

Kepware Products for Windows 2000, NT, XP and Server 2003

DCOM Configuration for KEPServerEX



KTSM-00010
Version 2.0.12

© 2006 Kepware Technologies

KEPWARE END USER LICENSE AGREEMENT AND LIMITED WARRANTY

The software accompanying this license agreement (the Software) is the property of Kepware Inc, and is protected by United States and International Copyright laws and International treaty provisions. No ownership rights are granted by this Agreement or possession of the Software. Therefore, you must treat the Licensed Software like any other copyrighted material (e.g., a book or musical recording), except that you may make a single copy for backup or archival purposes. Your rights and obligations in its use are described as follows:

1. You may use and display this software on a single computer.
2. You may make one copy of the software for archival purposes or you may copy the software onto your hard disk and hold the original for archival purposes.
3. You may not modify or attempt to reverse engineer the software, or make any attempt to change or even examine the source code of the software.
4. You may transfer the software to another computer using the utilities provided. However, the software must be used on only a single computer at one time.
5. You may not give or distribute copies of the software or written materials associated with the software to others.
6. You may not sub-license, sell, or lease the software to any person or business.

Return Policy

The original licensee of the software can return it within sixty (60) days of purchase. Please call us for a Return Material Authorization Number.

Limited Warranty

Kepware does not warrant that the Software will be error free; that it will satisfy your planned applications or that all defects in the Software can be corrected. If Kepware provides information or assistance regarding the use of the Software or otherwise, Kepware is not assuming the role of engineering consultant. Kepware disclaims responsibility for any errors or omissions arising in connection with engineering in which its Software or such information or assistance is used.

The foregoing is the sole and exclusive warranty offered by Kepware.

Kepware disclaims all other warranties, express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose, with regard to the licensed software and all accompanying materials.

In no event shall Kepware be liable for incidental or consequential damages, including lost profit, lost savings, lost opportunities, or other incidental or consequential damages arising out of the use or inability to use the licensed software, even if Kepware has been advised of the possibility of such damages.

Kepware's entire liability shall be, at Kepware's option, either (a) return of the price paid for the Software (or component), or (b) repair or replacement of the Software (or component) that does not meet Kepware's Limited Warranty and which is returned to Kepware within the warranty period. This shall be the sole and exclusive obligation of Kepware and your sole and exclusive remedy with respect to any such failure. The Limited Warranty is void if failure of the Software (or component) has resulted from accident, abuse or misapplication.

Support

Kepware provides unlimited e-mail support for all Software whether a demo or registered license. Kepware will provide a total of two hours free phone support for all registered Software after paying the applicable license fees. Kepware will provide unlimited phone support so long as you have paid Kepware any applicable maintenance or support fees and subject to the terms of those agreements. All corrections and maintenance releases will be made available through Kepware's Internet site. All major product releases of the Software are subject to upgrade fees. At no time will on-site support be provided without advance payment to Kepware for a minimum of two days on-site engineering support services, plus all expenses.

Trademarks

Kepware™ and KEPServerEX™ are trademarks of Kepware Technologies. All other trademarks, whether claimed or registered, are the exclusive property of their respective owners.

Kepware Technologies

400 Congress Street, 3rd Floor
Portland, Maine 04101

Sales: (207) 775-1660 x228

Technical Support: (207) 775-1660 x211

Fax: (207) 775-1799

E-mail: sales@kepware.com or
technical.support@kepware.com

Home page: www.kepware.com

Table of Contents

OVERVIEW	1
CONFIGURING DCOM FOR WIN NT / 2000 DOMAINS.....	2
USING THE INSTALL PROGRAM TO REGISTER THE SERVER.....	2
EDITING THE DCOM CONFIGURATION.....	3
CONFIGURING DCOM FOR WIN XP DOMAINS	11
USING THE INSTALL PROGRAM TO REGISTER THE SERVER.....	11
RUNNING THE DCOM CONFIGURATION UTILITY	12
CONFIGURING DCOM FOR WINDOWS XP SP2 / WINDOWS 2003 SERVER SP1	25
CONFIGURING THE FIREWALL	25
CONFIGURING DCOM.....	28
SUMMARY	32
CONFIGURING DCOM ON WORKGROUPS VS. DOMAINS.....	33
CONNECTING WORKGROUP TO WORKGROUP	33
CONNECTING WORKGROUP TO DOMAIN	33
CONNECTING DOMAIN TO WORKGROUP	33
APPENDIX A: USING THE OPC_REMOTE.REG FILE	34
PREPARING THE REMOTE PC	34
APPENDIX B: CONFIGURING DCOM FOR WIN 95/98 DOMAINS.....	35
PREPARING WIN95/98 FOR DCOM	35
USING THE INSTALL PROGRAM TO REGISTER THE SERVER.....	35
<i>Adding DCOM Support to Win 95.....</i>	<i>36</i>
EDITING THE DCOM CONFIGURATION.....	37

Overview

This document is intended to provide the user with information and instruction on how to configure the Distributed Component Object Model (DCOM) for use with KEPServerEX. Since Windows NT/ 2000 security is more advanced and the options differ from Windows 95/98, we have broken this document down into three components. The first component of the document covers configuring DCOM for Windows NT/2000, the second component covers configuring DCOM for 95/98, and the third component covers Windows XP/2003.

Note: In Windows NT DCOM may function differently from one Service Pack to another. Service Pack 6 was used in creating this document and therefore it is suggested that Service Pack 6 be installed before attempting the following procedures.

Note: In our DCOM testing we have experienced instances where DCOM configuration changes do not take effect until the PC has been rebooted. If you have DCOM settings configured correctly but cannot establish a remote connection, you may want to consider rebooting both the server and client PCs.

Warning: The following instructions for DCOM configuration allow for **all access by all users** for all DCOM components. If security is a factor with your applications, you must set DCOM security settings appropriately. We recommend proving connectivity with open access before reducing access privileges to specific users at the application level.

Configuring DCOM for Win NT / 2000 Domains

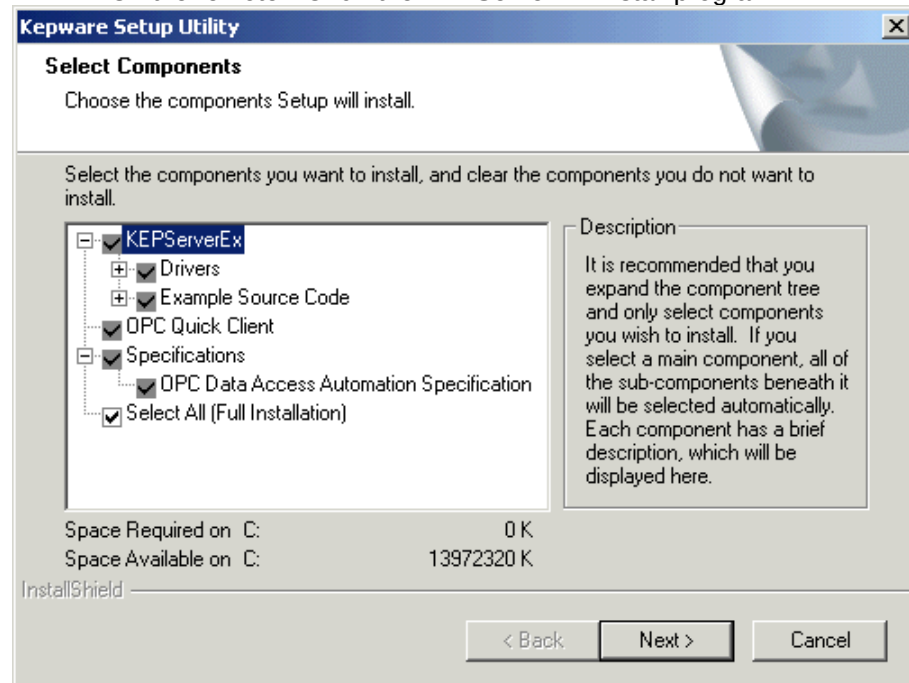
There may be variations in DCOM configuration between local and remote connections to KEPServerEX. Some client applications may not support browsing remote PC's for installed servers. For these clients you may need to add server registry entries to the client PC in order to obtain the proper CLSID for the server. The preferred method is running the server installation program and selecting only the OPC Quick Client for installation. If this cannot be done, then you can use the OPC_Remote.Reg file that is provided with the server install (see [Appendix A](#) for details on how to do this). If you are using another Operating System, see that section for instructions.

The first part of this document will explain the steps required to prepare for DCOM configuration on the remote PC.

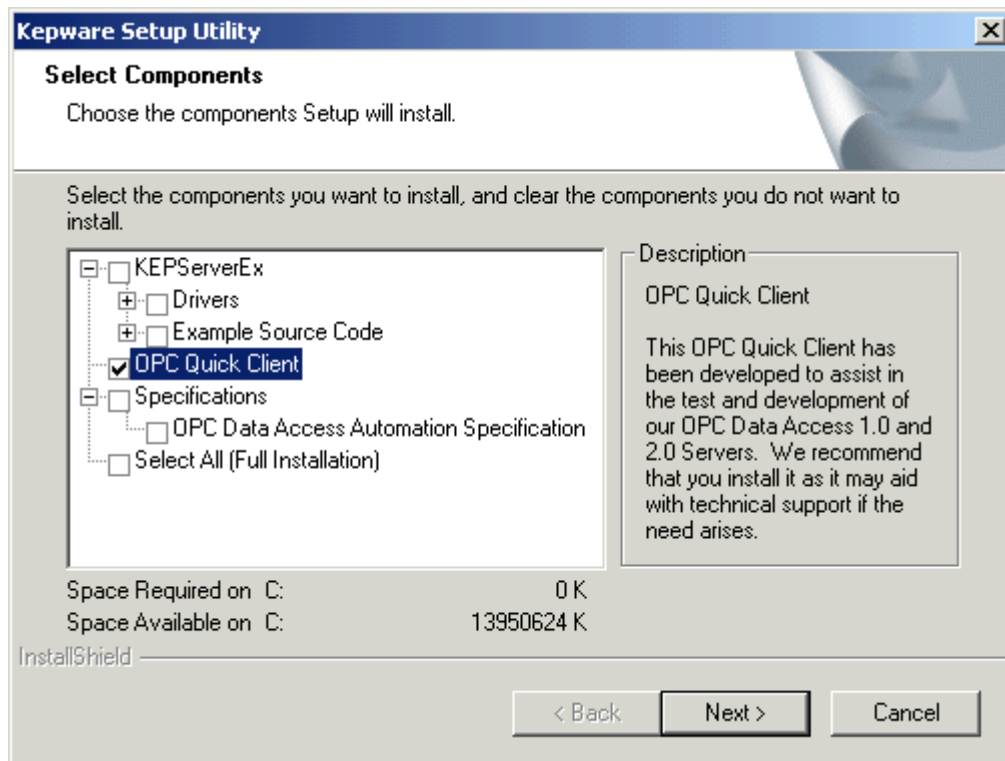
Using the Install Program to Register the Server

You may also use the server installation program to make the appropriate registry entries, and to ensure that all of the files needed to make a remote connection are present.

1. On the remote PC run the KEPServerEX Install program.



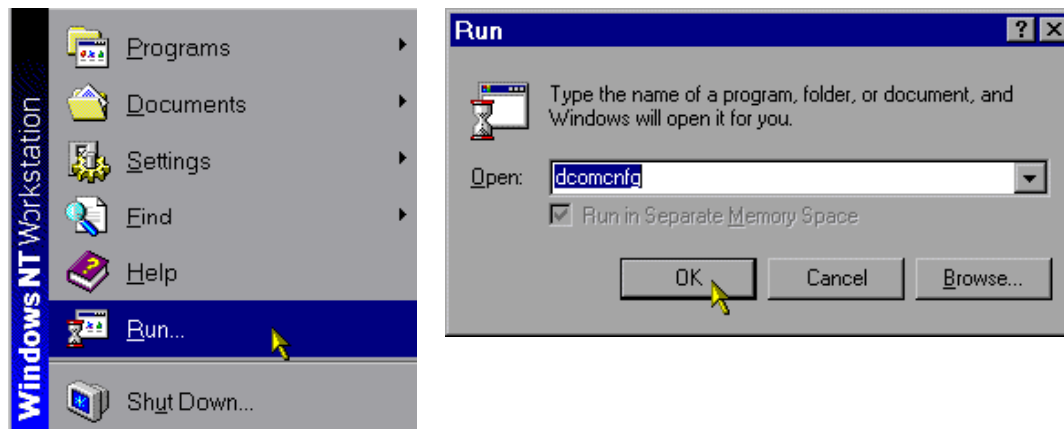
2. At the component selection page, deselect all the components except OPC Quick Client and click **Next** to continue with the install. We recommend installing the OPC Quick client to verify server connections.



Editing the DCOM Configuration

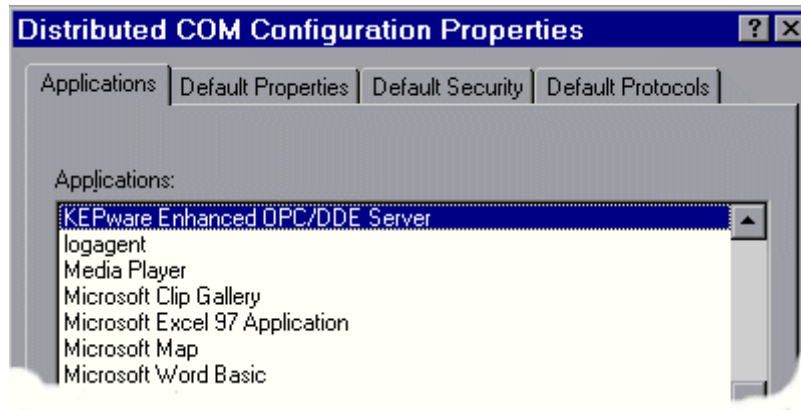
The following steps describe how to configure DCOM for remote, or local, connections to the KEPServerEX.

1. Select the Start button from the Desktop task bar and click **Run** and enter DCOMCNFG.EXE in the pop-up menu and run DCOMCNFG.EXE.



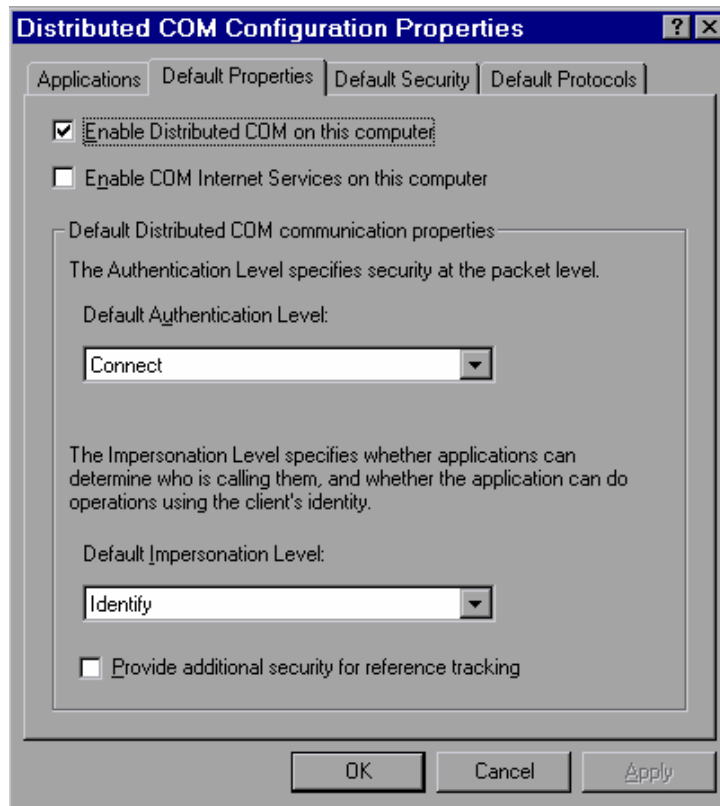
*DCOM Config (known as **DCOMCNFG.EXE**) is a utility that can be used to secure Distributed COM (DCOM) objects that have been created.*

2. A general DCOM configuration window will appear with four tabs. The foremost tab is Applications. All applications that can enable DCOM are listed here. The remaining three tabs are default configuration settings used by the listed applications. Changes made to the settings on these pages affect DCOM applications globally. The goal of these instructions is to allow all network users to access all DCOM applications. After a connection has been proven, the user may then choose individual applications from the list and customize their DCOM security properties for more control.

