Tech Support

support@logitek.es

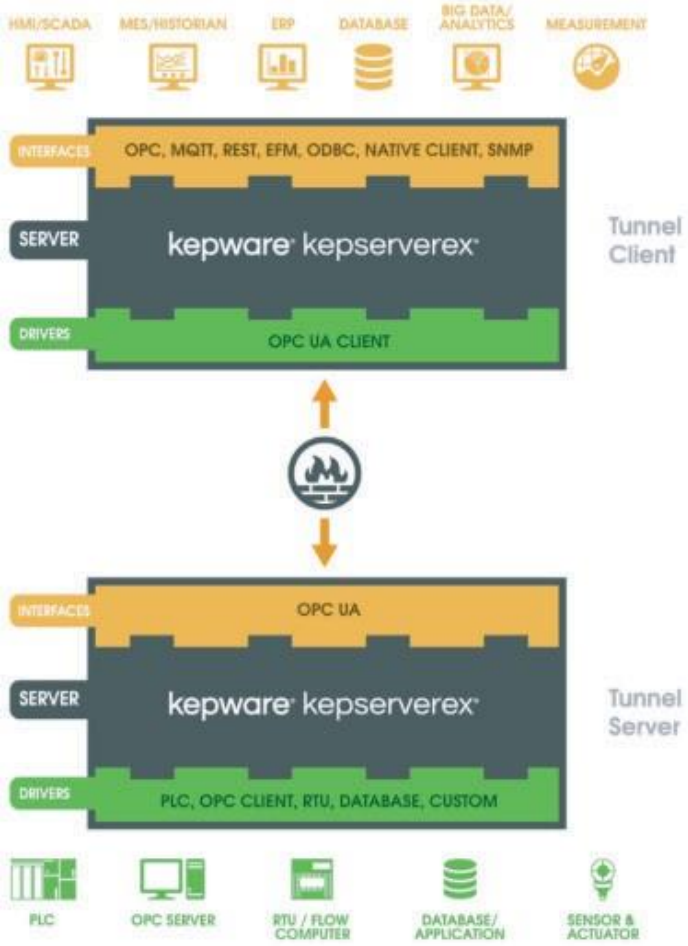
Agosto de 2018

Revisão1

Guia de comunicação via OPC UA com o KEPServerEX

Descrição geral

Este documento tem como objetivo indicar os passos necessários para estabelecer uma comunicação entre 2 KEPServerEX através da utilização do driver OPC UA Client.



Introdução

O OPC *Unified Architecture* (OPC UA) é um padrão de comunicações que se baseia na criação de um túnel através do qual os dispositivos comunicam. O OPC UA não necessita, nem de *callbacks* , nem da utilização do DCOM para efetuar ligações remotas. Além disso, simplifica significativamente a configuração da firewall, uma vez que basta criar uma exceção numa única porta.

Tunneling

O túnel utiliza uma arquitetura cliente/servidor para trocar dados em tempo real de uma forma segura e fiável através de *firewalls*, internet, *WAN*, *LAN*, *networks* e *VPNs*.

Para criar o túnel, deverá selecionar um *endpoint* que coincida, tanto com o servidor, como com o cliente.

Os *endpoints* apresentam o seguinte formato:

opc.tcp://<*IP* ou *PC name*>:49320(por defeito)

Depois de criar o *endpoint*, o passo seguinte é decidir se pretende aumentar a segurança do túnel ou não. Existem 2 tipos de segurança, uma baseada na encriptação de grelhas OPC UA e outra que consiste na autenticação de utilizadores.

Estes 2 tipos de segurança podem ser combinados das seguintes formas:

- Pode não ter segurança.
- Pode estar encriptado e sem autenticação.
- Pode estar encriptado e autenticado.
- Pode não ter encriptação, mas ter autenticação

