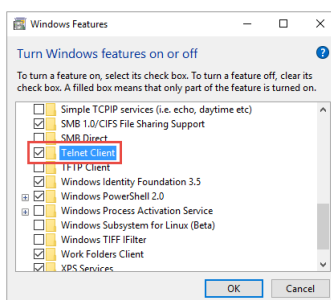
Skonfigurowana reguła pojawi się na liście reguł.

3. Sprawdzenie na komputerze z aplikacją kliencką OPC UA możliwości połączenia z serwerem OPC UA uruchomionego przez serwis OPC UA Service

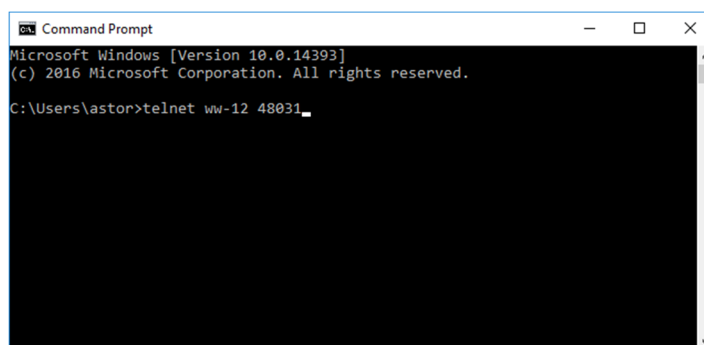
Po skonfigurowaniu reguły w zaporze Windows należy sprawdzić, czy jest możliwa komunikacja przez port, który wykorzystuje serwis OPC UA Service. Test połączenia należy wykonać na komputerze z aplikacją kliencką OPC UA, która ma zostać skonfigurowana do połączenia z serwerem OPC UA.



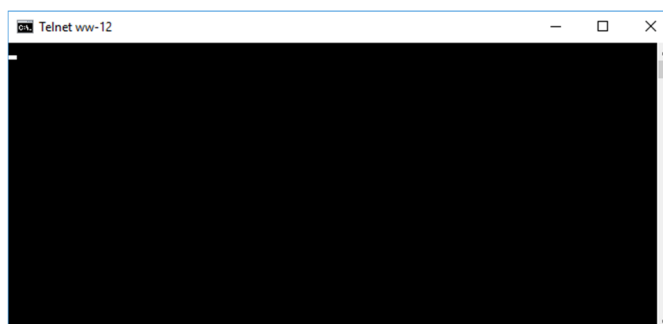
W tym celu w systemie Windows należy wejść do **Add or remove programs (Dodaj lub usuń programy)**, a następnie kliknąć **Programs and features (Programy i funkcje)** i wybrać **Turn Windows features on or off (Włącz lub wyłącz funkcje systemu Windows)**.



Spośród dostępnych funkcji należy zaznaczyć **Telnet Client (Klient Telnet)** i nacisnąć **OK**, aby zainstalować w systemie Windows tę funkcję.



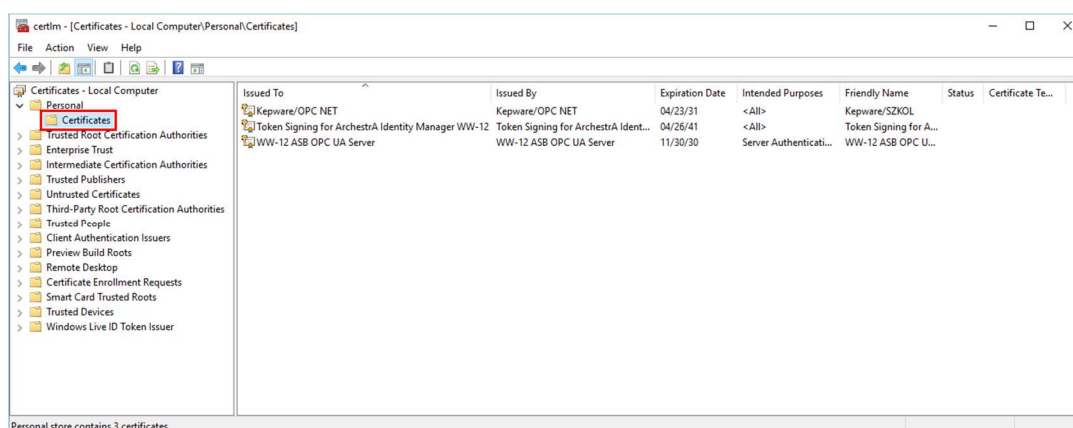
W kolejnym kroku w systemie Windows należy uruchomić linię komend i wpisać polecenie **telnet nazwa_komputera lub adres_IP nr_portu_serwera_OPC_UA** i nacisnąć Enter np. **telnet WW-12 48031**



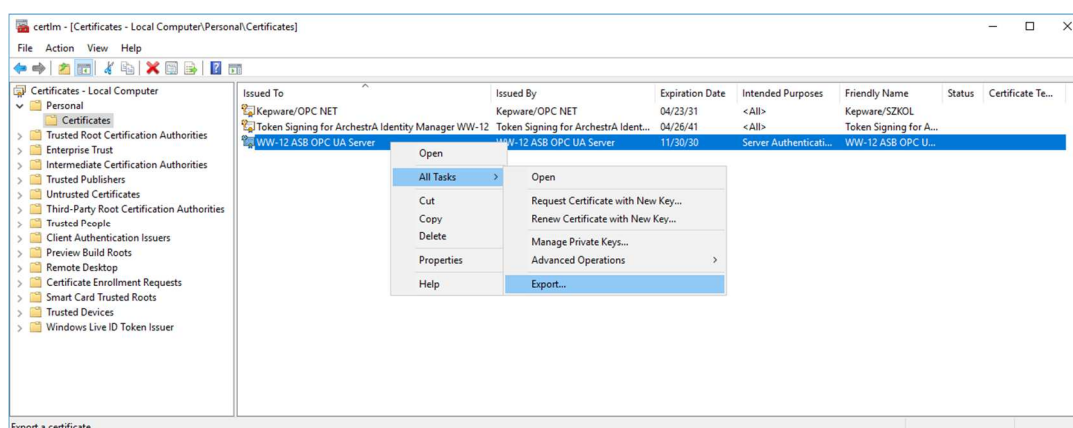
Jako wynik pojawi się kursor w lewym górnym rogu, który jest potwierdzeniem, że port jest dostępny w systemie Windows do komunikacji.

