



How to configure CIMON-SCADA OPC Server for Windows 7 and 8?



CIMON-SCADA OPC Server function is available only with WEB SERVER USB Dongle (Keylock).

These are conditions that should be met in order to properly configure and use OPC Server in SCADA:

- USB Dongle (Keylock) should be **CM04-SCADA 1-E or above** as shown in the below image.
In this example, UltimateAccess V3.03 is used for the FAQ manual.

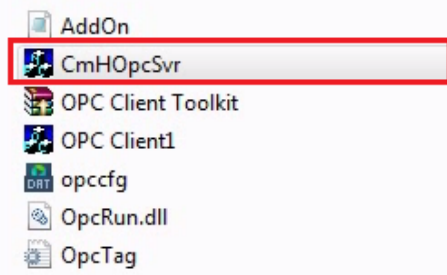
UltimateAccess (S/W license)			
• WEB SERVER			
NO	Model	Type	Description
1	CM04-SCADA 1-E	1 User	Development+Server+Mobile, Web & Network Clients
2	CM04-SCADA 5-E	2-5 Users	Development+Server+Mobile, Web & Network Clients
3	CM04-SCADA 10-E	6-10 Users	Development+Server+Mobile, Web & Network Clients
4	CM04-SCADA UNL-E	Unlimited Users	Development+Server+Mobile, Web & Network Clients

UltimateAccess (CIMON-SCADA) OPC Server Configurations

1. Go to Computer → Local Disk (C:) → CIMON → UltimateAccess → CIMON SCADA
And change the file name from “CmHOpcsvr.exe” to “CmHOpcsvr_B.exe.”

CmChartEditor.dll	5/28/2015 11:53 AM	Application extens...	643 KB
CmHOpcSvr_B	4/13/2015 9:47 PM	Application	51 KB
CmnCnet.dll	3/12/2014 11:48 AM	Application extens...	67 KB
CmnCnetS.dll	6/8/2015 10:56 AM	Application extens...	40 KB

2. Download and unzip “OPC Server Components” from CIMON website.



- Copy and paste the “CmHopcSvr” file from the [OPC Server Components] folder to the CIMON SCADA UltimateAccess installation folder. (This file is different from the existing file in the UltimateAccess installation folder).

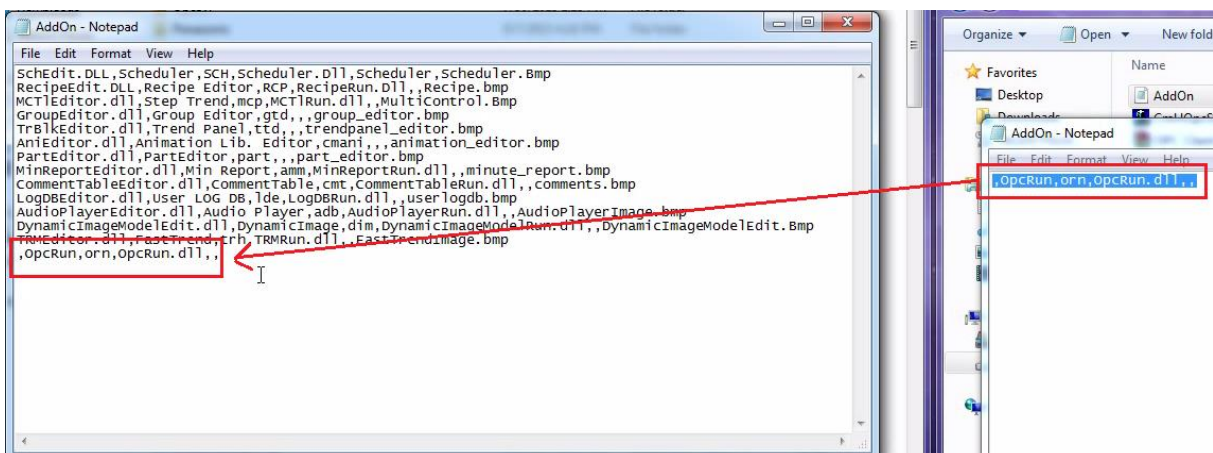
	CmChartEditor.dll	5/28/2015 11:53 AM	Application extens...	643 KB
	CmHopcSvr	5/9/2013 4:41 PM	Application	803 KB
	CmHopcSvr_B	4/13/2015 9:47 PM	Application	51 KB
	CmnCnet.dll	3/12/2014 11:48 AM	Application extens...	67 KB

- Click and open the “AddOn.lst” file in the UltimateAccess installation folder.
Type the below information in red to the “AddOn.lst” file.

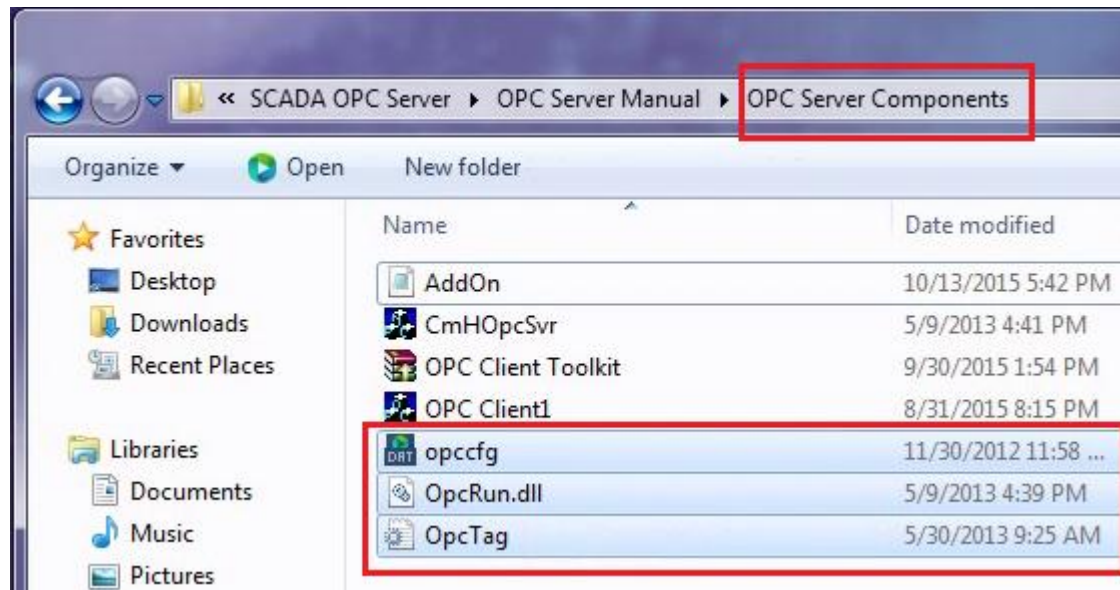
```

File Edit Format View Help
Schedit.DLL,Scheduler,SCH,Scheduler.dll,Scheduler,Scheduler.Bmp
RecipeEdit.DLL,Recipe Editor,RCP,RecipeRun.dll,,Recipe.bmp
MCTLEditor.dll,Step Trend,mcp,MCTLRun.dll,,MultiControl.Bmp
GroupEditor.dll,Group Editor,gtc,,group_editor.bmp
TrBlkEditor.dll,Trend Panel,ttc,,trendpanel_editor.bmp
AniEditor.dll,Animation Lib. Editor,cmani,,animation_editor.bmp
PartEditor.dll,PartEditor,part,,part_editor.bmp
MinReportEditor.dll,Min Report,amm,MinReportRun.dll,,minute_report.bmp
CommentTableEditor.dll,CommentTable,cmt,CommentTableRun.dll,,comments.bmp
LogDBEditor.dll,User LOG DB,lde,LogDBRun.dll,,userlogdb.bmp
AudioPlayerEditor.dll,Audio Player,adb,AudioPlayerRun.dll,,AudioPlayerImage.bmp
DynamicImageModelEdit.dll,DynamicImage,dim,DynamicImageModelRun.dll,,DynamicImageModelEdit.Bmp
TRMEditor.dll,FastTrend,trh,TRMRun.dll,,FastTrendImage.bmp
,OpcRun,orn,opcRun.dll,,
    
```

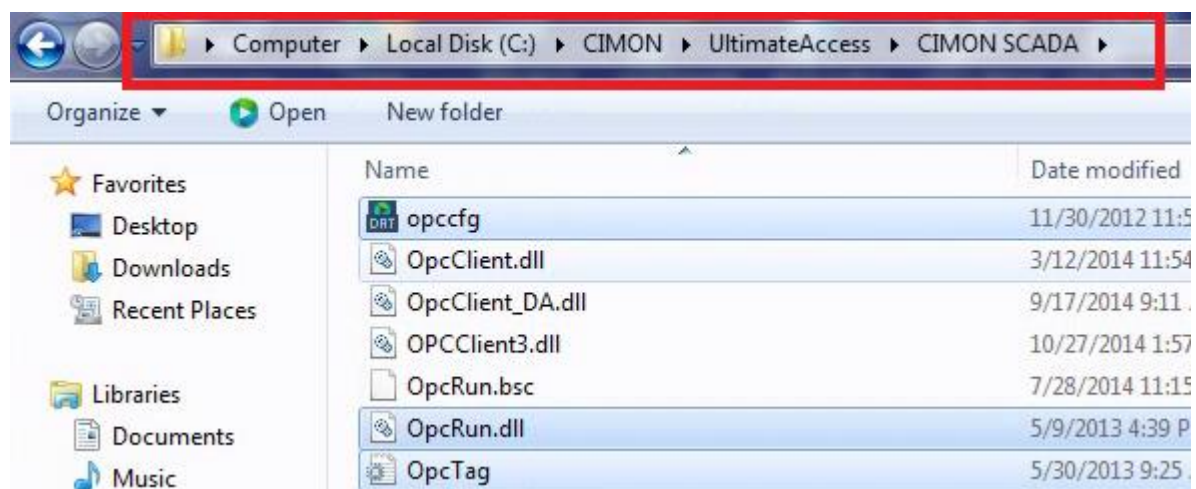
- Or you can just copy and paste “,OpcRun, orn, OpcRun.dll,,” from AddOn.lst file from the OPC Server Components folder to the AddOn.lst file in the UltimateAccess folder.



- Copy and paste the three files (opccfg.dat, OpcRun.dll, OpcTag.ini) from the OPC Server Components folder to the UltimateAccess installation folder.



- The three files are now located in the UltimateAccess installation folder.



