HOME

User Manual

DELMIA Process Engineer®

DCOM Settings

DELMIA

Foreword

This manual provides an introduction to the basic operations and functions of the DCOM Settings.

While developing these functions we have made every effort to create a clearly organized, easy-to-understand program structure.

A user-friendly interface as well as a clear menu guide will enable you to quickly learn how to operate the program and to get familiar with its functions so that you can carry out your planning tasks in a quick and reliable way.

No Liability or Guarantee

Our programs and manuals have been compiled with great care and to the best of our knowledge. They have also been tested in a production setting. However, we assume no liability and provide no guarantee that the software and related descriptions are free of error or are suitable for special purposes.

DELMIA assumes no liability for any damage that may arise from the use of this software. By using this software, the user acknowledges this exclusion from liability and shall hold DELMIA exempt from all claims.

Copyright

Modifications

Moreover, DELMIA retains the right to make modifications and improvements to the product described in this manual at any time without prior notification.

Table of Contents

1. Introduction

This manual explains how to use the Process Engineer DCOM Settings for your planning purposes.

1.1 How to Use this Manual

This manual enables you to get familiar with the operation and functions of the Process Engineer. This manual briefly describes:

- DCOM Setting Functions

Note

When handling the DCOM Setting functions, please also refer to the general introduction to Process Engineer in the General Introduction Manual.

Click General Introduction to access the manual.

1.2 Documentation Conventions and Symbols

The symbols used in this manual are intended to provide you with keys to the contents in an immediately understandable manner.

This symbol is used to introduce key concepts that are covered in the sections immediately following this symbol. As a result, this symbol most frequently appears at the beginning of chapters or sections.

Note

*This symbol is used to mark notes, which provide you with additional information you need to have for further work. You will either find the Note sign at the beginning of a chapter or in a particular text passage in the chapter. Texts bearing this sign are additionally marked with **Note**. The text is always in italics.*

Caution

*This symbol indicates that the text that follows describes particular circumstances that you must avoid to avoid potential errors with the operation of the program or harm to data. You will either find the Caution sign at the beginning of a chapter or near a particular text passage in the chapter. Texts that are introduced by this sign are additionally marked with **Caution**. The text is always in italics.*

This symbol marks examples which serve to illustrate a certain situation.

1 This symbol marks the individual operational steps involved in a particular operating instruction. Operating instructions describe operational steps, for example, how to open a menu or execute a function.

▪ This symbol marks listed subjects. The symbol for listed subjects can be either used to structure a continuous text or to list main subject keywords.

➢ This symbol marks list inside a bulleted or numbered list.

 This symbol marks cross reference information that is available in another manual.

1.3 New Functions in DCOM Settings

No new functionality has been added for this release.

2. Overview

The Process Engineer solution consists of three different layers. These three layers are database, server applications, and client applications. Part of the solution is the capability to run these three layers on different computer. The interaction between these layers is provided via technologies that provide network capabilities.

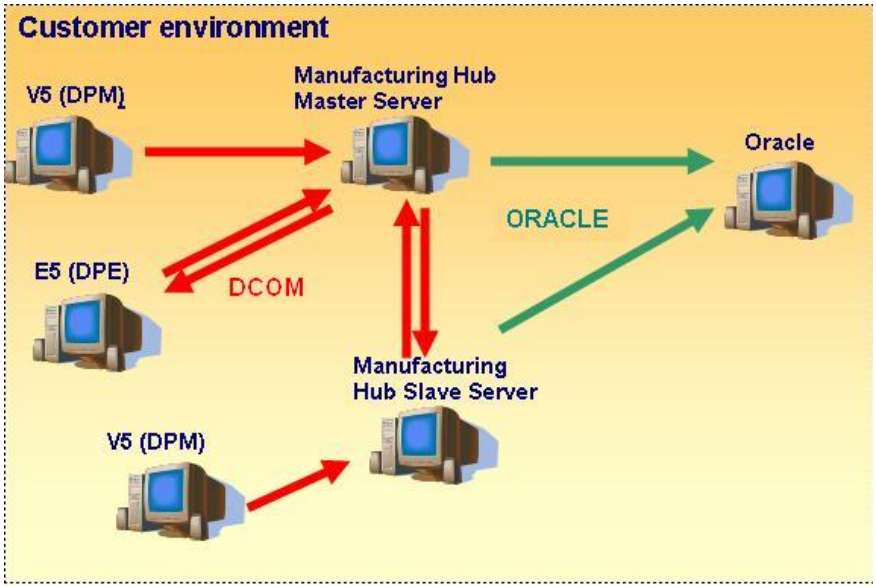

Figure 1: Process Engineer Layers

The solution used as database is Oracle. Oracle itself uses by default TCP/IP to communicate via network and therefore provides the technology that allows the communication between server and database.

This manual concentrates on explaining the setup of the other technology, which is used by the Server and Client part of the solution for network communication. This technology is called DCOM (Distribution Component Object Model).

2.1 Distribution Component Object Model

DCOM is a technology that was introduced by Microsoft in the mid 1990s. It has been developed on top of COM (formerly called also OLE). COM itself is a technology that initial was used for inter module/inter process communication inside computer boundaries. DCOM enhanced this technology by the capability to communicate via network. Internal DCOM uses **R**emote **P**rocedure **C**alls (RPC), which itself again is implemented base on the TCP/IP network protocol.

What makes DCOM difficult to install and to administrate is the security model, which it provides. This manual explains the settings that have to be customized on client and server side in order to enable the solution to work via network.

2.1.1 Callbacks

A callback represents in DCOM a connection that is build up backward from the server to the client. Since this type of connections are built up by DCOM in this way, in some scenarios customization effort on the Client OS is necessary. Server applications use these methods for asynchronous communication with the clients. In the context of DPE client (also called E5 client) callbacks are used in first instance for keeping the data on the client side up to date. Since DPM clients (also called V5 clients), compared to the DPE clients, ensure the consistency of the data in another way, they also do not need any callback mechanism.

The usage of callback, in our solution, is in majority the reason for client side customization. The manual will explain in which scenarios client side customization is required.

2.1.2 DCOM and Firewalls

The DCOM technology uses a dynamically assignment of TCP/IP ports for communication purposes. In theory DCOM could use all ports on an individual machine that are not used for other communication purposes. This fact and the fact that the solution is using the callback functionality of DCOM make the setup of our solution over Firewall boundaries very complex. Further explanations on how to setup DCOM cross Firewall boundaries can be found on the following Microsoft URL:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomfirewall.asp

2.2 Prerequisites

The changes described further in this manual are recommendations. They are based on Operation System installations where security policies are as they are shipped by Microsoft. In case the security policies have been changed by the customer further customization steps could be needed.

To execute the changes described in this manual you need to be logged in as **Local Administrator** on the machines on that changes have to be done.

3. Working with Enabled DCOM Authentication

Running the software with an enable DCOM Authentication means that a user authentication takes place when a connection is established. In order to authenticate the transfer of user contexts from one machine to another is performed. Per example the DPE Client, as in the following pictures shown, runs under the context of a user called **DPE User** (account of user under, which the log in to the client machine has been performed):

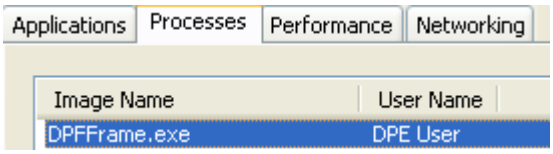

Figure 2: User Context

This user context is transferred to the server machine where first of all authentications takes place. In second instance security checks are done that determine if user has access permission.

Configuration of which mode the software uses happens via registry. By default the solution is installed to run with enabled DCOM Authentication. This means the **DisableAuthentication** value that is stored in the registry under the key **HKEY_LOCAL_MACHINE\SOFTWARE\DELMIA** is set by default to **0**. The flag has to be consistent on all server and client machines.

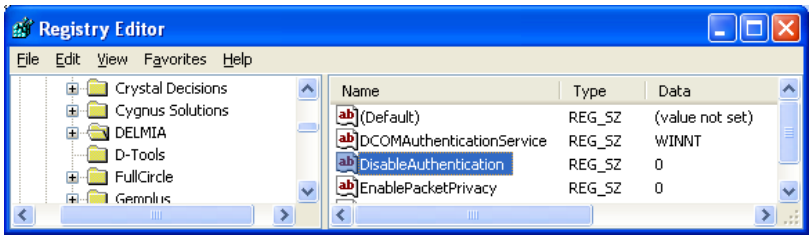

Figure 3: Registry Editor

Notes

We recommend the users to be logged in as a Domain User when working with the client software. Also we recommend the server process to run under a Domain User. The usage of a Domain User for the server process identity is suggested cause of the callback connections. The general use of Domain Users makes the administration and setting up of the solution easier.

3.1 Server Settings

When setting up the system the first thing to do, is to define the user identity under which the server processes have to run. We recommend the use of a **Domain User** that has **Local Administrator Rights** (*Please refer to the* Assign Local Administrator Rights to a User) for this purpose. Due to the call-back connections the server has to authenticate on the client machines. This means the user identity used by the server processes has to be known on the client machines (applies only in case client is a DPE client).

Generally spoken, if non domain users are used either as client user identity or server process identity, the only option is to make the user known by creating a user with the same name/password combination on the opposite machine.

The following steps have to be done in order to setup DCOM Permissions in the right way. How to do these steps will be explained further on in own sub chapters:

- The user identity has to be set for the Server Processes
- Set the Launch Permission for the Server Processes
- Set the Access Permission for the Server Processes
- Depending on the used server OS, machine policies have to be adapted.

For setting up the permissions in a convenient way we recommend setting up a **Domain Group** containing all users that work with the solution and also **the user identity of the server processes**:

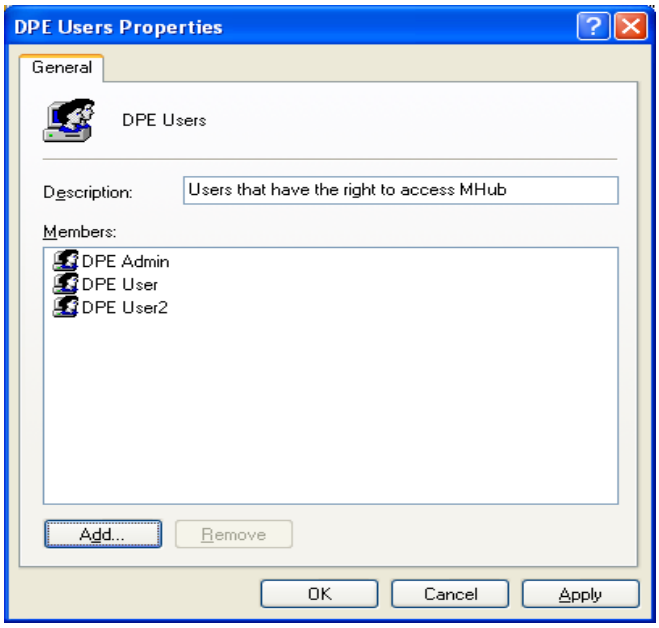

Figure 4: DPE User Properties

➢ If only one server machine is set up, in that case a **Local Group** is sufficient.

3.1.1 Configure the User Identity of the Server Processes

1) Start DCOM Configuration, *Please refer to the* Launching DCOM Configuration Tool.
2) Set DCOM Identity on required processes (*Please refer to the* Customizing Server Processes)

Figure 5: DPE Server Processes

3) Select **Properties**… on each server process.
4) Select the **Identity** tab:
5) Check the radio button This user and enter the user name (DPE Admin) and user password.
6) Confirm with **OK.**

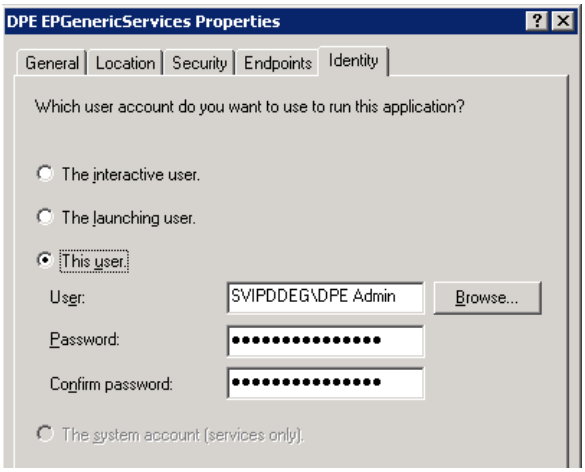

Figure 6: DPE EPGeneric Services Properties

7) The server processes from now should run under the **DPE Admin** user account.

