INDUSTRIAL AUTOMATION SOFTWARE
progea

Movicon™
MONITORING, VISION & CONTROL

DCOM

Distributed Component Object Model (White Paper)

OPC FOUNDATION MEMBER

Quality Certified UNI-EN ISO 9001:2000 SINCERT

1 Summary

2 About This Document

2.1 Scope of the Document

This document is written to introduce Movicon Representatives, Distributors, System Integrators and Customers with the upcoming technology and provide user training. It address DCOM configuration issues on Win 95/98, Win NT 4.0/2000 and Win XP. Reading of this paper will benefit while configuring the system in true distributed Client/Server environment over DCOM.

2.2 Copyright

2.3 Revision History

Version 1 – January 2004

2.4 Product Reference

The document is reffered at the Movicon 9.1 versions or later

3 Introduction

Distributed Component Object Model (DCOM) is fairly new concept based on foundation provided by Object Linking and Embedding (OLE). DCOM is also called "COM with a long wire" i.e. OLE or Component Object Model (COM) only works on local computer while DCOM extends the same concept over network with extended security features and application access privileges. DCOM is the technology that extends COM to allow components objects to live on remote machines.

DCOM is considered to be the latest technique introduced by Microsoft and accepted for software development by majority of vendors. This facilitates the process of connectivity and thus offers the users to select various components from different vendors without loosing the performance or functionality. This concept is heavily supported by Open Software Foundation.

DCOM was not invented overnight, instead it is coalescence of two separate paths of technological evolution as shown in figure.

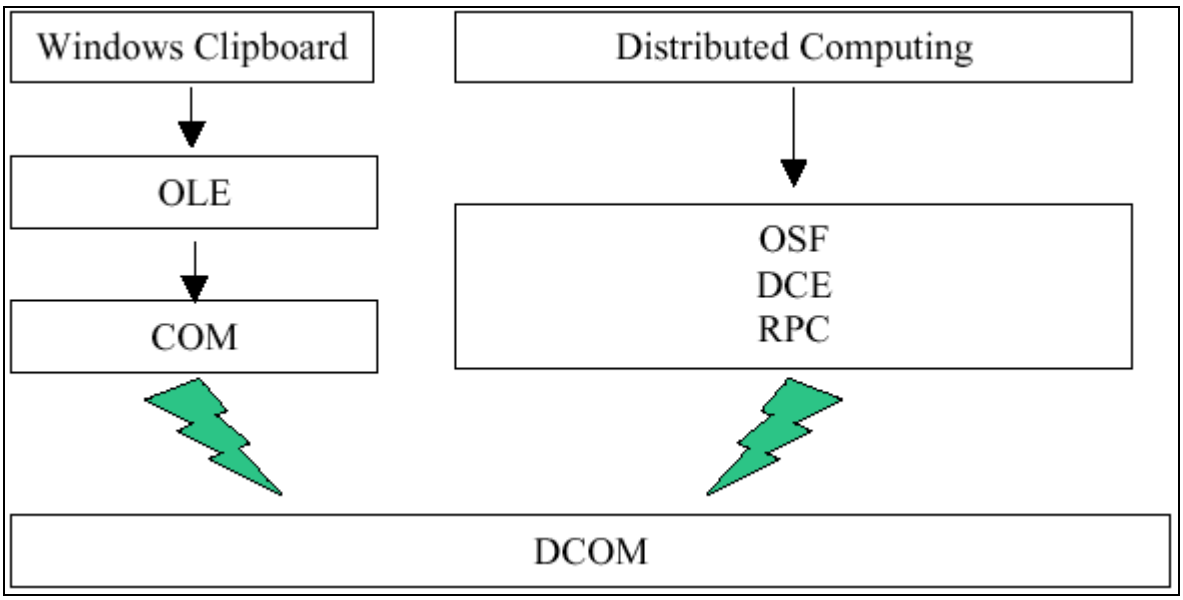


Figure 1 The evolution of DCOM

Starting from MS DOS, that could only run one application at time, the evolution of Multitasking Windows which fulfills the dream of multiple application concurrently . The desire for sharing data within the

applications was achieved via DDE. The clipboard offered cut, copy and paste operations, while OLE took one step further to offer editing of such objects. Over the years, OLE has faded into the background while COM has taken the center stage.

With the release of MS WIN NT 4.0 in 1996, COM gained the functionality necessary to invoke components that were running on remote computers connected via a network.

DCOM was also result of attempts made by various industry groups to get enough companies to define Standards and then agree to abide by them. Open Software Foundation (OSF) addressed the issue of distributed computed and out of this effort grew the specifications for the Distributed Computing Environment (DCE) . The outcome from OSF and DCE was a specification for communicating between computers known as Remote Procedure Call (RPC) that allows the applications on different computers to communicate. DCOM uses RPCs for its inter-computer communication and thus indicates how DCOM evolved from RPC.

4 Type of Components

Components come in one of three flavors: in-process, local or remote, depending on the structure of the code module and its relationship to the client process that will be using it.

4.1 In-Process

In-Process servers are loaded into the client's process space because they are implemented as DLLs. DLLs are code libraries that are loaded at run time by the operating system on behalf of programs that want to call functions in the DLLs. DLLs are always loaded into the address space of the calling process. This is important because in Windows 95 and Win NT each program (process) is loaded into its own private 32-bit address space for security and stability.
Since it is not normally possible to access memory locations beyond this private address space, DLLs need to be loaded in-process.

The main advantage of in-process servers is their speed. Since the objects are loaded in-process, no context switching is necessary to access their services, as is the case with DLLs. The only potential disadvantage to in-process servers is that since an in-process servers is in fact a DLL and not a complete application executable (EXE), it can be used only in the context of a calling program and cannot be run as a stand-alone application. ActiveX controls are implemented as in-process servers.

4.2 Local

A local server runs in a separate process on the same machine as the client. This type of server is an EXE of its own, thus qualifying as a separate process. Local servers are comparatively slower to access than in-process servers because the operating system must switch between processes and copy any data that needs to be transferred between the client and the server applications. The one advantage of local servers is that since they are EXE files, they can be run as stand-alone applications by the user without an external client.

4.3 Remote

Another type of component process is a remote server that runs on a separate machine connected via a network.
Remote servers therefore always run in another process. This functionality can be implemented using DCOM. The advantage of DCOM is that it does not require any special programming to enable this functionality.

5 Machine Setup Tips

The following section outlines some facts and requirements for the DCOM networking.

- ✓ DCOM be installed on Win 95 machine along with Internet Explorer 3.0x, since Win 95 does not come with DCOM as part of operating system. The installation files can be downloaded from www.microsoft.com or from Progea Movicon CdRom (<root>\DCOM95\). There are two self extracting files, double click for the installation.

- ✓ DCOM is part of Internet Explorer 4.0 but with an old build. Please read installation notes on installation of Internet Explorer 4.0. If you need to un-install DCOM or Internet Explorer 4.0 from you computer, choose reverse order as of your installation.

- ✓ Win NT/2000/XP and Win 98 come with DCOM as part of the operating system. There is Upgrade to WIN 98 DCOM available on Progea Movicon CdRom (<root>\DCOM98\). There are two self extracting files, double click for the installation. This upgrade to WIN 98 DCOM fixes the delay of opening Control Panel while some applications are running.

- ✓ Set *User Level Security* on the remote client as well as on remote server. This can only be done where you have a domain controller on the Network. Win NT Servers or Win NT workstation can act as domains on the network. This domain is required for user security clearance.

- ✓ Both Client and Server machines should be within the same network Domain or Workgroup.

6 DCOM Configuration

DCOMCNFG.EXE (DCOM Config) is a utility you can use to secure DCOM Objects you have created. This section describes the DCOM Configuration interfaces, options, and settings.

Because security is much more limited on Windows 95, the interface and options may differ on Win 95 /98 systems as of WIN NT 4.0/2000 and XP.

6.1 DCOM For Windows 95/98.

When you start DCOMCNFG from Start/Run you will see the main interface that divided into three tabs.

