	ssification	NAPOPC_CI	E6 FAQ				No.	1-005-E
Aut	hor	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	1/17
łc o	ow to co connec	onfigure t t with the	he Win e XP-80	dows 7 00-CE6	′ syster 5/XP-80	n setting 00-Atom	g for O h-CE6?	PC Clie
٩p	oli <u>es to :</u>							
		Platform		OS versior	ו	NAPOPC	_CE6 vers	ion
		PC	Wind Pro	ows 7 32/6 ofessional S	64 bits SP1	NAPOPC	_CE6 v1	.10
「he  . <u> </u>	Steps: nstallation	<u>n</u> NAPOPC_ST	DA Server	on Windov	ws 7 32/64	bits Profess	ional SP1	OS.
- <u>I</u>	Firewall Co	onfiguration						
(	Configure t	he firewa <mark>ll f</mark> or	the OPC C	Client (PC)	on Window	vs 7 <mark>32/64 b</mark> i	its Profess	sional SP1 (
5. <u> </u>	DCOM Cor	nfiguration						
(	Configure t	he DCO <mark>M for</mark>	the OPC C	lient (PC)	on Windov	vs 7 32/64 bi	its Profess	sional SP1 C
. <u> </u>	Local Secu	urity Policy C	onfigurati	on				
(	Configure to Professiona	he local secur al SP1 OS.	ity policy fo	or the OPC	Client (PC	C) on Windov	ws 7 32/64	1 bits
	<u>XP-8000-C</u>	<u>E6/XP-8000-/</u>	Atom-CE6	<u>Configura</u>	ation			
(	Configure t	he DCOM for	the OPC S	erver on th	ne XP-8000	0-CE6/XP-80	000-Atom-	CE6.
<u> </u>	Connect to	PAC Server						
	At last, con	nect the OPC	Client on t	he Window	va 7 ta tha			0 Atom CE

ICP DAS Co., Ltd. Technical document

Classification	NAPOPC_CE6	FAQ				No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	2/17

## 1. Installation

Step 1:

a. Use mouse to right-click on the installing program icon of NAPOPC\_ST DA Server, select the item 'Run as administrator'.



b. Click on 'Yes' to follow the installation steps.

😗 User	Account Control	
	Do you want unknown puł	to allow the following program from an plisher to make changes to this computer?
	Program name: Publisher: File origin:	NAPOPC_ST DA Server.exe <b>Unknown</b> Hard drive on this computer
💌 si	how details	Yes No
		Change when these notifications appear

Note: If need to download the NAPOPC\_ST DA Server for PC side, please go to website: <u>http://opc.icpdas.com/download.htm#PC</u>

Classification	NAPOPC_CE6	FAQ				No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	3/17

## 2. Firewall Configuration

### 2.1 Setting the firewall (Client-side)

Step 1:

a. Set up DCOM Firewall: Click 'Start' > 'Control Panel' > 'System and Security' > 'Windows Firewall' > 'Advanced settings'



b. Select 'Inbound Rules' on the left side, then select 'Performance Logs and Alerts (DCOM-In)' on the right side.

Inbound Rules		Inbound Rules				
Cutbound Rule	es	Name	Group	Profile	Enabled	Action
🌆 Connection Se	curity Rules	Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Domain	No	Allow
🔍 🌉 Monitoring		Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Private	No	Allow
		Remote Assistance (DCOM-In)	Remote Assistance	Domain	Yes	Allow
		Windows Management Instrumentation	Windows Management Instr	Domain	No	Allow
		Windows Management Instrumentation	Windows Management Instr	Private	No	Allow
		File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	No	Allow
		File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private	No	Allow
		Wetwork Discovery (NB-Name-In)	Network Discovery	Public	No	Allow
		🔇 Network Discovery (NB-Name-In)	Network Discovery	Private	Yes	Allow
		Wetwork Discovery (NB-Name-In)	Network Discovery	Domain	No	Allow
		File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private	No	Allow
		File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain	No	Allow
		Wetwork Discovery (NB-Datagram-In)	Network Discovery	Public	No	Allow
		Minternal Discourse (ND Data and Ta)	Matural Discourses	n	NI-	A II

