



Version 1.1.1



Beanair GmbH

#### Beanair GmbH

"Rethinking sensing technology" 2

## TN-RF-013-OPC-DCOM-Configuration

| 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<br>Validation | For<br>informatio<br>n |  |
| Reader     | Damon Parsy  |                   | Х                      |  |
| Author     | Maneli Parsy | Х                 |                        |  |

| MAILING LIST                            |              |   |   |  |
|---|--------------|---|---|--|
| Function Recipients For action For Info |              |   |   |  |
| Staffer 1                               | Maneli Parsy | Х |   |  |
| Staffer 2                               | Damon Parsy  |   | Х |  |

| 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               | <ul> <li>Chart update</li> <li>Vocabulary update</li> <li>DCOM configuration added</li> <li>User/Group configuration added</li> <li>Firewall configuration updated</li> </ul> |  |
| 1.1.1   | 10/05/2019 | Mohamed Bechir<br>Besbes | Weblinks Update   |  |

2.4GHz wireless sensors series

TN-RF-013-OPC-DCOM-Configuration

# Contents

| 1.  | TECHNICAL SUPPORT  |
|-----|--|
| 2.  | VISUAL SYMBOLS DEFINITION  |
| 3.  | ACRONYMS AND ABBREVIATIONS   |
| 4.  | RELATED DOCUMENTS84.1 Application Notes84.2 Technical Notes9   |
| 5.  | REFERENCES OF THIS DOCUMENT  |
| 6.  | DCOM OVERVIEW         11           6.1         What is DCOM?         11           6.2         What is OPCEnum?         11  |
| 7.  | USERS AND GROUPS127.1Domains and Workgroups127.2Adding a Local User137.3Adding a Local Group147.4Adding Users to a Group15 |
| 8.  | DCOM CONFIGURATION   |
| 9.  | FIREWALLS  |
| 10. | SUMMARY  |

# 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. Copyright: Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights are reserved.

Copyright © Beanair GmbH 2016.

## **1. TECHNICAL SUPPORT**

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

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  |
|--------|---|
|        | <u>Caution or Warning</u> – Alerts the user with important information<br>about Beanair wireless sensor networks (WSN), if this<br>information is not followed, the equipment /software may fail or<br>malfunction. |
|        | <u>Danger</u> – This information MUST be followed if not you may damage the equipment permanently or bodily injury may occur.   |
| 1      | <u>Tip or Information</u> – Provides advice and suggestions that may be useful when installing Beanair Wireless Sensor Networks.  |

TN-RF-013-OPC-DCOM-Configuration

2.4GHz wireless sensors series

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

# 4.2 TECHNICAL NOTES

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

# 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 <u>https://opcfoundation.org/</u>.

## 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

 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".

| 🜆 lusrmgr - [Local Users and Groups (Loca | al)]    | – 🗆 X                          |
|---|---------|--------------------------------|
| File Action View Help                     |         |                                |
| 🏟 📰 🗟 🛛 🖬                                 |         |                                |
| 💭 Local Users and Groups (Local)          | Name    | Actions                        |
| Groups                                    | 📕 Users | Local Users and Groups (Local) |
| Gloups                                    | Groups  | More Actions 🕨                 |
|   |         |                                |
|   |         |                                |
|   |         |                                |
|   |         |                                |
|   |         |                                |
|   |         |                                |
|   |         |                                |
|   |         |                                |
|   |         | ]                              |

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

| New User        |                             |        | ?   | ×  |
|-----------------|-----------------------------|--------|-----|----|
| User name:      | OPCUser1                    |        |     |    |
| Full name:      |                             |        |     |    |
| Description:    | User created for secure OP  | с      |     |    |
|                 |                             |        |     |    |
| Password:       | •••••                       |        |     |    |
| Confirm passwor | d: •••••                    |        |     |    |
| User must ch    | ange password at next logon |        |     |    |
| User cannot     | change password             |        |     |    |
| Password ne     | ver expires                 |        |     |    |
| Account is d    | sabled                      |        |     |    |
|                 |                             |        |     |    |
|                 |                             |        |     |    |
| Help            |                             | Create | Clo | se |

- 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

- 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**.

| New Group    |                              | ?   | $\times$ |
|--------------|------------------------------|-----|----------|
| Group name:  | OPCGroup                     |     |          |
| Description: | Group created for secure OPC |     |          |
| Members:     |                              |     |          |
|              |                              |     |          |
|              |                              |     |          |
|              |                              |     |          |
|              |                              |     |          |
|              |                              |     |          |
|              |                              |     |          |
| Add          | Remove                       |     |          |
|              |                              |     |          |
| Help         | Create                       | Clo | se       |