- ✓ Applications
- ✓ Default Properties
- ✓ Default Security

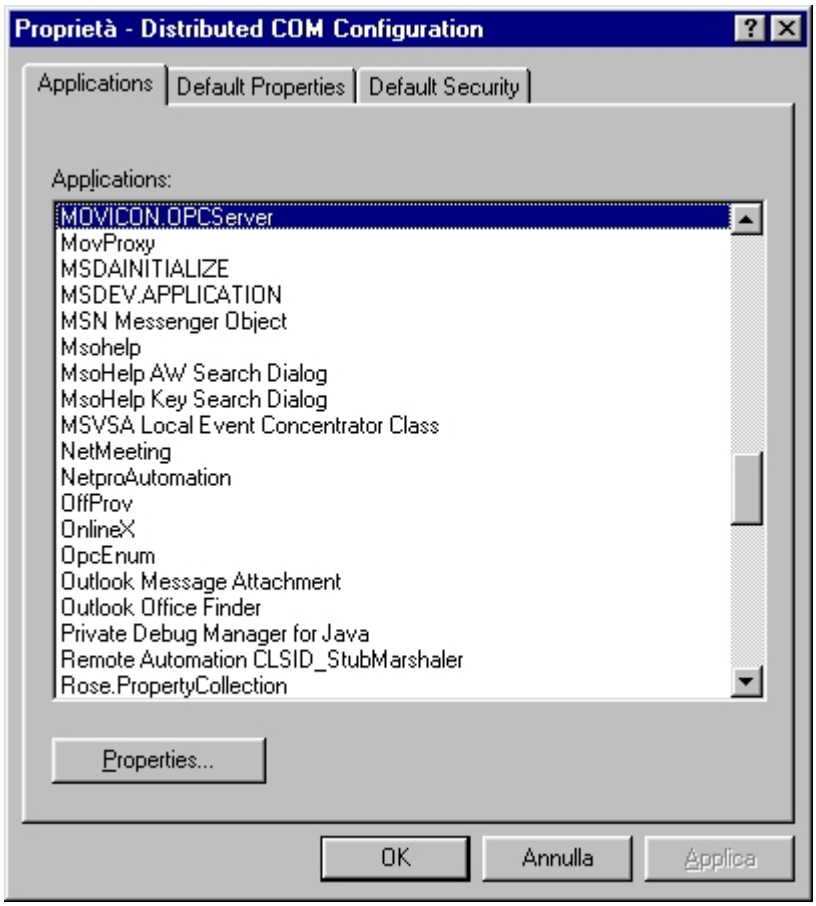
6.1.1 Applications Tab

The Applications tab shows each of the items registered under the following registry key:

HKEY_CLASSES_ROOT\AppId\

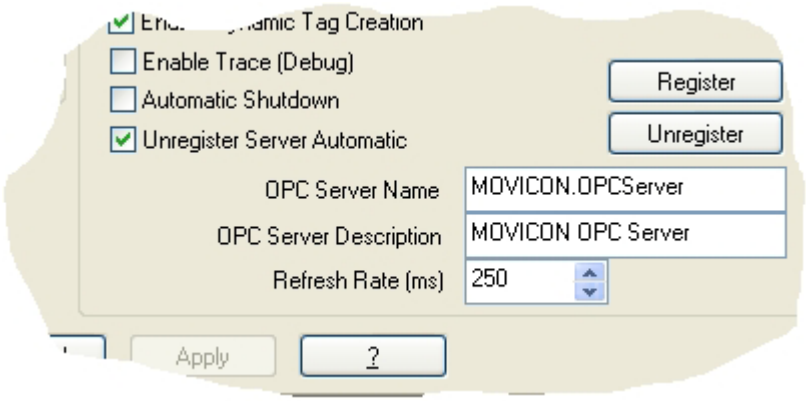
Beneath this key are all of the objects that can be launched on a remote machine. DCOM Config displays just the ProgIDs (friendly names) of each object, such as "Movicon.OPCServer". Some objects may register without registering a ProgID; in these cases, the GUID of the object will be displayed, such as "{047F5910-6CC5-11d3-9C2A-00105A3DD3AC}"

For each item listed in the Applications tab, properties for each application can be viewed by selecting an item and choosing the "Properties" button or by double-clicking an application name.



Progea suggestion:

The default application name for the Movicon 9.1 OPC Server is set to "MOVICON.OPCServer" but it can be changed in the "Server" dialog from the "Settings" menu.



6.1.2 Default Properties

Each of the values displayed under the Default Properties tab may be found under the following key in the registry:

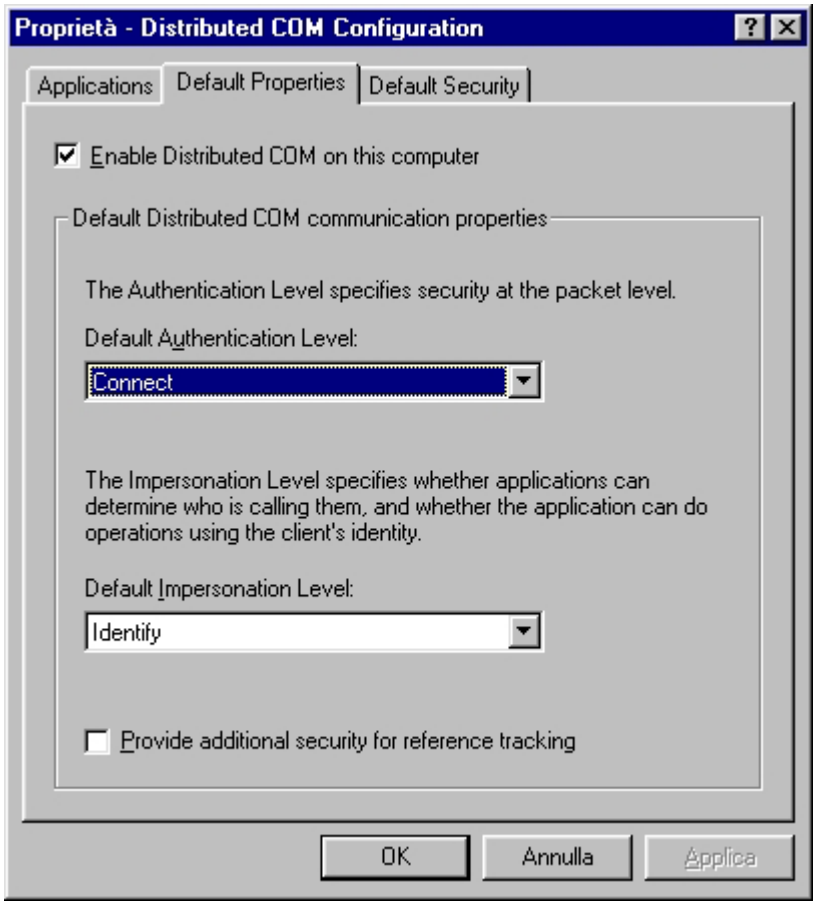
HKEY_LOCAL_MACHINE\Software\Microsoft\OLE

Enable Distributed COM on this computer:
The first item in the Default Properties tab is a check box:

"Enable Distributed COM on this computer"

This is a global setting for the entire machine. When this option is checked, the machine allows the creation of DCOM objects. If it is not checked, objects cannot be created via DCOM.

NOTE: You must reboot the system in order for a change in this setting to take effect.



Default Distributed COM Communication Properties
The second part of the Default Properties tab is the Default Distributed COM Communication Properties, which has of two levels:

a) Default Authentication Level.
b) Default Impersonation Level.

These two options can only be modified if DCOM is enabled on this system.

Default Authentication Level (Packet Level)

Authentication Levels are as follows;

Name	**Description**
None	No authentication.
Connect	Authentication occurs when a connection is made to the server. Connectionless protocols do not use this.

Note that "Connect" is used for connectionless protocols only. Windows 95 uses TCP, which is connection-based.

Default Impersonation Level

If no security is set at the object level, the server uses the security setting specified here as the default. The
possible values are:

Name	**Description**
Identify	The server can impersonate the client to check permissions in the ACL (Access Control List) but cannot access system objects
Impersonate	The server can impersonate the client and access system objects on the client's behalf

Provide additional security for reference tracking
The last item on the Default Security tab is a check box:

"Provide additional security for reference tracking"

This tells the server to track connected client applications by keeping an additional reference count. Checking this box uses more memory and may cause COM to slow down, but it ensures that a client application cannot kill a server process by artificially forcing a reference count to zero.

