

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

## How to configure the Windows 7 system setting for OPC Client to connect with the XP-8000-CE6/XP-8000-Atom-CE6?

Applies to :

<i>Platform</i>	<i>OS version</i>	<i>NAPOPC_CE6 version</i>
<i>PC</i>	<i>Windows 7 32/64 bits Professional SP1</i>	<i>NAPOPC_CE6 v1.10</i>

When connecting OPC Client on the Windows 7 to the XP-8000-CE6/XP-8000-Atom-CE6 controller (Server side), user has to configure the Windows 7 system setting first. This FAQ is a configuration description for the OPC Client on Windows 7 32/64 bits Professional SP1 Operating System to connect to the XP-8000-CE6/XP-8000-Atom-CE6, including the firewall, DCOM, local security policy... configuration.

### The Steps:

#### 1. [Installation](#)

Install the NAPOPC\_ST DA Server on Windows 7 32/64 bits Professional SP1 OS.

#### 2. [Firewall Configuration](#)

Configure the firewall for the OPC Client (PC) on Windows 7 32/64 bits Professional SP1 OS.

#### 3. [DCOM Configuration](#)

Configure the DCOM for the OPC Client (PC) on Windows 7 32/64 bits Professional SP1 OS.

#### 4. [Local Security Policy Configuration](#)

Configure the local security policy for the OPC Client (PC) on Windows 7 32/64 bits Professional SP1 OS.

#### 5. [XP-8000-CE6/XP-8000-Atom-CE6 Configuration](#)

Configure the DCOM for the OPC Server on the XP-8000-CE6/XP-8000-Atom-CE6.

#### 6. [Connect to PAC Server](#)

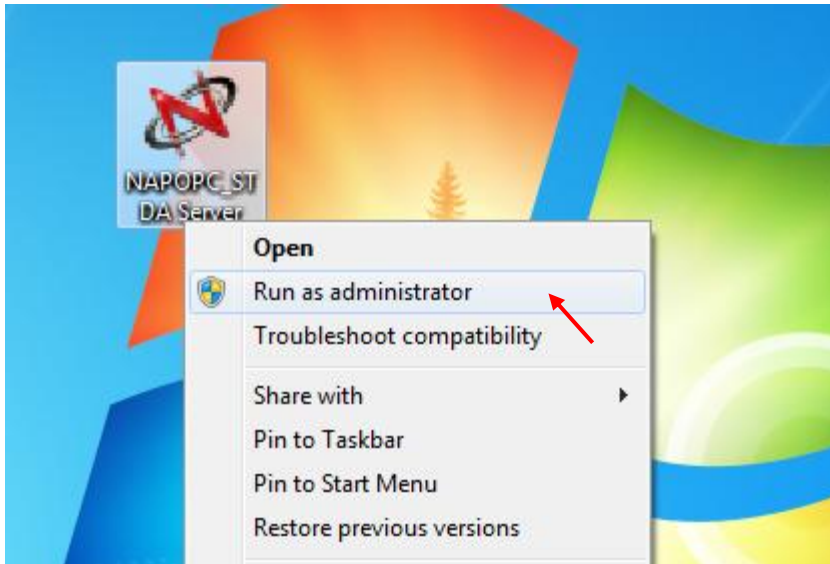
At last, connect the OPC Client on the Windows 7 to the XP-8000-CE6/XP-8000-Atom-CE6 OPC Server.

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

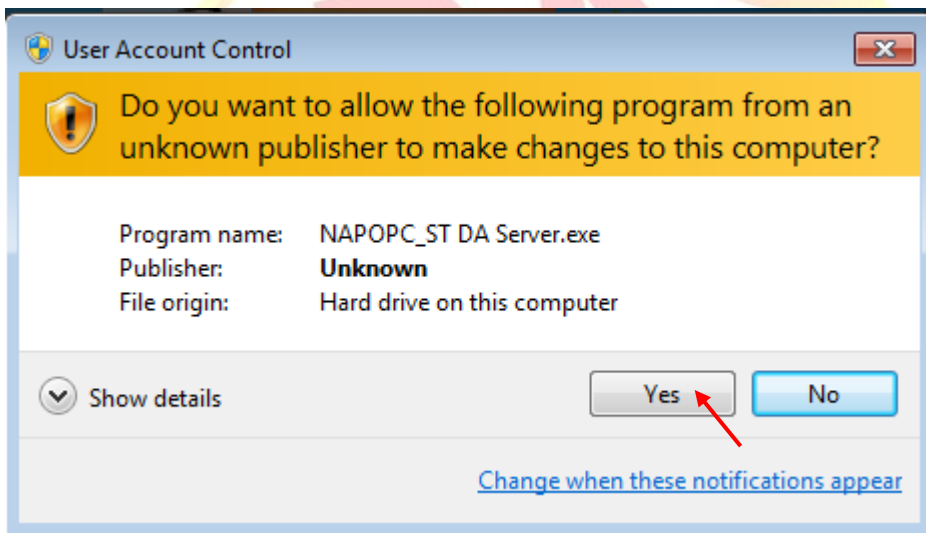
## 1. Installation

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.



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

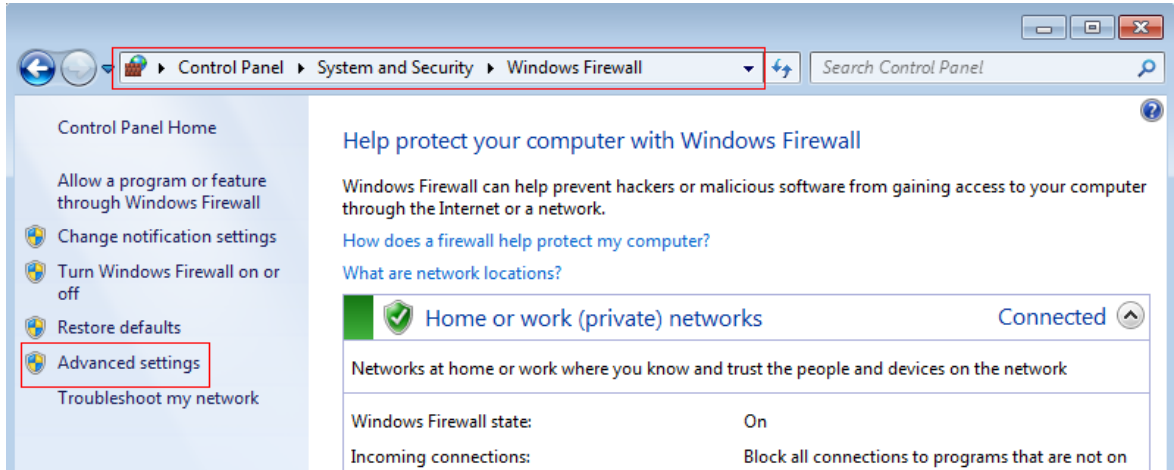
Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	3/17