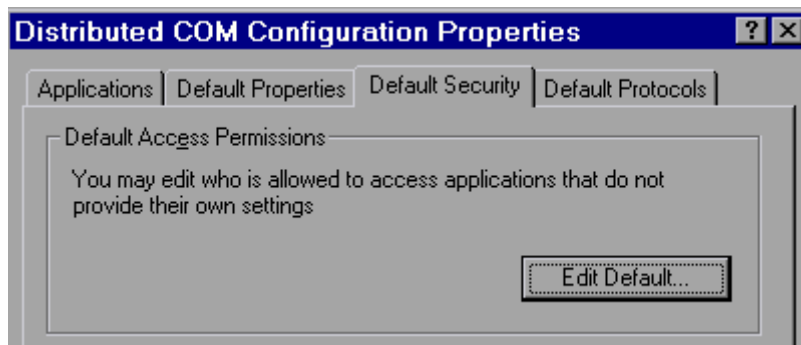


Note: It is very important to make sure that the **Apply** button is selected after changes are made in a DCOM settings page.

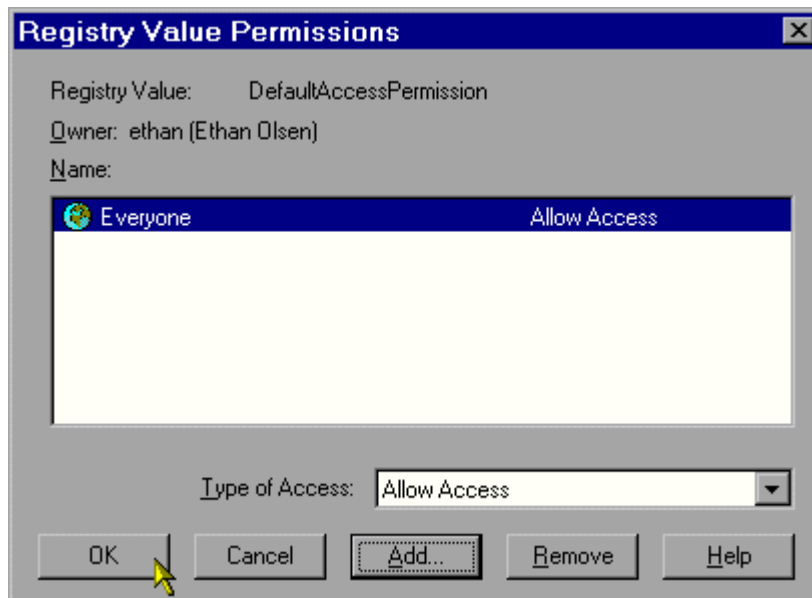
3. Under the Default Properties tab, “Enable Distributed COM on this computer” should be checked. Also, ensure that the “Default Authentication level:” is set to “Connect,” and the “Default Impersonation Level:” is set to “Identify”. Click the **Apply** button to administer the changes



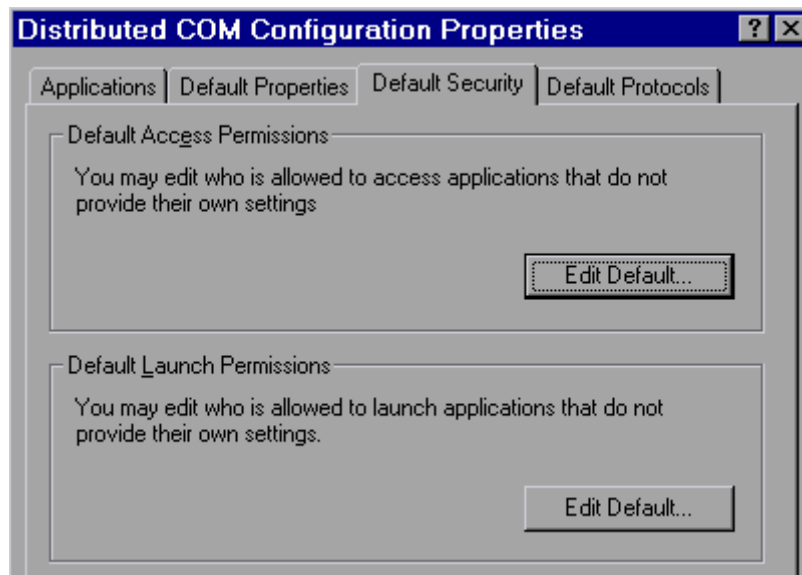
4. Select the Default Security tab and click the **Edit Default** button under “Default Access Permissions.”



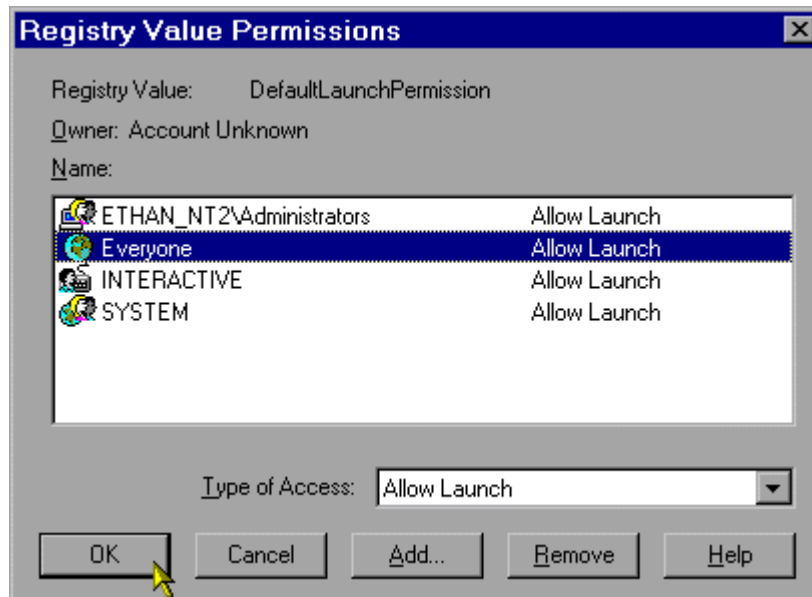
5. Add domain group "Everyone" with "Allow Access" to the permission list, then select **OK**. If you are planning to run the server as a service you will also need to add "System" with "Allow Access".



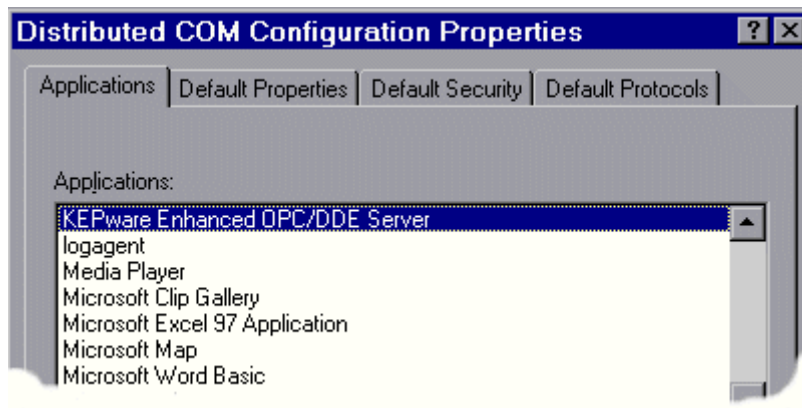
6. Now click the **Edit Default** button under "Default Launch Permissions."



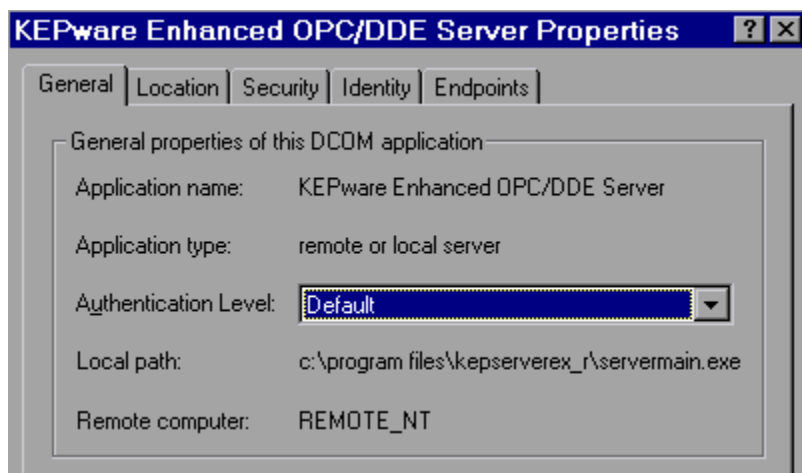
7. Add domain group “Everyone” with “Allow Launch” to the permission list, then select **OK**.



8. Choose the Applications tab and double-click on “KEPware Enhanced OPC/DDE Server”. This will call up the KEPServerEX-specific DCOM properties.



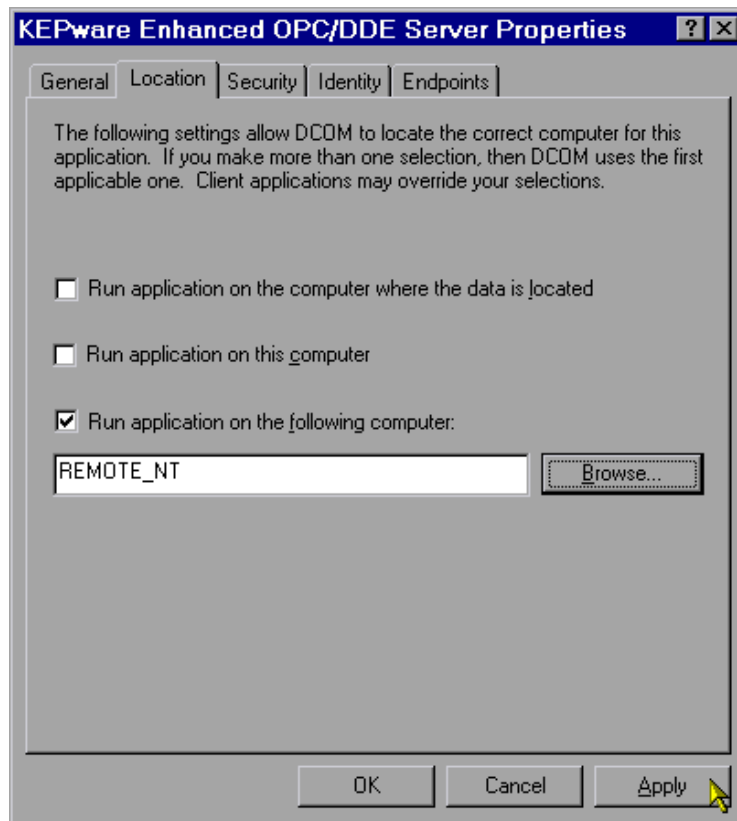
9. In the KEPServerEX-specific DCOM window, choose the Location tab.



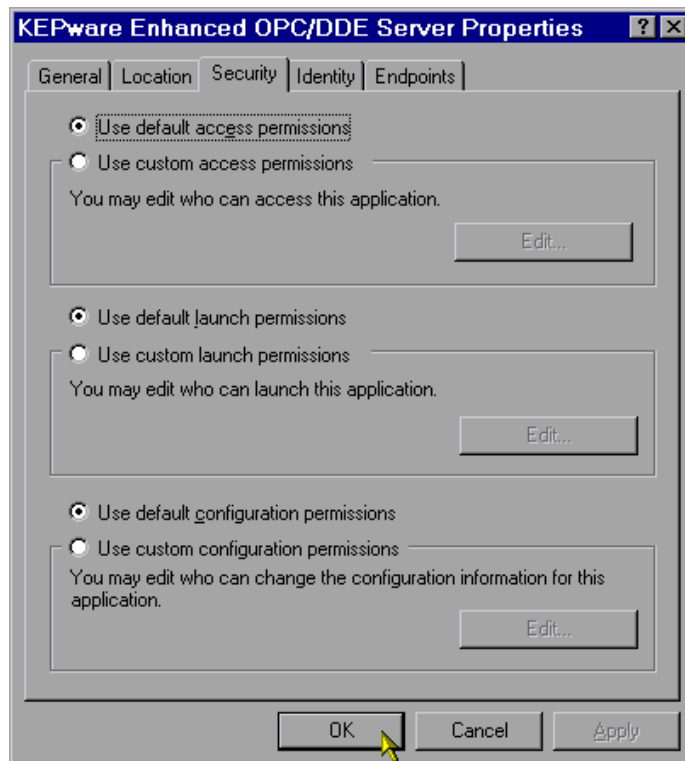
10. Most clients allow connections directly to the remote PC by entering the Name of the PC in the server connection dialog box. For applications that do not allow these types of connections, select “Run application on the following computer”. Next browse for the remote machine that contains the KEPServerEX application and select **Apply**. In this example the machine name is REMOTE_NT. For local connections you will leave “Run application on the computer where the data is located” checked.

Note: See Kepware’s Client Connectivity guide for information on how specific clients connect remotely to KEPServerEX.

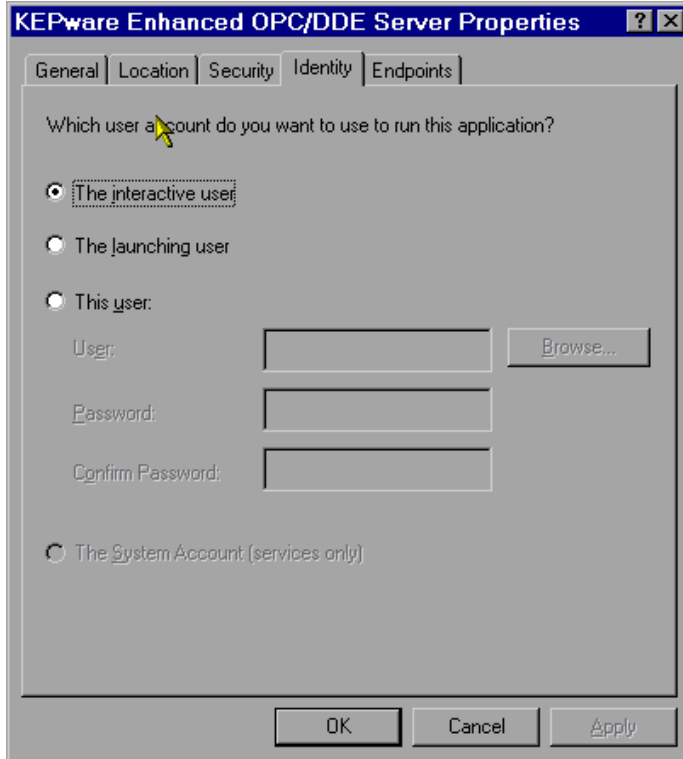
Warning: This dialog box will allow you to select more than one check box. If this happens it produces an error state. You must make sure that only one box is checked.



11. Choose the Security tab and ensure that the radio buttons for the Access permissions are set to default. Apply these changes.



