## **Connecting BCM v3.7 or below with NetPBX**

Follow the instructions below to connect a BCM v3.7 or below with NetPBX:

1. Make sure the CDRServer.EXE and Interop.CDRSERVERLib.dll files are placed in the same folder as NetPBX.EXE, usually located in {pf}\Tri-Line\NetPBX.

🚞 NetPBX					
File Edit View Favorites Tools	Help				
🕒 Back 👻 🕤 - 🏂 🔎 Se	earch 😥 Folders 🛛 🎹 🕇				
Address 🛅 C:\Program Files\Tri-Line\N	letPBX				
	Name 🔺	Size	Туре	Date Modified	
File and Folder Tasks 🛛 🛠	👏 CDRClient.dll	176 KB	Application Extension	17/05/2010 08:10	
📬 kitalua a manu falidar	🗂 CDRServer.exe	36 KB	Application	31/01/2005 14:57	
Make a new rolder	🖬 CDRServer.tlb	3 KB	TLB File	31/01/2005 14:57	
Publish this folder to the	🔊 Interop.CDRSERVERLib.dll	7 KB	Application Extension	23/10/2012 19:57	
Chara Mais Galdes	🗱 NetPBX.exe	92 KB	Application	23/10/2012 19:57	
Shale this folder	🔊 osa40.dll	1,112 KB	Application Extension	27/05/2010 03:24	
	🎇 Uninstall NetPBX	2 KB	Shortcut	24/10/2012 12:33	

- 2. Register **CDRServer.EXE** by running the command line with administrator privileges and typing the following command under the directory path of the NetPBX folder: **CDRServer.EXE/regserver**.
- 3. Open the computer's local security policies: Start -> Control Panel -> Administrative Tools -> Local Security Policy.

🐉 Local Security Settings		
File Action View Help		
← →   X 🖪   😫		
Security Settings     Account Policies     Account Policies     Da Local Policies     Public Key Policies     Software Restriction Policies     Software Restriction Policies     Software Policies on Local Computer	Name Account Policies Local Policies Public Key Policies Software Restriction Policies IP Security Policies on Local C	

4. Within the Security Settings\Local Policies\Security Options tree, change the following items as highlighted in the screenshot below:

😼 Local Security Settings			
File Action View Help			
⇔ ⇒ 🖻 🗙 🗗 🗟 😫			
📴 Security Settings	Policy /	Security Setting	
🗄 🧰 Account Policies	👪 Audit: Shut down system immediate	Disabled	
🖻 🧾 Local Policies	🔠 DCOM: Machine Access Restrictio	Not defined	
<u>Audit Policy</u>	BDCOM: Machine Launch Restrictio	Not defined	
User Rights Assignment	👪 Network access: Shares that can b	COMCFG,DFS\$	
E Cecurity Uptions	🔀 Network access: Sharing and secu	Guestionly - local us	
Public Key Policies	👪 Network security: Do not store LAN	Disabled	
Software Restriction Policies	👪 Microsoft network client: Digitally si	Disabled	
H Security Folicies on Local Computer	👪 Network access: Do not allow stor	Disabled	
	🔠 Network access: Let Everyone per	Disabled	
	👪 Network access: Named Pipes that	COMNAP,COMNOD	

- a. Network Access: Let Everyone permissions apply to anonymous users. Set this to Enabled.
- b. Network Access: Sharing security model for local accounts. Set this to Classic.
- C. DCOM: Machine Access Restrictions: Click on Edit Security and add the following user accounts: Anonymous, Everyone, Interactive, Network, System. Set each one to have full access rights.

DCOM: Machine Access Restrictions in Security Descriptor Defi	Access Permission	? ×
Template Security Policy Setting Explain This Setting	Security Limits	
DCDM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax If the security descriptor is left blank after defining the policy setting in the template, the policy setting will not be enforced.	Group or user names: ANDNYMOUS LOGON Everyone INTERACTIVE NETWORK SYSTEM	
Security descriptor:	Add Rem LOGON Allow Deny Local Access Allow Deny	ove
OK Cancel Apply.	DK Cancel	Apply

5. Next step is to modify the way DCOM behaves on the computer by executing the DCOM configuration program: Start -> Run -> DCOMCNFG [enter]. Browse the tree to the following location: Console Root -> Component Services -> Computers -> My Computer. Righ-click on My Computer for Properties and amend or update the following options:



a. On the **Default Properties** tab: Enable Distributed COM on this computer: tick the box for his option Default Authentication Level: set this to Connect Default Impersonation Level: Set this to Identify

My Computer Properties	? ×
Default Protocols   MSDTC   COM Security General   Options Default Properties	
Enable Distributed COM on this computer	
Enable COM Internet Services on this computer	
Default Distributed COM Communication Properties	
The Authentication Level specifies security at the packet level.	
Default Authentication Level:	
Connect	
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:	
Identify	
Security for reference tracking can be provided if authentication is use and that the default impersonation level is not anonymous. Provide additional security for reference tracking OK Cancel App	d

b. On the **COM Security** tab:

Go to the Access Permissions section and select Edit default .

Add the following accounts and set both local and remote access permissions: Anonymous, Everyone, Interactive, Network, Local Service and System.

My Computer Properties	?X Access Permission	<u>?</u> ×
General       Options       Default Properties         Default Protocols       MSDTC       COM Security         Access Permissions       You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.         Edit Limits       Edit Default         Launch and Activation Permissions       You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that	Default Security Group or user names: ANONYMOUS LOGON Everyone INTERACTIVE NETWORK SELF	Add Dem
determine their own permissions.	Permissions for SYSTEM Local Access Remote Access	
OK Cancel Apply		OK Cancel Apply

Go to the Launch and Activation Permissions Section and click on Edit default tab.

Add or update the following accounts to give them all local and remote access permissions: Anonymous, Everyone,

Interactive, Network, Local Service and System.

My Computer Properties		? ×
General	Options )	Default Properties
Default Protocols	MSDTC	COM Security
- Access Permissions -		
You may edit who is also set limits on ap	s allowed default access plications that determine	to applications. You may their own permissions.
	Edit Limits	Edit Default
Launch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to lar ou may also set limits on a permissions. Edit Limits	unch applications or applications that Edit Default
16	ОК	Cancel Apply

INTERACTIVE     LOCAL SERVICE     SYSTEM		لــ كمر ا
	Add	Remove
ermissions for SYSTEM	Allow	Deny
Local Launch	N	8
Local Activation	N	
Remote Activation		ē