

# Installing and Activating DCOM for LS Retail

Author: Eiður Már Arason Date: 13.02.2009

© Copyright 2007, LS Retail ehf. All rights reserved. All trademarks belong to their respective holders.

# Contents

1	Introduction	1
2	Server Installation	1
3	Client Installation	1
4	Server Configuration (2000 or 2003)	1
5	Client Configuration	
	5.1 Windows XP (With Service Pack2 and security updates)	2
	5.2 Windows 2000	5
6	Troubleshooting	7

# **1** Introduction

This document outlines how to install and configure DCOM for LS Retail. LS Retail offers an online setup. (Many POSs using same database). If the online setup is done with thin clients (Terminal Server Client or Citrix MetaFrame Client) and you want to use OPOS Devices such as Line Display, Cash Drawer etc. you will run into problems because these devices are usually connected to COM ports on the POS and port mapping will not work because some OPOS Drivers do not handle running many instances on the same machine. The solution to this is using DCOM (Distributed Component Object Model). With DCOM LS Retail can instantiate OPOS Controls on the remote machine (the POS) from the Terminal/Citrix Server. However, with more emphasis on security in Windows today (especially Window XP SP2) DCOM configuration has become more difficult and some of these security mechanisms have to be disabled in order for DCOM to work. It is therefore not recommended to use DCOM in an environment that is open to traffic from the internet. LS Retail ehf. takes no responsibility for the changes suggested in this document.

### 2 Server Installation

The LS Retail Toolbox should be installed on the Terminal/Citrix Server. This will install the OposMap control from LS Retail ehf that handles the DCOM initialization along with other controls and objects needed to run LS Retail.

# 3 Client Installation

The LS Retail Toolbox should be installed on the Terminal/Citrix Client. This will install and register OPOS Controls (COM objects) for the supported OPOS devices in LS Retail. The DCOM Service must be registered by running the **dcomopos.reg** file which is installed with the toolbox. Typically this file would end up in *C:\Program Files\LS Retail\Toolbox\OPOSControls\Remote*. Double-click on this file and select *yes*. If registry information is not successfully installed you must check your user permission. You must have write access to the registry.

## 4 Server Configuration (2000 or 2003)

Run DCOM Configuration (Start->Run **dcomcnfg**). Select the Default Properties tab and make sure that **Enable Distributed COM** on this computer is check marked.

# 5 Client Configuration

#### 5.1 Windows XP (With Service Pack2 and security updates)

 Run DCOM Configuration (Start->Run dcomcnfg). Find My Computer under Component Services -> Computers and open the properties dialog. Select the Default Properties tab and make sure that Enable Distributed COM on this computer is check marked.

Component Services			
🕞 File Action View Window Help			_18
⊨ → 🖻 🖬 🗡 💣 🔮 😫	10 🕒 📴 🖽 🗰 🏛	1 😐	
Console Root	My	Computer 4 object(s)	
Component Services  Computers  Ny Computer	My Computer Propert	ies	? 🛛
COM+ Applications	Default Protocols	Options	Default Properties
Costributed Transaction     Point Coning     Point Coning     Point Coning     Point Coning     Cost Coni	Enable Distributed C     Enable COM Interne	DM on this computer t Services on this comput	ter

2) Find the LSRetail OPOS Envelope 1.8 in the DCOM Config folder and open properties dialog. Select the Security tab and edit the Launch and Activation Permissions.

Component Services			×	
File Action View Window Help		_ 8	×	
E 🖪 × 🖻 🛛 😫 🛍 🕒	• 🟥 🗰 🗇 😕			
LegitCheckControl     Solution     LegitCheckControl     Solution     Logical Disk Manager Administrati     Logical Disk Manager Administrati     Logical Disk Manager Remote Clie     Listential OPOS Envelope 1.8     Solution     LuComServer     Machine Debug Manager     Media Player     Microsoft Agent Server 2.0     Microsoft Agent Server 2.0     Microsoft CLR Debugger 2003     Microsoft CLR Debugger 2003     Microsoft CLR Debugger 2003     Microsoft Development Environm     Microsoft Development Environm     Microsoft Development Environm     Microsoft Equation 3.0     Microsoft Equation 3.0     Microsoft Ercel Application     Microsoft Ercel Application	General Location Securit Launch and Activation Customize Access Permissions Customize	Interactive System	? ×	
Microsoft FrontPage  Microsoft Graph Application  Microsoft Help and Support Servi	Configuration Permissi	Permissions for ANONYMOUS LOGON Local Launch Remote Launch Local Activation Remote Activation	Add Allow V V	Remove
rary			ОК	Cancel

Add **ANONYMOUS LOGON** and give all access. **INTERACTIVE** and **SYSTEM** should have local launch and local activation.