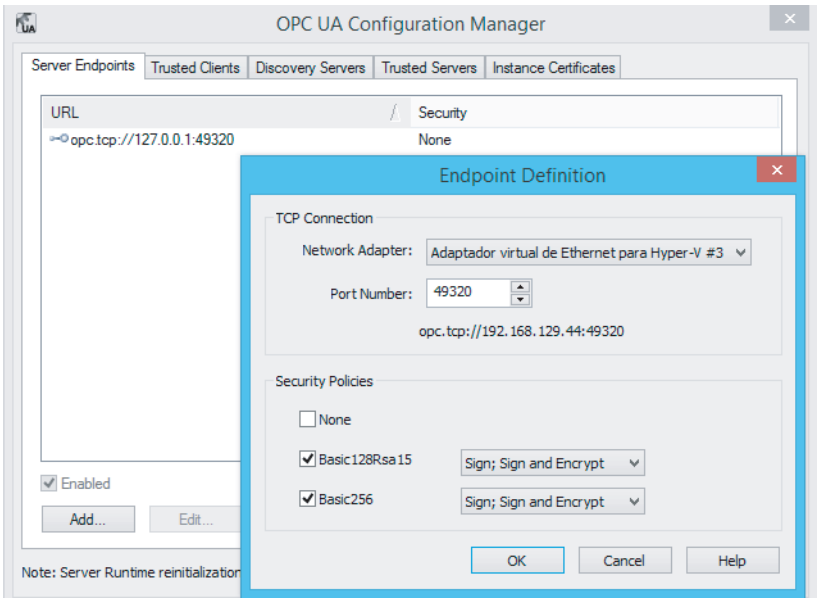
Em seguida, explicamos como poderá criar um túnel de comunicações sem segurança, com encriptação e com autenticação.

Comunicar OPC UA. Sem segurança

Antes de configurar o projeto KEPServerEX, é necessário criar o *endpoint* no servidor. Este *endpoint* deverá coincidir com o que for definido no driver OPC UA client. Para criar o endpoint:

a. Clicar com o botão direito do rato no ícone *KEPServerEX Administration* e selecionar *OPC UA Configuration*…

b. No separador *Server Endpoints*, clicar em *Add*...



c. Selecionar o cartão de rede adequado.

d. A porta 49320 está definida por defeito, mas pode ser alterada.

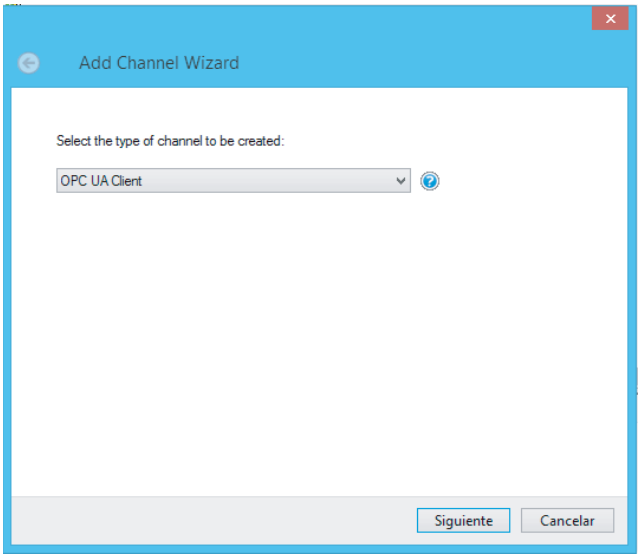
e. Selecionar *None* e desselecionar as restantes opções.

f. Para guardar a configuração, deverá parar o *Runtime* e iniciá-lo.

As propriedades da porta, tais como as *Security Policies* , devem coincidir, tanto com o *endpoint* do servidor, como com o *endpoint* definido no cliente.

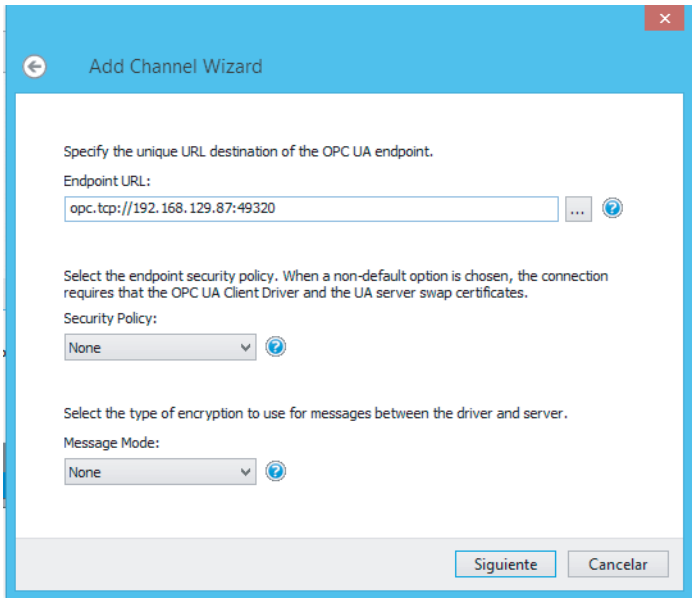
Assim que o *endpoint* estiver criado, poderá criar o projeto no KEPServerEX.