Classification	NAPOPC_CE	6 FAQ						No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Da	ate	Oct. 201	2	Page	4/17
c. Dou the	uble click on 'F picture below.	Performan	ce Logs a	and Ale	rts (D	COM-In)	' and	d set up the	options as
Pe	normance Logs an	a Alerts (DCC		aues		1 11			
	General	ts Progra	scope   ams and Servic	Advanc es	ed	Computers	_		
	(i) This is a	predefined rul	e and some of	its properti	ies canr	not			
	General	ea.							
	Name: Performa	ince Logs and	Alerts (DCOM	-In)					
	Descriptio	on:							
	Inbound remote [	rule for Perfon COM activatio	mance Logs ar on. [TCP-135]	nd Alerts to	allow	*			
	C Enab								
	Action								
		the connection							
		tomize							
	Block	the connection	n						
	0.000								
	Leam more about th	nese settings							
			ОК	Ca	ancel	Apply	/		
NOTE: L	Jser has to se Alerts (DCOM-	t up both   In)'.	orofiles (D	omain	& Pri	ivate…) c	of 'P	erformance	Logs and
·		ICP DAS	Co., Ltd.	Fechnic	al doc	cument			

Classification	NAPOPC_CE6 FAQ						1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	5/17

# 3. DCOM Configuration

# 3.1 Setting the DCOM (Client-side)

Step 1: Click the 'Start', key in 'MMC comexp.msc /32', and then execute it.



Classification	NAPOPC CE	FAQ					No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 20	012	Page	6/17
Classification Author Step 2: 0 to	NAPOPC_CEG Sun / Eva Click 'Compone select the 'Pro Console Root Component Sec Component Sec Computers Computers My Com Event Viewer (L Services (Local)	FAQ Version ent Servic perties'.	1.0.0         ces' > 'Computer         Image: Computer Refresh all comportion         New Window from         Properties         Help	Date Iters' > ' Iters' iters' iters' Iters' iters	Oct. 24 My Con	012 nputer'	No. Page , and mous	1-005-E 6/17 Se right-click
			Co. Ltd Teel	mical do	cument			

Classification	NAPOPC_CE	6 FAQ		1		No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	7/17
Step 3: Clic	ck 'Default Pro	perties' p	age, and set	up the o	ptions as the	e picture bel	ow.
M	y Computer Proper	ties			? 💌		
	Default Protoco	s O-tio	COM Security	efault Prope	SDTC		
	General	d COM on this		егаші гторе	aues		
	Enable COM Inte	met Services	on this computer				
	Default Distributed	COM Commu	nication Properties				
	The Authenticatio	n Level specif	ies security at the pa	acket level.			
	Default Authenti	cation Level:	•				
	The impercention		mine				
	who is calling then using the client's in	n, and whethe dentity.	r the application car	ndo operatio	ons		
	Default Impersor	nation Level:					
	Identify		•				
	Security for referent and that the defau	is used					
	Provide addi	tional security	for reference trackin	g	/		
	Loom more about or	tting these pr	anation				
	Learn more about se	aung these pro	<u>ppenies</u> .				
			OK Can	cel	Apply		
		ICP DAS	Co., Ltd. Tech	nical do	cument		

Author S	Sun / Eva	Version	100	Data	0 1 0010	_	
			1.0.0	Date	Oct. 2012	Page	8/17
Step 4: T	Then Click the	e 'COM S uter Properti neral ault Protocols s Permissions may edit who set limits on of applic securely h and Activat may edit who securely h and Activat may edit who securely Caution: affect th and/or r	Security' page ies Options COM : COM :	Date , and se , and se security eccess to a ermine their ermissions o ect, functio	Oct. 2012 et up the secu Pefault Properties MSDTC oplications. You may own permissions. can affect the ability n and/or run Edit Default applications or cations that n permissions can connect, function	Page urity as th	8/17 e steps below

a. Set up 'Access Permissions' > 'Edit Limits' as blow. (If no 'Everyone' option, please add it.)