## 2. Firewall Configuration

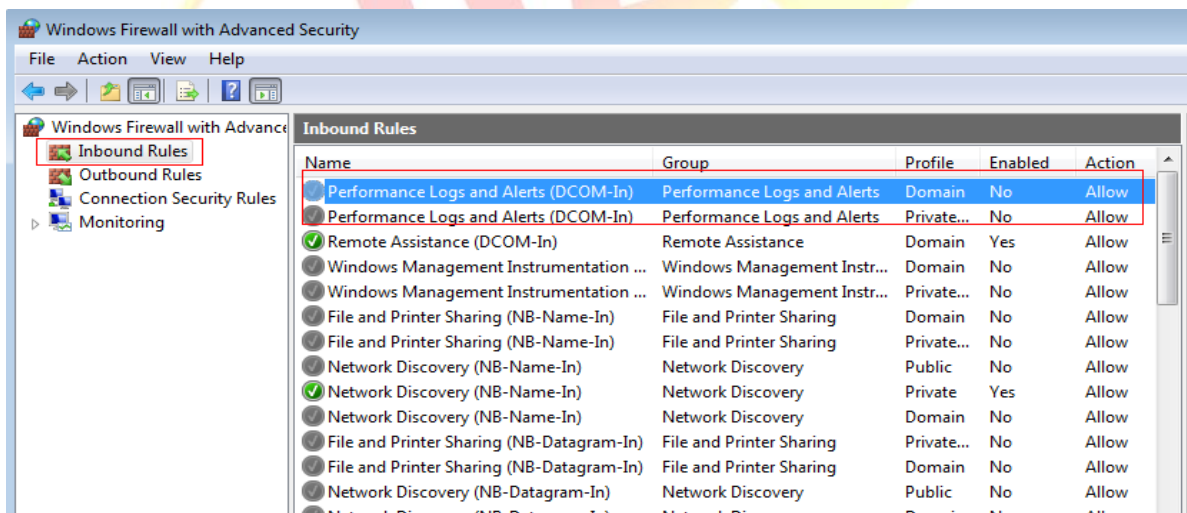
### 2.1 Setting the firewall (Client-side)

Step 1:

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

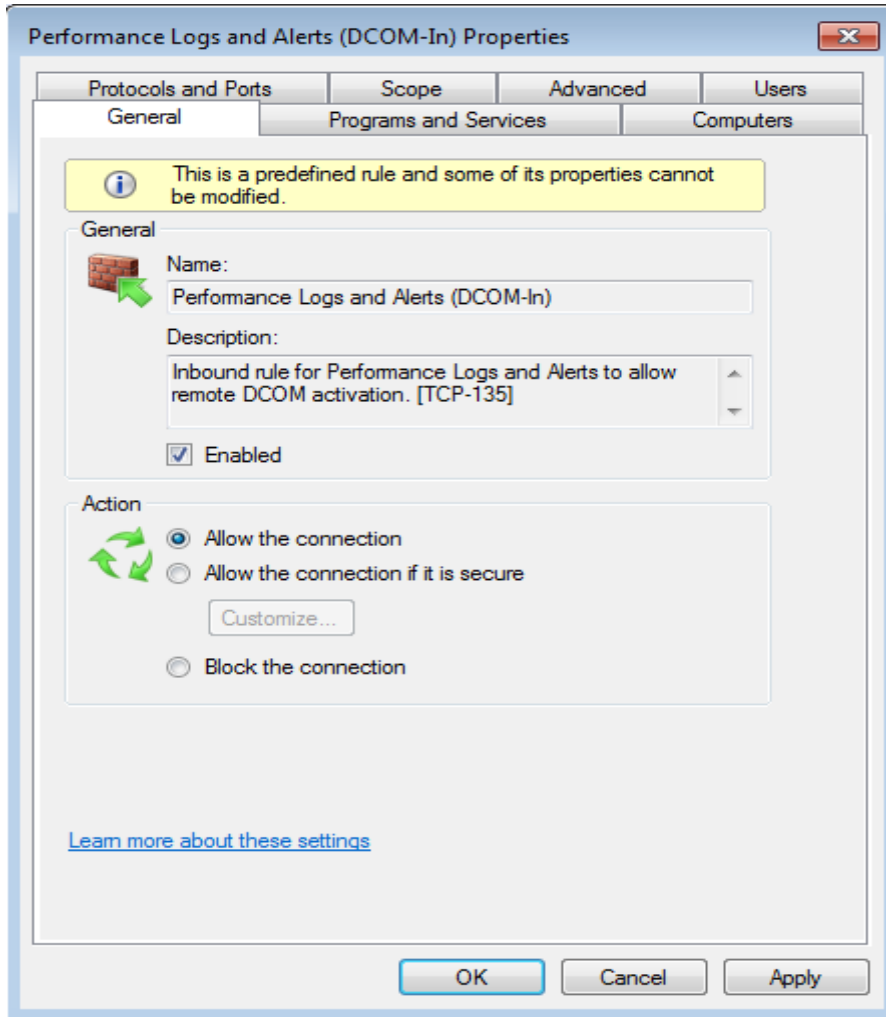


- b. Select 'Inbound Rules' on the left side, then select 'Performance Logs and Alerts (DCOM-In)' on the right side.



Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	4/17

- c. Double click on 'Performance Logs and Alerts (DCOM-In)' and set up the options as the picture below.



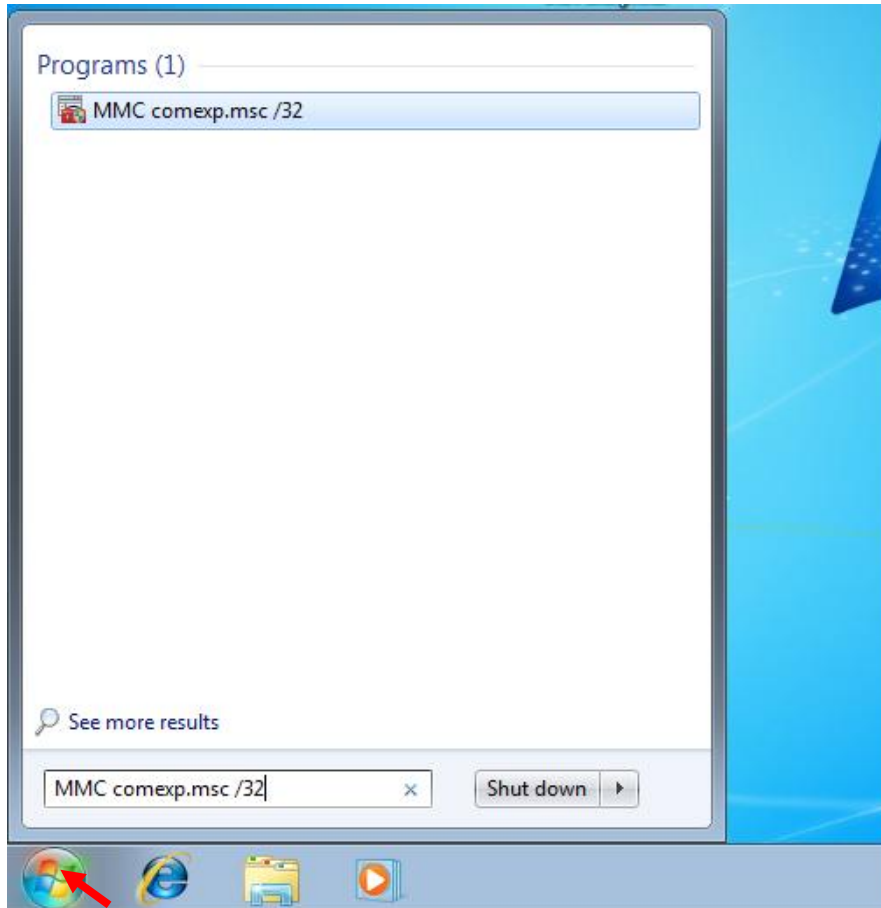
**NOTE:** User has to set up both profiles (Domain & Private...) of 'Performance Logs and Alerts (DCOM-In)'.

Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	5/17

### 3. DCOM Configuration

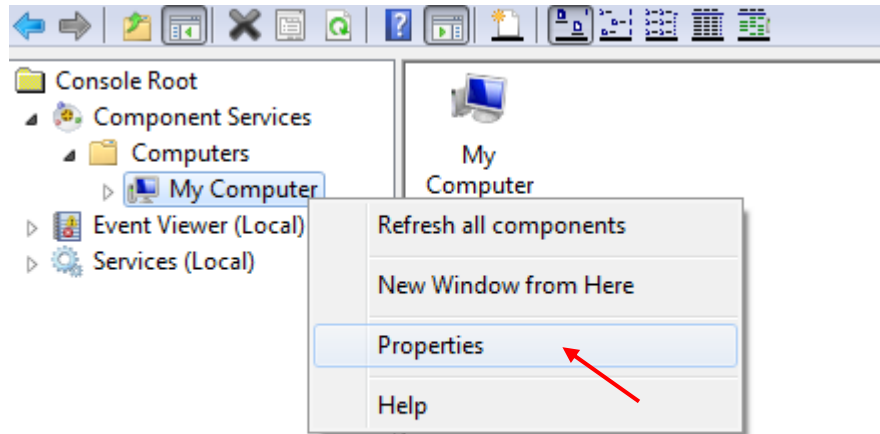
#### 3.1 Setting the DCOM (Client-side)

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



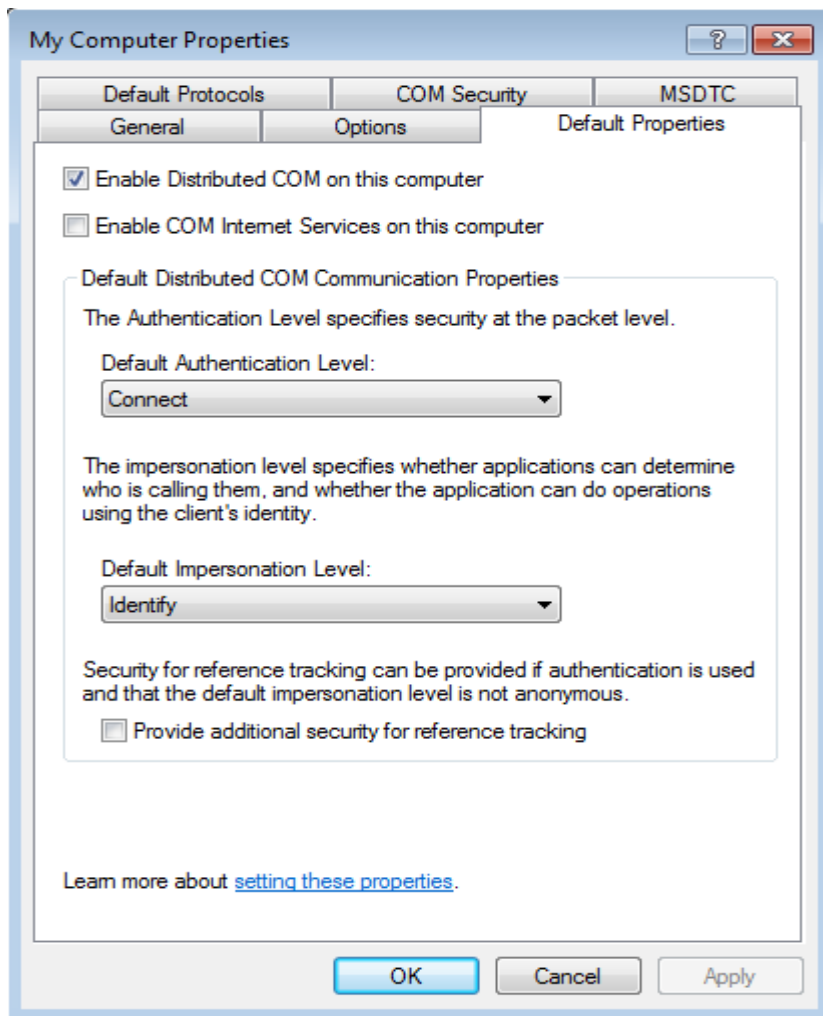
Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	6/17