- 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**.

| Select Users  | ×            |
|---|--------------|
| Select this object type:<br>Users or Built-in security principals | Object Types |
| From this location:<br>DESKTOP-FIFSQFQ                            | Locations    |
| Enter the object names to select ( <u>examples</u> ): OPCUser1    | Check Names  |
| Advanced 0  | K Cancel     |

- 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**.
- 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

- 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.

| 🖲 Component Services   | – 🗆 X |
|--|-------|
| 🥺 File Action View Window Help   | _ & × |
| ← ᆃ│ 2 📷 🗙 📾 @│ 🛛 📷 1 1 1 🔤 🖼 🏛 🏛  |       |
| Console Root Name Application ID ^ Actions   |       |
| V 💩 Component Services 🛛 🚔 Background Intelligent Tran {69AD4AEE-51BE-439b-A92 DCOM Config |       |
| Computers  |       |
| ✓ I My Computer BDEUILauncher Class {AB93B6F1-BE76-4185-A48 More Actions                   | •     |
| > 📫 COM+ Applications 🚔 BdeUlSrv 🛛 🗧 {C4AB7CB7-E735-48FF-AA                                |       |
| > 🛅 DCOM Config 🛛 🚔 BeanOpc_DA (EA1370BF-AC53-41F2-940                                     |       |
| See Strain Processes Bitmap Image {D3E34B21-9D75-101A-8C3                                  |       |
| Distributed Transact P Bluetooth AVCTP Service {B98C6EB5-6AA7-471E-B5C                     |       |
| Event Viewer (Local)   |       |
| Services (Local)   |       |
| CDTUHandler {F87EA55C-29CF-48B9-BEA  |       |
| CElevateWlanUi {86F80216-5DD6-4F43-953E  |       |
| CExcel12Converter Class {82780E93-DEDB-4666-8CE  |       |
| CFmlfsEngine host {82D94FB3-7FE6-4797-BB72   |       |
| CImeSearchIntegration Class {920f80d3-5ef0-40dd-9a5e-                                      |       |
| CImeServerChs {6a498709-e00b-4c45-a018   |       |
| CImeServerCht {531fdebf-9b4c-4a43-a2aa-  |       |
| Cloud Change Wnf Monitor {276D4FD3-C41D-465F-8C/   |       |
|  |       |

- 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.**

| BeanOpc_DA Properties ? X                              |
|--|
| General Location Security Endpoints Identity           |
| General properties of this DCOM application            |
| Application Name: BeanOpc_DA                           |
| Application ID: {EA1370BF-AC53-41F2-940D-3A834208BBFB} |
| Application Type: Local Server                         |
| Authentication Level: Default ~                        |
| Local Path:  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Leam more about <u>setting these properties</u> .      |
| OK Cancel Apply  |

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

| BeanOpc_DA Properties  | ?   | $\times$     |
|--|---|--------------|
| General Location Security Endpoints Identity   |   |              |
| The following settings allow DCOM to locate the correct of<br>application. If you make more than one selection, then DC<br>applicable one. Client applications may overide your select | computer for t<br>COM uses the<br>ctions. | nis<br>First |
| Run application on the computer where the data is loc  | ated.                                     |              |
| Run application on this computer.  |   |              |
| Run application on the following computer:   |   |              |
|  | Browse                                    |              |
|  |   |              |
|  |   |              |
|  |   |              |
|  |   |              |
|  |   |              |
|  |   |              |
| Learn more about <u>setting these properties</u> .   |   |              |
| OK Cancel  | Ap  | ply          |

## 7. Open the **Security** tab.

| BeanOpc_DA Properties                              | ? ×          | , |
|--|--------------|---|
| General Location Security Endpoints Ide            | entity       |   |
| Launch and Activation Permissions                  |              |   |
| ◯ Use Default                                      |              |   |
| Customize  | Edit         |   |
| Access Permissions                                 |              |   |
| ◯ Use Default                                      |              |   |
| <ul> <li>Customize</li> </ul>                      | Edit         |   |
| Configuration Permissions                          |              |   |
| ◯ Use Default                                      |              |   |
| <ul> <li>Customize</li> </ul>                      | Edit         |   |
|  |              |   |
| Learn more about <u>setting these properties</u> . |              |   |
| ОК   | Cancel Apply |   |

- 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.

