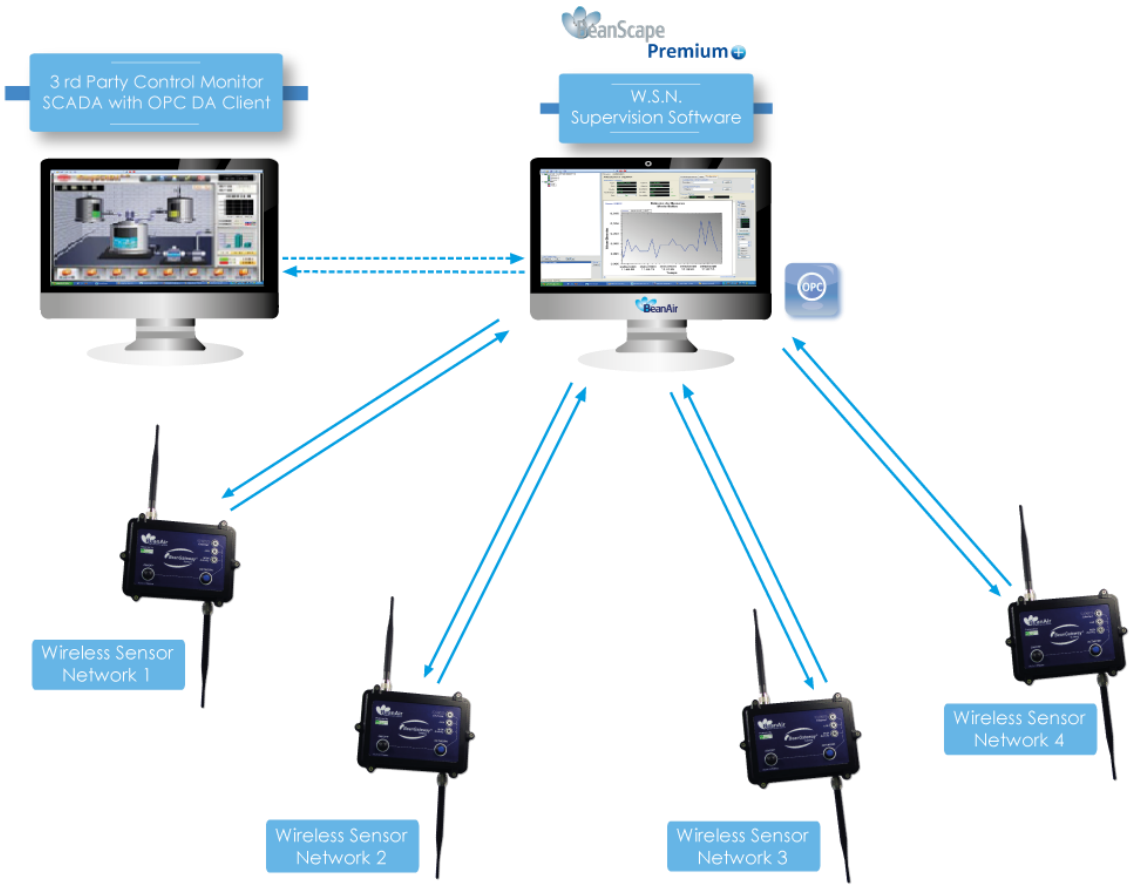
BeanAir

Version 1.1.1

USER MANUAL

OPC Server add-on (BeanScape® Premium+)



BeanAir

Rethinking Sensing Technology

2.4 GHz

DOCUMENT			
Document number		**Version**	V1.1.1
External Reference	TN_RF_013	**Publication date**	10/05/2019
Author	Fahd ESSID, Application Engineer		
Internal Reference		**Project Code**	
Document Name	OPC DCOM Configuration		

VALIDATION			
Function	**Recipients**	**For Validation**	**For information**
Reader	Damon Parsy		X
Author	Maneli Parsy	X	

MAILING LIST			
Function	**Recipients**	**For action**	**For Info**
Staffer 1	Maneli Parsy	X	
Staffer 2	Damon Parsy		X

Updates			
Version	**Date**	**Author**	**Evolution & Status**
1.0	20/02/2012	Maneli PARSY	• **First version of the document**
1.1	27/12/2018	Fahd ESSID	• **Chart update** • **Vocabulary update** • **DCOM configuration added** • **User/Group configuration added** • **Firewall configuration updated**
1.1.1	10/05/2019	Mohamed Bechir Besbes	• **Weblinks Update**

Contents

Disclaimer

The information contained in this document is the proprietary information of Beanair.

The contents are confidential and any disclosure to persons other than the officers, employees, agents or subcontractors of the owner or licensee of this document, without the prior written consent of Beanair GmbH, is strictly prohibited.

Beanair makes every effort to ensure the quality of the information it makes available. Notwithstanding the foregoing, Beanair does not make any warranty as to the information contained herein, and does not accept any liability for any injury, loss or damage of any kind incurred by use of or reliance upon the information.

Beanair disclaims any and all responsibility for the application of the devices characterized in this document, and notes that the application of the device must comply with the safety standards of the applicable country, and where applicable, with the relevant wiring rules.

Beanair reserves the right to make modifications, additions and deletions to this document due to typographical errors, inaccurate information, or improvements to programs and/or equipment at any time and without notice.

Such changes will, nevertheless be incorporated into new editions of this document.

1. TECHNICAL SUPPORT

For general contact, technical support, to report documentation errors and to order manuals, contact ***Beanair Technical Support Center*** (BTSC) at:
tech-support@Beanair.com

For detailed information about where you can buy the Beanair equipment/software or for recommendations on accessories and components visit:

www.Beanair.com

To register for product news and announcements or for product questions contact Beanair's Technical Support Center (BTSC).

Our aim is to make this user manual as helpful as possible. Please keep us informed of your comments and suggestions for improvements. Beanair appreciates feedback from the users.

2. VISUAL SYMBOLS DEFINITION

Visual	*Definition*
	***Caution or Warning** – Alerts the user with important information about Beanair wireless sensor networks (WSN), if this information is not followed, the equipment /software may fail or malfunction.*
	***Danger** – This information MUST be followed if not you may damage the equipment permanently or bodily injury may occur.*
	***Tip or Information** – Provides advice and suggestions that may be useful when installing Beanair Wireless Sensor Networks.*

3. ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
CCA	Clear Channel Assessment
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
GTS	Guaranteed Time-Slot
kSps	Kilo samples per second
LLC	Logical Link Control
LQI	Link quality indicator
LDCDA	Low duty cycle data acquisition
MAC	Media Access Control
PAN	Personal Area Network
PER	Packet error rate
RF	Radio Frequency
SD	Secure Digital
SSD	Smart shock detection
WSN	Wireless sensor Network

4. RELATED DOCUMENTS

In addition to this ***User Manual***, please consult the application notes & technical notes mentioned below:

4.1 APPLICATION NOTES

Document name (Click on the weblink)	Related product	Description
AN_RF_007 :" Beanair_WSN_Deployment"	All BeanAir products	Wireless sensor networks deployment guidelines
AN_RF_006 – „How to extend your wireless range"	All BeanAir products	A guideline very useful for extending your wireless range
AN_RF_005 – BeanGateway ® & Data Terminal Equipment Interface	BeanGateway ®	DTE interface Architecture on the BeanGateway ®
AN_RF_003 - "IEEE 802.15.4 2.4 GHz Vs 868 MHz"	All BeanAir products	Comparison between 868 MHz frequency band and a 2.4 GHz frequency band.
AN_RF_002 – "Structural Health monitoring on bridges"	All BeanAir products	The aim of this document is to overview Beanair® products suited for bridge monitoring, their deployment, as well as their capacity and limits by overviewing various Data acquisition modes available on each BeanDevice®.

4.2 TECHNICAL NOTES

Document name (Click on the weblink)	Related product	Description
TN_RF_013 – « OPC configuration »	BeanScape® Premium+	The aim of this document is to help deploying the OPC DA and all associated services.
TN_RF_012– « BeanDevice® battery life in streaming mode »	All the products	The aim of this document is to describe the autonomy performance of the BeanDevice® SmartSensor® and ProcessSensor® product line in streaming packet mode.
TN_RF_011 – « Coexistence of Beanair WSN at 2.4GHz »	All the products	This document aims to highlight the issues affecting co-existence of Beanair WSN (IEEE 802.15.4) in the presence of interference.
TN_RF_010 – « BeanDevice® Power Management »	All the BeanDevice®	This technical note describes the sleeping & active power mode on the BeanDevice®.
TN_RF_009 – « BeanGateway ® management on LAN infrastructure »	BeanGateway ®	BeanGateway ® integration on a LAN infrastructure
TN_RF_008 – "Data acquisition modes available on the BeanDevice®"	All the BeanDevice®	Data acquisition modes available on the BeanDevice®
TN_RF_007 – "BeanDevice® DataLogger User Guide "	All the BeanDevice®	This document presents the DataLogger feature on the BeanDevice®
TN_RF_006 – "WSN Association process"	All the BeanDevice®	Description of the BeanDevice® network association
TN_RF_005 – "Pulse counter & binary Data acquisition on the BeanDevice® SUN-BN"	BeanDevice® SUN-BN	This document presents Pulse counter (ex: energy metering application) and binary Data acquisition features on the BeanDevice® SUN-BN.
RF_TN_003- "Aggregation capacity of wireless sensor networks"	All the products	Network capacity characterization of Beanair Wireless Sensor Networks
RF_TN_002 V1.0 - Current consumption in active & sleeping mode	BeanDevice®	Current consumption estimation of the BeanDevice in active and sleeping mode
RF_TN_001 V1.0- Wireless range benchmarking	BeanDevice®	Wireless range benchmarking of the BeanDevice®

5. REFERENCES OF THIS DOCUMENT

The information in this document is open source and was edited from several shared experiences.

The essential reference of OPC DA is OPC foundation, you can get more information by visiting https://opcfoundation.org/.

6. DCOM OVERVIEW

The purpose of this document is to provide information to quickly establish a secure DCOM connection between an OPC server and a client running Microsoft Windows 7 or later.

6.1 WHAT IS DCOM?

Distributed Component Object Model (DCOM) is an extension of Component Object Model (COM) that allows COM components to communicate among objects on different computers. DCOM uses Remote Procedure Call (RPC) to generate standard packets that can be shared across a network, which in turn allows COM to communicate beyond the boundaries of the local machine.

Because DCOM poses a security threat, care should be taken to not expose more than what is required for the application. Although multiple security layers exist, it is still possible that some part of the system will be compromised.

6.2 WHAT IS OPCENUM?

The OPC server stores OPC specific information in the registry. Since OPC clients need to be able to discover servers running on both the same machine and remote machines, there needs to be a standard method for accessing this registry information (which is not available for remote access). To do so, a component called OPCEnum is provided by the OPC Foundation. OPCEnum is an executable that is typically installed on a computer along with the OPC server. It runs as a System service and provides a means to browse the local machine for OPC servers and then expose the list to the OPC client.

7. USERS AND GROUPS

To ensure that an OPC connection is secure, create users and groups exclusively for this purpose. These can be added manually by any user with the appropriate credentials.