Step 2: Click 'Component Services' > 'Computers' > 'My Computer', and mouse right-click to select the 'Properties'.



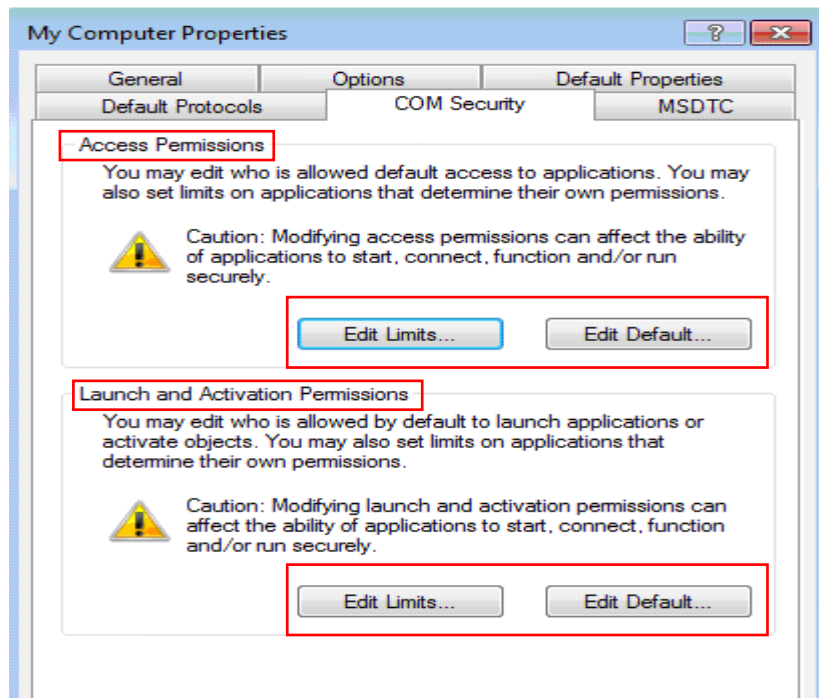
Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	7/17

Step 3: Click 'Default Properties' page, and set up the options as the picture below.

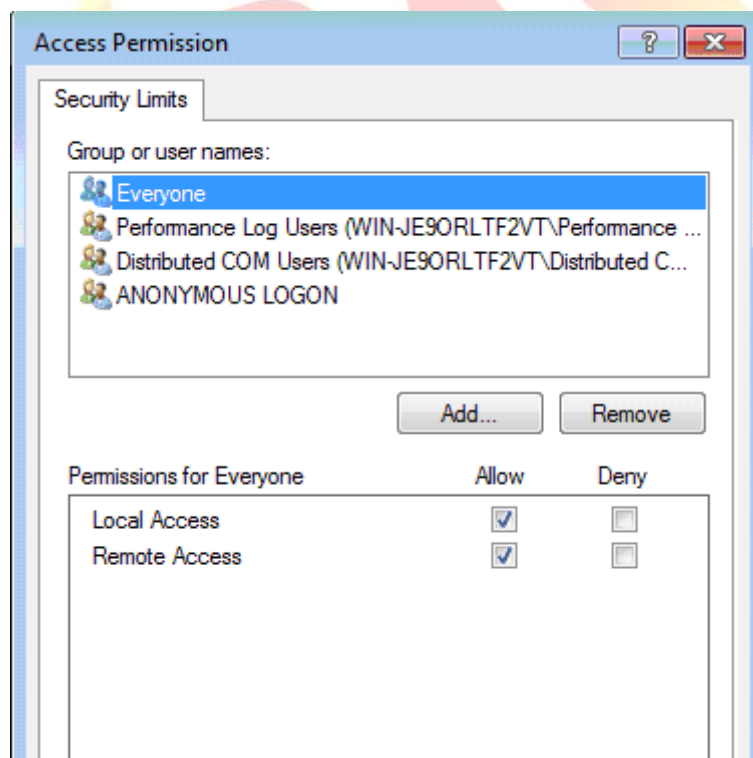


Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	8/17

Step 4: Then Click the 'COM Security' page, and set up the security as the steps below.