TN-RF-013-OPC-DCOM-Configuration 2.4GHz wireless sensors series 10. In Launch and Activation Permissions, select Add. Select Users or Groups Х Select this object type: BeanOpc\_DA Properties X 7 Users, Groups, or Built-in security principals Object Types... General Location Security Endpoints Identity Launch and Activation Permissions From this location: O Use Default Customize Edit... DESKTOP-FIFSQFQ Locations... Access Permissions Launch and Activation Permissi O Use Default Security Enter the object names to select (examples): Customize Group or user names: OPCGroup Check Names Configuration Permis O Use Default Customize Permissions for Admin Local Launch Remote Launch Local Activation Remote Activation OK Advanced... Cancel Learn more about setting these p OK OK Cancel

- 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.

| Launch and Activation Permission | n               | ?      | ×   |
|----------------------------------|-----------------|--------|-----|
| Security                         |                 |        |     |
| Group or user names:             |                 |        |     |
| Administrators (DESKTOP-FIF      | SQFQ\Administra | tors)  | ^   |
| ANONYMOUS LOGON                  | 5010000         |        |     |
| an OPCGroup (DESKTOP-FIFSG       | (FQ\OPCGroup)   |        | ~   |
| <                                |                 | >      |     |
|                                  | Add             | Remove |     |
| Permissions for OPCGroup         | Allow           | Deny   |     |
| Local Launch                     | $\checkmark$    |        |     |
| Remote Launch                    | $\leq$          |        |     |
| Local Activation                 |                 |        |     |
| Remote Activation                | $\leq$          |        |     |
|                                  |                 |        |     |
|                                  |                 |        |     |
|                                  |                 |        |     |
|                                  |                 |        |     |
|                                  | ОК              | Cano   | cel |

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**.

| BeanOpc_DA Proper             | ties        |               |          |      | ?   | $\times$ |
|-------------------------------|-------------|---------------|----------|------|-----|----------|
| General Location              | Security    | Endpoints     | Identity |      |     |          |
| Launch and Act                | ivation Pe  | emissions     |          |      |     |          |
| ⊖ Use Default                 |             |               |          |      |     |          |
| <ul> <li>Customize</li> </ul> |             |               |          | Ed   | lit |          |
| Access Permissi               | ions        |               |          |      |     |          |
| ⊖ Use Default                 |             |               |          |      |     |          |
| Customize                     |             |               |          | Ed   | lit |          |
| Configuration Pe              | emissions   |               |          |      |     | 1        |
| O Use Default                 |             |               |          |      |     |          |
| <ul> <li>Customize</li> </ul> |             |               |          | Ed   | lit |          |
|                               |             |               |          |      |     |          |
| Learn more about se           | atting thes | e properties. |          |      |     |          |
|                               |             | ОК            | Ca       | ncel | Арр | ly       |

- 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.

| N-RF-013-OPC-DCOM-Co | nfiguration |
|----------------------|-------------|
|----------------------|-------------|

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

| eanOpc_DA Properties                       | ? ×                  | Select Users or Groups                         | ×            |
|--|----------------------|--|--------------|
| Launch and Activation Permissions          | any .                |  |              |
| O Use Default                              |                      | Select this object type:                       |              |
| Customize                                  | Edit                 | Users, Groups, or Built-in security principals | Object Types |
| Access Permissions                         |                      | From this location:                            |              |
| O Use Default                              |                      | DESKTOP-FIESOEO                                | Laartiana    |
| Customize                                  | Edit                 |  | Locations    |
| Configuration Permissions                  |                      | Enter the object names to select (examples):   |              |
| O Use Default                              | Access Permission    | OPCGroup                                       | Check Names  |
| Customize                                  | Contra               |  | Check Humos  |
| Learn more about setting these properties. | Group or user names: | Advanced                                       | OK Cancel    |
| ОК   | Съ                   | Add Bemove                                     |              |
|  | Permissions          | Allow Deny                                     |              |
|  | Local Access         |  |              |
|  | Remote Access        |  |              |
|  |                      |  |              |
|  |                      |  |              |
|  |                      |  |              |
|  |                      |  |              |
|  |                      | Cancer   |              |

- 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.

| ccess Permission         |                    | ?      | $\times$ |
|--------------------------|--------------------|--------|----------|
| Security                 |                    |        |          |
| Group or user names:     |                    |        |          |
| Sector Everyone          |                    |        |          |
| SYSTEM                   |                    |        |          |
| Administrators (DESKTOP- | FIFSQFQ\Administra | tors)  |          |
| ANONYMOUS LOGON          |                    |        |          |
| CPCGroup (DESKTOP-FIF    | SQFQ (OFCGroup)    |        |          |
|                          |                    | D      |          |
|                          | Add                | Remove |          |
| Permissions for OPCGroup | Allow              | Deny   |          |
| Local Access             | $\checkmark$       |        |          |
| Remote Access            |                    |        |          |
|                          |                    |        |          |
|                          |                    |        |          |
|                          |                    |        |          |
|                          |                    |        |          |
|                          |                    |        |          |
|                          |                    |        |          |
|                          |                    |        |          |
|                          |                    |        |          |

- 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.