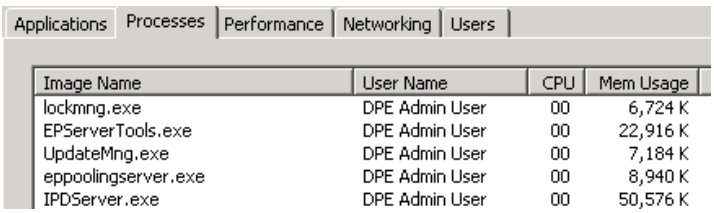

Figure 7: Server Processes

3.1.2 Set Process Launch Permissions

1) Select **Properties…** on each server process (DPE…) in DCOM configuration Tool.
2) Select **Customize** and **Edit** to set the Launch Permissions. Exit the dialog with **OK.**

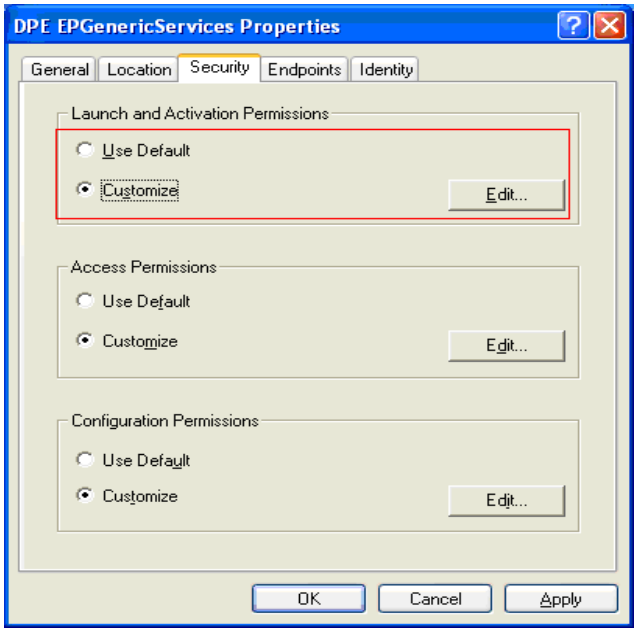

Figure 8: Launch Permissions

3) Assign **DPE User** Group all Permissions and exit with **OK**

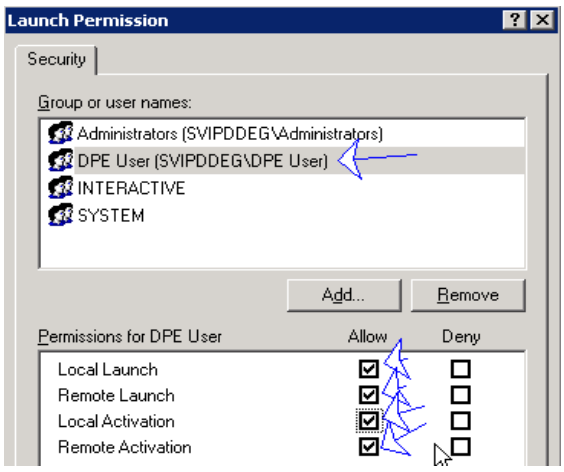

Figure 9: DPE User Group

3.1.3 Set Process Access Permissions

1) Select **Properties…** on each server process (DPE…) in DCOM configuration Tool.
2) Select **Customize** and **Edit** to set the Access Permissions. Exit the dialog with **OK.**

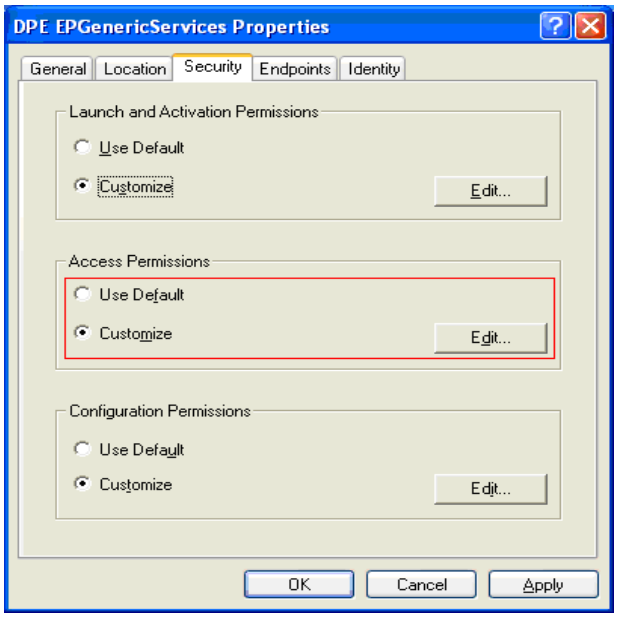

Figure 10: Access Permissions

3) Assign **DPE User** Group all Permissions and exit with **OK.**

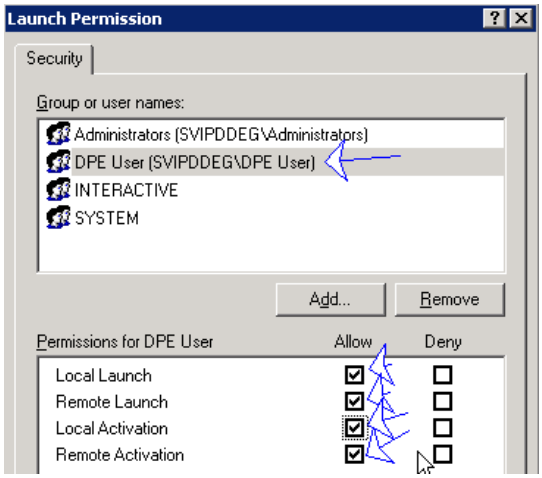

Figure 11: Launch Permissions

3.1.4 Windows Server 2003 SP1 (and newer) Policies Add-ons

With the introduction of Windows Server 2003 SP1, new DCOM policies have been introduced that determine who has the right to launch and access DCOM processes at the machine level. There are two methods to obtain these rights, dependent upon whether it is a domain or local group that is seeking launch or access rights.

For Domain Groups

The following is the recommended method when a domain group should obtain DCOM rights.

A new local group called 'Distributed COM Users' has been introduced in Windows 2003 SP1. By default, members of this group have the right to launch and access DCOM processes, therefore adding a user or domain group to this group provides the rights to launch and access DCOM processes on the server machine. To make a user or a domain group a member of the 'Distributed COM Users' group, perform the following steps:

1) Select **Start /Control Panel** from the Windows taskbar.
2) Start **Administrative Tools** in Control Panel view or menu.
3) Start **Computer Management** in **Administrative Tools** view.
4) Select **System Tools** for managing 'Local Users and Groups'.

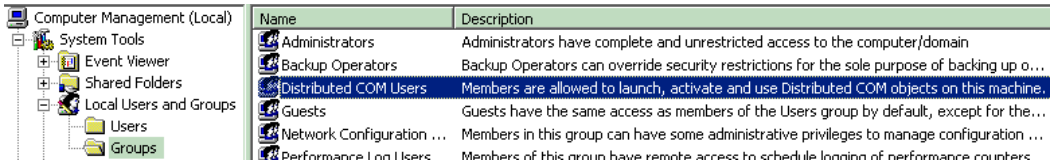

Figure 12: Distributed COM Users List Entry

5) Double click **Distributed COM Users** list entry. Add the user or domain group to the list of members in the displayed dialog box.

For Local Groups

When working with a local group, the following steps are required to obtain launch and access rights for DCOM processes on the server:

1) Start Local Security settings. (*Please refer to the* Launching Local Policies Configuration)
2) Select **Security Options** and edit DCOM Machine Access and Launch Restrictions.

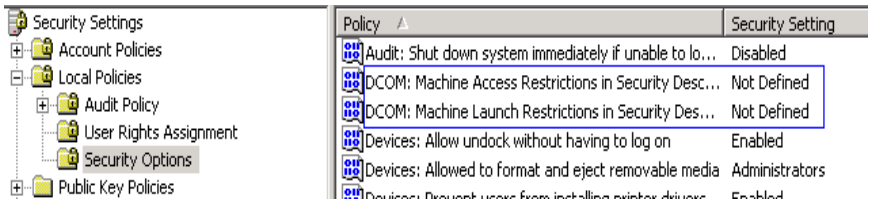

Figure 13: Security Options

3) Open **Properties** on DCOM: Machine Access Restriction.

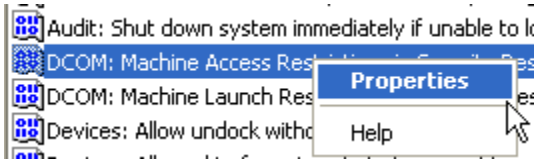

Figure 14: Open Properties

4) Press **Edit Security…**

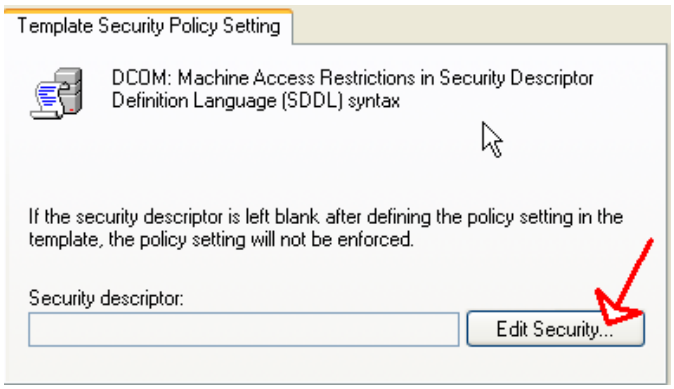

Figure 15: Template Security Policy Setting

5) Add group DPE User.

6) Allow Access from Local/Remote.

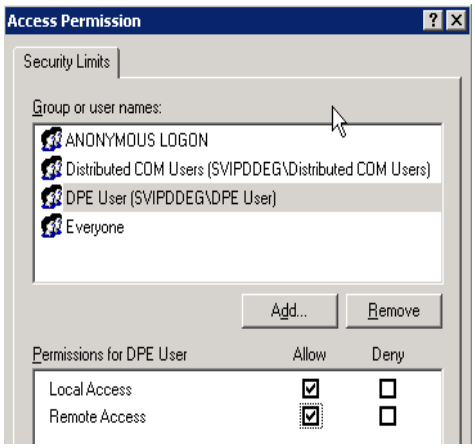

Figure 16: Access Permissions

7) Confirm with **OK** (two times).

8) Open **Properties DCOM: Machine Launch Restriction** …

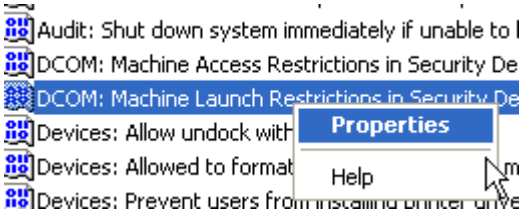

Figure 17: Properties DCOM: Machine Launch Restriction

9) Select **Edit Security…**

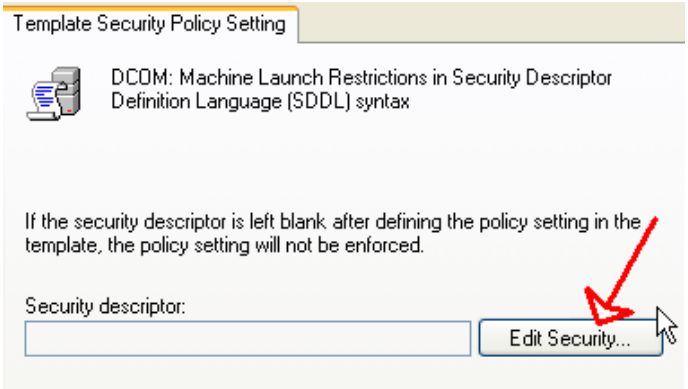

Figure 18: Template Security Policy Setting

10) Add group **DPE User** to user list in dialog.

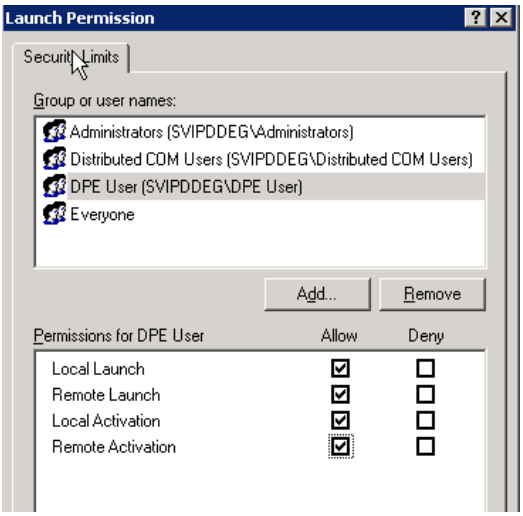

Figure 19: Add DPE User

11) Assign to **DPE User** group all permissions.

12) Confirm with **OK** (two times).

3.2 Working across Network Domains

In case the solution should run across Network Domain boundaries the client user account has to be known on the server machine. The options here:

- Work with trusted Network Domains.
- Create a Domain user with the same name/password combination in the server domain.
- Create a local user with the same name/password combination on the server machine.

In case a DPE Client is connecting to a server across Network Domain boundaries the same applies for the server process identity. It has to be known on the client machine.

Another alternative is not to work with enabled Authentication. *Please refer to the* Working with Disabled DCOM Authentication.

4. Working with Disabled DCOM Authentication

First step for running DCOM with a disabled Authentication is to set the registry value **DisableAuthentication** under **HKEY_LOCAL_MACHINE\SOFTWARE\DELMIA** to **1** (Default is 0). The flag has to be consistent on all server and client machines.

