



Configurazione di DCOM e Cndex per sistemi Windows desktop e windows CE

Pag. 1 di 18

Sommario

INTRODUZIONE	2
LIVELLO DI AUTENTICAZIONE.....	2
MODIFICA DELLA MODALITÀ DI CONNESSIONE A CNDEX	2
<i>Activation Rights (Diritti di Attivazione)</i>	2
<i>Identità</i>	3
WINNBI 3.1 E SUCCESSIVE.....	3
CONNESSIONE A CNDEX DA UN'APPLICAZIONE .NET	4
ADATTARE L'APPLICAZIONE .NET A CNDEX	4
<i>C#</i>	4
<i>VB.NET</i>	4
REGISTRARE UN UTENTE CON IL PROTOCOLLO NTLM SU OPENCONTROL E PRIMALOGIC	6
<i>Remote Desktop su PrimaLogic</i>	6
REGISTRARE UN UTENTE CON IL PROTOCOLLO NTLM SU CEWIN	8
COMPATIBILITÀ DELLE APPLICAZIONI .NET CON CNDEX SU SISTEMI OPERATIVI A 64 BIT	9
ABILITARE L'ACCESSO REMOTO A CNDEX VERSIONE DESKTOP	11
<i>Configurazione di DCOM sul sistema server</i>	11
<i>Configurazione di Cndex</i>	13

Introduzione

Il presente documento contiene le informazioni necessarie per la configurazione di DCOM su sistemi Windows desktop allo scopo di abilitare l'utilizzo del sistema come server Cndex. Il documento contiene inoltre alcune informazioni utili a sviluppatori C++ e C#/VB.NET.

Livello di Autenticazione

DCOM utilizza il livello di autenticazione più alto tra quelli richiesti rispettivamente dal client e dal server, ovvero se il server richiede CONNECT (CONNESSIONE) e il client richiede NONE (NESSUNA) l'handshake avviene con livello di autenticazione CONNECT.

In una connessione verso un server DCOM Windows CE non si usa mai un livello di autenticazione superiore a CONNECT. Per maggiori dettagli:

<http://msdn2.microsoft.com/en-us/library/ms862115.aspx>

Modifica della modalità di connessione a Cndex

Quando un client si connette ad un server DCOM, ed entrambi specificano la modalità di autenticazione NONE, il server acconsente alla connessione senza eseguire alcuna verifica sulle credenziali del client. Pertanto non è necessario che l'utente, con le cui credenziali il client cerca di connettersi al server DCOM, sia registrato sulla macchina dove è in esecuzione il server (oppure riconosciuto come utente di dominio se la macchina fa parte di un dominio). Su sistemi XTend questa modalità di autenticazione elimina la necessità di registrare gli utenti tramite NTLMUser.exe.

A partire da WinNBI 3.1 gli applicativi si connettono a Cndex utilizzando la modalità di autenticazione NONE, ovvero nessuna autenticazione. La configurazione del protocollo di sicurezza DCOM, inclusa la modalità di autenticazione, avviene tramite chiamata alla API CoInitializeSecurity all'interno di CndexLink.dll.

Il server Cndex, sia versione Win32 che Windows CE, già nelle versioni precedenti richiedeva il livello di autenticazione NONE tramite CoInitializeSecurity, per cui non è stata necessaria alcuna modifica.

In entrambi i casi la modalità di autenticazione selezionata tramite CoInitializeSecurity ha la precedenza sulle impostazioni di default selezionate tramite Pannello di Controllo oppure dcomcnfg.exe.

Activation Rights (Diritti di Attivazione)

Il contenuto di questa sezione non si applica ai sistemi Windows CE.

Per poter attivare un server DCOM da un sistema remoto è necessario fornire all'account SYSTEM (usato per l'esecuzione della maggior parte dei servizi di Windows) diritti di accesso al server stesso. Il mancanza di tali diritti il sistema non è in grado di lanciare il server a fronte di una richiesta da parte di un sistema remoto.

Su sistemi desktop, è necessario aprire il pannello Servizi Componenti->Computer->Risorse del Computer->Protezione COM, nel riquadro Autorizzazioni di Accesso premere il pulsante Modifica Limiti, nel pannello che si apre abilitare l'accesso remoto per l'utente ANONYMOUS LOGON (ACCESSO ANONIMO). Se non esiste questo utente è necessario inserirlo. Chiudere il pannello. Nel riquadro Autorizzazioni di esecuzione e attivazione premere Modifica Limiti e ripetere la medesima operazione.

Identità

È necessario specificare l'identità del server, ovvero le credenziali sotto le quali gira il server una volta lanciato. Esistono tre opzioni:

1. L'utente interattivo

Pro: è facile determinare quale identità assume il server.

Contro: richiede che un utente abbia eseguito il login sulla macchina dove risiede il server DCOM, altrimenti l'esecuzione del server stesso risulta impossibile.

2. L'utente che lancia il server

Questa opzione prevede che il server assuma l'identità dell'utente remoto che ha richiesto il primo accesso, e quindi l'esecuzione del server.

Pro: il server riceve le proprie credenziali direttamente dal client.

Contro: quest'opzione non può essere utilizzata insieme alla modalità di autenticazione NONE, perché in questo caso l'identità dell'utente remoto è sconosciuta al server. Inoltre, con quest'opzione il sistema crea un'istanza del server per ogni utente remoto che richiede l'accesso. Questo comportamento va in conflitto con le specifiche di funzionamento di Cndex.

3. Un utente specifico

In questo caso le credenziali dell'utente devono essere configurate tramite DCOMCNFG oppure via software. Per la configurazione via software si veda il code sample DCOMPERM in Microsoft Platform SDK.

Pro: assegnare un utente specifico agevola il controllo sui privilegi del server DCOM.

Contro: l'utente assegnato deve essere stato precedentemente configurato nella macchina oppure nel dominio di cui la macchina fa parte.

WinNBI 3.1 e successive

Configurazione di Cndex per WinNBI 3.1 e successive:

Metodologia di autenticazione: NONE (nessuna autenticazione).