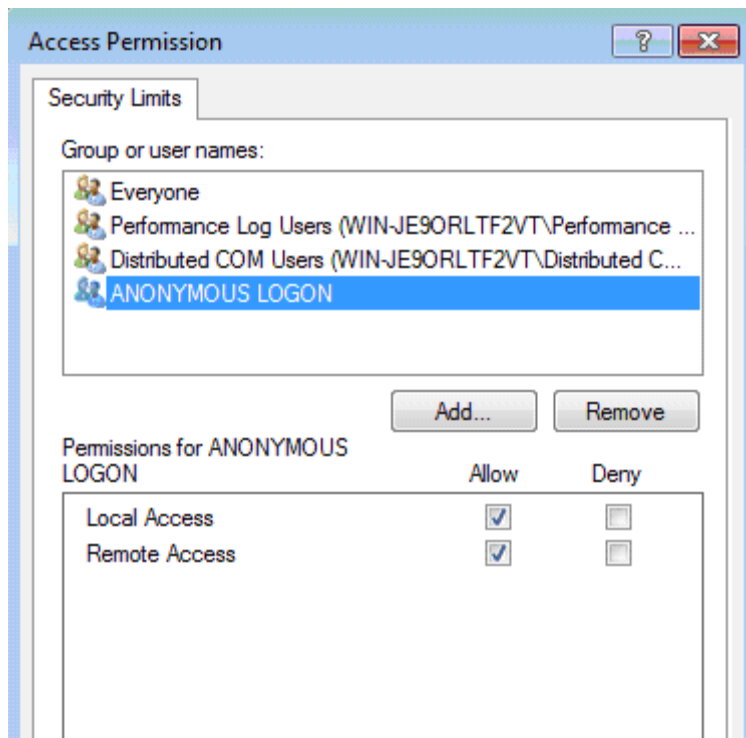


- a. Set up 'Access Permissions' > 'Edit Limits' as blow. (If no 'Everyone' option, please add it.)

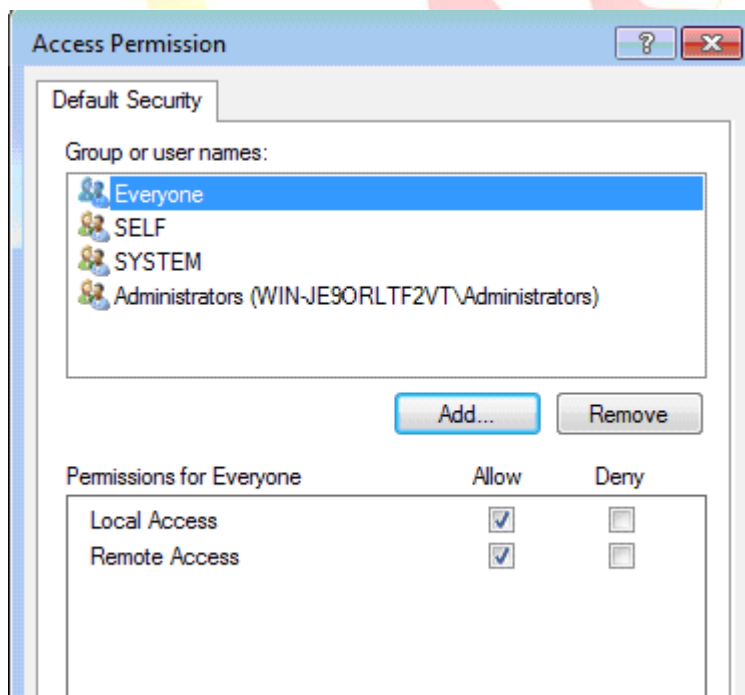




Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	9/17

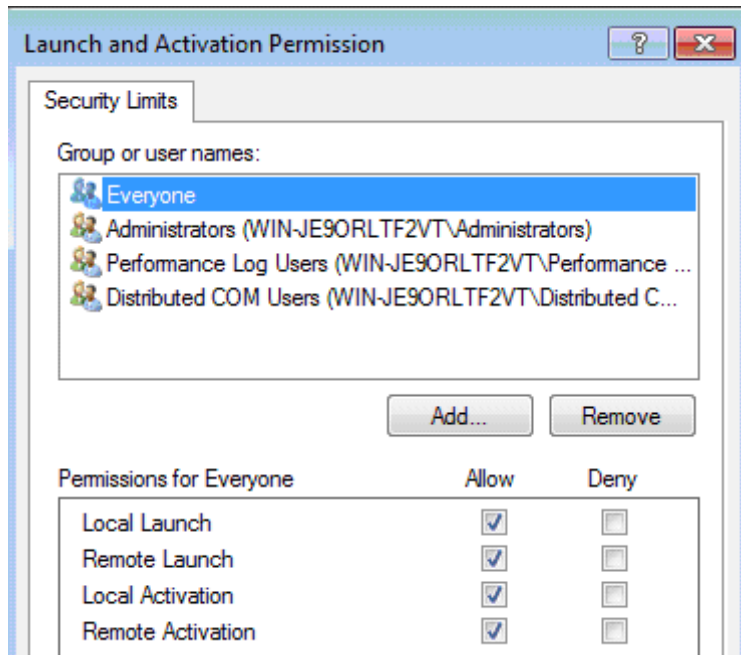


- b. Set up 'Access Permissions' > 'Default Security' as below (if no 'Everyone' option, please add it.)

