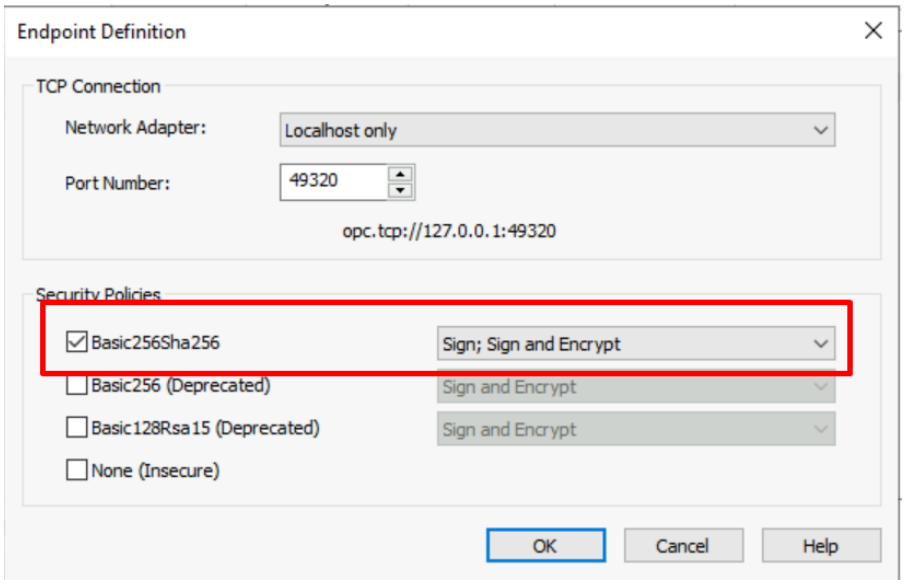
Kepware and Tulip Setup

1. Download Kepware from this Link
2. Install the latest version of Kepware
3. After Installation, search for the **OPC UA Configuration** in Windows Search Bar
4. Open OPC UA Configuration, go to the Server Endpoints and open the URL having 127.0.0.1:49320 and make the Following Configuration



5. Go to Windows Defender Firewall with Advanced Security and create a new Inbound rule with following configurations

   a. Select TCP

   b. Select Specific Local Ports 49320

   c. Select the Allow the Connection

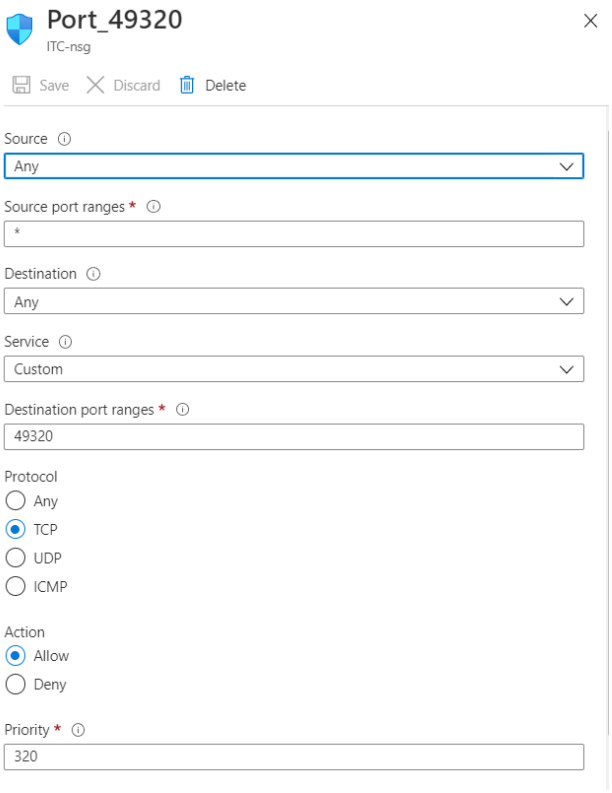
   d. Unselect Public

   e. Name it As OPC UA Server Interface (Kepware). (Optional)