4. Konfiguracja certyfikatów w systemie Windows

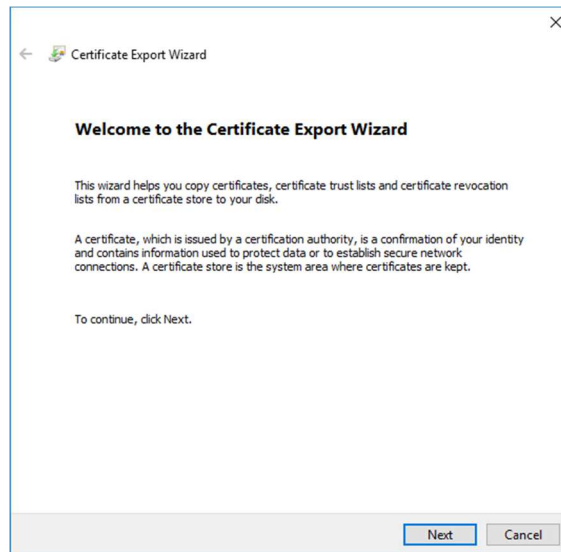
Na komputerze, na którym została uruchomiona usługa serwera OPC UA dla Application Server, należy w systemie Windows uruchomić **Manage Computer Certificates (Zarządzanie certyfikatami komputerów)**.



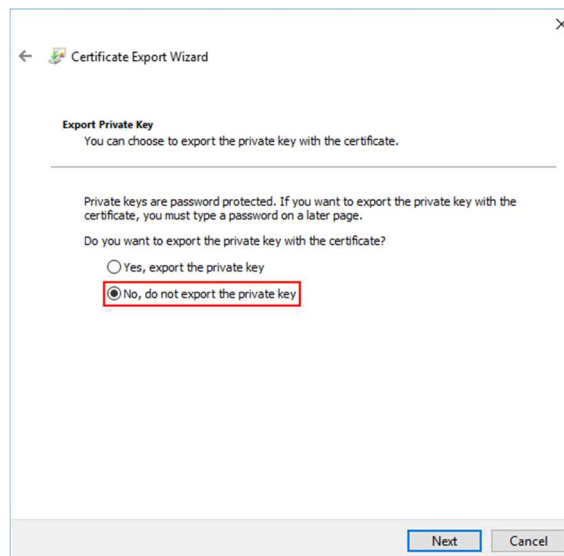
Pojawi się okno **certlm**, w którym po lewej stronie należy rozwinąć **Personal (Osobisty)**, a następnie kliknąć **Certificates (Certyfikaty)**.



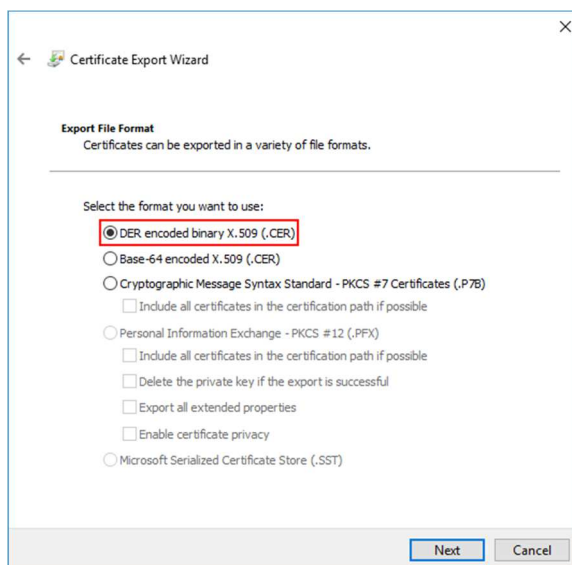
Na liście certyfikatów należy odszukać certyfikat o nazwie <nazwa komputera> **ASB OPC UA Server**, kliknąć na niego prawym przyciskiem myszy, wybrać **All Tasks**, a następnie **Export**.



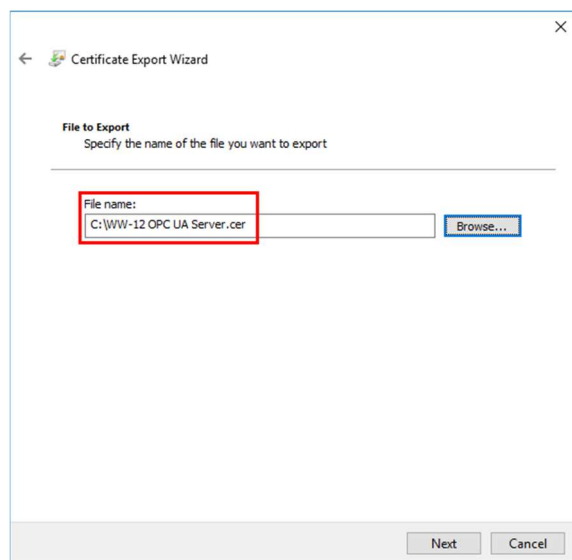
Pojawi się okno **Certificate Export Wizard**. Należy wcisnąć przycisk **Next**.



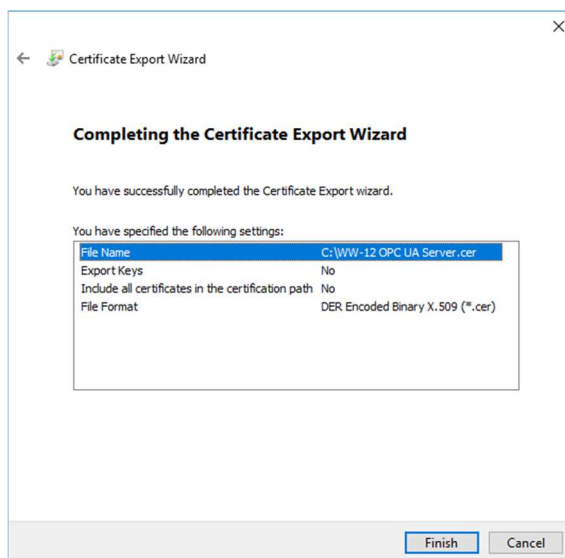
W następnym oknie należy zaznaczyć opcję **No, do not export the private key** i nacisnąć przycisk **Next**.



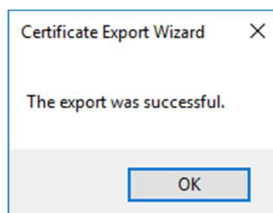
W kolejnym oknie należy zaznaczyć opcję **DER encoded binary X.509 (.CER)** i nacisnąć przycisk **Next**.