- 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.

| -013-OPC-DCOM-Configuration 2.4GHz wireless sensors |  |  | wireless sensors | ensors series |  |
|---|--|--|------------------|---------------|--|
| Component Services                                  |  |  | _                |               |  |
| 💩 File Action View Window                           | Help                                       |  |                  | - 8           |  |
| 🗢 🔿 🙍 📰 🗙 🗐 🙆 🛛                                     | 1 🖬 11 12 22 22 22 22 22 22 22 22 22 22 22 |  |                  |               |  |
| Console Root  | Name                                       | Application ID                         | Actions          |               |  |
| 🗸 💩 Component Services                              | 🖀 BDEUILauncher Class                      | {AB93B6F1-BE76-4185-A488-A9001B105B    | DCOM Config      |               |  |
| ✓   | BdeUlSrv                                   | {C4AB7CB7-E735-48FF-AADD-39D09668F     | Decom coning     |               |  |
| 🗸 💽 My Computer                                     | BeanOpc_DA                                 | {EA1370BF-AC53-41F2-940D-3A834208BB    | More Actions     |               |  |
| > 🧮 COM+ Applica                                    | 🖀 Bitmap Image                             | {D3E34B21-9D75-101A-8C3D-00AA001A1     |                  |               |  |
| ✓   | Bluetooth AVCTP Service                    | {B98C6EB5-6AA7-471E-B5C5-D04FD677DI    |                  |               |  |
| > 🚔 %SystemR  | 🖀 Bluetooth User Service                   | {9980CAAB-B154-408C-B5FD-29A701E408    |                  |               |  |
| > 🚔 %SystemR  | BrowserBrokerServer                        | {DD9C53BC-8441-4B94-BD0E-36E6E02A6E    |                  |               |  |
| s 🔤 %systemrc                                       | 🖀 CDTUHandler                              | {F87EA55C-29CF-48B9-BEA2-ED578EC830    |                  |               |  |
| > 🐣 %systemrc                                       | 🖀 CElevateWlanUi                           | {86F80216-5DD6-4F43-953B-35EF40A35AE   |                  |               |  |
| > 🐣 %systemrc                                       | CExcel12Converter Class                    | {82780E93-DEDB-4666-8CEF-E83D451CC5    |                  |               |  |
| · · · · · · · · · · · · · · · · · · ·               | CEmlfcEngine host                          | /82D0/EB3_7EE6_/707_BB72_0A886C66073   |                  |               |  |
| > 🐣 %systemrc 🗡                                     | = crimisengine nost                        | (02D341D3-11E0-4131-DD12-3A000C00012 Q |                  |               |  |

- 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.

| BeanOpc_DA Properties               |                                 | ? ×    |
|-------------------------------------|---------------------------------|--------|
| General Location Security           | Endpoints Identity              |        |
| Which user account do you           | want to use to run this applica | ition? |
| The interactive user                |                                 |        |
|                                     |                                 |        |
|                                     |                                 |        |
| User:                               | KTOP-FIFSQFQ\OPCUser1           | Browse |
| Password:                           | •••••                           |        |
| Confirm password:                   | •••••                           |        |
| O The system account (ser           | vices only).                    |        |
|                                     |                                 |        |
|                                     |                                 |        |
|                                     |                                 |        |
|                                     |                                 |        |
| l                                   |                                 |        |
| Learn more about <u>setting the</u> | ese properties.                 |        |
|                                     | OK Cancel                       | Apply  |

- 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

- 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.

| les Component Services   |   | _                                      | □ ×   |
|--|---|--|-------|
| Image: Second   | Help  |  | _ & × |
| Console Root<br>Component Services<br>Computers<br>Computers<br>COM+ Applicatio<br>COM+ Applicatio<br>COM+ Config<br>COM+ C | lame<br>COM+ Applications<br>DCOM Config<br>Running Processes<br>Distributed Transaction Coordi | Actions<br>My Computer<br>More Actions | •     |