 *Progea suggestion:*

The reccommended settings for this DCOM dialog are:

- ✓ *Enable Distributed COM on this computer → "Enabled"*
- ✓ *Default Authentication Level (Packet Level) → "Connect"*
- ✓ *Default Impersonation Level → "Identify"*
- ✓ *Provide additional security for reference tracking → "Disabled"*

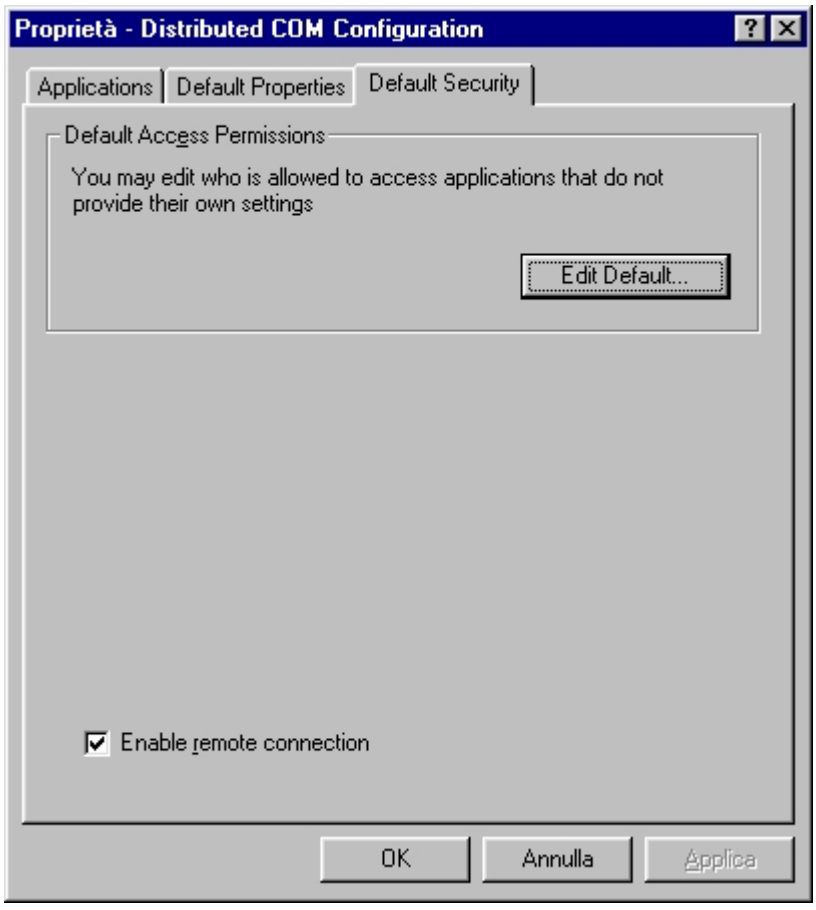
6.1.3 Default Security

The third tab is for setting up default security permissions for all applications. The values stored here can be found in the Windows registry at the following location:

HKEY_LOCAL_MACHINE\Software\Microsoft\OLE

Default Access Permission

This value determines the users and groups that can access an object when no other access permissions are provided.



Click on Edit Default to add or remove the users from the list. You can grant or deny users access permissions on the machine. This list of users is obtained from the domain where the user is logged in.

Progea suggestion:

The reccommended settings for this DCOM dialog are:

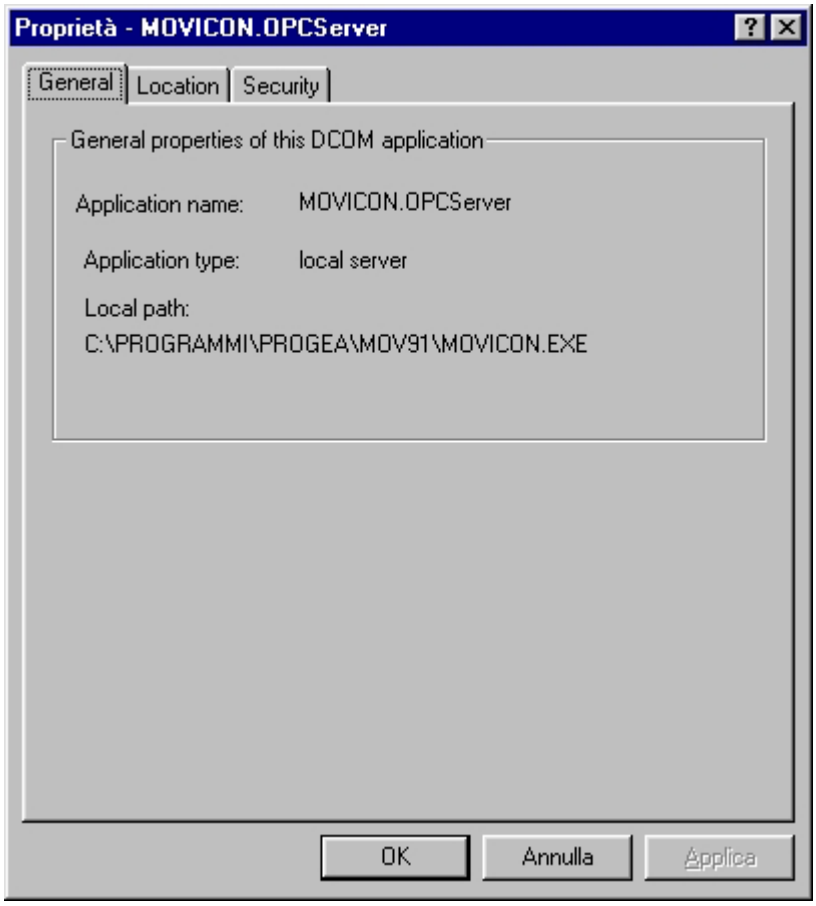
- ✓ *Default Access Permission → "Everyone"*
- ✓ *Enable remote connection → "Enabled"*

6.1.4 Application Properties

On the Application tab if you select a particular application and click on properties button, it will open interface for setting properties of that application. There are three tabs i.e. General, Location and Security.

General

This only displays general information about the application.



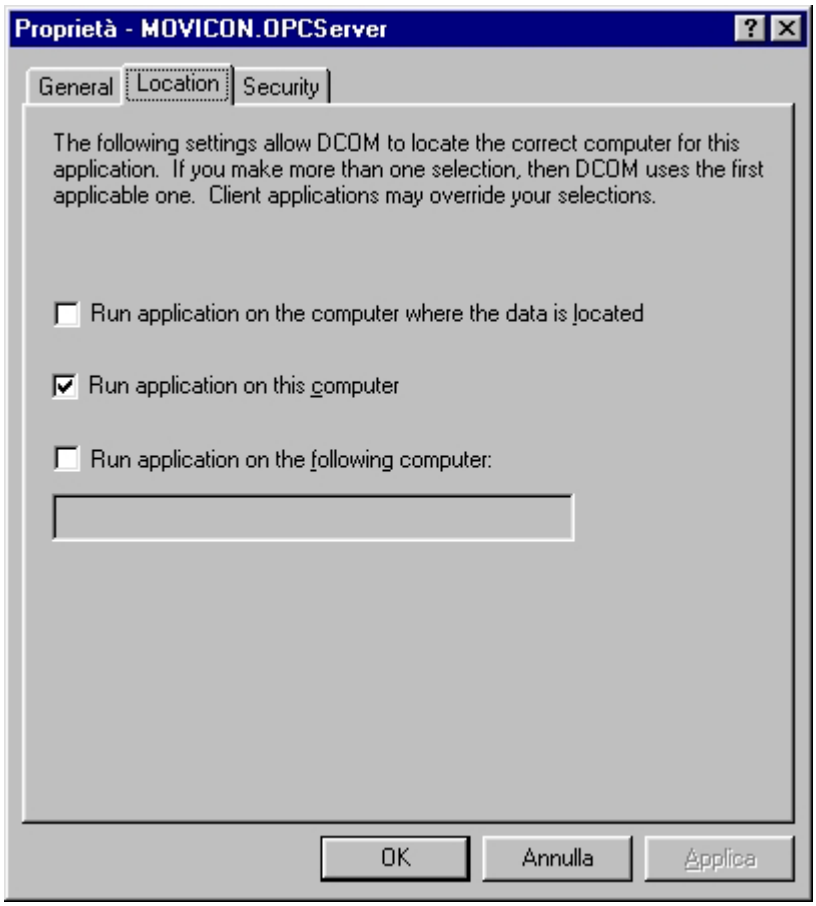
Location

This tab is used to determine where DCOM will execute the application. Here you can specify where to run your application. There are three possible choices:

a) Run application on the computer where the data is located: if selected, DCOM will execute the application where the data is located. This is useful only if the application provides a data file for the server application.

b) Run application on this computer: indicates that the DCOM application should run on the local machine.

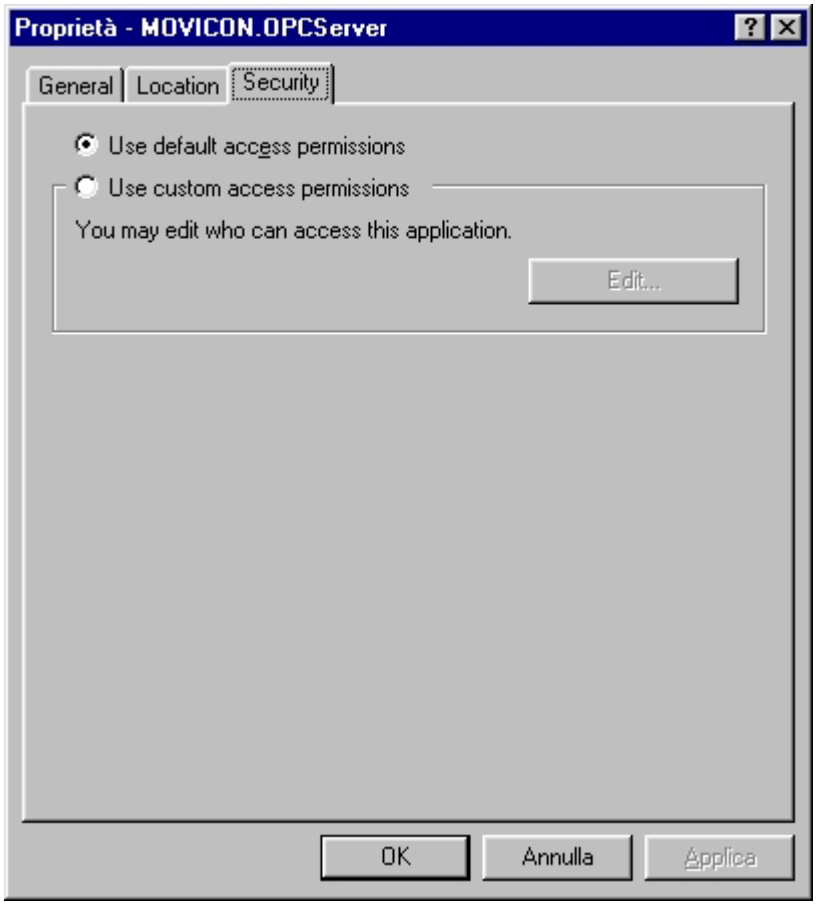
c) Run application on the following computer: allows you to specify a computer on which to execute. It requires node name of the computer where application is located. Some application do not support network browsing of tags, in these cases you can register the server locally and have a choice to run on another machine. When this option is selected, at client's call the server will start on remote location.



If more than one of the above is selected, DCOM will use the first applicable option. Client applications may also override this setting.

Security
There are two options either" use the default security option" in which case you do not need to add any users. Default security access permissions are applied to this application.

In case of "use custom access permissions" you can grant access to users only for this application instead for all application from default security.



Progea suggestion:

The reccommended settings for this DCOM dialog are:

- ✓ *Location → "Run Application on this computer"*
- ✓ *Security → "Use default access permissions"*

6.2 DCOM For Windows NT 4.0/2000

When you start DCOMCNFG from Start/Run you will see the main interface that divided into four tabs.

- ✓ Applications
- ✓ Default Properties
- ✓ Default Security
- ✓ Default Protocols

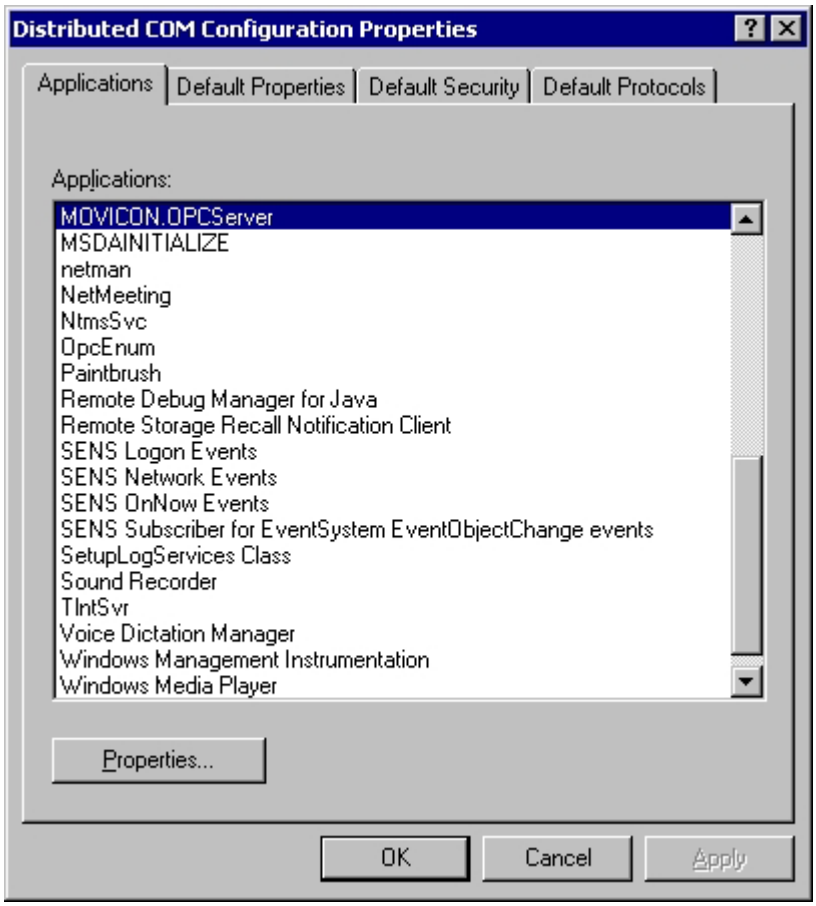
6.2.1 Applications Tab

The Applications tab shows each of the items registered under the following registry key:

HKEY_CLASSES_ROOT\AppId\

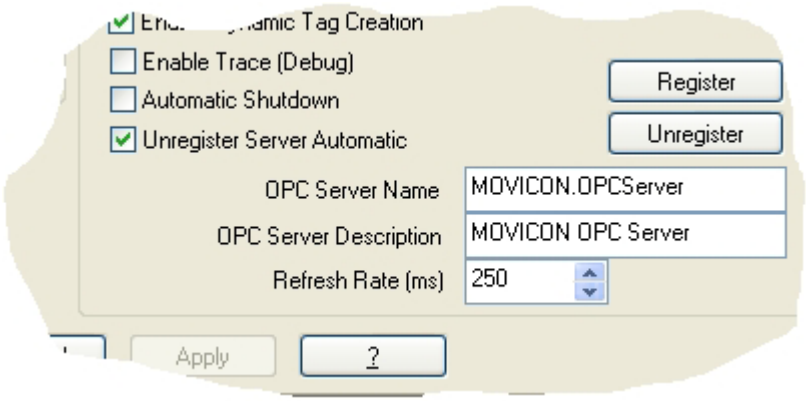
Beneath this key are all of the objects that can be launched on a remote machine. DCOM Config displays just the ProgIDs (friendly names) of each object, such as "MOVICON.OPCServer". Some objects may register without registering a ProgID; in these cases, the GUID of the object will be displayed, such as "{047F5910-6CC5-11d3-9C2A-00105A3DD3AC}".

For each item listed in the Applications tab, properties for each application can be viewed by selecting an item and choosing the "Properties" button or by double-clicking an application name.