g. Adicionar um novo canal e selecionar o driver OPC UA Client.



h. Deixar todos os parâmetros por defeito em *Write Optimizations Write Optimizations, Non-Normalized Float Handling, UA Session* e *Authentication.*

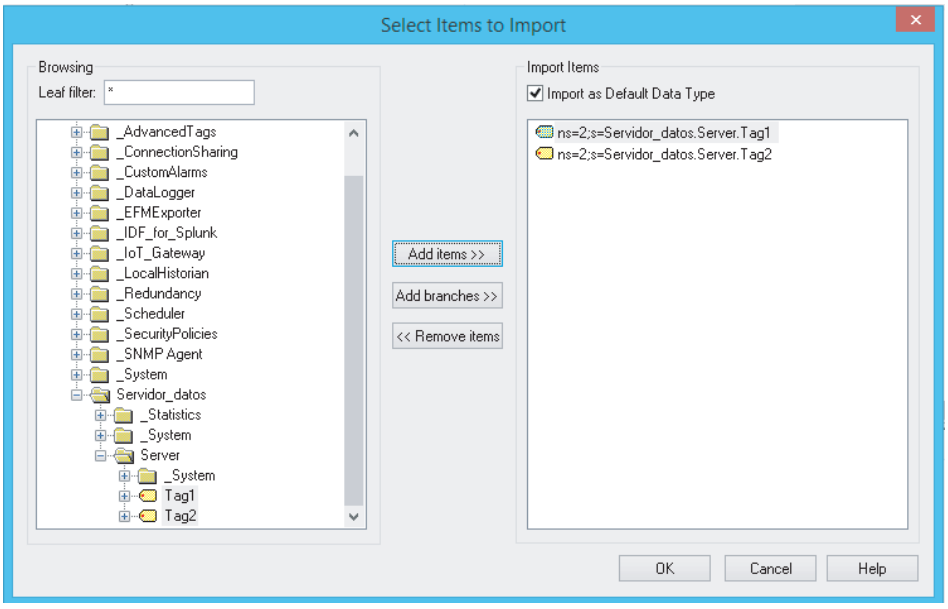
i. No separador *Endpoint url*, selecionar o *endpoint* do servidor OPC UA e em *Security Policy* selecionar *None*.



Nota: Recomendamos que configure o *endpoint* de forma manual, uma vez que ativar o navegador de servidores UA demora mais tempo, dado que é necessário ativar a porta 4840 da firewall. Além disso, não é possível efetuar o *Browse* através de VPNs.

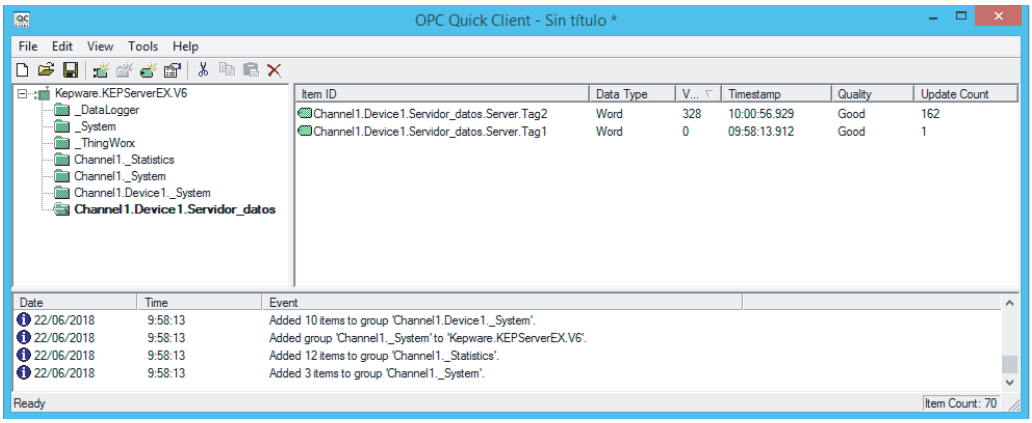
j. Adicionar um *Device* e deixar todos os parâmetros por defeito.

k. Selecionar *Select import items...*, se estiver corretamente configurado será exibida uma janela com as *tags* do servidor UA. Selecionar os itens e clicar em *Add items*>>.