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

| My Computer Properties  |   |  | ?                       | $\times$ |
|---|---|--|-------------------------|----------|
| Default Protocols   | COM Sec   | curity                                       | MSDTC                   |          |
| General   | Options   | Defa   | ult Properties          |          |
| ✓ Enable Distributed COM ☐ Enable COM Internet Set                                    | on this computer<br>ervices on this cor                         | mputer                                       |                         |          |
| Default Distributed COM (   | Communication Pr  | operties                                     |                         |          |
| The Authentication Level  | specifies security  | at the pack                                  | et level.               |          |
| Default Authentication  | Level:  |  |                         |          |
| Connect   |   | $\sim$                                       |                         |          |
| who is calling them, and v<br>using the client's identity.<br>Default Impersonation L | whether the applic  | cation can do                                | operations              |          |
| Identify  |   | $\sim$                                       |                         |          |
| Security for reference trac<br>and that the default imper                             | cking can be prov<br>sonation level is r<br>ecurity for referen | rided if authe<br>not anonymo<br>ce tracking | ntication is use<br>us. | d        |
|   | -   |  |                         | - 1      |
| Learn more about <u>setting th</u>  | ese properties.   |  |                         |          |
|   | ОК  | Cancel                                       | Appl                    | у        |

- 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.

| My Computer Proper  | ties   |  |  |                                      | ?  | × |
|---|--|--|--|--------------------------------------|--|---|
| General   |  | Options  |  | Defa                                 | ault Properties  |   |
| Default Protocols   | 3  | COM Sec  | curity                                   |                                      | MSDTC  |   |
| - Access Permissions  | s  |  |  |                                      |  |   |
| You may edit wh<br>also set limits on   | o is allo<br>applica   | owed default acc<br>ations that determ   | ess to<br>ine the                        | applic<br>air ow                     | cations. You may<br>n permissions.                           | ' |
| Caution<br>of applic<br>securely  | : Modif<br>cations<br>y.   | ying access pem<br>to start, connect   | nissions<br>, funct                      | s can<br>ion ar                      | affect the ability<br>nd/or run                              |   |
|   |  | Edit Limits  |  | E                                    | Edit Default   | 1 |
| You may edit wh<br>activate objects.<br>determine their o<br>Caution<br>affect th<br>and/or the | tion Pe<br>o is allo<br>You m<br>wn per<br>: Modif<br>ne abilit<br>run sec | emissions<br>owed by default to<br>ay also set limits<br>missions.<br>ying launch and<br>ty of applications<br>curely. | o launo<br>on app<br>activat<br>to starf | ch ap<br>licatio<br>ion po<br>t, con | plications or<br>ons that<br>emissions can<br>mect, function |   |
|   |  | Edit Limits  |  | E                                    | Edit Default   |   |
| Learn more about <u>set</u>   | tting the  | ese properties.  |  |                                      |  |   |
|   |  | ОК   | C  | ance                                 | Appl   | y |

- 9. Select Edit Limits in the Access Permissions group.
- 10. Select the **ANONYMOUS LOGON** group account in the **Group or user names** list.

| Access Permission                  |                  | ?      | $\times$ |
|------------------------------------|------------------|--------|----------|
| Default Security                   |                  |        |          |
| Group or user names:               |                  |        |          |
| SYSTEM                             |                  |        |          |
| Administrators (DESKTOP-FIF        | SQFQ\Administrat | ors)   |          |
| ANONYMOUS LOGON                    |                  |        |          |
|                                    |                  |        |          |
|                                    | Add              | Remove |          |
| Permissions for ANONYMOUS<br>LOGON | Allow            | Deny   |          |
| Local Access                       | $\checkmark$     |        |          |
| Remote Access                      | $\checkmark$     |        |          |
|                                    |                  |        |          |
|                                    |                  |        |          |
|                                    |                  |        |          |
|                                    |                  |        |          |
|                                    |                  |        |          |
|                                    | ОК               | Canc   | el       |

- 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.

| My Computer Propert  | ies   |  |  |   | ?  | $\times$ |
|--|---|--|--|---|--|----------|
| General  |   | Options  |  | Default                                   | Properties   |          |
| Default Protocols  |   | COM Sec  | cunty  |   | MSDTC  |          |
| Access Permissions<br>You may edit who<br>also set limits on a<br>Caution:<br>of applic<br>securely                    | o is allo<br>applica<br>Modify<br>ations                                  | wed default acc<br>tions that determ<br>ving access perm<br>to start, connect  | ess to a<br>ine thei<br>issions<br>, functio   | pplicati<br>rown p<br>can aff<br>on and/  | ons. You may<br>ermissions.<br>ect the ability<br>or run |          |
|  |   | Edit Limits  |  | Edit                                      | Default  |          |
| Launch and Activat<br>You may edit who<br>activate objects.<br>determine their ov<br>Caution:<br>affect th<br>and/or m | ion Per<br>o is allo<br>You ma<br>wn per<br>Modify<br>e ability<br>un sec | missions<br>wed by default to<br>ay also set limits<br>nissions.<br>ving launch and a<br>y of applications<br>urely. | o launcł<br>on appli<br>activatic<br>to start, | n applic<br>ications<br>on perm<br>connec | ations or<br>that<br>issions can<br>ct, function         |          |
|  |   | Edit Limits  |  | Edit                                      | Default  |          |
| Learn more about <u>sett</u>   | ing the   | ese properties.  |  |   |  |          |
|  |   | ОК   | Ca   | ancel                                     | Apply  | ŗ        |