12. The final step is to select the Identity tab from the application specific DCOM pages, and ensure that the “Interactive user” radio button is selected. Then select the **Apply** button. Select **OK** to exit the application specific DCOM window, and then choose **OK** again to exit the general DCOM window



At this point you should be able to connect to the server from the remote PC. If you installed the OPC Quick Client use it as a test and then try the client you are planning to use.

Configuring DCOM for Win XP Domains

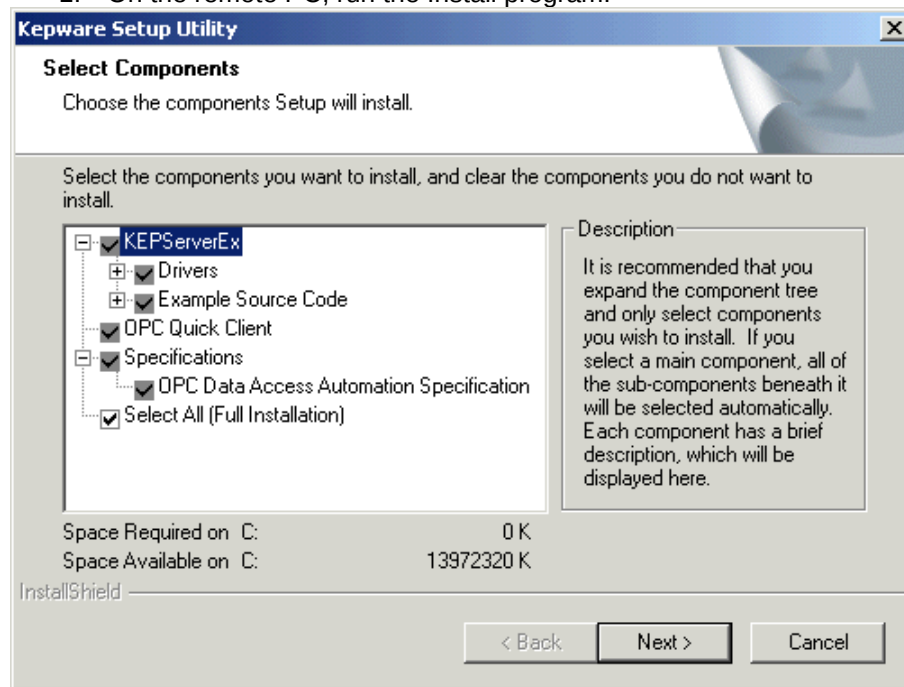
There may be variations in DCOM configuration between local and remote connections to KEPServerEX. Some client applications may not support browsing remote PC's for installed servers. For these clients you may need to add server registry entries to the client PC in order to obtain the proper CLSID for the server. The preferred method for adding the registry entries is running the server installation program and selecting only the OPC Quick Client for installation. If this cannot be done, then you can use the OPC_Remote.Reg file that is provided with the server install. (See [Appendix A](#) for details on how to do this.) If you are using another Operating System see that section for instructions.

The first part of this document will explain the steps required to prepare for DCOM configuration on the remote PC.

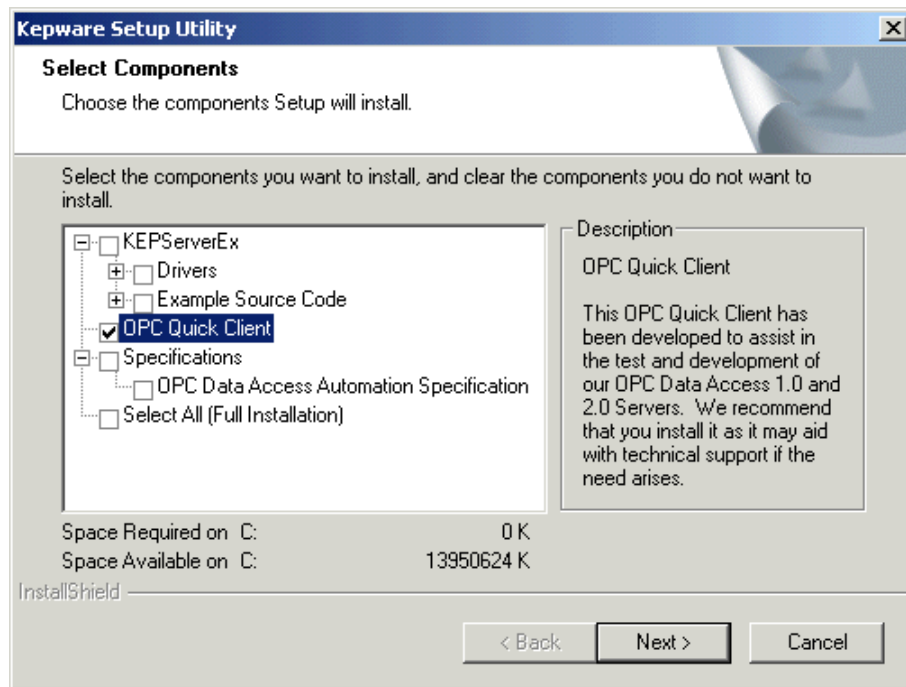
Using the Install Program to Register the Server

You may also use the server installation program to make the appropriate registry entries and to ensure that all of the files needed to make a remote connection are present.

1. On the remote PC, run the Install program.



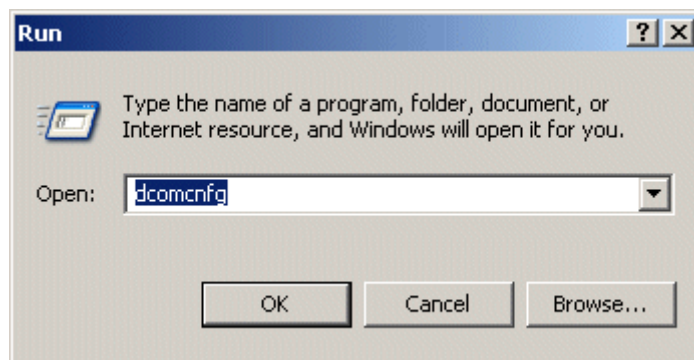
2. At the component selection page, deselect all the components except for OPC Quick Client, and click **Next** to continue with the install. We recommend installing the OPC Quick client to verify server connections.



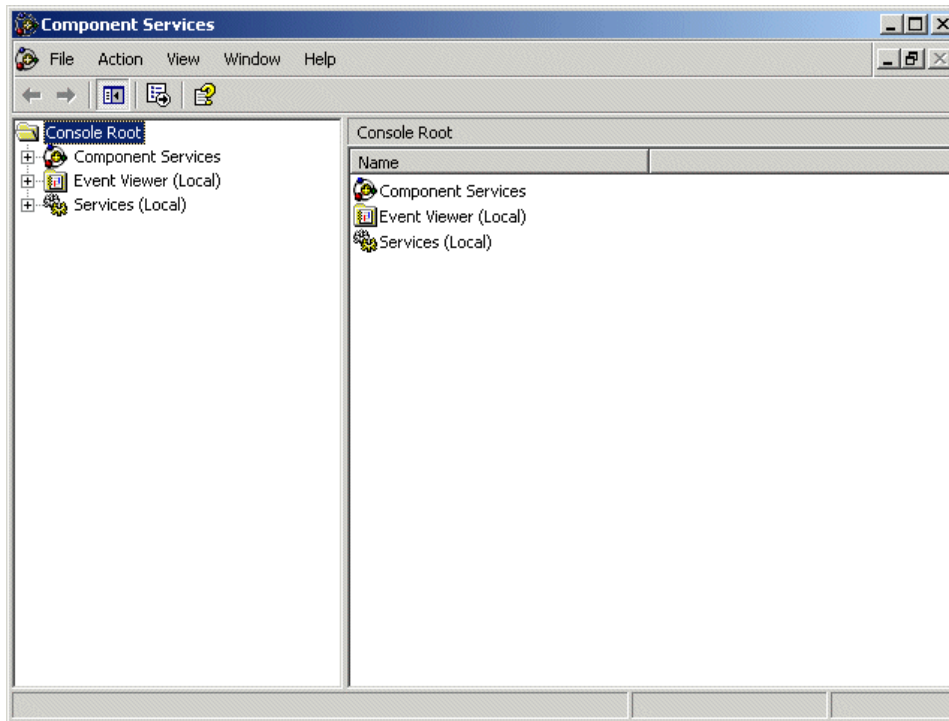
Running the DCOM Configuration Utility

Starting Windows Components like DCOM Configuration on Windows XP is slightly different in comparison to Windows NT, or Windows 2000.

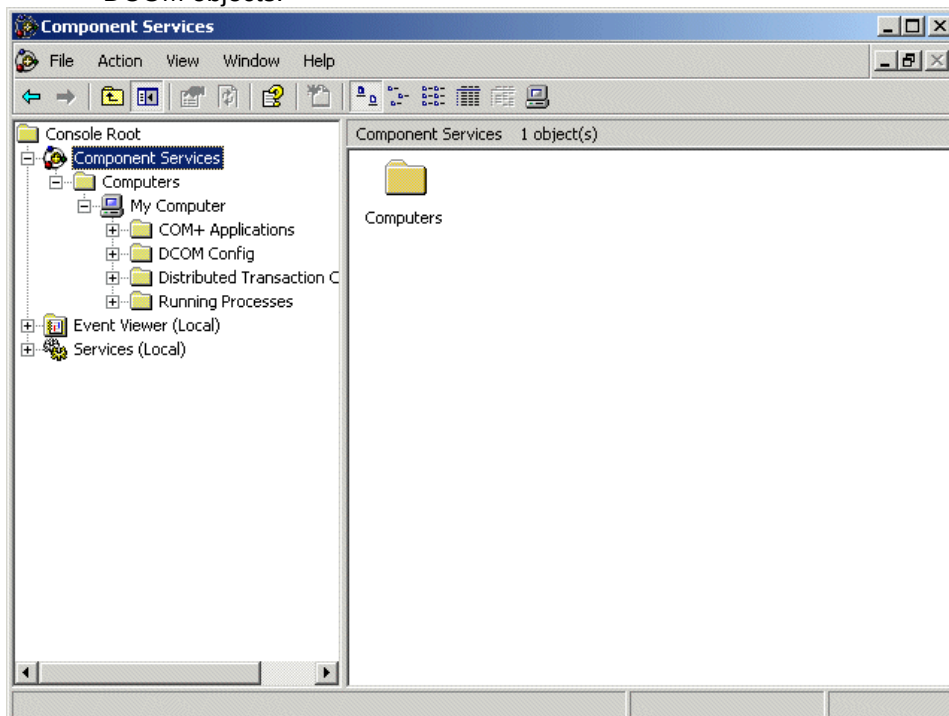
1. Type DCOMCNFG in the Start Menu / Run dialog to launch DCOM Properties (XP launches Component Services, DCOM Properties are located here).



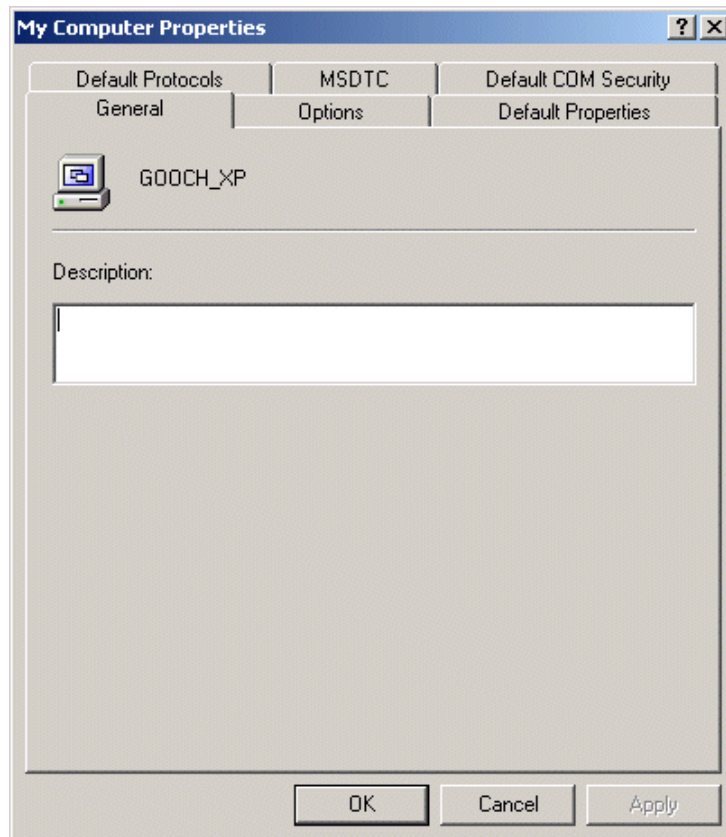
2. Component Services is the home page of the DCOMCNFG run command.



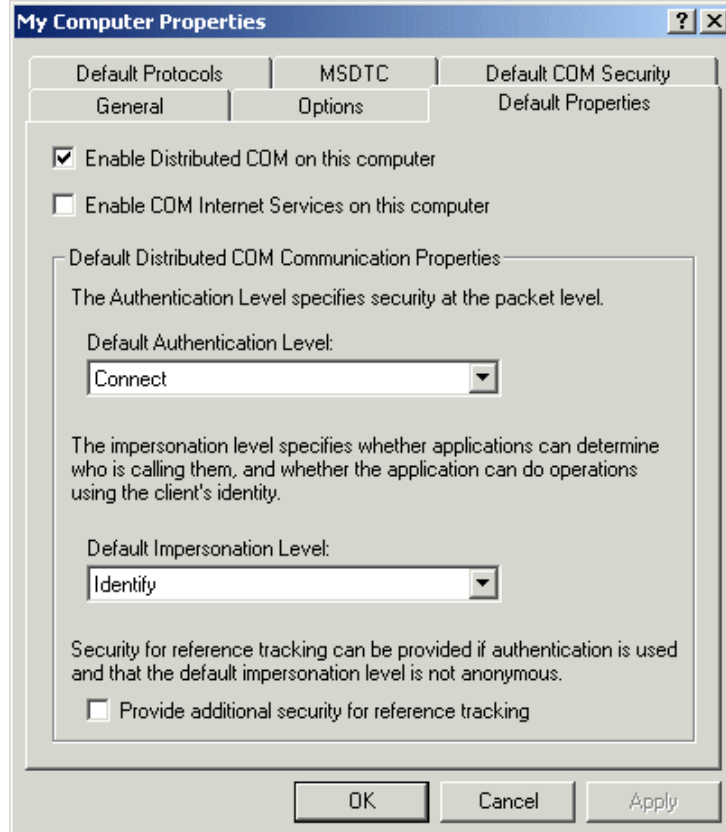
3. Click the Plus sign next to Component Services, Computers, and My Computer to expand the branches of the directory tree. This page shows My Computer (Used for accessing Default DCOM Properties), and the folder which contains all the DCOM objects.