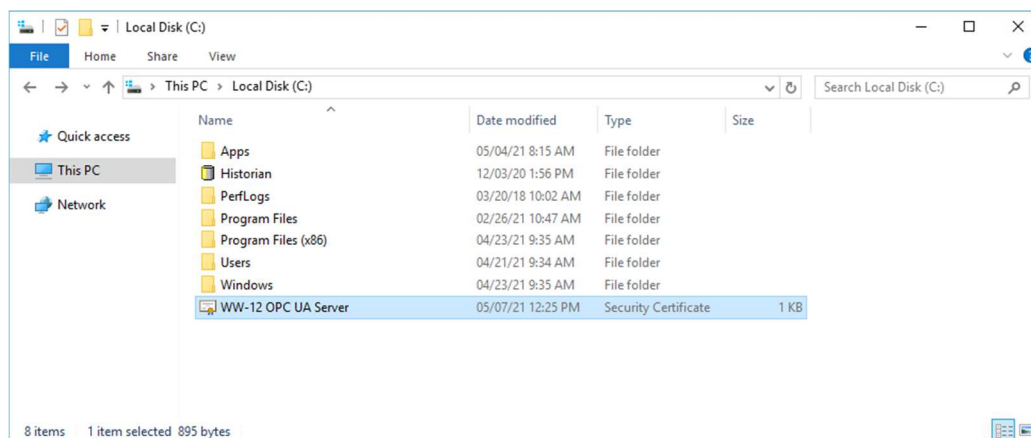
W następnym oknie w polu **File name** należy wpisać miejsce zapisu oraz nazwę dla eksportowanego certyfikatu np. **C:\<nazwa komputera> OPC UA Server.cer**, nacisnąć przycisk **Next**.



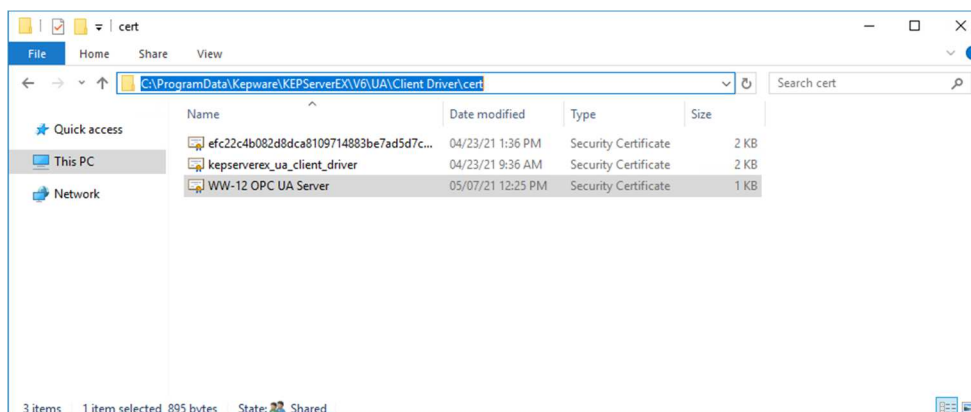
W kolejnym oknie należy nacisnąć przycisk **Finish**.



Pojawi się komunikat **The export was successful**. Należy nacisnąć przycisk **OK**.



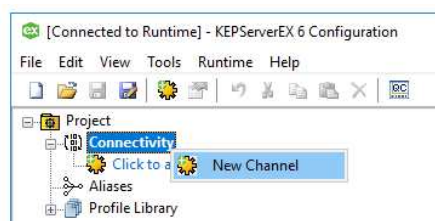
Zostanie utworzony plik z certyfikatem.



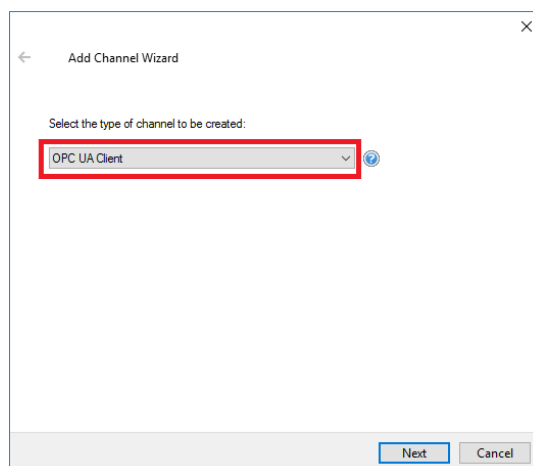
W kolejnym kroku należy skopiować wyeksportowany certyfikat do folderu **C:\ProgramData\Kepware\KEPServerEX\V6\UA\Client Driver\cert** na komputerze, na którym zainstalowany jest program **KEPServerEX**. Folder **ProgramData** domyślnie jest ukryty, więc w systemie Windows należy włączyć pokazywanie ukrytych elementów.

5. Konfiguracja połączenia programu klienckiego OPC UA na przykładzie programu KEPServerEX

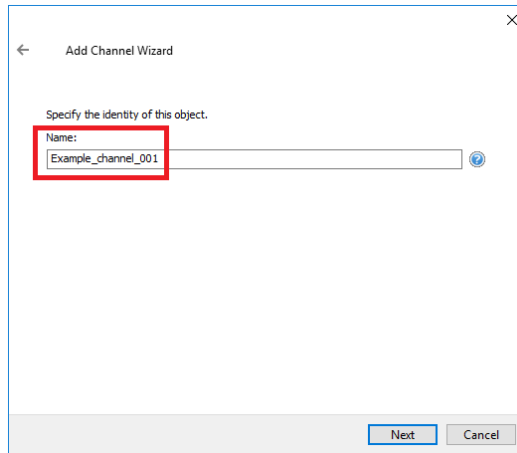
Po zainstalowaniu oprogramowania **KEPServerEX** należy uruchomić program **KEPServerEX 6 Configuration**.



Następnie należy kliknąć prawym przyciskiem myszy na **Connectivity** i wybrać opcję **New Channel**.



W oknie **Add Channel Wizard** z rozwijanego menu należy wybrać opcję **OPC UA Client** i nacisnąć przycisk **Next**.



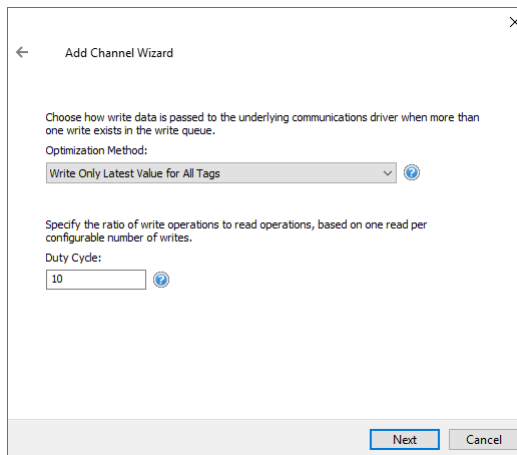
← Add Channel Wizard

Specify the identity of this object.