7.1 DOMAINS AND WORKGROUPS

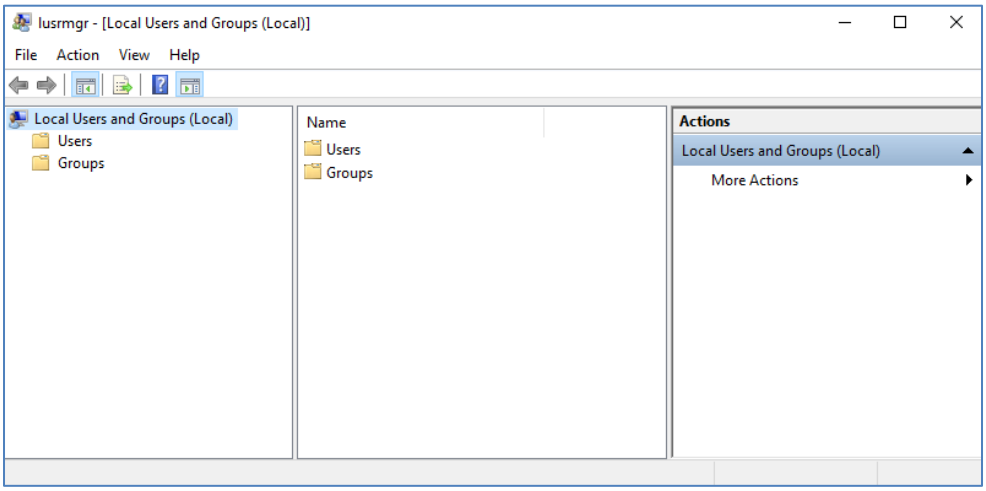
When working in a workgroup, each user must be created locally on each computer involved in the connection. In addition, each user account must have the same password for authentication to take place. An empty password is not valid in most cases. Because there may be changes to the local security policy on each computer, remote connectivity within a workgroup is potentially the least secure connection.

When working in a domain, local users and groups do not need to be added to each computer. A domain uses a central database that contains user accounts and security information. If you prefer to work in a domain, a network administrator may need to implement the changes.

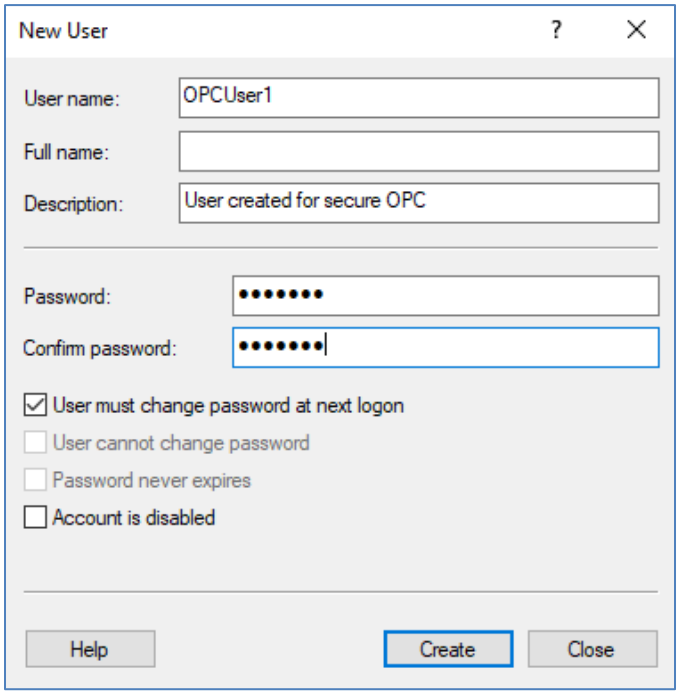
To mix domains and workgroups, both computers will need to authenticate with the smaller of the two options. This means that the domain computer will require the same configuration as if it were on a workgroup. Local user accounts must be added to the domain computer.

7.2 ADDING A LOCAL USER

1. Launch the **Local User and Groups** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start** | **Run** and then typing "lusrmgr.msc".



2. Next, click **Users**. Then, select **Action** | **New User.**



3. Type the appropriate information in the dialog box.

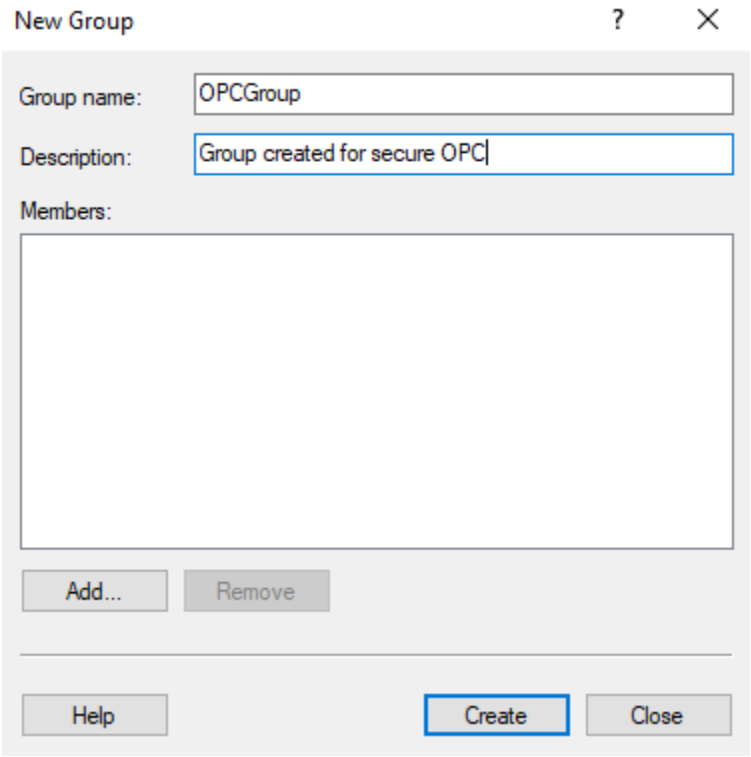
4. Change the following options as required:
   - **User must change password at next logon**
   - **User cannot change password**
   - **Password never expires**
   - **Account is disabled**

5. Click **Create**. Then, click **Close.**

7.3 ADDING A LOCAL GROUP

1. Launch the **Local User and Groups** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start** | **Run** and then typing "lusrmgr.msc".

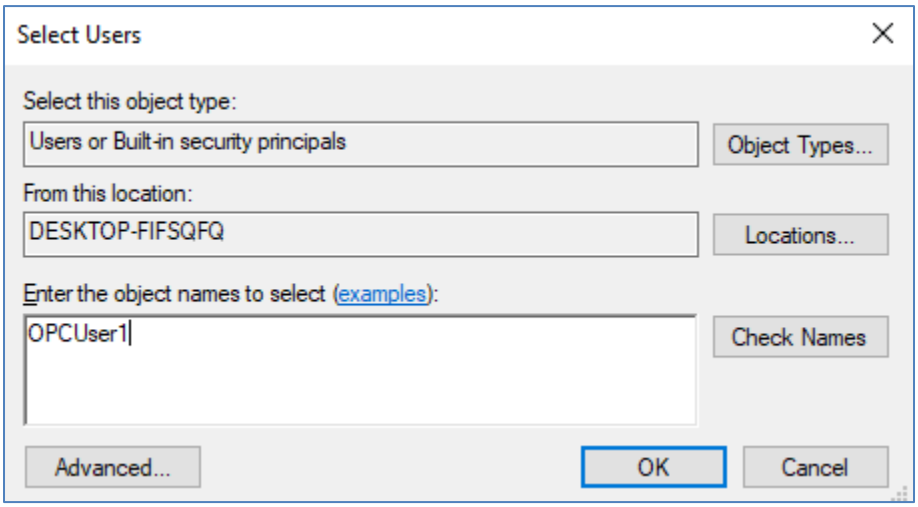
2. Click **Groups** and then select **Action** | **New Group**.



3. In **Group name**, type a name for the new group.
4. In **Description**, type a description of the new group.
5. Click **Create** and then click **Close**.

7.4 ADDING USERS TO A GROUP

1. Launch the **Local User and Groups** snap-in.
2. Next, select **Groups**. Then, right-click on the group in which a member will be added and point to **All Tasks**. Click **Add to Group** | **Add**.



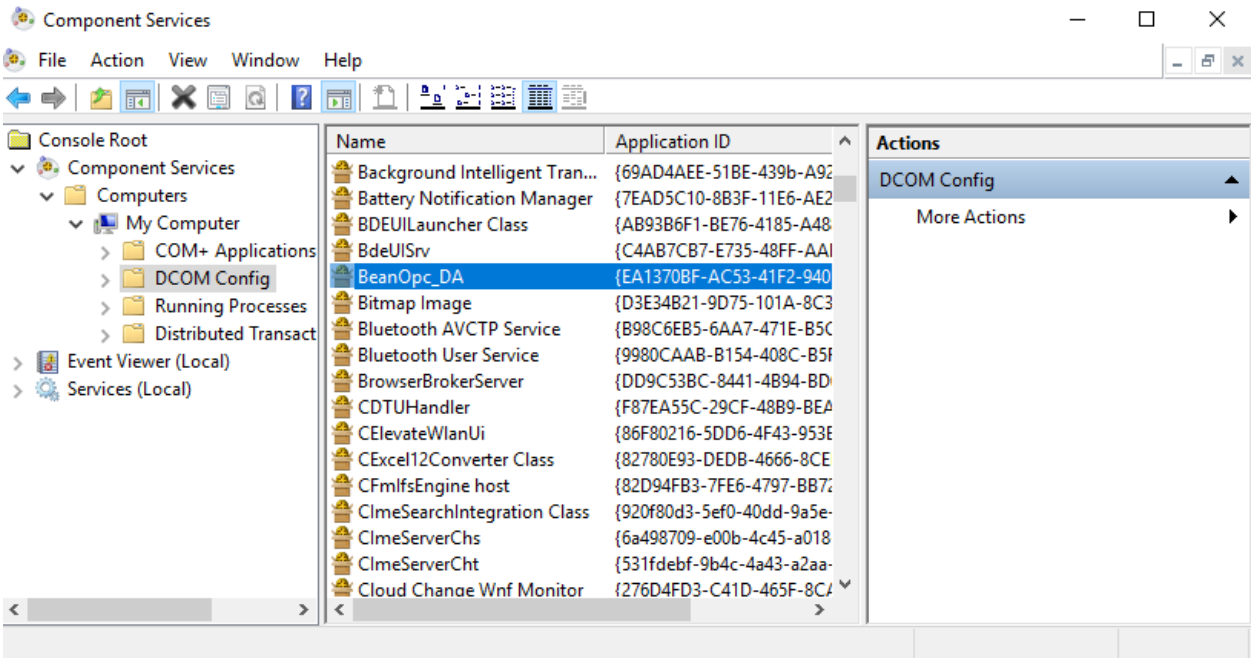
3. In **Object Types**, select the types of objects to find.
4. In **Locations**, click the domain or the computer that contains the users to add. Then, click **OK**.
5. Type the name of the user or group that will be added to the group and then click **OK.** To validate the user or group names being added, click **Check Names.**

8. DCOM CONFIGURATION

The computer running the OPC server must make changes to the application and system levels in order to setup DCOM correctly.

8.1 CONFIGURING THE APPLICATION

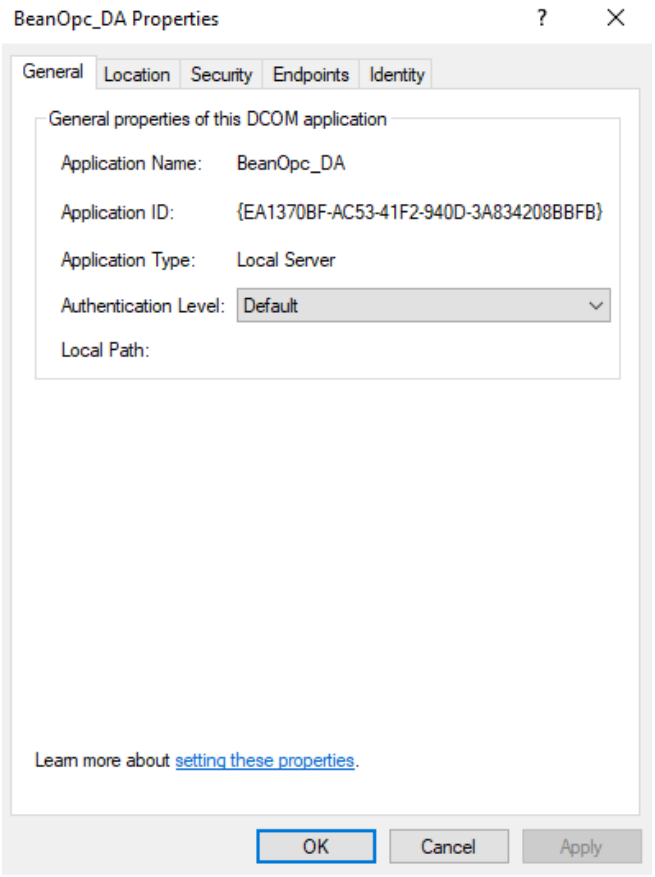
1. Launch the **Component Services** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start** | **Run** and then typing "dcomcnfg".
2. Under **Console Root**, expand **Component Services**, **Computers**, **My Computer** and **DCOM Config**.