Group or user names:	IN-JE9ORLTF2VT	Performance
ANONYMOUS LOGON	N-JE9ORLTF2VT\U	listributed C
	Add	Remove
Permissions for Everyone	Allow	Deny
Local Access	V	
Remote Access	✓	

Classification	NAPOPC_CE6	FAQ				No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	9/17
Author	Sun / Eva Access Permi Security Limit Group or us Security Limit Security Limit Group or us Security Limit Security Limit Group or us Security Limit Security Limit Security Limit Group or us Security Limit Security Limit Secu	Version ssion s er names: one mance Log Us uted COM Us YMOUS LOG for ANONYM cess Access	1.0.0 sers (WIN-JE9ORLT ers (WIN-JE9ORLTF iON Add 10US Al	Date F2VT\Perfo 2VT\Distrib	Oct. 2012	Page	9/17
b. 5	Set up 'Access	Permissi	ons' > 'Defau	It Securi	tv' as below	(if no 'Eve	rvone' option

b. Set up 'Access Permissions' > 'Default Security' as below (if no 'Everyone' option, please add it.)

Default Security			
Group or user names:			
& Everyone			1
& SELF			
SYSTEM			
& Administrators (WIN-JE9ORI	LTF2VT\Administrate	ors)	
	Add	Remove	
Permissions for Everyone	Allow	Deny	
Local Access	<b>V</b>	[""]	
Remote Access	<b>V</b>		

Classification	NAPOPC_CE6	FAQ				No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	10/17

c. Set up 'Launch and Activation Permission' > 'Edit Limits' as below (If no 'Everyone' option, please add it.)

aunch and Activation Permiss	sion	? <mark>×</mark>
Security Limits		
Group or user names:		
Serveryone		
& Administrators (WIN-JE90	RLTF2VT\Administr	ators)
I XII Performance Log Lleare A	WIN-JE9ORLTF2VT	\Performance
Dent - COMU		Division I I
Log Users (N	/IN-JE9ORLTF2VT\	Distributed C
Stributed COM Users (N	/IN-JE9ORLTF2VT\	Distributed C
Stributed COM Users (N	/IN-JE9ORLTF2VT	Distributed C
Permissions for Everyone	/IN-JE9ORLTF2VT Add Allow	Distributed C Remove
Permissions for Everyone	/IN-JE9ORLTF2VT Add Allow	Distributed C Remove Deny
Permissions for Everyone Local Launch Remote Launch	/IN-JE9ORLTF2VT Add Allow	Distributed C Remove
Permissions for Everyone Local Launch Remote Launch Local Activation	VIN-JE9ORLTF2VT Add Allow	Distributed C Remove Deny

d. Set up 'Launch and Activation Permission' > 'Default Security' as below (If no 'Everyone' option, please add it.)

Group or user names:			
SYSTEM			
& Administrators (WIN-JE9OR	LTF2VT\Administrat	ors)	
Sector Everyone			
M INTERACTIVE			
		Permana	
	Add	Remove	
Permissions for Everyone	Allow	Deny	
Local Launch	$\checkmark$		
Remote Launch			
Local Activation			
Remote Activation	$\checkmark$		
Learn about access control and	permissions		
	ОК	Cancel	

Classification	NAPOPC_CE6	FAQ				No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	11/17

# Step 5: Click "My Computer" > "DCOM Config", then right key click on "NAPOPC DA Server" and select "Properties".



Step 6: Click "Location" tag, check the option "Run application on the following computer" and enter the IP address of the Server.