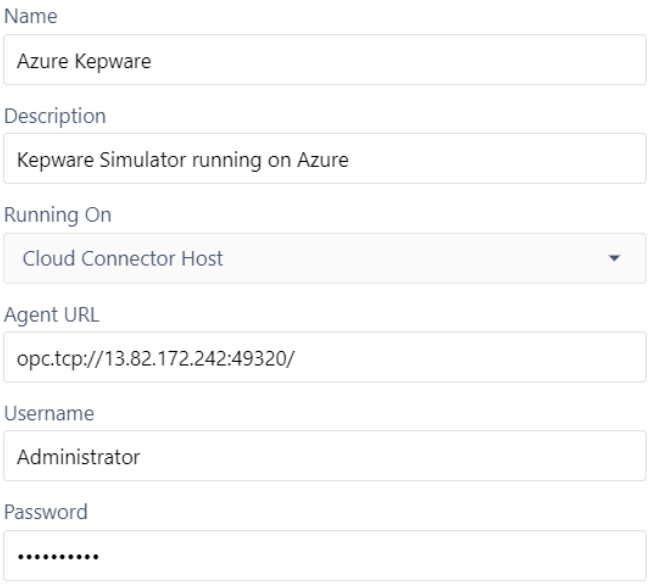
6. Create the Inbound rule for the Azure VM by going to Networking Tab as Shown below

Priority	Name	Port	Protocol	Source	Destination	Ac
300	RDP	3389	TCP	Any	Any	
310	Port_4334	4334	TCP	Any	Any	
320	Port_49320	49320	TCP	Any	Any	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	

Kepware and Tulip Setup



7. Go to Tulip Environment and go to the Shop Floor → Machines → Machine Data Sources
8. Press on **Create Connector** and type the following configurations:

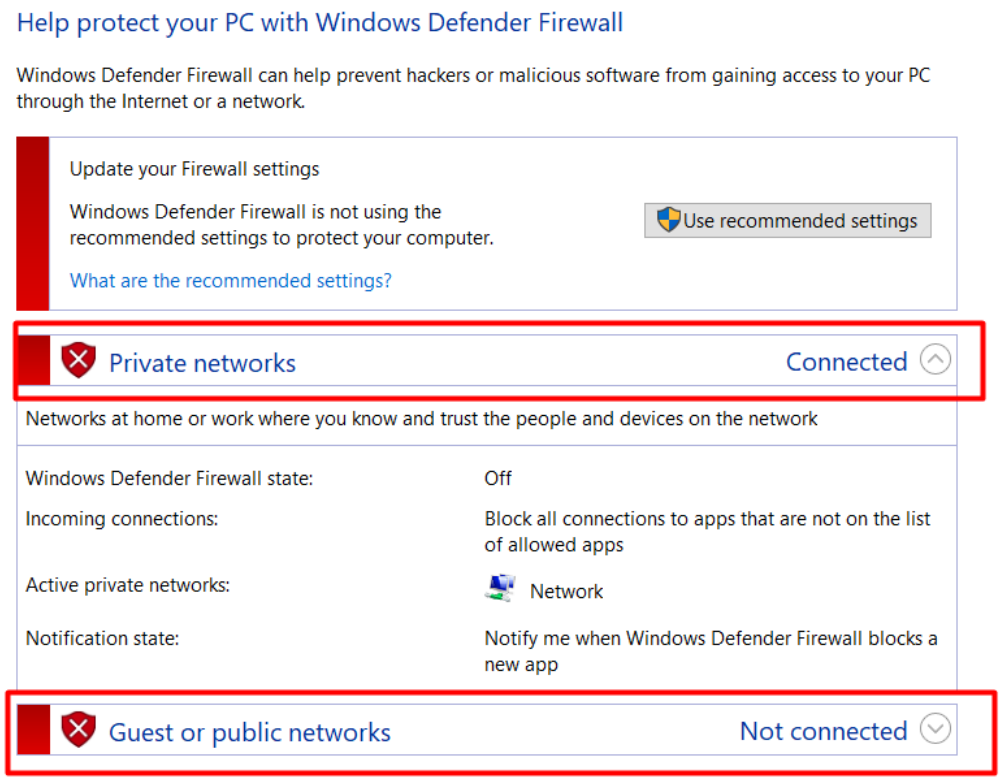


9. Press on Test, if everything goes as Documented then test gets passed and save button gets enabled.

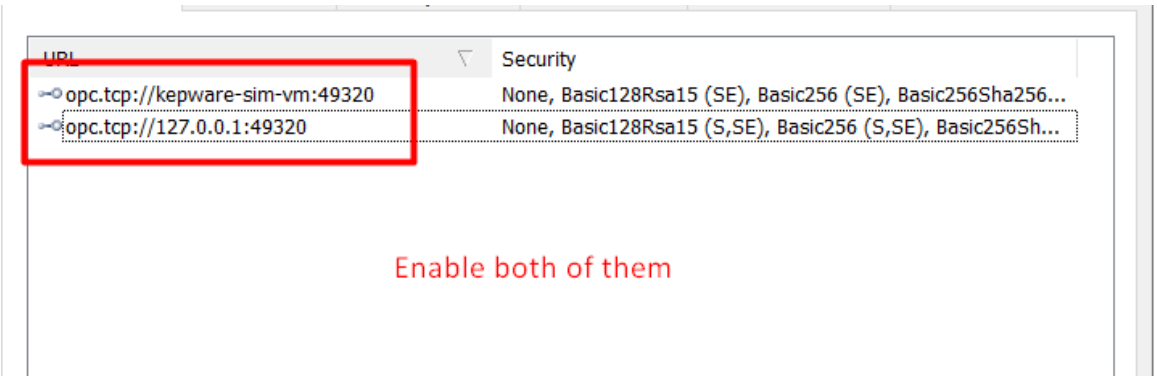
Kepware and Tulip Setup

Even after this changes the Tulip is not able to connect, then do the follow the below steps

1. Disable the Firewall in the Azure VM:

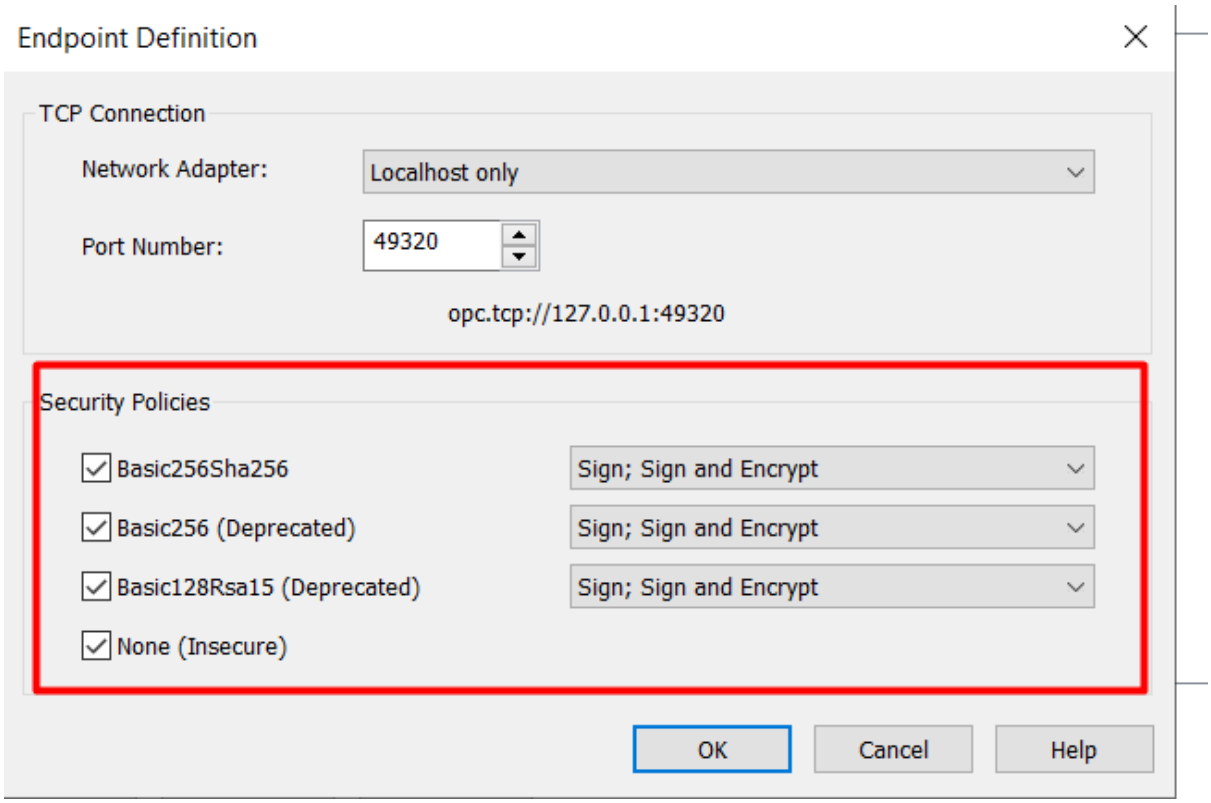


2. Enable the of the Server Endpoints in the OPC UA Configuration



Kepware and Tulip Setup

3. Enable all of the Security Policies thar are present in the Server EndPoints:



Resources:

https://www.youtube.com/watch?v=pumlhz_h0Qs