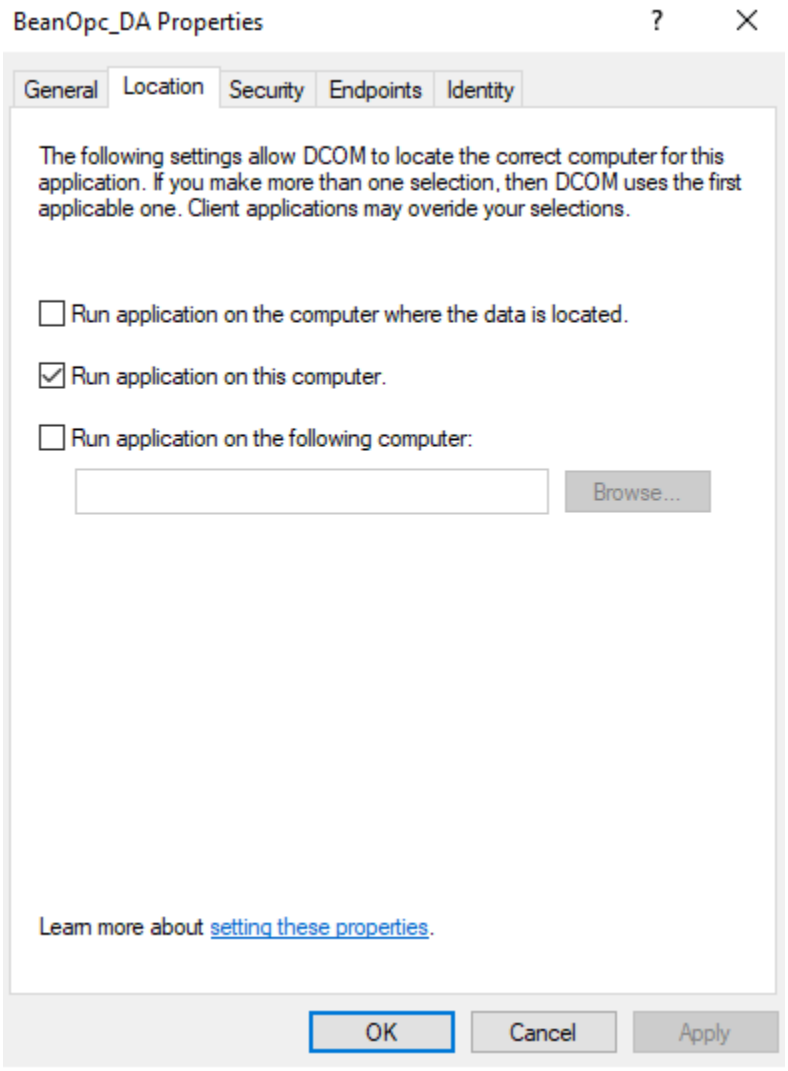
3. Browse the DCOM enabled objects until the OPC server "BeanOpc_DA" application is located.

4. Right-click on the server application and select **Properties**.

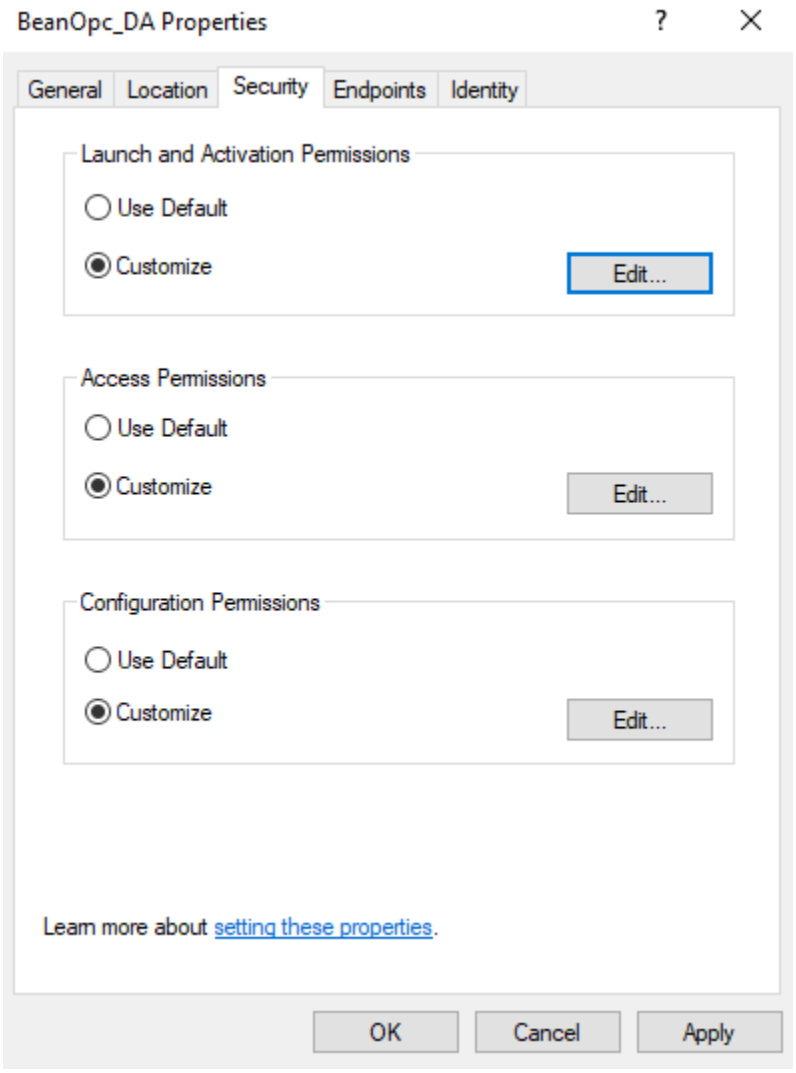
5. Open the **General** tab. Then, verify that the **Authentication Level** is set to **Default.**



6. Open the **Location** tab. Then, verify that only the **Run application on this computer** option is enabled.



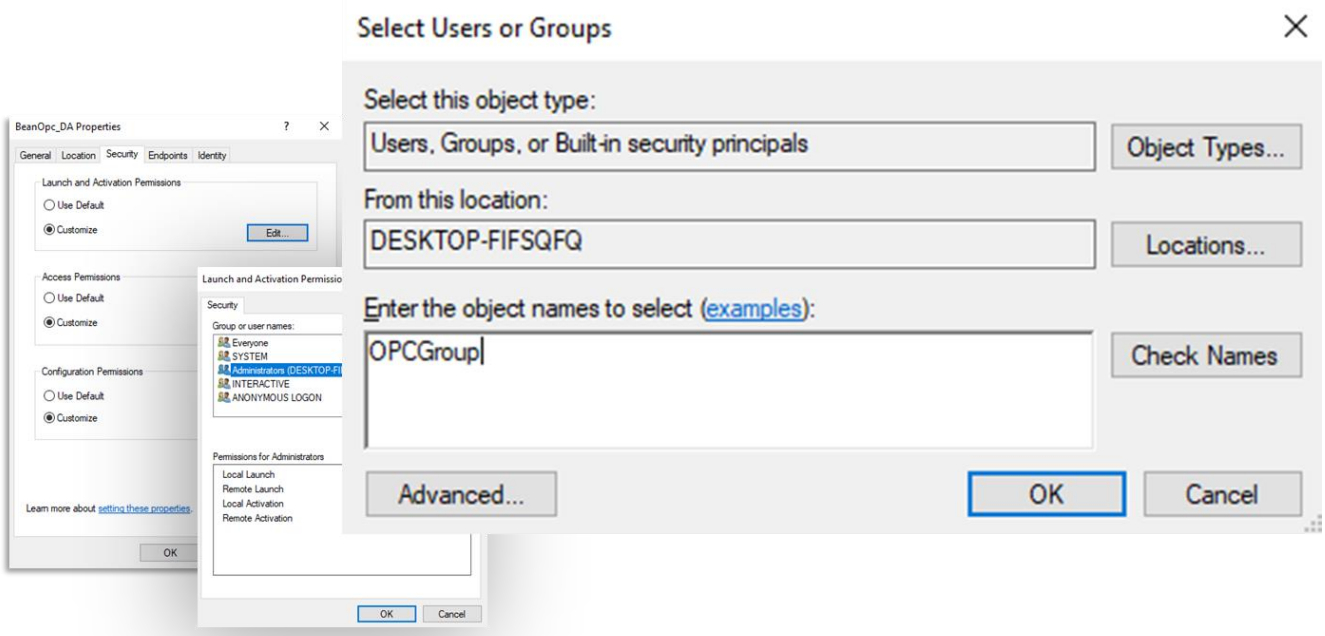
7. Open the **Security** tab.



8. In **Launch and Activation Permissions**, select **Customize**. Here, users and groups can be granted permission to start the OPC server if it is not already running.

9. Click **Edit.**

10. In **Launch and Activation Permissions**, select **Add**.



11. In **Object Types**, select the desired object type.

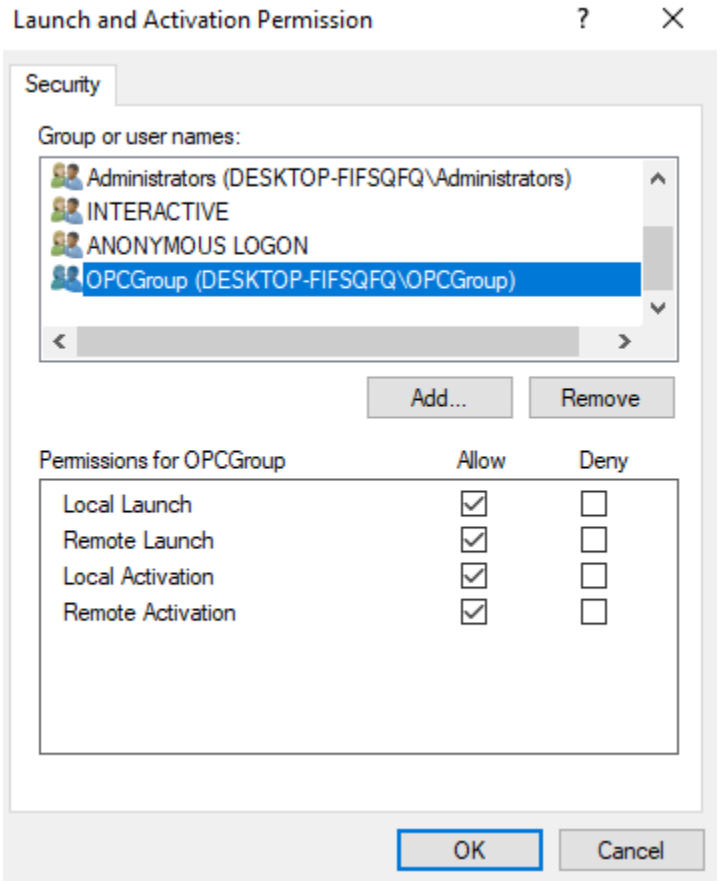
12. In **Locations**, click the domain or the computer that contains the users or groups that will be added. Then, click **OK**.

13. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.

14. After the account has been validated, click **OK**.

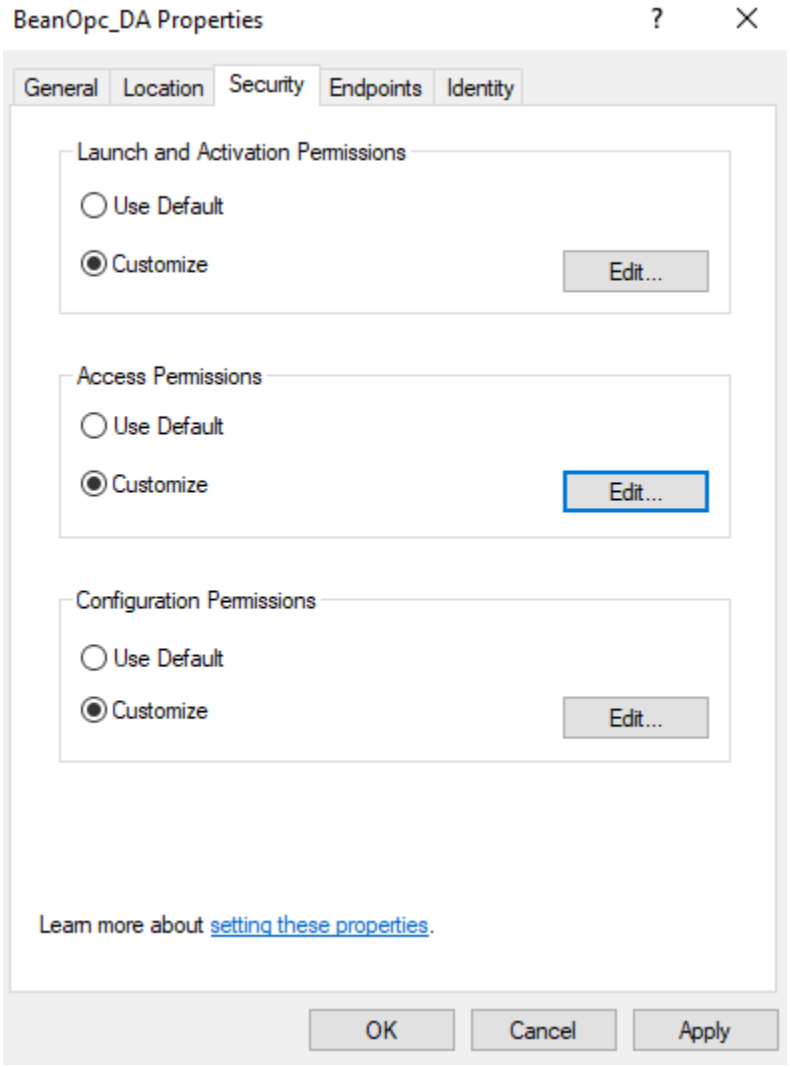
15. Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the **Group or user names** list.

16. Next, select the new user or group.



17. To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.

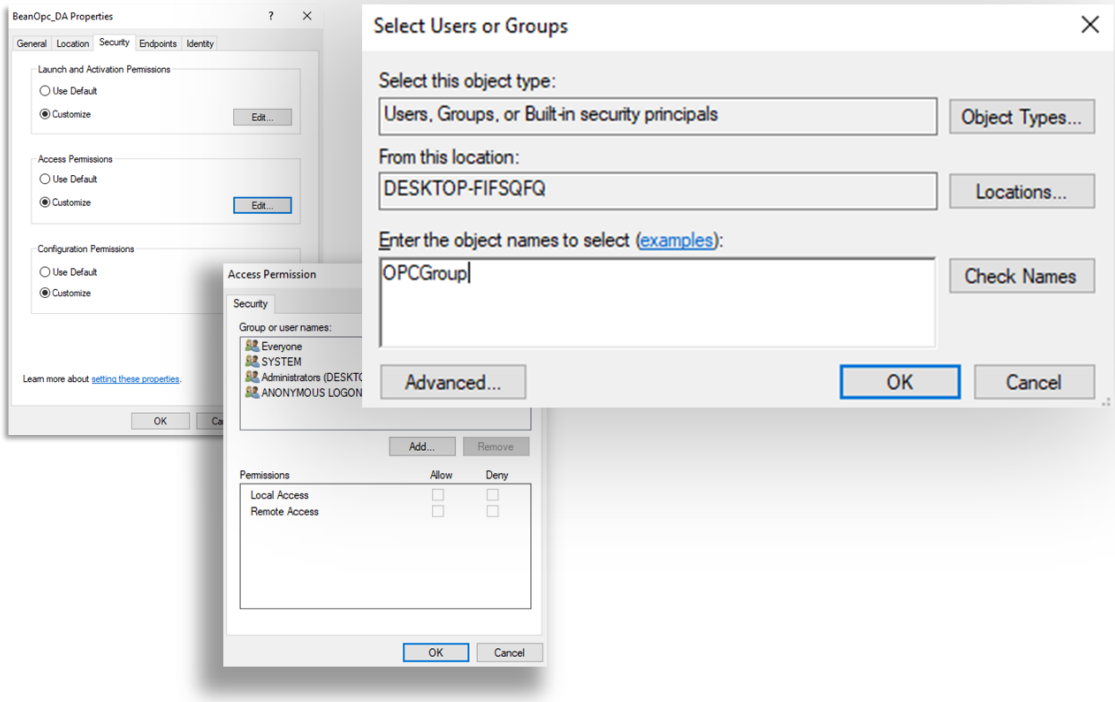
18. Repeat the process for all accounts that have been added. Then, click **OK**.



19. Select **Customize** in the **Access Permissions** group. Here, users and groups can be granted permissions to make calls to the OPC server. These calls include browsing for items, adding groups and items, or any other standard OPC call.

20. Click **Edit**.

21. In **Access Permissions**, select **Add**.



22. In **Object Types**, select the desired object type.

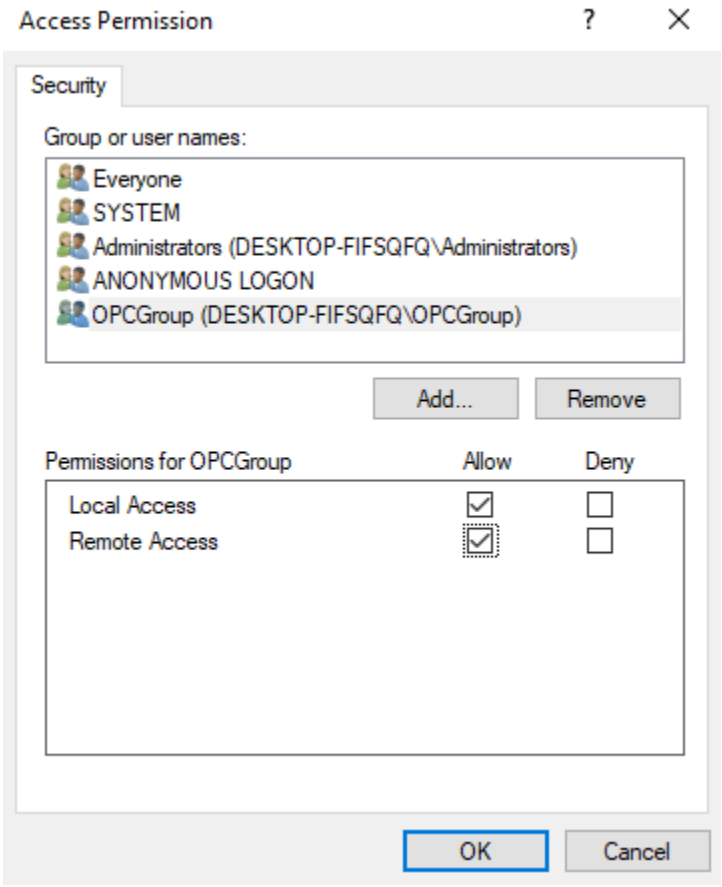
23. In **Locations**, click the domain or the computer that contains the users or groups that will be added. Then, click **OK**.

24. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.

25. After the account has been validated, click **OK**.

26. Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the **Group or user names** list.

27. Select the new user or group.



28. To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.
29. Repeat the process for all accounts that have been added. Then, click **OK**.
30. Click **OK** to close the **Application Properties** window.

8.2 CONFIGURING THE APPLICATION IDENTITY (OPTIONAL)

The **Identity** needs to be set when the process mode is set to Interactive and one of the following conditions is present:

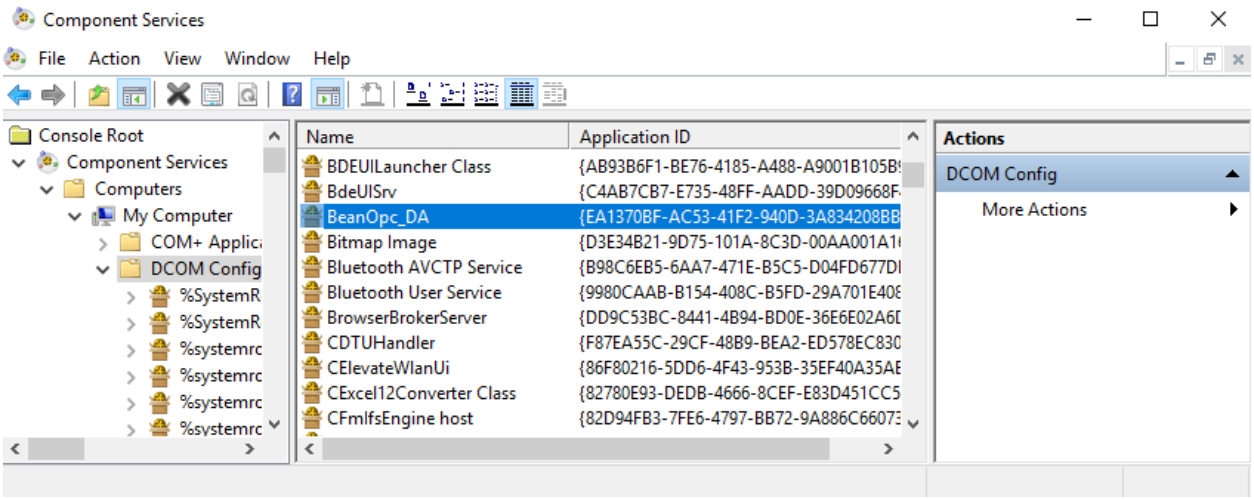
- The computer that is being used as the server is required to run with multiple user accounts.
- Users that have not been granted DCOM permissions will be using the computer.

Setting the Identity to **This user** allows a specific user account to be selected to run the application. Clients are then directed to the account allowing a connection to be made to the server. The specified user is not required to be logged on to the Windows operating system in order for this to happen.

Note: In this case, the specified user must be part of the Administrators group.

If not, the server will not start.