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

#### 14. In Launch and Activation Permissions, select Add.

| Select Users or Groups                         | ×            |
|--|--------------|
| Select this object type:                       |              |
| Users, Groups, or Built-in security principals | Object Types |
| From this location:                            |              |
| DESKTOP-FIFSQFQ                                | Locations    |
| Enter the object names to select (examples)    |              |
| OPCGroup                                       | Check Names  |
| Advanced                                       | OK Cancel    |

- 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.

| aunch and Activation Permission                             | n                                | ? >                    |
|---|----------------------------------|------------------------|
| Security Limits   |                                  |                        |
| Group or user names:  |                                  |                        |
| Administrators (DESKTOP-FIF<br>& Performance Log Users (DES | SQFQ\Administra<br>KTOP-FIFSQFQ\ | tors) 🔺<br>Performance |
| Section (DESKTOP-EIESC                                      |                                  | Distributed C          |
|   | (retor coloup)                   | ~                      |
| <   |                                  | >                      |
|   | Add                              | Remove                 |
| Permissions for OPCGroup                                    | Allow                            | Deny                   |
| Local Launch  | $\checkmark$                     |                        |
| Remote Launch   | $\checkmark$                     |                        |
| Local Activation  |                                  |                        |
| Remote Activation   |                                  |                        |
|   |                                  |                        |
|   |                                  |                        |
|   |                                  |                        |
|   |                                  |                        |
|   |                                  |                        |

- 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".

| 🔗 W          | /indows Defender Firewall                           |  |  |
|--------------|---|--|--|
| $\leftarrow$ | $ ightarrow ~ \uparrow 	heta > 	heta$ Sontrol Panel | > All Control Panel Items > Windows Defender Fit   | rewall   |
|              | Control Panel Home                                  | Help protect your PC with Windows Def  | ender Firewall   |
| 1            | Allow an app or feature<br>through Windows Defender | Windows Defender Firewall can help prevent hackers<br>through the Internet or a network. | or malicious software from gaining access to your PC                   |
|              | Firewall  | Private networks   | Not connected 📀  |
| <b>•</b>     | Change notification settings                        |  |  |
| •            | Turn Windows Defender<br>Firewall on or off         | Guest or public networks   | Connected 🔗  |
| ا 🌎          | Restore defaults                                    | Networks in public places such as airports or coffee                                     | shops  |
| <b>•</b>     | Advanced settings                                   | Windows Defender Firewall state:   | On   |
|              | Troubleshoot my network                             | Incoming connections:  | Block all connections to apps that are not on the list of allowed apps |
|              |   | Active public networks:  | 🗮 globalnet 2  |
|              |   | Notification state:  | Notify me when Windows Defender Firewall blocks a<br>new app           |

- 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).

| Customize settings for each type of network                                 |
|---|
| You can modify the firewall settings for each type of network that you use. |
| Private network settings  |
| Turn on Windows Defender Firewall   |
| Block all incoming connections, including those in the list of allowed apps |
| Notify me when Windows Defender Firewall blocks a new app                   |
| O Turn off Windows Defender Firewall (not recommended)                      |
| Public network settings   |
| Turn on Windows Defender Firewall   |
| Block all incoming connections, including those in the list of allowed apps |
| Notify me when Windows Defender Firewall blocks a new app                   |
| Turn off Windows Defender Firewall (not recommended)                        |
| •   |
|   |
|   |

- 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).

| at are the risks of allowing an app to communicate? |       | - Uni   | ange sett           | ing |
|---|-------|---------|---------------------|-----|
| llowed apps and features:                           |       |         |                     |     |
| Name  |       | Private | Public              | ^   |
| 🗹 OneNote   |       |         |                     |     |
| OPC Server Enumerator 1.10                          |       |         |                     |     |
| ☑ OPC TCP test                                      |       | ✓       | ✓                   |     |
| 🗹 Paint 3D  |       | ✓       | ✓                   |     |
| Performance Logs and Alerts                         |       |         |                     |     |
| 🗹 pluginhost.exe                                    |       |         | <ul><li>✓</li></ul> | i.  |
| ☑ Print 3D  |       |         | ✓                   |     |
| Proximity Sharing                                   |       |         | ✓                   |     |
| Remote Assistance                                   |       |         |                     |     |
| 🗌 Remote Desktop                                    |       |         |                     |     |
| 🗆 Remote Event Log Management                       |       |         |                     |     |
| Remote Event Monitor                                |       |         |                     | ×   |
|   | Detai | s       | Remov               | e   |
|   |       |         |                     |     |