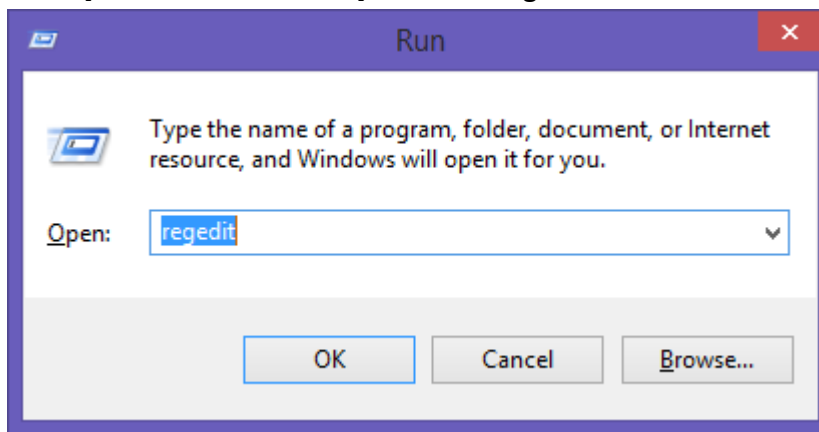
***This is the end of the UltimateAccess (CIMON-SCADA) OPC Server configurations.
Now, we're going to learn how to configure DCOM and Firewall in Windows 7 and 8.**

Windows DCOM and Firewall Configurations

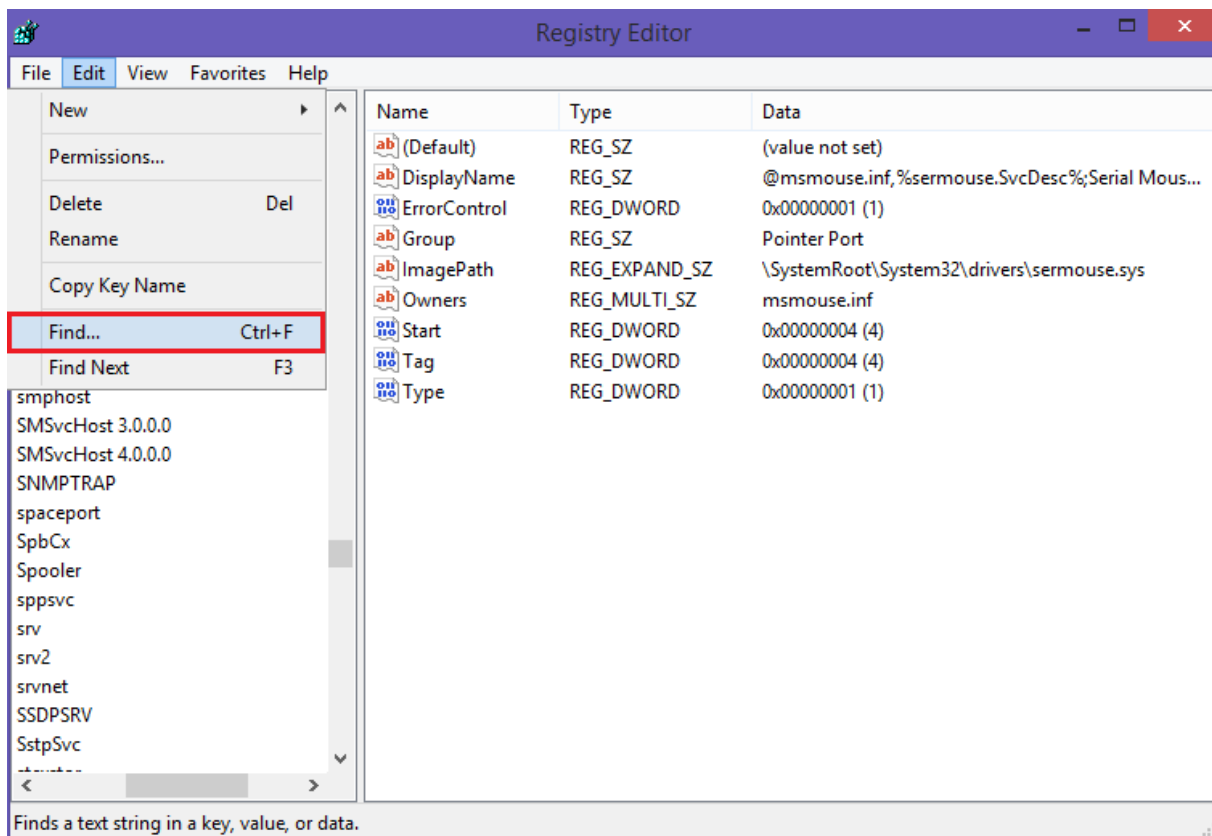
The configurations for Vista / Windows 7 / Windows 8 are as follows.

1. If your PC is Windows 8, these additional settings must be done prior to the step 2.
The step 1 only applies to Windows 8.

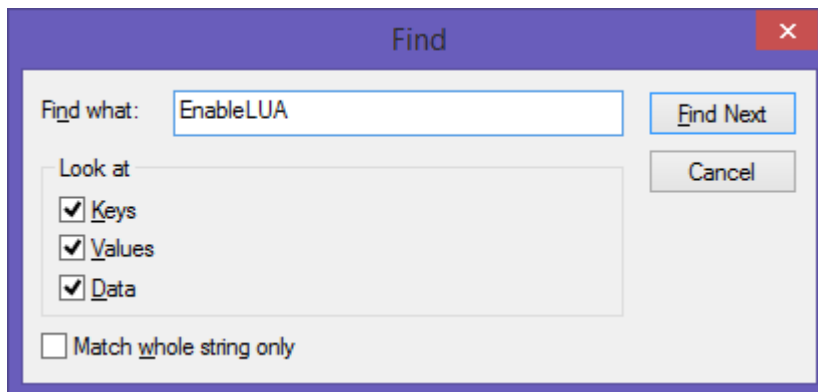
- Press [Windows button + R] and run “regedit.”



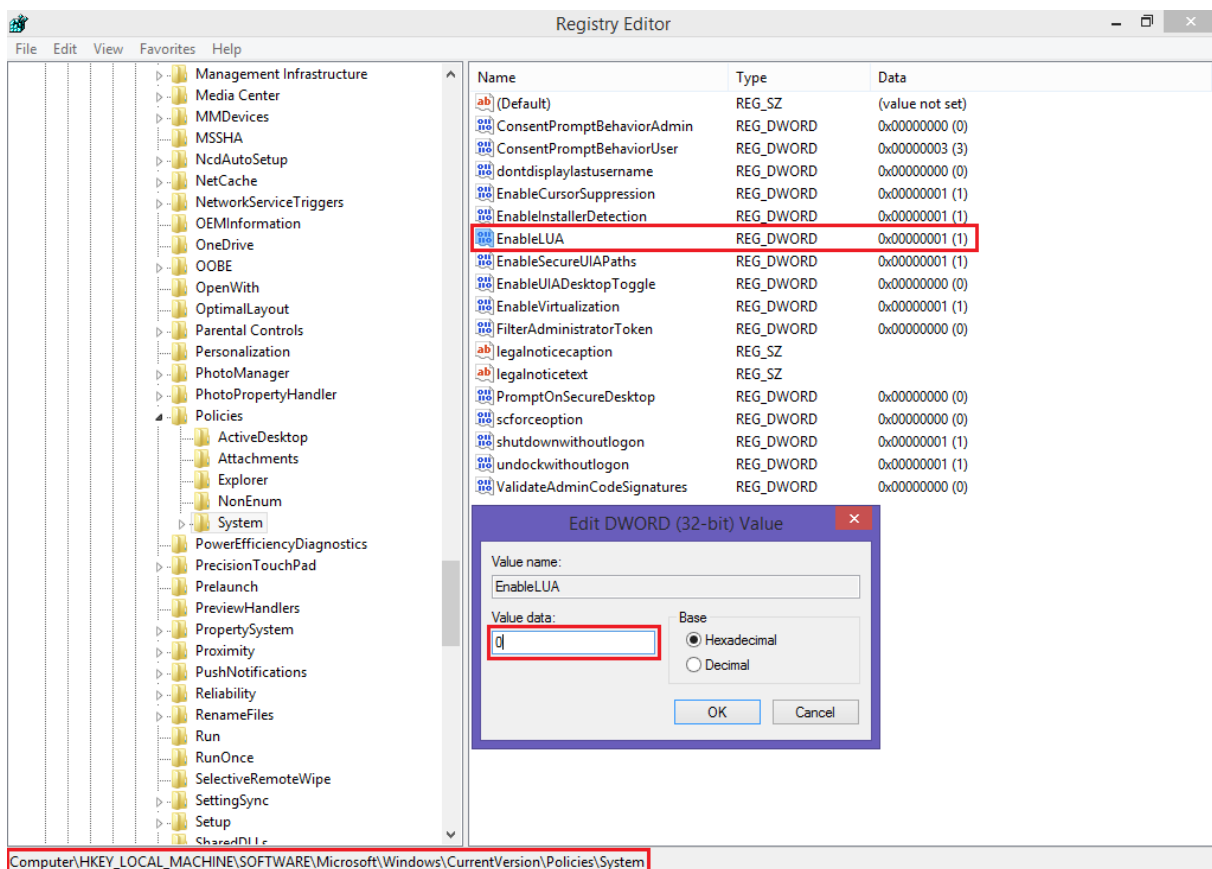
- In the Registry Editor dialog, go to Edit → and click “Find” (Shortcut keys: Ctrl + F).



- In the Find dialog, search for “EnableLUA.”

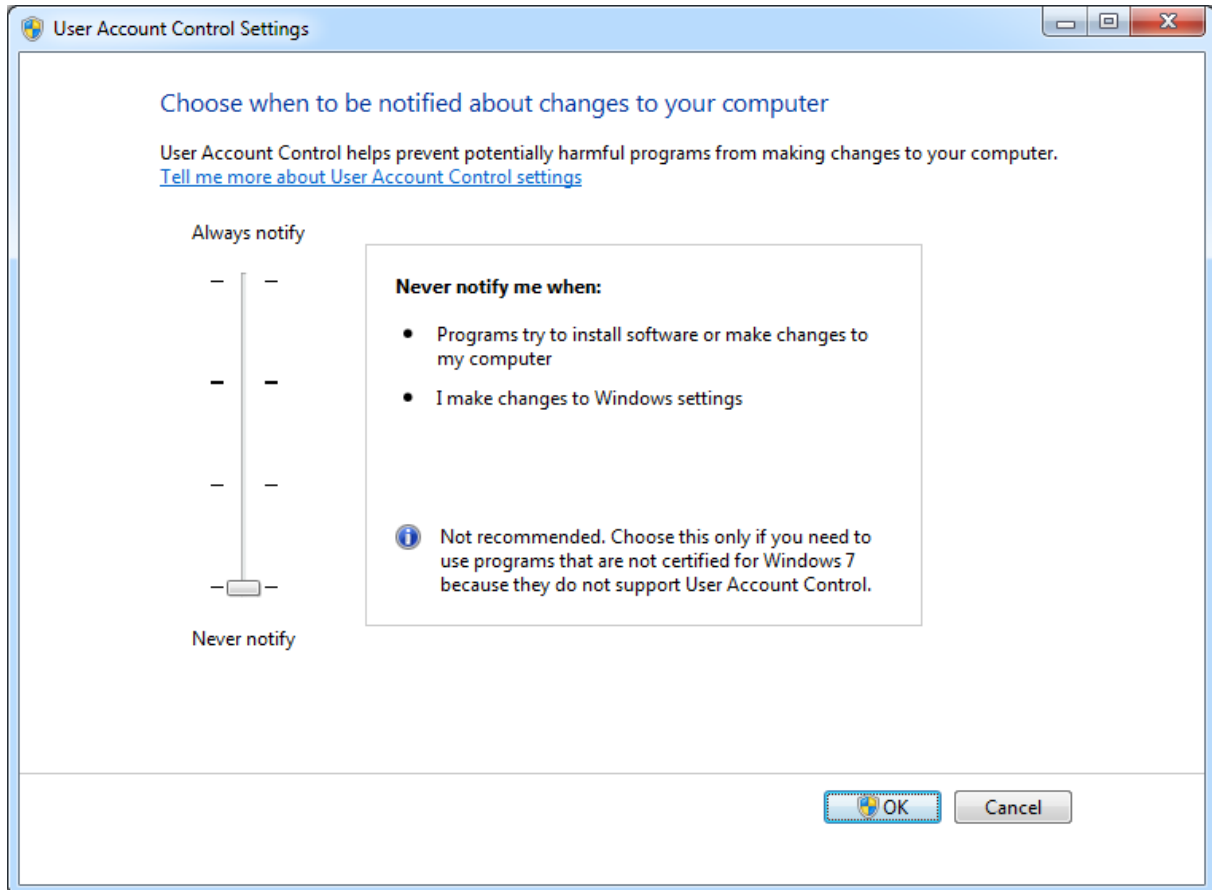


- Make sure that the status bar located in the bottom of the Registry Editor displays `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
If not, press F3 key and continue to look for a next search until you find it.
- When the search is completed, double-click **EnableLUA**.
- Change the Value data from 1 to 0.
- Close the Registry Editor dialog and restart the computer.