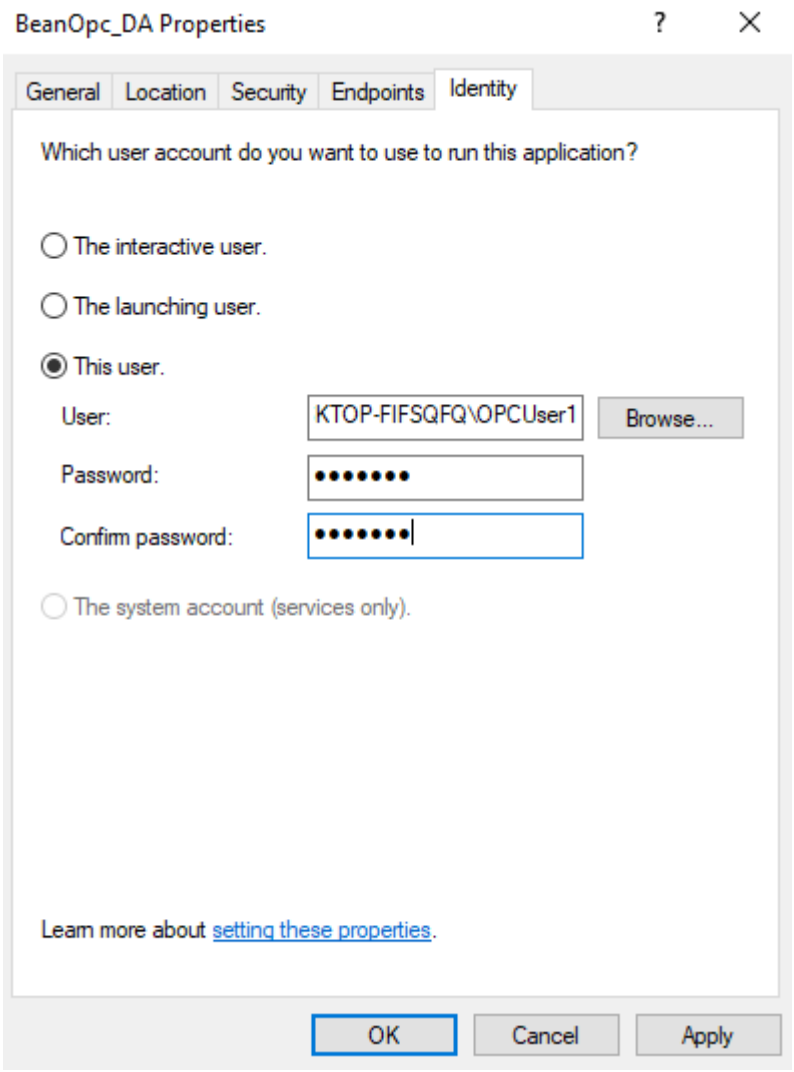
1. Launch the **Component Services** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start** | **Run** and then typing "dcomcnfg".
2. Under **Console Root**, expand **Component Services**, **Computers**, **My Computer** and **DCOM Config**.



3. Browse the DCOM enabled objects until the OPC server "BeanOpc_DA" application is located.

4. Right-click on the server application and then select **Properties**.

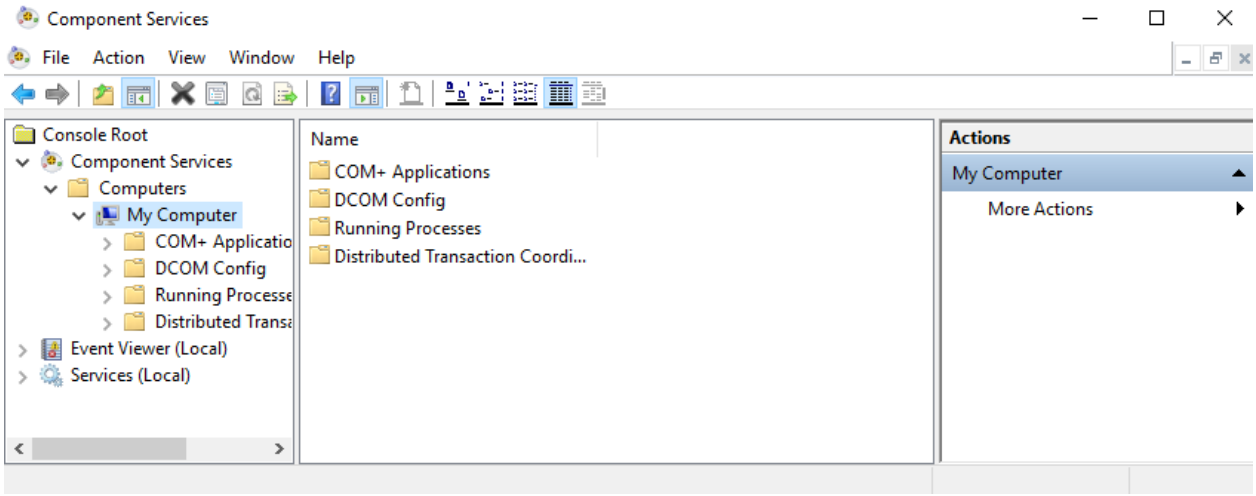
5. Next, select the **Identity** tab.



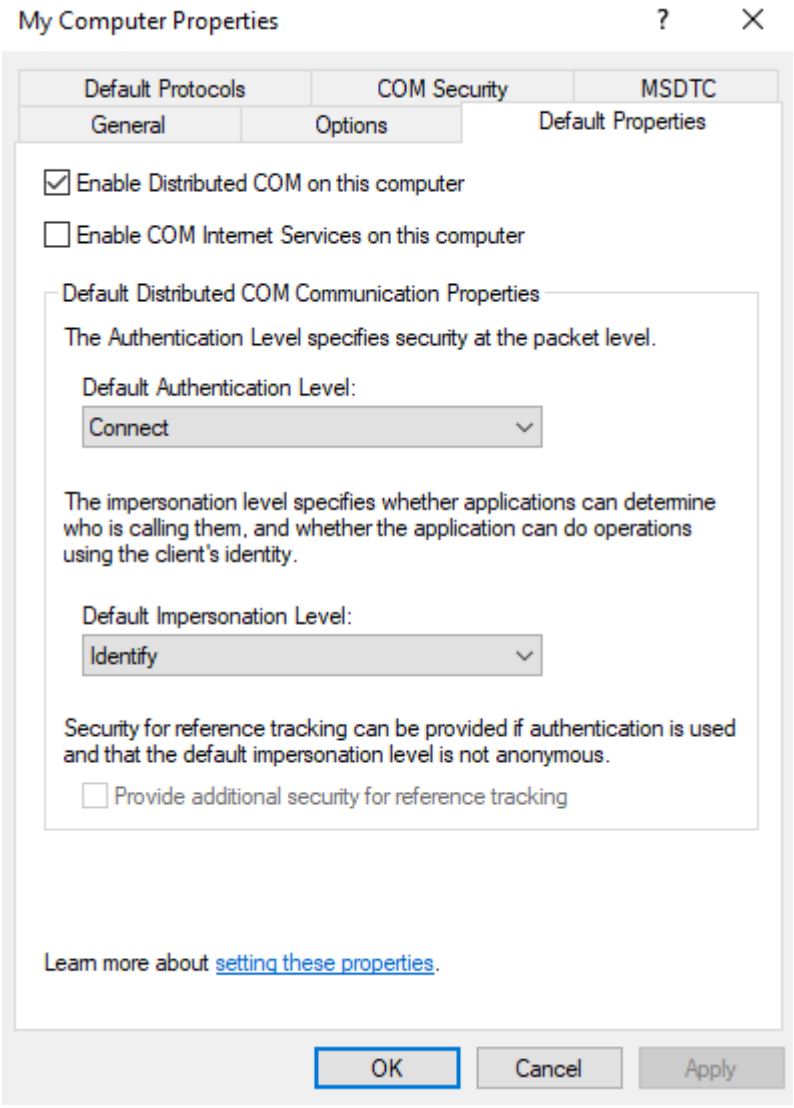
6. Enter the user name or click **Browse** to launch the **Select User** dialog to assist in selecting a valid user name.
7. Enter and confirm the password of the user that has been chosen to run the server application.
8. Select **OK** to close the **Server Properties**.

8.3 CONFIGURING THE SYSTEM

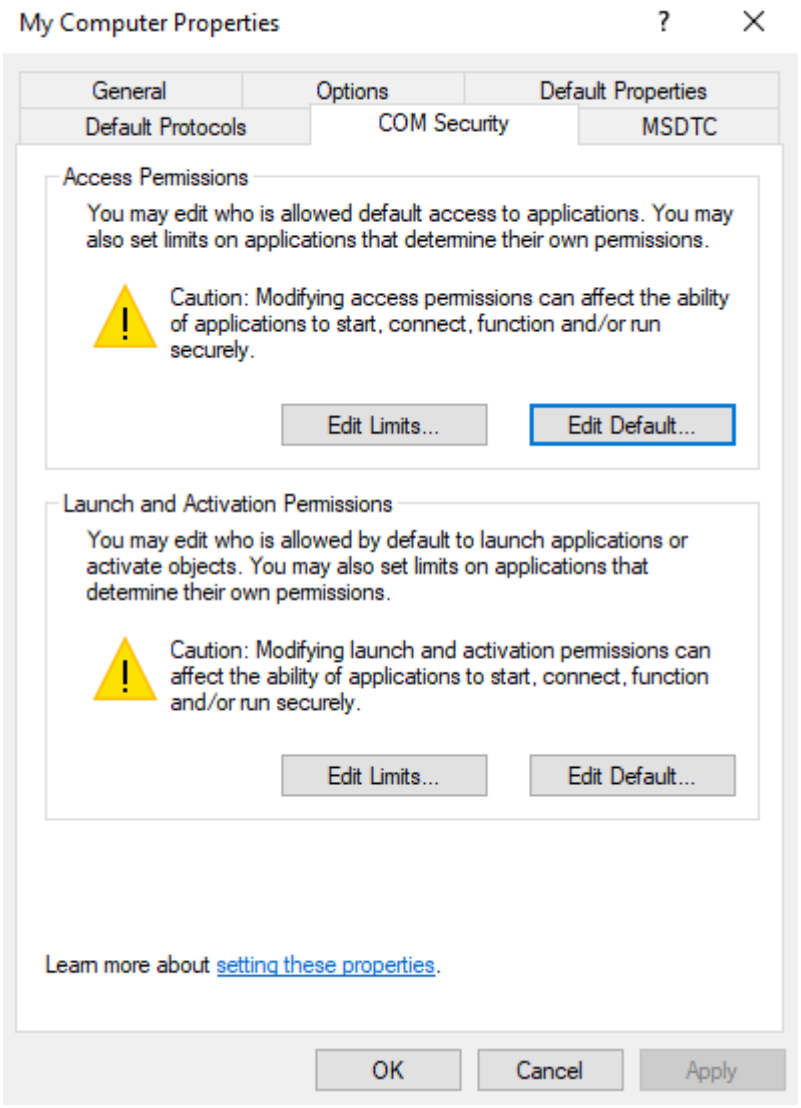
1. Launch the **Component Services** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start** | **Run** and then typing "dcomcnfg".
2. Under **Console Root**, expand **Component Services** and **Computers**.