- 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).

| Name   |      | Private      | Public | ^ |
|--|------|--------------|--------|---|
| ✓ BeanScape                                    |      |              |        |   |
| BranchCache - Content Retrieval (Uses HTTP)    |      |              |        |   |
| BranchCache - Hosted Cache Client (Uses HTTPS) |      |              |        |   |
| BranchCache - Hosted Cache Server (Uses HTTPS) |      |              |        |   |
| BranchCache - Peer Discovery (Uses WSD)        |      |              |        |   |
| 🗹 Candy Crush Saga                             |      | $\checkmark$ | ✓      |   |
| Captive Portal Flow                            |      | $\checkmark$ | ✓      |   |
| Cast to Device functionality                   |      | $\checkmark$ | ✓      |   |
| ✓ Connect                                      |      | $\checkmark$ | ✓      |   |
| Connected Devices Platform                     |      | $\checkmark$ | ✓      |   |
| Core Networking                                |      | $\checkmark$ | ~      |   |
| ✓ Cortana                                      |      | ✓            | ✓      | Y |
|  | Deta | ails         | Remov  | e |

• Go to Inbound Rules and Enable BeanScape and OPCEnum.



| Windows Defender Firewall wit  | h Advanced Security                          |                            |         |           |         | - 🗆 X             |
|--------------------------------|--|----------------------------|---------|-----------|---------|-------------------|
|                                |  |                            |         |           |         |                   |
| Windows Defender Firewall with | Inbound Rules                                |                            |         |           |         | Actions           |
| Inbound Rules                  | Name   | Group                      | Profile | Enabled / | Acti ^  | Inbound Rules     |
| Connection Security Rules      | 🔮 Aeroadmin                                  |                            | Public  | Yes /     | Allo    | 🐹 New Rule        |
| > 🔍 Monitoring                 | 🥑 Aeroadmin                                  |                            | Public  | Yes /     | Allo    | Filter by Profile |
|                                | BeanScape                                    |                            | Public  | Yes /     | Allo    |                   |
|                                | 😻 BeanScape                                  |                            | Private | Yes /     | Allo    | Y Filter by State |
|                                | SeanScape                                    |                            | Private | Yes /     | Allo    | Filter by Group   |
|                                | 🔇 BeanScape                                  |                            | Public  | Yes /     | Allo    | View              |
|                                | BeanScape                                    |                            | Public  | Yes /     | Allo    | P. Danta          |
|                                | 😵 BeanScape                                  |                            | Public  | Yes /     | Allo    | Paste             |
|                                | 🔮 Firefox (C:\Program Files\Mozilla Firefox) |                            | Private | Yes A     | Allo    | 🖸 Refresh         |
|                                | 😻 Firefox (C:\Program Files\Mozilla Firefox) |                            | Private | Yes /     | Allo    | 📑 Export List     |
|                                | 🔮 Microsoft Office Outlook                   |                            | Public  | Yes A     | Allo    | 2 Help            |
|                                | 🔮 Microsoft OneNote                          |                            | Public  | Yes /     | Allo    |                   |
|                                | Microsoft OneNote                            |                            | Public  | Yes /     | Allo    | Selected Items    |
|                                | Microsoft SharePoint Workspace               |                            | Public  | Yes /     | Allo    | Disable Rule      |
|                                | Microsoft SharePoint Workspace               |                            | Public  | Yes /     | Allo    | K Cut             |
|                                | OPC Server Enumerator 1.10                   |                            | Public  | Yes /     | Allo    |                   |
|                                | OPC Server Enumerator 1.10                   |                            | Public  | Yes /     | Allo    | Сору              |
|                                | OPC Server Enumerator 1.10                   |                            | Domain  | Yes /     | Allo    | 🔀 Delete          |
|                                | OPC Server Enumerator 1.10                   |                            | Domain  | Yes /     | Allo    | 2 Help            |
|                                | 🔮 pluginhost.exe                             |                            | Public  | Yes /     | Allo    |                   |
|                                | 🔮 pluginhost.exe                             |                            | Public  | Yes /     | Allo    |                   |
|                                | 😻 Teamviewer Remote Control Application      |                            | Public  | Yes A     | Allo    |                   |
|                                | 🧭 Teamviewer Remote Control Application      |                            | Public  | Yes /     | Allo    |                   |
|                                | 🥑 Teamviewer Remote Control Service          |                            | Public  | Yes A     | Allo    |                   |
|                                | 🔮 Teamviewer Remote Control Service          |                            | Public  | Yes /     | Allo    |                   |
|                                | 🧭 AllJoyn Router (TCP-In)                    | AllJoyn Router             | Domai   | Yes A     | Allo    |                   |
|                                | 🧭 AllJoyn Router (UDP-In)                    | AllJoyn Router             | Domai   | Yes /     | Allo    |                   |
|                                | 😻 App Installer                              | App Installer              | Domai   | Yes A     | Allo    |                   |
|                                | BranchCache Content Retrieval (HTTP-In)      | BranchCache - Content Retr | All     | No /      | Allor Y |                   |
| < >                            | <  |                            |         |           | >       | 1                 |