Quest'opzione è selezionata via software sia dal server Cndex che dai client (WinNBI) e non necessita di configurazione manuale da pannello di controllo. Gli applicativi di terze parti che si connettono a Cndex utilizzando CndexLink.dll non necessitano di modifiche software, in quanto CndexLink.dll esegue tutte le operazioni necessarie prima di connettersi al server. Gli applicativi che non usano CndexLink.dll devono chiamare CoInitializeSecurity specificando la modalità di autenticazione NONE prima di eseguire qualsiasi accesso ad un server DCOM, anche diverso da Cndex, perché in caso contrario il sistema chiama automaticamente CoInitializeSecurity con parametri di default, solitamente con livello di autenticazione CONNECT.

Server Identity: interactive user (utente interattivo)

Quest'opzione corrisponde alla soluzione 1 esposta nel paragrafo precedente. Su sistemi Windows CE essa non è rilevante. Su sistemi Windows desktop è necessario impostare l'identità del server in Pannello di Controllo

->Strumenti di Amministrazione->Servizi Componenti->Config DCOM->cndex->tasto destro e selezionare Proprietà, selezionare il tab Identità, selezionare Utente interattivo.

Con questa impostazione sarà possibile connettersi ad un server Cndex su un sistema desktop solamente dopo che un utente ha eseguito il login dalla console del sistema stesso.

Connessione a Cndex da un'applicazione .NET

Un applicativo .NET eseguito in modalità di debug interattivo dall'IDE di Visual Studio chiama automaticamente `CoInitializeSecurity` all'avvio, caricando le impostazioni di sicurezza di default del sistema. Quest'automatismo impedisce sia all'applicativo che alla dll `CndexLinkUser` di impostare la sicurezza di DCOM, perché la chiamata a `CoInitializeSecurity` può essere eseguita una volta sola. Ogni chiamata successiva a `CoInitializeSecurity` restituisce l'errore 0x80010119 (RPC_E_TOO_LATE). Per maggiori dettagli:

<http://support.microsoft.com/kb/239561/en-us>

Lo stesso fenomeno si verifica quando un'applicazione .NET carica un assembly CLR, perché anche in questo caso è richiesto il marshalling delle interfacce DCOM.

Esistono due soluzioni a questo problema che non richiedono interventi sul CNC: la prima consiste nel modificare l'applicazione .NET in modo che `CoInitializeSecurity` venga invocata al momento giusto, ovvero prima che il marshalling delle interfacce DCOM abbia luogo. La seconda soluzione, peraltro non consigliata, richiede la modifica delle impostazioni di sicurezza di default di DCOM sulla macchina che esegue l'applicazione .NET, in modo che esse corrispondano a quelle richieste per la connessione a Cndex. Una terza soluzione, che è anche la migliore per gli sviluppatori, consiste nella registrazione dell'account utente sul CNC.

Adattare l'applicazione .NET a Cndex

Esistono due differenti procedure, una per applicazioni scritte in C# e una per applicazioni VB.NET. Entrambe le procedure richiedono che un file sorgente (`COMInvoke.cs` or `COMInvoke.vb`) venga inserito nell'applicazione principale. È necessario selezionare il file corrispondente al linguaggio in cui è scritta l'applicazione. I file per entrambi i linguaggi si trovano nella sottodirectory `UserLibrary` della directory di installazione di WinNBI se WinNBI è installato sulla macchina. Il file sorgente deve essere inserito nell'applicazione principale e non in un assembly cui l'applicazione fa riferimento.

C#

Aggiungere `COMInvoke.cs` all'applicazione.

Identificare la procedura `Main()` nell'applicazione. Di solito si trova in `Program.cs`.

All'inizio della funzione `Main()` inserire la riga di codice:

```
PrimaElectronics.COMUtilities.COMInvoke.InvokeDefaultCoInitializeSecurity();
```

VB.NET

Aggiungere `COMInvoke.vb` all'applicazione.

Verificare se l'applicazione utilizza gli eventi dell'application framework aprendo le proprietà del progetto e selezionando il tab `Application`. Se il checkbox "Enable application framework" è contrassegnato, l'applicazione utilizza gli eventi dell'application framework.

Se l'applicazione utilizza gli eventi dell'application framework:

Nel tab `Application` delle proprietà del progetto premere il pulsante `View Application Events`.

Nella casella a tendina `Class Name` (a sinistra sopra la finestra del codice) selezionare "My Application Events".

Nella casella a tendina `Method Name` (a destra sopra la finestra del codice) selezionare "Startup".

Nella funzione `MyApplication_Startup()` aggiungere la linea di codice:

```
PrimaElectronics.COMUtilities.COMInvoke.InvokeDefaultCoInitializeSecurity()
```

Se l'applicazione non utilizza gli eventi dell'application framework:

Nella finestra principale dell'applicazione (nell'esempio MainForm) aggiungere la funzione:

```
<STAThread()> _
Public Shared Sub Main()
    PrimaElectronics.COMUtilities.COMInvoke._
        InvokeDefaultCoInitializeSecurity()
    ' Declare a variable named frm of type MainForm.
    Dim frm As MainForm
    ' Instantiate (create) a new MainForm object and assign
    ' it to variable frm.
    frm = New MainForm ()
    ' Call the Application class' Run method
    ' passing it the MainForm object created above.
    Application.Run (frm)
End Sub
```

Nel tab Application delle proprietà del progetto individuare la casella a tendina “Startup object” e selezionare “Sub Main”.

<Fine della procedura specifica per linguaggio>

È inoltre necessario assicurarsi che la funzione Main() (C#) o Sub Main() (VB.NET) non contenga dichiarazioni di reference a tipi definiti in un assembly, ad eccezione degli assembly del .NET framework. La presenza di una simile dichiarazione obbligherebbe il compilatore JIT a caricare l'assembly prima di compilare la funzione Main, scatenando il marshalling delle interfacce di DCOM e in pratica rendendo inutile la chiamata a InvokeDefaultCoInitializeSecurity(). Ad esempio:

```
[STAThread]
static void Main()
{
    PrimaElectronics.COMUtilities.COMInvoke.
        InvokeDefaultCoInitializeSecurity();

    Assembly1.A a;
    a = new Assembly1.A();
    Application.Run(new MainForm(a));
}
```

In quest'esempio, nella funzione Main si dichiara una variabile reference al tipo A definito nell'assembly Assembly1. Dato che il compilatore JIT deve allocare lo stack per tutte le variabili locali dichiarate in Main() prima di eseguirla, Assembly1 viene caricato per acquisire la definizione di Assembly1.A prima di eseguire la chiamata a InvokeDefaultCoInitializeSecurity().