Name:
Example_channel_001

Next Cancel

W następnym oknie w polu **Name** należy wpisać nazwę dla tworzonego kanału i nacisnąć przycisk **Next**.



← Add Channel Wizard

Choose how write data is passed to the underlying communications driver when more than one write exists in the write queue.

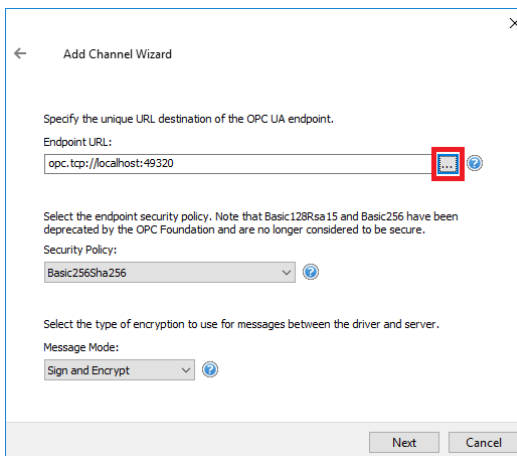
Optimization Method:
Write Only Latest Value for All Tags

Specify the ratio of write operations to read operations, based on one read per configurable number of writes.

Duty Cycle:
10

Next Cancel

W kolejnym oknie należy nacisnąć przycisk **Next**.



← Add Channel Wizard

Specify the unique URL destination of the OPC UA endpoint.

Endpoint URL:
opc.tcp://localhost:49320


Select the endpoint security policy. Note that Basic128Rsa15 and Basic256 have been deprecated by the OPC Foundation and are no longer considered to be secure.

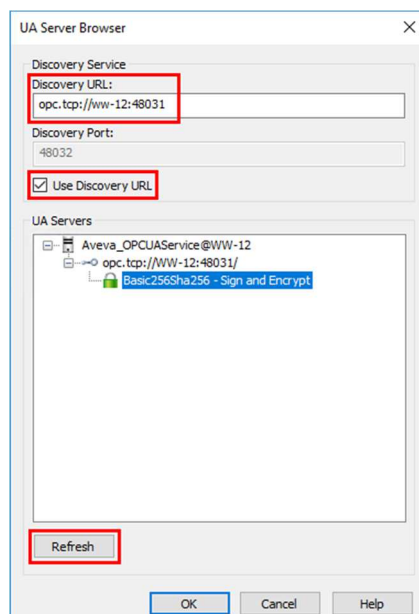
Security Policy:
Basic256Sha256

Select the type of encryption to use for messages between the driver and server.

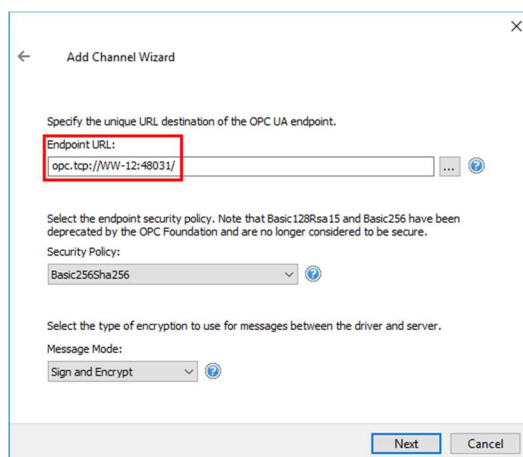
Message Mode:
Sign and Encrypt

Next Cancel

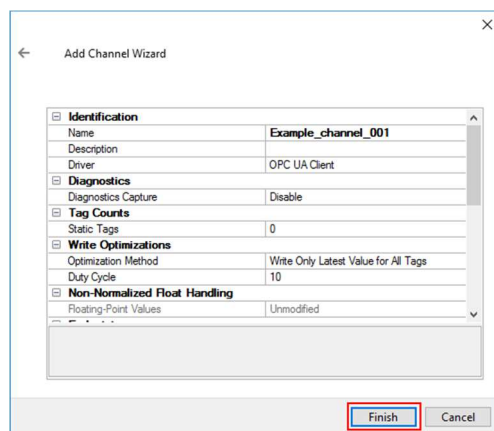
W następnym oknie należy kliknąć na ikonę  znajdującą się po prawej stronie pola **Endpoint URL**.



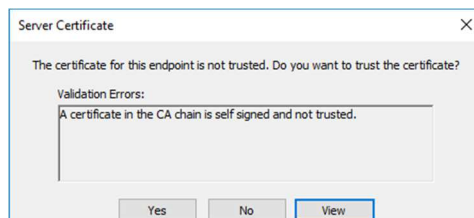
Pojawi się okno **UA Server Browser**. W oknie **UA Servers** należy zaznaczyć **Use Discovery URL** i w polu **Discovery URL**: należy wpisać adres w postaci **opc.tcp://nazwa_komputera_z_uruchomionym_serwisem OPC-UA_Service:OPC-UA_Service_Port_Number/** i nacisnąć **Refresh**. Wtedy w oknie **UA Servers** pojawi się serwer OPC UA uruchomiony jako OPC UA Service. Należy zaznaczyć **Basic256Sha256 - Sign and Encrypt** i nacisnąć **OK**.



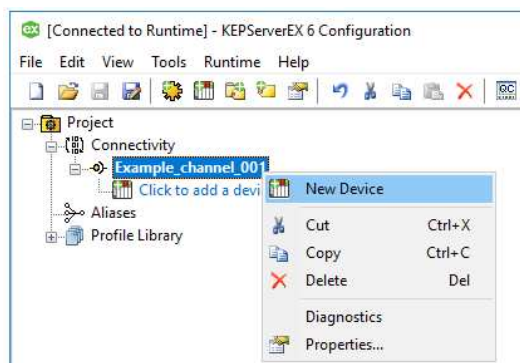
W polu **Endpoint URL** pojawi się skonfigurowany adres w postaci **opc.tcp://nazwa_komputera_z_uruchomionym_serwisem OPC-UA_Service:OPC-UA_Service_Port_Number/**. Należy nacisnąć przycisk **Next**.