 Change the Local Policy. XP Service Pack 2 and XP Security Updates have tightened the access to DCOM Servers. Start -> Run gpedit.msc

🚡 Group Policy			
Eile Action View Help ← → È II > P b			
🛒 Local Computer Policy	Policy 🖉	Security Setting	^
Computer Configuration  Software Settings  Software Settings  Scripts (Startup/Shutdown)  Scripts (Startup/Shutdo	Accounts: Administrator account status     Accounts: Guest account status     Accounts: Limit local account use of blank passwords to console     Accounts: Rename administrator account     Accounts: Rename guest account     Addit: Audit the access of global system objects     Audit: Audit the use of Backup and Restore privilege     Audit: Shut down system immediately if unable to log security a	Enabled Disabled Enabled Administrator Guest Disabled Disabled Disabled	
Gecurity Options	鍵 DCOM: Machine Access Restrictions in Security Descriptor Defini 酸 DCOM: Machine Launch Restrictions in Security Descriptor Defin	O:BAG:BAD:(A;)	

Open Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.

Open (double click) the **DCOM: Machine Access Restrictions in Security Descriptor Language (SDDL) syntax**.

DCOM: Ma	chine Access Restrictions i	n Security Descri ?
Template !	Security Policy Setting	
ccess Permission		curity Descriptor
Security Limits		
Group or user names:		policy setting in the
Everyone		policy socard in the
		Edit Security
	Add Remove	ncel Apply
Permissions for ANONYMOU LOGON	S Allow Deny	
Local Access		
Remote Access		
1		
	OK Can	cel

Give ANONIMOUS LOGON and Everyone all access.

Open (double click) the "DCOM: Machine Launch Restrictions in Security Descriptor Language (SDDL) syntax".

			curity Descriptor
ecurity Limits			
Group or user names:		-	
Administrators (EIDUR-DES ANONYMOUS LOGON Evervone	K\Administrators)	i.	policy setting in the
			Edit Securitu
		Bamaua	Edit Occurry
Dentifier to Addition to	Add	- nemove	hcel Appl
-ermissions for Administrators	Allow		
Remote Launch			
Local Activation			
Hemote Activation			

Give **ANONIMOUS LOGON** all access and **Everyone** access to Local Launch and Local Activation.

- If the POS belongs to a workgroup instead of a domain, make sure that it does not use simple file sharing.
   Open Windows Explorer or double click on My Computer, click Tools, then go to Folder Options, click View and uncheck <u>Use simple file sharing (recommended)</u> in advanced settings.
- 5) If you are using workgroups or you are crossing domain for example POS is in a workgroup and Server is on a domain etc. you should create a local user identical to the user used to logon to the server. This user must have the same username and password as the user used to log on to the server, even if that user is a domain user. You can add users by running **compmgmt.msc** from the run option in start menu.

📙 Com	puter M	anage	ment
📃 Eile	Action	⊻iew	Window
$\Leftrightarrow \Rightarrow$	1	1	6
Comp	uter Mana ystem Too Event \ Shared Local U Cocal U Cocal U Cocal U Cocal U Cocal U Cocal U Cocal U Cocal U Cocal U	agemen bls /iewer Folders sers and ars oups	t (Local) d Groups

Open Local Users and Groups and right-click on the Users folder and New User...