Progea suggestion:

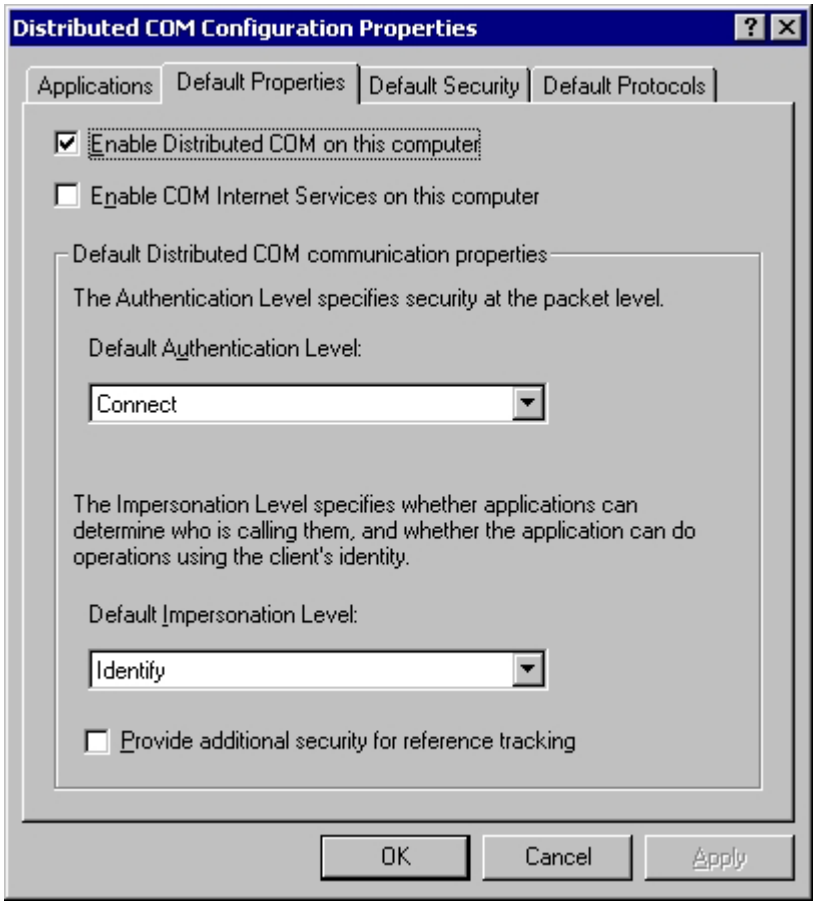
The default application name for the Movicon 9.1 OPC Server is set to "MOVICON.OPCServer" but it can be changed in the "Server" dialog from the "Settings" menu.



6.2.2 Default Properties

Each of the values displayed under the Default Properties tab may be found under the following key in the registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\OLE



Enable Distributed COM on this computer

The first item in the Default Properties tab is a check box:

"Enable Distributed COM on this computer"

This is a global setting for the entire machine. When this option is checked, the machine allows the creation of DCOM objects. If it is not checked, objects cannot be created via DCOM.

NOTE: You must reboot the system in order for a change in this setting to take effect.

Default Distributed COM Communication Properties
The second part of the Default Properties tab is the Default Distributed COM Communication Properties, which has of two levels:

a) Default Authentication Level.
b) Default Impersonation Level.

These two options can only be modified if DCOM is enabled on this system.

Default Authentication Level (Packet Level)

Authentication Levels are as follows;

Name	Description
None	No authentication.
Connect	Authentication occurs when a connection is made to the server. Connectionless protocols do not use this
Call	
Packet Integrity	This authenticates that the data has come from the client, and checks that the data has not been modified.
Packet Privacy	In addition to the checks made by the other authentication techniques, this encrypts the packet.
Default	May vary depending upon operating system.

Note that "Connect" and "Call" are used for connectionless protocols only. Windows NT uses a connectionless protocol, UDP, by default. However, Windows 95 uses TCP, which is connection-based. Windows 95 machines can only accept calls on the "None" or "Connect" levels.

Default Impersonation Level

If no security is set at the object level, the server uses the security setting specified here as the default. The possible values are:

Name	Description
Anonymous	The client is anonymous. This setting is not currently

	supported by DCOM.
Identify	The server can impersonate the client to check permissions in the ACL (Access Control List) but cannot access system objects.
Impersonate	The server can impersonate the client and access system objects on the client's behalf.
Delegate	In addition to the Impersonate level, this level can impersonate the client on calls to other servers. This is not supported in the current release of DCOM.

Provide additional security for reference tracking
The last item on the Default Security tab is a check box:

"Provide additional security for reference tracking"

Which tells the server to track connected client applications by keeping an additional reference count. Checking this box uses more memory and may cause COM to slow down, but it ensures that a client application cannot kill a server process by artificially forcing a reference count to zero.

Progea suggestion:

The reccommended settings for this DCOM dialog are:

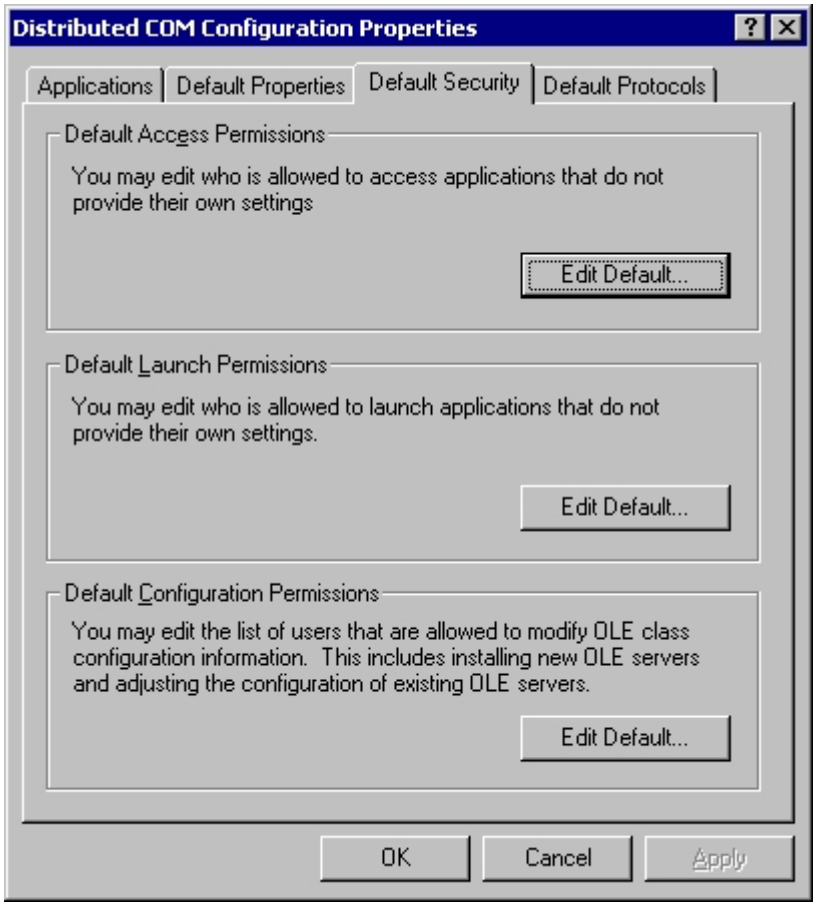
- ✓ *Enable Distributed COM on this computer → "Enabled"*
- ✓ *Default Authentication Level (Packet Level) → "Connect"*
- ✓ *Default Impersonation Level → "Identify"*
- ✓ *Provide additional security for reference tracking → "Disabled"*

6.2.3 Default Security

There are three options under the Default Security tab. Each of the values stored here can be found in the Windows registry at the following location:

HKEY_LOCAL_MACHINE\Software\Microsoft\OLE

The three options are:



Default Access Permission

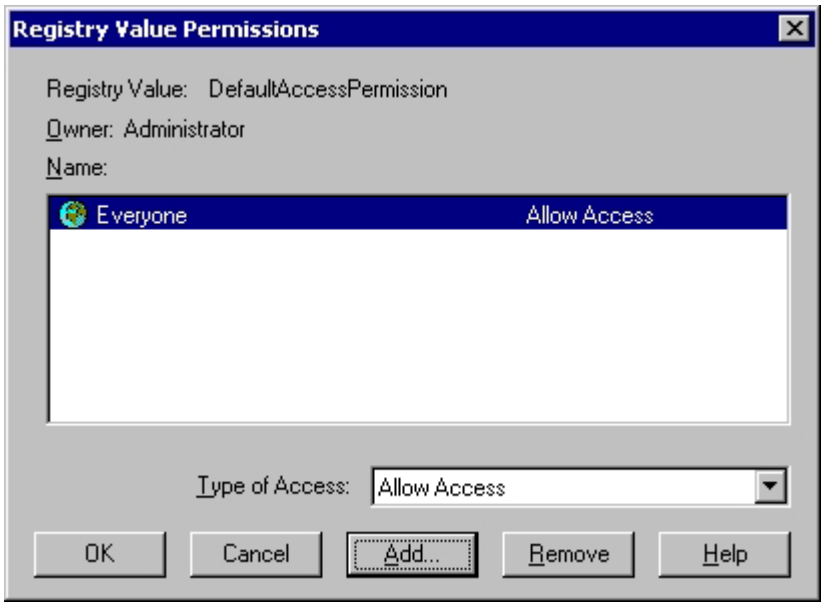
This value determines the users and groups that can access an object when no other access permissions are provided.

For information on how to give individual access permissions to specific DCOM objects, see the "Application Properties" section later in this document. By default, access is provided to the "System" and "Interactive" groups.

Default Launch Permission
This value determines the users and groups that can launch an object when no other access permissions are provided. For more information on how to give individual launch permissions to specific DCOM objects, see the section "Application Properties" later in this document.

Default Configuration Permission
This value determines the users and Groups that may read or modify configuration information for DCOM applications. This also includes which users and groups will have permission to install new DCOM servers.

System Groups:
There are several group accounts you will find when you configure users and groups.



The following list is a summary of which user belongs to each group:

Group	Description
Interactive	Includes all users who log on to a Windows NT system locally (at the console). It does not include users who connect to NT include users who connect to NT resources across a network or are started as a server.
Network	Includes all users who connect to Windows NT resources across a network. It does not include those

	who connect through an interactive logon.
Creator/Owner	The Creator/Owner group is created for each sharable resource in the Windows NT system. Its membership is the set of users who either create resource (such as a file) and those who take ownership of them.
Everyone	All users accessing the system, whether locally, remotely, or across the network.
System	The local operating system.

The list above includes the group accounts that are intrinsic to Windows NT systems. Your particular network may include more groups from which you may choose. In order to determine the membership of each custom group account, you must contact your network administrator.

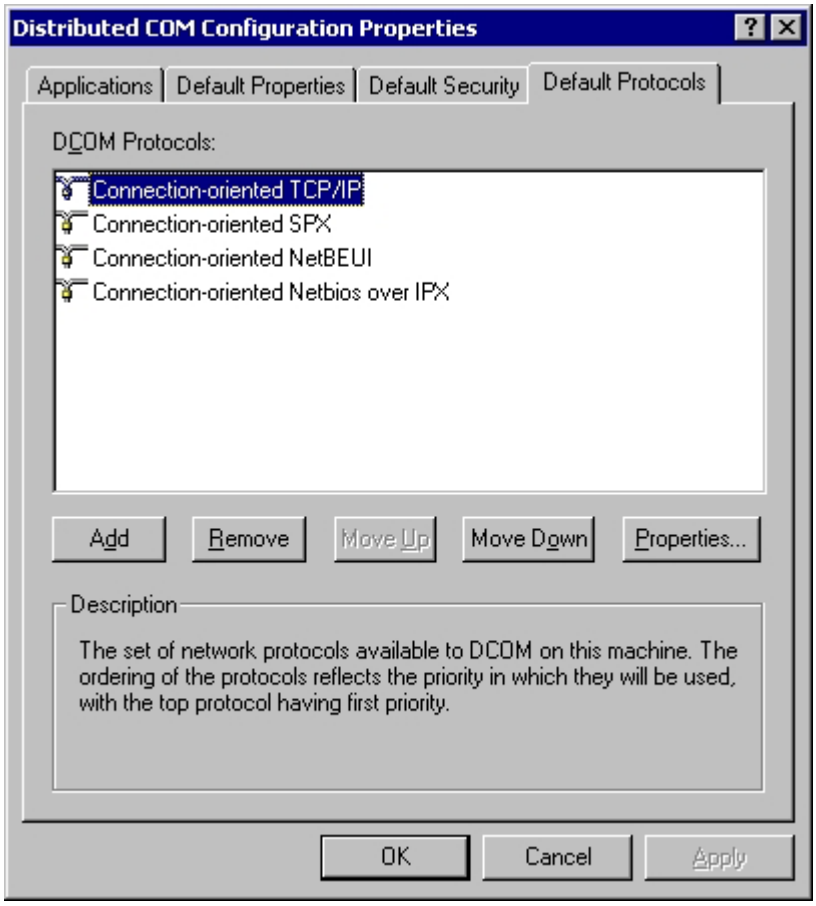
Progea suggestion:

The reccommended settings for this DCOM dialog are:

- ✓ *Default Access Permission → "Everyone"*
- ✓ *Default Launch Permission → "Everyone"*
- ✓ *Default Configuration Permission → Don't change i*

6.2.4 Default Protocols

The dialog show the list of the protocols available for connecting to COM objects registered in the computer. The protocols will be used in the order.



Progea suggestion:

Ensure that the TCP/IP protocols is the first name of the list.

6.2.5 Application Properties

You can specify custom settings for individual DCOM applications by choosing the Properties button on the "Applications" tab in DCOM Config. The following section describes each tab (General, Location, Security, Identity) and setting found within Application Properties.

General
The General tab provides general information about the application, displaying the Application name, type (local server or remote server), authentication level and location (local path or remote computer).

The General Table retrieves all of its information from subkeys of the following registry key:

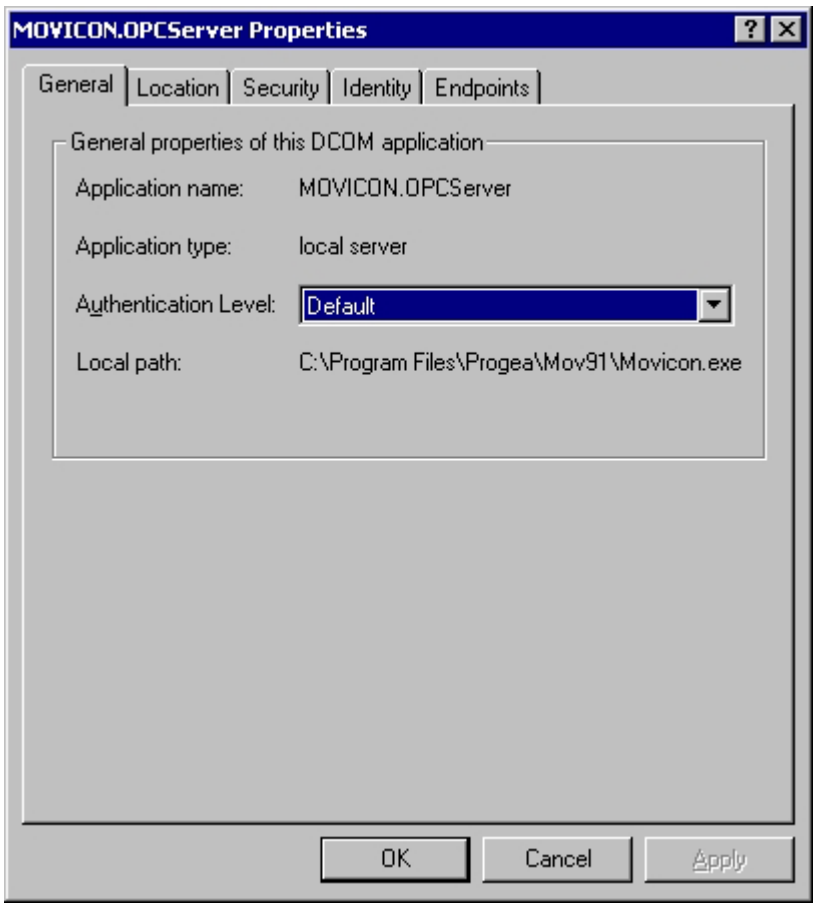
HKEY_CLASSES_ROOT\CLSID\{...CLSID...}

where {...CLSID...} is the unique CLSID for the Object Server currently being viewed.

Authentication Level

Sets packet-level security on communications between applications. This setting applies to the selected application. The possible values are:

Name	**Description**
None	No security-checking occurs on communications between application.
Default	The level of security is set to the default for installed Authentication service.
Connect	Secutiry-checking occurs for only the initial connection.
Call	Security-checking occurs on every call for the duration of the connection.
Packet	The sender's indentify is encrypted to ensure the authenticity of the sender.
Packet Integrity	The sender's identify and signature are encrypted to ensure the authenticy od the sendere and to ensure that packets have not been changed during transit.
Packet Privacy	The entire packet, including the data, and the sender's identify and signature are encrypted for macimum security.