Nota: Se, quando selecionar *Select import items* for exibida uma janela de erro, em vez da janela referida anteriormente, o *event logger* irá apresentar o motivo pelo qual não foi estabelecida uma ligação ao servidor OPC.

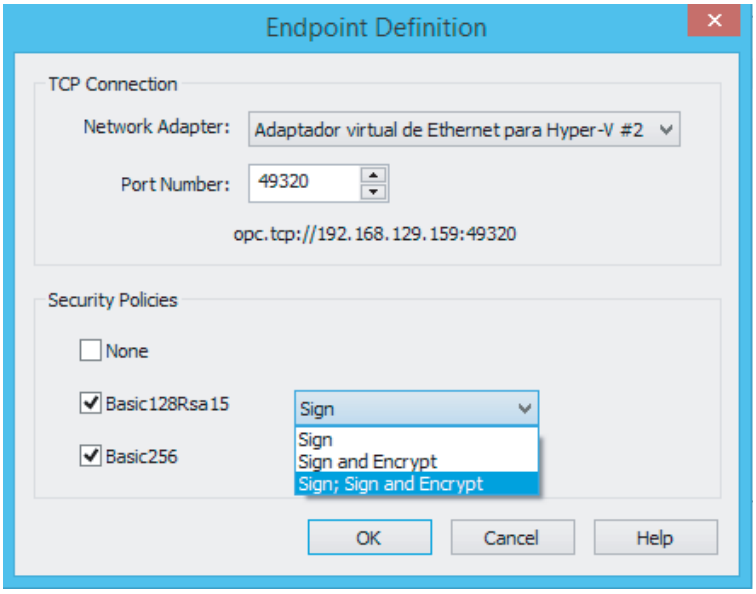
l. Para verificar se existe uma boa comunicação, abrir o QuickClient.



Comunicar OPC UA. Encriptado

Uma das características do OPC UA é a possibilidade de permitir a encriptação das comunicações entre o servidor e o cliente. Para isso, o primeiro passo consiste em atribuir segurança ao *endpoint.*

1. Nos endpoints criados, selecionar a opção *edit*. Caso não haja nenhum *endpoint* criado, siga os passos descritos na secção anterior.
2. Em *Security Policies*, selecionar as opções *Basic128Rsa15* e/ou *Basic256* e selecionar *Sign, Sign and Encrypt* ou *Sign; Sign and Encrypt.*

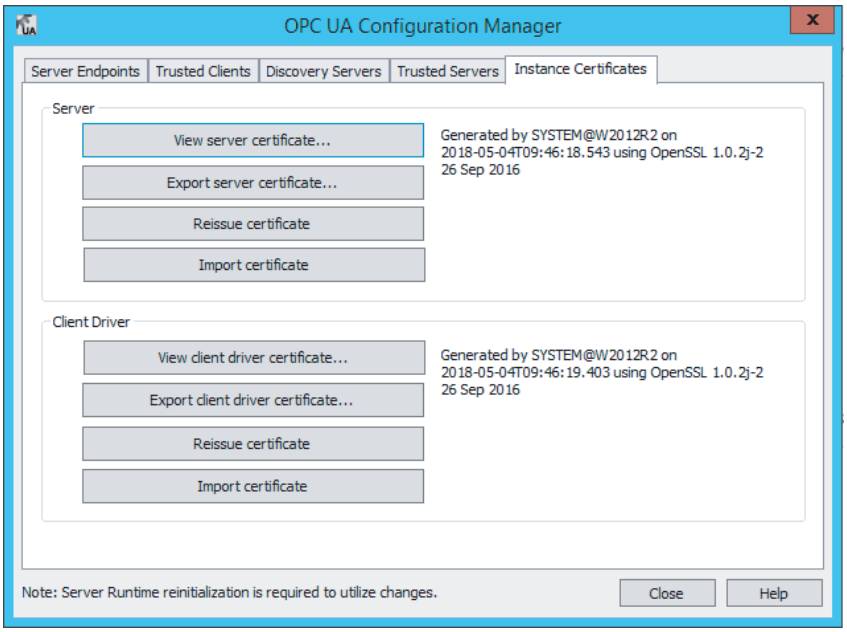


Nota: Estas opções correspondem a diferentes níveis de encriptação das mensagens.