2. User Account Control Settings

- Control Panel → User Accounts → Run “User Account Control Settings”
- Click “Change User Account Control settings.”



- Select the control level as [Never notify] and click [OK].
- Restart your computer to apply the new setting value.

3. Create a New Account

- Control Panel → User Accounts → Add or remove user accounts
- Create a new account as Administrator type (i.e. “opcserver”).
- Register a password for the new account.
- In order for the OPC function to work properly, the newly added account must be logged on with the exact same account name and the password for both OPC Server PC and OPC Client PC.

4. The installation of the OPC Core Components

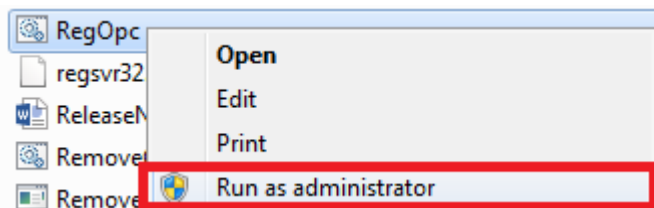
- Go to the [UltimateAccess installation folder] → Open the [OpcSvr] folder.
- Activate the [Setup] file and install the OPC Core Components.



- If the installation does not proceed normally, go to the www.opcfoundation.org website and install the latest version (x86 required).

5. Registration of CmHOPCSvr

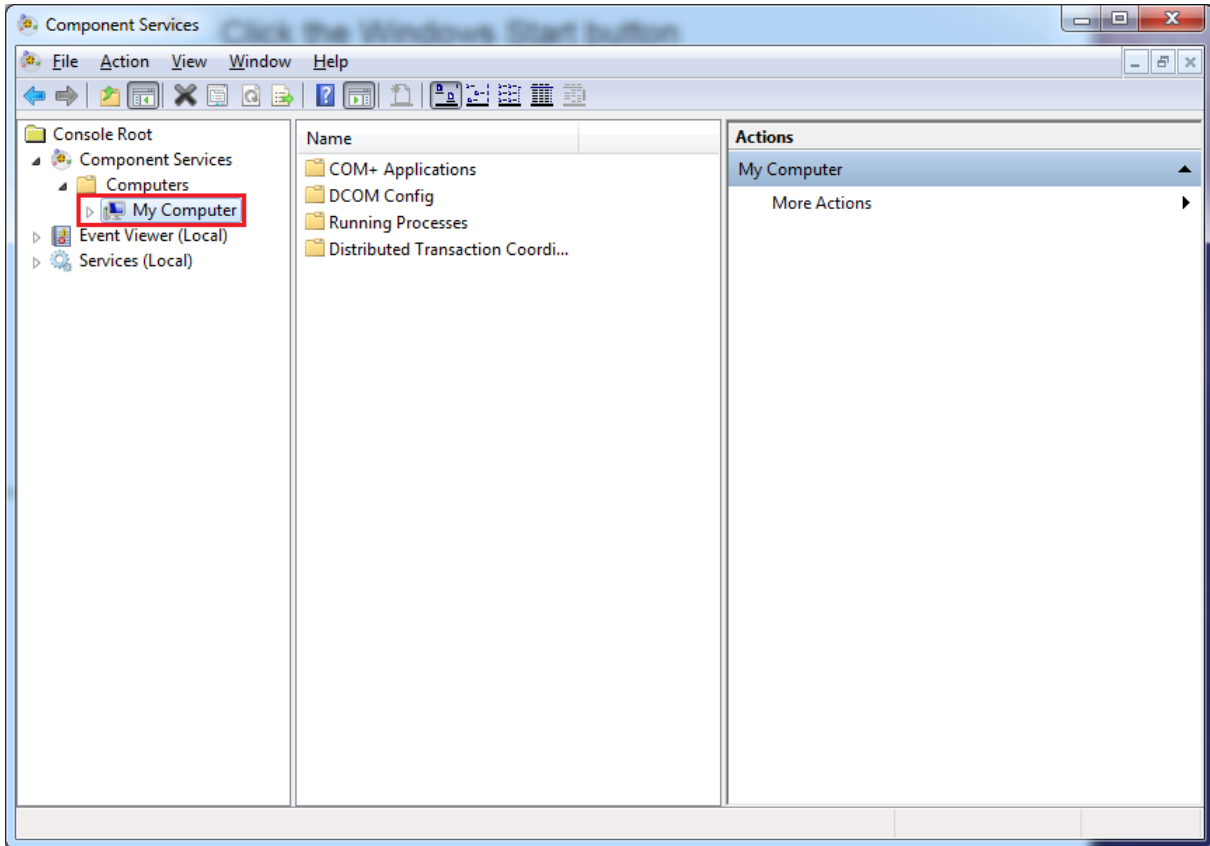
- Go to the UltimateAccess installation folder.
- Right-click the [RegOpc.bat] file and [Run as administrator].



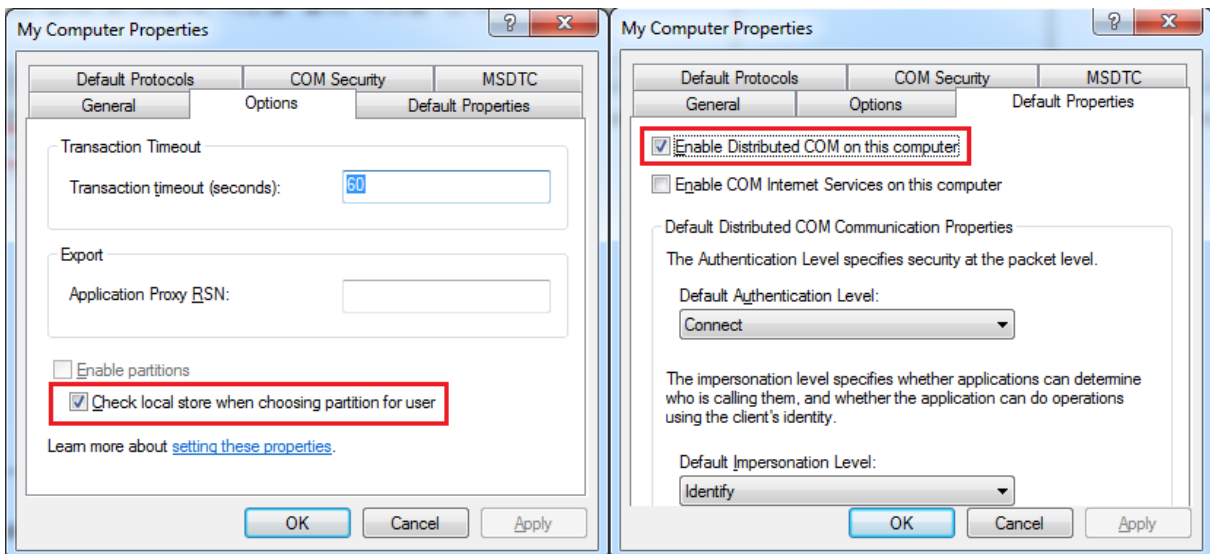
- In the Command Prompt window, move to the CIMON-SCADA installation folder and type in **CmHOpcSvr/regserver** to execute.
- This process registers the OPC Service on Windows.

6. DCOM Configurations

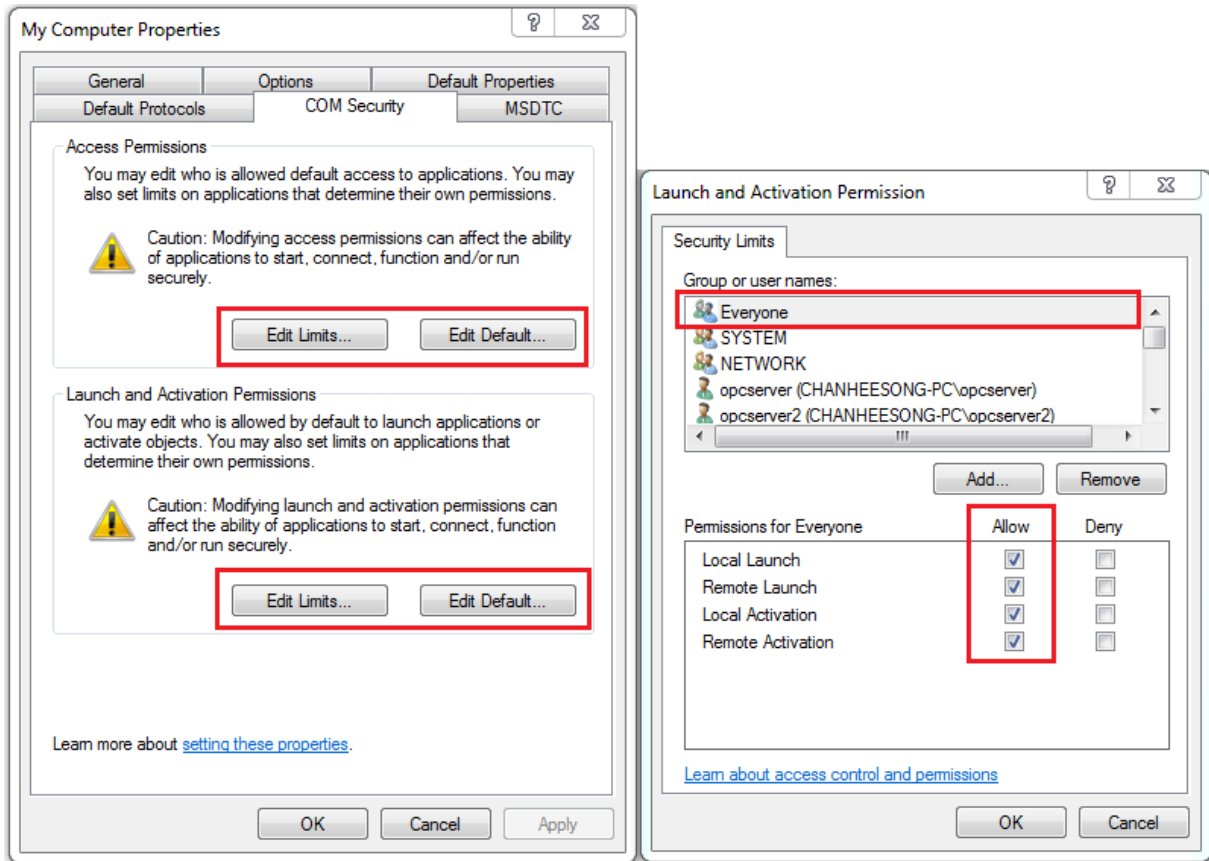
- Click the Windows Start button and type in “dcomcnfg” in the search box.