3. Right-click on **My Computer** and then select **Properties**.
4. Next, select the **Default Properties** tab.

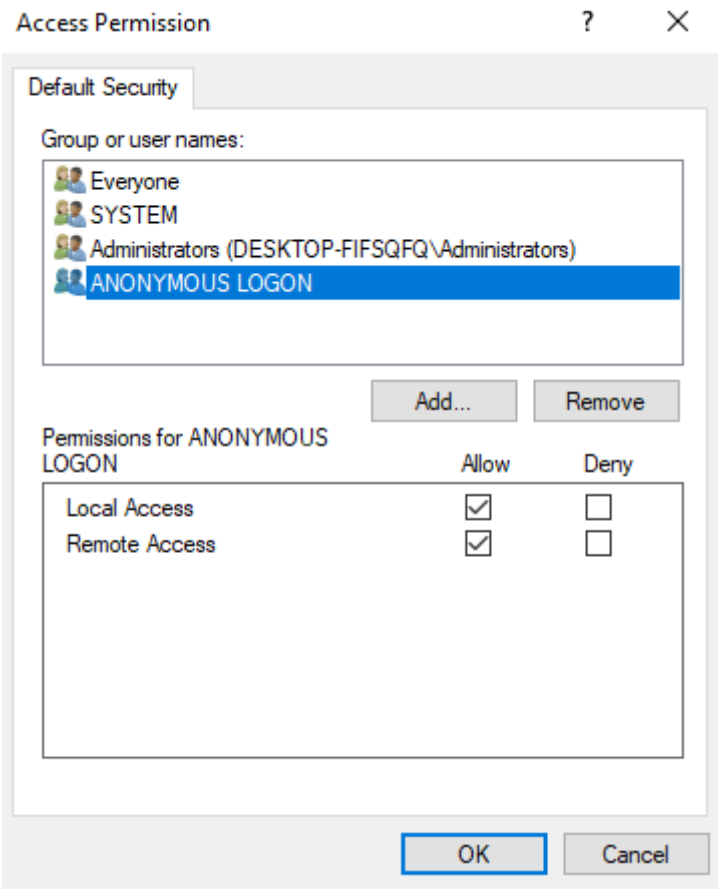


5. Verify that the **Enable Distributed COM on this computer** option is enabled.
6. Select **Connect** for the **Default Authentication Level**.
7. Select **Identify** for the **Default Impersonation Level**.
8. Next, select the **COM Security** tab.



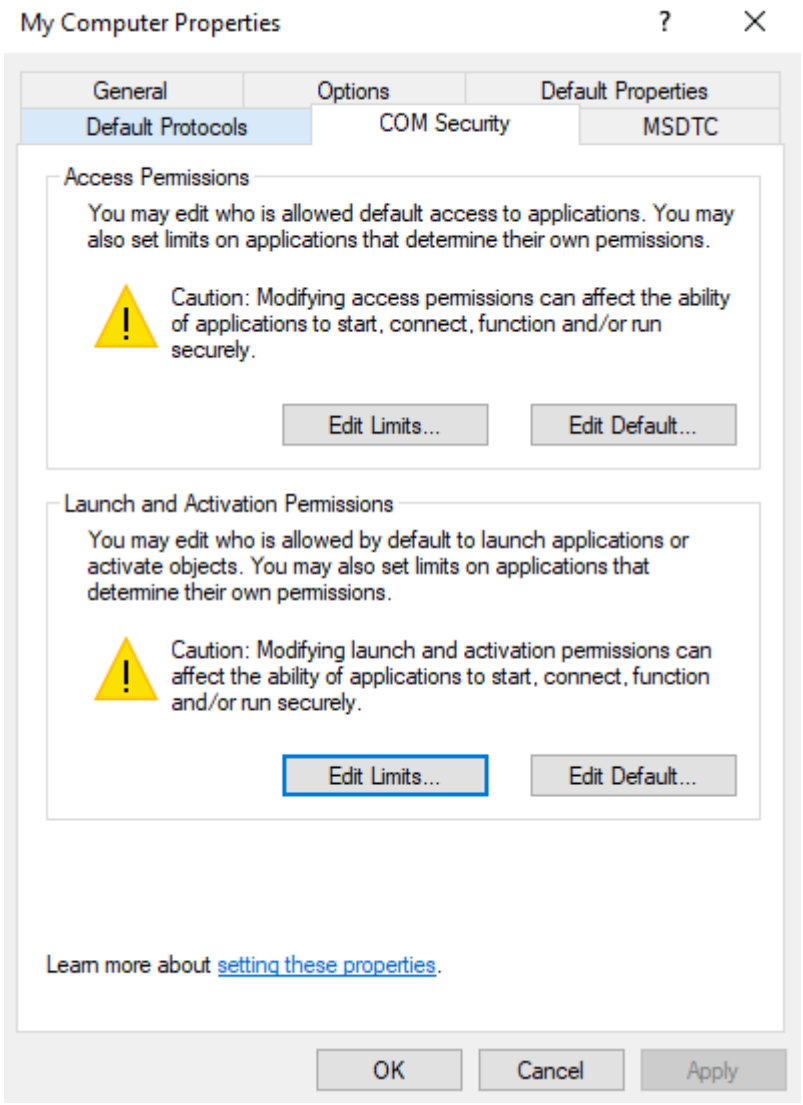
9. Select **Edit Limits** in the **Access Permissions** group.

10. Select the **ANONYMOUS LOGON** group account in the **Group or user names** list.

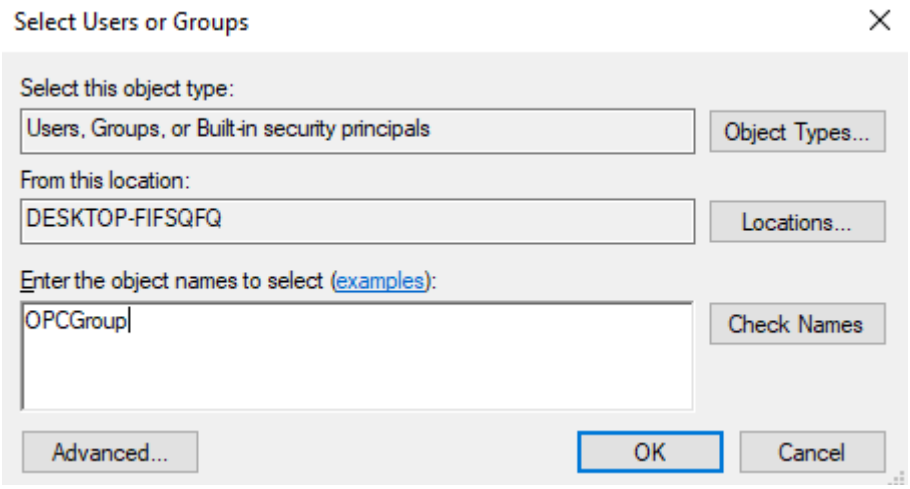


11. Enable the local and remote permissions for this group. OPCEnum overrides DCOM settings and opens accessibility to everyone.

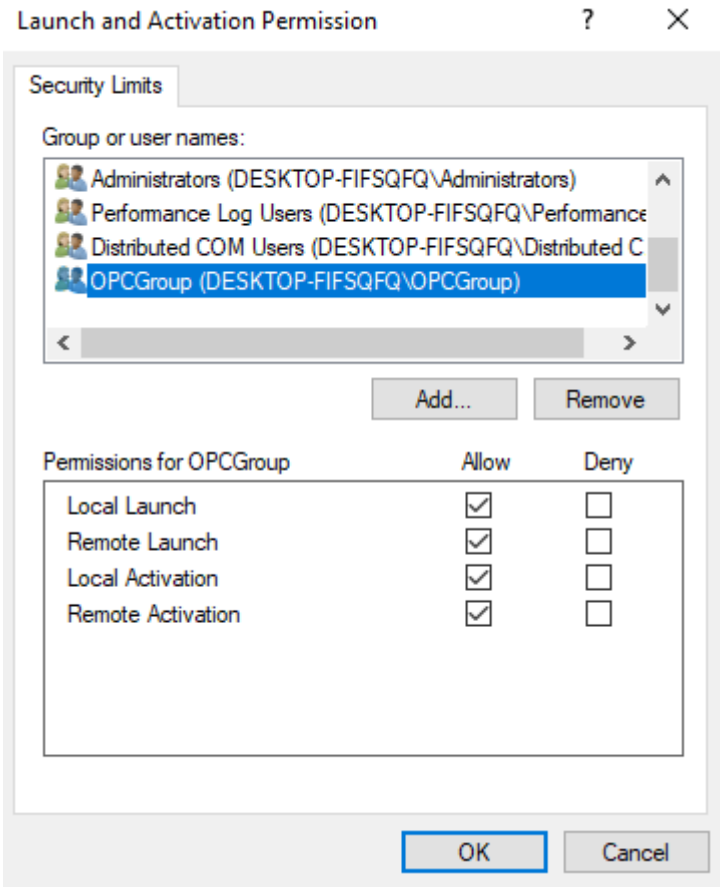
12. Click **OK** to return to the **COM Security** tab.



13. In the **Launch and Activation Permissions** group, select **Edit Limits**.
14. In **Launch and Activation Permissions**, select **Add**.



15. In **Object Types**, select the desired object type.
16. In **Locations**, click the domain or the computer that contains the users or groups that will be added. Then, click **OK**.
17. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.
18. After the account has been validated, click **OK**.
19. Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the **Group or user names** list.
20. Next, select the new user or group.



21. To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.
22. Repeat the process for all accounts that have been added. Then, click **OK**.
23. Click **OK** to close the **My Computer** properties window.

8.4 APPLYING CHANGES

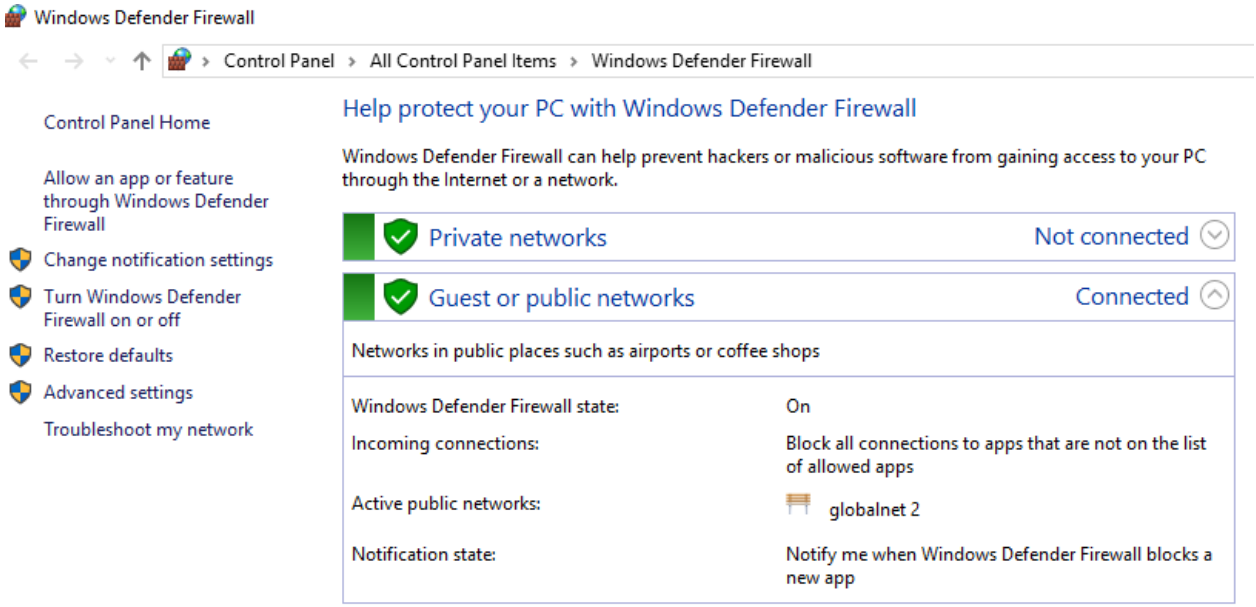
After the DCOM settings have been modified, the changes made may not be applied immediately. While some operating systems require a reboot for DCOM changes to take effect, others will only require restarting the Runtime. To do so, right- click on the **Administration** icon in the **System Tray** and then select **Stop Runtime**. Once the Runtime has stopped, the **Start Runtime** menu item will be enabled and ready for selection.