NAPOPC_ST DA Server Properties	
General Location Security Endpoints Identity	
The following settings allow DCOM to locate the correct computer for this application. If you make more than one selection, then DCOM uses the first applicable one. Client applications may overide your selections.	
Run application on the computer where the data is located.	
Run application on the following computer:       192.168.1.46       Browse	
Learn more about setting these properties.	
OK Cancel Apply	
ICP DAS Co. I td. Technical document	

Classification	NAPOPC_CE	6 FAQ				No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	12/17
Step 7:	Click "Identity"	tag to set	up the use	er.			
	NAPOPC_ST DA Ser	ver Properties	Identity	8			
	Which user accou	nt do you want to	o use to run this ar	oplication?			
	The interactive The lauraching	user.					
	<ul> <li>The launching</li> <li>This user.</li> </ul>	user.					
	User:			Browse			
	Password: Confirm passwor	d:					
	The system action	count (services o	nly).				
	Learn more about	setting these proj	perties.				
			OK Ca	ncel App	ply		
Description:			5	1			

### • The interactive user

Click to specify that the application runs under the identity of the user who is currently logged on to the computer. This user's security credentials are used when the application is authenticated to access resources. (The Windows Desktop login is required, and the login account must be the same as the connecting account.)

### The launching user

Click to specify that the application runs using the security context of the user who started the application (the launching user) so that the application can be authenticated in the domain. The launching user may be the same as the interactive user. (The application must be executed first, and the executing account must be the same as the connecting account.)

### This user

Click to specify that the application runs using the security context of the specified user account so that it can be authenticated in the domain. Type the user name and password. (It can connect without login the Windows Desktop, and the application is executed and secured by the assigned user name and password.)

### • The system account

Click to specify that the server application runs using the security context of the built-in System account. This option is available only for applications that are installed as a service. (Not support)



Author       Sun / Eva       Version       1.0.0       Date       Oct. 2012       Page       14/17         Step 2: Click 'Security Settings' > 'Local Policies' > 'Security Options' Select "Network security: LAN Manager authentication level".         Security Settings       Security Settings       Security Settings       Security Setting         Account Policies       Microsoft network server: Digitally sign communications (fr
Step 2: Click 'Security Settings' > 'Local Policies' > 'Security Options'         Security Settings         Security Settings         Account Policies         Account Policies         Audit Policy         Audit Pol
<ul> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Local Policy</li> <li>Local Policy</li></ul>
<ul> <li>Account Policies</li> <li>Local Policies</li> <li>Audit Policy</li> <li>Quer Rights Assignment</li> <li>Security Options</li> <li>Windows Firewall with Advanced Sect</li> <li>Network List Manager Policies</li> <li>Network access: Allow anonymous SID/Name translation</li> <li>Network access: Do not allow anonymous enumeration of S</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Network access: Do not allow anonymous enumeration of S</li> <li>Network access: Do not allow anonymous enumeration of S</li> <li>Network access: Do not allow anonymous enumeration of S</li> <li>Network access: Do not allow anonymous enumeration of S</li> <li>Network access: Do not allow anonymous enumeration of S</li> <li>Network access: Named Pipes that can be accessed anonym</li> <li>Network access: Restrict anonymous access to Named Pipes</li> <li>Network access: Restrict anonymous access to Named Pipes</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed anonymously</li> <li>Not Defined</li> <li>Network access: Shares that can be accessed ano</li></ul>
Network security: Allow Local System to use computer ident       Not Defined         Network security: Allow LocalSystem NULL session fallback       Not Defined         Network Security: Allow PKU2U authentication requests to t       Not Defined         Network security: Configure encryption types allowed for Ke       Not Defined         Network security: Do not store LAN Manager hash value on       Enabled         Network security: Force logoff when logon hours expire       Disabled         Network security: LAN Manager authentication level       Not Defined         Network security: LDAP client signing requirements       Negotiate signing         Network security: Minimum session security for NTLM SSP       Require 128-bit encrypti         Network security: Restrict NTLM: Add remote server excepti       Not Defined         Network security: Restrict NTLM: Add server exceptions in t       Not Defined         Network security: Restrict NTLM: Add server exceptions in t       Not Defined         Network security: Restrict NTLM: Add server exceptions in t       Not Defined         Network security: Restrict NTLM: Add server exceptions in t       Not Defined         Network security: Restrict NTLM: Add server exceptions in t       Not Defined         Network security: Restrict NTLM: Add server exceptions in t       Not Defined



