

# **Advantech SE Technical Share Document**

Date	2019 / 09 / 25					
Cohoran	■ FAQ □ SOP	<b>Related Product</b>	WebAccess/SCADA, OPCDA			
Category	Driver Tech Note					
Abstract Setting DCOM for OPC under Windows 7 (32 / 64 bit)						
Keyword	WebAccess, OPCDA Server, OPCDA Client, DCOM					
Related OS	N/A					
	I	Revision History				
Date	Version	Author	Reviewer	Description		
2019/05/20	V1.0	Eden.Sun		Update		

### Problem Description & Architecture:

## Setting DCOM for OPC under Windows 7 (32 / 64 bit)

Brief Solution - Step by Step:

# 1. Windows 7 (32 / 64 bit) configuration overview

This tutorial walks through the DCOM configuration and security settings under Windows 7 to configure an OPC server



- User access authorization control
- Windows firewall

The precondition is opc server and client computers need to have **the same Windows System login account**.

The steps to securely configure the OPC Server are: first of all, setting the wide DCOM protocol security authorizations for the computer access (MyComputer) then create some exceptions on the firewall so the OPC client can access the OpcEnum which gives the list of the OPC servers running on the machine, and last, configure the DCOM access permissions for OpcEnum and the OPC server.

The steps described in this tutorial will not follow this order to make it shorter



# **2.** OPC Server Settings

### A. Wide security "MyComputer" settings

• Managing the settings for the general computer access, users and permissions

Press 🔀 + **R** to open the Run menu type "**DCOMCNFG**" on the text area and press **ENTER** to open the Component Services window

dcomcnfg	
₽ See more results	

• Under: Component Services -> Computers, Right-click on "My Computer" and Choose the "Properties" from the menu.

Click the "Default Properties" Tab and configure as follow:

Enable Distributed COM on this computer checked.

Default Authentication Level Connect

Default Impersonation Level Identify

Component Services		
🙆 File Action View Window Help	My Computer Properties	
	Default Protocols COM Security	MSDTC
Console Root Component Services My Computer Event Viewer (Local) Services (Local)	General       Options         Inters       Image: Enable Distributed COM on this computer         Enable COM Internet Services on this computer         Default Distributed COM Communication Properties         The Authentication Level specifies security at the point of the impersonation level specifies whether applicate who is calling them, and whether the application causing the client's identity.         Default Impersonation Level:         Identify         Security for reference tracking can be provided if a and that the default impersonation level is not anor         Provide additional security for reference tracking the security for tracking the security	Default Properties



• Click on the "COM Security" tab

For the "Access Permissions", we need to check **user accounts** are exist and give that local and remote access, it is necessary to request user account information, also add the users accounts and/or groups who should be able to access the COM service in this machine.

Click "Edit Limits" button within the "Access Permissions" Hit Add enter the object name (8 users account are below.) Hit OK Check local access and remote access boxes Click OK.
 Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM", "INTERACTIVE", "NETWORK", "Everyone", "Performance Log Users" and "Distributed COM Users") Repeat the operations until completed.



• Click "Edit Default" button within the "Access Permissions" Hit Add enter the object name (7 users account are below.) Hit OK Check local access and remote access boxes Click OK.

Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM", "INTERACTIVE", "NETWORK", "Everyone" and "SELF")

Repeat the operations until completed.



For the "Launch and Activation Permissions" configure as needed, adding only permissions to the users and/or groups who should be able to access the COM service in this machine, setting the permissions. To assign permissions to a special group or user, add it and check the desired boxes.

• Click "Edit Limits" button within the "Launch and activation Permissions "Hit Add enter the object name (8 users account are below.) hit OK check the desired allow or deny boxes click OK.

Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM", "INTERACTIVE", "NETWORK", "Everyone", "Performance Log Users" and "Distributed COM Users") Repeat the operations until completed.

* + 2 🕅 X 🗆 🖁	ly Computer Properties	1414
Console Root  Component Services  Computers  Computers  Configuration  Configurat	General Default Properties Default Protocols COM Security Access Permissions You may edd who allowed default access to applications. You may allo as thinks on applications that determine there own permissions. Caution: Modifying access permissions can effect the ability of applications to start, connect, function and/or rus securely. Eddt Limits. Eddt Limits. Eddt Default.	Launch and Activation Permission
	Launchs and Activation Permassons You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that defamine their own permasions. Automation is a structure of activation permassons can and/or run securely. Edit Limits Edit Default.	Add Permissions for Everyone Nor Deny Local Launch IV Everyone Reside Launch IV Everyone Ever
	Learn more about setting Treas properties	Learn about access control and permaterins CK Cancel

• Click "Edit Default" button within the "Access Permissions" Hit Add enter the object name (6 users account are below.) hit OK check the desired allow or deny boxes click OK.

Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM",



#### "INTERACTIVE", "NETWORK" and "Everyone")

Repeat the operations until completed.



Press OK at end to save settings.



### B. "OpcEnum" Settings

Manage the users/groups that should be able to see the existing OPC servers running on the machine (It is possible to give authorisation to many users/groups to see the existing OPC servers running but authorise different users/groups to access to different servers. See: 4. Permissions settings)

● Under: Component Services → Computers → My Computer → DCOM Config, find "OpcEnum" on the list right click on it and Choose "Properties" from the menu.



- On the tab "General", Authentication Level chooses the "Default".
- On the tab "Location", check the box "Run application on this computer" (If it can use.).
- On the tab "Security", Launch and Activation Permissions and Access Permissions choose the "Use Default", and Configuration Permissions choose the "Customize".



# **AD\ANTECH**

Enabling an Intelligent Planet

### C. "Kepware Communication Server X.XX" Settings

Manage the users/groups that should be able to see the existing OPC servers running on the machine (It is possible to give authorisation to many users/groups to see the existing OPC servers running but authorise different users/groups to access to different servers. See: 4. Permissions settings)

● Under: Component Services→Computers→My Computer→DCOM Config, find "Kepware Communication Server X.XX" on the list right click on it and Choose "Properties" from the menu.



- On the tab "General", Authentication Level chooses the "Default".
- On the tab "Location", check the box "Run application on this computer" (If it can use.).
- On the tab "Security", Launch and Activation Permissions and Access Permissions choose the "Use Default", and Configuration Permissions choose the "Customize".



**ADVANTECH** 

Enabling an Intelligent Planet

#### **D. OPC Server process Settings**

Under: Component Services → Computers → My Computer → DCOM Config, find OPC process on the list for this example we install the "BwOpcServerDA and BwOpc ServerAE", right click on it and Choose "Properties" from the menu.

A Component Services A: File Action View Window Help				
** 200 X0 8 00 1	IYBE D			
Console Root -	Name	Application ID +	Actions	
🔺 🌺 Component Services	🔮 Background Intelligent Transfer Service	(69AD4AEE-51BE-4395-A82C-86	DCOM Config	
My Computers COM- Anninetim COM- Anninetim DCOM Config Skystembol/Skystem3 Skystembol/Skystembol/Skystem3 Sk	BOEUD.aurcher Class     BdeUDSv     Bitmap Image     Bluewire unpairing blevebion surrogate     BuwArchive.Class1     BuwArchive.Class2     BuwArchive.Class2     BuwArchive.Class2     BuwArchive.Class2     BuwArchive.Class2     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class2     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class3     BuwArchive.Class     BuwArchive.Class     BitmapHandet.all     DisShiExcill     BitmArchive.Class     BitmapHarchive.class     BitmArchive.Class     BitmArchive.Class     BitmArchive.Class     BitmArchive.Class     BitmArchive.Class     BitmArchive.Class     BitmArchive.Class     BuwArchive.Class     BitmArchive.Class     BitmArchive.cla	(489)BHT-6CT-4187-A91-A91 (C489)CBHT-6CT-4187-A91-A91 (C4887C87-673-48FF-ADD-1) (D115/528-1075-101A-1C11b-40) (D115/528-1073-494-1483-40) (2018/528-1073-494-1483-40) (2018/528-1073-494-1483-40) (2018/528-1073-494-400-400-400-400-400-400-400-400-400	More Action:	¢

- On the tab "General", Authentication Level chooses the "Default".
- On the tab "Location", check the box "Run application on this computer" (If it can use.).
- On the tab "Security", Launch and Activation Permissions and Access Permissions choose the "Use Default", and Configuration Permissions choose the "Customize".