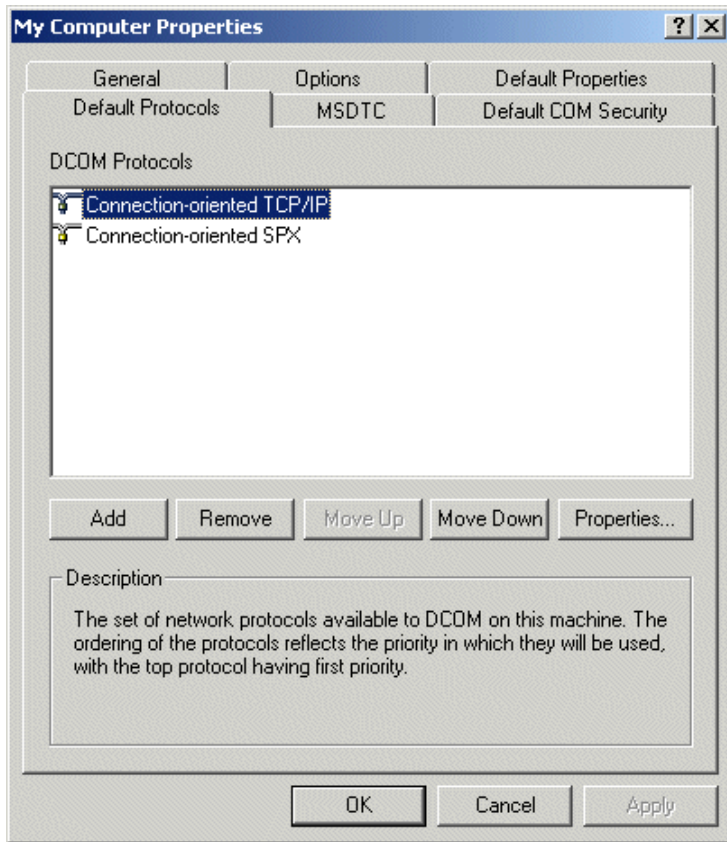
4. Right-click My Computer on the Component Services page and select Properties. It will bring you to the General tab of the DCOM properties for this PC.



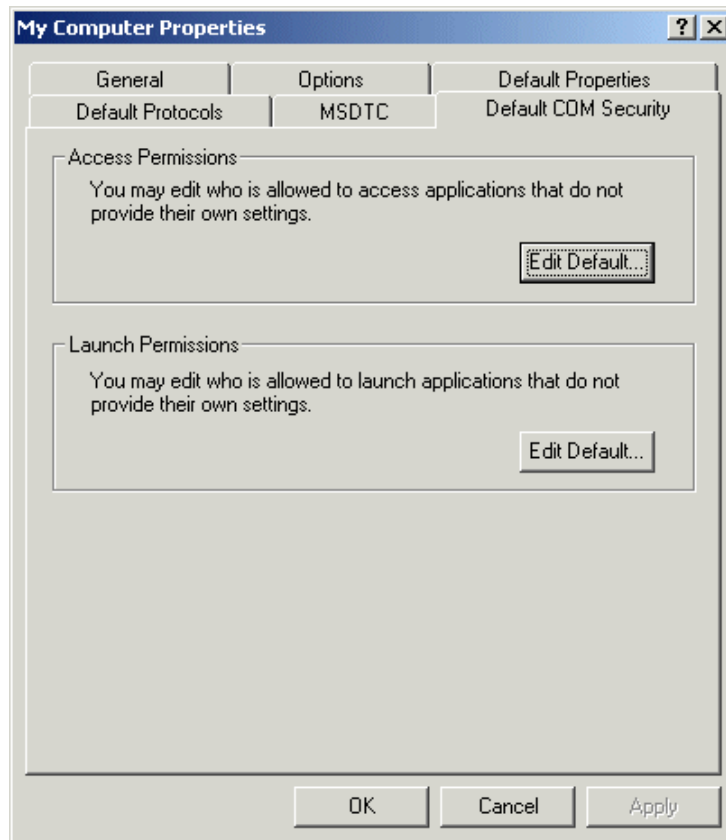
5. Select the Default Properties tab. Verify that "Enable Distributed COM on this computer" is checked. The "Default Authentication Level" should be set to Connect, and the "Default Impersonation Level" should be set to Identify.



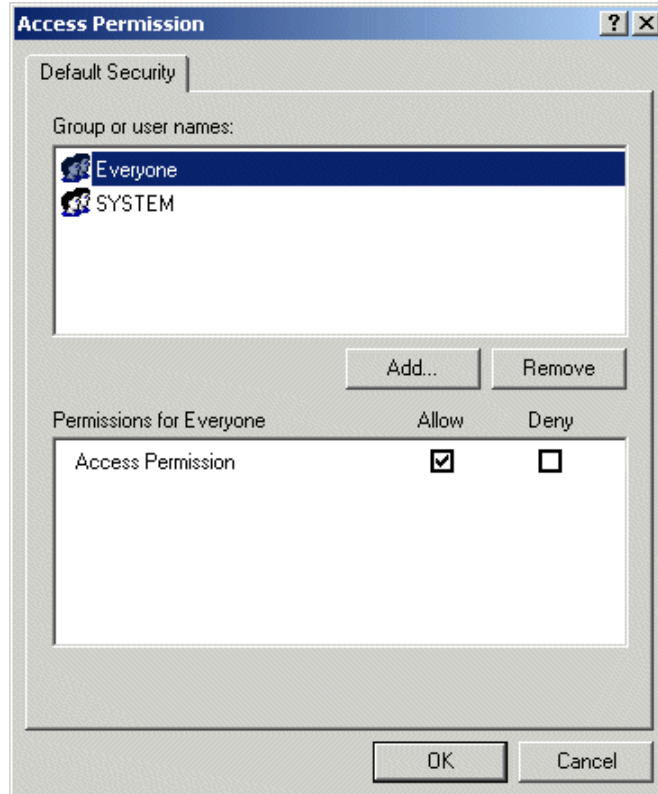
- Next, select the Default Protocols tab. On this tab you should see the data transfer protocols that are currently selected for this PC. You can add additional protocols from here if needed.



- Select the Default COM Security tab and click the **Edit Default** button under "Access Permissions."



8. You may see Groups and Users listed for the Default Access Permissions. You will need to add them by clicking on the **Add** button.



9. Once the Users, or Groups, window is open, click the **Advanced** button.

Select Users or Groups [?] [X]

Select this object type:
 Users, Groups, or Built-in security principals Object Types...

From this location:
 KEPDOMAIN Locations...

Enter the object names to select (examples):
 Check Names

Advanced... OK Cancel

10. Enter your search criteria and click Find Now to list all of the Users and Groups that meet your selection criteria.

Select Users or Groups [?] [X]

Select this object type:
 Users, Groups, or Built-in security principals Object Types...

From this location:
 KEPDOMAIN Locations...

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts
☐ Non expiring password

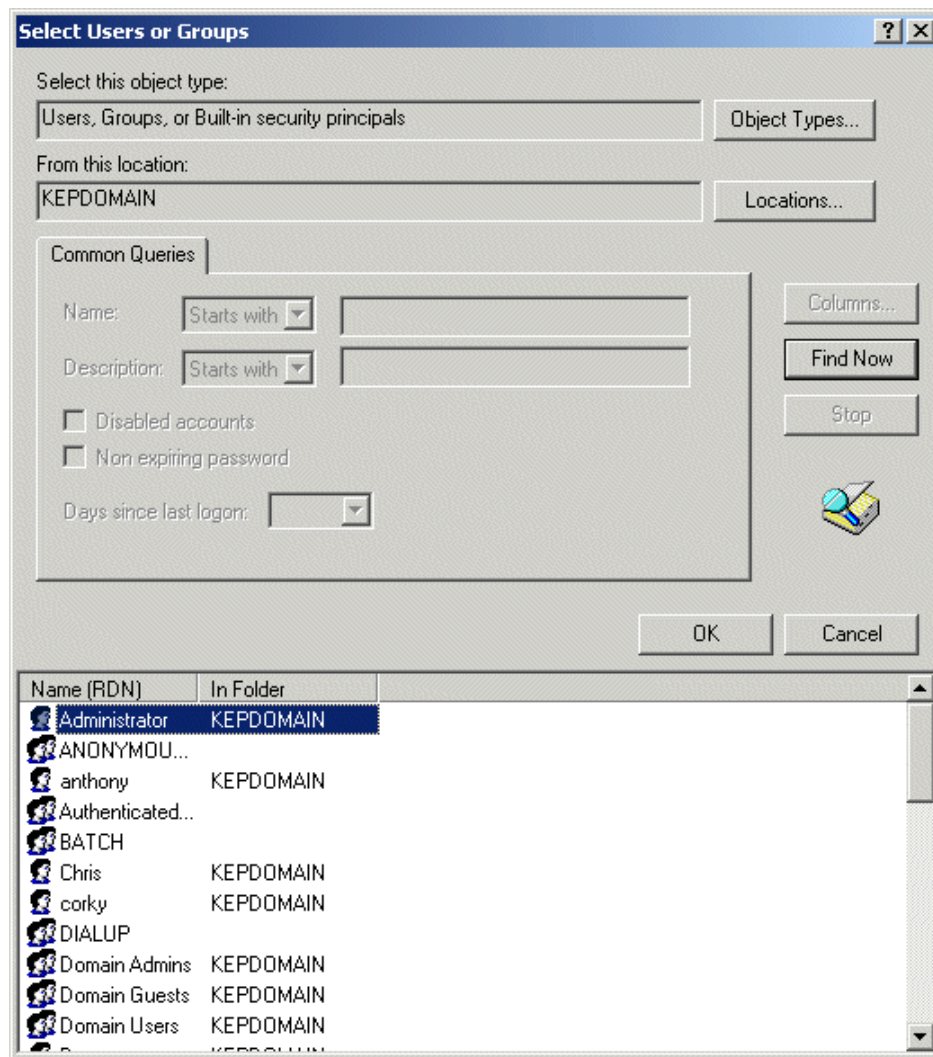
Days since last logon:

Columns... Find Now Stop

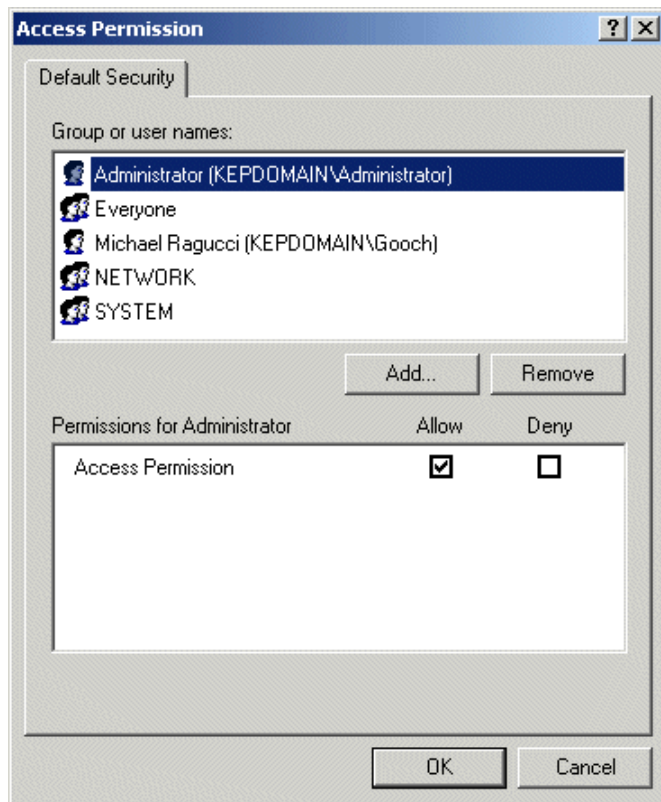
OK Cancel

Name (RDN)	In Folder

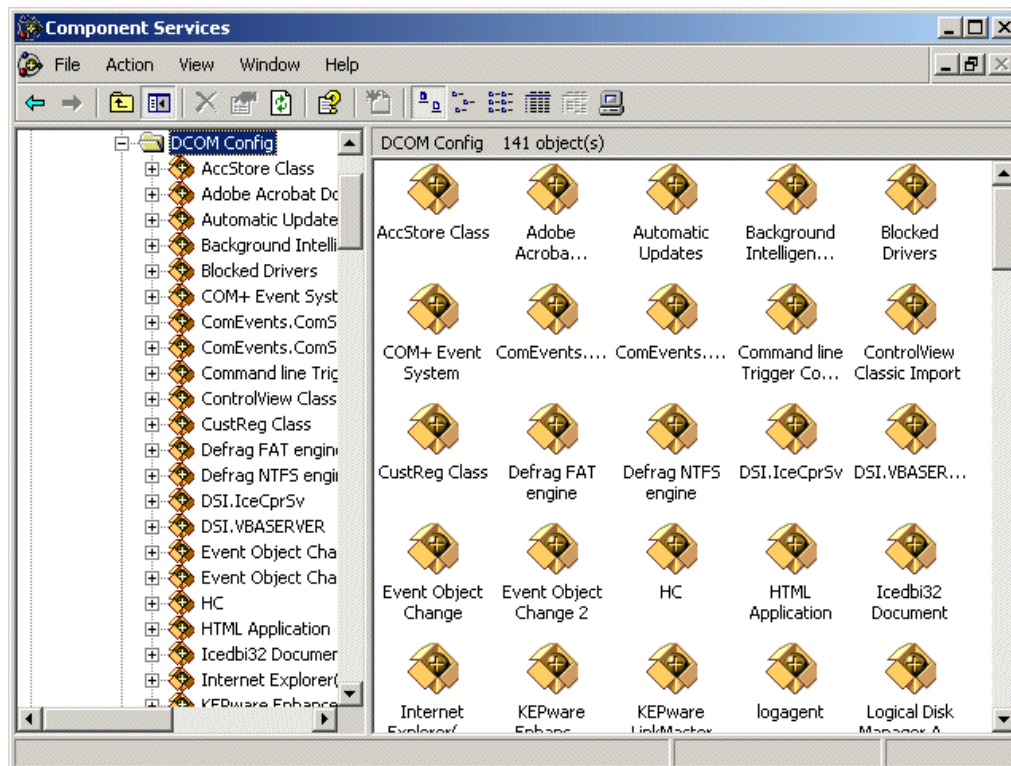
11. From the list, select the users or groups that you wish to add and click **OK**.



12. You will have to add Everyone and System, like you did with the other Operating Systems. In addition, you have to add Network in Windows XP Operating Systems.

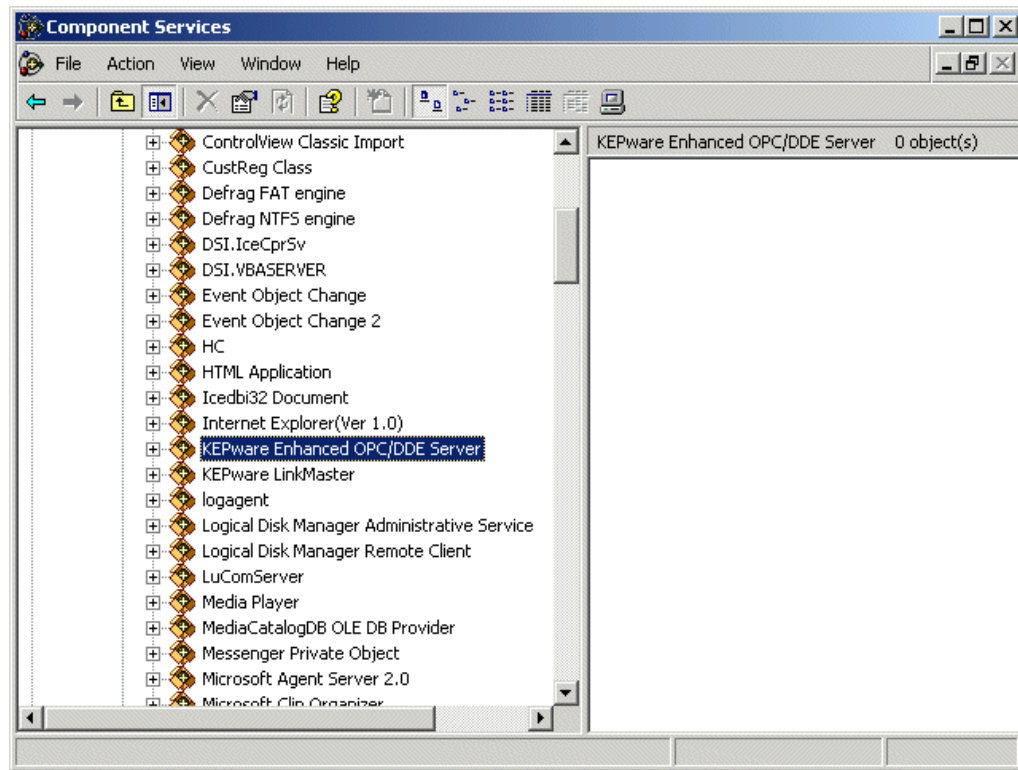


13. Click **OK** when you are done with Access Permissions and repeat the same process with Launch Permissions.
14. Next, select and expand the DCOM Config folder in the directory tree.