Cla	ssification	NAPOPC_CE	6 FAQ				No.	1-005-E
Aut	hor	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	16/17
<b>5.</b> 5.1	XP-8000 Set up t On th refer NAPC The c	-CE6/XP-80 the DCOM of the Server side, to the Section DPC_CE5.	00-Atom the XP-80 set up the 3.2.1 "Set site: <u>http://</u>	D-CE6 Co 00-CE6/X DCOM o up the Se	Dnfigurati P-8000-Ato f the XP-80 erver side (X com/downle	on m-CE6 (Ser 00-CE6/XP-4 (PAC)" in the oad.htm#XP-8	ver side) 8000-Atom a user mar 8000-CE6	n-CE6. Please rual of
<b>6.</b> 6.1	Connect Run the Step	to PAC Sel "NI Server E 1: Select the S	rver xplorer" ( server nam	( <b>2.4.1) for</b> ne "N <mark>AP</mark> OI	<mark>the conn</mark> ed P <mark>C.Sv</mark> r" to c	ction connect (as t	he picture)	)
	Ready	oject - Server Explorer 2.4.1 ters Edit View Options Connection Matri Matri NAPC OPC Connection Matri Matri NAPC OPC Connection Matri Matri NAPC	Help Server: Machine: Run As:	me (Device) It Ite Press the 'Cont NAPOPC.Svr \\192.168.1.40 Remote Server	m ID Value nect' button to connect to th	Timestamo Pe OPC Server.	Quality	
			ICP DAS	Co., Ltd. 7	Fechnical doo	cument		

Classification	NAPOPC_CE6	FAQ				No.	1-005-E
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	17/17

Step 2: when the connection is ok, you can get the NAPOPC data of XP-8000-CE6/XP-8000-Atom-CE6.

Image: Network           Image: Computer           Image: Watrikon.OPC.Simulation           Image: Natrikon.OPC.Simulation           Image: Natrikon.OPC.Simulation	Name (Device\It	Item ID 8024 1.AOs.Ch00	Value	Timestamp	Quality
Computer     Matrikon.OPC.Simulation     Matrikon.OPC Simulation 1     Simulation 1     P	8024_1.AOs	8024 1.AOs.Ch00			Quanty
Matrikon.OPC.Simulation Matrikon.OPC Simulation 1 NAPOPC.Svr	🖉 8024 1.AOs	552203.Choo	0	10:15:37:000	Value good
Matrikon OPC Simulation 1		8024_1.AOs.Ch01	0	10:15:37:000	Value good
E	Ø 8024_1.AOs	8024_1.AOs.Ch02	0	10:15:37:000	Value good
1 63 115 1.0	8024_1.AOs	8024_1.AOs.Ch03	0	10:15:37:000	Value good
Wizard Group	87017RC_2	87017RC_2.AIS.C	0.001	10:15:37:000	Value good
8024_1.AOs.Ch00	97017RC_2	87017RC_2.AIS.C	0.001	10:15:37:000	Value good
8024_1.AOs.Ch01	97017RC_2	97017RC_2.AIS.C	0.001	10:15:57:000	Value good
8024_1.AOs.Ch02	\$7017RC_2	87017RC_2.Als.C	0.001	10:15:37:000	Value good
8024_1.AOs.Ch03	\$7017RC_2	87017RC 2 Ale C	0.001	10:15:37:000	Value good
87017RC_2.AIs.Ch00	# 87017RC 2	87017RC 2.AIs.C	0.001	10:15:37:000	Value good
87017RC_2.AIs.Ch01	\$ 87017RC 2	87017RC 2.AIs.C	0.001	10:15:37:000	Value good
87017RC_2.AIs.Ch02				10120101000	for good
87017RC_2.AIs.Ch03					
87017RC_2.Als.Ch05					
87017RC_2.Als.Ch06					
57017RC_2.AIs.Ch07					
eady	C:\Program Files\Na	tional Instruments\na	ati.ccdb		

ICP DAS Co., Ltd. Technical document