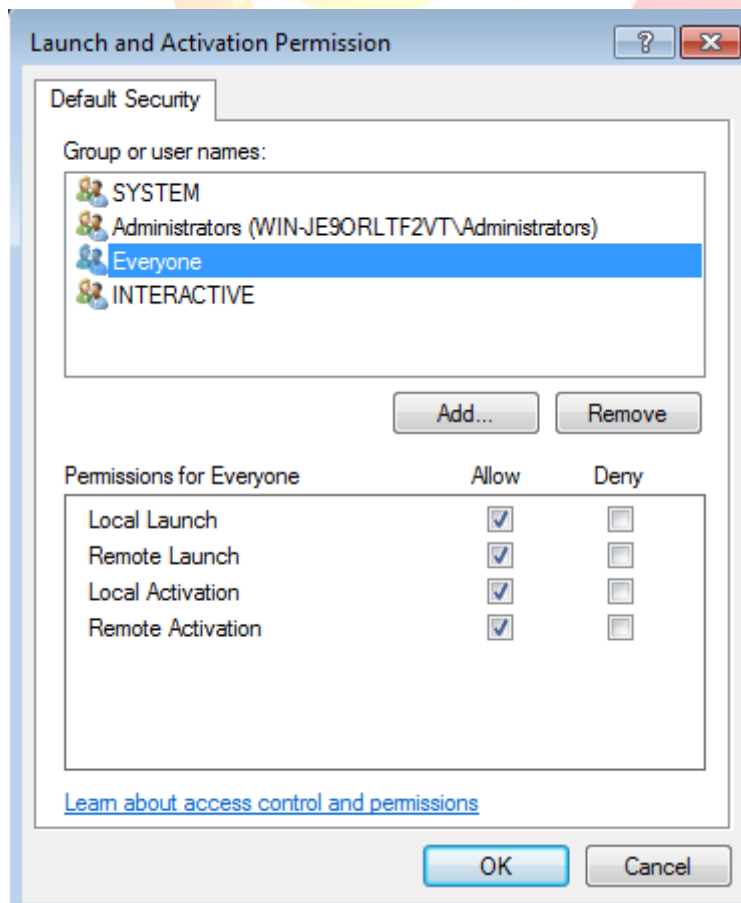


Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	10/17

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

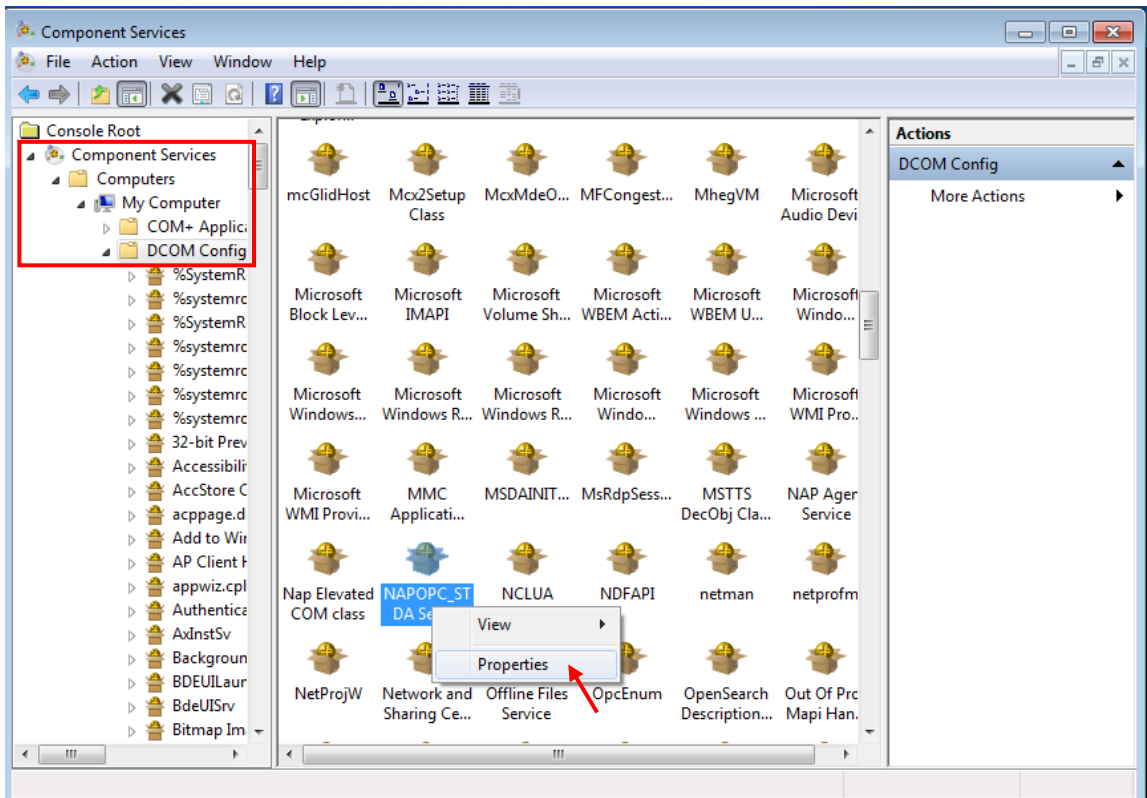


- d. Set up 'Launch and Activation Permission' > 'Default Security' as below (If no 'Everyone' option, please add it.)

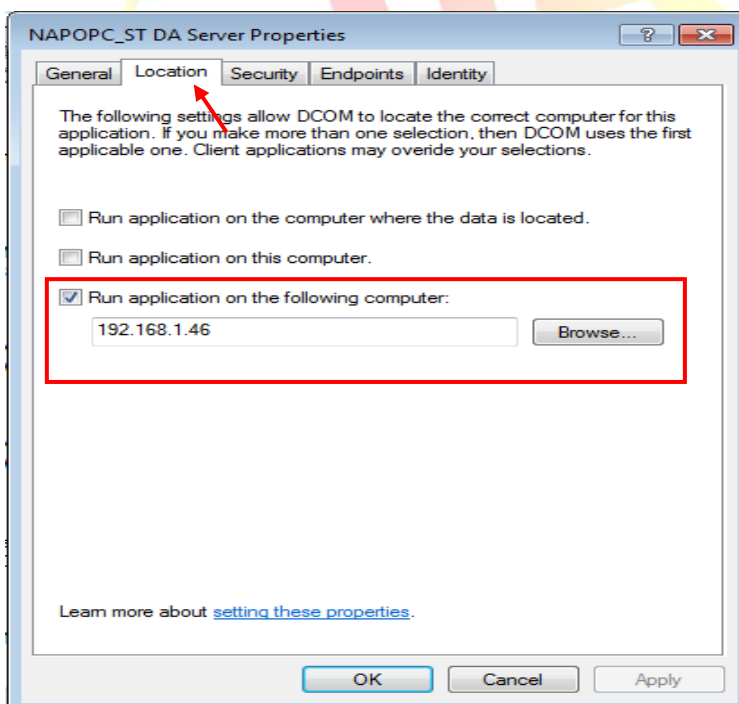


Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	11/17

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

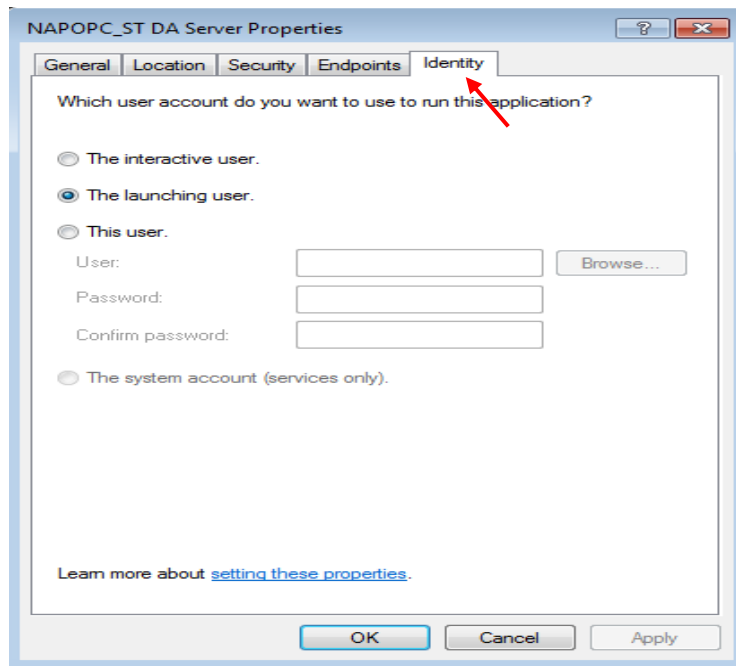


Step 6: Click "Location" tag, check the option “Run application on the following computer” and enter the IP address of the Server.



Classification	NAPOPC_CE6 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 user.



#### Description:

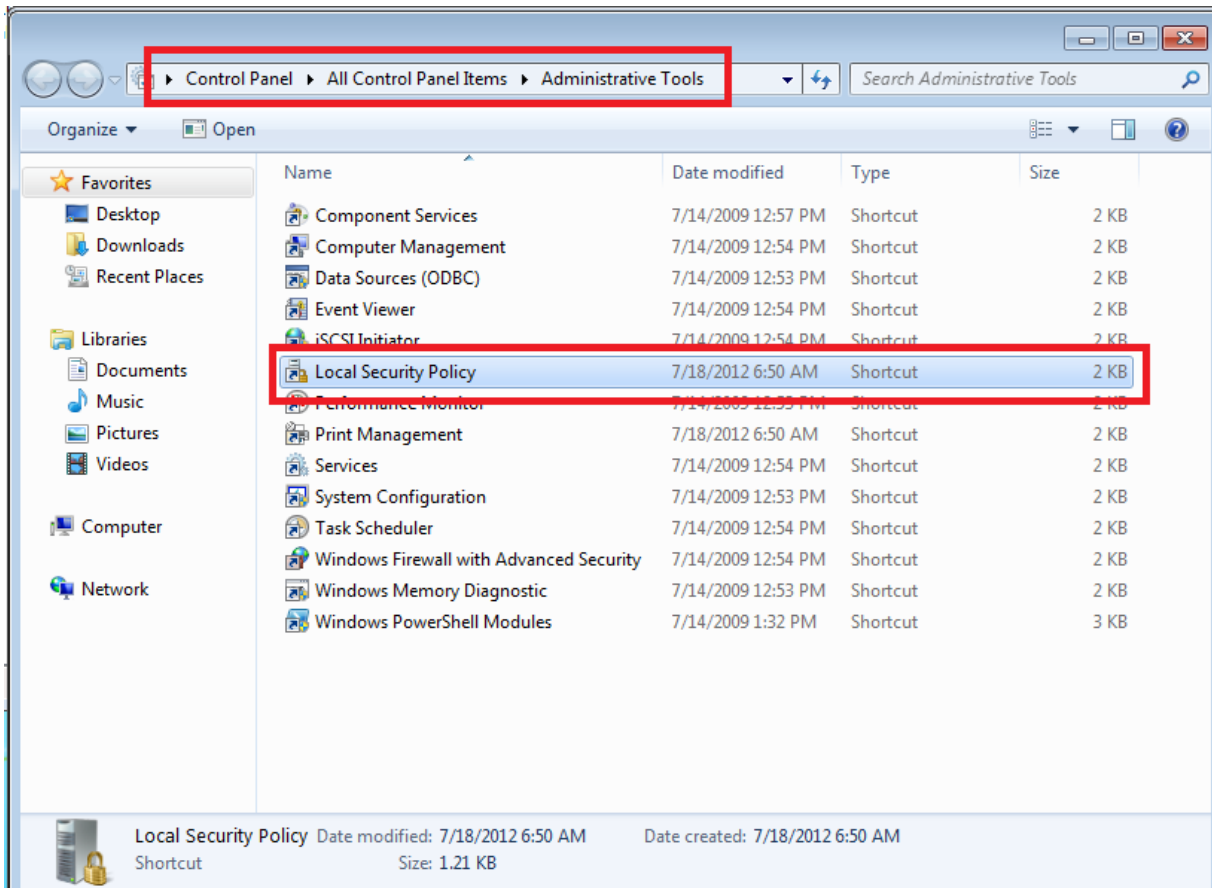
- **The interactive user**  
Click to specify that the application runs under the identity of the user who is currently logged on to the computer. This user's security credentials are used when the application is authenticated to access resources. (The Windows Desktop login is required, and the login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

Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	13/17

## 4. Local Security Policy Configuration

### 4.1 Setting the Local Security Policy (Client-side)

Step 1: Click 'Start' > 'Control Panel' > 'System Management Tool'.  
Select "Local Security Policy"



Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	14/17

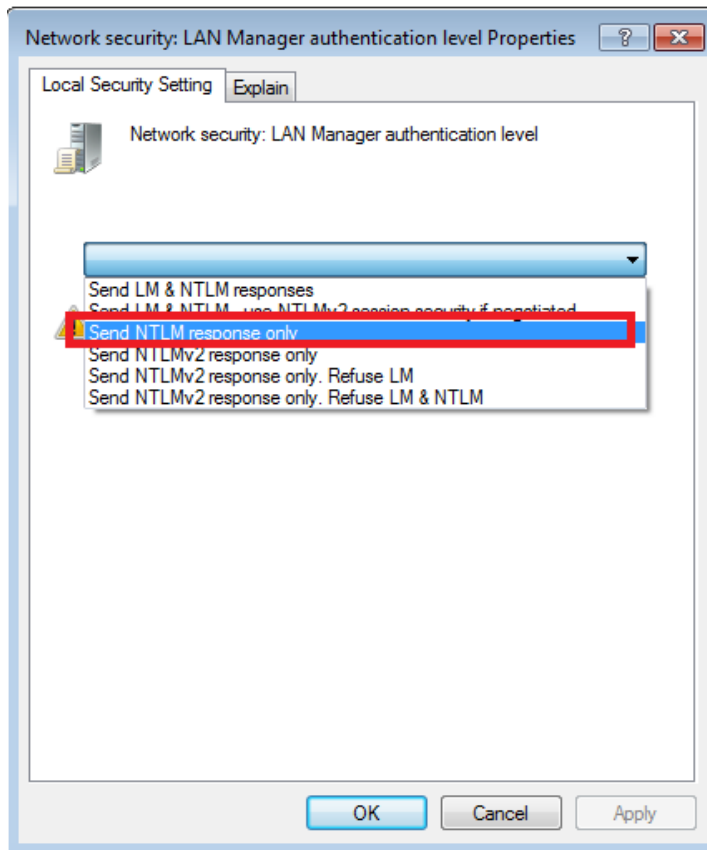
Step 2: Click 'Security Settings' > 'Local Policies' > 'Security Options'  
 Select "Network security: LAN Manager authentication level".

The screenshot shows the Windows Security Settings application. On the left, a tree view is expanded to 'Security Settings' > 'Local Policies' > 'Security Options'. The main pane displays a list of policies. The policy 'Network security: LAN Manager authentication level' is highlighted with a blue selection bar and a red border. The policy is currently set to 'Not Defined'.

Policy	Security Setting
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when logon ho...	Enabled
Microsoft network server: Server SPN target name validation...	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of S...	Enabled
Network access: Do not allow anonymous enumeration of S...	Disabled
Network access: Do not allow storage of passwords and cre...	Disabled
Network access: Let Everyone permissions apply to anonym...	Disabled
Network access: Named Pipes that can be accessed anonym...	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub...	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes...	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accou...	Classic - local users auth...
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
<b>Network security: LAN Manager authentication level</b>	<b>Not Defined</b>
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
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: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined

Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	15/17

Step 3: Set it to “Send NTLM response only”.



Policy	Security Setting
Network access: Do not allow anonymous enumeration of S...	Disabled
Network access: Do not allow storage of passwords and cre...	Disabled
Network access: Let Everyone permissions apply to anonym...	Disabled
Network access: Named Pipes that can be accessed anonym...	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub...	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes...	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accou...	Classic - local users auth...
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
<b>Network security: LAN Manager authentication level</b>	<b>Send NTLM response only</b>
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
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: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined

Classification	NAPOPC_CE6 FAQ				No.	1-005-E	
Author	Sun / Eva	Version	1.0.0	Date	Oct. 2012	Page	16/17

## 5. XP-8000-CE6/XP-8000-Atom-CE6 Configuration

### 5.1 Set up the DCOM of the XP-8000-CE6/XP-8000-Atom-CE6 (Server side)

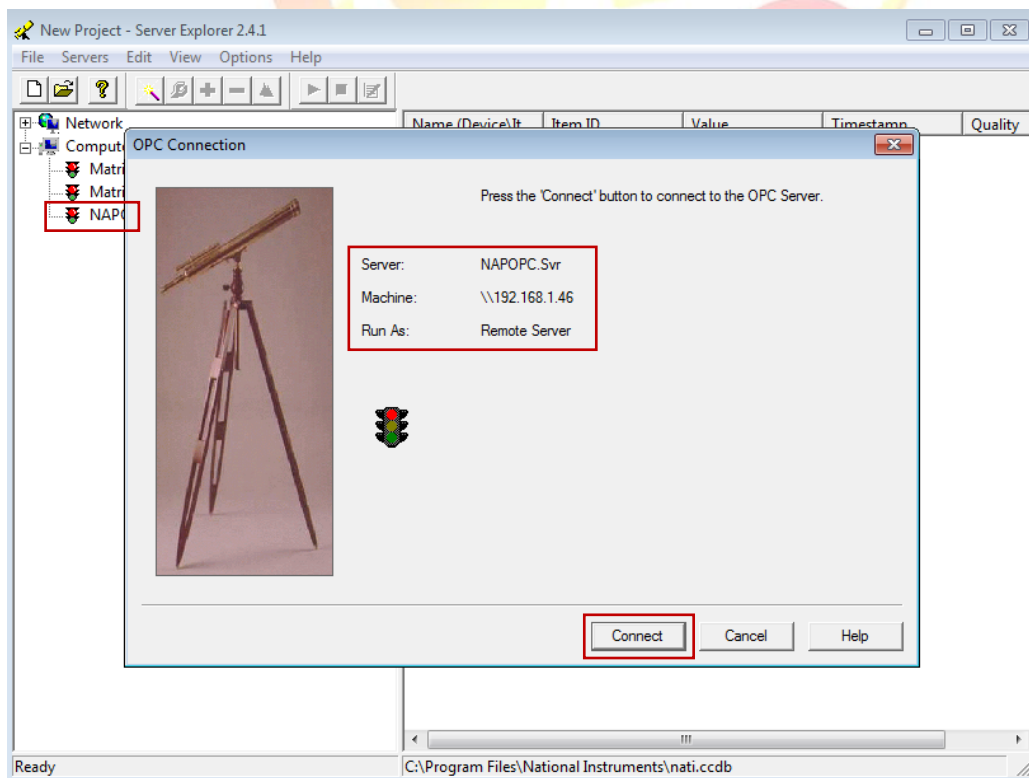
On the Server side, set up the DCOM of the XP-8000-CE6/XP-8000-Atom-CE6. Please refer to the Section 3.2.1 “Set up the Server side (XPAC)” in the user manual of NAPOPC\_CE5.

The download website: <http://opc.icpdas.com/download.htm#XP-8000-CE6>

## 6. Connect to PAC Server

### 6.1 Run the “NI Server Explorer” (2.4.1) for the connection

Step 1: Select the Server name “NAPOPC.Svr” to connect (as the picture)





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.