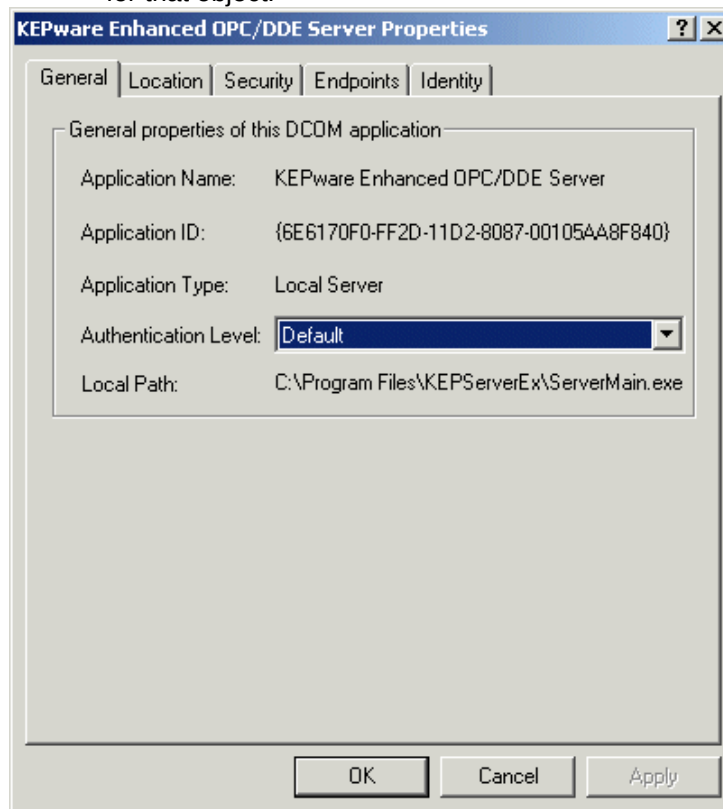


15. Scroll down the list of applications that support DCOM until you see the "Kepware Enhanced OPC/DDE Server".

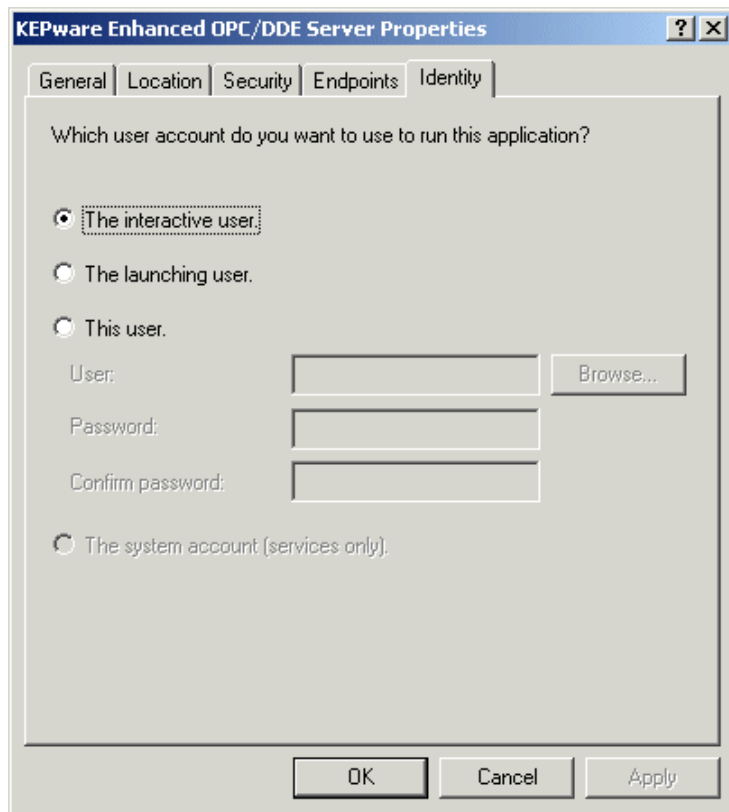
16. Right click on the server object and select Properties.



17. Right clicking on a DCOM object opens the General tab of the Property window for that object.

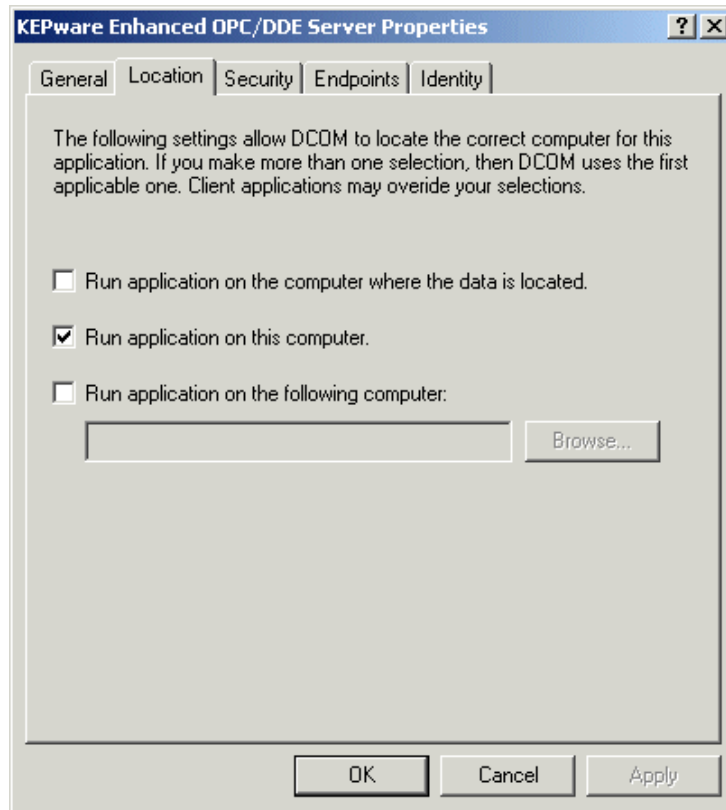


18. Select the Identity tab. The Identity should be set to "The interactive user."

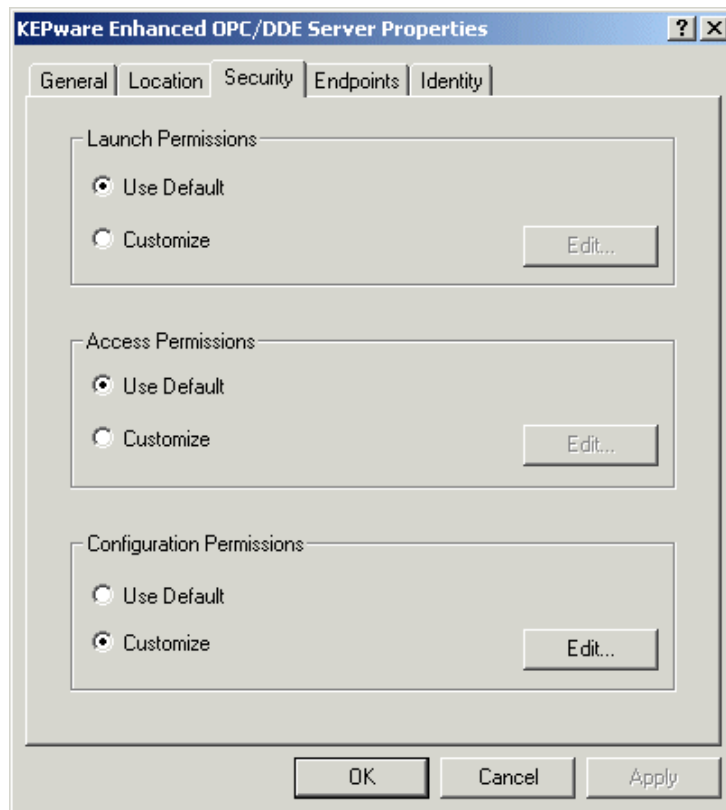


19. Select the Location tab. For local software client connections you will select "Run application on this computer." You will make the same selection if you are connecting the client software to a mix of multiple remote, or multiple remote and local, servers. If you want to limit the software client connections to only one remote server location, select "Run this application on the following computer," and enter, or browse for the PC the remote server is running on.

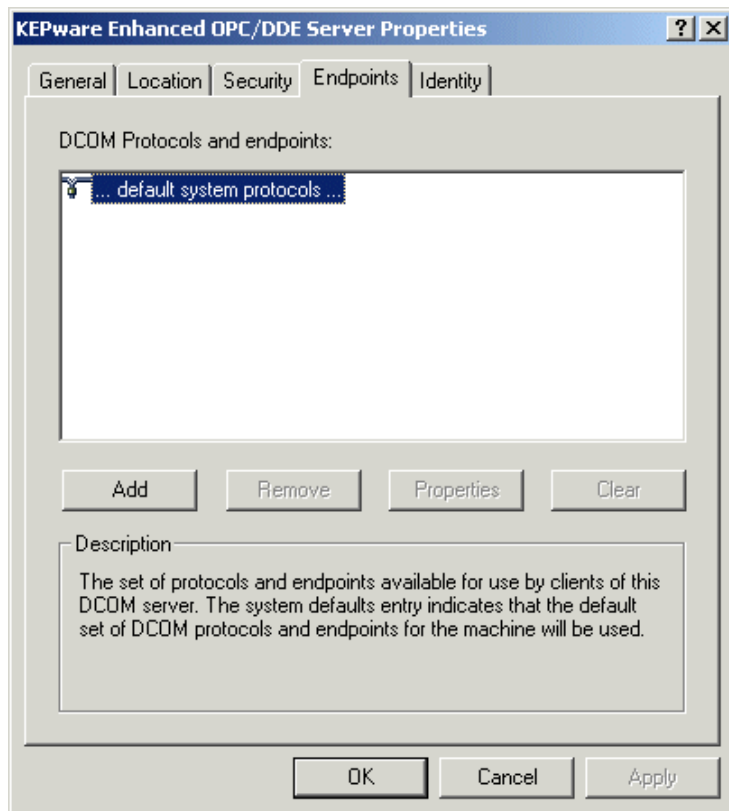
Warning: This dialog box will allow you to select more than one check box. If this happens it produces an error state. You must make sure that only one box is checked.



20. Select the Security tab. Launch and Access Permissions should be set to “Use Default” and Configuration Permissions should be set to “Customize.”



21. Select the Endpoints tab. This should be set to use the “default system protocols.”



22. Click **OK** to save the DCOM settings.

At this point you should be able to connect to the server from the remote PC. If you installed the OPC Quick Client test the DCOM settings with it, then try the client you are planning to use.

Configuring DCOM for Windows XP SP2 / Windows 2003 Server SP1

Introduction

The major goal of Windows XP Service Pack 2 (SP2) and Windows 2003 Server Service Pack 1 (SP1) is to reduce common available scenarios for malicious attack on Windows XP. This is done by improvement in shielding Windows XP and 2003 Server from the network, enhanced memory protection, safer handling of e-mail, and Internet Explorer security enhancements.

Most OPC clients and servers use DCOM to communicate over the network. When XP SP2 and 2003 Server SP1 are installed in their default configuration, OPC communication via DCOM will cease to work. This paper describes the settings necessary to restore OPC communications when using XP SP2, and 2003 Server SP1.

Two of the SP2/SP1 security enhancements directly impact OPC over DCOM. First, DCOM limit settings have been added. Secondly, the Windows firewall has been enhanced, and is turned on by default.

Since the callback method used by OPC essentially turns the OPC client into a DCOM server and the OPC server into a DCOM client, the instructions provided here must be followed on all nodes that contain OPC servers or clients.

Note: OPC communication that is confined to a single machine, using COM but not DCOM, will continue to function normally after the installation of XP SP2 / 2003 Server SP1 without following the instructions contained in this document.

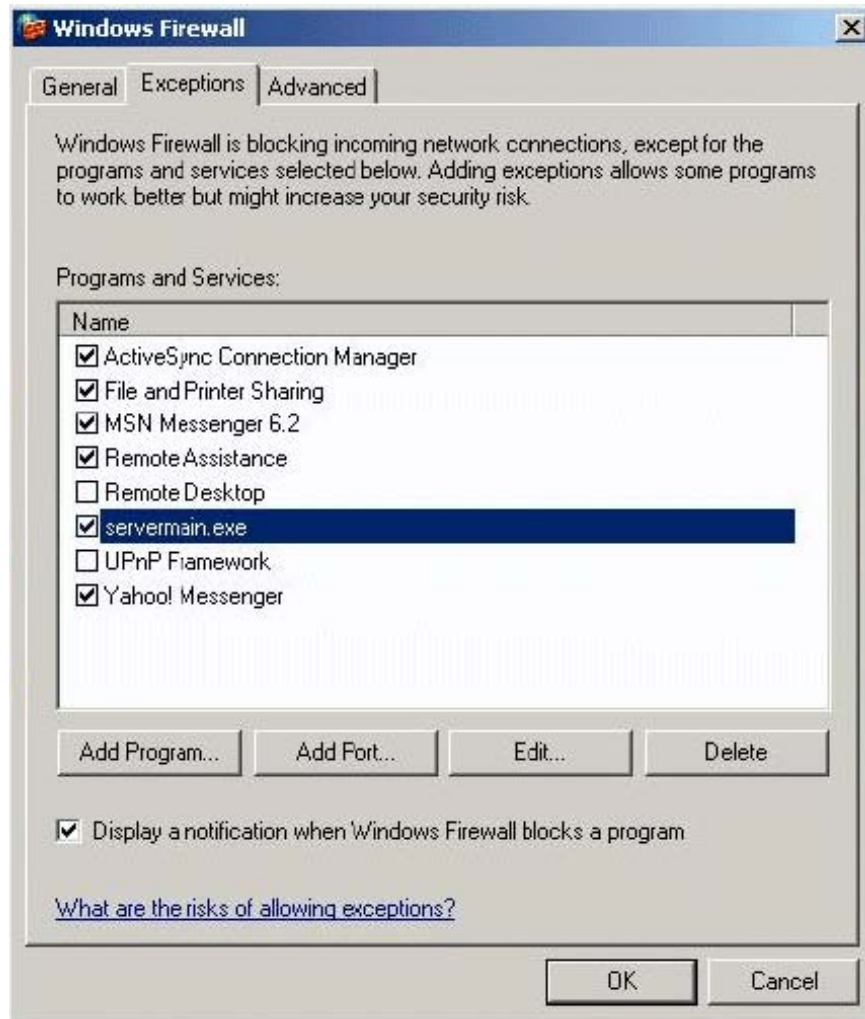
Windows Firewall

The Windows Firewall allows traffic across the network interface when initiated locally, but by default stops any incoming “unsolicited” traffic. However, this firewall is “exception” based, meaning that the administrator can specify applications and ports that are exceptions to the rule and can respond to unsolicited requests.