Per evitare questo problema, è necessario modificare il codice:

```
[STAThread]
static void Main()
{
    PrimaElectronics.COMUtilities.COMInvoke.
        InvokeDefaultCoInitializeSecurity();

    Application.Run(new MainForm(new Assembly1.A()));
}
```

La funzione Main() modificata non dichiara un reference esplicito ad Assembly1.A, invece passa un reference implicito ad A direttamente al costruttore della form principale. In questo modo Assembly1 non viene caricato fino a quando non viene invocato il costruttore di A, permettendo ad `InvokeDefaultCoInitializeSecurity()` di inizializzare la sicurezza di DCOM con le impostazioni adatte alla connessione a Cndex.

NOTA: questa soluzione non impedisce ad un'applicazione eseguita dall'ambiente di sviluppo di Visual Studio di invocare `CoInitializeSecurity()`, perché in questo caso la chiamata viene eseguita da Visual Studio stesso.

Registrare un utente con il protocollo NTLM su OPENControl e PrimaLogic

Questa procedura permette al CNC di riconoscere le credenziali dell'utente quando l'applicazione tenta di connettersi al server Cndex.. Dato che DCOM utilizza il protocollo di sicurezza NTLM per l'autenticazione, una semplice applicazione per registrare un utente con NTLM viene fornita insieme a tutti i modelli di OPENControl e PrimaLogic.

- Dal desktop di OPENControl, premere Start->Run.
- Digitare il comando:

`\SSD\Osai\XTend\bin\NTLMUser.exe` (OPENControl su Windows CE 5.0)

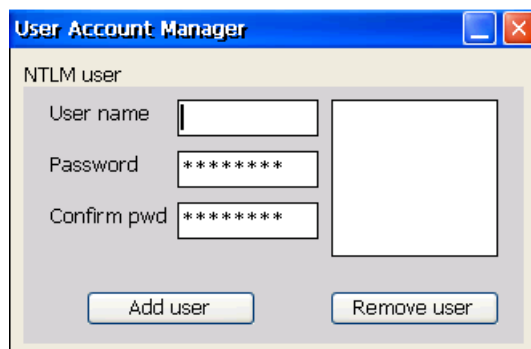
oppure

`\SSD\Osai\XTend\bin\NTLMUserCE60.exe` (OPENControl su Windows CE 6.0)

oppure

`\SSD\Osai\PrimaLogic\bin\NTLMUserCE60.exe` (PrimaLogic)

- Premere OK. La finestra di NTLMUser apparirà sul desktop.



- Digitare nome utente e password, dopodiché premere "Add user". Il nome utente inserito apparirà nel riquadro di destra della finestra NTLMUser.
- Premere Start->Programs->Regflush per rendere permanente la registrazione dell'utente.

NOTA: la password viene salvata nel registro di sistema mediante la codifica 3DES, impedendo la sottrazione della medesima da parte di un utente non autorizzato che riesca ad ottenere l'accesso a sistema.

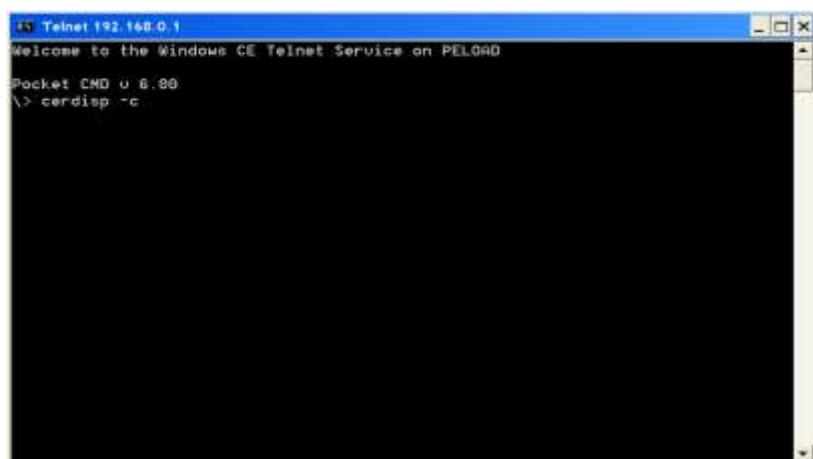
Remote Desktop su PrimaLogic

A differenza di OPENControl, non è possibile collegare video e tastiera ad un PrimaLogic. Tuttavia, il desktop di Windows CE su PrimaLogic può essere utilizzato da un PC collegato al PrimaLogic attraverso una connessione LAN, preferibilmente in point-to-point con un cavo crossover. Sul PC client aprire il prompt dei comandi ed aprire una connessione telnet verso il PrimaLogic tramite la riga di comando:

```
telnet <IP address of the PrimaLogic> (usually 192.168.0.1)
```

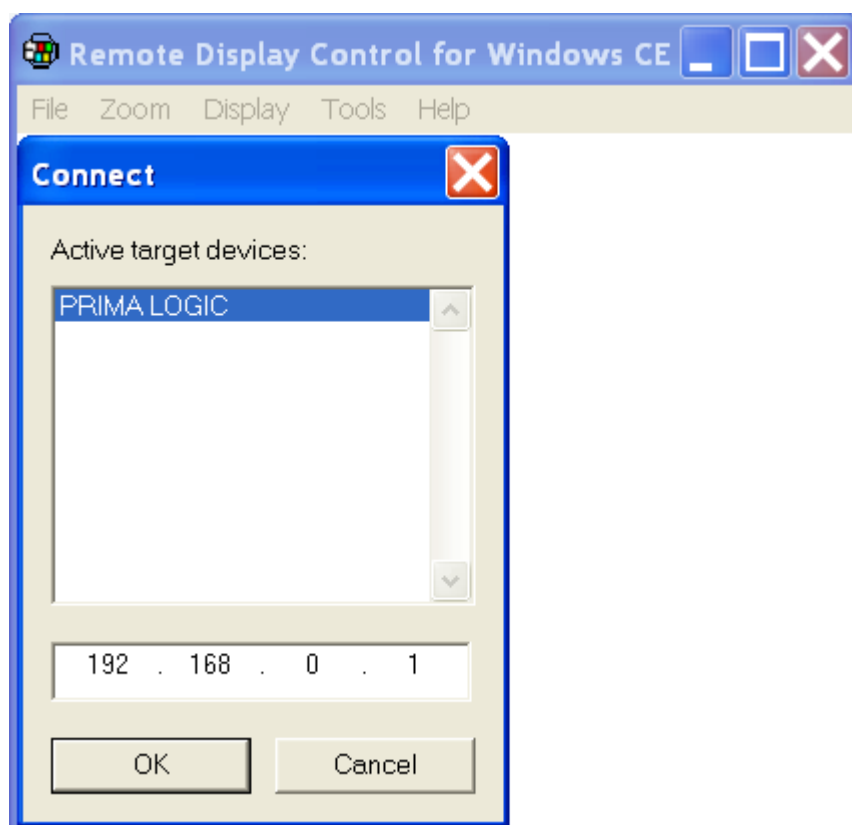
Dopo che la connessione telnet è stata creata digitare il comando:

```
cerdisp -c
```



NOTA: non chiudere la finestra del prompt dei comandi finché non è terminato l'utilizzo di Remote Desktop.

Lanciare l'eseguibile cerhost_CE60.exe, situate nella sottodirectory Utility della directory di installazione di WinNBI. Dal menu File selezionare Connect. Dopo alcuni secondi la voce "PRIMA LOGIC" apparirà nel riquadro superiore. Selezionare la voce e premere OK. Remote Desktop è ora pronto all'utilizzo. A partire da questo punto la procedura per la registrazione dell'utente è identica a quella per OPENControl.



Registrare un utente con il protocollo NTLM su CeWin

Questa procedura è praticamente identica a quella descritta per OPENControl. Tuttavia è necessario agire sul registro di sistema modificando i file di configurazione di CeWin. La procedura deve essere eseguita sul sistema host di CeWin, ovvero il sistema dove CeWin è in esecuzione, non sul sistema che esegue l'applicazione client.

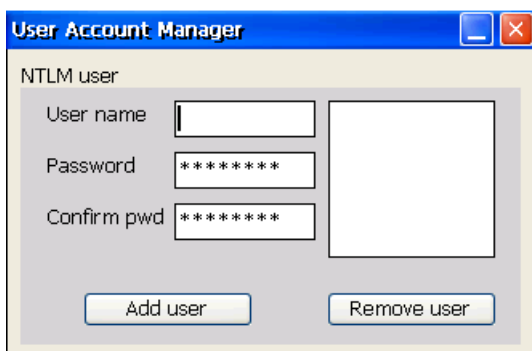
- Aprire il un editor di testo il file Os.config situato nella directory di installazione di CeWin.
- Inserire al fondo del file il seguente testo:

```
[HKEY_LOCAL_MACHINE\init\BootVars]
"MasterKeyFileDir"="\Network\SSD\Osai\"
```

- Riavviare CeWin.
- Dal remote desktop di CeWin, premere Start->Run.
- Digitare il comando:

```
\Network\SSD\Osai\XTend\bin\NTLMUserCE60.exe
```

Premere OK. La finestra di NTLMUser apparirà sul desktop.



- Digitare nome utente e password, dopodiché premere “Add user”. Il nome utente inserito apparirà nel riquadro di destra della finestra NTLMUser.
- Dal remote desktop di CeWin, premere Start->Run.
- Digitare il comando:

```
\Network\SSD\Osai\XTend\bin\ReadNTLM.exe
```

- Dal sistema host di CeWin, aprire il file ntlmkey.txt situato nella directory \Network\SSD. Copiare le due righe corrispondenti al nome utente inserito, ovvero:

```
[HKEY_LOCAL_MACHINE\Comm\Security\UserAccounts\<username>]
"NT"=hex:01,00.....
```

- Incollare le due righe in coda al file Os.config.

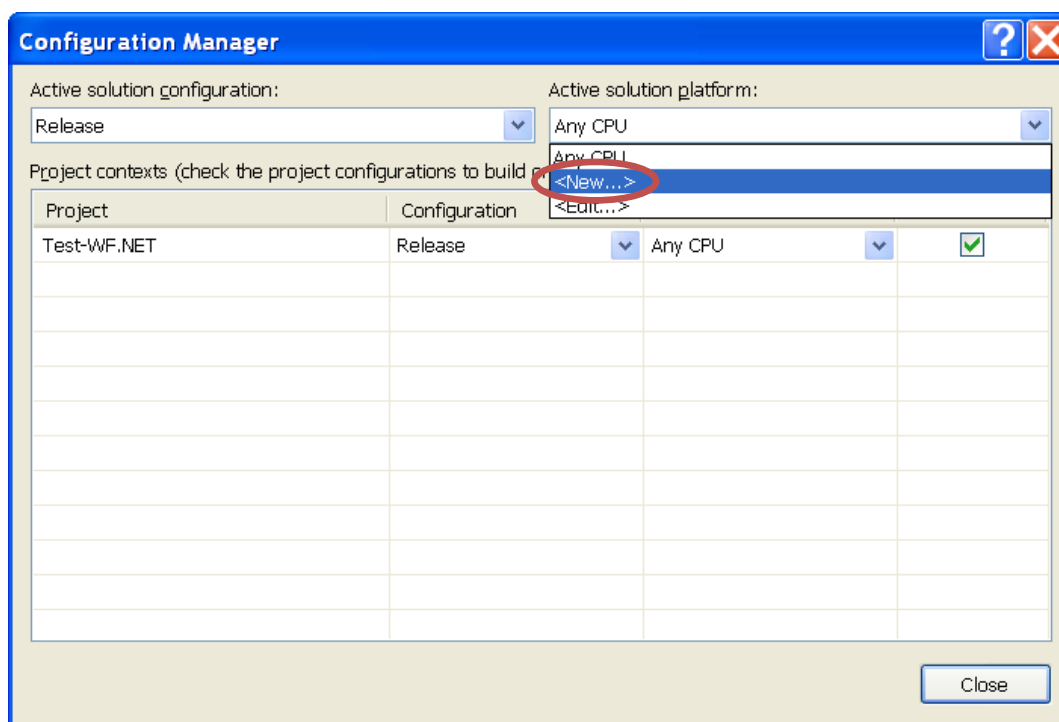
NOTA: la password viene salvata nel registro di sistema mediante la codifica 3DES, impedendo la sottrazione della medesima da parte di un utente non autorizzato che riesca ad ottenere l'accesso a sistema.

Compatibilità delle applicazioni .NET con Cndex su sistemi operativi a 64 bit

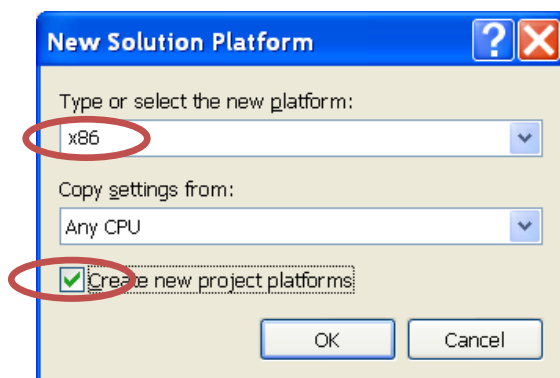
WinNBI e Cndex sono distribuiti unicamente nella versione a 32 bit. I sistemi operativi a 64 bit, come ad es. Windows7 64 bit, sono pienamente in grado di eseguire codice a 32 bit, tuttavia con alcune limitazioni. In particolare, un eseguibile a 64 bit non è in grado di collegare dinamicamente una libreria a 32 bit e viceversa.

Se un eseguibile .NET viene generato con la piattaforma di default “Any CPU”, il compilatore JIT lo adatta automaticamente al tipo di sistema operativo allo scopo di ottenere le prestazioni migliori. In breve, se l’eseguibile gira su un sistema a 64 bit viene automaticamente compilato a 64 bit dal compilatore JIT. Dato che Cndex e le relative DLL sono disponibili solamente in versione a 32 bit, un’applicazione a 64 bit che tenta di collegarsi a Cndex genera un’eccezione “DLL non trovata”, anche se WinNBI è installato correttamente sul sistema. Per aggirare il problema, il progetto Visual Studio deve essere configurato in modo da generare un eseguibile che giri in modalità 32 bit, a prescindere dall’architettura del sistema operativo.

1. Aprire il progetto .NET in Visual Studio, quindi selezionare Build->Configuration Manager dal menu.
2. Nella finestra Configuration Manager, dal pannello Active Platform selezionare <New...>.



3. Dalla finestra di dialogo selezionare “x86” come nuova piattaforma. Verificare che il flag “Create new project platforms” abbia la spunta, quindi premere OK.

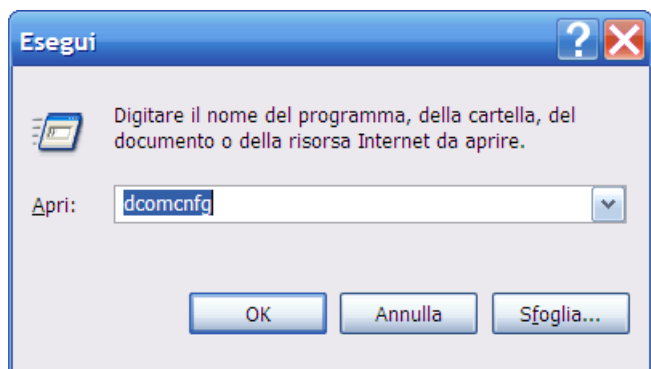


Abilitare l'accesso remoto a Cndex in un sistema desktop

Il contenuto di questa sezione si applica solo nel caso in cui sia necessario utilizzare un PC desktop come server Cndex remoto, ad esempio per connettersi ad un sistema Serie10 che non si trova nella stessa rete locale del sistema client, oppure nel caso in cui sia necessario connettersi al file system logico di un PC desktop da FileBrowser o Program Manager.

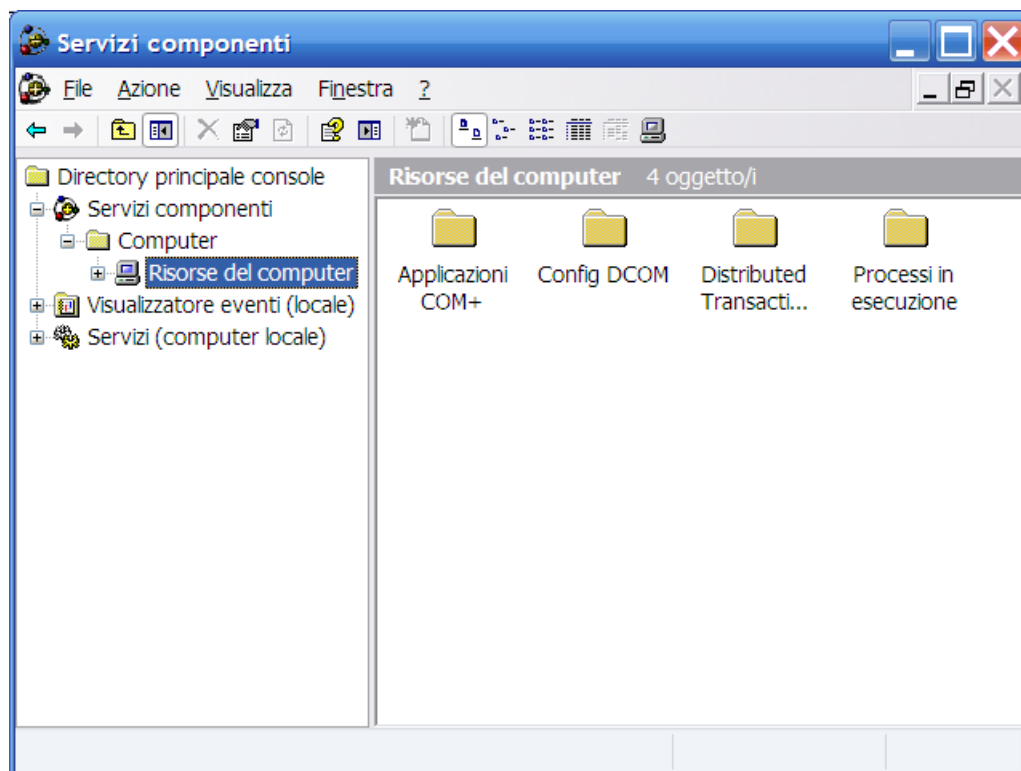
Configurazione di DCOM sul sistema server

Da Pannello di Controllo aprire Strumenti di Amministrazione->Servizi Componenti. In alternativa dalla riga di comando eseguire “dcomcnfg”.



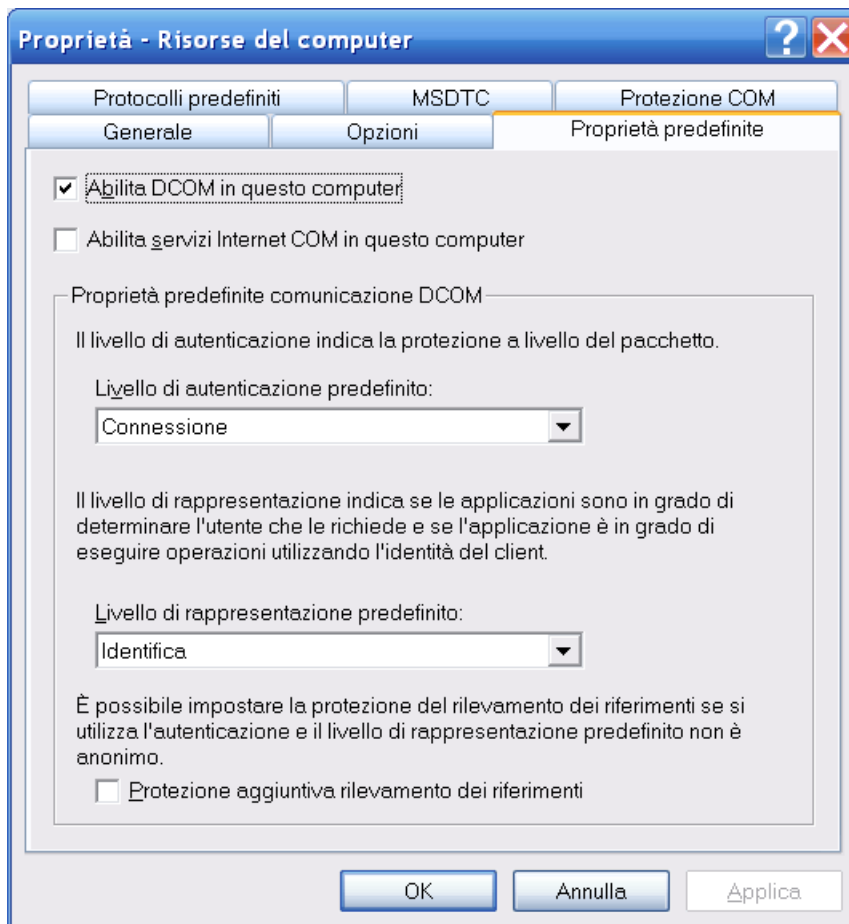
Abilitazione di DCOM

Da “Servizi Componenti” selezionare Computer->Risorse del Computer. Mediante il tasto destro su Risorse del Computer selezionare “Proprietà”.



Dal pannello Proprietà selezionare il tab “Proprietà predefinite”:

- ☐ abilitare il check box “Abilita DCOM su questo computer”;

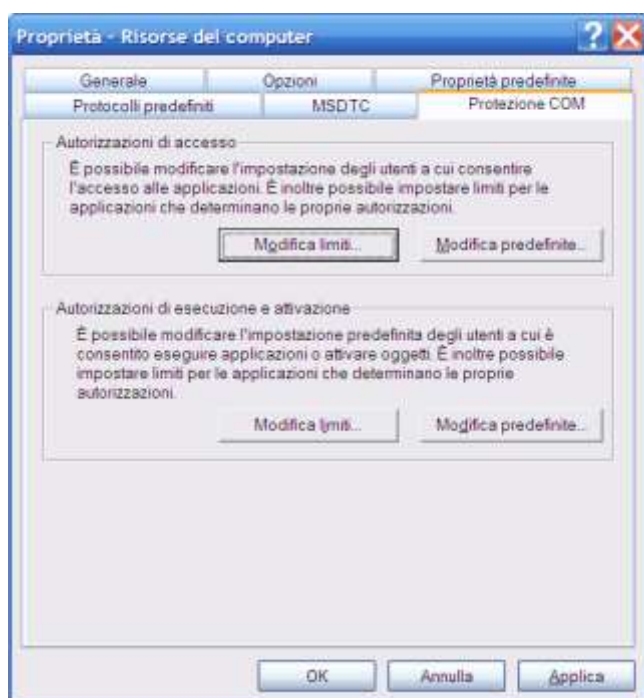


Autorizzazioni di esecuzione e accesso remoto

Selezionare il tab “Protezione COM”. Nel riquadro “Autorizzazione di accesso” premere il pulsante “Modifica Limiti”. Dal pannello autorizzazioni di accesso inserire, se non è già presente, l’utente “ACCESSO ANONIMO” (se versione inglese “ANONYMOUS LOGON”). Abilitare tutti i diritti di accesso per l’utente ACCESSO ANONIMO e premere OK.

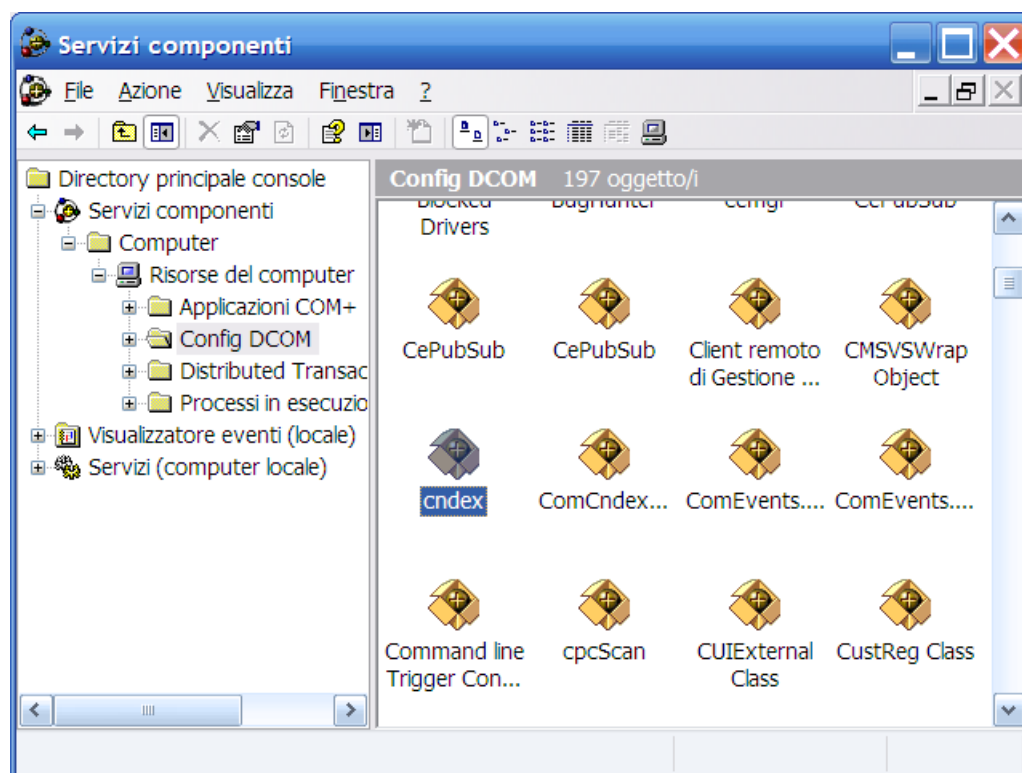
Nel riquadro “Autorizzazioni di esecuzione e attivazione” premere il pulsante “Modifica Limiti” e ripetere l’operazione descritta al punto precedente. Una volta terminato premere OK nel pannello “Proprietà” di Risorse del Computer.

La configurazione dei diritti di accesso di default di DCOM è terminata. Ora è necessario impostare i diritti di accesso specifici di Cndex.

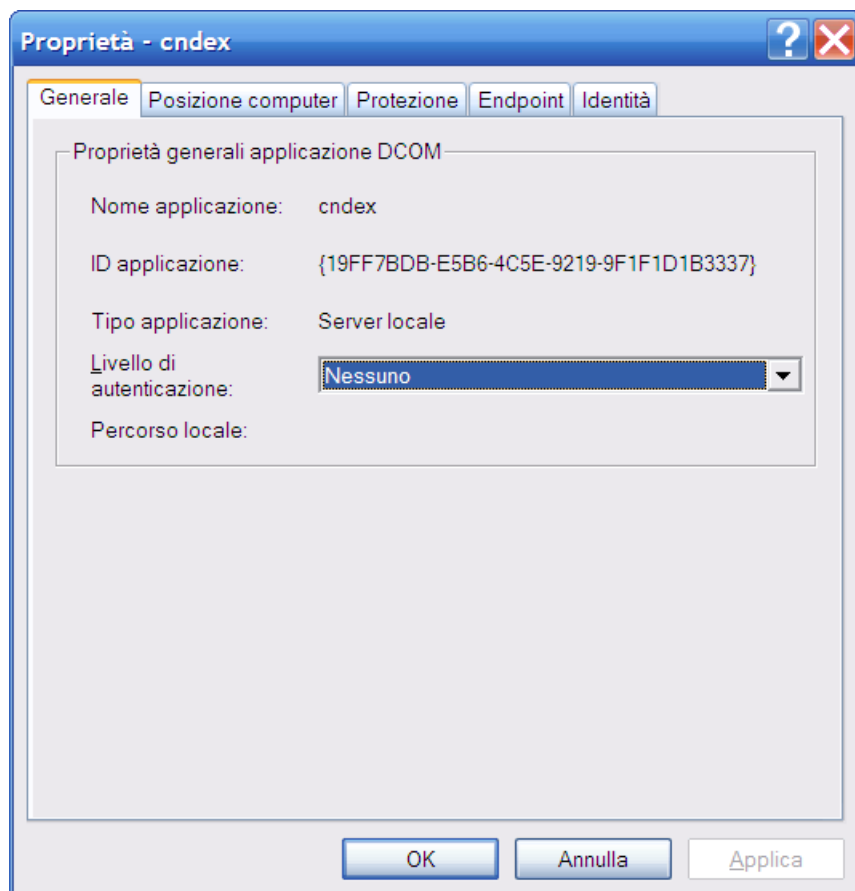


Configurazione di Cndex

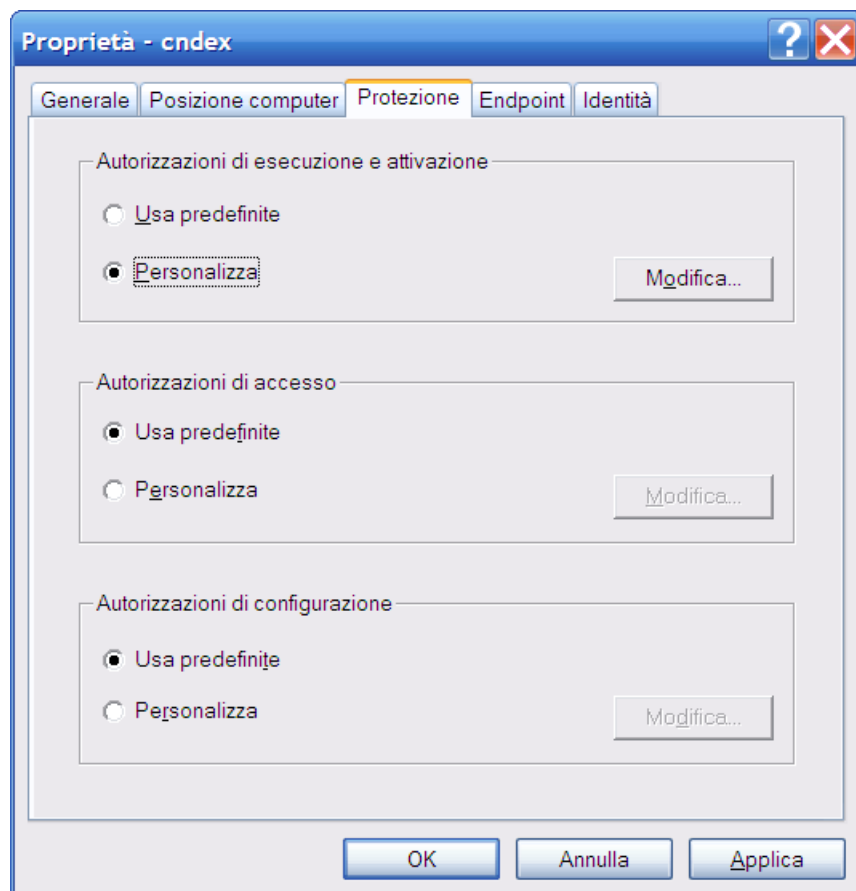
Dal pannello Servizi Componenti selezionare il nodo “Config DCOM”. Nel pannello di destra selezionare “Cndex”. Con il tasto destro del mouse aprire il pannello “Proprietà” di Cndex.



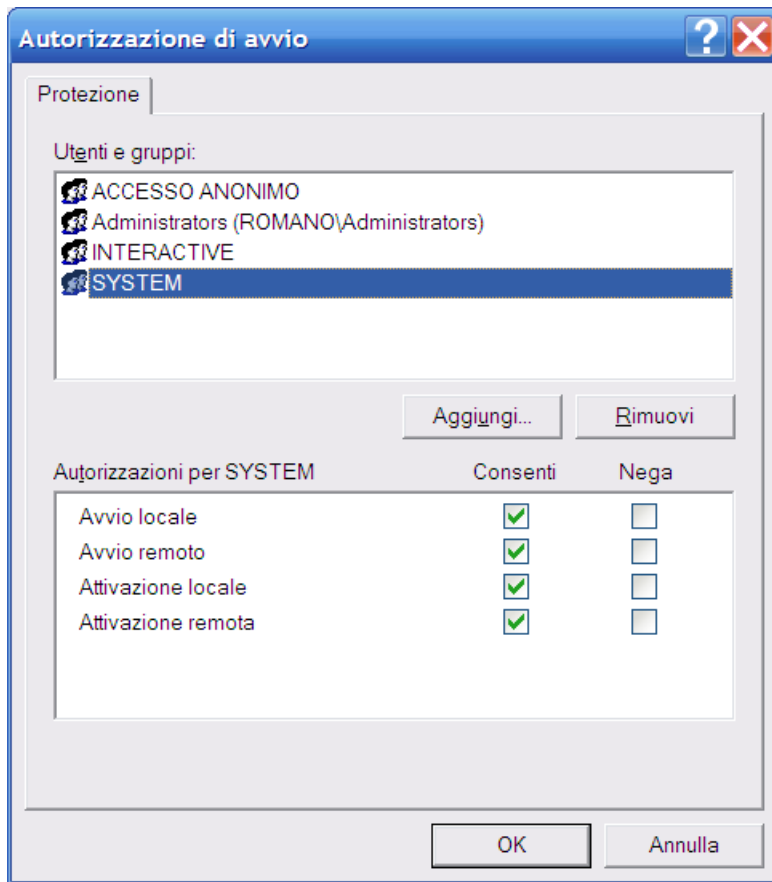
Dal pannello Proprietà di Cndex selezionare il tab “Generale”. Selezionare il livello di autenticazione “Nessuno”.



Selezionare il tab “Protezione”. Nel riquadro “Autorizzazioni di esecuzione e attivazione” selezionare “Personalizza” e premere il pulsante “Modifica”.



Dal pannello “Autorizzazioni di Avvio” aggiungere, se non è già presente, l’utente “ACCESSO ANONIMO” (se versione inglese “ANONYMOUS LOGON”) ed abilitare tutti i diritti per il medesimo. Aggiungere quindi, se non è già presente, l’utente “SYSTEM” ed abilitare tutti i diritti per il medesimo. Premere OK.



Ripetere l’operazione per i riquadri “Autorizzazioni di accesso” e “Autorizzazioni di configurazione”.

Selezionare il tab “Identità” del pannello Proprietà di Cndex. Selezionare il radio button “Utente interattivo”. Premere OK nel pannello proprietà di Cndex. La procedura di configurazione è così terminata.

NOTA: con quest’ultima impostazione è necessario che un utente esegua il login sul sistema Windows desktop affinché il medesimo possa essere utilizzato come server Cndex.

The image shows a Windows-style dialog box titled "Proprietà - cndex". It has five tabs: "Generale", "Posizione computer", "Protezione", "Endpoint", and "Identità". The "Identità" tab is selected. Inside the dialog, there is a text label: "Selezionare l'account utente che si desidera utilizzare per eseguire l'applicazione." Below this, there are three radio buttons: "Utente interattivo" (which is selected), "Utente che esegue l'avvio", and "Utente seguente". Below the radio buttons, there are three text input fields labeled "Utente:", "Password:", and "Conferma password:". To the right of the "Utente:" field is a button labeled "Sfoglia...". At the bottom of the dialog, there are three buttons: "OK", "Annulla", and "Applica".