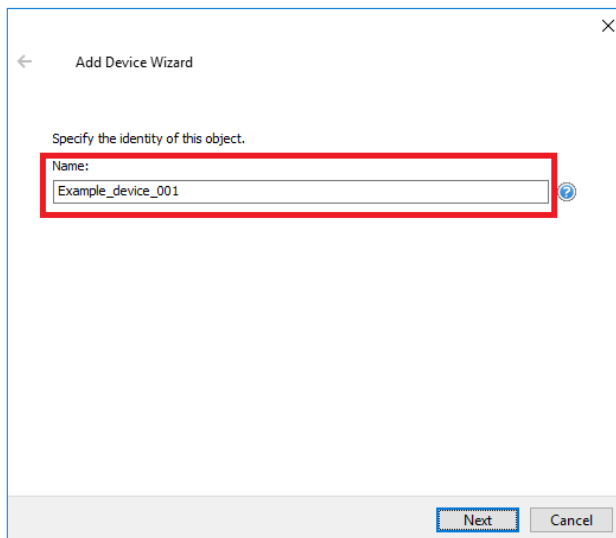
W kolejnych oknach należy pozostawić domyślne ustawienia. W ostatnim oknie należy nacisnąć przycisk **Finish**.



Pojawi się komunikat **The certificate for this endpoint is not trusted. Do you want to trust the certificate?** Należy nacisnąć przycisk **Yes**.



W następnym kroku w programie **KEPServerEX 6 Configuration** należy kliknąć prawym przyciskiem myszy na nowo utworzony kanał i wybrać opcję **New Device**.



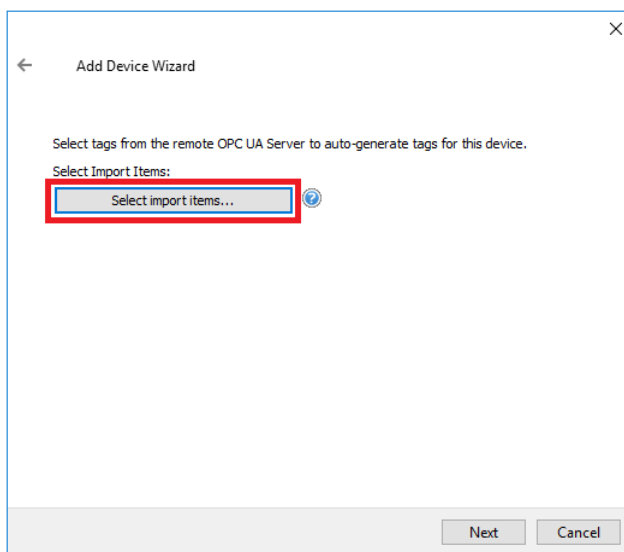
← Add Device Wizard

Specify the identity of this object.

Name:
Example_device_001

Next Cancel

W polu **Name** należy wpisać nazwę dla tworzonego urządzenia i przejść do następnego okna klikając przycisk **Next**.



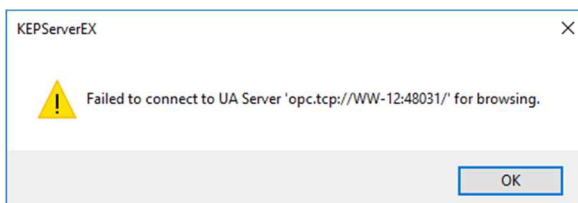
← Add Device Wizard

Select tags from the remote OPC UA Server to auto-generate tags for this device.

Select Import Items:
Select import items...

Next Cancel

W kolejnych oknach należy pozostawić domyślne ustawienia, aż do okna z przyciskiem **Select import items**, który należy nacisnąć.

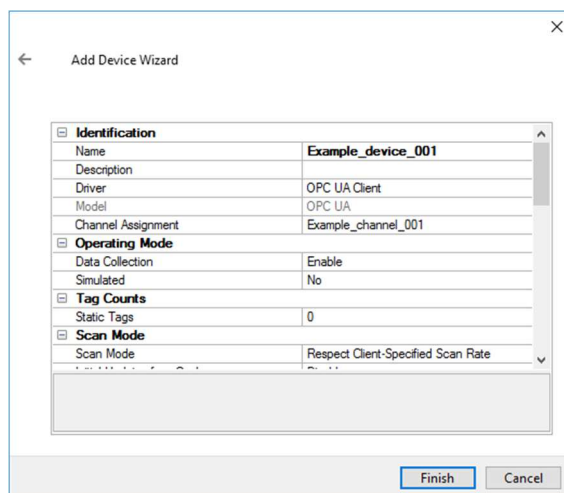


KEPServerEX

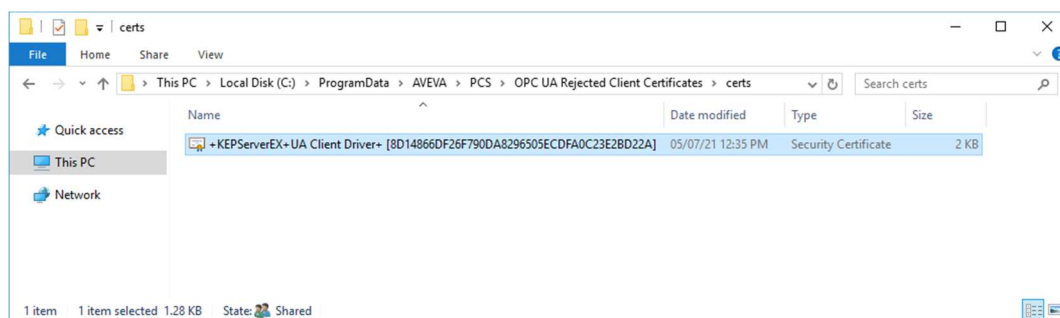
Failed to connect to UA Server 'opc.tcp://WW-12:48031/' for browsing.