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

|          | Actions             |  |
|----------|---------------------|--|
| i ^      | Inbound Rules       |  |
| <b>7</b> | 🚉 New Rule          |  |
| 2        | Y Filter by Profile |  |
| 2        | Y Filter by State   |  |
| ,<br>,   | 🝸 Filter by Group   |  |
| y        | View                |  |
| 2        | Q Refresh           |  |
| y I      | 🛃 Export List       |  |

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

| Prew Inbound Rule Wizard                                  |  |  |  |
|---|--|--|--|
| Rule Type   | veste  |  |  |
| Stare-  | Arcaro.  |  |  |
| Steps:<br>Protocol and Ports<br>Action<br>Profile<br>Name | What type of rule would you like to create?  Program Rule that controls connections for a program.  Prodefined:  Alloyn Router Rule that controls connections for a Windows experience.  C Custom Custom rule. |  |  |
|   | < Back Next > Cancel   |  |  |

| Does this rule apply to TCP or U     | DP?                                 |
|--------------------------------------|-------------------------------------|
| ● TCP ○ UDP                          |                                     |
| Does this rule apply to all local po | orts or specific local ports?       |
| Specific local ports:                | 135 <br>Example: 80, 443, 5000-5010 |

- 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).

| Customize settings for each type of network                                 |
|---|
| You can modify the firewall settings for each type of network that you use. |
| Private network settings  |
| Turn on Windows Defender Firewall   |
| Block all incoming connections, including those in the list of allowed apps |
| Notify me when Windows Defender Firewall blocks a new app                   |
| O Turn off Windows Defender Firewall (not recommended)                      |
| Public network settings   |
| Turn on Windows Defender Firewall   |
| Block all incoming connections, including those in the list of allowed apps |
| Notify me when Windows Defender Firewall blocks a new app                   |
| Turn off Windows Defender Firewall (not recommended)                        |
| •   |
|   |
|   |

- 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).

| Allow apps to communicate through Windows Defender Firewall              |          |              |              |
|--|----------|--------------|--------------|
| To add, change, or remove allowed apps and ports, click Change settings. |          |              |              |
| What are the risks of allowing an app to communicate?                    |          |              |              |
| Allowed apps and features:   |          |              |              |
| Name   | Private  | Public       | ^            |
| ✓ BeanScape  |          |              |              |
| BranchCache - Content Retrieval (Uses HTTP)                              |          |              |              |
| BranchCache - Hosted Cache Client (Uses HTTPS)                           |          |              |              |
| BranchCache - Hosted Cache Server (Uses HTTPS)                           |          |              |              |
| BranchCache - Peer Discovery (Uses WSD)                                  |          |              |              |
| ✓ Candy Crush Saga   | ✓        | ✓            |              |
| Captive Portal Flow  | ✓        | $\checkmark$ |              |
| Cast to Device functionality   | ✓        | ✓            |              |
| ✓ Connect  | ✓        | $\checkmark$ |              |
| Connected Devices Platform   | ✓        | ✓            |              |
| Core Networking  | ✓        | ✓            |              |
| 🗹 Cortana  | ✓        | ✓            | $\checkmark$ |
| Deta   | iils     | Remove       | ż            |
|  | Allow an | other app    | )            |
|  |          |              |              |

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

| New Inbound Rule Wizard     Rule Type                                  | ۱<br>۲                                      |
|--|---|
| Select the type of firewall rule to c                                  | reate.                                      |
| Steps:<br>Pule Type<br>Protocol and Ports<br>Action<br>Profile<br>Name | What type of rule would you like to create? |
|  | < Back Next > Cancel                        |

| Does this rule apply to TCP or UD    | )P?                          |
|--------------------------------------|------------------------------|
| <ul><li>TCP</li><li>UDP</li></ul>    |                              |
| Does this rule apply to all local po | rts or specific local ports? |
| ○ All local ports                    |                              |
| Specific local ports:                | 135                          |
|                                      | Example: 80, 443, 5000-5010  |
|                                      |                              |

- 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 <u>http://www.opcfoundation.org/.</u>