6) Firewalls should be turned off while configuring

DCOM to work on Windows XP. If you are using the standard windows XP firewall you can turn it off by opening **Control Panel** -> **Windows Firewall** and select **Off.** 

	bws Firewall
ieneral	Exceptions Advanced
8	Your PC is not protected: turn on Windows Firewall
Windov from ga	vs Firewall helps protect your computer by preventing unauthorized users ining access to your computer through the Internet or a network.
١	O <u>O</u> n (recommended)
Ŭ	This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
	Don't allow exceptions
	Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
8	③ Off (not recommended)
Ŭ	Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
Window	ws Firewall is using your domain settings.
WINDOW	

#### 5.2 Windows 2000

- 1) Run DCOM Configuration (Start->Run dcomcnfg).
- 2) On the **Default Properties** tab, activate DCOM by selecting **Enable distributed COM** on this computer.

Distributed COM Configuration Properties	? ×		
Applications Default Properties Default Security Default Protocols			
Enable Distributed COM on this computer			
Enable COM Internet Services on this computer			
Default Distributed COM communication properties	- II		
The Authentication Level specifies security at the packet level.			
Default Authentication Level:			
(None)			
The Impersonation Level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity. Default Impersonation Level:			
Provide additional security for reference tracking			
OK Cancel Apple	,		

3) On the Applications tab, locate the LSRetail OPOS Envelope 1.8 icon, (see below).



4) Press the Properties button and select the Security tab.

OPOS Envelope 1.5.3 (FEF) Properties	? ×
General Security Identity Endpoints	
<ul> <li>Use default access permissions</li> <li>Use custom access permissions</li> <li>You may edit who can access this application.</li> </ul>	
<ul> <li>Use default launch permissions</li> <li>Use custom launch permissions</li> <li>You may edit who can launch this application.</li> </ul>	
Use default configuration permissions     Use custom configuration permissions     You may edit who can change the configuration information for this     application.     Edit	
OK Cancel Apply	

- 5) Select **Use custom access permissions** and then press the Edit Button to add **Everyone** and **Domain Users** to the list of those with access to this DCOM object.
- 6) Select **Use custom launch permissions** and then press the Edit Button to add **Everyone** and **Domain Users** to the list of those with access to this DCOM object.

7) If you are using workgroups or you are crossing DOMAIN. E.g. POS is in a WORKGROUP and Server is on a DOMAIN etc. You have to create a local user identical to the user used to logon to the server. This user must have the same username and password as the user used to log on to the server, even if that user is a domain user.

You can add users by running "compmgmt.msc" from the run option in start menu.



Open Local Users and Groups and right click on the Users folder and New User...

# 6 Troubleshooting

Because of the complexity in Windows Client Server communication regarding roles, permissions etc. there are many things that can cause DCOM not to work. Especially in Windows XP(Sp2). The Configuration in earlier chapters should cover the most common cases. There is however a possibility that you have gone through the configuration above but your DCOM Solution is still not working. Here are some of the know issues.

#### 6.1 Use Local System account for the RPC Service

Your hardware is not compatible to new Windows XP Security Updates. This is a strange error that happens on some PC and seems to be hardware related. The RPC (Remote Procedure Call) Service on the client cannot be contacted by the server and therefore DCOM cannot be activated.

#### Solution:

Change the "Log On As" for the RPC Service to "Local System".

#### a) Run "services.msc"

- b) Find the "Remote Procedure Call (RPC)" Service and open the properties dialog.
- c) Select the "Log On" tab, click on the "Local System Account" and select OK.
- d) Restart the computer.

#### 6.2 Enable Dynamic Client Name in Citrix Client Configuration

You citrix client is not configured to use Dynamic Client Name. If you specify a Client Name in the ICA Setting in Citrix Client Config the server might not be able to find the client (POS) to activate the DCOM Server.

#### Solution:

Enable Dynamic Client Name in ICA Setting in Citrix Client Configuration.

#### 6.3 Use Static Endpoint for the DCOM application

If you are having problems with firewalls you might have specify a static endpoint (port) for the LS Retail OPOS Envelope DCOM application.

This is done by opening properties dialog for the "LSRetail OPOS Envelope" in the DCOMCNFG console. Select the "Endpoints" tab and then properties button for the "Connection-oriented TCP/IP" protocol. Then you can select to Use static endpoint.



In this example the port number is set to 14666 but this can be basically any available port number.

If you run into further problems with DCOM that are not listed here please send detailed information on your problem to <a href="mailto:support@lsretail.com">support@lsretail.com</a>