3. Reiniciar o *runtime* para guardar a configuração do *endpoint*.

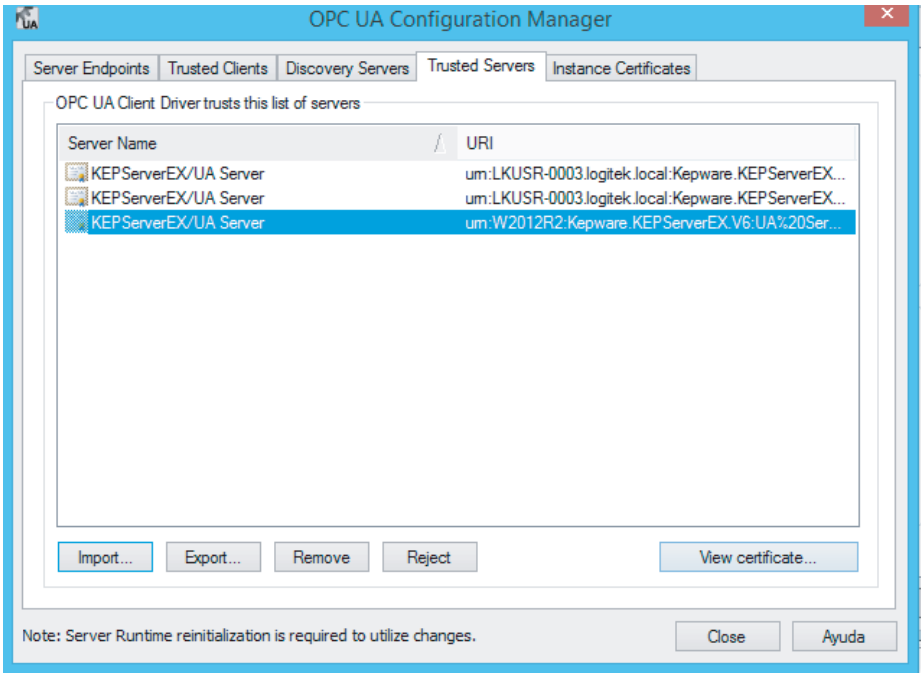
Em seguida, deverá proceder à criação dos certificados para troca posterior.