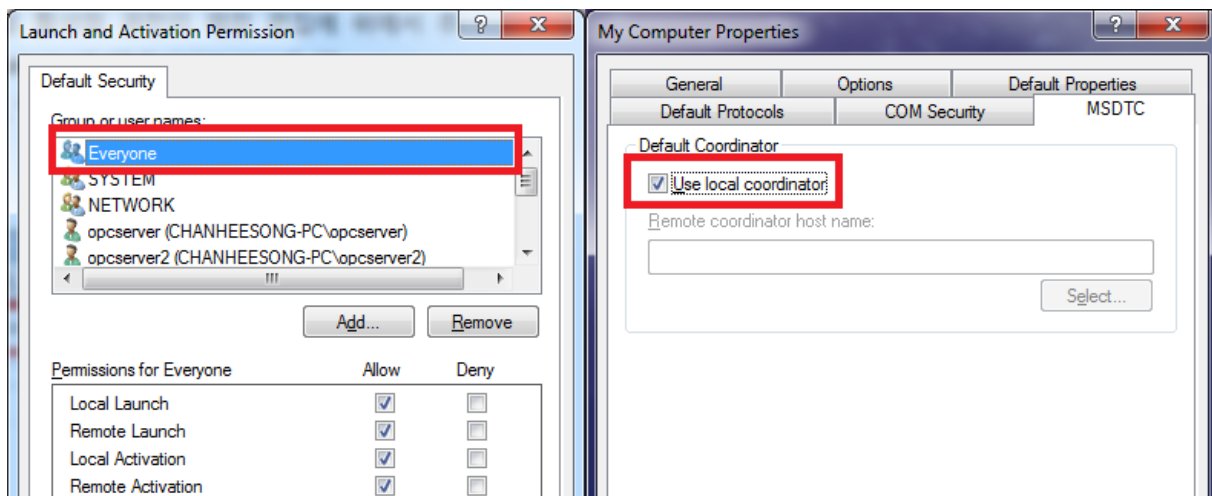
- [Component Services] → [Computers] → Right-click [My Computer] and select [Properties].



- Set the configurations as above for [Options] and [Default Properties].



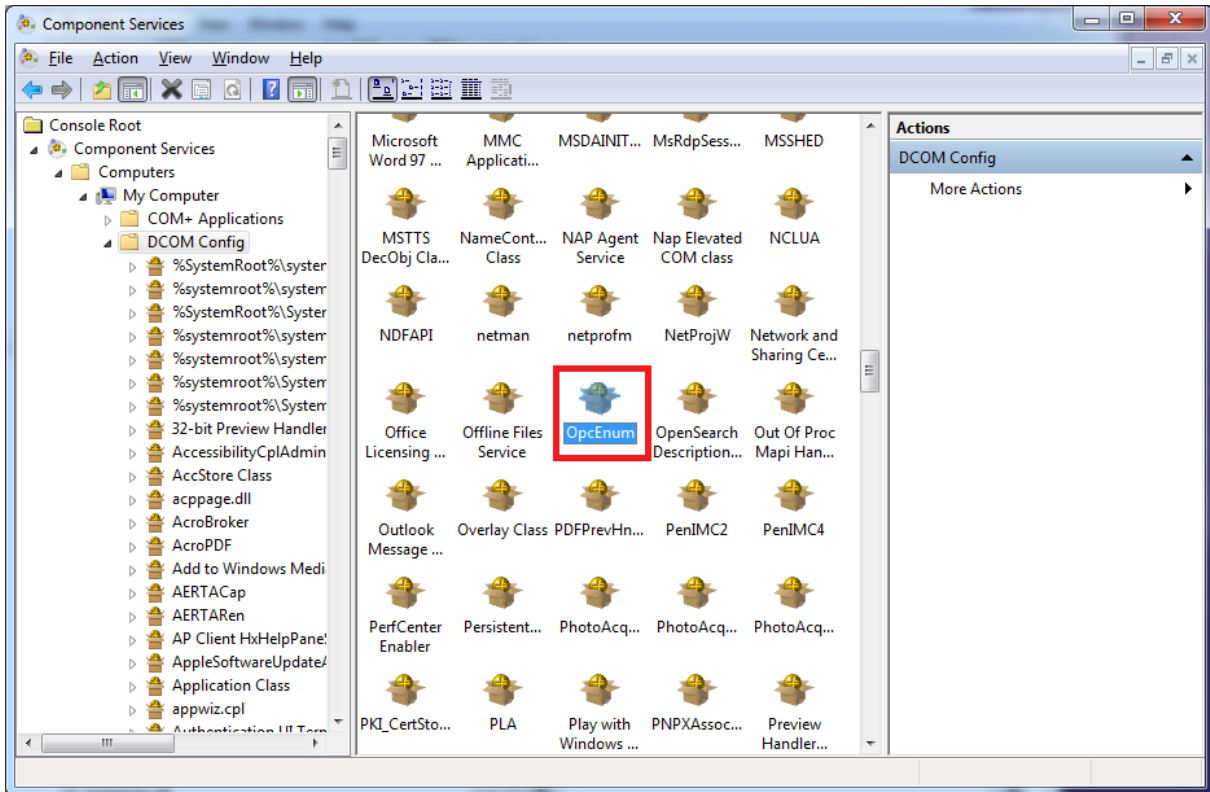
- After moving to the [COM Security] tab, add the new account (“**opcserver**”) along with “**Administrator**”, “**Administrators**”, “**Anonymous Logon**”, “**Everyone**”, “**Interactive**”, “**Network**”, “**System**” in the [Access Permissions] → [Edit Limits...] and [Launch and Activation Permissions] → [Edit Limits...] and select “**Allow**” for everyone.
- Set the same configurations as above for [Edit Default...]



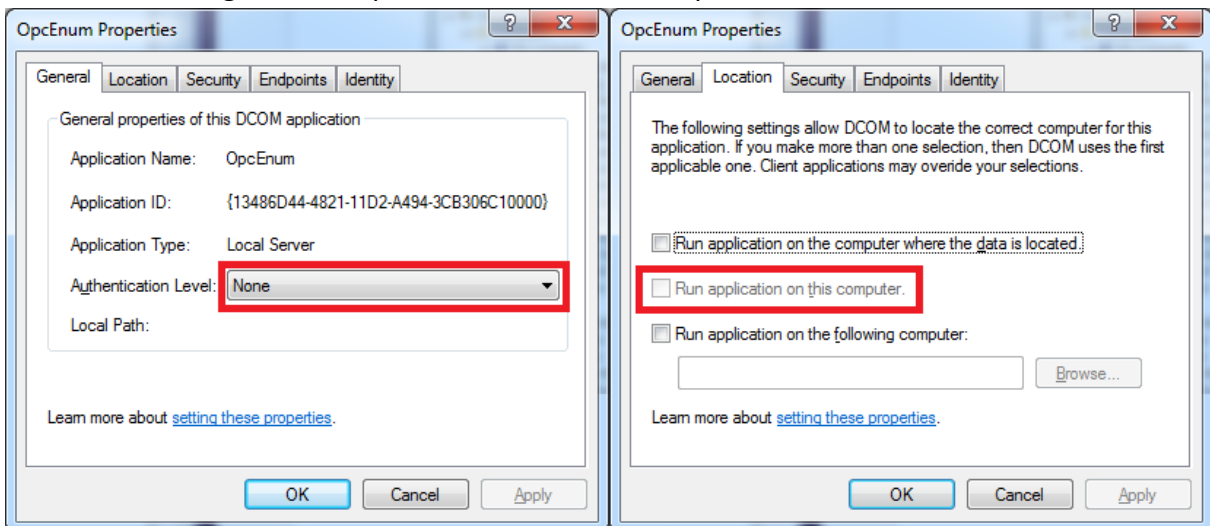
- Go to [MSDTC] tab and select “**Use local coordinator.**”

Frequently Asked Question

- When the configurations are completed, click [Apply] and then [OK].
- [Component Services] → [Computers] → [My Computer] → [DCOM Config].



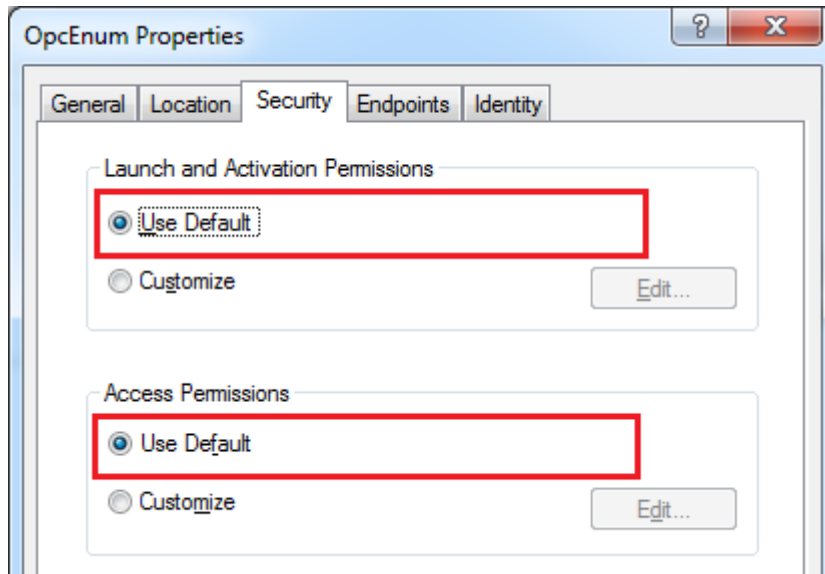
- Right-click “OpcEnum” and select “Properties.”