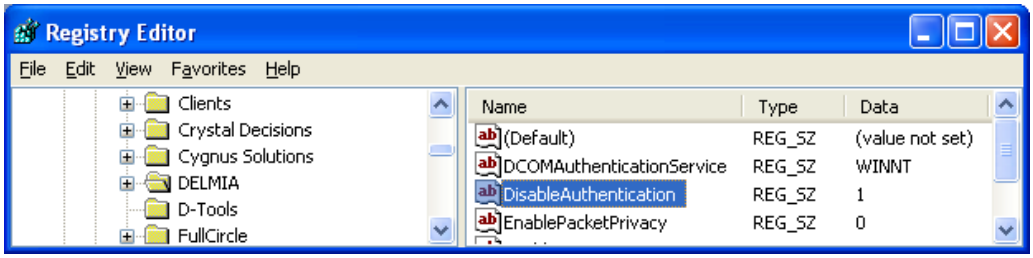

Figure 20: Registry Editor

4.1 Working with Disabled Authentication

- Novell network. For further information have a look on the DCOM Settings for Multiple Clients
- This discuss DCOM settings for multiple clients on Novell networks without a Windows Domain Controller chapter.
- When solution is setup over multiple network domains that run not as trusted domains. A disabled Authentication could provide in this case an easier way to administrate security through whole the solution.

4.2 Server Settings

4.2.1 Configure the User Identity of the Server Processes

The process identity of the server process has to be set up in the same way as with enabled DCOM Authentication. *Please refer to the* Working with Enabled DCOM Authentication.

4.2.2 Permissions on Server Processes

For connecting and accessing server processes by the client applications the Launch and Access Permissions have to be set up. For this purpose the DCOM Configuration Tool has to be started. *Please refer to the* Launching DCOM Configuration Tool section. In order to know which server processes to setup, *Please refer to the* "Customizing Server Processes".

Set Process Launch Permissions:

1) Select **Properties…** on each server process.
2) Select **Customize** and **Edit** to set Permissions. Exit the dialog with **OK**.

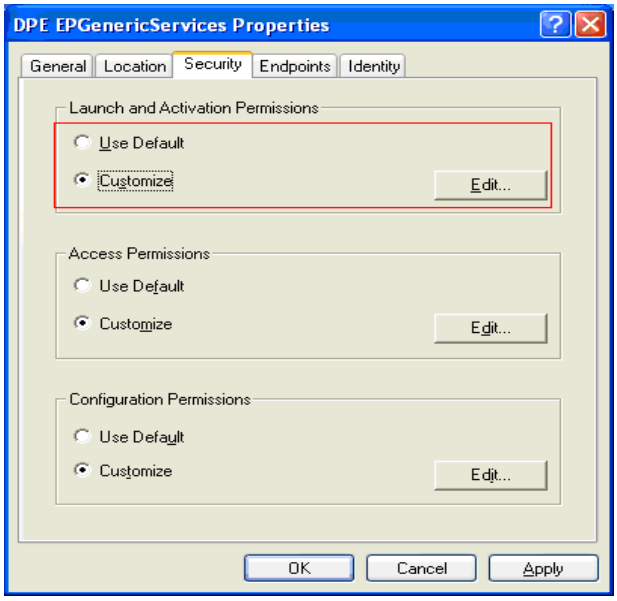

Figure 21: Set Permissions

3) Assign **Everyone** Group all Permissions:

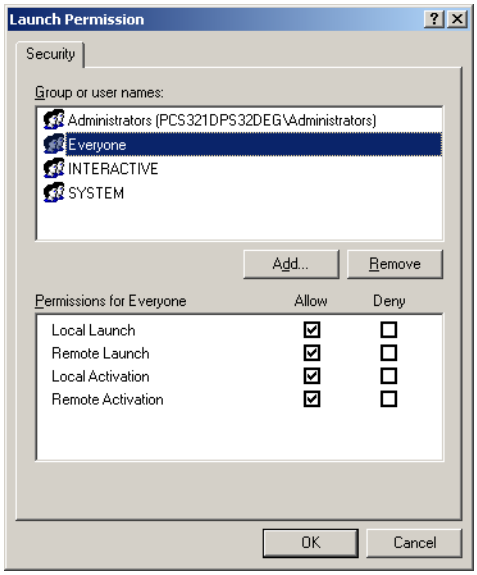

Figure 22: Launch Permissions

4.2.2.1 Set Process Access Permissions

1) Select **Properties…** on each server process

2) Select **Customize** and **Edit** to set the Permissions. Exit the dialog with **OK.**

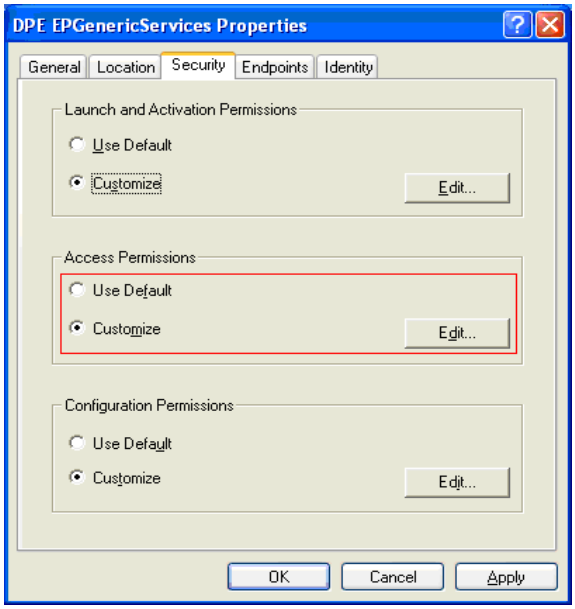

Figure 23: Access Permissions

3) Assign **Everyone** Group all Permissions:

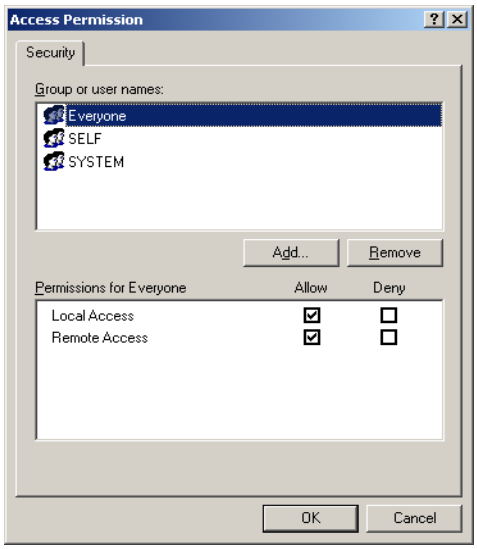

Figure 24: Assign Permissions

4.2.3 Windows Server 2003 (and newer) Policies Add-ons

4.2.3.1 Configure Network Access Permission on Machine Level

1) Start Local Security settings, for further information *Please refer to the* Launching Local Policies Configuration.

2) Navigate in the tree and select the Policy Network access: Let Everyone permissions apply to anonymous users.

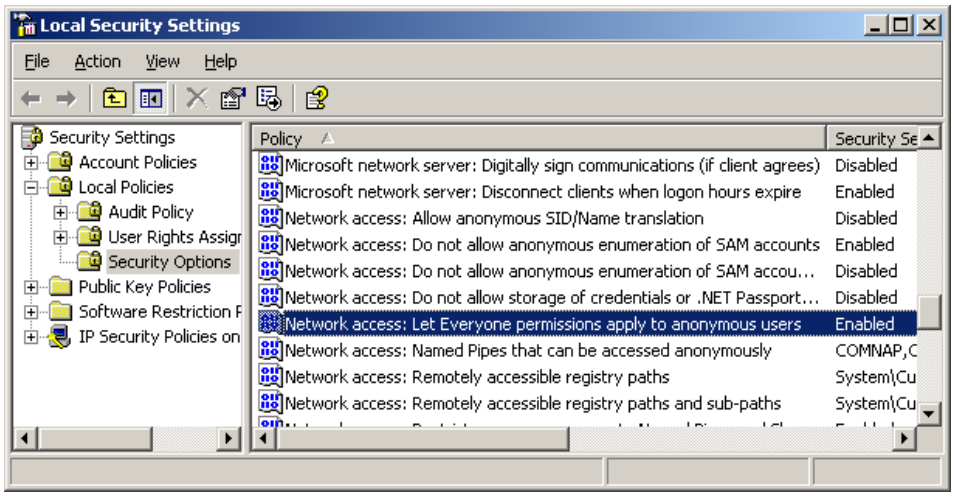

Figure 25: Local Security Settings

3) Start **Properties** Dialog by selecting **Properties…** in the context menu on the selected item.

4) Enable Security setting by checking the radio button. Exit the dialog with **OK.**

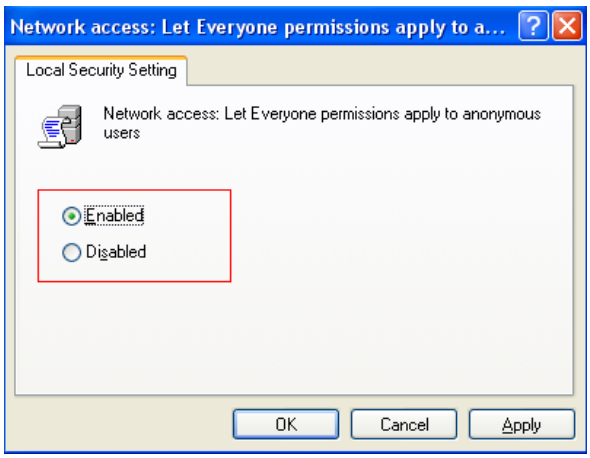

Figure 26: Enable Security Setting

4.2.4 Windows Server 2003 SP1 (and newer) Policies Add-ons

4.2.4.1 Set DCOM Launch and Access Permissions on Machine Level

With the introduction of Windows Server 2003 SP1 also new DCOM policies have been introduced. These policies control on a machine level, which is allowed to launch and access DCOM processes. For setting up these in an adequate way please refer to the following steps.

1) Start Local Security settings, for further information, *Please refer to the* Launching Local Policies Configuration.

2) Navigate in the tree and select the Policy **DCOM: Machine Access Restrictions…**

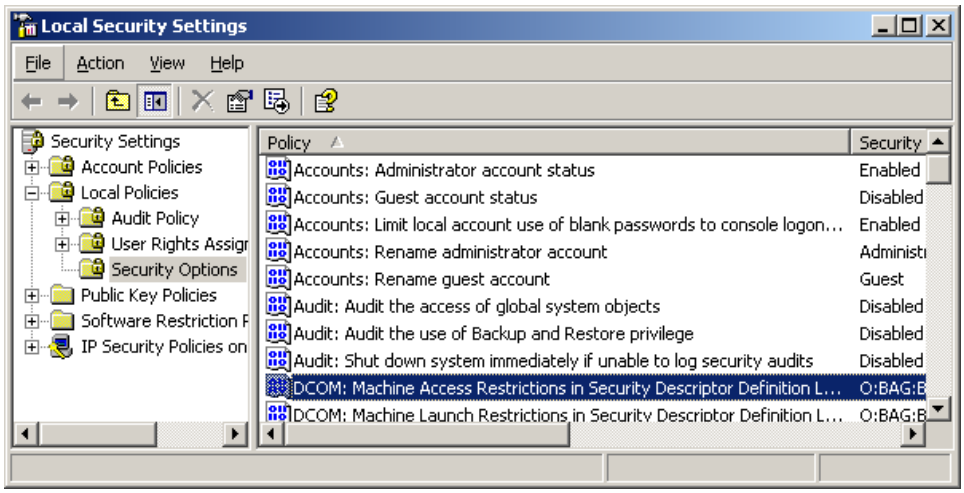

Figure 27: Local Security Settings

3) Start **Access Permission** Dialog by selecting **Properties…** in the context menu on the selected item.

4) Assign to **Everyone** and **Anonymous Logon** Group all Permissions and exit the dialog with **OK.**

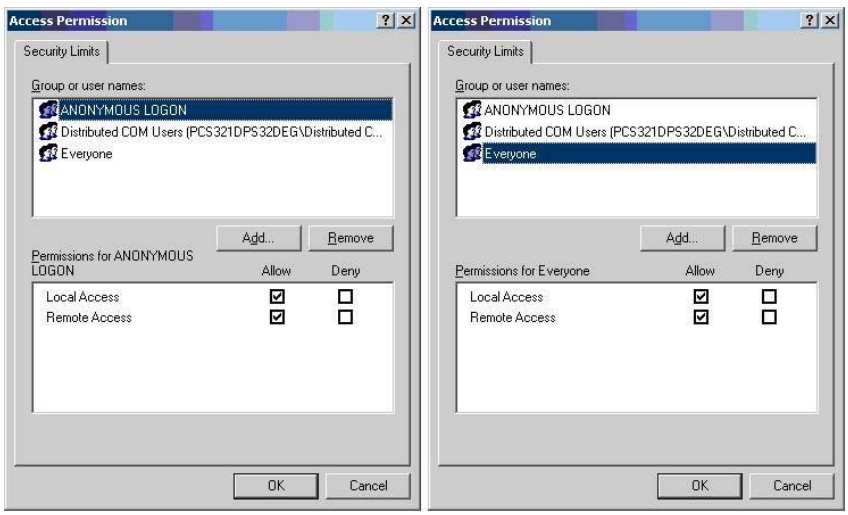

Figure 28: Access Permissions

5) Navigate in the tree and select the Policy **DCOM: Machine Launch Restrictions…**

6) Start **Launch Permission** Dialog by selecting **Properties…** in the context menu on the selected item.

7) Assign to **Everyone** Group all Permissions and exit the dialog with **OK.**

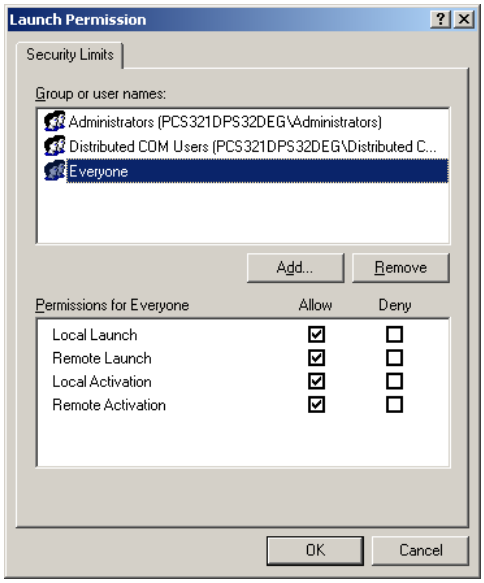

Figure 29: Launch Permissions

4.3 Client Settings

4.3.1 Windows XP SP2 Operation System add-ons

With the introduction of Windows XP SP2 also new DCOM policies have been introduced. These policies control on a machine level, which is allowed to launch and access DCOM processes. For setting up these in an adequate way please refer to the following steps:

1) Start Local Security settings, for further informations, *Please refer to the* Launching Local Policies Configuration.

2) Navigate in the tree and select the Policy **DCOM: Machine Access Restrictions…**

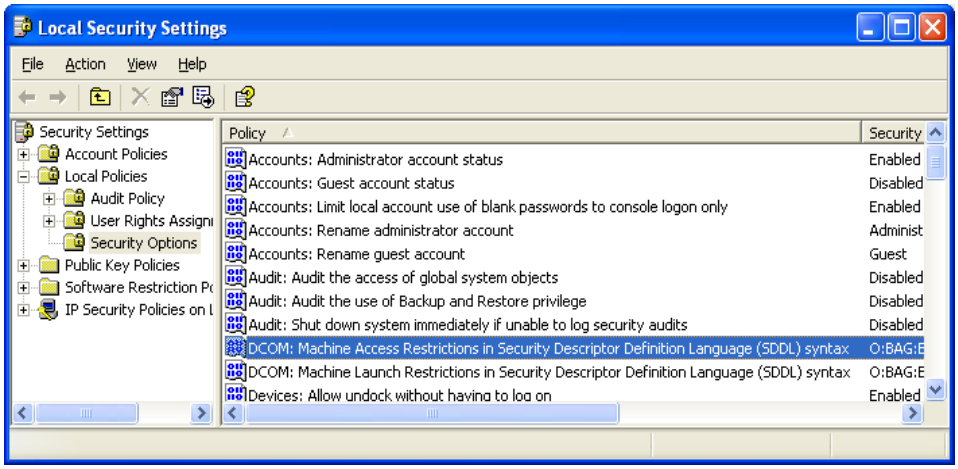

Figure 30: Local Security Settings

3) Start **Access Permission** Dialog by selecting **Properties…** in the context menu on the selected item.

4) Assign to **Everyone** and **Anonymous Logon** Group all Permissions and leave the dialog with **OK.**

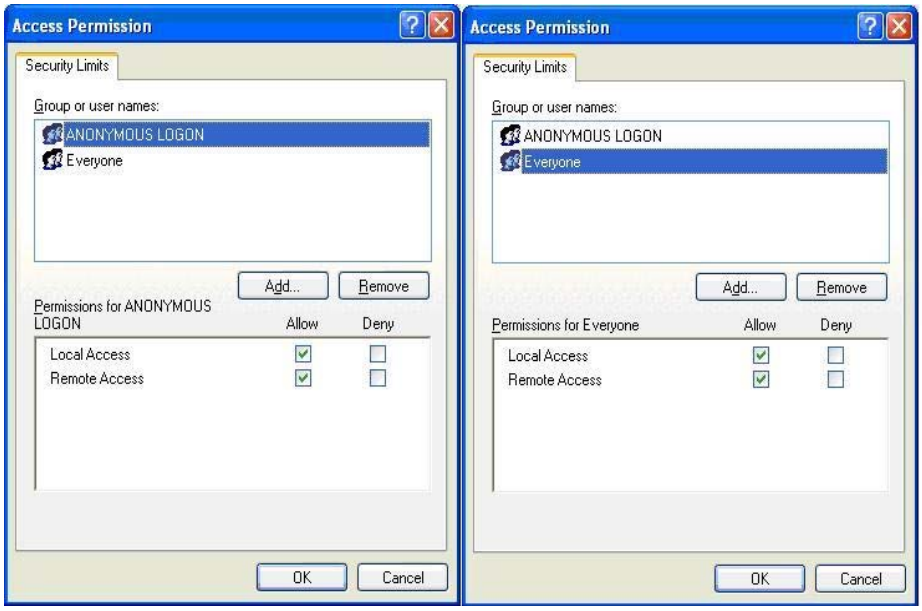

Figure 31: Access Permissions

5) Navigate in the tree and select the Policy DCOM: Machine Launch Restrictions…

6) Start **Launch Permission** Dialog by selecting Properties… in the context menu on the selected item.

7) Assign to Everyone Group all Permissions and leave the dialog with **OK**.

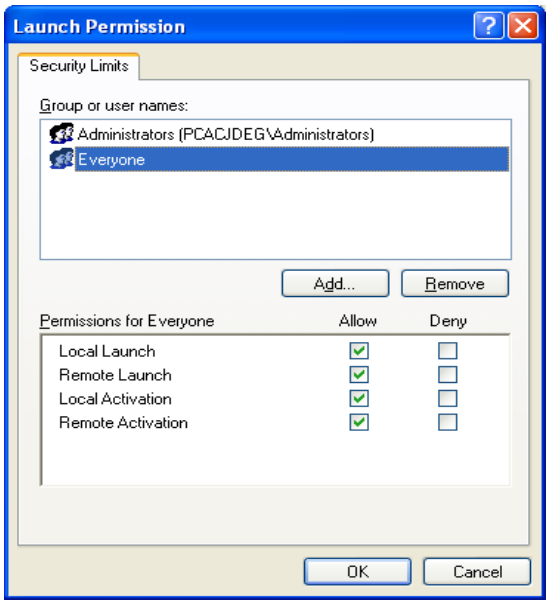

Figure 32: Launch Permission

5. Working with DCOM Encryption

By default, DCOM communication is not encrypted and sensitive data may be visible to non-privileged entities, i.e. when communication is routed through public or wireless networks. Therefore, DCOM allows configuring marshalling to be encrypted.

For running DCOM with encryption, an enabled DCOM Authentication is mandatory. In order to run DCOM with encryption all steps explained in the chapter Working with Enabled DCOM Authentication have to be fulfilled. Furthermore the registry value “EnablePacketPrivacy” under “HKEY_LOCAL_MACHINE\SOFTWARE\DELMIA” has to be set to “1” (Default is 0).

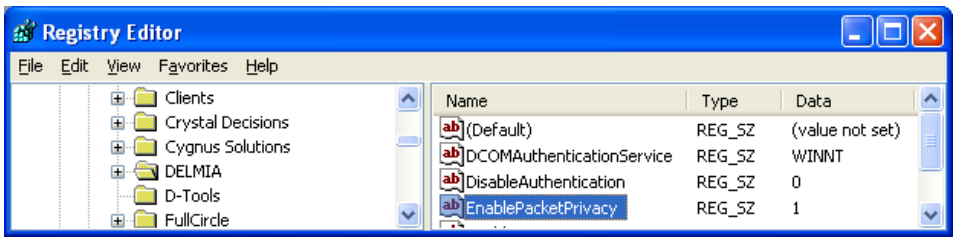

Figure 33: Registry Settings

In order to encrypt security relevant data it is mandatory to modify the server side “EnablePacketPrivacy” value. The change of this value on the client side is not needed.

As encryption algorithm RC4 with a key length of 128bit (supported by OS till Windows 2000 service pack 2 and newer) is used. This encryption algorithm is provided by the DCOM Authentication Service “NTLMSSP”.

6. Customizing Server Processes

The decision which server processes to setup depends from different aspects:

1) The following process have always to be customized:

- DPE PPRServer
- DPE Server Tools

2) On a **Master** server additionally the following processes have to be customized:

- DPE Pooling Server
- DPE Lock Manager
- DPE Update Manager

3) When working with DPM clients the **DPE EPGenericServices** process has to be customized on **Slave** and **Master**.

4) When working with **SSO** (Single Sign On) **the DPE EPSSOService** process has to be customized on **Slave** and **Master**.

5) When working with enabled **P&O Logging** or **Logging of Access to Export controlled data** additionally the **DPE EPLogger** process has to be customized (customer is free to decide where to run, on the Master only, on all server machines or …).

6.1 Assign Local Administrator Rights to a User

1) On server machine select **Start/Control Panel** from the Windows taskbar.
2) Start **Administrative Tools** in Control Panel view or menu.
3) Start **Computer Management** in **Administrative Tools** view.
4) Select **System Tools** for managing 'Local Users and Groups'.

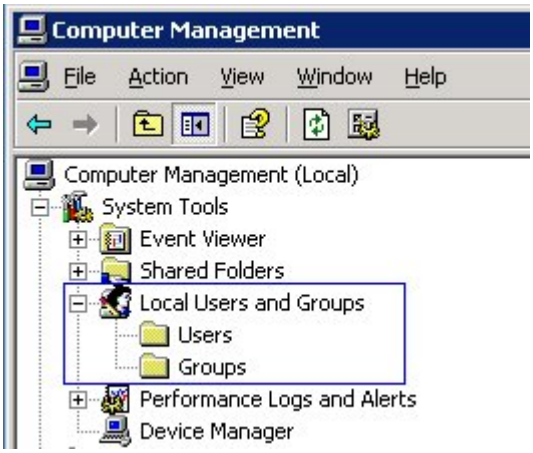

Figure 34: Computer Mnagement

5) Add Domain User here **DPE Admin** to group of 'Administrators' on server machine.

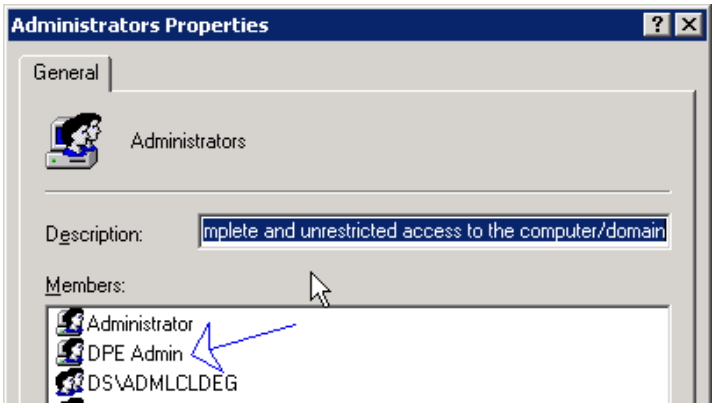

Figure 35: Administrator's Properties

6.2 Launching DCOM Configuration Tool

Windows XP and Windows Server 2003

1) Select **Start/Control Panel** from the Windows taskbar.
2) Start **Administrative Tools** in **Control Panel** view or menu.
3) Start **Component Services** in **Administrative Tools** view.
4) The **Component Services** window appears. Navigate through the Component Services tree as shown by the following picture. (When selecting the **DCOM Config** item confirmation dialog boxes may be displayed, asking you to accept some key numbers. Accept the numbers by selecting Yes in these dialog boxes).

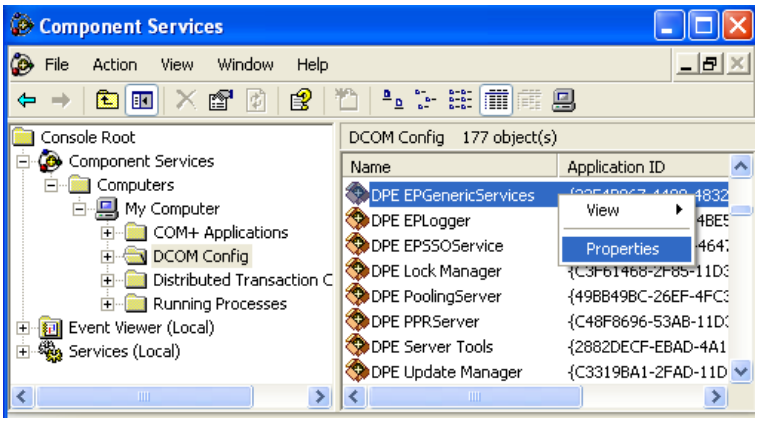

Figure 36: Componenet Services

Windows 2000

1) Select **Start/Run** from the Windows taskbar.
2) Enter the command "**DCOMCNFG**" in the Run dialog box, and click **OK** to launch the program (When DCOMCNFG is launched it may display a confirmation dialog box asking you to accept some key numbers. Accept the numbers by selecting **Yes** in these dialog boxes).
3) The **Distributed COM Configuration Properties** dialog box appears:

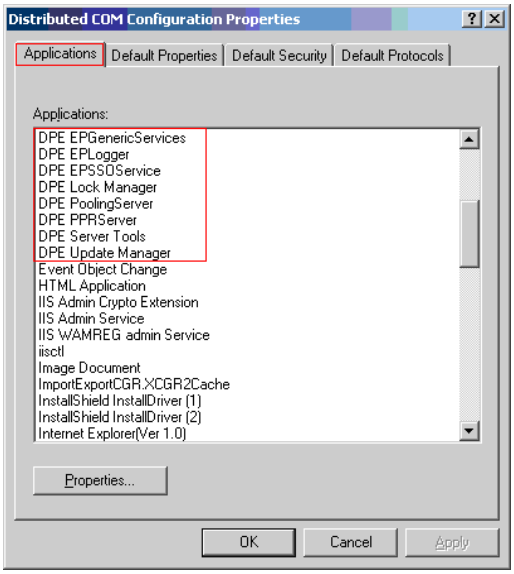

Figure 37: Distributed COM Configuration Properties Dialog

6.3 Launching Local Policies Configuration

1) Select **Start/Control Panel** from the Windows taskbar.
2) Start **Administrative Tools** in **Control Panel** view or menu.
3) Start **Local Security Policies** in **Administrative Tools** view.
4) The Local Security Policies window appears. Navigate through the Component Services tree as shown by the following picture.