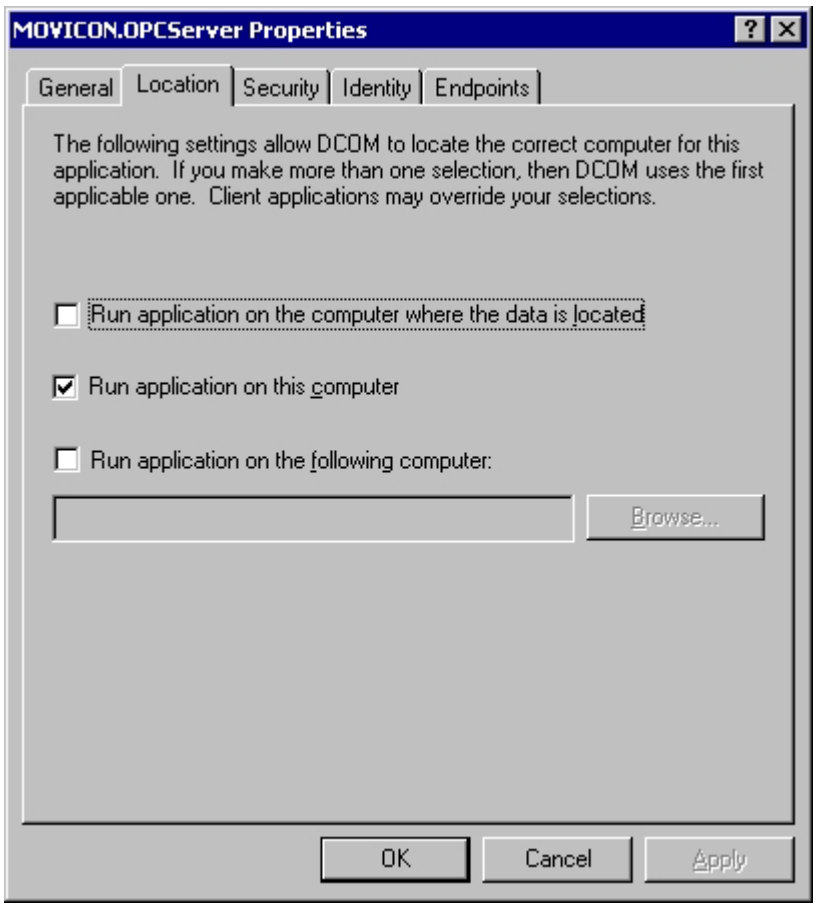


Location

This tab is used to determine where DCOM will execute the application. There are three possible choices:

a) Run application on the computer where the data is located: if selected, DCOM will execute the application where the data is located. This is useful only if the application provides a data file for the server application.
b) Run application on this computer: indicates that the DCOM application should run on the local machine.
c) Run application on the following computer: allows you to specify a computer on which to execute. (This feature is currently unavailable on Windows NT 4.0 systems, Windows NT 4.0 does not support full security delegation.).

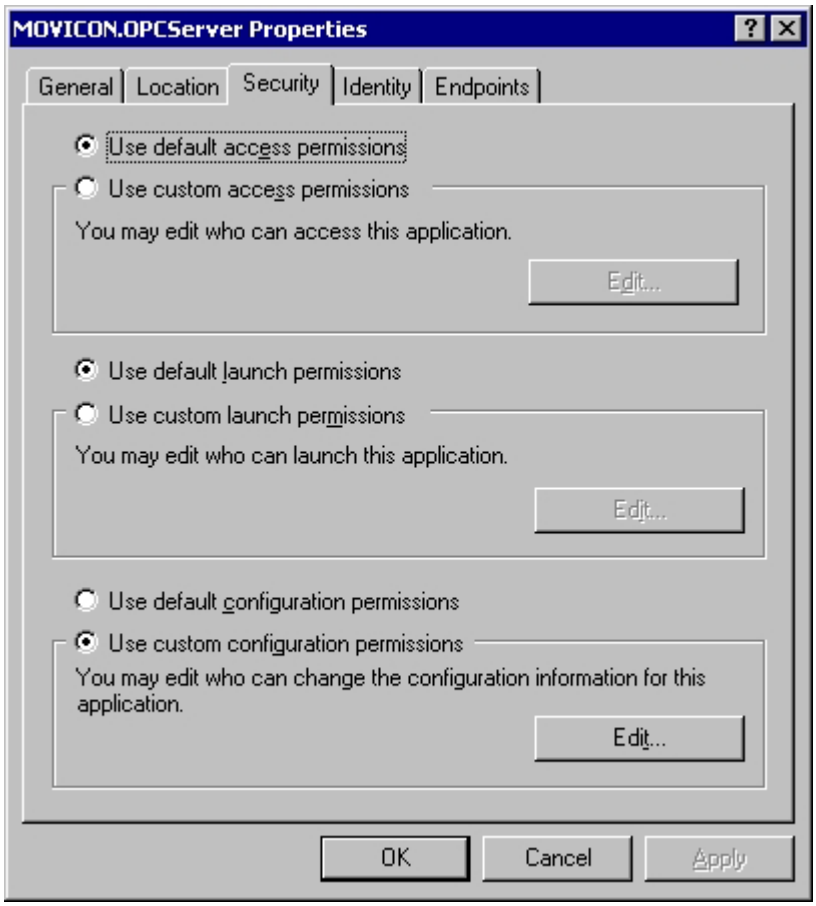
If more than one of the above is selected, DCOM will use the first applicable option. Client applications may also override this setting.



Security
On the Security tab, you can customize settings for the following individual application permissions:

a) Access Permissions.
b) Launch Permissions.
c) Configuration Permissions.

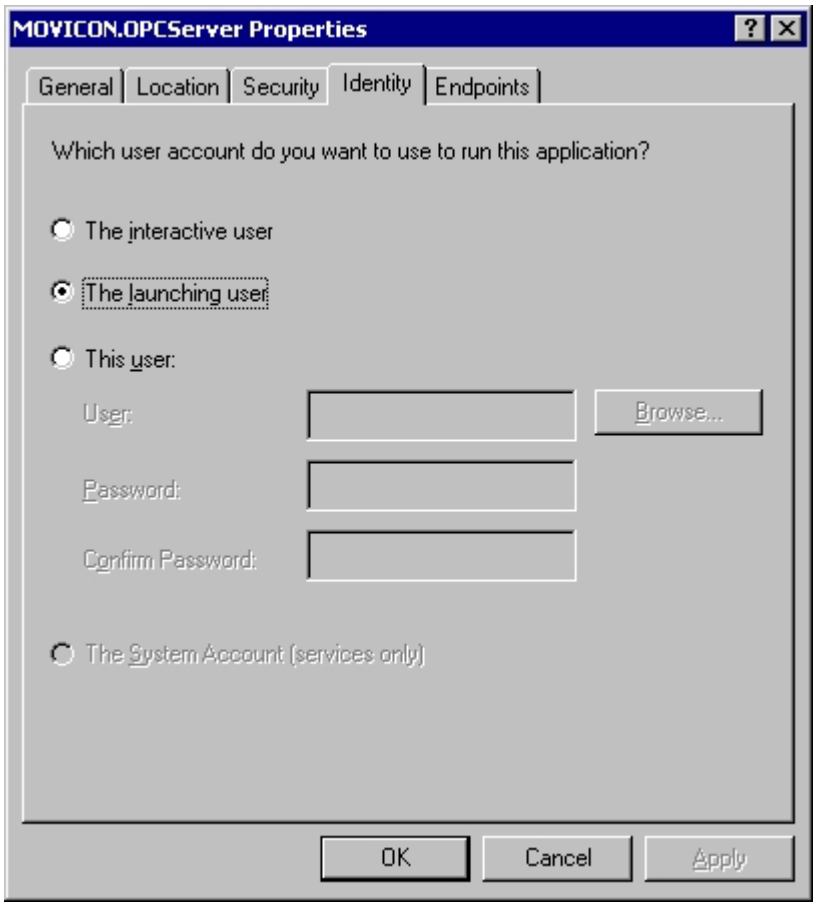
If you do not customize these settings, the default security settings are used. For more information about the Security tab, see the section earlier in this article on "Default Security".



Identity

This tab is used to determine which account you want to use to run the application. There are four choices by which the system determines which account your DCOM object will run under:

a) The Interactive User: the application will run using the security context of the user currently logged onto the computer. If this option is selected and the user is not logged on, then the application will not start.
b) The Launching User: the application will run using the security context of the user who started the application. The launching user and the interactive user may be the same.
c) This User: you may specify the user whose security context will be used to run the application.
d) The System Account: this is available only for NT services that use DCOM.