BerOpcServerBA and BerOpcServerAE Properties	BwOpclanerDA and BwOpclanerAl Arepetter	BwOpcServerDA and BwOpcServerAE Properties
General Lucation Security Endpoints Intensity	General Location Security Endpoints Mervily	Beneral Lacator Security Endoornis Identity
Sensul popolies of the DCOM application Application Name: SinOpcSenveX4 and BnOpcServeX4E Application ID: (INSDE358.20.57.41EA-0028-3458879767A4)	The following tetrings allow DCOM to locate the correct consider to the application. If you make more than one stelection, then DCOM use the fail applicable one. Diant applications may owned your selections.	Learch and Activation Premissions
Application Type: Local Server	E Run application in the computer where the data is located.	
SufferitionLeve Defaul	TRun application an the company.	Actan Persinara
LocalPath	Pun application on the following computer:	Use Delaw     Octomer
		Configuates Persenioro
Learn vers about <u>antras Transmiss</u>	Learness about <u>anima Tana anamina</u>	Learn new about <u>perfection presentes</u>

Exit the DCOMCNFG



# **3.** Server Firewall Settings

Configure the firewall exceptions

Press 🎟 + **R** to open the Run menu type " **wf.msc**" on the text area and press **ENTER** to open the Component Services window



### A. OPC Server Enumerator exception

Right click Inbound Rules and choose New Rule from the drop down menu, the Inbound Rules wizard will appear

Indows Eine	wall with Advance	Amount Balan		_	_		Action
Inbound B	ules	Renting Francis		Beeffe	Freehold	1.12	Informat Bular
Outboo	New Rules.	and the strength of the streng	Bitt Descending	A 1	Enabled	- î 1	and the first
Connec	Eiter by Drofile	ercaching (Content-In)	Bits Peercaching	AS	D4D	2	New Kule
Monito	Elkerky Gate	ercaching (APC)	orts Peercaching	48	neo Nie	28	Filter by Profile
-	Piker by state	<ul> <li>Bereaching (MCD In)</li> </ul>	OTTS Researching	A.0	FND File	21	Tilter by State
	View	Cache Context Rational (MTTP to)	Buis Peercaching ResoluCasha, Contrast Rate	48	Ne	<u></u>	V Filter by Group
	12/01/02	Cache Mostad Cache Senar (HTT	BranchCache - Content Net	42	Nie	1011	
	Refresh	Cache Press Discourse (AVCD. In)	BranchCache - Rosted Cach	A8	Nio.	2	View
	Export List	et to a Network Projector (TCD, In)	Connect to a Network Dusia	Domain	Nio	2	Cl. Refresh
	Help	et to a Network Projector (TCP-In)	Connect to a Network Projest	Private	No	2	🔒 Export List
	1.00	Connect to a Network Projector (ICP-II)	Connect to a Network Proje.	Private	No	2	E Helo
	0	Connect to a Network Projector (WSD Ev	Connect to a Network Project	Domain	Nn	Å	III Hep
	ě	Connect to a Network Projector (WSD Ev.	Connect to a Network Proje	Domain	No	2	
	ě	Connect to a Network Projector (WSD Ev	Connect to a Network Proje.	Drivate	No	2	
	ē	Connect to a Network Projector (WSD-In)	Connect to a Network Proje-	A.8	No	- A	
		Core Networking - Destination Unreacha	Core Networking	48	Ves	A	
	0	Core Networking - Destination Unreacha	Core Networking	AR	Yes	A	
	0	Core Networking - Dynamic Host Config	Core Networking	All	Ves	A	
	ē	Core Networking - Dynamic Host Config.	Core Networking	All	Ves	A	
	e	Core Networking - Internet Group Mana	Core Networking	AE	Yes	A	
		Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	A	
	0	Care Networking - IPv6 (IPv6-In)	Core Networking	AB	Ves	A	
		Core Networking - Multicast Listener Do	Core Networking	AB	Ves	A	
	6	Core Networking - Multicast Listener Qu	Core Networking	AB	Yes	A	
	0	Core Networking - Multicast Listener Rep.	. Core Networking	AB	Ves	A	
	0	Core Networking - Multicast Listener Rep.	Core Networking	AB	Yes	A	
	0	Core Networking - Neighbor Discovery A.	Core Networking	AB	Yes	A	
	0	Core Networking - Neighbor Discovery S.	Core Networking	AB	Ves	A	
	0	Core Networking - Packet Too Big (ICMP.	Core Networking	All	Yes	A	
	0	Core Networking - Parameter Problem (L.	Core Networking	AB	Ves	A	
	6	Core Networking - Router Advertisement.	. Core Networking	All	Ves	A	
	0	Core Networking - Router Solicitation (IC.	Core Networking	All	Yes	A	
	0	Core Networking - Teredo (UDP-In)	Core Networking	All	Ves	A	