OK

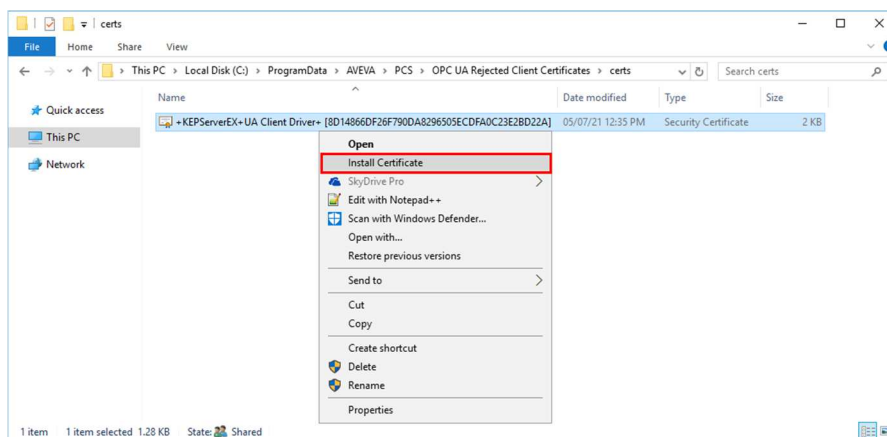
Pojawi się komunikat o nieudanym połączeniu z serwerem wynikający z braku skonfigurowania certyfikatu pochodzącego od klienta OPC UA na komputerze, na którym został uruchomiony serwis serwera OPC UA. Należy nacisnąć przycisk **OK**, a następnie **Next**.



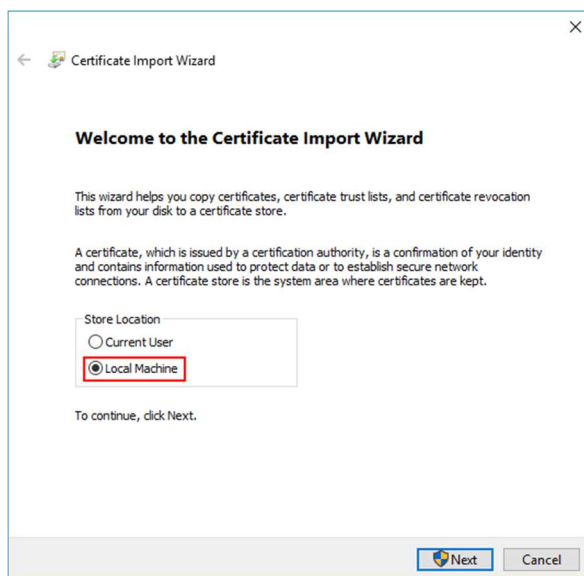
W kolejnym oknie należy nacisnąć przycisk **Finish**.



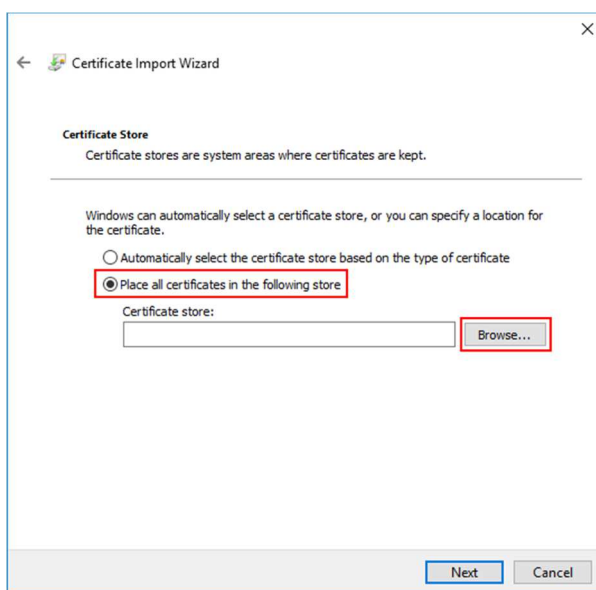
W następnym kroku należy otworzyć folder **C:\ProgramData\AVEVA\PCS\OPC UA Rejected Client Certificates\certs** na komputerze, na którym został uruchomiony serwis OPC UA Server. W tym folderze umieszczane są certyfikaty pochodzące od aplikacji klienckich OPC UA, których próba nawiązania połączenia z serwerem Application Server OPC UA Server zakończyła się niepowodzeniem. Folder **ProgramData** domyślnie jest ukryty, więc w systemie Windows należy włączyć pokazywanie ukrytych elementów.



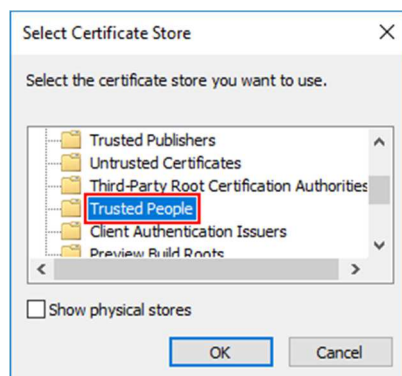
W tym przykładzie w folderze **C:\ProgramData\AVEVA\PCS\OPC UA Rejected Client Certificates\certs** znajduje się certyfikat pochodzący od aplikacji klienckiej **KEPServerEX**. Należy zaznaczyć plik z certyfikatem, kliknąć prawym przyciskiem myszy i wybrać opcję **Install Certificate**.



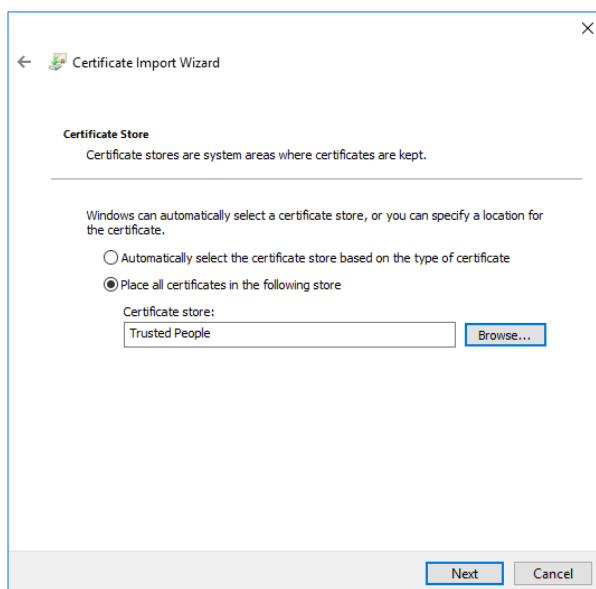
Pojawi się okno **Certificate Import Wizard**, w którym należy wybrać opcję **Local Machine**, a następnie nacisnąć przycisk **Next**.