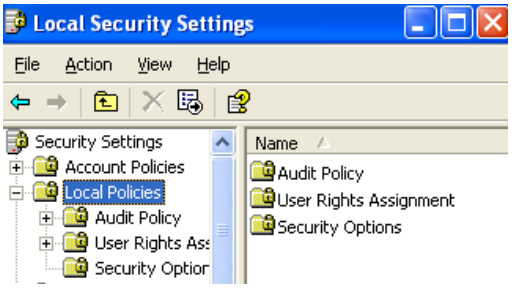

Figure 38: Local Security Settings

7. Enabling DCOM

By default, as shipped by Microsoft, DCOM is enabled on OS platforms. To enable DCOM on the OS the followings steps have to be performed:

1) Launch the DCOM configuration Too. *Please refer to the* Launching DCOM Configuration Tool.

Windows 2000

2) On **Windows 2000** you are now in the right dialog.

Windows XP/ Windows Server 2003

3) On **Windows XP/ Windows Server 2003** you have to navigate in the tree to **My Computer** item and select **Properties…**

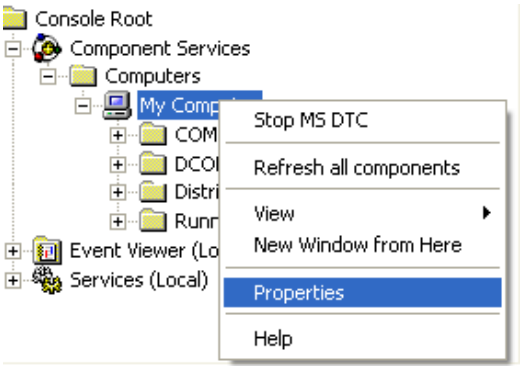

Figure 39: My Computer Navigation

4) Select the **Default Properties** tab and check if DCOM is enabled.

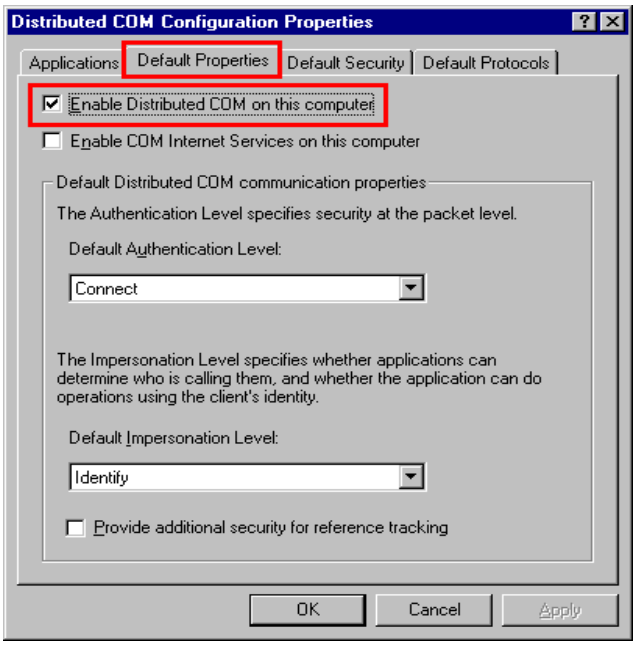

Figure 40: Default Properties Tab

8. Customizing Windows Firewall

An enabled Windows Firewall prevents by default the start of incoming connections. In the context of the DPE client an enabled Windows Firewall means customization effort is required. Otherwise the callbacks (First chapter) used by the solution will not work properly and Error messages rights after the Login appear.

For setting up a DPM client this section can be skipped. The DPM client works without callbacks therefore no customization effort is required here.

8.1 Disable Windows Firewall

1) Select **Start/Control Panel** from the Windows taskbar.
2) Start **Windows Firewall** in Control Panel view or menu.

Figure 41: Windows Firewall

3) Select Off in General Page in **Windows Firewall Properties** dialog.

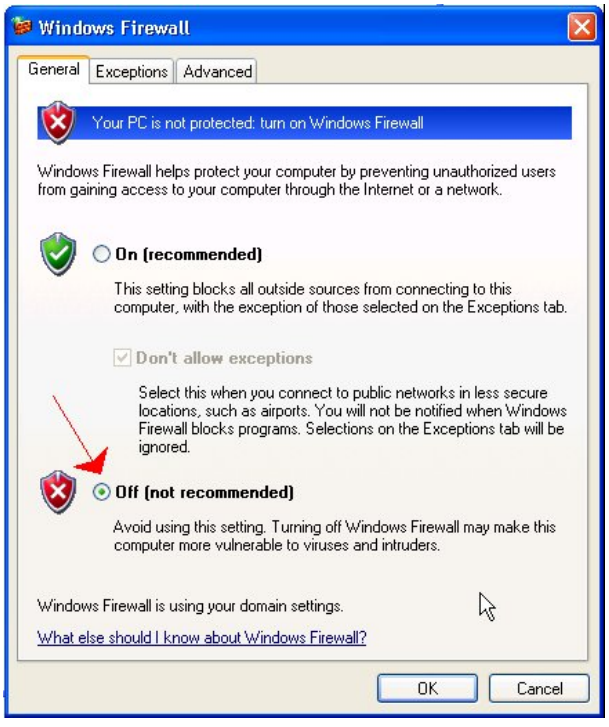

Figure 42: Windows Firewall Properties Dialog

8.2 Enable DPE Client to run on Windows XP SP2 with an Enabled Windows Firewall

1) Select **Start/Control Panel** from the Windows taskbar.
2) Start **Windows Firewall** in **Control Panel** view or menu.

Figure 43: Windows Firewall

3) Select **On (recommended)** in General Page in **Windows Firewall Properties** Dialog.

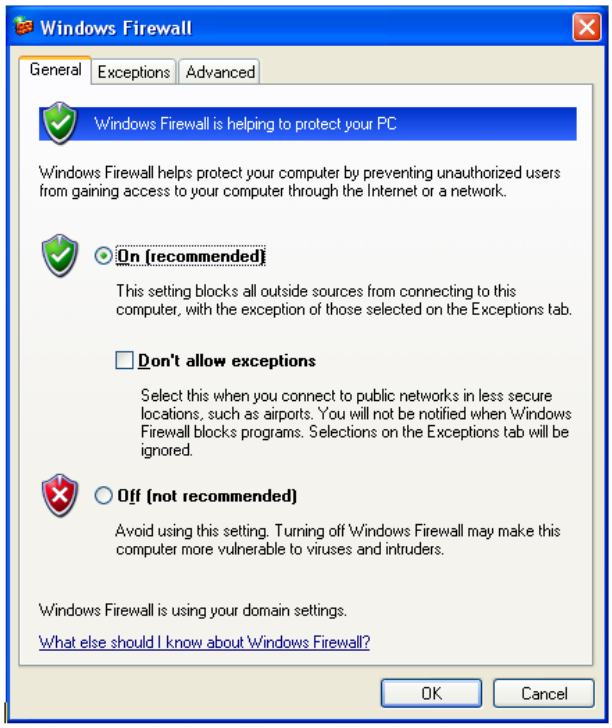

Figure 44: Windows Firewall Dialog

4) Press button **Add Port**…
5) Enter as port name: DCOM.
6) Enter as port number: 135.
7) Select TCP protocol and confirm with **OK**.

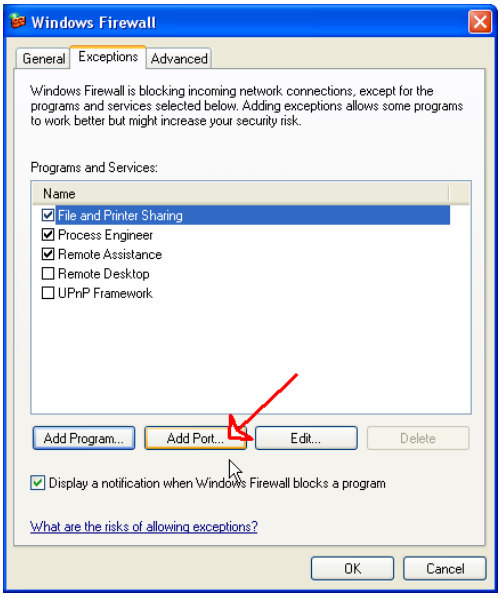

Figure 45: Add Port

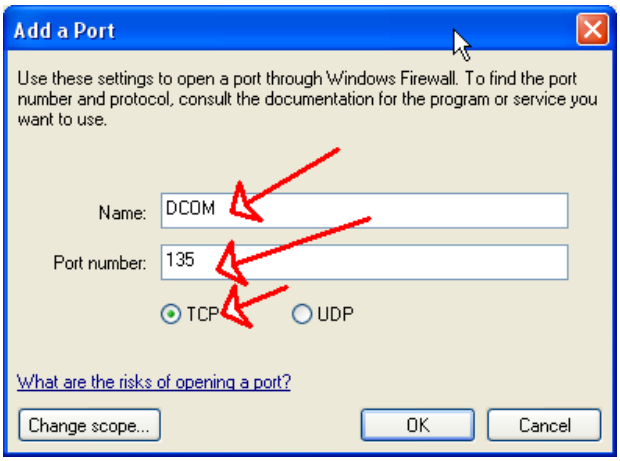

Figure 46: Add a Port

8) Go to page Exceptions and press Button '**Add Program**…' and select Process Engineer [DPFFrame.exe] in list of programs.

9) Confirm with **OK**.

Note

If you want to use DPE Balancing application; add also EPBalancing.exe in exceptions list.

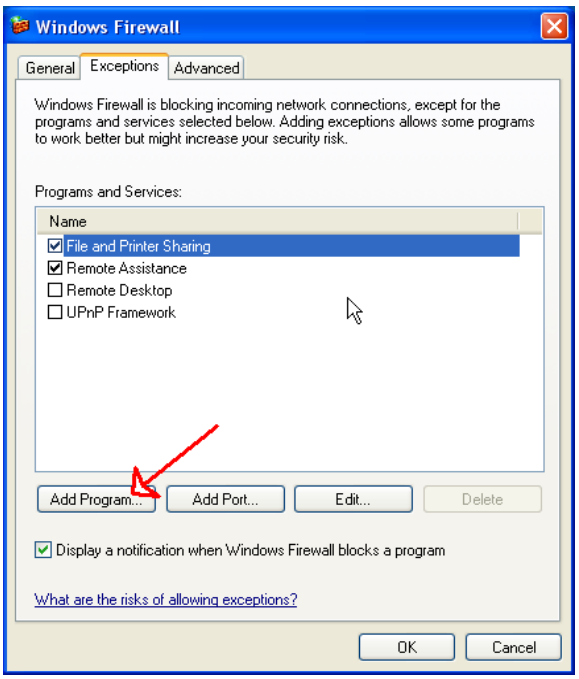

Figure 47: Add Program Button

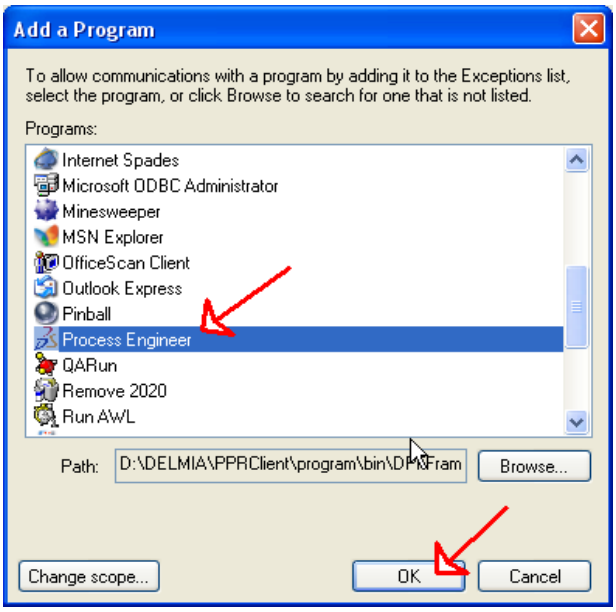

Figure 48: Add Program Dialog

10) Please confirm that DCOM and Process Engineer is set to true in list of exceptions

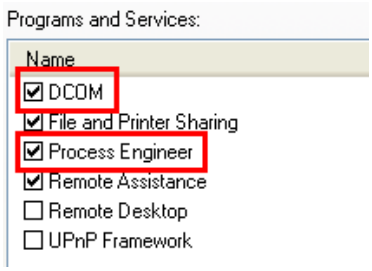

Figure 49: Programs and Services

8.3 Enable Server Processes to run on Windows Server 2003 SP1 with an Enabled Windows Firewall

For the setup of the Server Processes on Windows Server 2003 SP1 with enable Windows Firewall the same steps are required, as for the DPE client on a Windows XP SP2 with enable Windows Firewall. The only difference is, instead of customizing exceptions for Process Engineer and the Balancing module you have to customize exceptions for the server process.