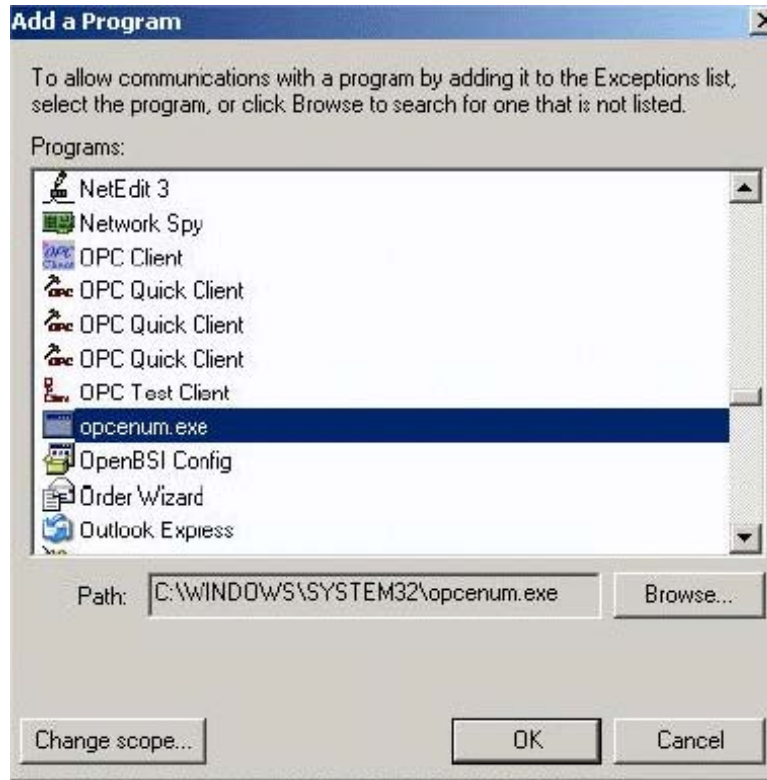
The firewall exceptions can be specified at two main levels, the application level and the port and protocol level. The application level is where you specify which applications are able to respond to unsolicited requests and the port and protocol level is where you can specify the firewall to allow or disallow traffic on a specific port for either TCP or UDP traffic. To make KEPServerEX work via DCOM, changes need to be made on both levels.

Configuring the Firewall

1. By default, the Windows firewall is set to “On”. This setting is recommended by Microsoft and by OPC to give your machine the highest possible protection. For troubleshooting, you may wish to temporarily turn off the firewall to prove or disprove that the firewall configuration is the source of any communication failure.



2. The Windows Firewall can be opened by clicking on the Firewall icon in the Windows Control Panel. Once opened, select the “Exceptions” tab and add all OPC Clients and Servers to the exception list. Also add Microsoft Management Console (mmc.exe found in the Windows\System32 directory) and the OPC utility OPCEnum (opcenum.exe found in the Windows\System32 directory). These last two files may not appear in the Add a Program list and will have to be found by using the Browse button. Lastly you need to ensure that File and Printer Sharing is checked. This is not typically enabled on new installations of the Operating System.



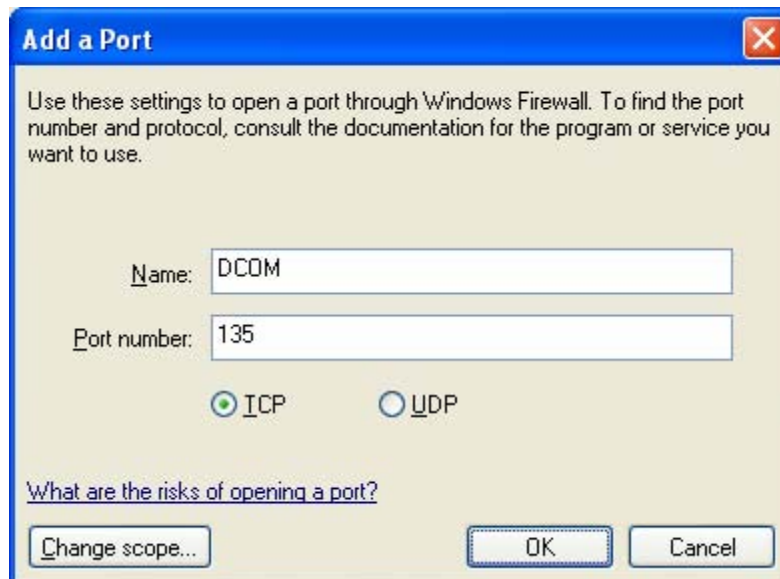
3. Add TCP port 135 as it is needed to initiate DCOM communications, and allow for incoming echo requests. In the Exceptions tab of the Windows Firewall, click on Add Port.

In the Add a Port dialog, fill out the fields as follows:

Name: DCOM

Port number: 135

Choose the TCP Radio Button



DCOM Enhancements

Service Pack 2 for Windows XP/ Windows 2003 Server Service Pack 1 has also made some security enhancements to DCOM; two in particular need to be taken into consideration when using OPC on a network: First, the default Launch and Access permissions dialogs have been modified to allow the user to configure “limits” on the permissions given to applications using DCOM. Secondly, for each user now defined in the Launch and Access permissions, both local and remote access can be explicitly defined.

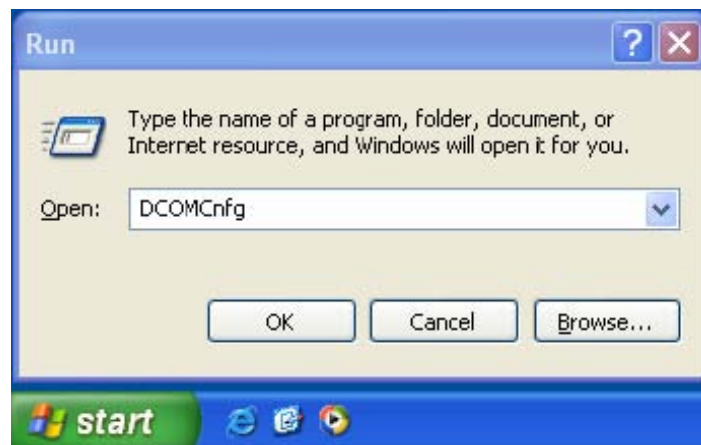
A brief background on default Launch and Access permissions in DCOM: Launch permissions define who can launch a COM based application (such as an OPC server) both over the network or locally. Access permissions define who can access that application once it has been launched. Applications can get their Launch and Access permissions from one of three places: they can use explicitly defined setting for their application, they can use the default permissions or they can set their own permissions programmatically. Because an application could set its own permissions programmatically, the explicitly defined or default settings, although set properly, may not be used and therefore the user is not able to explicitly have control over these settings. To overcome this security flaw, Microsoft has added “limits” to the DCOM security settings from Launch and Access to limit the permissions that an application can use. This limit prevents the application from using permissions beyond what is specified in the DCOM configuration settings. By default the limits set by Service Pack 2 / Service Pack 1 will not allow for OPC communications over the network.

In addition to the new permissions limits, one must now specify if the user or group specified has permissions locally or remotely (or both). In order for OPC applications to work over the network with DCOM, the permissions must be set such that remote users can launch and/or access the OPC servers and clients on the machine.

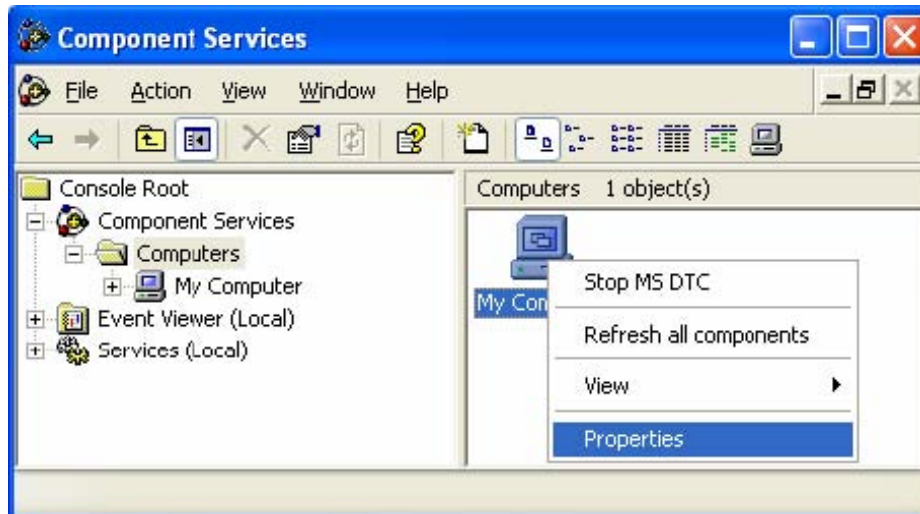
Configuring DCOM

Follow these steps to configure DCOM for KEPServerEX Communications using Windows XP Service Pack 2 / Windows 2003 Server Service Pack 1:

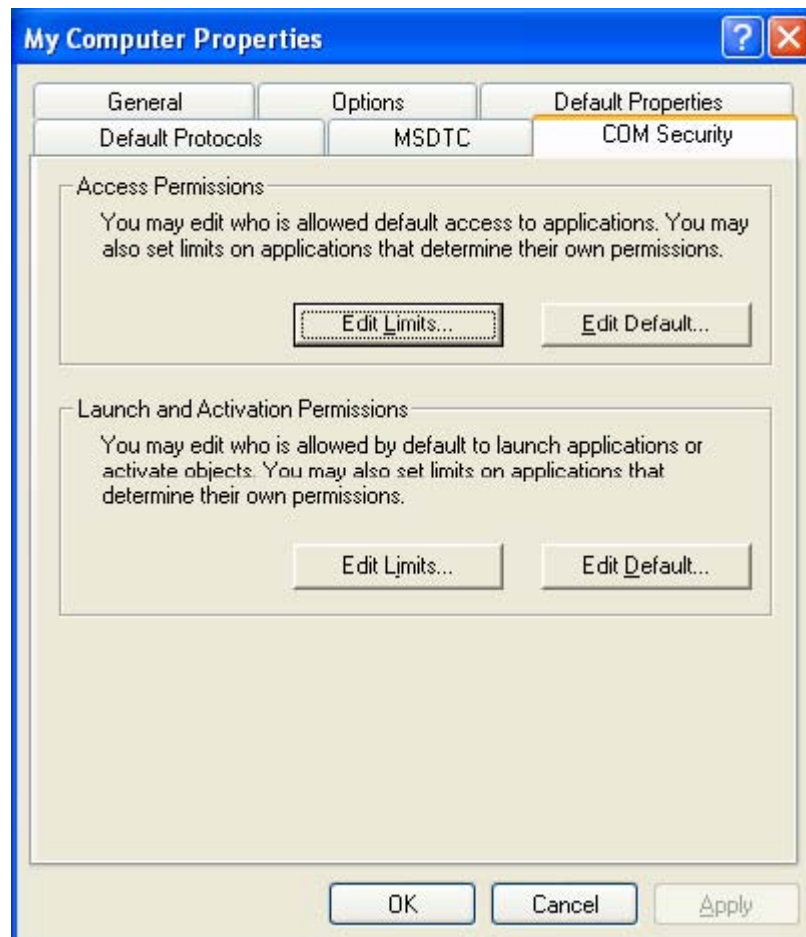
1. Go to Start -> Run and type DCOMCnfg and click on **OK**.



2. Click on Component Services under the Console Root to expand it.
3. Click on Computers under Component Services to expand it.
4. Right-click on My Computer in the pane on the right, and select Properties



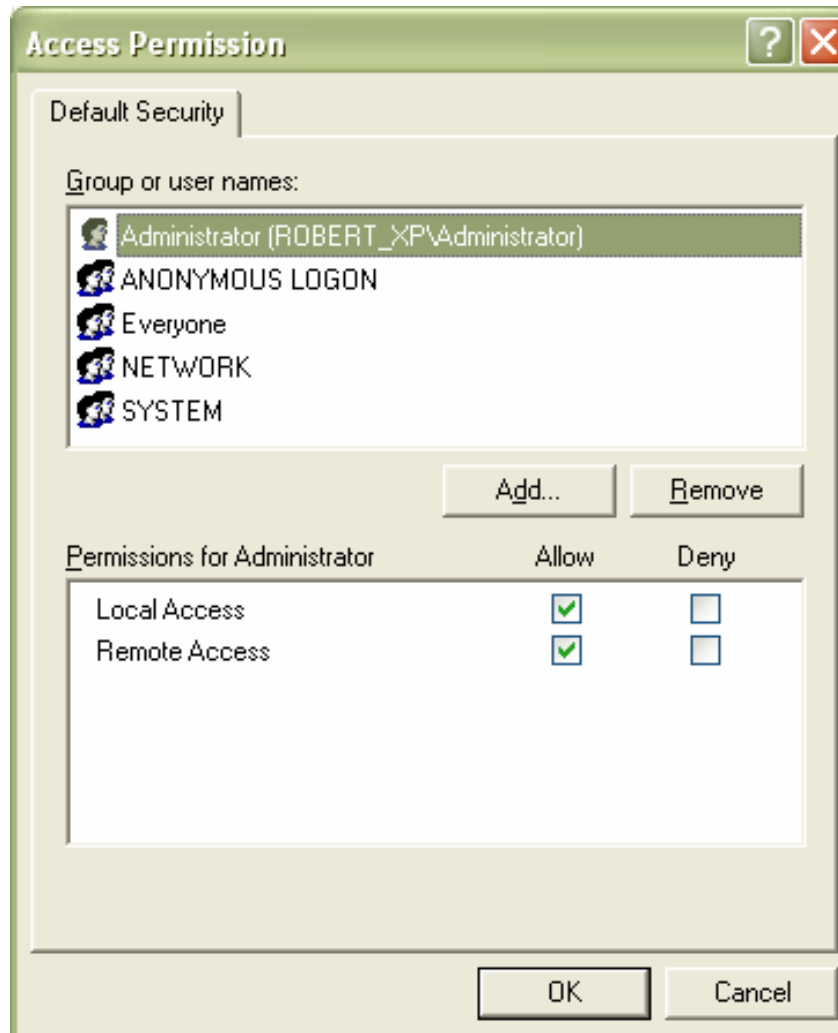
5. Go to the COM Security tab. Note these are the four permission configurations that we will have to edit:



6. Edit the Limits for Access and Launch

Access Permissions – Edit Limits...

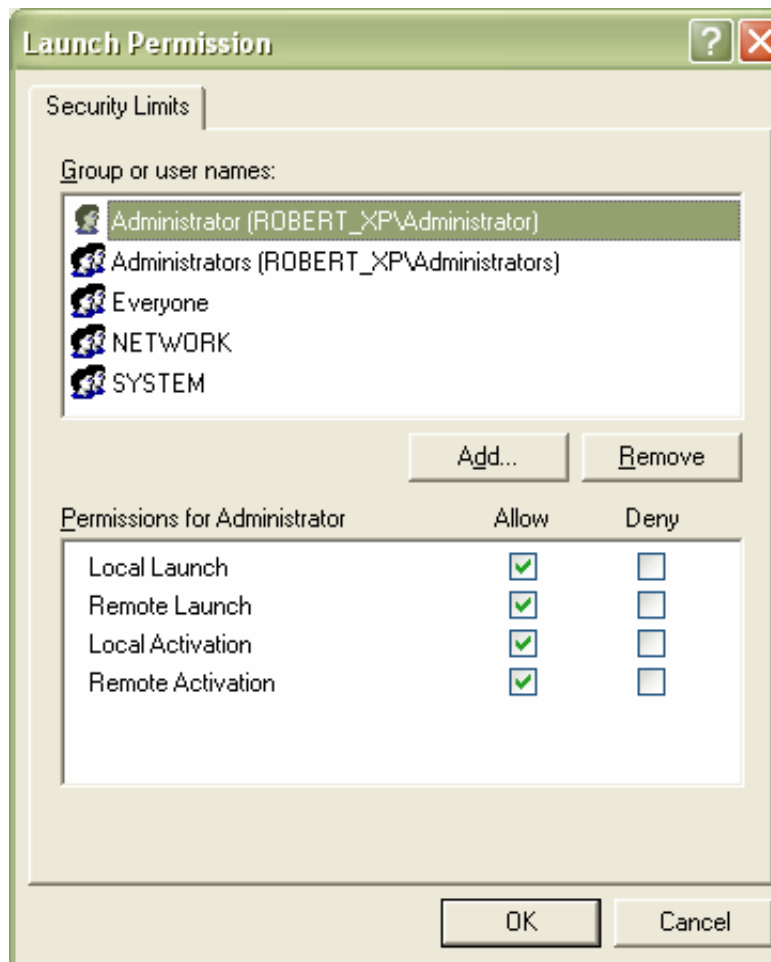
You need to check the Remote Access box for the user labeled ANONYMOUS LOGIN in this dialog. This is necessary for OPC Enum to function.