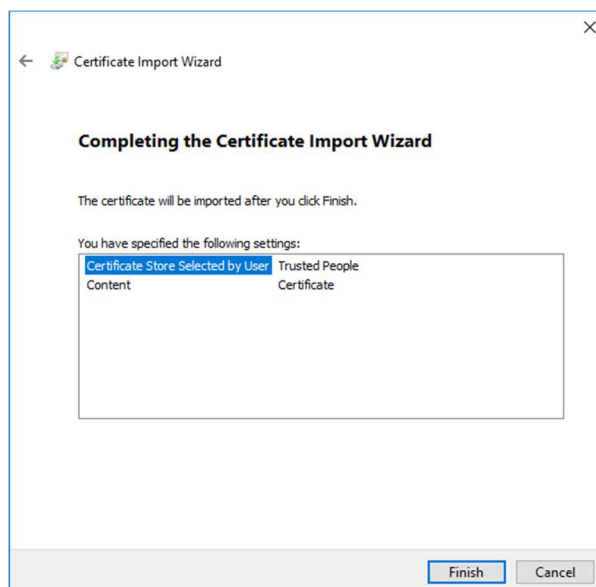
W następnym oknie należy zaznaczyć opcję **Place all certificates in the following store** i nacisnąć przycisk **Browse**, znajdujący się po lewej stronie pola **Certificate store**.



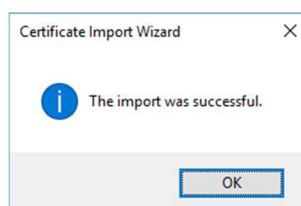
Pojawi się okno **Select Certificate Store**. Należy wybrać z listy opcję **Trusted People (Zaufane osoby)** i nacisnąć przycisk **OK**.



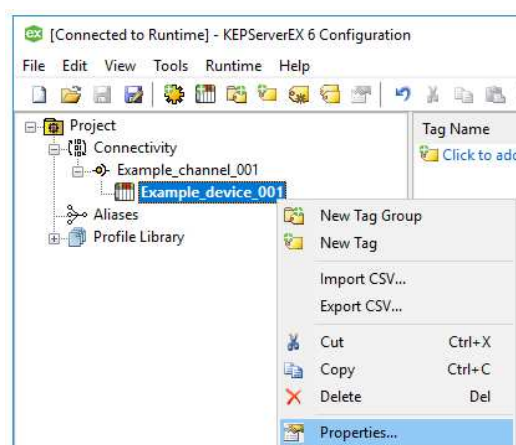
Należy nacisnąć przycisk **Next**, aby przejść do następnego okna.



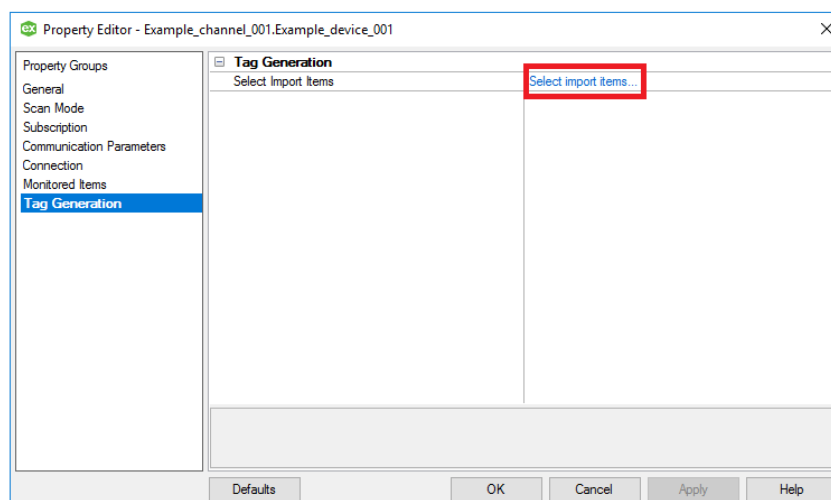
W kolejnym oknie należy nacisnąć przycisk **Finish**.



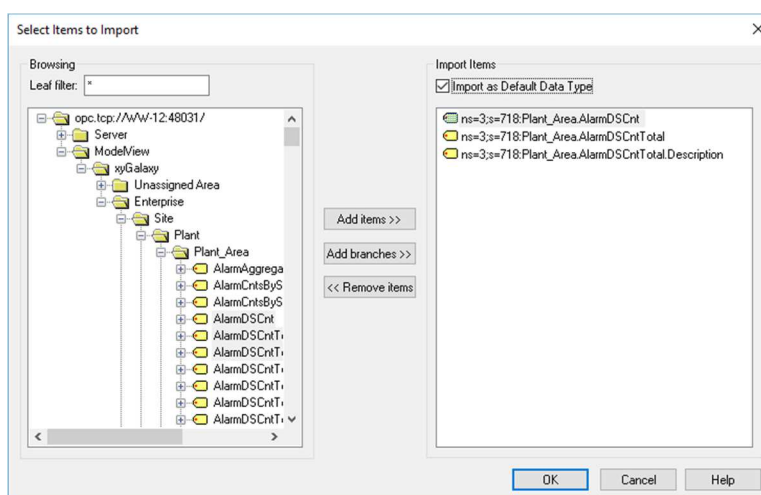
Pojawi się komunikat **The import was successful**. Należy nacisnąć przycisk **OK**.



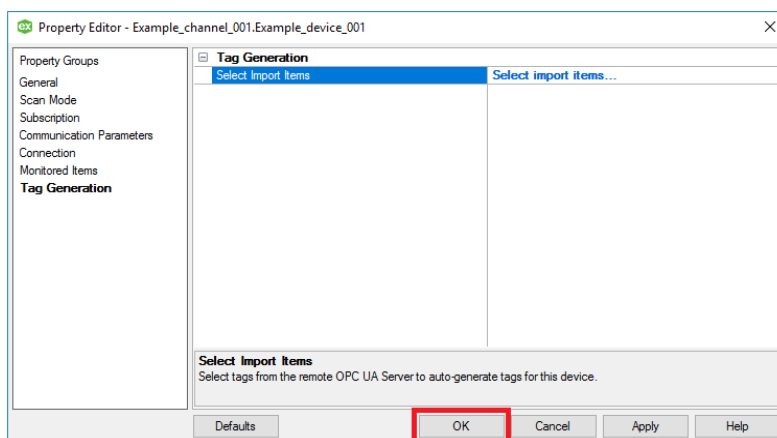
W następnym kroku należy powrócić do programu **KEPServerEX 6 Configuration**, kliknąć prawym przyciskiem myszy na wcześniej dodane urządzenie i wybrać opcję **Properties**.