For which server processes you need to configure exceptions, *please refer to* the Customizing Server Processes

Example DPE PPRServer (…*PPRServer\program\bin\IPDServer.exe*)

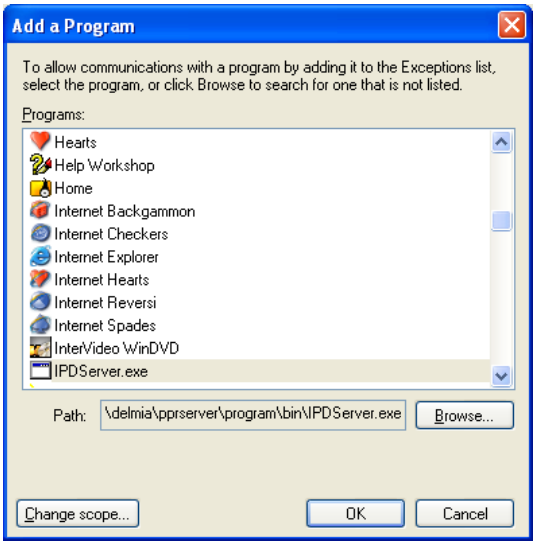

Figure 50: Add a Program

Installation paths for the remaining server process:

- DPE Server Tools (…\PPRServer\program\bin\epservertools.exe)
- DPE Pooling Server (…\PPRServer\program\bin\eppoolingserver.exe)
- DPE Lock Manager (…\PPRServer\program\bin\LockMng.exe)
- DPE Update Manager (…\PPRServer\program\bin\UpdateMng.exe)
- DPE EPGenericServices (…\PPRServer\program\bin\epgenericservices.exe)
- DPE EPLogger (…\PPRServer\program\bin\EPLogger.exe)
- DPE EPSSOService (not used remote, no customization required)

Note

Do not forget to setup the exception for the port 135.

8.4 Enable DPE Client to run on Windows7 with an Enabled Windows Firewall

1) Windows firewall needs to be turned ON.

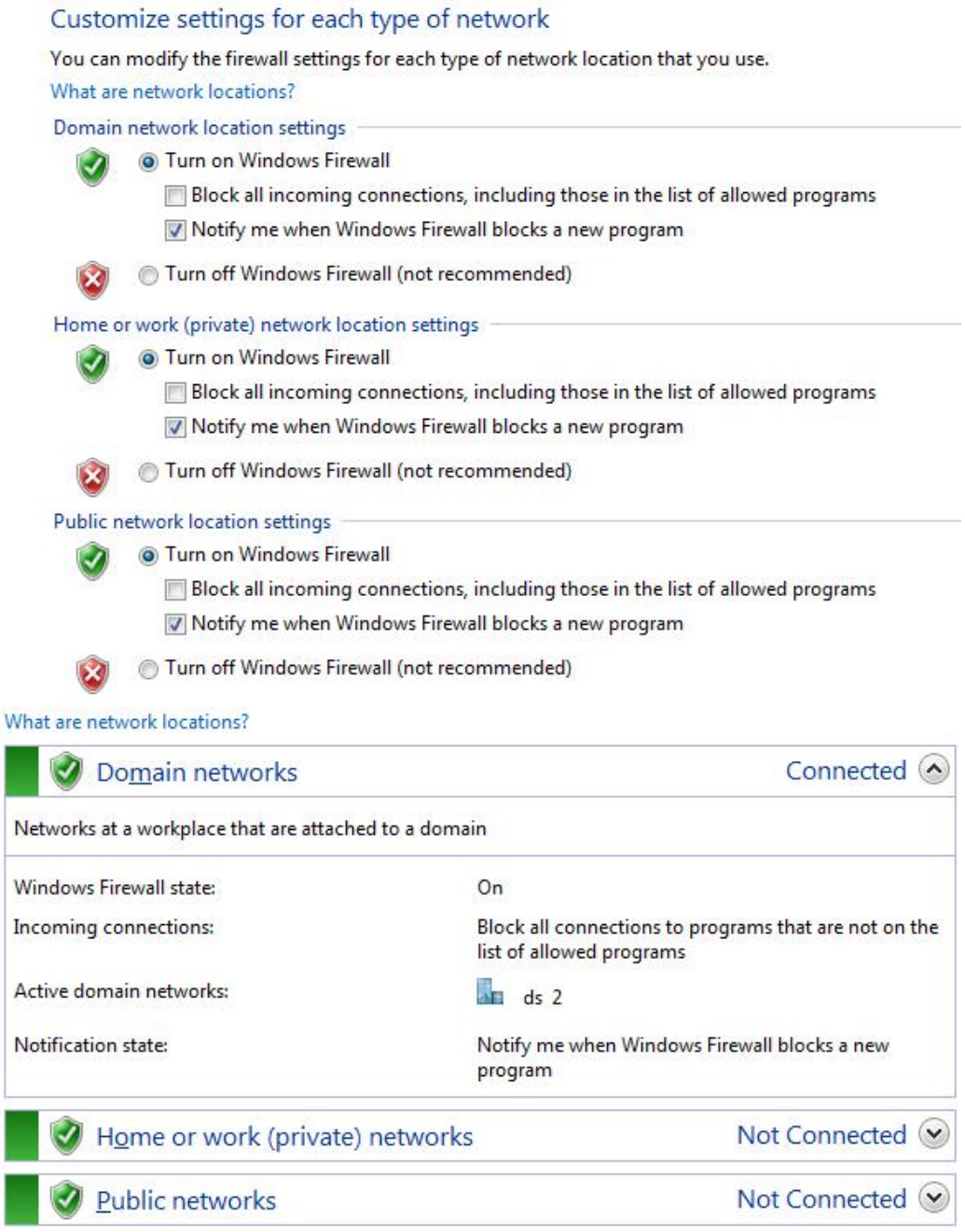

Figure 51: Turn On Windows Firewall

2) Add DPE Process Engineer in the exception list which is allowed to communicate through windows firewall.

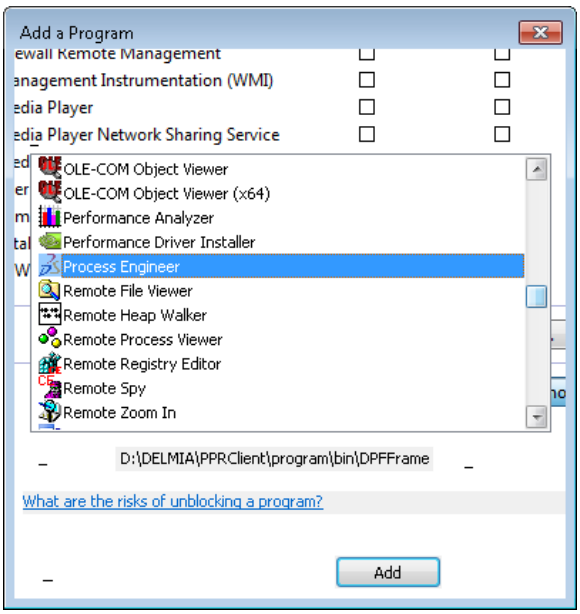

Figure 52: Add DPE Process Engineer in the Exception List

3) Make sure Remote Assistance (process named svchost.exe) is also enabled in the exception list which is allowed to communicate through windows firewall and DCOM port 135 added.

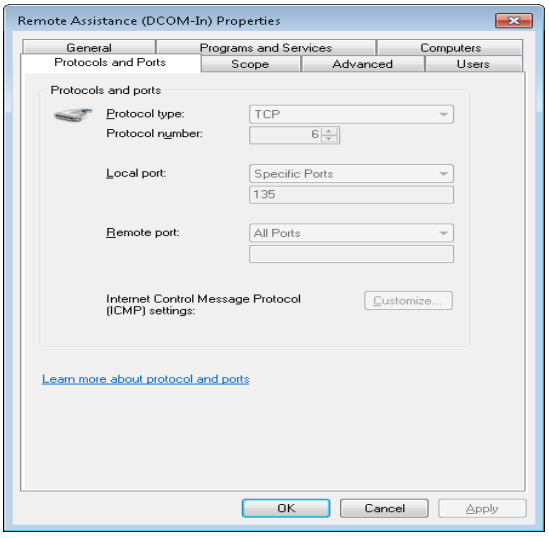

Figure 53: Remote Assistance (process named svchost.exe) must be Enabled in the Exception List

Note

If any connection problem noticed cross check in Windows advance firewall settings then the inbound rules shown below get enabled.

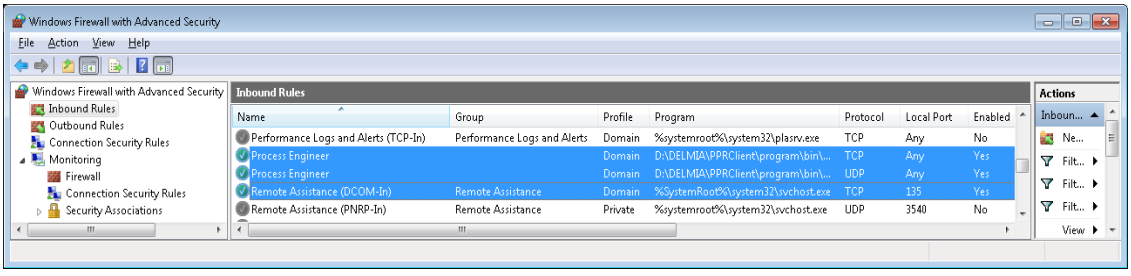

Figure 54: Inbound Rules

9. Checklist for Connection Problems

The settings explained here in this section are shipped by Microsoft by default in a way which allows our solution to work. This is the reason, why they have not been mentioned in the previous chapters.

Prerequisites are:

1) DCOM has to be enabled on Client and Server side (By default it is enabled).

2) With Windows XP SP2, Windows Server 2003 SP1 and Windows Server 2003 64 Bit a **Windows Firewall** is shipped with the OS. The standard for Windows XP SP2, when it is installed, is an enabled Firewall. For the other mentioned OS it is disabled. Our solution is by default not able to run over Firewall. Therefore, you have two options disable the Firewall or Customize the Firewall to run with the solution.

3) The computer has to be accessible from network (The setting need to be fulfilled for server machines always, for client machines in case DPE client is running on)

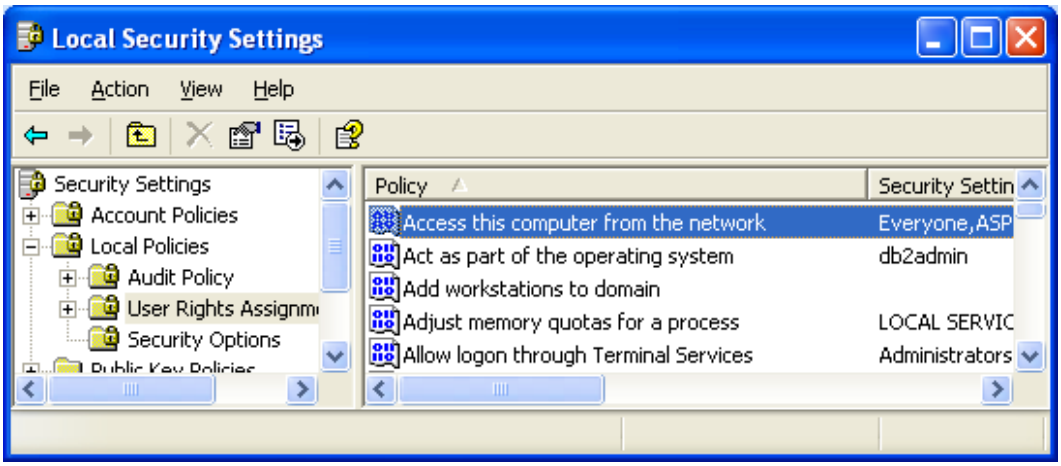

Figure 55: Local Security Settings

This setting has to be consistent with the **Deny access to this compute from network** setting:

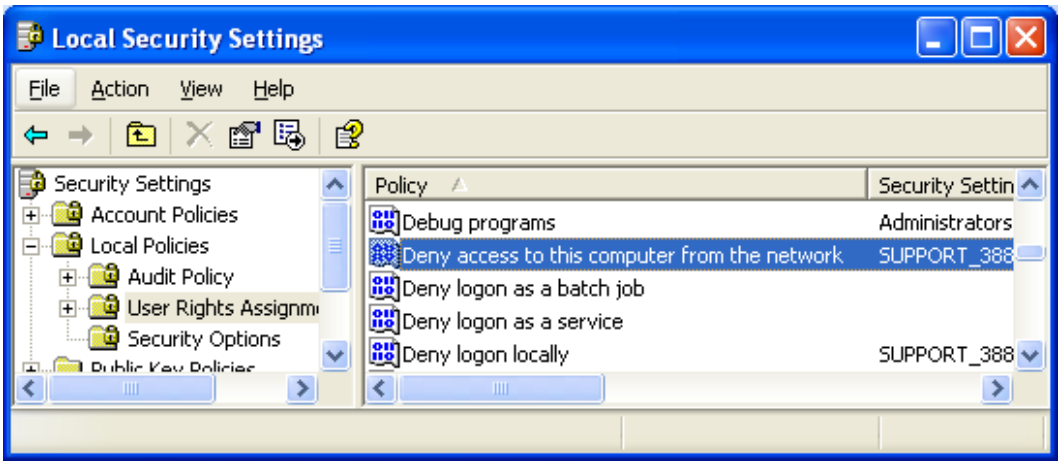

Figure 56: Deny Access to this Compute from Network Setting

4) The user identity under which the server processes run has to have right to **Log on as a batch job** (By default, when the identity of the first

process is set in the DCOM configuration, the user is added to list of users that have this right)