Launch and Activation Permissions – Edit Limits...

You need to check the remote boxes for the users labeled Everyone in this dialog.

Note: Since Everyone includes all authenticated users, it is often desirable to add these permissions to a smaller subset of users. One suggested way to accomplish this is to create a group named "KEPServerEX Users" and add all user accounts to this group which will execute KEPServerEX or your OPC Client, then substitute "KEPServerEX Users" everywhere that Everyone appears in these configuration dialogs.



7. Edit Default Permissions for Access and Launch

For each user (or group) that participates in OPC communication (e.g. "KEPServerEX Users"), make sure that both the Local Allow and Remote Allow checkboxes are both checked. If the User accounts or Group accounts do not appear then you will need to add them and then check permissions as we did with Everyone in the following figures.

Access Permissions per user

Permissions for Everyone	Allow	Deny
Local Access	☒	☐
Remote Access	☒	☐

Launch and Activation permissions per user

Permissions for Everyone	Allow	Deny
Local Launch	☒	☐
Remote Launch	☒	☐
Local Activation	☒	☐
Remote Activation	☒	☐

8. Reboot the PC when you have completed making the changes to DCOM.

References

Information used in preparing this document was provided by the OPC Foundation White Paper entitled "Using OPC via DCOM with Microsoft Windows XP Service Pack 2."

Summary

Although this document is written for KEPServerEX, the DCOM settings specified apply to all Kepware OPC server products including LinkMaster, U-CON Protocol Server, and iSNMP OPC Server. If you have any additional questions please contact Kepware Technical Support.

Configuring DCOM on Workgroups Vs. Domains

Although most projects will be done on Network Domains, there are still many places that continue to use Workgroups for their networks, or may even have mixed configurations. Unfortunately DCOM is really designed for Domains. Remote connectivity using Workgroups will require some extra configuration of the security settings. DCOM security will let a client or server application know whether the User who is running the server (or client application) is a secure DCOM user. If one, or the other, is not a user, you will not establish a connection to the server. This generally manifests itself with failed connection errors.

The primary difference between a Network Domain and a Network Workgroup is the way that security is handled. Domains have a central Access Control List (ACL). The act of logging on to the Domain provides centralized user permissions which are applied to all PCs on the domain. In Workgroups the ACL is maintained by each PC. That means that you have to add every user to every PC.

The following are known configurations for Workgroups, and the steps you will need to do to get remote connectivity working on them.

Connecting Workgroup to Workgroup

When connecting a server from one workgroup PC to another you will need the same user names, and security settings on both PCs.

Note: To launch the server you have to be an administrator. Many people using NT or higher operating systems choose to run the server as a service to avoid creating administrator accounts for all users.

Connecting Workgroup to Domain

When connecting from a workgroup to a domain, you need to verify that the client application located on the Workgroup PC is set to accept responses sent from the server located on the Domain PC. This means you must add any user that could be running the server on the Domain PC to the local security settings. It is ideal to run the server as a service on the Domain to reduce the number of entries you may need. You will also need to make sure the local administrator/login is added to the default security.

Note: To launch the server you have to be an administrator. Many people using NT or higher operating systems choose to run the server as a service to avoid creating administrator accounts for all users.

Connecting Domain to Workgroup

When connecting from a Domain PC to a Workgroup PC, you need to add the name of the Domain user to the Workgroup PCs user list. You will also need to add the Workgroup user who is running the PC to the Domain PCs local user list. On the Workgroup PC, you will set it up like you were connecting from it to the domain.

Note: To launch the server you have to be an administrator. Many people using NT or higher operating systems choose to run the server as a service to avoid creating administrator accounts for all users.

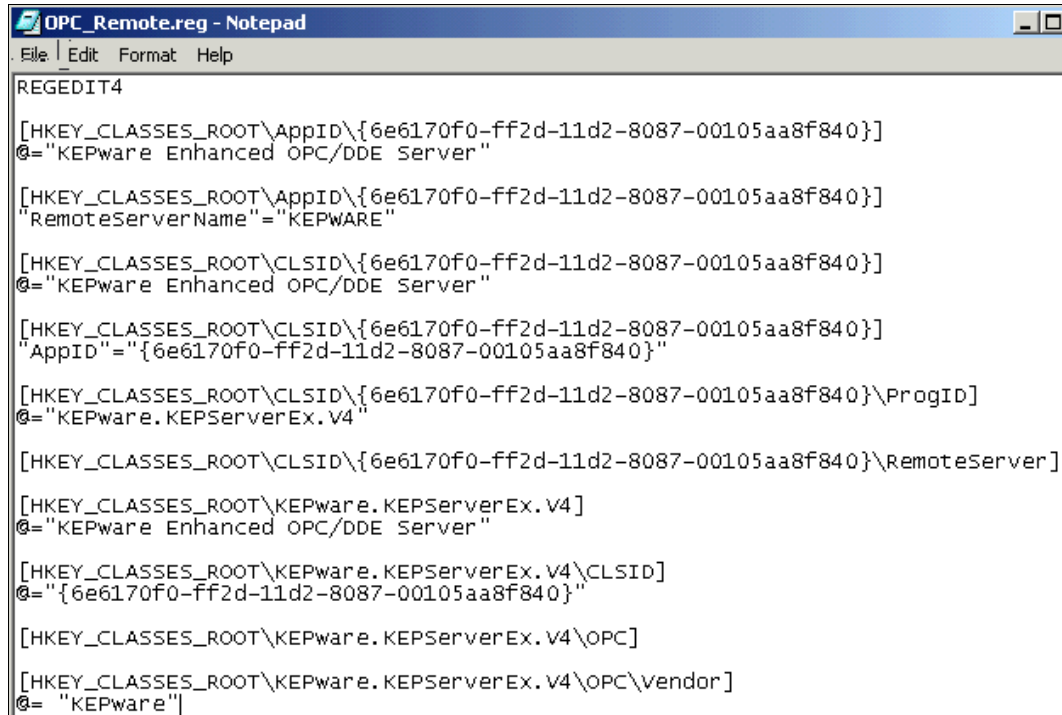
In order to set DCOM Security in a Workgroup, you have to have the PC set for UserLevel Security *not* Share Level Security. If you are on Win 95 or Win 98 you will have to set the security before you install the DCOM patch. If you do not, then you will not be able to run the DCOMConfig.exe program or will get errors when trying to add the security settings.

Appendix A: Using the OPC_Remote.Reg File

Preparing the Remote PC

If the intended *client* machine does not have a registered version of the KEPServerEX on it, you must take the initial step of registering the server on that machine. The following steps explain this procedure.

1. On the KEPServerEX pc, open the server's root directory \KEPServerEX, and find the file called opc_remote.reg. Make a copy of this file and take it to the remote PC.
2. On the intended remote client machine, paste this file on to your C: drive (or any available hard drive on that machine).
3. Right click on this file and choose Edit on the drop down menu.



```
REGEDIT4

[HKEY_CLASSES_ROOT\AppID\{6e6170f0-ff2d-11d2-8087-00105aa8f840}]
@="KEPware Enhanced OPC/DDE Server"

[HKEY_CLASSES_ROOT\AppID\{6e6170f0-ff2d-11d2-8087-00105aa8f840}]
"RemoteServerName"="KEPWARE"

[HKEY_CLASSES_ROOT\CLSID\{6e6170f0-ff2d-11d2-8087-00105aa8f840}]
@="KEPware Enhanced OPC/DDE Server"

[HKEY_CLASSES_ROOT\CLSID\{6e6170f0-ff2d-11d2-8087-00105aa8f840}]
"AppID"="{6e6170f0-ff2d-11d2-8087-00105aa8f840}"

[HKEY_CLASSES_ROOT\CLSID\{6e6170f0-ff2d-11d2-8087-00105aa8f840}\ProgID]
@="KEPware.KEPServerEx.v4"

[HKEY_CLASSES_ROOT\CLSID\{6e6170f0-ff2d-11d2-8087-00105aa8f840}\RemoteServer]

[HKEY_CLASSES_ROOT\KEPware.KEPServerEx.v4]
@="KEPware Enhanced OPC/DDE Server"

[HKEY_CLASSES_ROOT\KEPware.KEPServerEx.v4\CLSID]
@="{6e6170f0-ff2d-11d2-8087-00105aa8f840}"

[HKEY_CLASSES_ROOT\KEPware.KEPServerEx.v4\OPC]

[HKEY_CLASSES_ROOT\KEPware.KEPServerEx.v4\OPC\Vendor]
@="KEPware"
```

4. In the first few lines of this file you should see "RemoteServerName"="KEPWARE". Replace "KEPWARE" with the name of the PC/Machine that is running KEPServerEX.
5. Save the changes to the file and exit.
6. Double click on the file name to register KEPServerEX server. A message box will be displayed on the screen to verify that the information was installed correctly in the registry. The client machine may now be configured to connect via DCOM to the remote server machine.

Note: You may need to place two up-to-date OPC files (from our disc or the OPC foundation) into the C:\Windows\System32 folder. These files are **opccommn_ps.dll** and **opcproxy.dll**. You may have to register them at the DOS command prompt, for example, C:\WINNT\SYSTEM32\regsvr32 opccommn_ps.dll Another way to get these files is to install the server on the remote machine.

Appendix B: Configuring DCOM for Win 95/98 Domains

Note: Effective with release version 4.200.353, KEPServerEx no longer supports operation on workstations running Microsoft Windows 95, Windows 98 and Windows ME operating systems.

There may be variations in DCOM configuration between local and remote connections to KEPServerEX. Some client applications may not support browsing remote PCs for installed servers. For these clients, you may need to add server registry entries to the client PC in order to obtain the proper CLSID for the server. The preferred method for adding the registry entries is running the server installation program and selecting only the OPC Quick Client for installation. If this cannot be done, then you can use the OPC_Remote.Reg file that is provided with the server install (see [Appendix A](#) for details on how to do this). If you are using another Operating System see that section for instructions.

Preparing Win95/98 for DCOM

Windows 95/98 is, by default, set for share-level access control. It must be set for user level.

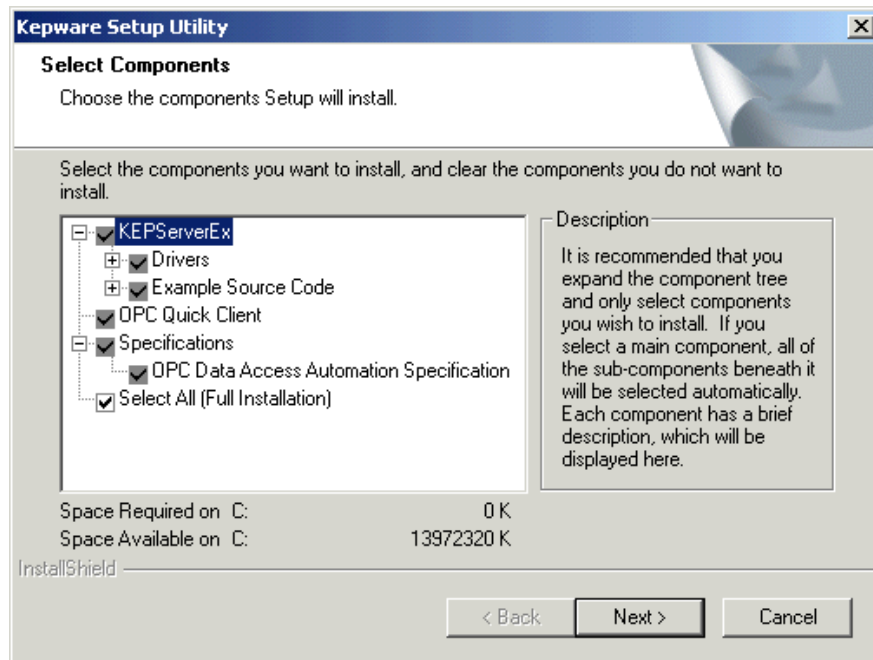
1. Choose Start/Settings/Control Panel.
2. Open the Network applet in the Control Panel, and select the Access Control tab.
3. Select User- Level Access Control and click **OK**.

Before you can use Windows 95/98 DCOM, the machine must be configured to run DCOM applications. This requires a few more steps than you would normally take with the Windows NT or Windows 2000 DCOM setup. Also, unlike Windows NT and Windows 2000, which allow a client to launch a server remotely, it is absolutely necessary for the server component (KEPServerEX) to be running *before* a client can connect to it in Windows 95/98.

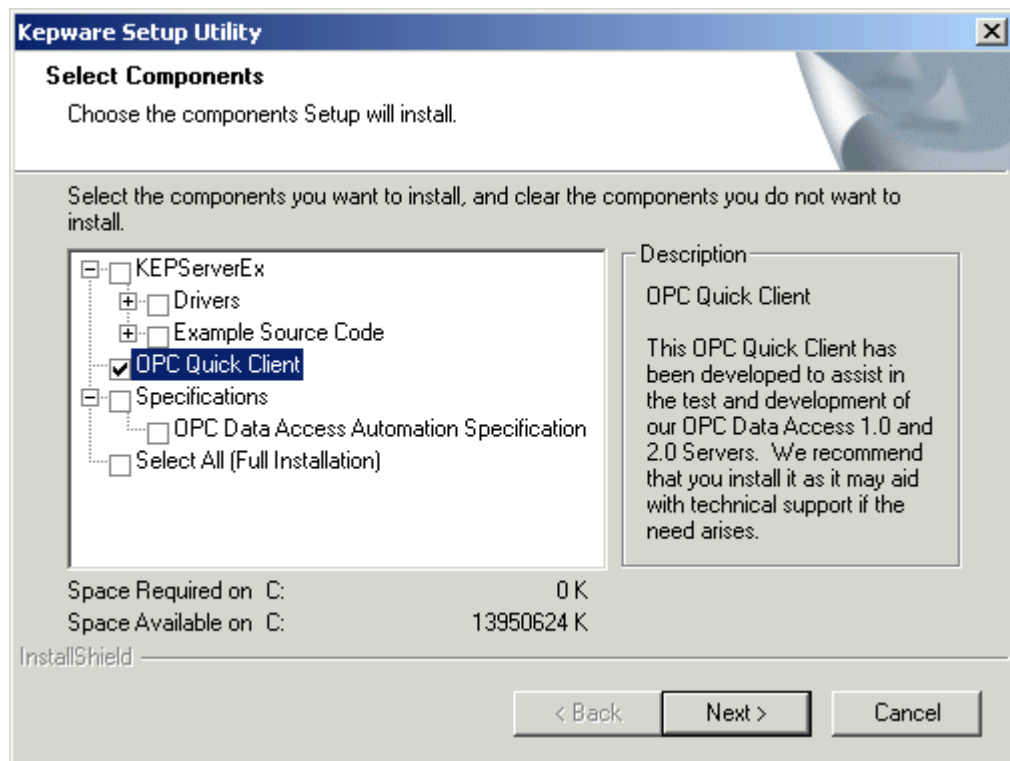
Using the Install Program to Register the Server

You may also use the server installation program to make the appropriate registry entries and to ensure that all of the files needed to make a remote connection are present.