Progea suggestion:

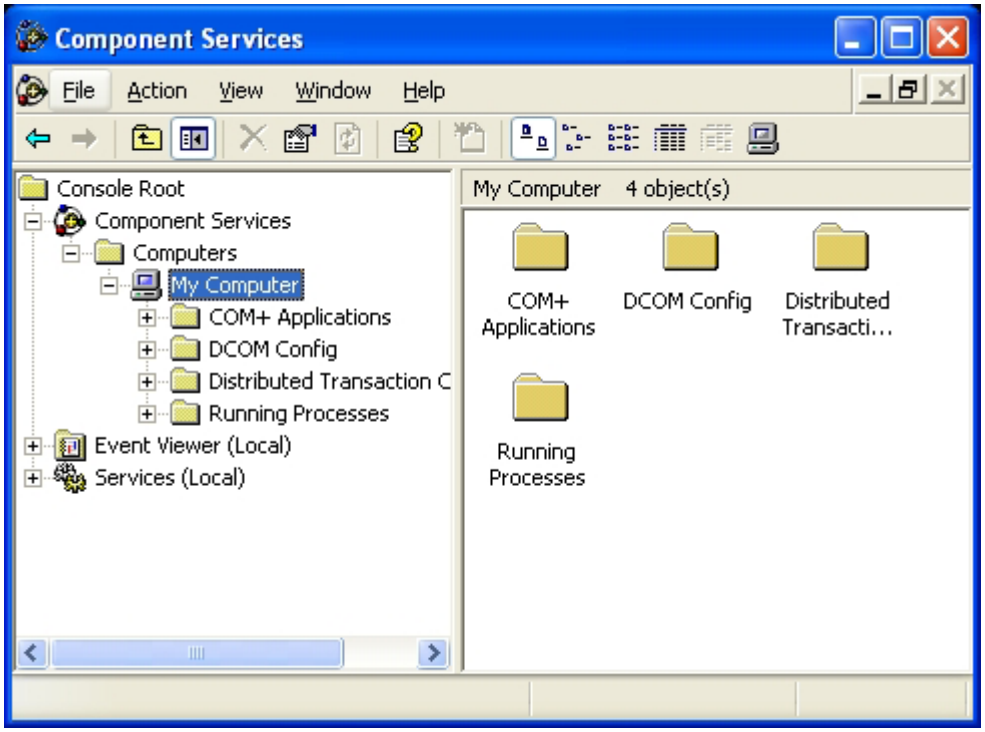
The reccommended settings for this DCOM dialog are:

- ✓ *General/Authentication Level → "None"*
- ✓ *Location → "Run application on this computer"*
- ✓ *Security/Access Permissions → "Use Default"*
- ✓ *Security/ Launch Permissions → "Use Default"*
- ✓ *Security/ Configuration Permissions → "Use custom"*
- ✓ *Identity → "The Launching User"*

6.3 DCOM For Windows XP

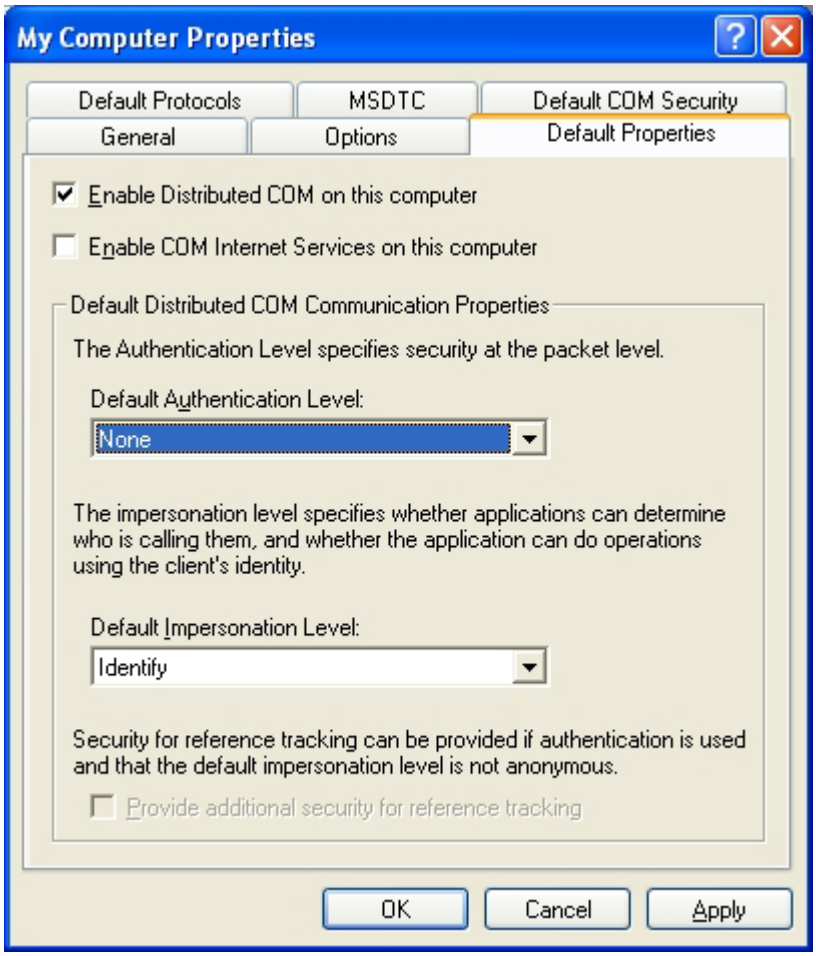
There are minor variations between configuring DCOM on Windows NT/2000 operatyng system and Windows XP. The part of this document will explain only the steps required to show the DCOM dialog configuration.

When you start DCOMCNFG from Start/Run you will see the main interface that divided into two windows.



6.3.1 General Properties

The right click on “My Computer” on the “Component Services” page and select “Properties”. It will bring you to the “General” tab of the DCOM properties. These properties are the same described in the previous part of this document for Windows NT/2000 operatyng system. Please, see its for more details.

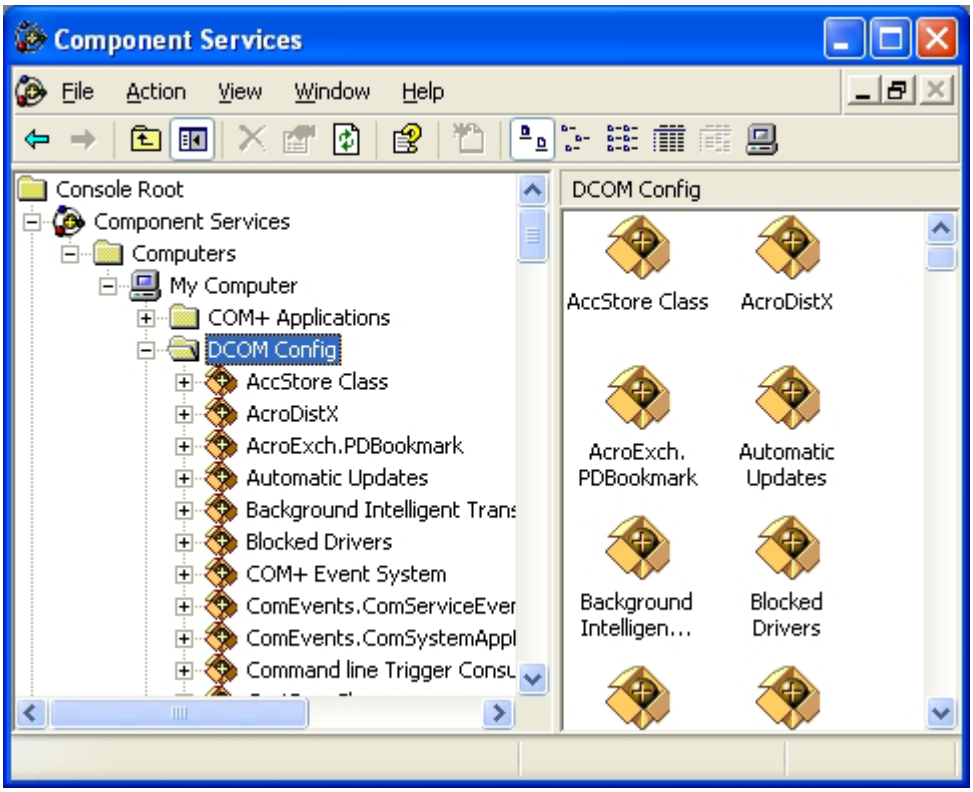


6.3.2 Applications List

You can select and expand the "DCOM Config" folder in the directory tree. The folder shows each of the items registered under the following registry key:

HKEY_CLASSES_ROOT\AppId\

Beneath this key are all of the objects that can be launched on a remote machine. DCOM Config displays just the ProgIDs (friendly names) of each object, such as "MOVICON.OPCServer". Some objects may register without registering a ProgID; in these cases, the GUID of the object will be displayed, such as "{047F5910-6CC5-11d3-9C2A-00105A3DD3AC}".



6.3.3 Application Properties

For each item listed in the Applications tab, properties for each application can be viewed by selecting an item and choosing the "Properties" item's menu after a right click. These properties are the same described in the previous part of this document for Windows NT/2000 operatyng system. Please, see its for more details.