4. Nos dois KEPServerEX, ir para *OPC UA Configuration Manager* e para o separador *Instance Certificates*.

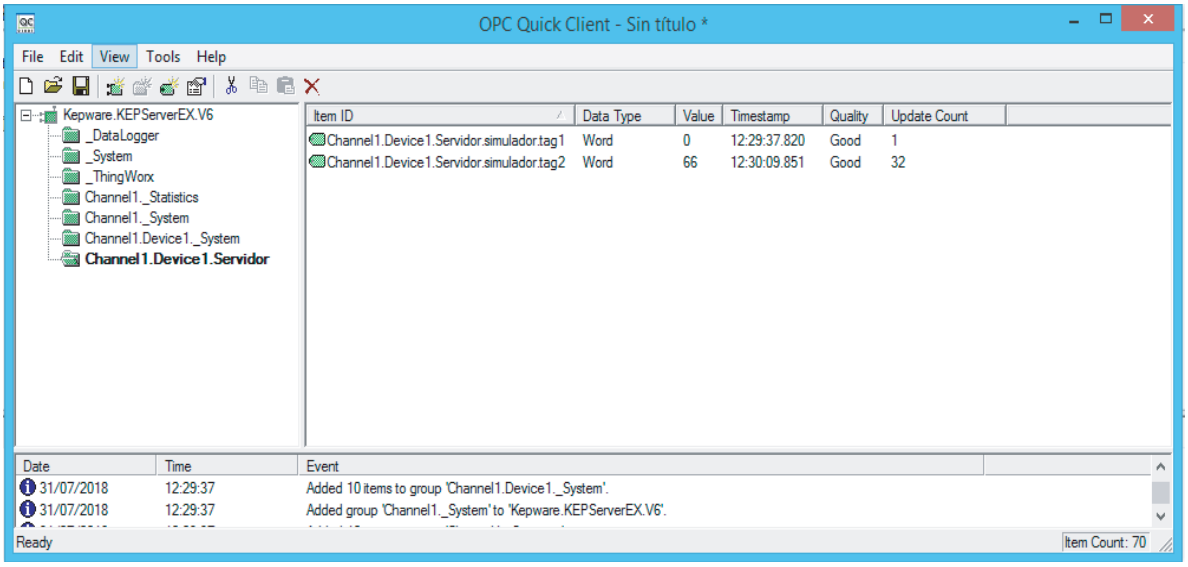


5. No KEPServerEX definido como servidor, selecionar a opção *Export server certificate…* e no KEPServerEX definido como cliente selecionar a opção *Export client driver certificate…*
6. Ao selecionar estas opções, irá criar os certificados.

   Nota: Recomendamos que altere o nome dos ficheiros, em vez de deixar o nome atribuído por defeito.
7. O certificado criado pelo servidor terá de ser enviado para a máquina do cliente, importando o ficheiro através do separador *Trusted Servers.*



8. O certificado criado pelo cliente terá de ser enviado para a máquina do servidor, importando o ficheiro através do separador *Trusted Clients.*
9. Assim que a troca de certificados estiver concluída, seguir os passos a-f e utilizar o QuickClient para verificar as comunicações.



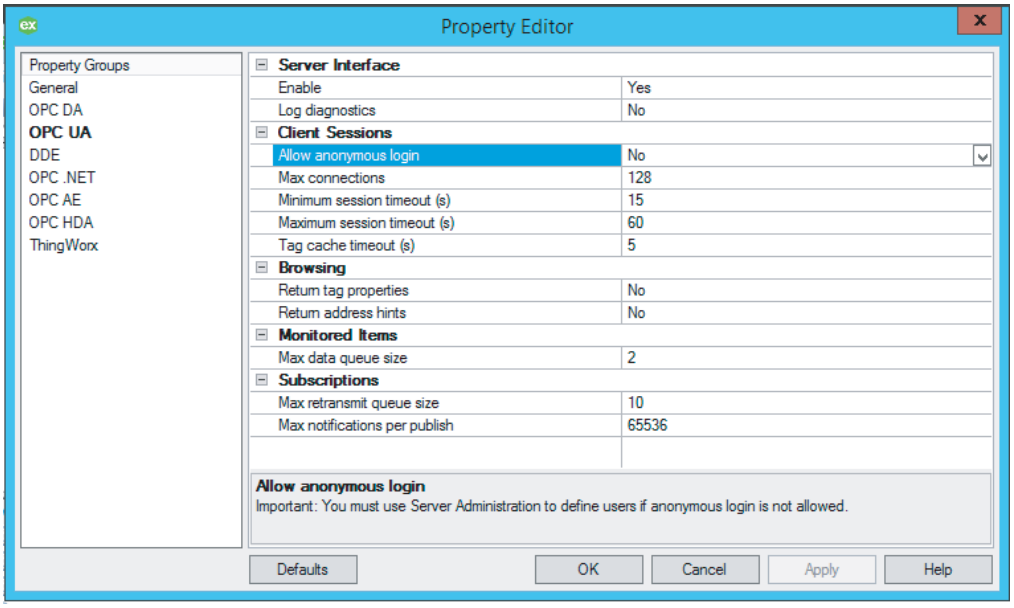
Comunicar OPC UA. Autenticação

Além da troca de certificados, para encriptar as grelhas de envio de informação, o OPC UA pode acrescentar segurança baseada na autenticação do utilizador.