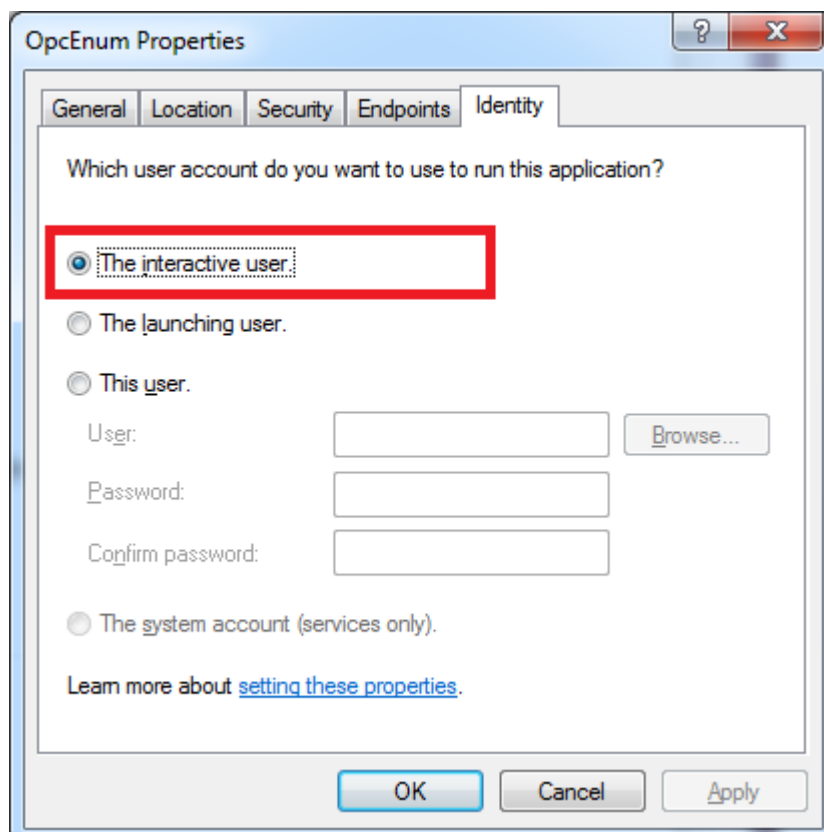
- Select the values as above for [General] and [Location] tabs.

Frequently Asked Question

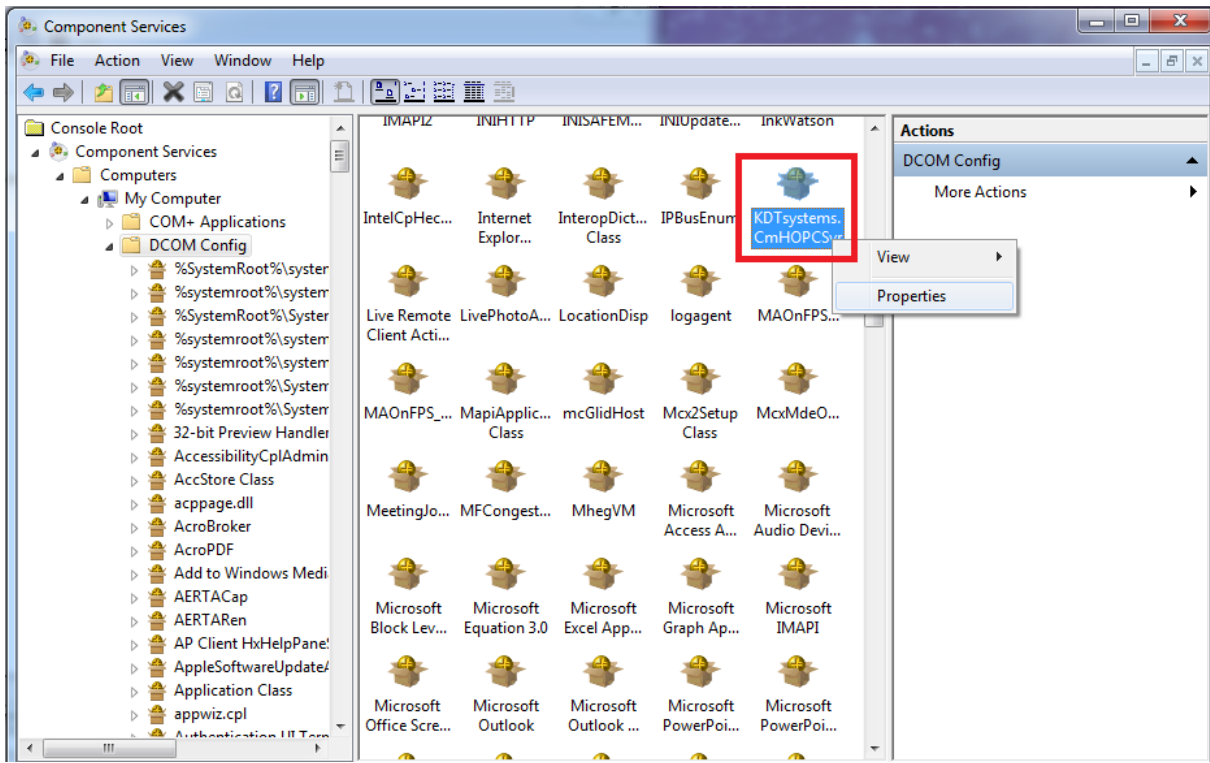
- Select “Use Default” for Permissions in [Security] tab.



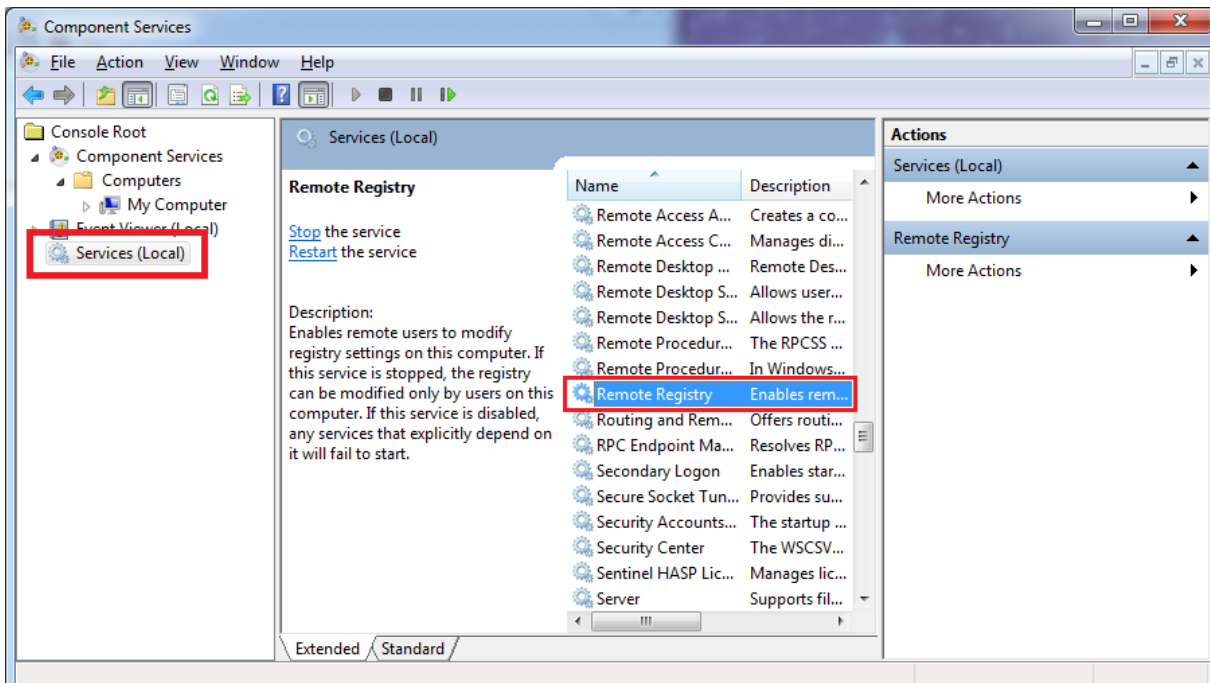
- Select “The interactive user” in [ID] tab and click [OK].



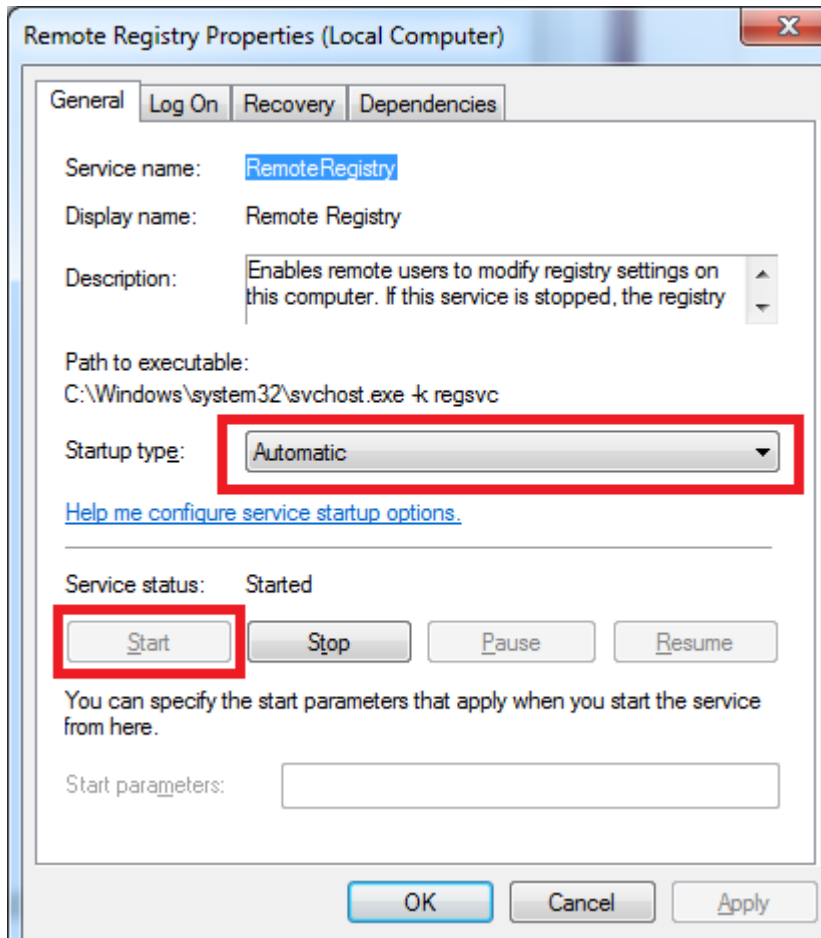
- Right-click “KDTsystems.CmHOPCSvr”, “CimonX.Document” and set the same configurations as above in the Properties.