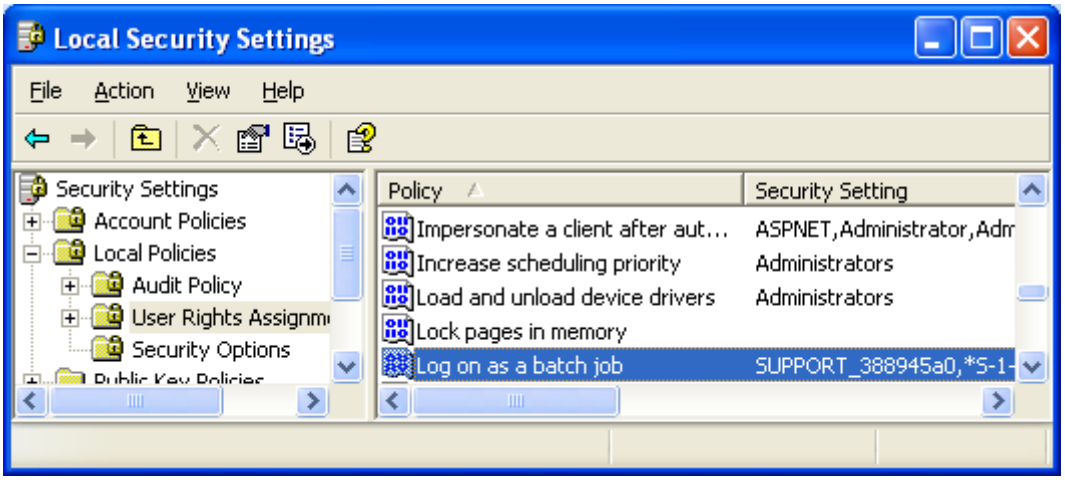

Figure 57: Log on as a Batch Job

This setting has to be consistent with the **Deny log on as batch job** setting:

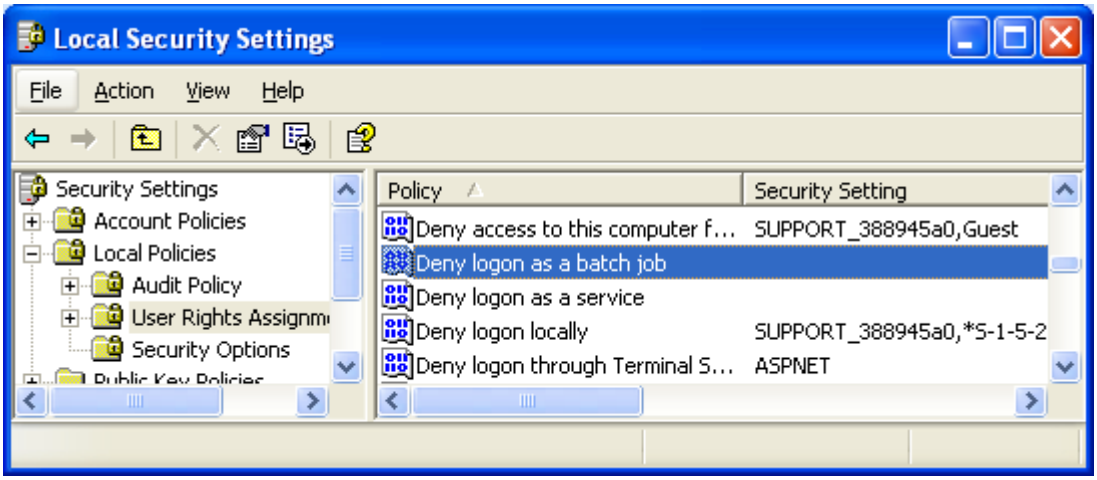

Figure 58: Deny Log on as Batch Job Setting

10. DCOM Settings for Multiple Clients

This discuss DCOM settings for multiple clients on Novell networks without a Windows Domain Controller.

Since there is no domain when working in a Novell environment, there is no domain user available. In this case, a local user on the PPR server must be authorized to launch DCOM processes.

- In this case, the user for DCOM identity stays the same.
- On the clients, this user must be created. This means that if a local user "DELMIA_DCOM" (for example) is used for DCOM identity on the server, a user "DELMIA_DCOM" must be created with the same password on each PPRClient.

This solution is possible in Windows domains if there is no domain user available. For example:

- username: **dpe5**
- password: **dpe5**

In a Novell network without a Windows Domain, the user dpe5 (in this example) must exist on the server machine as a local user with administrator privileges and on all clients as a local user with the same password as on the server.

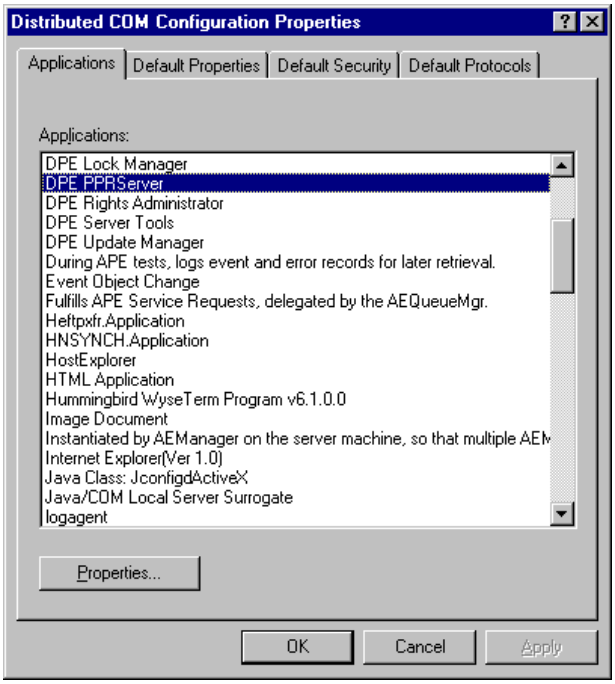

Figure 59: Distributed COM Configuration

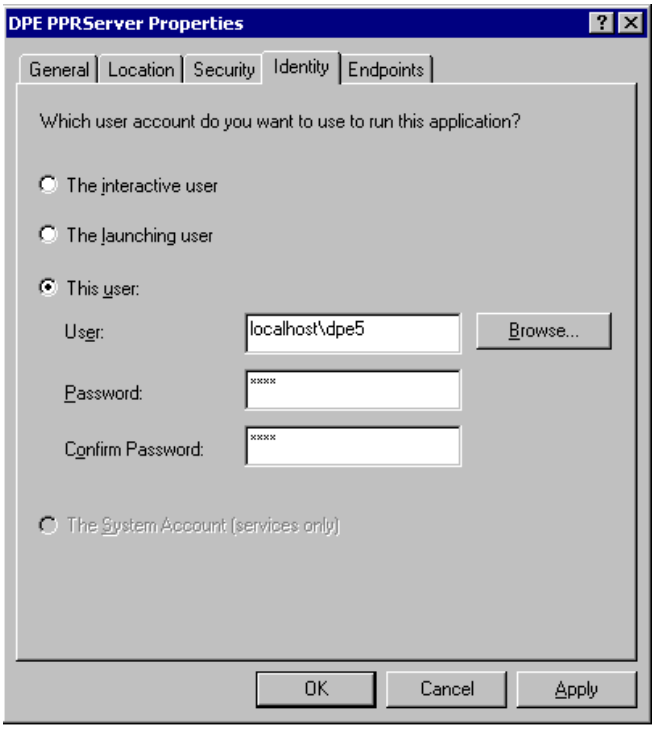

Figure 60: DPE PPR Server Properties

1) On the client machines, the user **dpe5** with password **dpe5** must also be created:

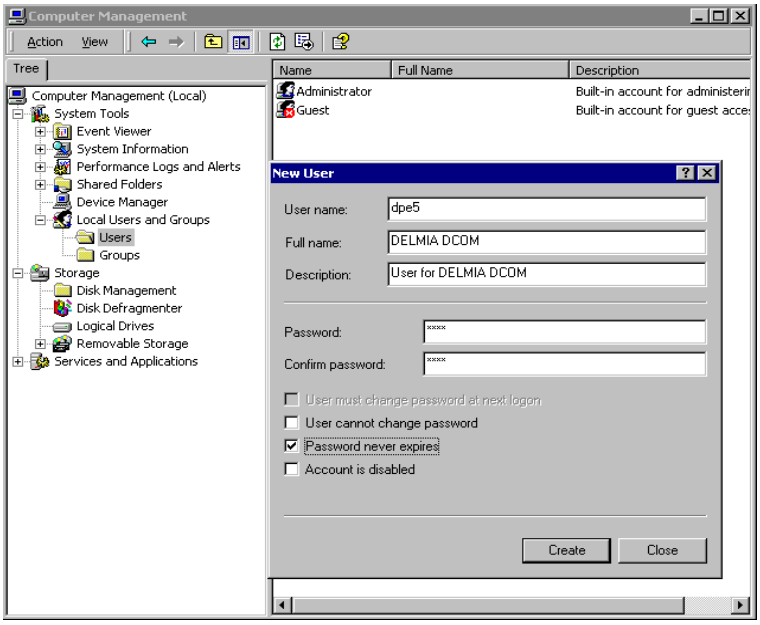

Figure 61: New User

10.1 Authentication

For authentication from server to client, an additional policy for accessing the client must also be set.
On Windows, select
`User management/Policy/User Rights/Access this computer from network/Add/user "dpe5"` (the DCOM identity user):

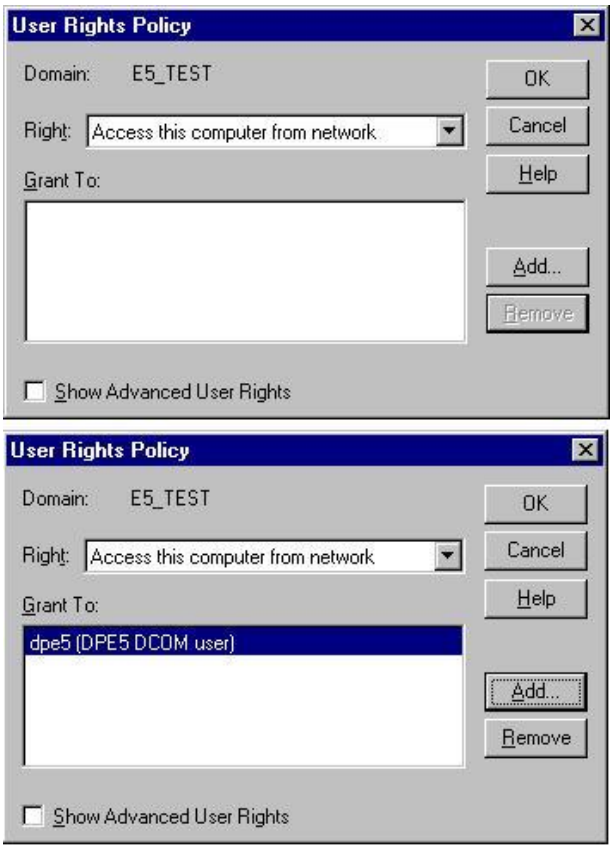

Figure 62: User Right Policy

Note

The dpe5 username and password are only used as examples in the scenario above. Any name may be used; however it is important to use the same username and password for the client, server and DCOM-identity on the server.

11. DCOM HTTP Tunneling

11.1 General

In order to use DCOM HTTP Tunneling several installation requirements to activate MS CIS (COM Internet Services) and RPC over HTTP must be followed (details see section setup and client and server machine configuration below).

The new connection modus has to work using the COM garbage collector. Connecting a client has to receive an interface to a connection object, as long as the connection object exists the connection is valid. As soon as the connection object is destroyed, either by release from the client or by the COM Garbage Collector, the connection object has to kick of the normal server deregister mechanism.

DCOM HTTP-Tunneling can only be used for client-server connections. Connections between server processes on several machines (DPE Master/Slave) cannot be tunneled. Considering this scope a firewall protection allowing only traffic on HTTP port 80 is installed between client and server. If a firewall has to be placed between several server machines it must allow all DCOM port traffic. Respecting security requirements the location of several server machines within the company network should be choose carefully.

Using HTTP-Tunneling has an impact on the DPE system performance depending on the kind of data transferred over the client server connection and the network latency time and bandwidth.

Functional Changes Server

For the new connection modus additional points have to be ensured:

1) Disable the periodical check of the server to ensure if client is still alive.
2) Disable the server termination notification mechanism. The server notifies client about the server termination or the termination done via the ServerTools.
3) Disable the HasCommitToBeDone mechanism. Server notifies client about to change status of the Save button (disabling and enabling Save button).

Functional Changes Client

In the EPIPDClient module provide a possibility to connect to server using the new connection modus.

4) Disable registration of server callback in the UpdateDispatcher module.
5) Disable registration of update callback in the ConfigfactoryCache module. In generally this means that as long as clients are connected to the system no changes to customization data are allowed.