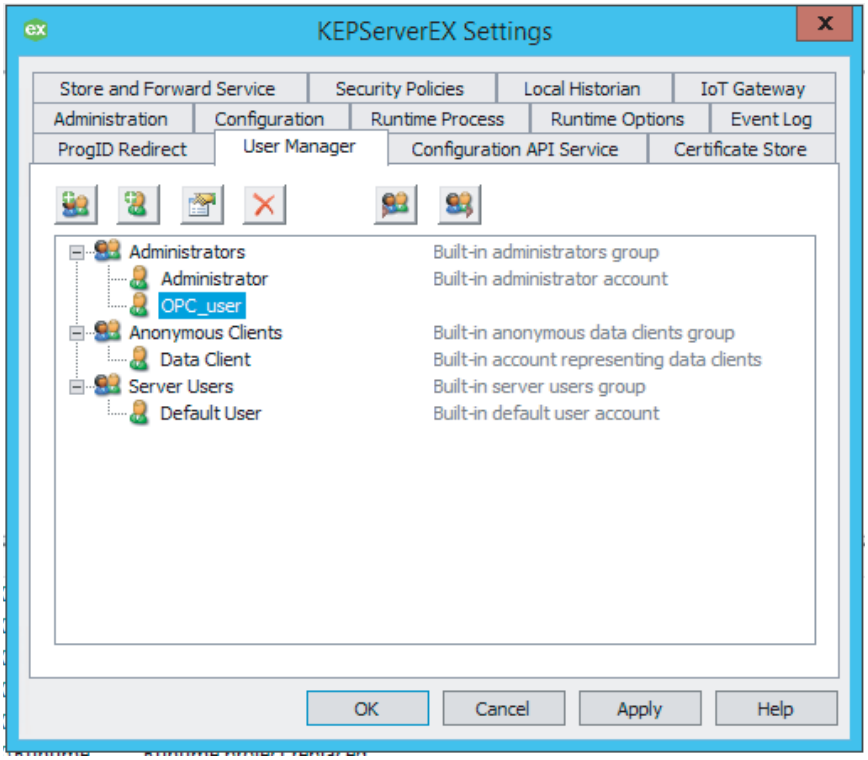
Servidor OPC UA

No KEPServerEX que funciona como servidor, deverá configurar as seguintes propriedades:

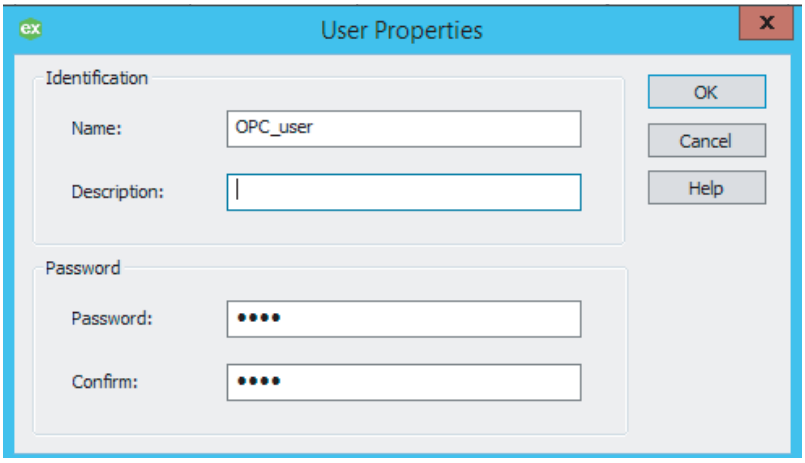
1. *Allow anonymous login*: Para aceder a esta propriedade, ir para *KEPServerEX Configuration* > *Edit* > *Properties* > OPC UA e selecionar No.



2. Criação do utilizador: Para criar o utilizador, ir para KEPServerEX Administration >Settings…> User Manager



Para criar um novo utilizador, selecionar a opção *New user*. Será exibida a seguinte janela, onde terá de definir o nome de utilizador e a respetiva palavra-passe.