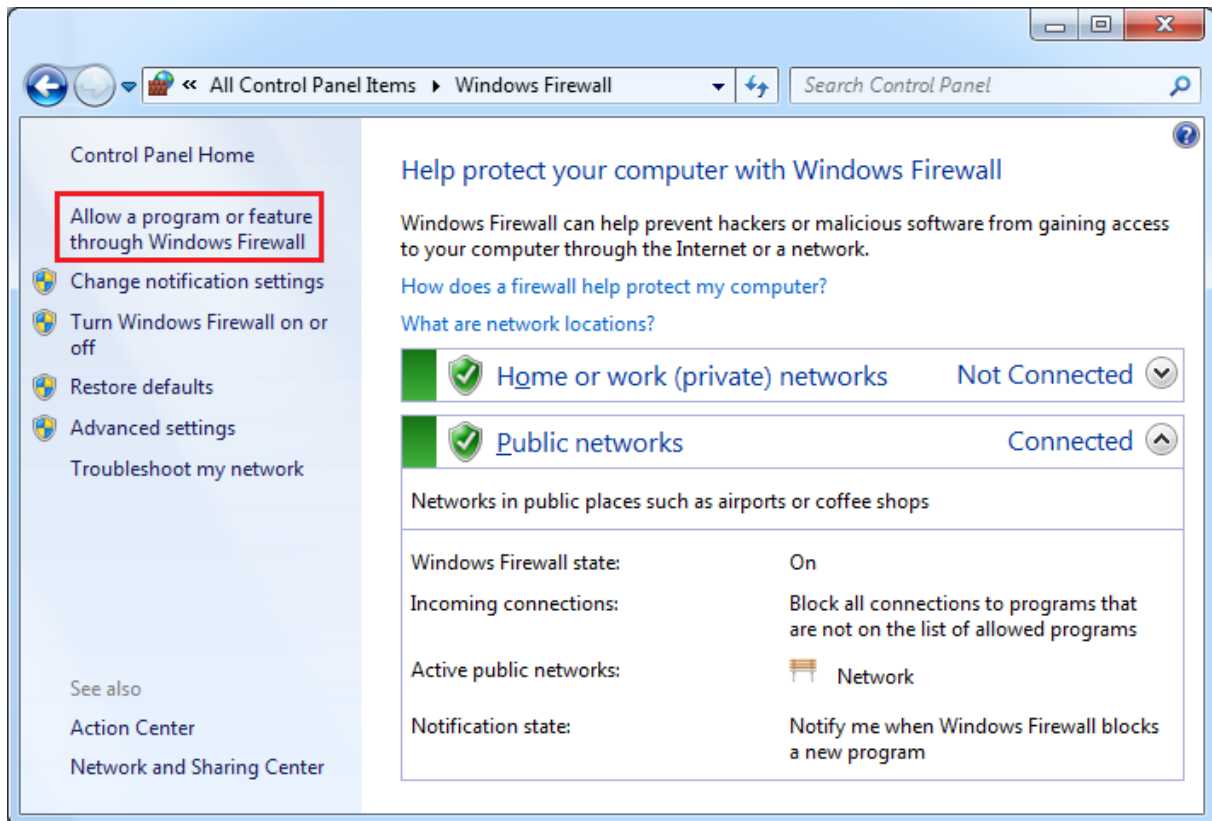
- Select “Services (Local)” → Right-Click Remote Registry and select Properties.



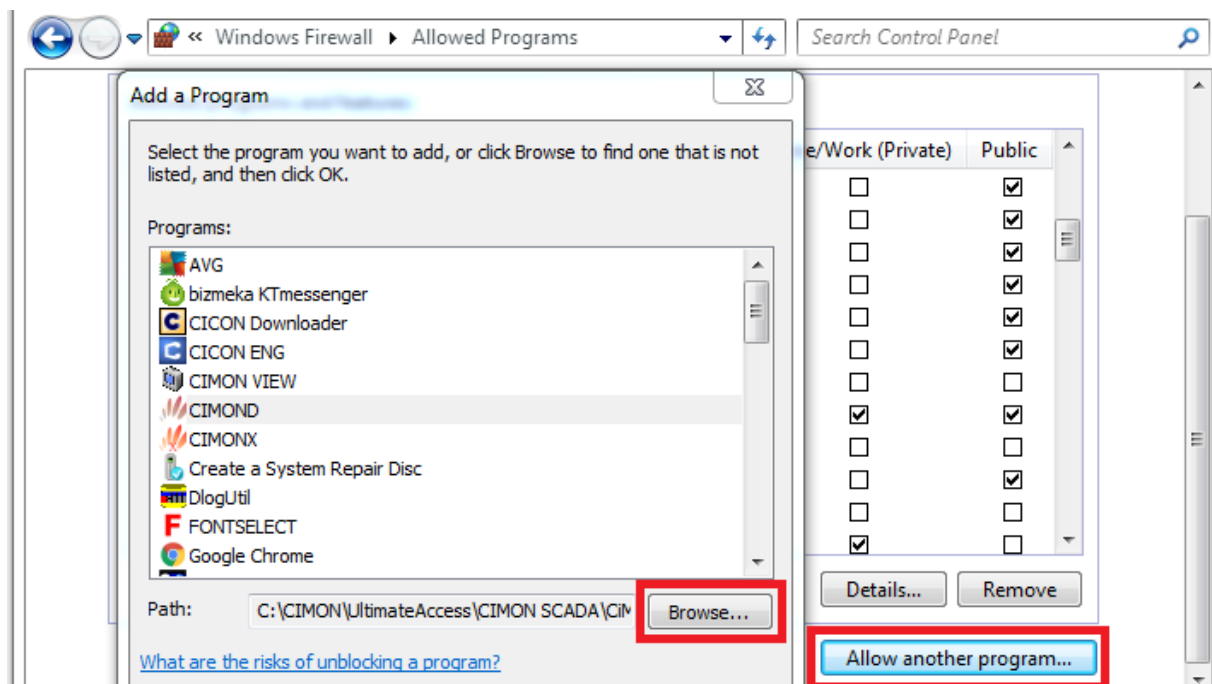
- Select Startup type as “Automatic” and click the [Start] button to initiate the service.



7. Firewall configurations

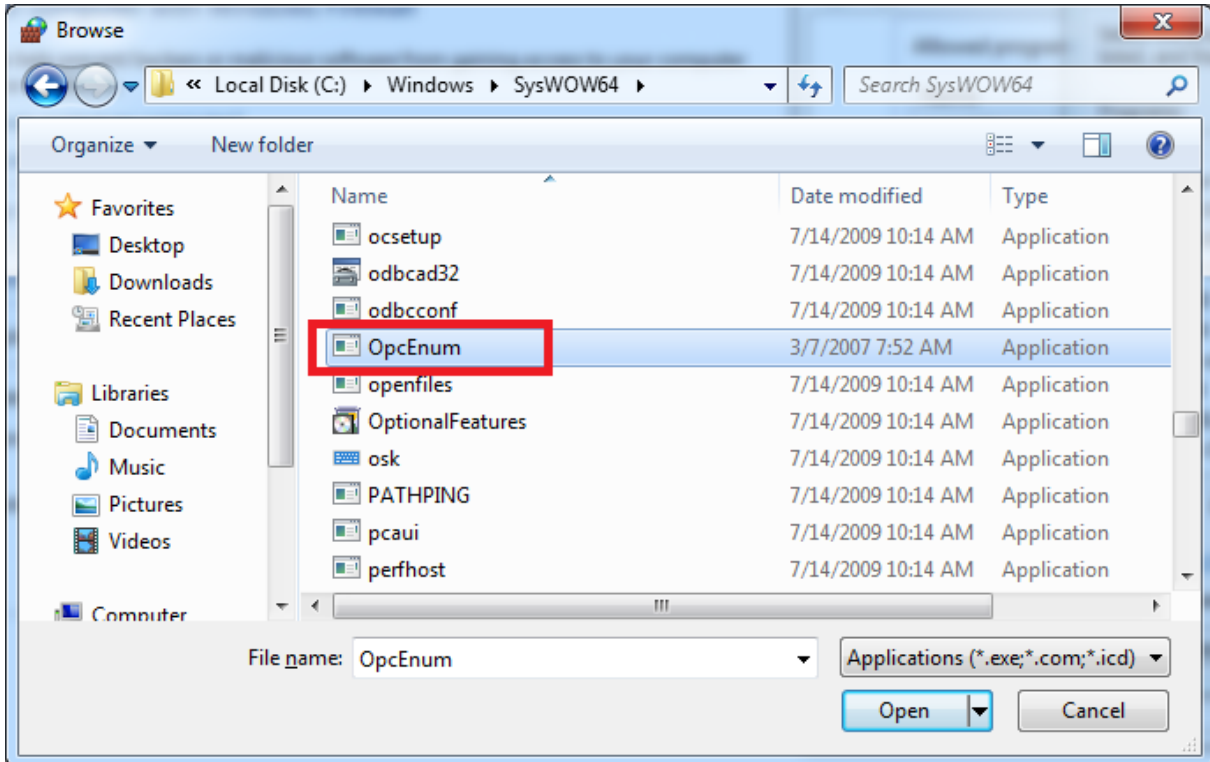


- Control Panel → Windows Firewall
- Select “Allow a program or feature through Windows Firewall”