Clients that use COM HTTP Tunneling do not receive

- Update messages.
- Notifications about the termination of server.
- Notifications about the termination of their transactions via ServerTool.
- No com objects created on client side cannot be passed to the server.
- The Auto relation asynchrony callback mechanism can’t be used.

- If the client is remotely terminated from the ServerTools-Client, it does not receive a confirmation message after disconnecting from the PPR server. The PPR client will only recognize the disconnection status if the user tries to fetch data which are still not cached on client side or if calling other server functions directly. In this case the client will display an error message indicating an invalid transaction.

Functional changes ServerTools-Client

The ServerTools-Client can be switched to a callbackless connection mode by registry:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Delmia\EPServerToolsUI

entry: connectionmode

value:

0 – using callbacks for a non-tunneled server connection

1 – callbackless server connection supporting HTTP-Tunneling

Restrictions for connectionmode = 1:

- The ServerTools-Client does not support the interactive client termination, instead the immediate termination of the server connection is proceeded. ServerPool and Machine nodes in the navigator tree are not updated automatically.
- A lower updating frequency for the server process view and the load index view is used:
  low: 6 sec.
  normal: 3 sec.
  high: 1 sec.

➢ The ServerTools-Client does not support the interactive client termination, instead the immediate termination of the server connection is proceeded

➢ ServerPool and machine nodes in the navigator tree are not updated automatically

➢ Lower updating frequency for the server process view and the load index view

➢ The Process Monitor view and the PoolingServer LoadMonitor view are refreshed only in the active window – to actualize data in inactive views these windows must be set as foreground window first.

11.2 Setup

If DCOM-HTTP Tunneling should be used for a client server connection, the following system requirements must be fulfilled:

11.2.1 System Requirements

11.2.1.1 Client Machine

- Windows2000 Workstation

11.2.1.2 Server Machine

- Windows2000 Server
- IIS 5.0 (Internet Information Server)
- RPC-Proxy installed

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/cis.asp

Consider installation and configuration of system internet components (MS Internet Explorer) may affect proceeding of HTTP tunneled DCOM RPC calls:

Known influences are:

- Proxy Server for Internet Explorer (security and server domain name resolution)
- Configuration of the Default Webpage in IIS
- PPC-Proxy configuration in IIS (access permissions)

11.2.2 Client and Server Machine Configuration

The DCOM HTTP-Tunneling is supported by Windows 2000 and must be activated on each client and server machine. To activate the Tunneling communication protocol the DCOM configuration tool dcomcnfg.exe is used. After opening dcomcnfg.exe in the property tab ‘standard protocols’ the DCOM protocol ‘Tunneling TCP/IP’ must be added. The protocol order is different for a client and a server machine:

Protocol Order Client Machine

- Tunneling TCP/IP
- Connection oriented TCP/IP
- Other protocols

Protocol Order Server Machine

- Connection oriented TCP/IP
- Tunneling TCP/IP
- Other protocols

For a server machine the Tunneling protocol must be listed below the TCP/IP protocol because communication between server processes does not support

Tunneling. The communication protocol will be selected by the first protocol match for the communication partners.

In the dcomcnfg property tab ‘standard properties’ the check box:

Activate COM Internet Services on this computer

1) Must be enabled.
2) After setting up the DCOM protocols the system must be rebooted. More information about the DCOM Tunneling configuration:

Client Machine

http://support.microsoft.com/default.aspx?scid=kb;en-us;265340

Server Machine

http://support.microsoft.com/default.aspx?scid=kb;EN-US;282261

The DCOM standard protocol setup is effective for all DCOM components of the machine. Setting up the machine standard protocol list is the only valid configuration for client and server machines.

11.2.2.1 Client Specific System Configuration

- If using a Proxy Server (Internet configuration), it must be configured to allow HTTP connect on port 80 without authentication.
- To establish a http tunneled server connection, the client must be able to resolve the server domain. The server domain name resolution can be provided by a domain name server or can be registered in the Windows system32 HOST file. The name resolution can be checked by typing <server_machine>.<domain>
- In the MS Internet Explorer – the server default web page should be displayed. Consider the proxy server configuration for the availability of the server domain resolution.
- Copy registry key “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings” to “HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings” and “HKEY_USERS\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings”

11.2.2.2 Server Specific System Configuration

1) The connection timeout in the IIS Default Webpage must be specified high enough to cover the actual network availability (minimum 300second).
2) The RPC-Proxy must be listed as ISAPI-Filter for the server machine in the IIS (configured by the Windows2000 COM Internet Services Proxy installation of Networking Services).
3) The DCOM security settings for the DPE server processes remain valid if DCOM Tunneling is used and must be set equally for all server processes as described in the DPE DCOM security configuration.
4) Add the following registry entry
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy
   Entry: “AllowAnonymous”
   Type: DWORD Value
   Value: 00000001

For more information *please refer*:
http://support.microsoft.com/kb/833003/en-us

5) Check the registry entry "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy\ValidPorts" value should be configured as follows :
<Server-name>:593;<Servername>.<Domainname>:593;<ServerIPAddress>:593;<Servername>:100-5000;<Servername>.<Domainname>:100-5000;<ServerIPAddress>:100-5000.

6) Replace <…> with the actual names.
<ServerIPAddress> is IP address of the server machine.

11.2.3 Example

A WAN with a firewall has to be simulated or installed to test the new connection scenario. Also a V5 client has to be provided that uses the new method.

To test the HTTP tunneled client server connection, the firewall placed between client and server has only to allow traffic on port 80. It is not possible to install a firewall between several server machines – the inter-server communication cannot be tunneled. If a firewall must be installed between two server machines the normal DCOM traffic must be allowed. The V5 client should load, save, and do all operation that normally works.

To prepare the Test DCOM HTTP Tunneling must be activated on all client and server machines. Tunneling must be activated on the Windows system and additionally the E5 client installation must be switched for Tunneling usage.

To check if the RPC-Proxy is installed in the server machine, in the IIS console (Windows administration -> Internet Information Services) within the standard web page entry, a node RPC must be displayed with an entry *rpcproxy.dll*.

From the client machine, the default web page of the IIS on the server must be accessible - to check server access open the Internet Explorer on the client and enter:

- <server_name>.<server_domain>
- (replace <...> with the names)
- The default webpage (e.g. 'under construction') should be displayed.

Enable DCOM Tunneling mode in the PPR client installation by setting the registry entry 'connectionmode'

- HKEY_LOCAL_MACHINE\SOFTWARE\Delmia\ergoplan\ connectionmode = 1
- HKEY_LOCAL_MACHINE\SOFTWARE\Delmia\EPServerToolsUI\ connectionmode = 1

Enable Windows DCOM Tunneling protocol on the server machine:

1) Open dcomcnfg.exe on the server machine.
2) Select standard protocol tab.

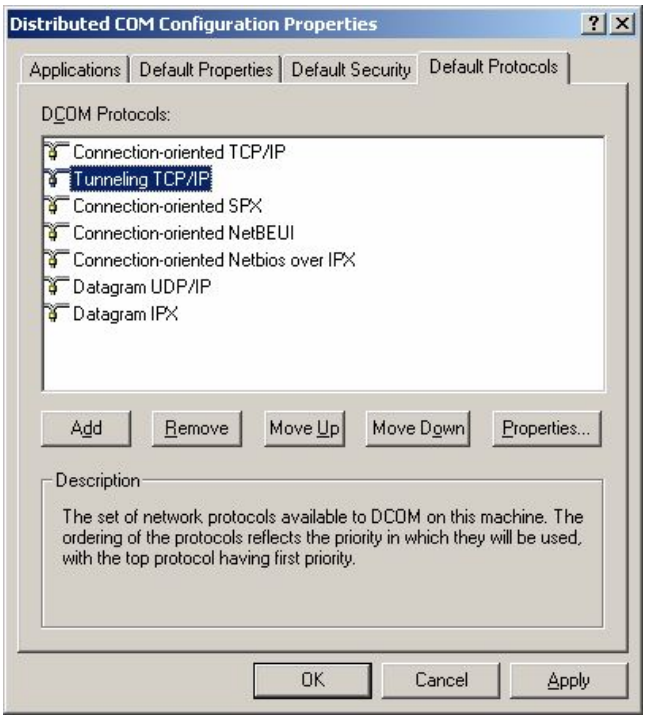

Figure 63: Protocol Tab

3) Add the protocol 'Tunneling TCP/IP'.

4) Move the Tunneling protocol on second position after 'Connection oriented TCP/IP'.

5) Select **Default Properties** tab:

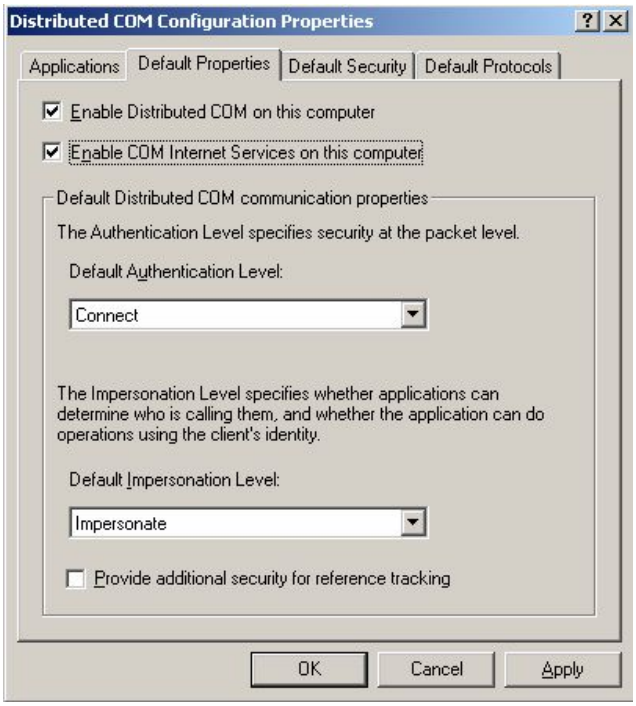

Figure 64: Enable Checkbox Activate COM Internet Services on this Computer

6) Enable checkbox '**Activate COM Internet Services on this computer**'.

7) Reboot the server machine.

- More information in: http://support.microsoft.com/default.aspx?scid=kb;EN-US;282261.

Enable Windows DCOM Tunneling protocol on the client machine:

8) Open *dcomcnfg.exe* on the client machine.

9) Select standard protocol tab.

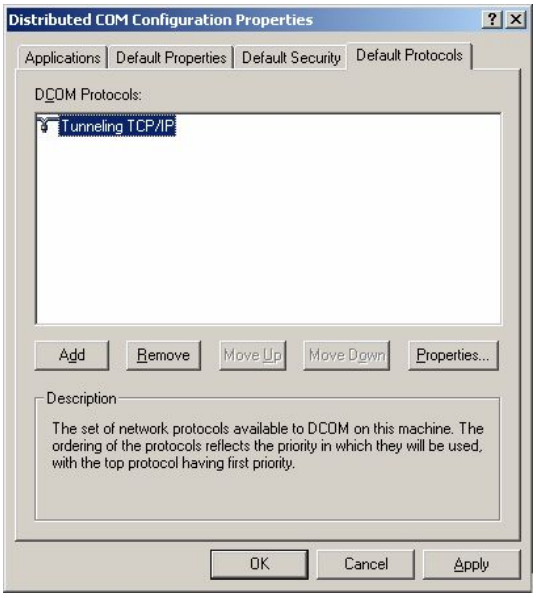

Figure 65: Enable Windows DCOM Tunneling Protocol

10) Add the protocol 'Tunneling TCP/IP'.

11) Move the Tunneling protocol on top position.

12) To be sure that no other protocol is used on the client for the test, remove all other protocols

13) Select **Default Properties** tab.

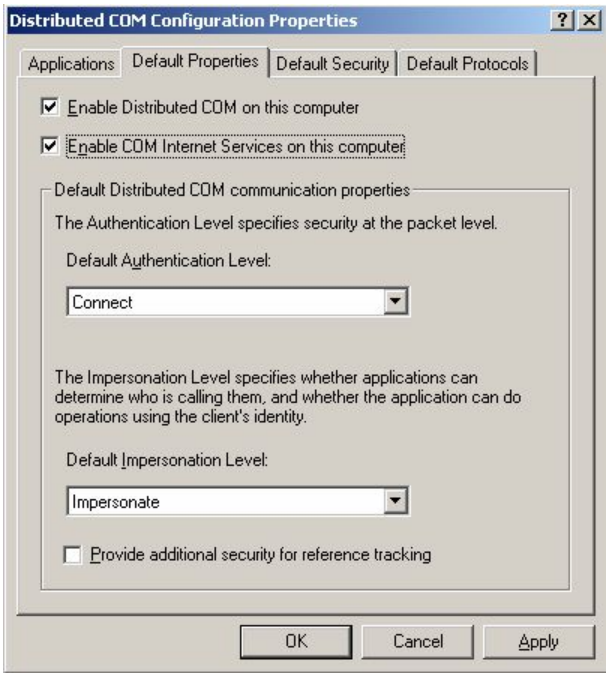

Figure 66: Select Default Properties Tab

14) Enable checkbox '**Activate COM Internet Services on this computer**',

15) Reboot the client machine,

- More information in http://support.microsoft.com/default.aspx?scid=kb;en-us;265340

Additional a robustness test has to be done. The following issues have to be evaluated:

- How does the Garbage Collector of COM work?
- How robust is the network connection? Is it very sensitive or does the IIS handle Communication problems?

List of Figures

Index

N