• 20 • 00								
Windows Firewall with Advance	Inforund Rules						Actions	
Inbound Rules	Name	Group	*	Profile.	Enabled	A.*	Inbound Rules	
Connection Security Rules	New Inbound Rule Wisard	and the second	and a second					
Monitoring	Rule Type Select the type of freesal rule to create Steps: Pluie Type Action Profile Name	What type of rule would Program Public functions on Post Rule that controls on Presidefined: INTS Presenating Rule that controls on Custom Custom rule.	you like to create? medians for a prog medians for a TCP medians for a Win	an. or UOP pot. love experien	os ech	Ned >	- Cancel	
	Core Networking - Teredo (UDR	-In) Core Netwo	orking	All	Yes	A		
	4					×		

- Go to inbound rules and add to the exceptions list Chose program and hit next>
- chose This program path, hit Brows find opcenum.exe double click it and hit next> ( the path should be: Windows7 32 bit machine → c:\windows\system32\opcenum.exe Windows7 64 bit machine and Windows Server 2008 R2
   →C:\Windows\SysWOW64\opcenum.exe)
- Chose Allow the connection and hit Next>
- Check the desired boxes ( in our example we only check Domain ) hit Next>
- Give a name to the connection rule and a description if you desire to then **hit Finish**.

#### **B. OPC Server exception**

- Right click Inbound Rules and choose New Rule from the drop down menu, the Inbound Rules wizard will appear
- Chose program and hit next>
- chose This program path, hit Brows find your OPC server executable double click it and hit next>
- Chose Allow the connection and hit Next>
- Check the desired boxes hit Next>
- Give a name to the connection rule and a description if you desire to, then hit Finish.

Exit the firewall configuration window Restart windows



# 4. Permissions settings

The server permissions can be managed according to the level of access we want to give, for example if we have a worckgroup (WG) how can access a server and we want user A (UA) to be able to access OPCserverA and user B (UB) to be able to access only OPCserverB, we should set. permissions as follow:

OpcEnum  $\rightarrow$  WG

OPCserverA  $\rightarrow$  WG\UA

OPCserverB  $\rightarrow$  WG\UB

And allow remote and\or local operations for each one of them.

# 5. OPC Client Settings (Same like OPC server Setting)

### A. Wide security "MyComputer" settings

• Managing the settings for the general computer access, users and permissions

Press III + R to open the Run menu type "DCOMCNFG" on the text area and press ENTER to open the Component Services window



• Under: Component Services -> Computers, Right-click on "My Computer" and Choose the "Properties" from the menu.

Click the "Default Properties" Tab and configure as follow:
 Enable Distributed COM on this computer checked.
 Default Authentication Level Connect
 Default Impersonation Level Identify

## AD\ANTECH

**Enabling an Intelligent Planet** 

🥵 Component Services		
🌬 File Action View Window Help	My Computer Properties	_ 5 ×
File Action View Window Help       Image: Console Root       Component Services       Computers       Image: Computer       Image: Compu	Default Protocols       COM Security       MSDTC         General       Options       Default Properties         Image: Comparison of the structure of the struc	
	OK Cancel Apply	

#### • Click on the "COM Security" tab

For the "Access Permissions", we need to check **user accounts** are exist and give that local and remote access, it is necessary to request user account information, also add the users accounts and/or groups who should be able to access the COM service in this machine.

Click "Edit Limits" button within the "Access Permissions" Hit Add enter the object name (8 users account are below.) Hit OK Check local access and remote access boxes Click OK.
 Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM", "INTERACTIVE", "NETWORK", "Everyone", "Performance Log Users" and "Distributed COM Users") Repeat the operations until completed.



File Action View With	ty Computer Properties	
Console Root Component Services Computers My Computer COM- Appl COM- Appl COM- Appl COM- Configuration COM- COM- Confi	General Default Protocols         Default Properties MSDTC           Access Permissions         COM Security         MSDTC           Access Permissions         Tournay edit who is allowed default access to applications. You may note all who is allowed default access to applications. You may an applications to start. connect, function and/or run accessed.         Tournay edit who is allowed default access to applications. You may an applications to start. connect, function and/or run accessed.           Cast Default         Edit Default           Cast on: Modifying access permissions can affect the ability of applications to start. connect, function and/or run securely.         Edit Default           Cast on: Modifying access permissions         Edit Default         Edit Default           Launch and Activation Permissions         Edit Initia.         Edit Default           Castor: Modifying launch and activation permissions can advote depacts. You may also all inits on applications or activates depacts. You may also all inits on applications in that default or numerical.         Edit Default           Castor: Modifying launch and activation permissions.         Edit Linits         Edit Default	Access Permussion
	Learn nime about <u>setting these properties</u>	Leven whold access control and pertonnens OK Cancel

Click "Edit Default" button within the "Access Permissions" Hit Add enter the object name (7 users account are below.) Hit OK Check local access and remote access boxes Click OK.

Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM", "INTERACTIVE", "NETWORK", "Everyone" and "SELF")

Repeat the operations until completed.

Computers     Computers     Constructers     Constru	Properties More Actions Access Permission
Computers     Computers	More Actions More Actions Access Permission
Event Viewer (Local) Access Permissions You may edit who is allowed default access to applicat also set limits on applications that determine their own p Caution: Modifying access certaispens can all	Arcest Permission
Services (Local) You may add who is allowed default access to applicat also set limits on applications that determine their own p     Caulian: Modifying access pertrisions can all	ans Youmay
Eavier. In appearers an appearers has dealers and a	Default Security
Caution: Modilying access pertrasport can all	Stan or une sames
of applications to start, connect, function and	Annan All Concest
securely	A SELF
Edition Edit	Delast SYSTEM
	R. Administration (WA ENG Vadministration)
Launch and Activation Permissions	
You may edit who is allowed by default to launch apply activate objects. You may also set limits on application	alfons or Add. Remove
determine their own permissions.	Permissions for Everyone Allow Deny
Caution: Modifying launch and activation perm	stokins can Local Access 🗵 🗒
and/or run accurely.	Renole Access 🗵 🖻
Erit Landz Eri	Detext.
and a straight of the second second second second	Learn about access control and permissions
Learn more about setting these properties	OK Cased
W. W.	UK Cake

For the "Launch and Activation Permissions" configure as needed, adding only permissions to the users and/or groups who should be able to access the COM service in this machine, setting the permissions. To assign permissions to a special group or user, add it and check the desired boxes.

Click "Edit Limits" button within the "Launch and activation Permissions "Hit Add enter the object name (8 users account are below.) hit OK check the desired allow or deny boxes click OK.
 Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM",



"INTERACTIVE", "NETWORK", "Everyone", "Performance Log Users" and "Distributed COM Users")

Repeat the operations until completed.

File Action View W	Ay Computer Properties	
Compole Root Component Services Component Services Computers My Computer COM+ Appl DCDM Conf Running Pro DCDM Cord Service (lacal)	General Options Default Properties Default Protocols COM Security Access Permissions You may edd who is allowed default access to applications. You may also set limits on applications that default access to applications. You may also set limits on applications that default access permissions can effect the ability of applications to start, connect, function and/or run securely. Edd Limits. Edd Default	Launch and Activation Permission
	Launch and Activation Permissions You may edit into is allowed by default to launch applications or activate depicts. Your may also set limits on applications that determine their own permissions. Caston: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or no securely. Edit Limits Edit Default.	
	Learn more about setting these properties	Learn about access curitral and permatative OK Cancel

• Click "Edit Default" button within the "Access Permissions" Hit Add enter the object name (6 users account are below.) hit OK check the desired allow or deny boxes click OK.

Hit Add enter the users accounts and/or groups wanted. ("Administrators", "ANONYMOUS LOGON", "SYSTEM", "INTERACTIVE", "NETWORK" and "Everyone")

Repeat the operations until completed.

Component Services Component Services Computers E M My Computer E Event Viewer (Local) Services (Local)	My Computer Properties	Actions	
			My Computer
	Default Protocols CDM Security MSDTC		More Actions
	Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.	Launch and Activation Permission	
		Default Security	
	Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.	Group or user names:	
		AL.	
	Edit junds Edit Default.	K SYSTEM     K NETWORK     Advancestation (WA-ENGVAdministration)	
	Learnch and Activation Premissions You may edit who is allowed by default to launch applications of advanter object. You may also suff finits on applications that determine their own premissions determine their own premissions to dark, connect, function and/or run securely. Edit Londs.	A INTERACTIVE	
		The second second second	Add. Fiersown
		Pentissions for Everyone	Allow Derg
		LocalLaurch	821 III
		Local Activation	20 E
		Remote Activation	10 E
	Learn nove about anting them associates	Learn alreat access control and permissions	
			(

Press OK at end to save settings.

- Pin Definition (in case of serial connection):
- Reference: