






# **DCOM**

## **Configuration Manual**

**IM19S60-E**

Notices
<ul style="list-style-type: none"> <li>● The reproduction, transmission or use of this document or its contents is not permitted without express written authority.</li> <li>● Information and specifications in this document are subject to change without notice.</li> <li>● While information in this document is well edited and checked, mistake or omission may exist. Please don't hesitate to contact SUPCON if you have any question about this document.</li> <li>● Please contact SUPCON via email "SMS@supcon.com" if you have any question.</li> </ul>

Trademarks
<p>Trademarks or marks SUPCON, SPlant, Webfield, ESP-iSYS, MultiF, InScan, SupField are all registered, registering or using by Zhejiang SUPCON Technology Co., Ltd., which owns the properties of all trademarks or marks above. Without the written authority from Zhejiang SUPCON Technology Co., Ltd, no individual or company shall use any trademarks or marks above. We reserve the right to take legal action for any individual or company using trademarks or marks above illegally.</p>

Symbol Definition	
	<b>WARNING:</b> Indicates information that a potentially hazardous situation which, if not avoided, could result in serious injury or death.
	<b>RISK OF ELECTRICAL SHOCK:</b> Indicates information that Potential shock hazard where HAZARDOUS LIVE voltages greater than 30V RMS, 42.4V peak, or 60V DC may be accessible.
	<b>ESD HAZARD:</b> Indicates information that Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices
	<b>ATTENTION:</b> Identifies information that requires special consideration.
	<b>TIP:</b> Identifies advice or hints for the user.

# Table of Contents

<b>DCOM Configuration .....</b>	<b>1</b>
<b>Section 1 Overview .....</b>	<b>1</b>
<b>Section 2 Preliminary Preparation of Configuration.....</b>	<b>2</b>
<b>Section 3 DCOM Configuration .....</b>	<b>3</b>
3.1 Configure Server .....	3
3.1.1 Configure Component Services.....	3
3.1.2 Configure Folder Options .....	14
3.1.3 Configure System Service .....	15
3.1.4 Configure System Security Strategy.....	17
3.2 Configure Client.....	18
<b>Section 4 Configuration Interface Access Path .....</b>	<b>19</b>
4.1 Windows XP .....	19
4.2 Windows 7 .....	19
4.3 Windows Server 2003 .....	19
4.4 Windows Server 2008 Standard 64-bit .....	20
4.5 Windows 10.....	21
4.6 Windows Server 2016 Standard 64-bit .....	22
<b>Section 5 Information of OPC Server.....</b>	<b>24</b>
<b>Section 6 Revision.....</b>	<b>25</b>

# DCOM Configuration

## Section 1 Overview

---

OPC, as a universal industrial standard used widely, is usually used for the inter-connection between DCS and the process of the other system software. If OPC server and OPC client are not running in the same computer, it needs to perform OPC remote connection and DCOM configuration for both computers.

## Section 2 Preliminary Preparation of Configuration

---

Before configuring DCOM, make sure:

- Windows operating system should be installed and configured according to responding installation specification.
- User should use “administrator” to login Windows on the computer which is as sever and client. Only the administrator-level user could set user account and configure DCOM.
- Communication between DCOM sever and DCOM client is well.(User can use the command “ping”)
- The account and password of current user on the server should accord with that on the client. For example, if the account and password of computer running client software are DcomUser and abc, the account and password of server software have to be DcomUser and abc, too.



---

**Attention:**

**Both the account and the password should be the same. And empty password is not allowed.**

---

## Section 3 DCOM Configuration

---

This section takes Windows 7 operation system as an example to introduce how to configure DCOM. Configuration methods in other operation systems are similar.

Restart the computer after DCOM configuration completed. Server and client should login by the same user name and password, and the password should not be null.

### 3.1 Configure Server

Configure following items for server:

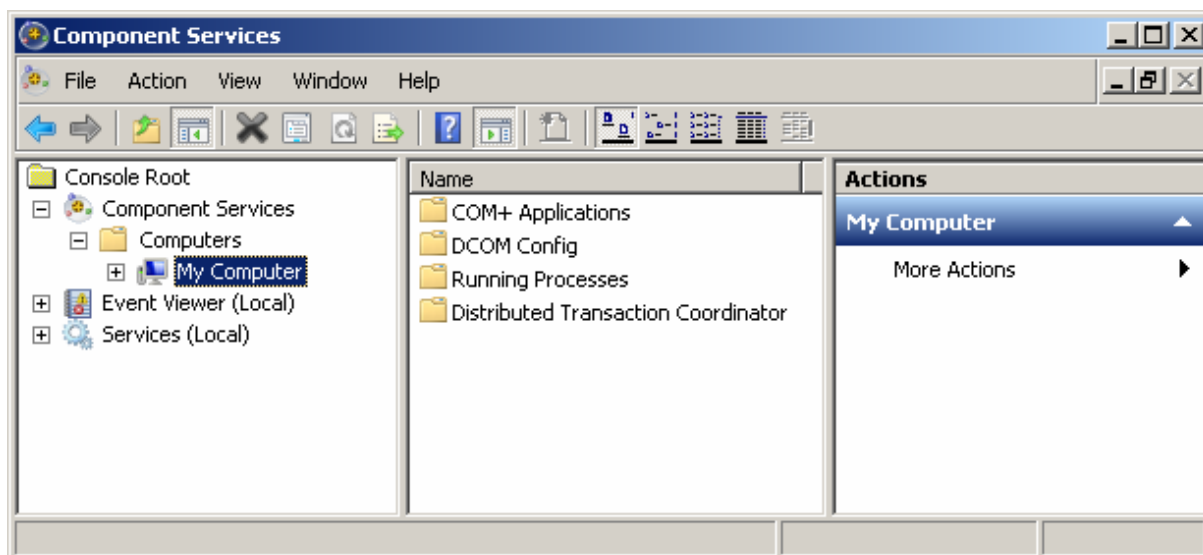
- Configure “Computer” properties.
- Configure “OpcEnum” properties.
- Configure OPC server properties.
- Configure folder options.
- Configure system service.
- Configure system security strategy.

#### 3.1.1 Configure Component Services

Enter into the “Component Services” interface by the following instruction, as shown in Figure 3-1.

- For 32-bit operation system, input “DCOMCNFG” in “Run” dialog.
- For 64-bit operation system, input “mmc -32” in “Run” dialog, and add “Component Services” in the window popped up.

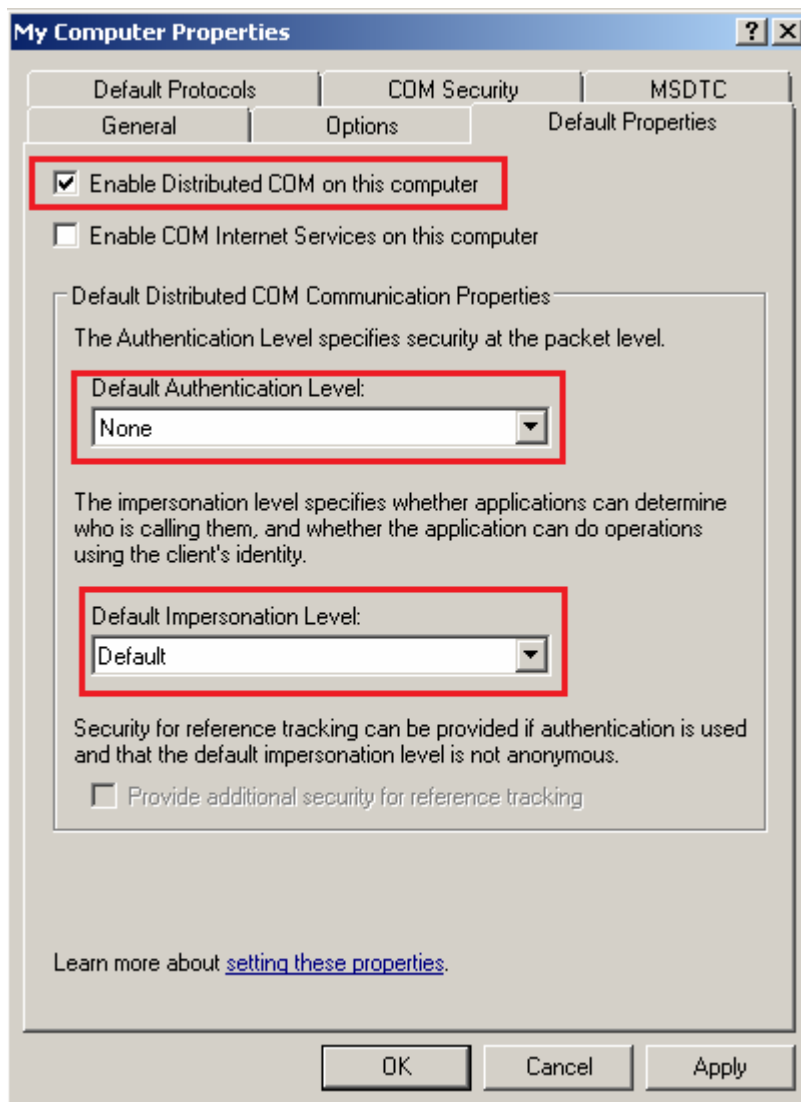
Operations in 64-bit windows 7 are the same as operations in windows server 2008. For details, please refer to Step 1 in “4.4 Windows Server 2008 Standard 64-bit”.



**Figure 3-1 Component Services**

### **Configure Computer Properties**

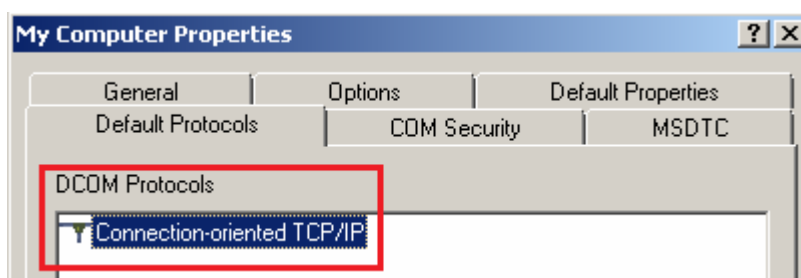
Select [Component Services/ Computers/ My Computer] in Figure 3-1, right-click “My Computer” and select “Properties”, and select “Default Properties” tab in the interface popped up. Settings for items are shown in Figure 3-2.



**Figure 3-2 Default Properties**

- Select “Enable Distributed COM on this computer”.
- Set “Default Authentication Level” as “None”.
- Set “Default Impersonation Level” as “Default”.

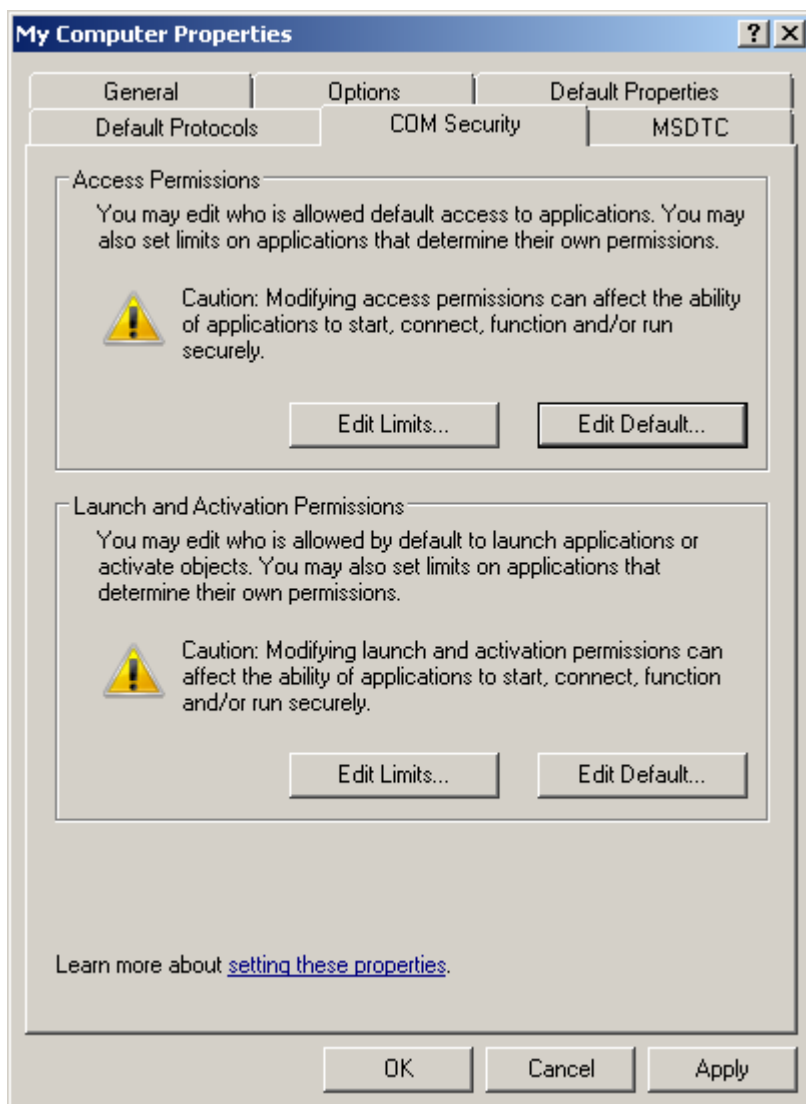
Switch to “Default Protocols” tab, as shown in Figure 3-3.



**Figure 3-3 Default Protocols**

Switch to “COM Security” tab, as shown in Figure 3-4.





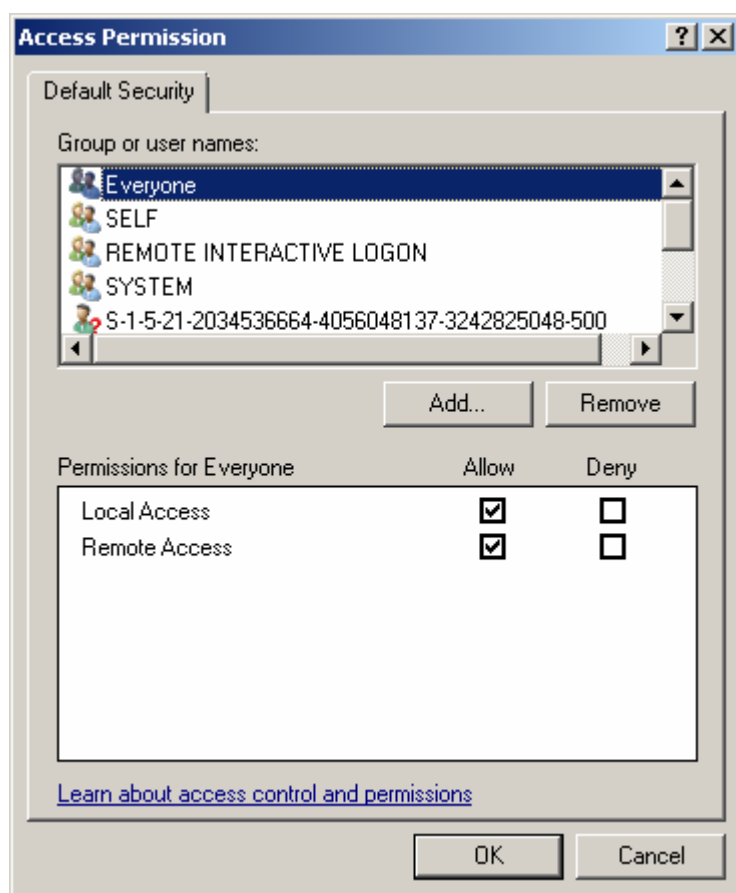
**Figure 3-4 COM Security**

Click buttons “Edit Limits” and “Edit Default” for both “Access Permissions” and “Launch and Activation Permissions” panes, and add following users:

- Everyone
- Interactive
- ANONYMOUS LOGON
- Administrator
- Administrators
- SYSTEM

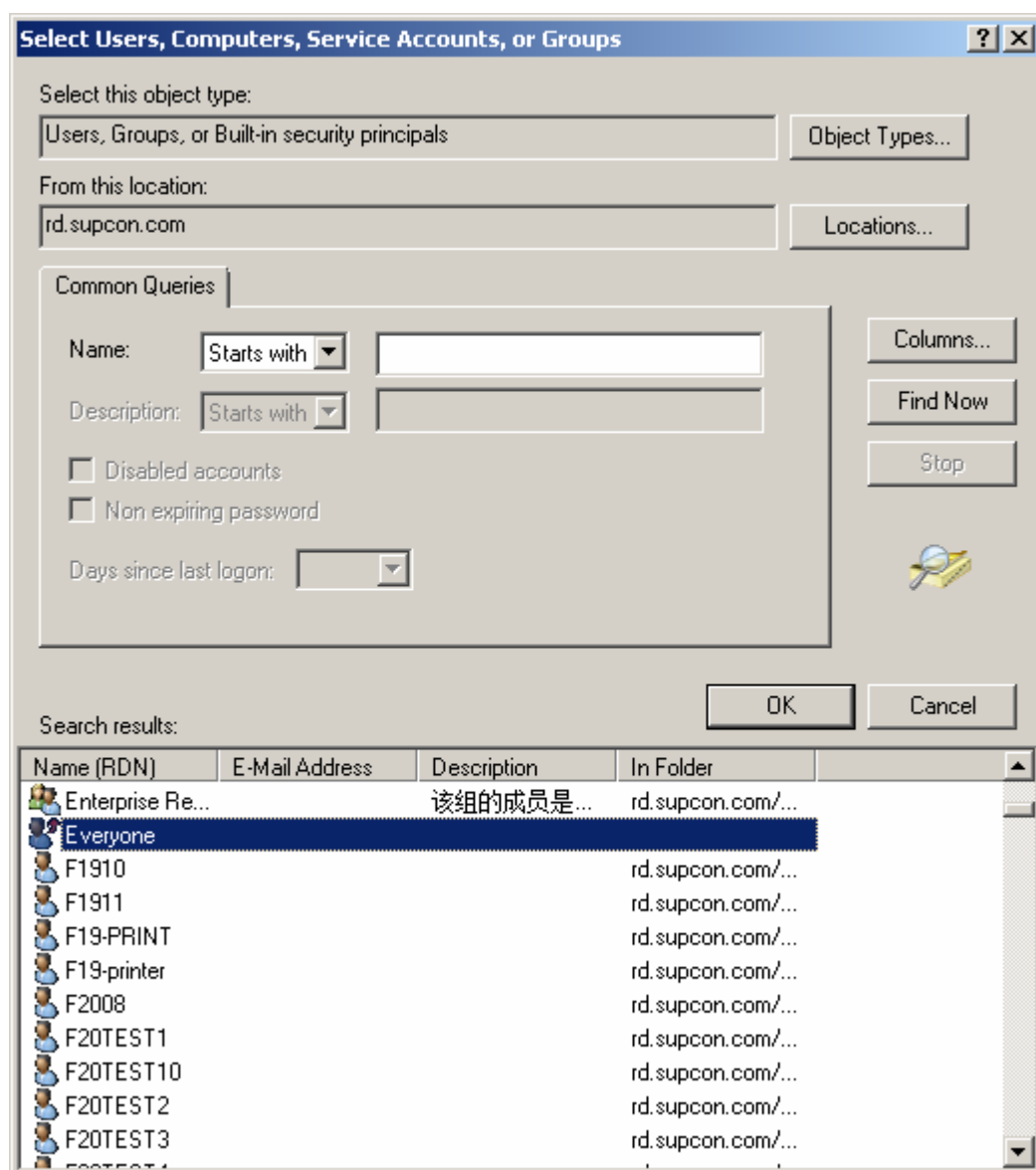
Take settings for “Edit Default” of “Everyone” as an example, steps to add user are shown below:

Click “Edit Default” for “Access Permissions”, to pop up the interface in Figure 3-5.



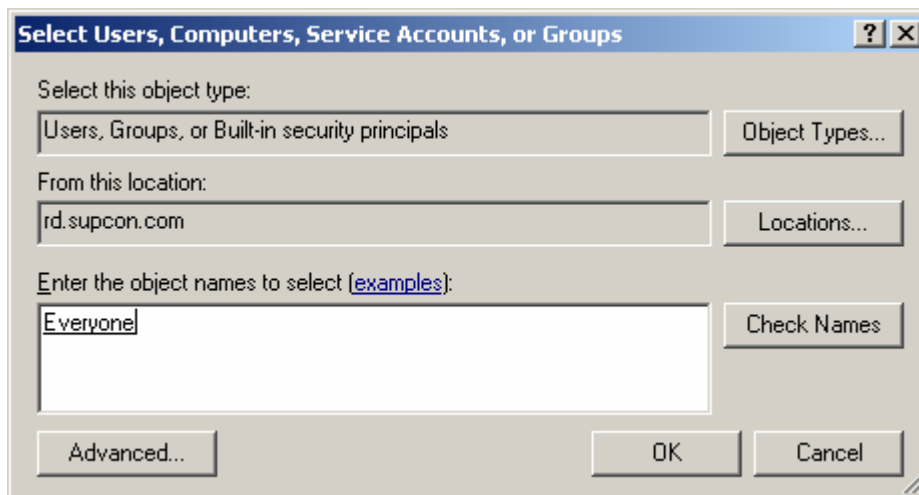
**Figure 3-5 Access Permission**

Click “Add” and click “Advanced” in the interface popped up, and then click “Find Now”, select “Everyone”, as shown in Figure 3-6.



**Figure 3-6 Select Users, Computer, Service Accounts, or Groups**

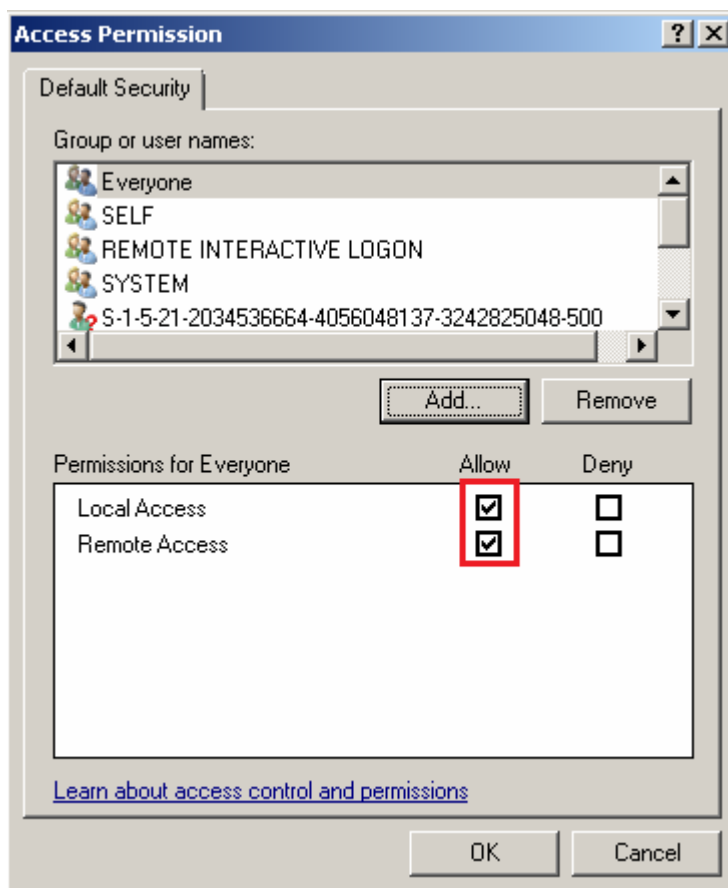
Click "OK" to view the selected user, as shown in Figure 3-7.



**Figure 3-7 View user name**

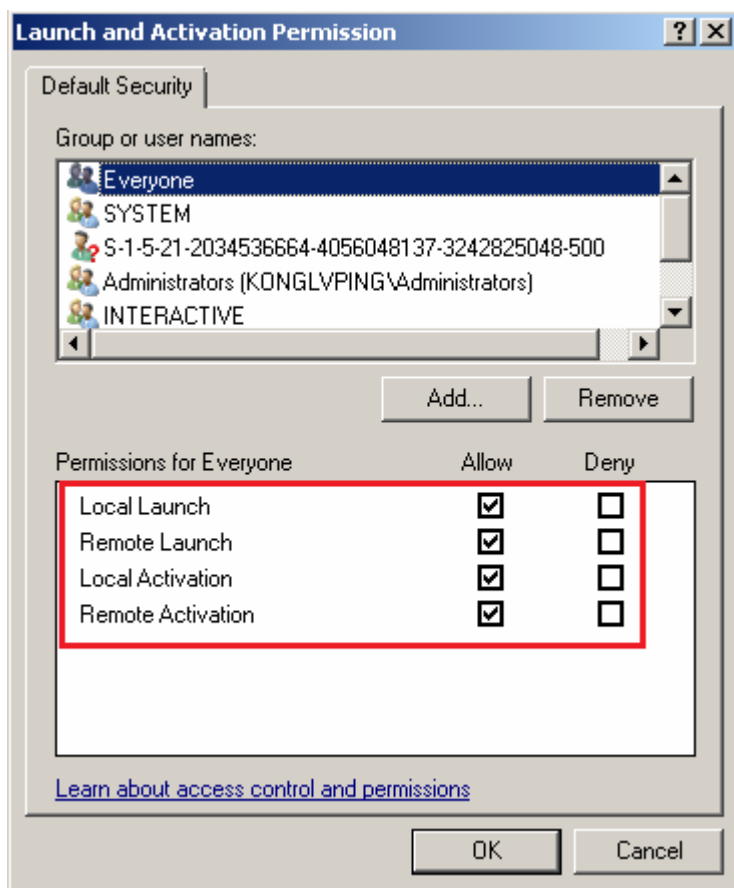
Click "OK" to add "Everyone" successfully.

Select "Everyone" and select "Allow" for both local and remote access, as shown in Figure 3-8.



**Figure 3-8 Add "Everyone" to access permission**

The interface adding "Everyone" user permissions in "Launch and Activation Permission" is shown in Figure 3-9.

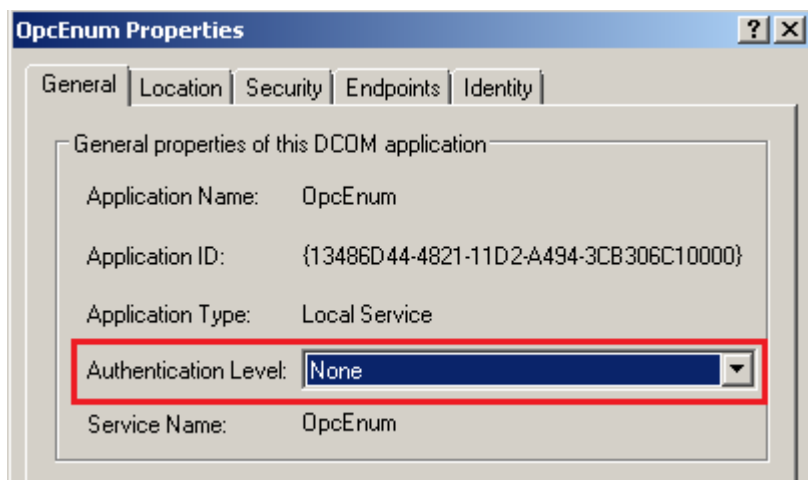


**Figure 3-9** Add “Everyone” to launch and activation permission

Please make sure that the 6 user permissions added are selected as “Allow”.

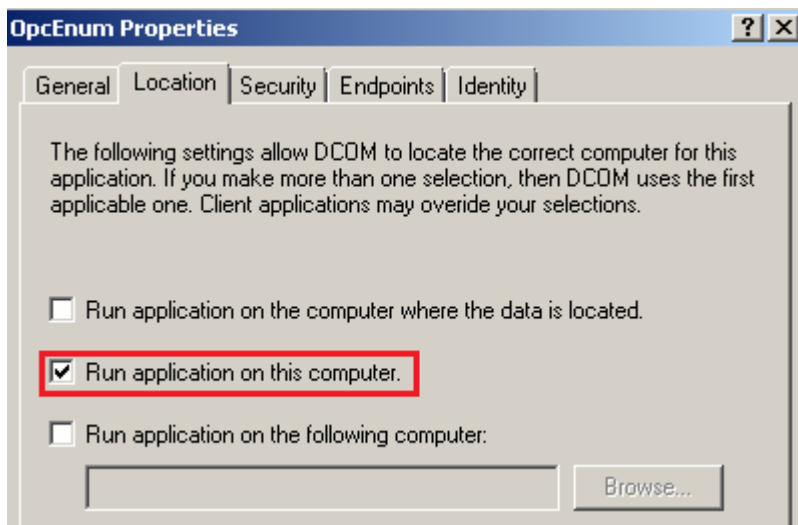
### Configure OpcEnum Properties

Select [Component Services/ Computers/ My Computer/ DCOM Config/ OpcEnum], right-click and select “Properties”, and select “General” tab. Change “Authentication Level” as “None”, as shown in Figure 3-10.



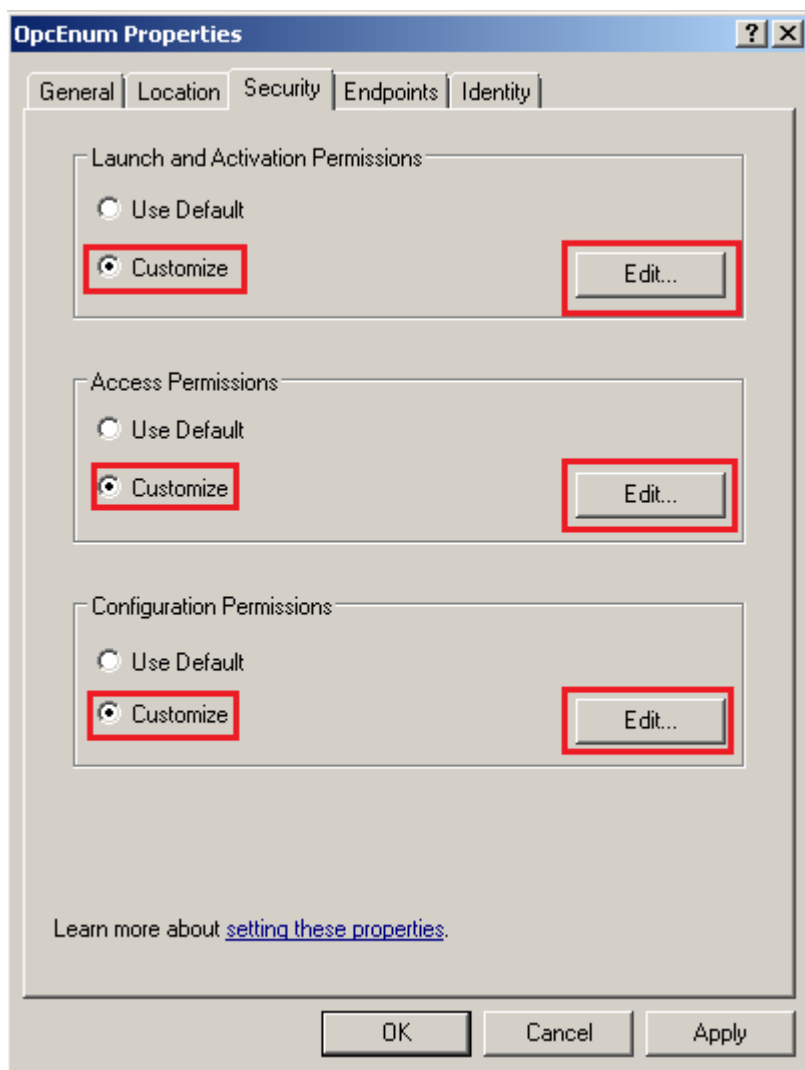
**Figure 3-10** General

Select “Location” pane, the setting is shown in Figure 3-11.



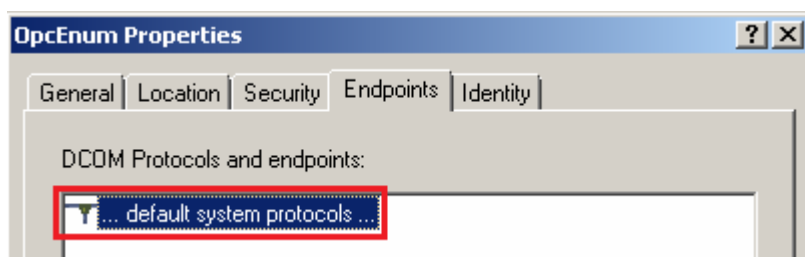
**Figure 3-11 Location**

Select “Security” tab. Select “Customize” for 3 permissions, as shown in Figure 3-12. Click “Edit” buttons one by one to add users “Everyone”, “Interactive”, “ANONYMOUS LOGON”, “Administrator”, “Administrators”, “SYSTEM”. All permissions are set as “Allow”. Operations steps are shown from Figure 3-5 to Figure 3-9.



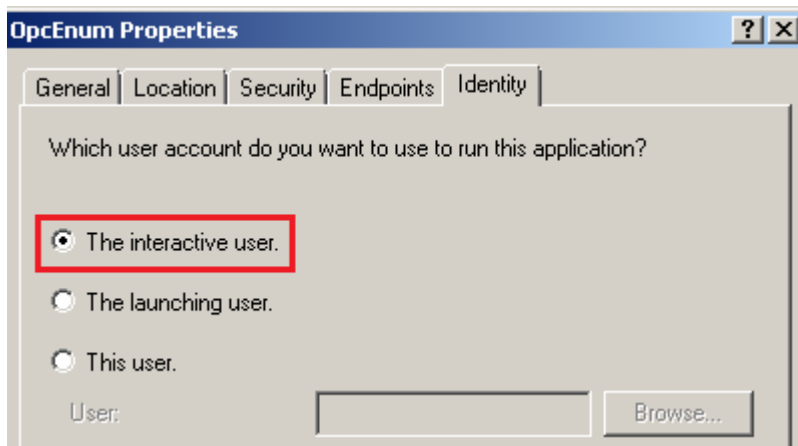
**Figure 3-12 Security**

Select "Endpoints" tab, the setting is shown in Figure 3-13.



**Figure 3-13 Endpoints**

Select "Identity" and select "The interactive user", as shown in Figure 3-14.



**Figure 3-14 Identity**

If the option “The interactive user” is disabled, enable the selection according to the following steps:

1. Find the path of the application opcenum.exe by computer's function Search.
2. Open the dialog “Run” by the key combination Windows+R and execute cmd command in “Run” dialog. Open the cmd interface
3. Use the command cd to switch to the path of opcenum.exe and execute the commands “opcenum /unregserver”, as the Figure 3-15 shows.
4. Execute the commands “opcenum /regserver” in the cmd interface.

```
C:\Windows\Prefetch>cd C:\Windows\SysWOW64
                                     Switch to the path of opcenum.exe
C:\Windows\SysWOW64>opcenum /unregserver
                                     Excute the commands
C:\Windows\SysWOW64>opcenum /regserver
```

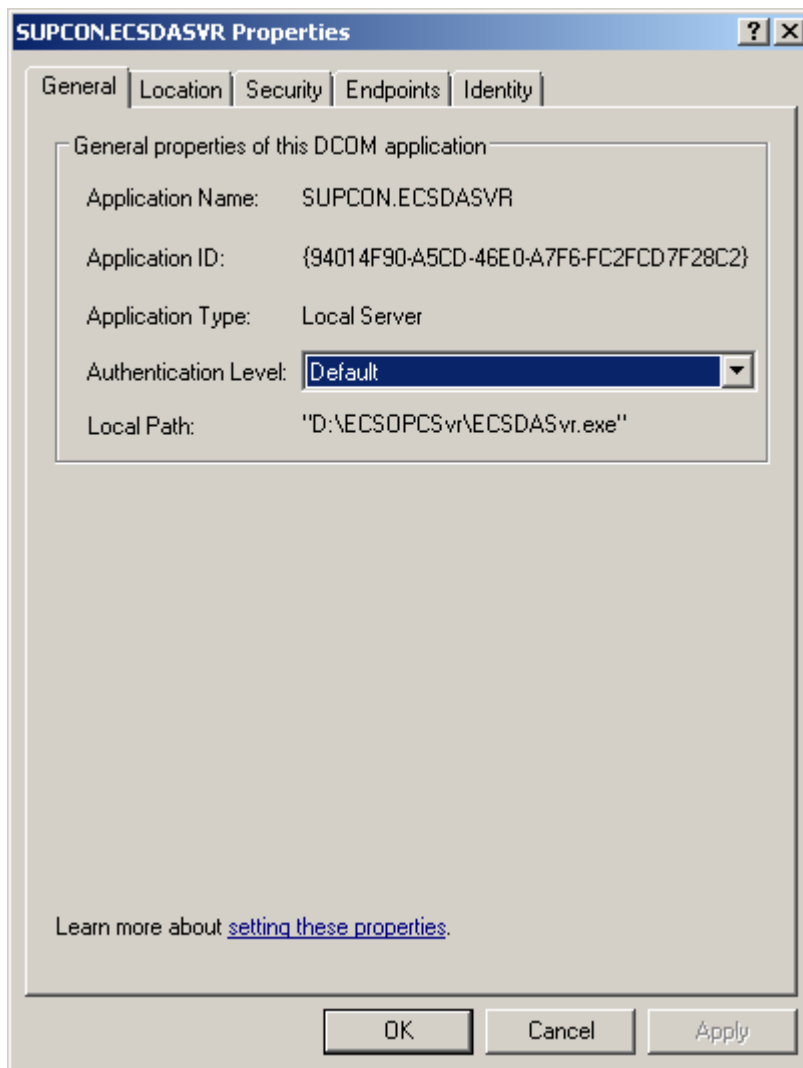
**Figure 3-15 Enable the selection according to the steps**

### Configure OPC Server Properties

Take ECSDASVR server as an example, select [Component Services/ Computers/ My Computer/ DCOM Config/ SUPCON.ECSDASVR], right-click and select “Properties”, to open the ECSDASVR properties interface, as shown in Figure 3-16.

Configuration of ECSDASVR server is the same as OpcEnum.

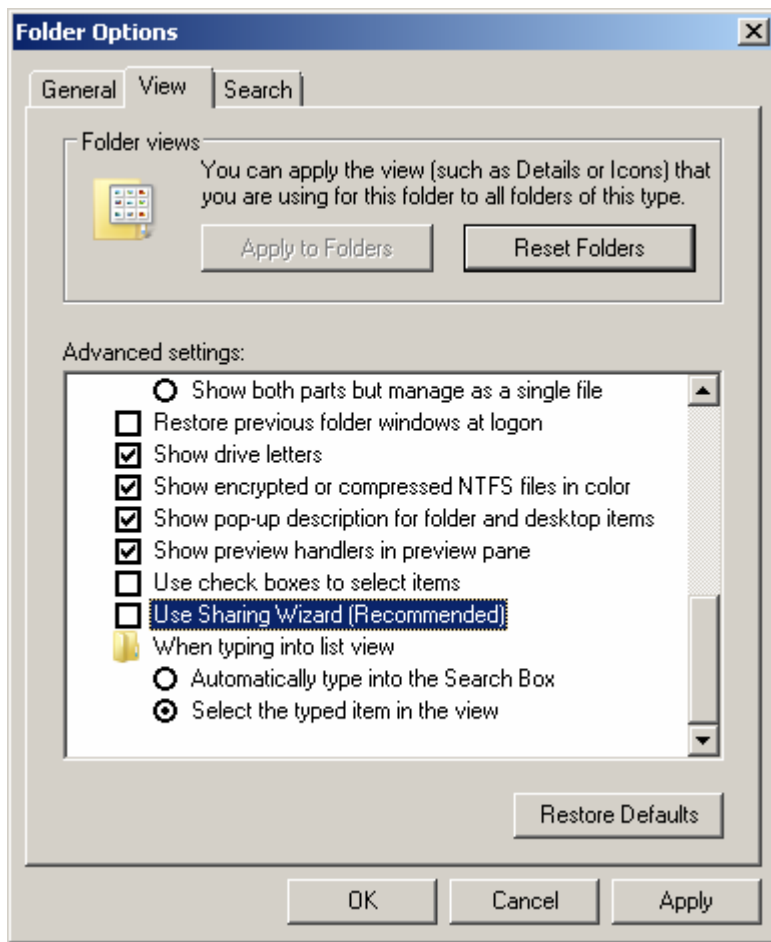




**Figure 3-16 ECSDASVR properties**

### 3.1.2 Configure Folder Options

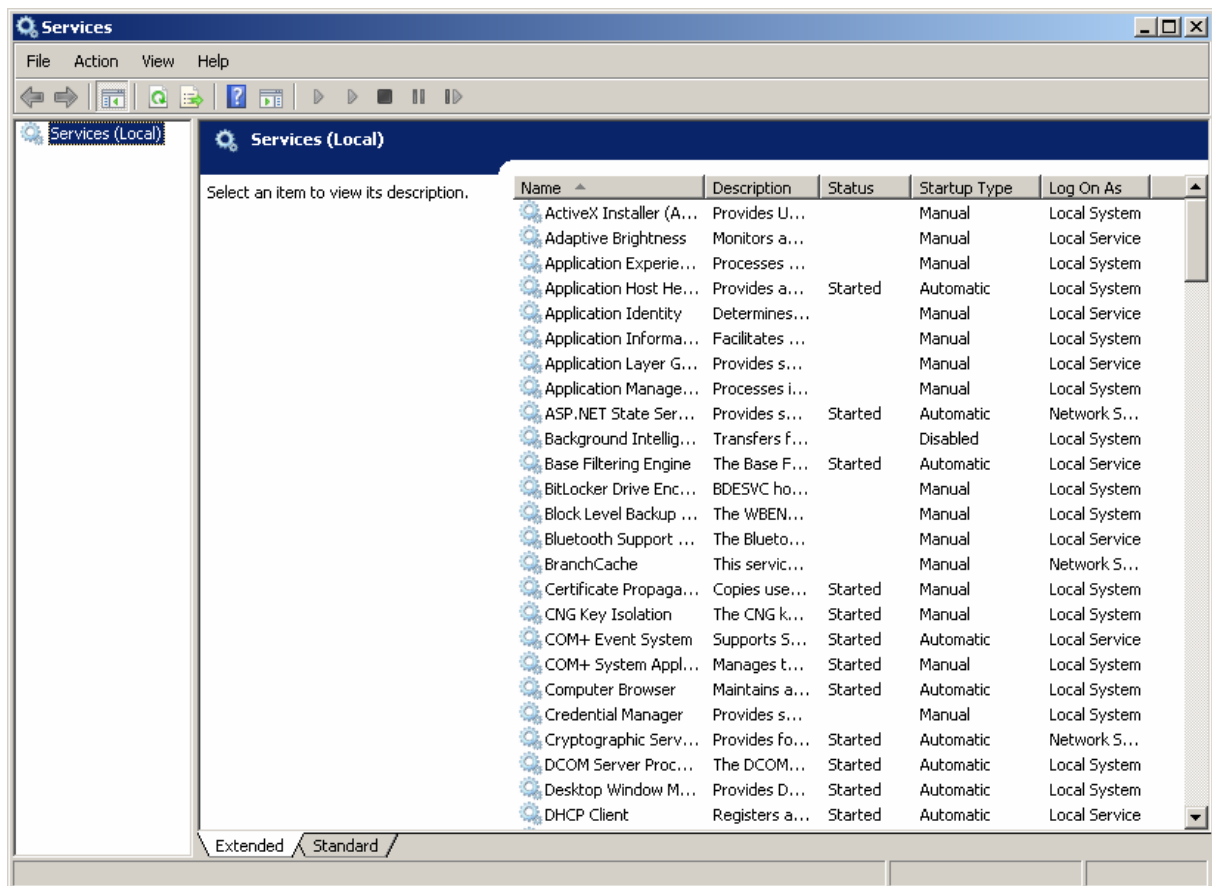
Double-click "Computer" icon on desktop to open its interface. Select [Organize/ Folder and search options] to open the "Folder Options" interface. Select "View" tab, unselect "Use Sharing Wizard (Recommended)", as shown in Figure 3-17.



**Figure 3-17 Folder Options**

### 3.1.3 Configure System Service

Select [Start/ Control Panel/ System and Security/ Administrative Tools/ Services] to open the “Services” interface, as shown in Figure 3-18.



**Figure 3-18 Services**

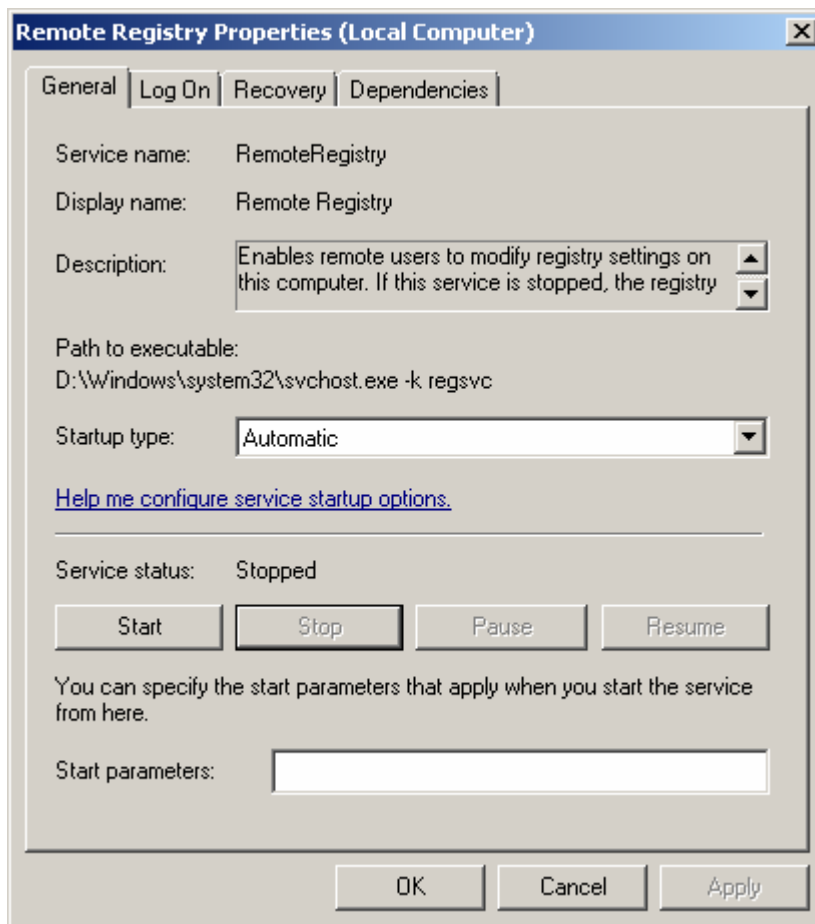
Make sure items below are “Started”, as shown in Figure 3-19.

Computer Browser	Maintains a...	Started	Automatic	Local System
DCOM Server Process Launcher	The DCOM...	Started	Automatic	Local System
Remote Procedure Call (RPC)	The RPCSS...	Started	Automatic	Network S...
Remote Procedure Call (RPC) Locator	In Window...	Started	Automatic	Network S...
Remote Registry	Enables re...	Started	Automatic	Local Service
Routing and Remote Access	Offers rout...	Started	Automatic	Local System
RPC Endpoint Mapper	Resolves R...	Started	Automatic	Network S...

**Figure 3-19 Check items status**

If the item selected is “Disabled”, please start it by the following operation.

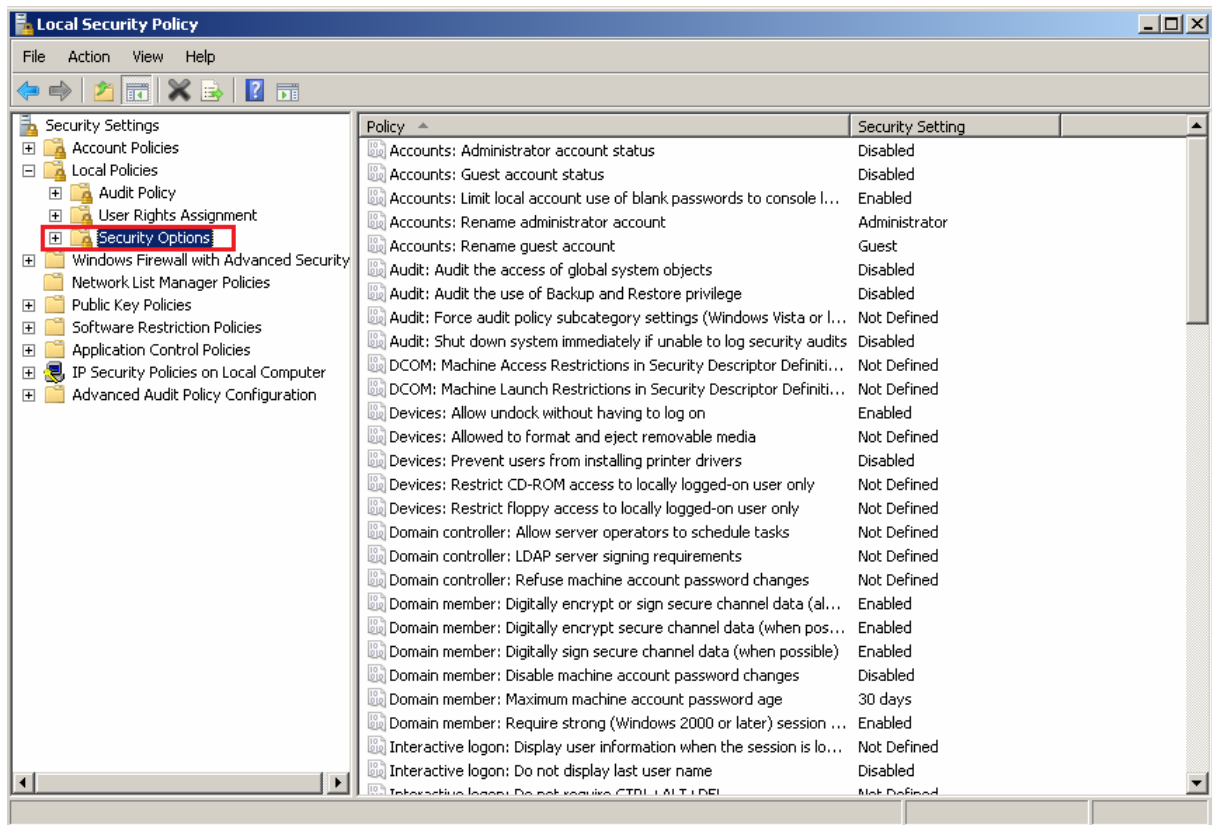
Double-click the item to pop up the dialog shown in Figure 3-20, click “Start” to start it.



**Figure 3-20 Service status**




### 3.1.4 Configure System Security Strategy

Press the keys "Win+R" to pop up the "Run" dialog, input "secpol.msc" to enter into "Local Security Policy" interface, as shown in Figure 3-21.



**Figure 3-21 Local Security Policy**

Set the “Security Setting” status of following items as shown in Figure 3-22.

 Accounts: Guest account status	Enabled
 Network access: Let Everyone permissions apply to anonymous users	Enabled
 Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves

**Figure 3-22 Security settings**

## 3.2 Configure Client

Configure following items for client computer:

- Configure “Computer” properties: configuration method and contents are same with server, please refer to 3.1.1.
- Configure “OpcEnum” properties: configuration method and contents are same with server, please refer to 3.1.1.
- Configure folder options: configuration method and contents are same with server, please refer to 3.1.2.
- Configure system service: configuration method and contents are same with server, please refer to 3.1.3.
- Configure system security strategy: configuration method and contents are same with server, please refer to 3.1.4.

## Section 4 Configuration Interface Access Path

---

Different operation systems have different access paths for configuration interface

### 4.1 Windows XP

1. Configuration Interface Access of Component Services

Select [Start/ Run] and input "DCOMCNFG" to open the "Components Services" interface.

2. Configuration Interface Access of Folder Options

Open "Computer" interface, select [Tools/ Folder Options]. Select "View" tab, unselect "Use Simple File Sharing (Recommended)".

3. Configuration Interface Access of System Service

Select [Start/ Settings/ Control Panel (Classical View)/ Administrative Tools/ Services].

4. Configuration Interface Access of System Security Strategy

Press the keys "Win+R" to pop up the "Run" dialog, input "secpol.msc" to enter into "Local Security Policy" interface.

### 4.2 Windows 7

"Section 3 DCOM Configuration" describes how to configure DCOM taking the Window 7 OS as example (including 32-bit OS and 64-bit OS).



---

**Tip:**

**Only the start of "Component Services" is different between 64-bit window 7 and 32-bit window 7, other operations are same.**

---

### 4.3 Windows Server 2003

1. Configuration Interface Access of Component Services

Select [Start/ Run] and input "DCOMCNFG" to open the "Components Services" interface.

2. Configuration Interface Access of Folder Options

Open "Computer" interface, select [Tools/ Folder Options]. Select "View" tab, unselect "Use Simple File Sharing (Recommended)".

3. Configuration Interface Access of System Service

Select [Start/ Settings/ Control Panel (Classical View)/ Administrative Tools/ Services].

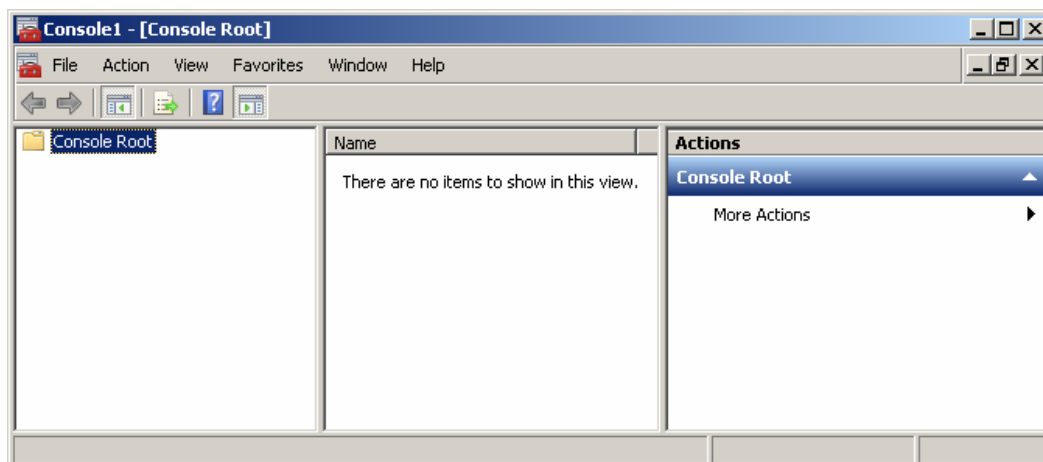
#### 4. Configuration Interface Access of System Security Strategy

Press the keys “Win+R” to pop up the “Run” dialog, input “secpol.msc” to enter into “Local Security Policy” interface.

### 4.4 Windows Server 2008 Standard 64-bit

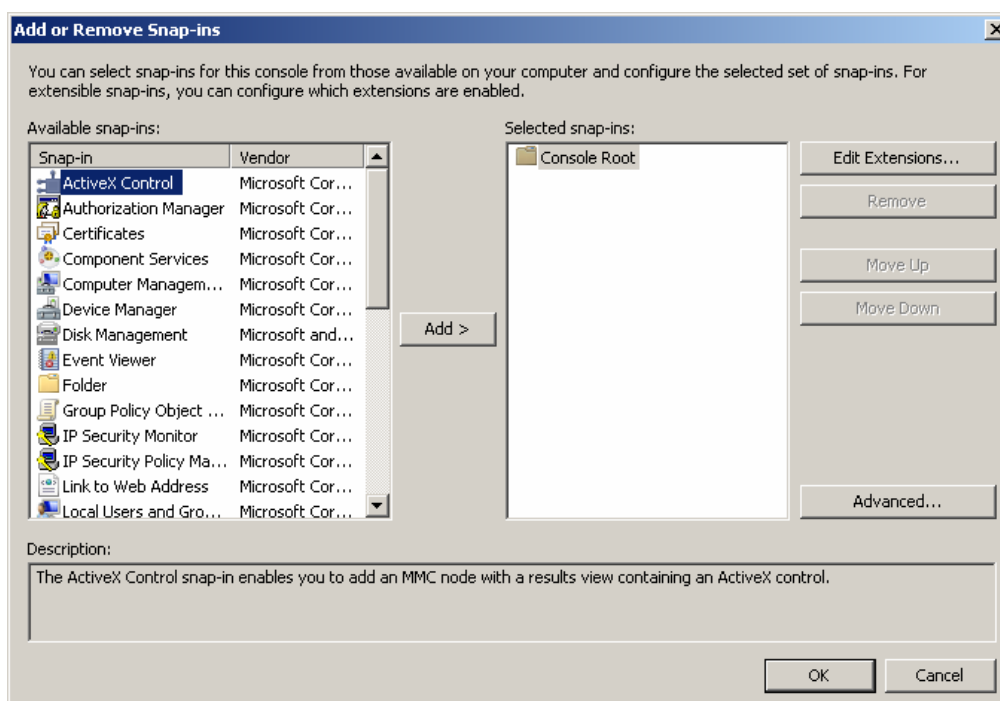
#### 1. Configuration Interface Access of Component Services

Select [Start/ Run] and input “mmc -32” to open the “Console Root” interface, as shown in Figure 4-1.



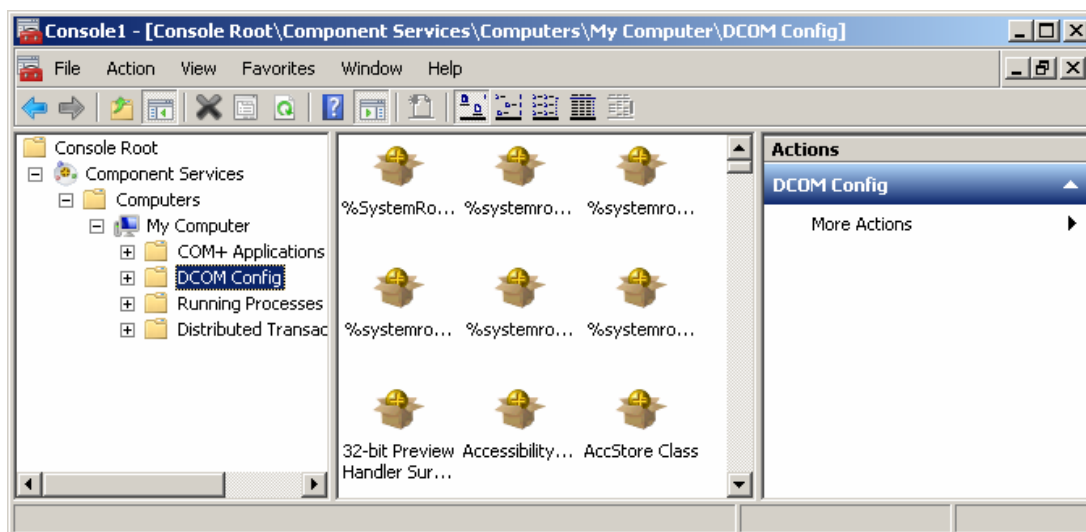
**Figure 4-1 Console1 interface**

Click [File/ Add/Remove Snap-in...] to open the following window, as shown in Figure 4-2.



**Figure 4-2 Add or Remove Snap-ins**

Select “Component Services” in “Available snap-ins” pane, then click “Add” and “OK” to add component services to console root, as shown in Figure 4-3. Configure DCOM as below for the component service added.



**Figure 4-3 Add component services to console root**

## 2. Configuration Interface Access of Folder Options

Open “Computer” interface, select [Start/ Computer/ Organize/ Folder and search options]. Select “View” tab, unselect “Use Sharing Wizard (Recommended)”.

## 3. Configuration Interface Access of System Service

Select [Start/ Control Panel/ System and Security/ Administrative Tools/ Services].

## 4. Configuration Interface Access of System Security Strategy

Press the keys “Win+R” to pop up the “Run” dialog, input “secpol.msc” to enter into “Local Security Policy” interface.

# 4.5 Windows 10

## 1. Configuration Interface Access of Component Services

- For 32-bit operation system, input “DCOMCNFG” in “Run” dialog to configure DCOM.
- For 64-bit operation system, input “mmc -32” in “Run” dialog, and add “Component Services” in the window popped up to configure DCOM.

Operations in 64-bit windows 7 are same to operations in windows server 2008. For detail, please refer to “1” in “4.4 Windows Server 2008 Standard 64-bit”.



### Attention:

In Windows 10 operation system, please set “Default Impersonation Level” as “Identify”.

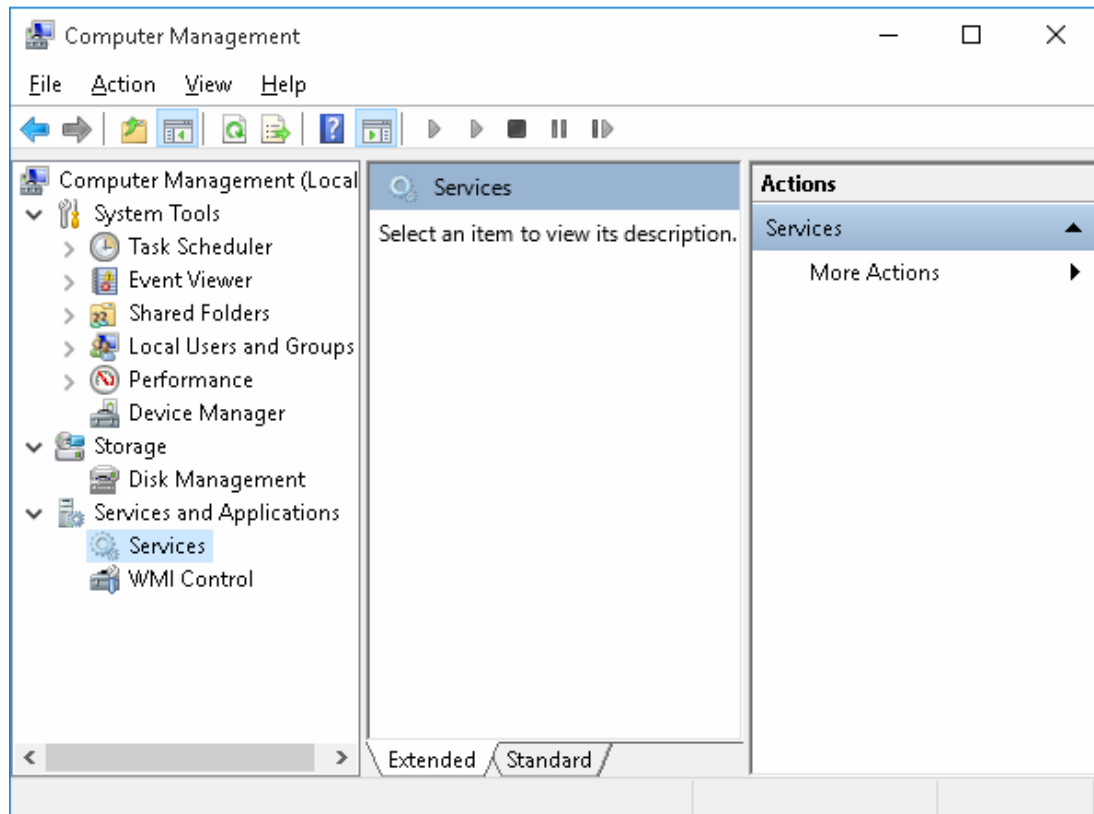
## 2. Configuration Interface Access of Folder Options



Open “This PC” interface, select [View/ Options]. Select “View” tab, unselect “Use Simple File Sharing (Recommended)”.

### 3. Configuration Interface Access of System Service

Right click “This PC” and select “Manage” in the right-click menu, pop up the “Computer Management” interface, then select “Services” below “Services and Applications”, as shown below.



**Figure 4-4 Service list window**

### 4. Configuration Interface Access of System Security Strategy

Press the keys “Win+R” to pop up the “Run” dialog, input “secpol.msc” to enter into “Local Security Policy” interface.

## 4.6 Windows Server 2016 Standard 64-bit

### 1. Configuration Interface Access of Component Services

Select [Start/ Windows System/ Command Prompt] and input “mmc -32” to open the “Components Services” interface for DCOM configuration. The steps of configuration are similar to the operations in Windows Server 2008 Standard system (64-bit), please refer to the first step in the chapter “Windows Server 2008 Standard 64-bit”.

### 2. Configuration Interface Access of Folder Options

Open “This PC” interface, select [View / Options]. Select “View” tab, unselect “Use Sharing Wizard (Recommended)”.

### 3. Configuration Interface Access of System Service

Select [Start/ Control Panel (Administrative Tools)/ Administrative Tools/ Services].

4. Configuration Interface Access of System Security Strategy

Press the keys “Win+R” to open the “Run” dialog, input “secpol.msc” to enter into “Local Security Policy” interface.

## Section 5 Information of OPC Server

The OPC server information of SUPCON main system and product is shown in Table 5-1.

**Table 5-1 Information of OPC server**

Control System or Product	OPCServer	Description
ECS-100/JX-300X/JX-300XP	SUPCON.JXServer	Independent software: OPC Server
ECS-700	SUPCON.SCRTCore	Integrated with VisualField
	SUPCON.ECSDASVR	Independent software: ECSOPCSvr.exe
	SUPCON.ECSAESVR	
G3/G5/G5Pro	SUPCON.GCSServer	Integrated with GCSContrix
TCS-900	SUPCON.TCSOPCDASVR	Integrated with SafeContrix
VxSCADA	SUPCON.VxSCADA	Integrated with VxSCADA
SAMS	SUPCON.SAMS	Integrated with SAMS
	SUPCON.SAMSAEServer	
MISGate	SUPCON.MISGateOPC	Integrated with MISGate
	SUPCON.OPCConnectGate	
PIMS	SUPCON.PIMS	Integrated with PIMS
VxCollector	SUPCON.RCIOPC	Integrated with VxCollector



**Tip:**

For usage about OPC server, please refer to the user manuals of corresponding software.

## Section 6 Revision

**Table 6-1 Retrofit list of the version**

Document Version	Applicable Version	Remarks
V1.0	Achieve interconnection via OPC (remote connection)	The first version
V1.1 (20121228)	Achieve interconnection via OPC (remote connection)	
V2.0 (20151023)	For OPC interconnection.	Rewrite.
V2.1 (20161011)	For OPC interconnection.	Add setting steps of Windows 10 operation system.
V2.2 (20170510)	For OPC interconnection.	Add code.
V2.3 (20171103)	For OPC interconnection.	Add setting steps of Windows Server 2016 Standard 64-bit operation system.
V2.4 (20190225)	For OPC interconnection.	<ul style="list-style-type: none"> <li>● Modify the description about opcenum.</li> <li>● Modify the description and the setting of Default Impersonation Level in Windows 10 operation system.</li> </ul>
V2.5 (20200707)	For OPC interconnection.	Add illustration about G5Pro in the section "Information of OPC Server".
V2.6 (20201028)	For OPC interconnection.	Adjust the description location of the component services configuration portal.