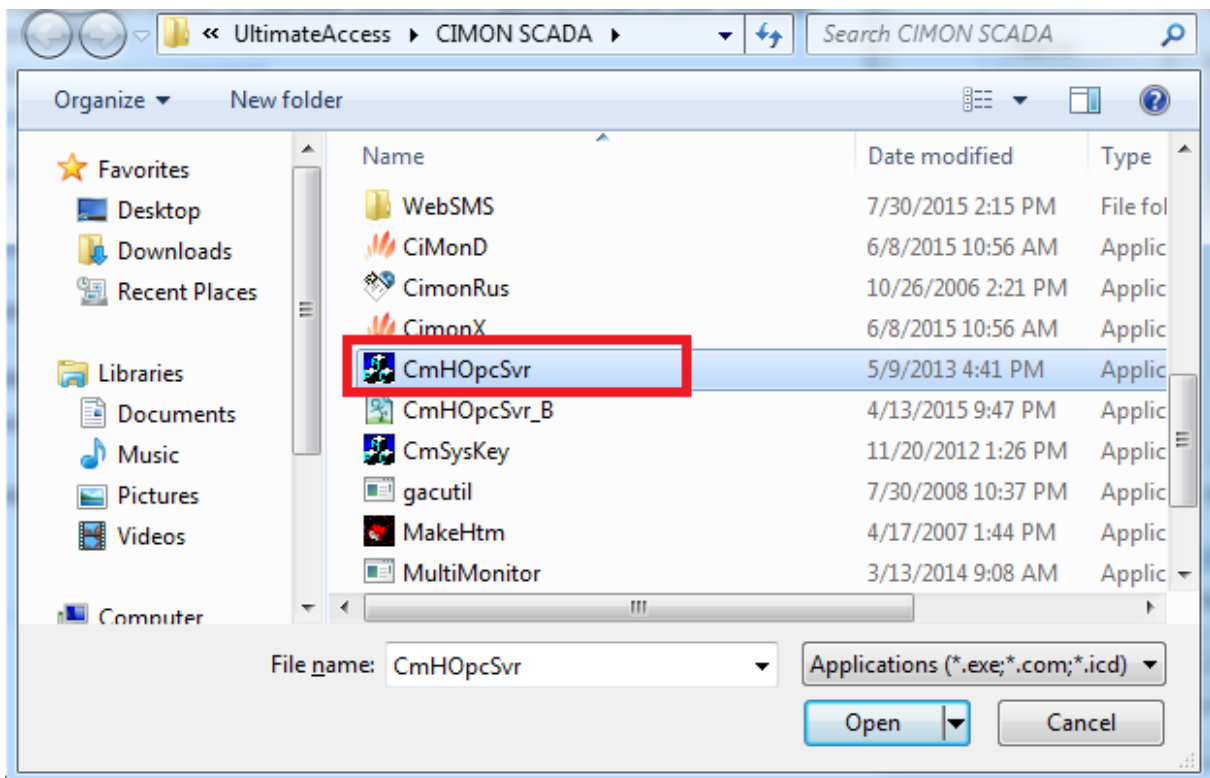


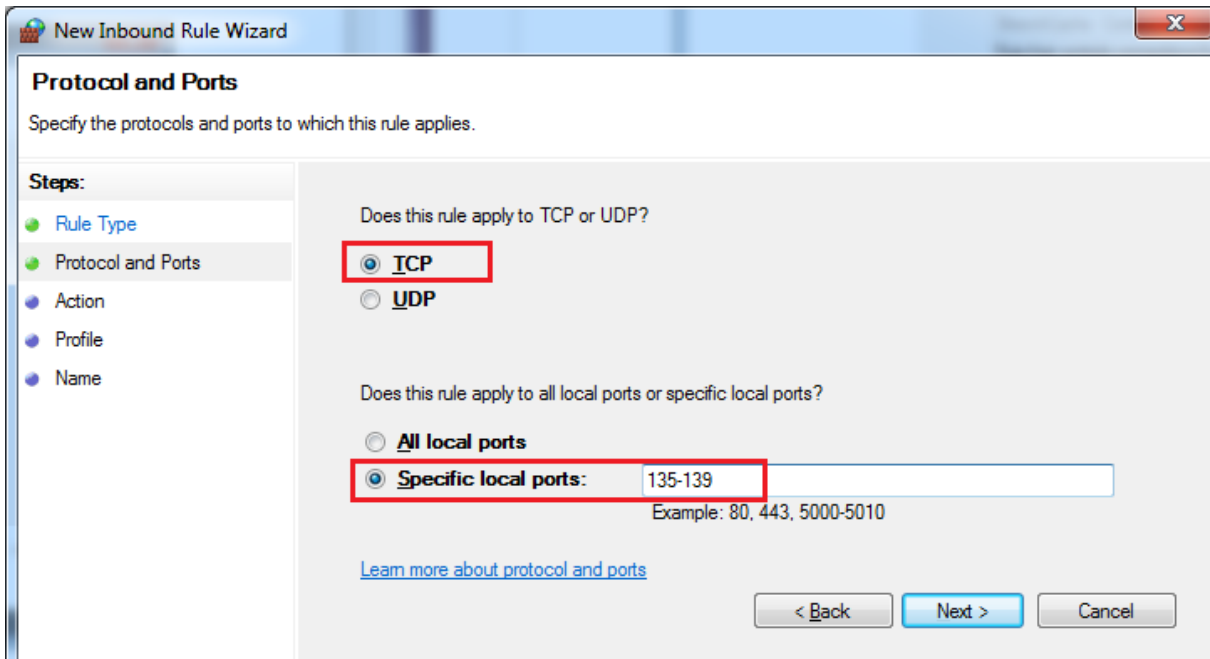
Frequently Asked Question

- Click [Allow another program] to add the file from the path below.
C:\Windows\System32\OpcEnum.exe (**32-bit Operating System**)
C:\Windows\SysWOW64\OpcEnum.exe (**64 bit Operating System**)



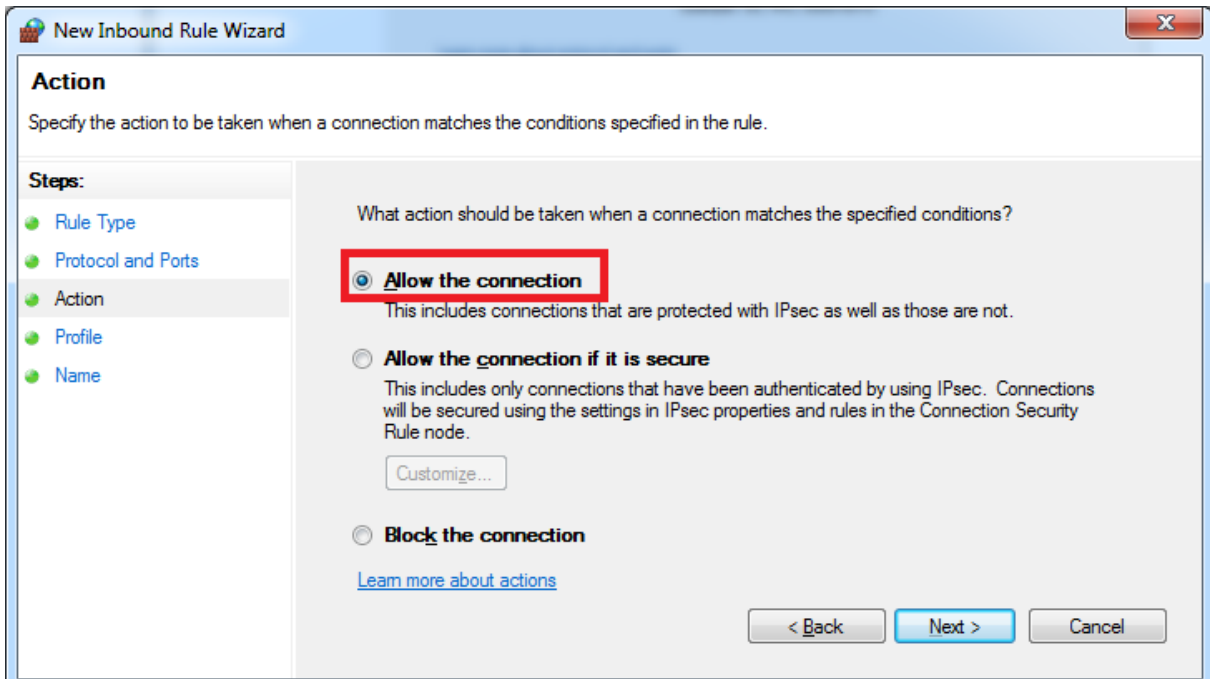
C:\CIMON\UltimateAccess\CIMON SCADA\CmHOpcSvr





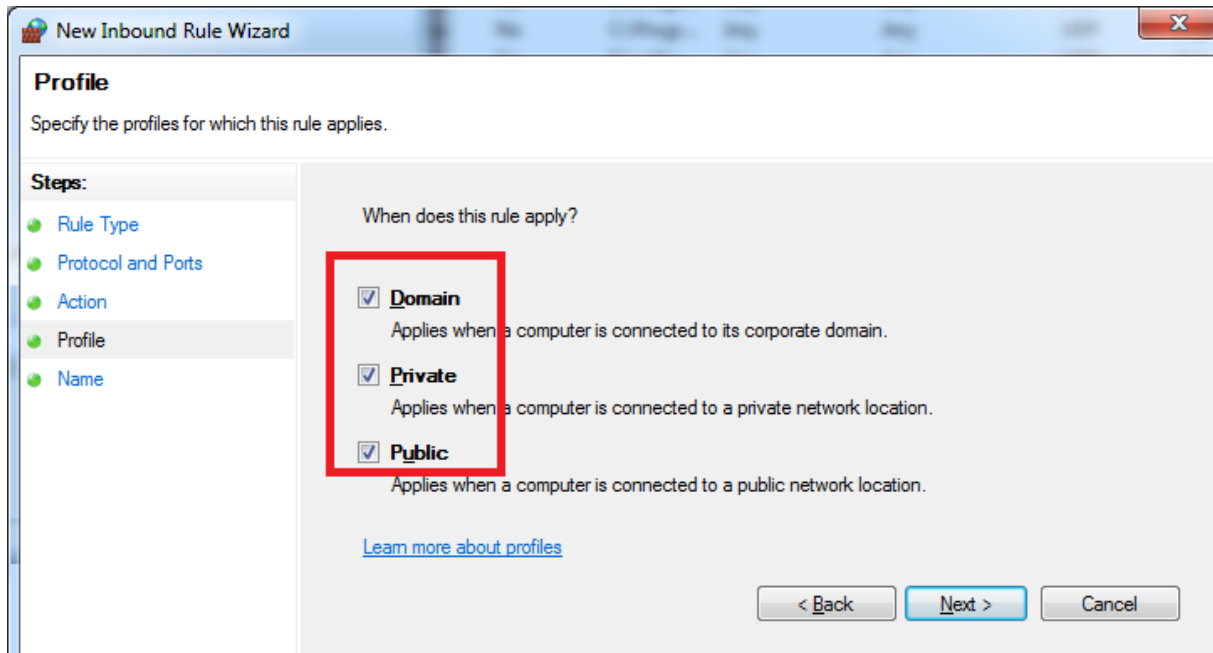
The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports' (highlighted), 'Action', 'Profile', and 'Name'. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected and highlighted with a red box) and 'UDP'; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports:' (selected and highlighted with a red box). The 'Specific local ports:' field contains the text '135-139' and has an example below it: 'Example: 80, 443, 5000-5010'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about protocol and ports' is also present.

- Select “TCP” and enter “135-139” for specific local ports. This opens all ports from 135 to 139. Click [Next].

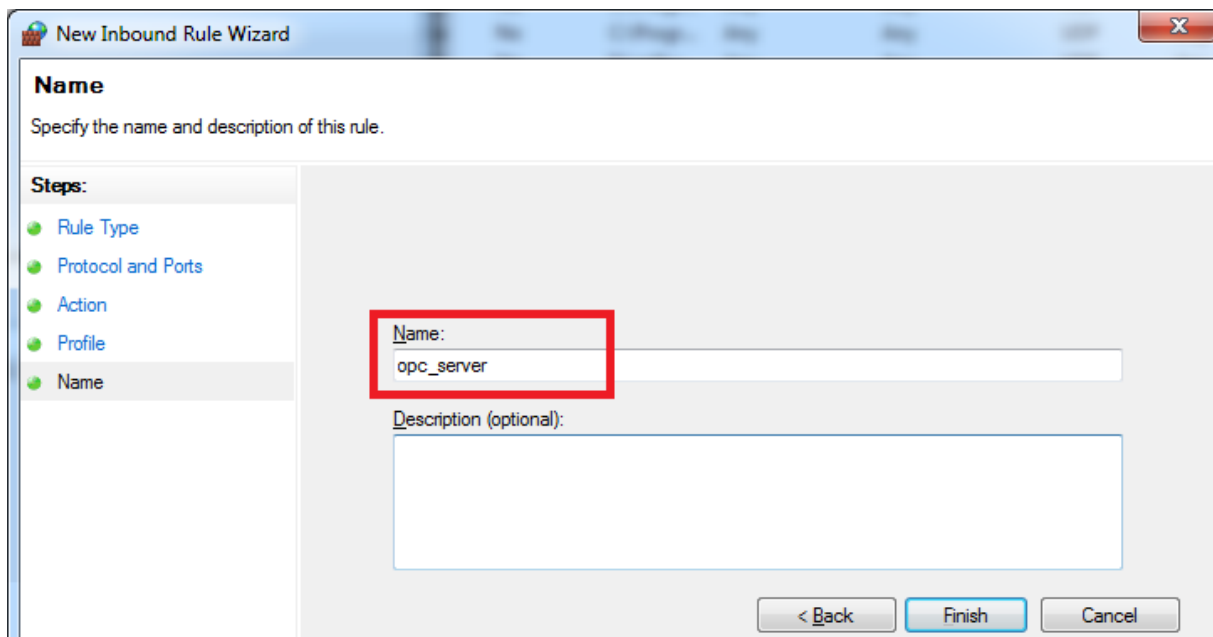


The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action' (highlighted), 'Profile', and 'Name'. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (selected and highlighted with a red box), 'Allow the connection if it is secure', and 'Block the connection'. Below the 'Allow the connection' option is a text description: 'This includes connections that are protected with IPsec as well as those are not.' Below the 'Allow the connection if it is secure' option is a text description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button. Below the 'Block the connection' option is a text description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about actions' is also present.