9. FIREWALLS

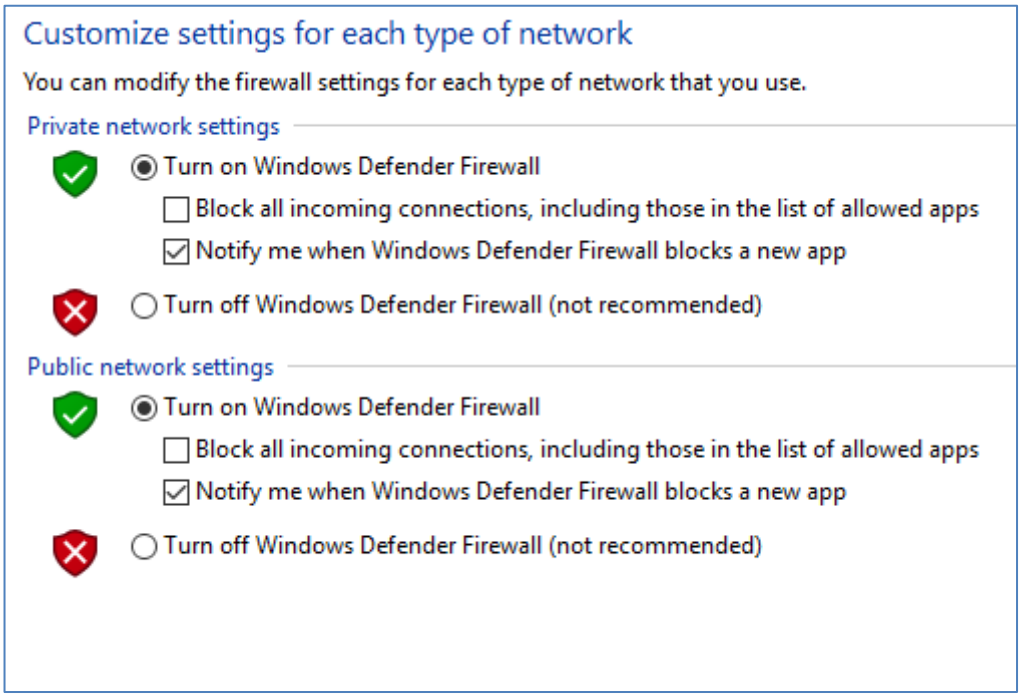
In some cases, it is easier to turn off any firewalls that may be running on both the client and server machine before DCOM is setup. Once a connection has been successfully created, it is recommended that the firewall security is restored, and the correct exceptions are added.

9.1 SERVER SIDE EXCEPTIONS

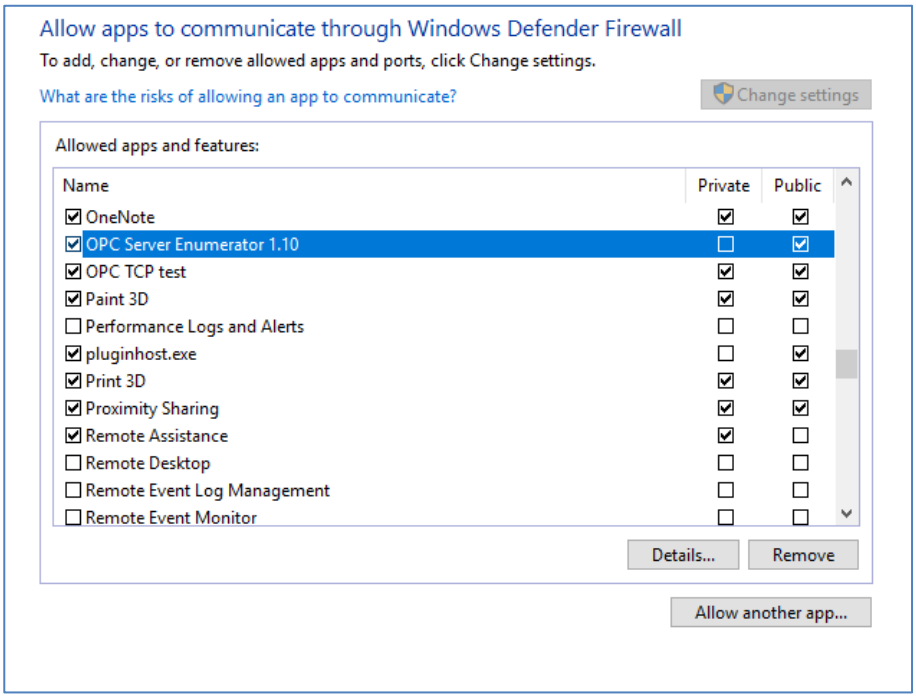
- Launch the **Windows Firewall** by selecting **Start** | **Run** and then typing "firewall.cpl".



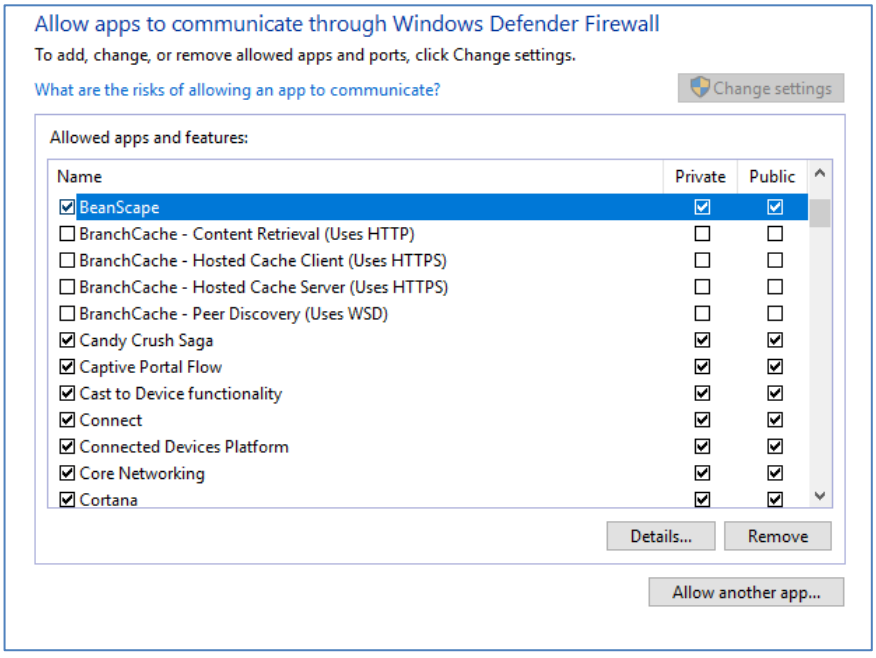
- Windows 7, 10 or Windows Server 2008 will not directly display the settings dialog. To view the dialog, select **Change Settings**.
- Next, select the **Change notification settings (or General for other windows versions)**.



- Verify that the firewall is enabled by choosing **On**.
- Next, select the **Allow an app or feature throught Windows Defender Firewall (or Exceptions for other windows versions)**.
- Click **Allow another application** to browse and then locate **OPCEnum.exe**. This is located in *C:\Windows\System32*.
- Click **Add (or OK)**.

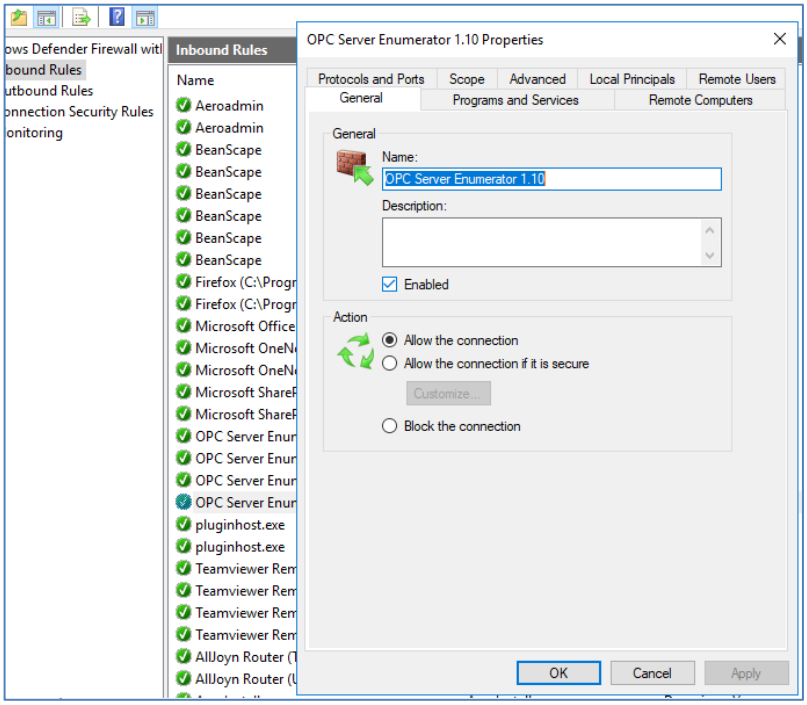


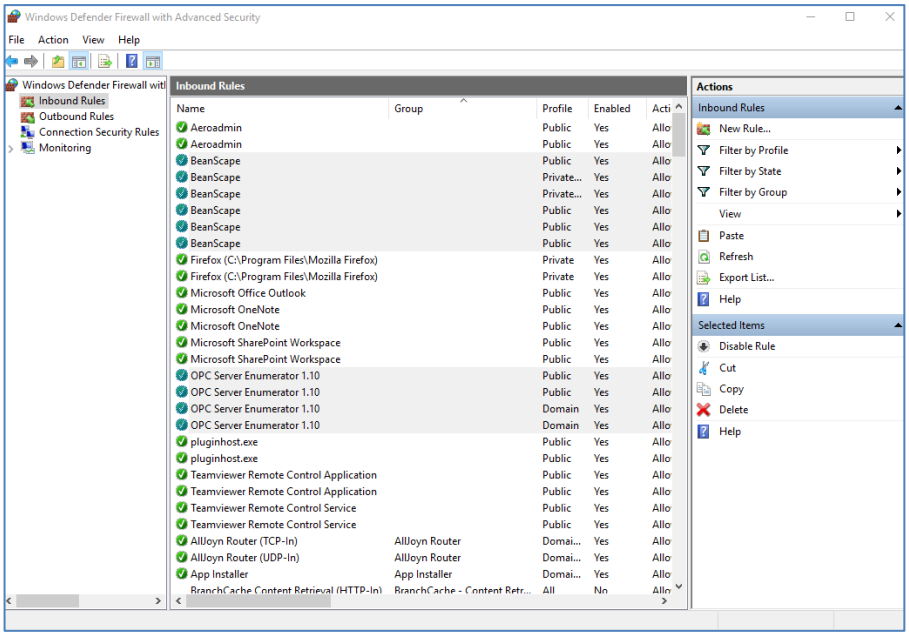
- Next, locate the OPC server application's executable file "BeanScape". This is usually located in *C:\Program Files (x86)\BeanScape2.4Ghz Premimum+*
- Click **Add (or OK)**.



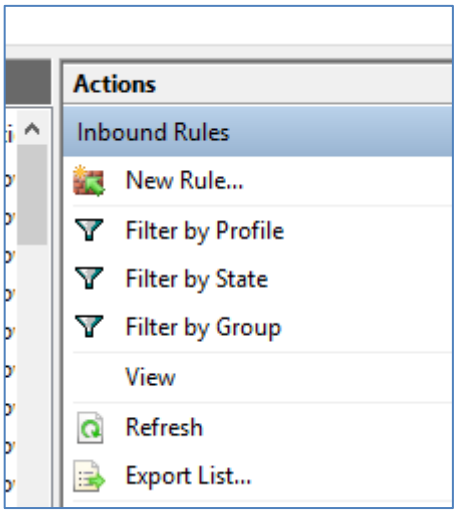
We can do the same steps from Advanced settings

- Go to Inbound Rules and Enable BeanScape and OPCEnum.