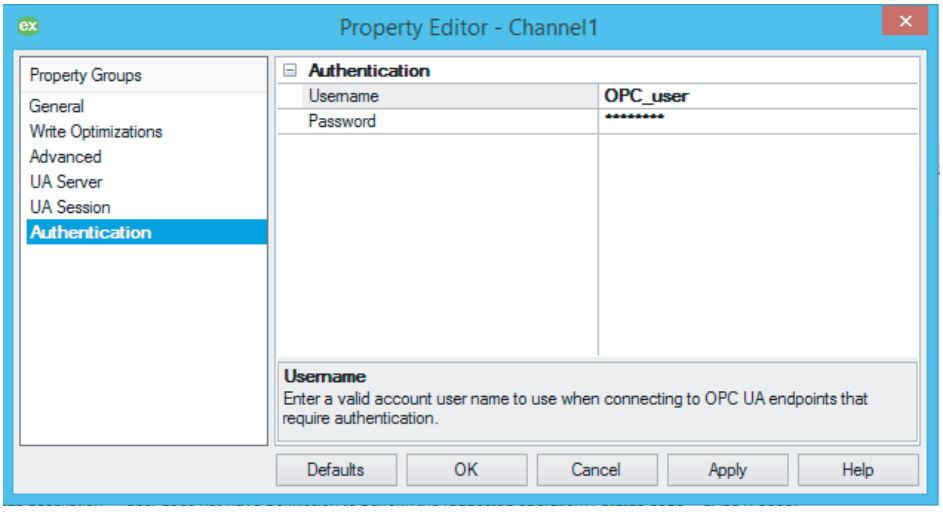
Por fim, aplique todas as alterações.

Nota: Não é necessário reiniciar o *runtime* para guardar a nova configuração.

Driver OPC UA client

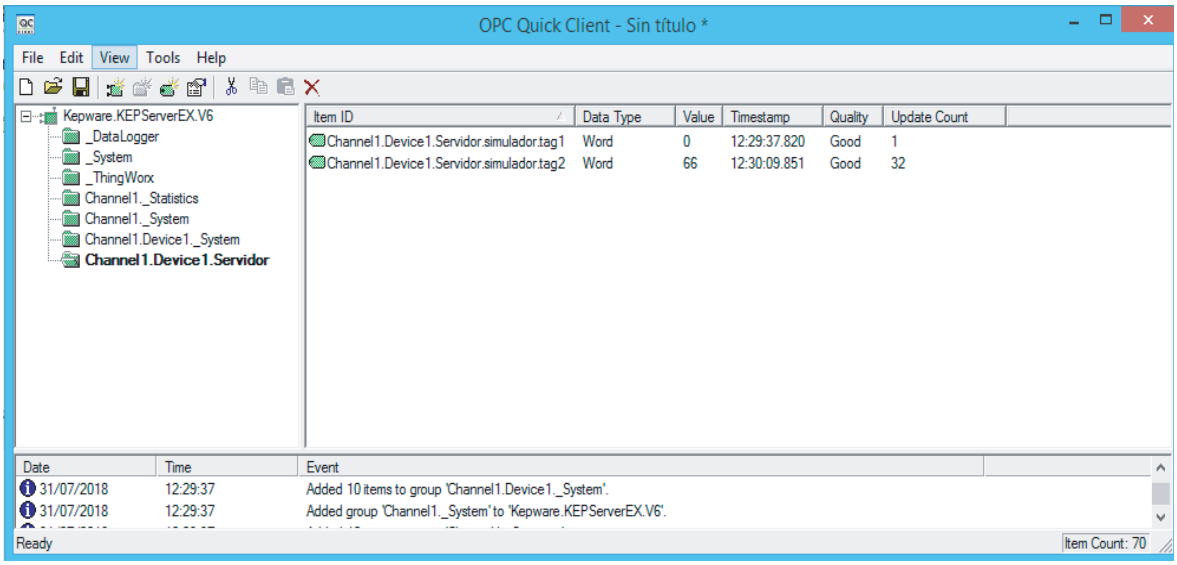
No KEPServerEX definido como cliente, criar um canal (seguindo os passos g-l).

Na propriedade do canal *Authentification*, introduzir o utilizador e a palavra-passe criados no passo anterior.



Se os utilizadores forem coincidentes, irá aparecer a seguinte mensagem: <Channel> | Channel failed to connect. | Status description = "User does not have permission to perform the requested operation.", Status code = 0X801F0000.

Por fim, utilizar o *QuickClient* para verificar se as comunicações foram estabelecidas corretamente.



Informação adicional

Nota Importante: esta Nota Técnica é entregue "as is", ou seja, como complemento à documentação do produto, estando excluída do âmbito do Apoio Técnico. Como tal, a Logitek não assume qualquer responsabilidade por eventuais problemas de funcionamento decorrentes do conteúdo da presente nota técnica.

Nota Técnica elaborada por

Mikel Carril