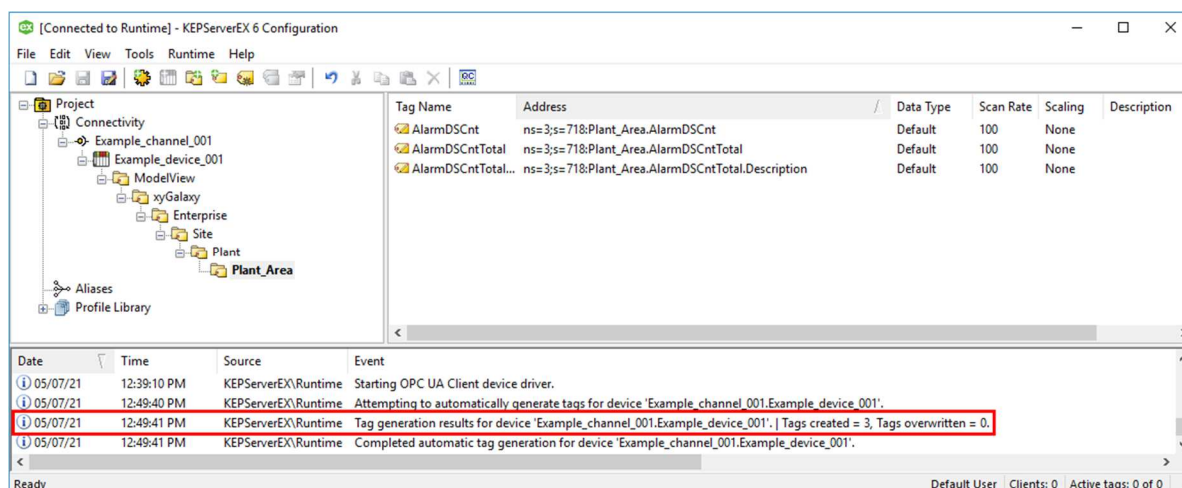
Pojawi się okno **Property Editor**, w którym po lewej stronie w oknie **Property Groups** należy zaznaczyć **Tag Generation**, następnie po prawej stronie kliknąć **Select import items**.



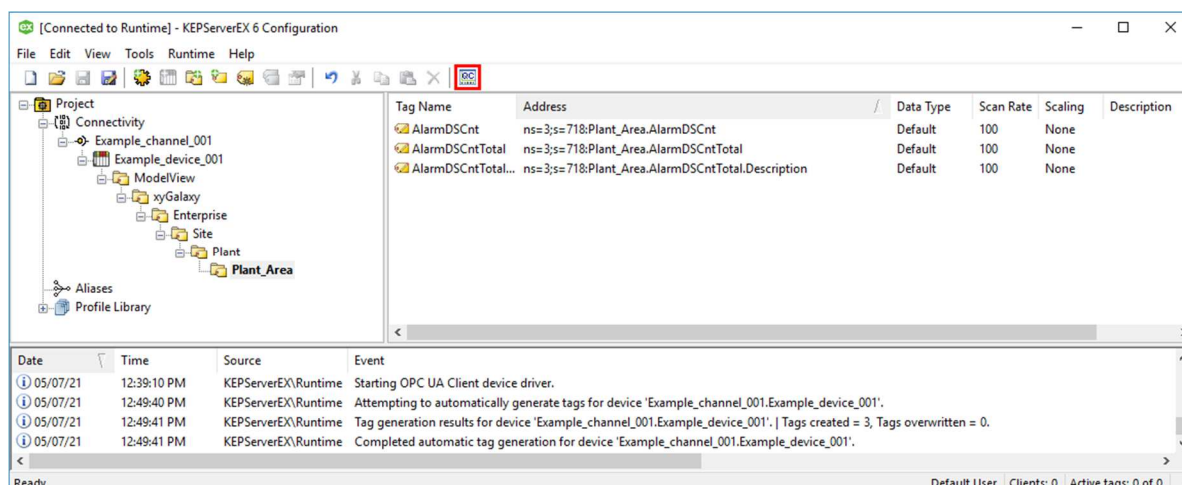
Pojawi się okno **Select Items to Import**, w którym w oknie **Browsing** należy rozwinąć **opc.tcp://nazwa_komputera_z_uruchomionym_serwisem_OPC_UA_Service:OPC_UA_Service_Port_Number/** oraz **ModelView**. Wtedy zostanie pokazana struktura widoku **Model** znajdującego się w wybranym projekcie aplikacji Platformy Systemowej. Zaznaczając wybrane atrybuty obiektów należy nacisnąć przycisk **Add items >>**. Atrybuty zostaną dodane do okna **Import Items**. Należy zaznaczyć opcję **Import as Default Data Type** i nacisnąć przycisk **OK**.




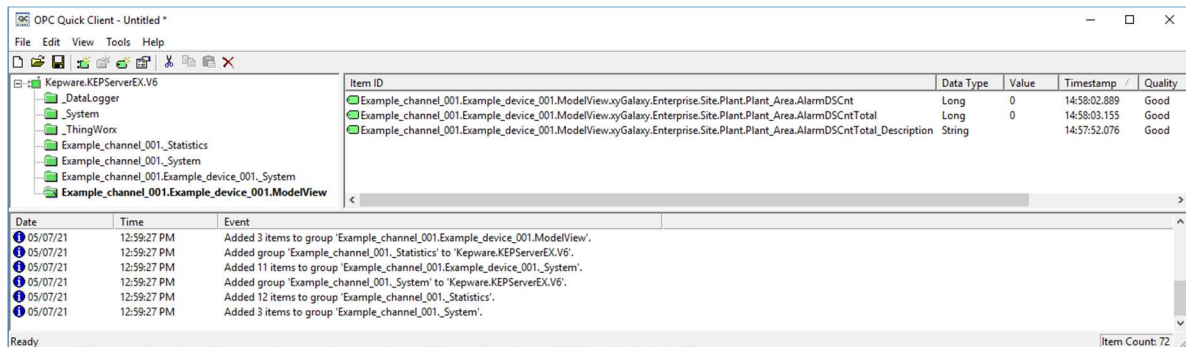
W oknie **Property Editor** należy nacisnąć **OK**.



W konfiguracji programu **KEPServerEX 6 Configuration** pojawi się wybrana lista zmiennych, a w oknie u dołu komunikat o utworzeniu zmiennych.



W kolejnym kroku należy sprawdzić możliwość odczytania wartości zmiennych. W tym celu należy uruchomić program **OPC Quick Client** naciskając ikonę .



W oknie znajdującym się po lewej stronie należy zaznaczyć element o nazwie **<nazwa kanału>.<nazwa urządzenia>.ModelView**. Wtedy w oknie po prawej stronie pojawią się zmienne, a w kolumnie **Value** ich bieżące wartości.