- Select “Allow the connection” and click [Next].



- Select “Domain”, “Private”, “Public” and click [Next].



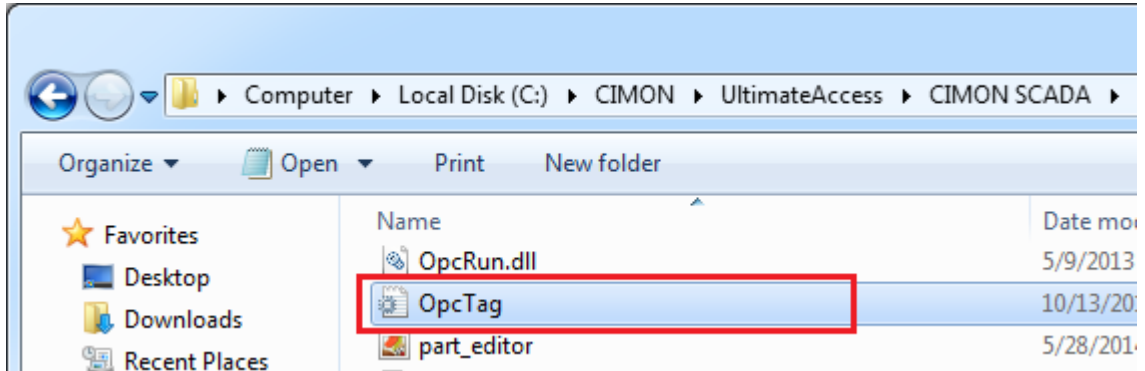
- Type in the name for the new inbound rule (i.e. “opc_server”) and click [Finish].

***This is the end of the Windows DCOM and Firewall configurations.**

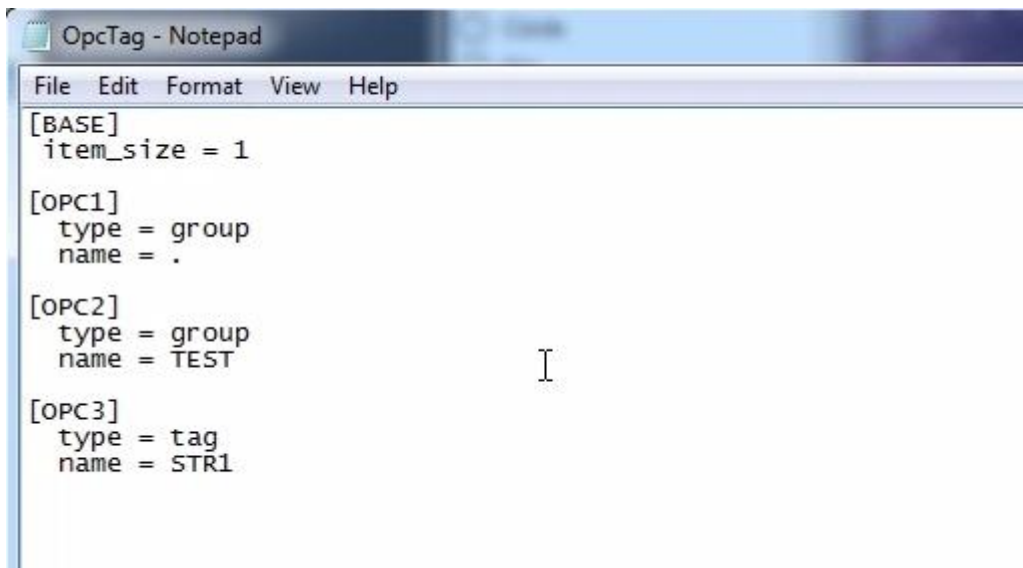
Now, we’re going to see how SCADA (OPC Server) communicates with an OPC Client PC.

UltimateAccess (CIMON-SCADA) OPC Server Communication with an OPC Client PC

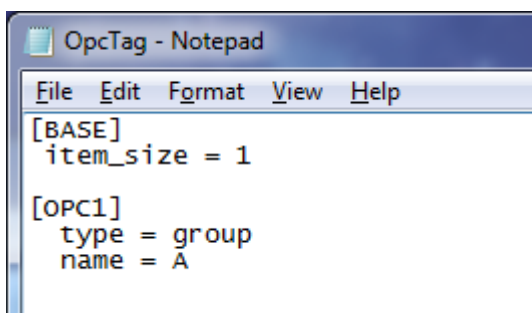
1. Execute Cimond and open a new project.
2. Register a group tag named "A." This group tag name will be identical with OPC tag.
3. Go to UltimateAccess installation folder and open "OpcTag.ini" file.



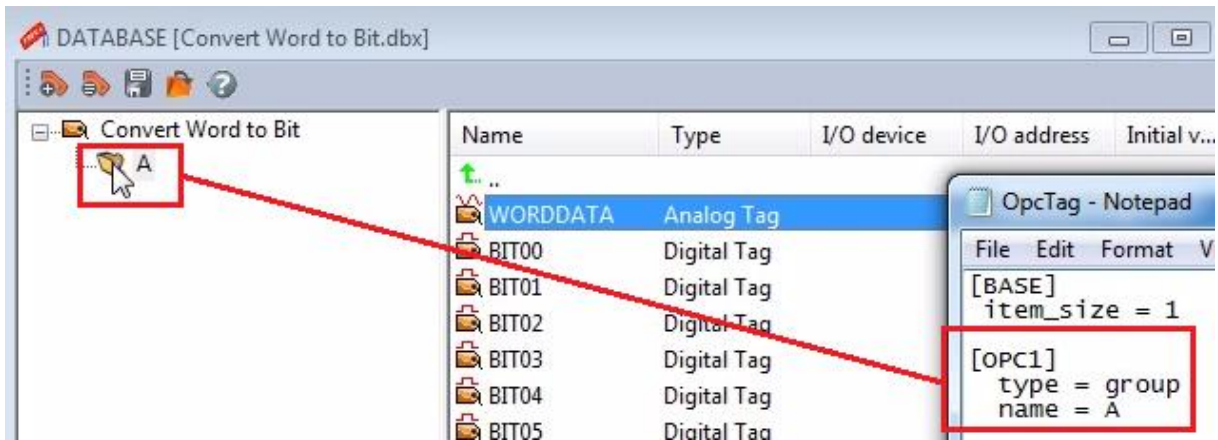
4. When you first open it, the "OpcTag.ini" file will be displayed as below.



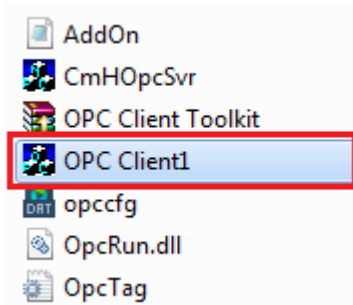
5. Edit the name of the OPC group tag to "A" as previously configured in Cimond.



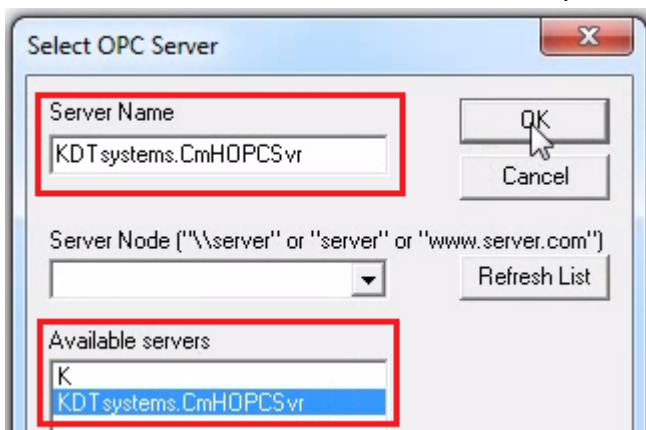
- Ensure that the group tag "A" in Cimond is identical with that of OpcTag.ini file.



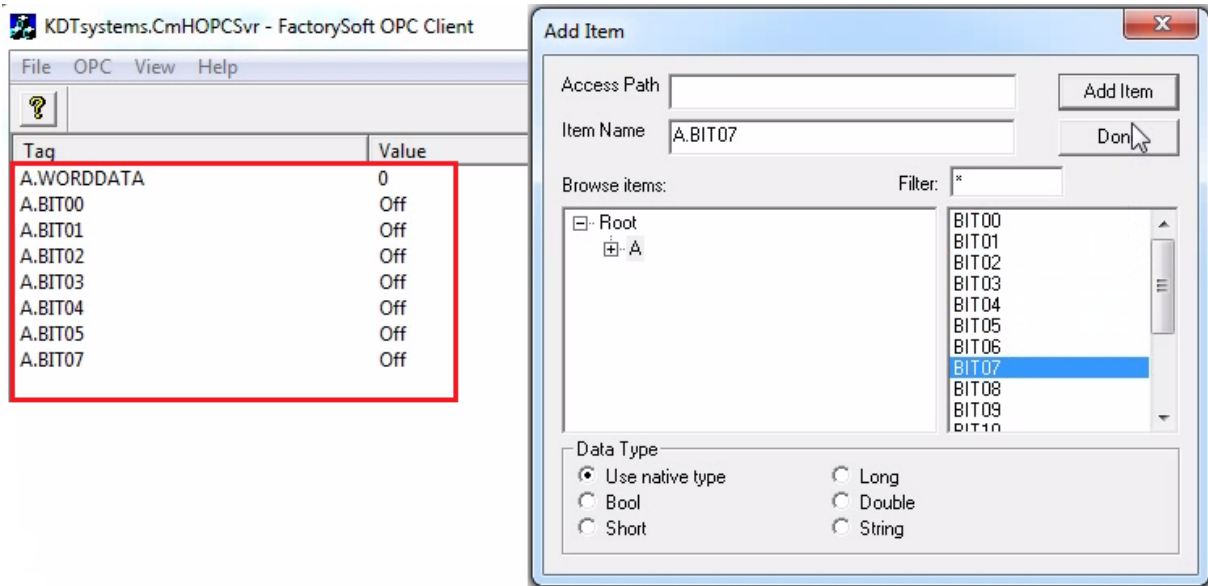
- Save the OpcTag.ini file and run Cimond. Cimond must be running at all times in order to communicate between OPC Server and OPC Client.
- Run "**OPC Client1.exe**" file from the [OPC Server Components] folder downloaded from CIMON website.



- Go to [OPC] → [Connect] and select "KDT systems.CmHOPCSvr" for OPC Server.



10. Go to [OPC] → [Add Item] and select the tags that you want to communicate.



11. You can write and read data value between **(CIMON SCADA) OPC Server** and **OPC Client program** vice versa.