1. On the remote PC run the Install program.



- At the component selection page, deselect all the components except for OPC Quick Client, and click **Next** to continue with the install. We recommend installing the OPC Quick client to verify server connections.



Adding DCOM Support to Win 95

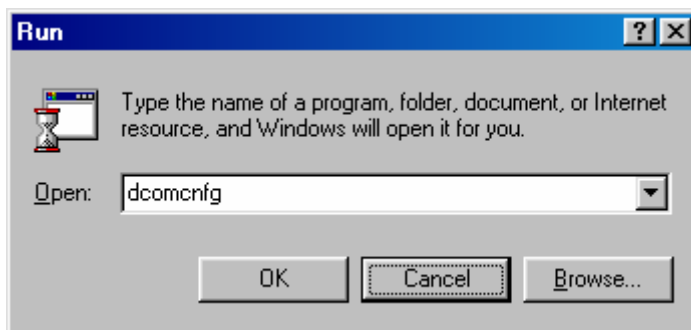
- For Windows 95 users, you must obtain both DCOM95.EXE, and DCM95CFG.EXE (if you don't have them already) in order to configure DCOM, since it is not native to Windows 95. You can acquire these files from the Microsoft web site:

DCOM95.EXE is also available on the Microsoft Visual Basic CD-ROM 5.0 (Enterprise, Professional or Standard editions) in the \Pro\Tools\DCOM95 directory

2. To install DCOM95, double-click DCOM95.EXE. You must reboot your system after the install to secure the changes. (NOTE: If you plan to install DCM95CFG.EXE then it would be best to reboot after both installations have been completed.)
3. Double-click to install DCM95CFG.EXE (this will allow you to run the DCOMCNFG.EXE, which you will use later.) You then must reboot the machine after the installation is complete.

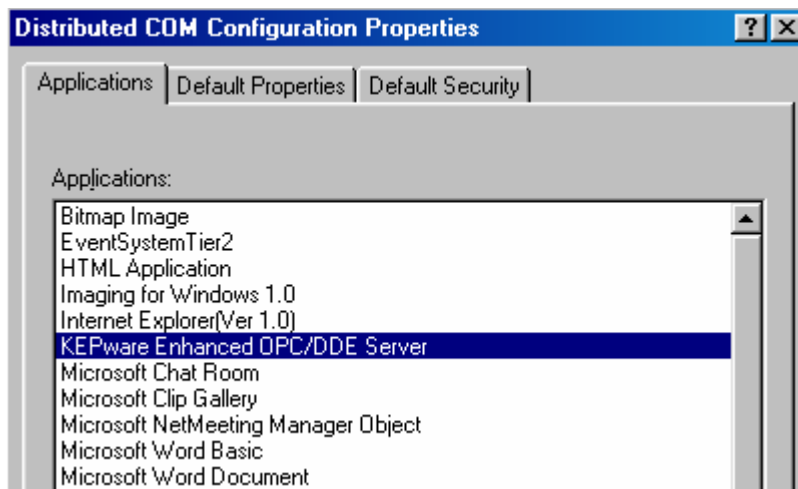
Editing the DCOM Configuration

1. Click Start / Run, enter DCOMCNFG.EXE, and click **OK**.



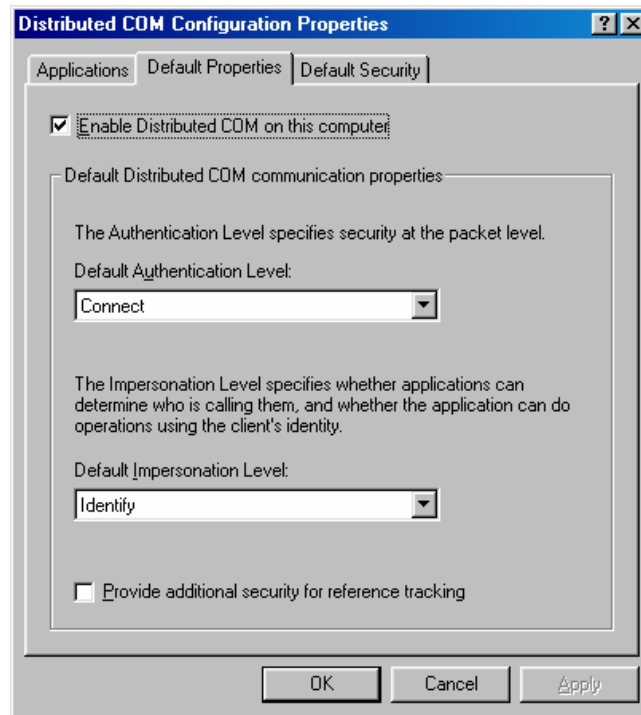
DCOM Config (known as DCOMCNFG.EXE) is a utility that can be used to secure Distributed COM (DCOM) objects that have been created.

2. A general DCOM configuration window will appear with three tabs. The foremost tab is Applications, which lists all applications that can enable DCOM. The next two tabs are default configurations used for all the listed applications. Changes made to these tabs affect DCOM applications globally. Pertaining to security, the approach of the following instructions is to allow all network users access to all DCOM applications. After a connection has been established; the user may choose individual applications from the list and customize their DCOM security properties for more control.

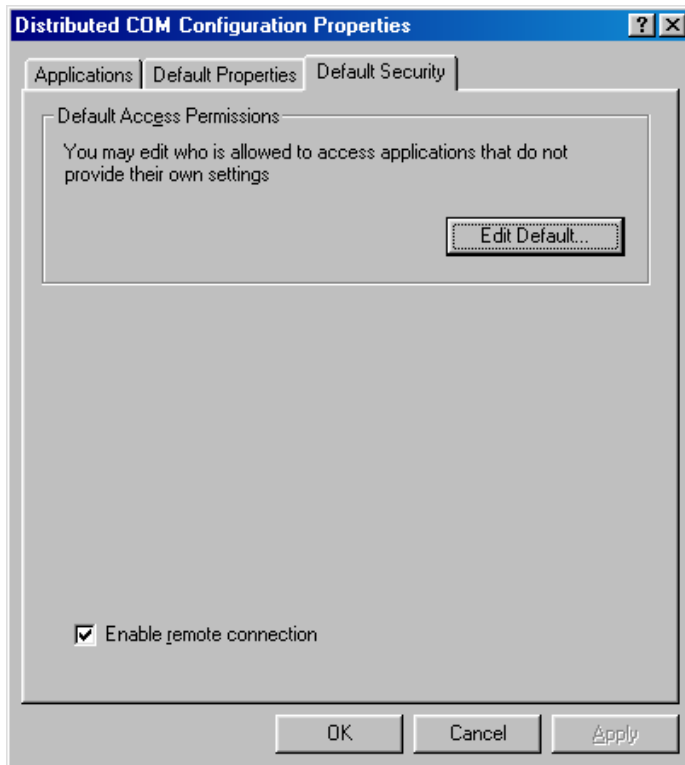


Note: It is very important to make sure that the **Apply** button is selected after each change made in a DCOM settings tab.

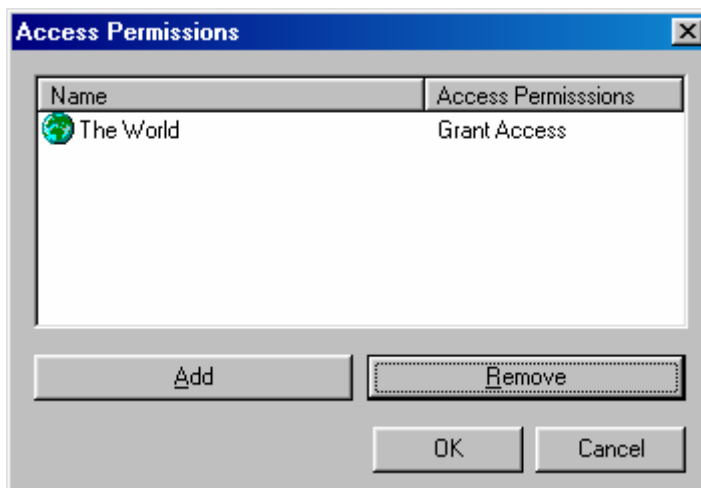
3. Under the Default Properties tab, “Enable Distributed COM on this computer” should be checked. Also, ensure that the “Default Authentication level:” is set to “Connect” and the “Default Impersonation Level:” is set to “Identify”. Click the **Apply** button if possible to administer the changes.



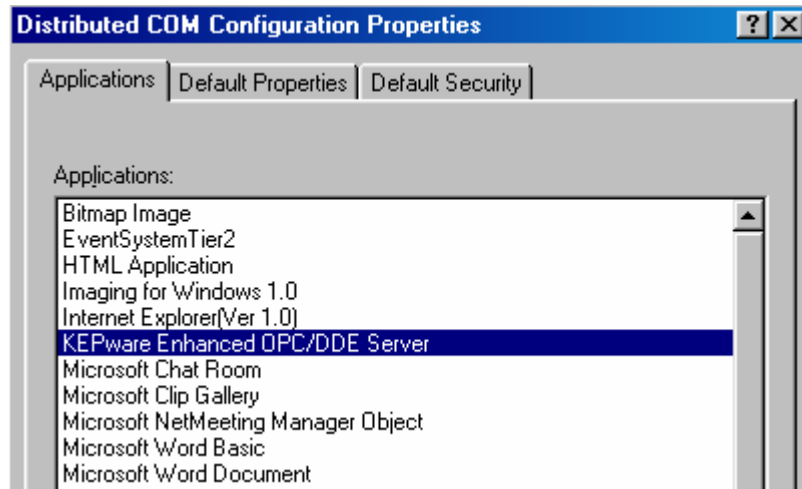
4. Select the Default Security tab and click the “Enable remote connection” box to allow for remote connections, then click the **Edit Default** button to view “Default Access Permissions”.



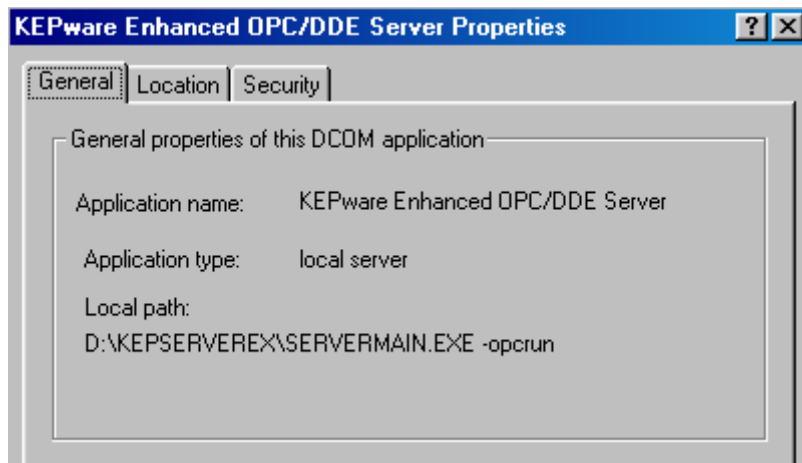
5. Add user group "The World" with "Grant Access" to the permission list. Then select **OK**. If you are going to connect to a server running on a Win NT/2000 PC as a service you will also need to add "System" with "Grant Access" to the permissions list.



6. Click the **Apply** button, then select the Applications tab. Double-click on "KEPware Enhanced OPC/DDE Server". This will access the applications specific DCOM properties



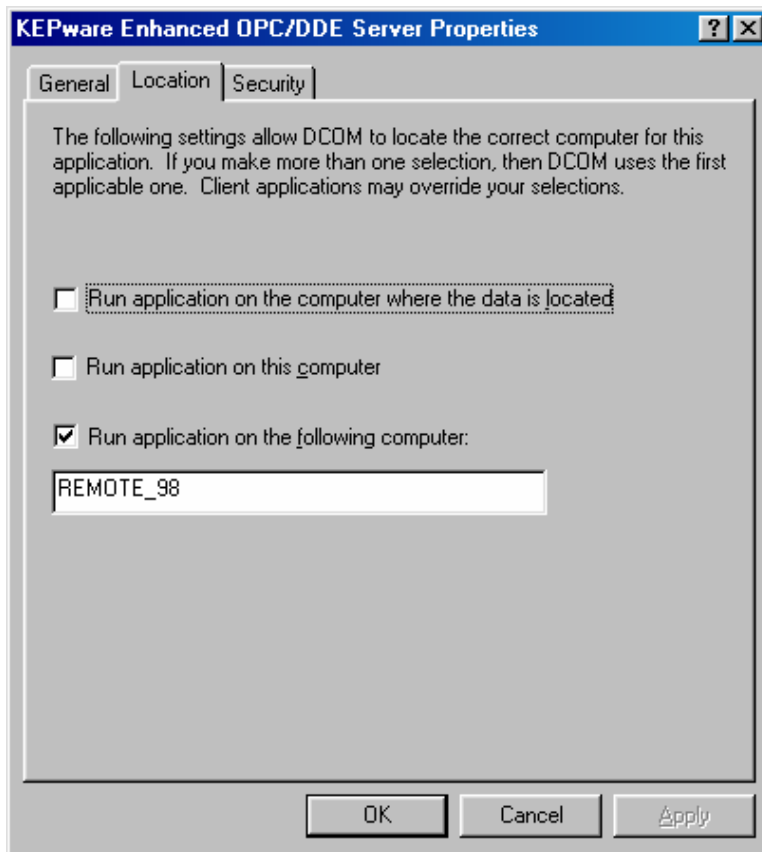
7. In KEPServerEX's application specific DCOM window, choose the Location tab.



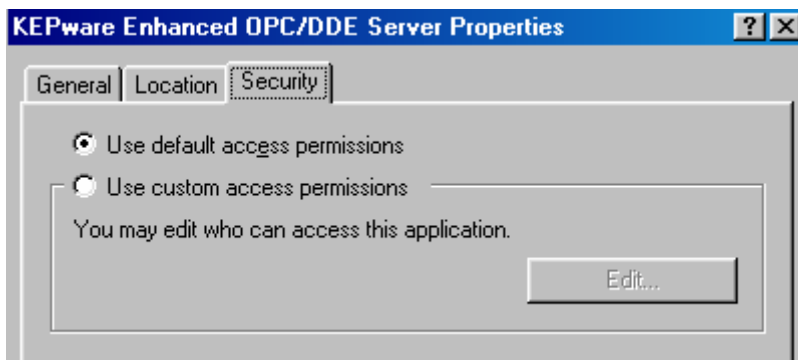
8. Most clients will allow you to connect directly to the remote PC by entering the name of the PC in the server connection dialog box. For applications that do not allow direct connections, select "Run application on the following computer". Next, browse for the remote machine that contains the KEPServerEX application, and select **Apply**. In this example the machine name is REMOTE_NT. For local connections you will leave "Run application on the computer where the data is located" checked.

Note: See Kepware's Client Connectivity guide for information on how specific clients connect remotely to KEPServerEX.

Warning: This dialog box will allow you to select more then one check box. If this happens it produces an error state. You must make sure that only one box is checked.



9. Choose the Security tab and verify the radio buttons for the Access permissions are set to default. Click **Apply** to accept these changes.



10. Choose **OK** from the bottom of the application specific DCOM display window.
11. Choose **OK** from the bottom of the general DCOM display window.
12. Reboot the computer to secure the new DCOM configuration.

At this point you should be able to connect to the server from the remote PC. If you installed the OPC Quick Client use it to test the connection, and then try the client you are planning to use.