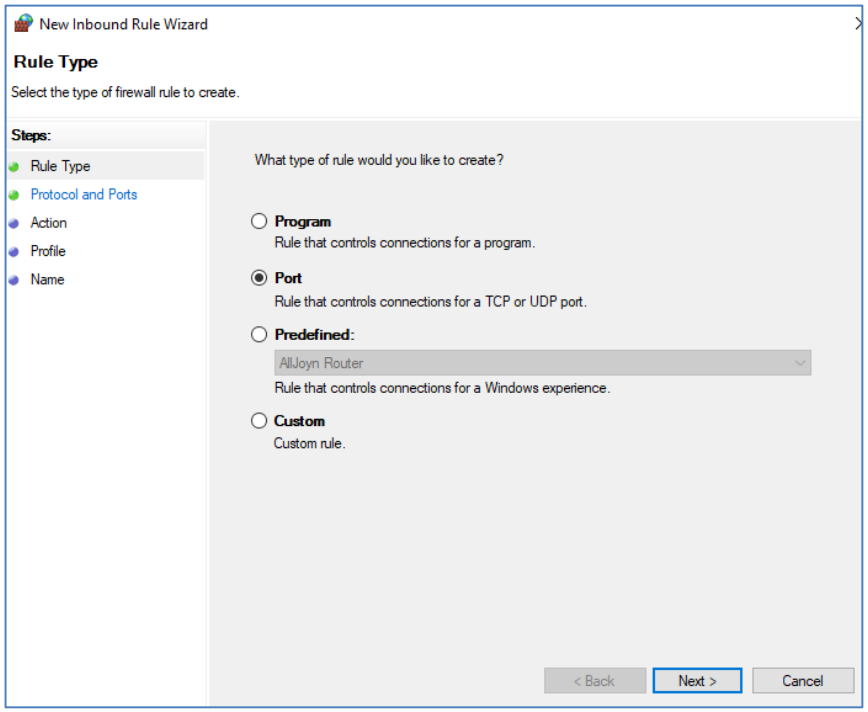


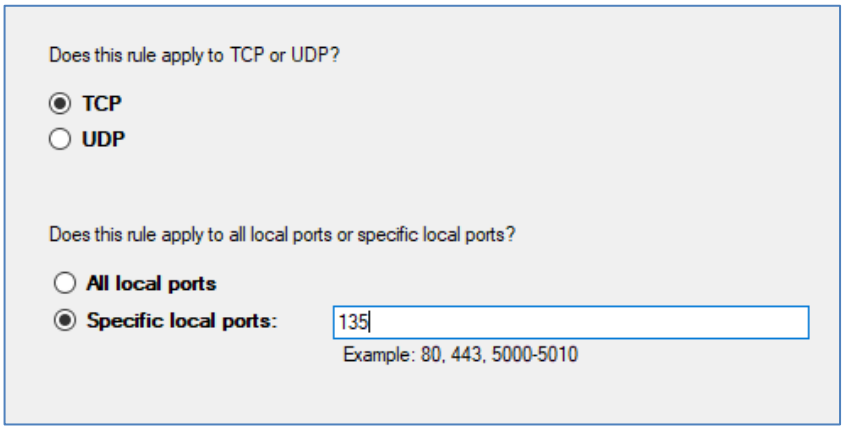


- If you can not find OPC Enum and BeanScape on the list, Go to **New Rule** and follow the steps.



- To **Add port,** Go also to New Rule and select **Port**.

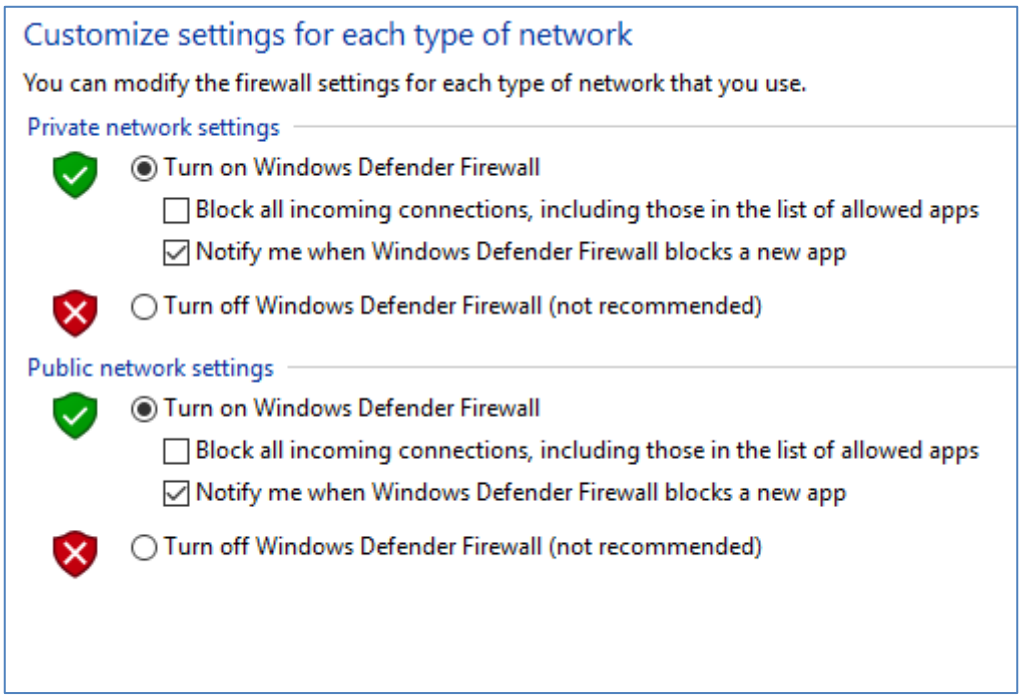




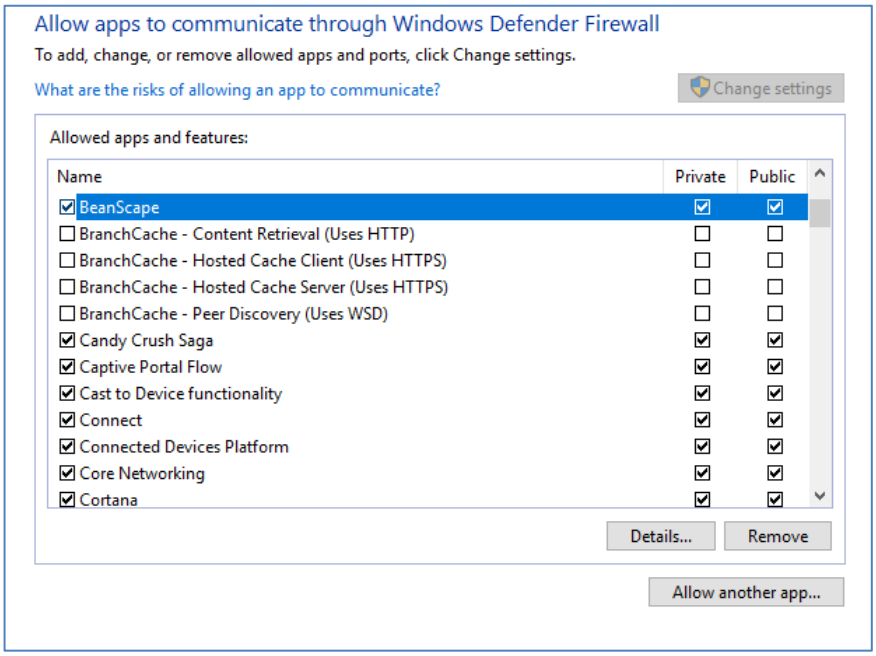
- In **Name**, enter **TCP Port 135**. This port is commonly used for allowing clients to discover and utilize a DCOM service.
- In **Port number**, enter **135**.
- Verify that the correct **Protocol** is selected. The default setting is **TCP**.

9.2 CLIENT SIDE EXCEPTIONS

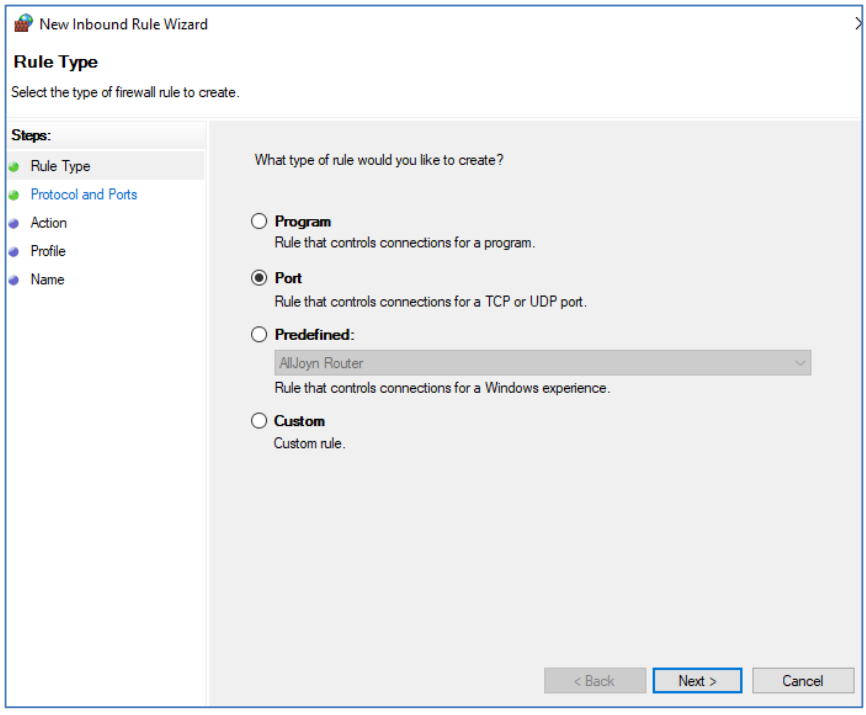
- Windows 7, 10 or Windows Server 2008 will not directly display the settings dialog. To view the dialog, select **Change Settings**.
- Next, select the **Change notification settings (or General for other windows versions)**.

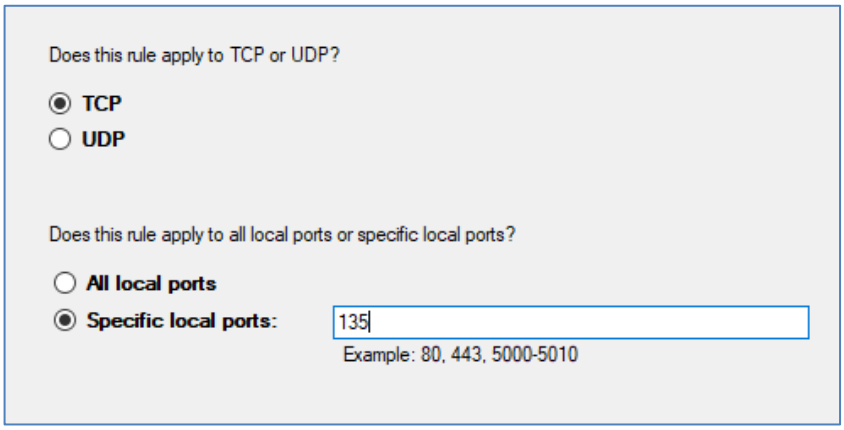


- Verify that the firewall is enabled by choosing **On**.
- Next, select the **Exceptions** tab.
- Click **Add program**.
- Next, click Browse Next, locate the OPC server application's executable file "BeanScape". This is usually located in C:\Program Files (x86)\BeanScape2.4Ghz Premimum+
- Click **Add (or OK).**



- To **Add port,** Go also to New Rule and select **Port**.





- In **Name**, enter **TCP Port 135**. This port is commonly used for allowing clients to discover and utilize a DCOM service.
- In **Port number**, enter **135**.
- Verify that the correct **Protocol** is selected. The default setting is **TCP**.

10. SUMMARY

Because OPC uses DCOM to allow remote communications, it is imperative that it is correctly configured. Users can create a secure connection by following the instructions in this document. For more information, refer to the OPC Foundation's support documentation at http://www.opcfoundation.org/.