NORTEL

Product Bulletin

Bulletin Number: P-2005-0026-Global
Date: 31 January 2005

CallPilot 3.0 and the 201i IPE Platform - Using Microsoft Remote Desktop Connection

Introduction

CallPilot 3.0*, on the 201i IPE platform, will utilize the Microsoft Remote Desktop Connection (RDC) client application for remote maintenance and support of the server. This is a change from the original plan to offer it as an optional means for remote maintenance.

The intent of this document is to facilitate the introduction of RDC into Nortel Channel Partner service and support groups. It provides:

- Reason for change to Microsoft RDC (on the 201i IPE platform)
- What is Microsoft RDC
- Assessment of impact to Partners
- Microsoft RDC Technology Overview
- Comparison of Microsoft RDC and Symantec pcAnywhere
- References and Related Documents
- RDC client installation and configuration information
- Guidelines for using this client with a CallPilot 3.0 server.

Use of this document should greatly minimize impact and confusion for those performing remote administration/maintenance tasks on the CallPilot 3.0 201i IPE or other 3.0 platforms.

Reason for change to Microsoft Remote Desktop Connection

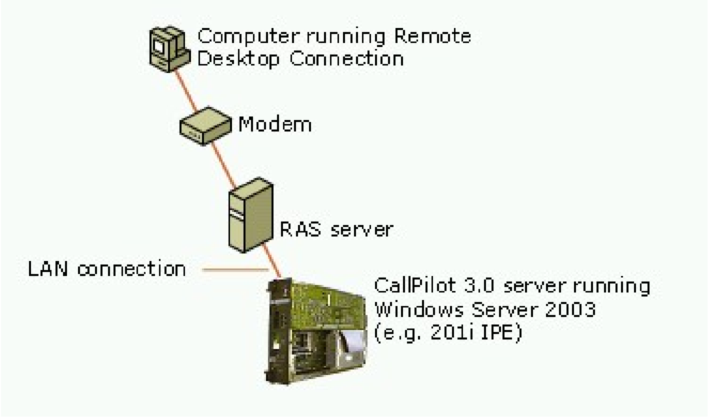
Extensive testing has shown that Symantec pcAnywhere causes occasional memory corruption and blue screen crashes when used on a CallPilot 201i IPE server running release 3.0 software. The use of RDC in place of pcAnywhere is required to achieve General Availability (GA) for CallPilot 3.0 on the 201i because an interaction among pcAnywhere, Windows 2003 OS, and the CallPilot video subsystem is expected to take some time to resolve.

Note: The pcAnywhere interaction issue observed on the CallPilot 201i IPE has not been observed with the 703t Tower or 1002rp Rackmount and thus pcAnywhere is still available on these CallPilot 3.0 servers.

What is Microsoft Remote Desktop Connection

Remote Desktop for Administration (formerly known as Terminal Services in Remote Administration mode) is installed by default on all Windows Server 2003 family operating systems which CallPilot 3.0 runs on. The Remote Desktop Connection client can be used to connect to a CallPilot 3.0 server for remote administration. It requires the same TCP/IP network connection (LAN, VPN or RAS dial-up) as pcAnywhere utilizes.

Microsoft Remote Desktop Connection comes with all CallPilot 3.0 platforms. However, the 703t Tower and 1002rp Rackmount platforms will continue to also offer the pcAnywhere remote maintenance and support functionality option.


Computer running Remote Desktop Connection
Modem
RAS server
LAN connection
CallPilot 3.0 server running Windows Server 2003 (e.g. 201i IPE)

Remote Desktop Connection allows you to create and configure your connection, save your connection settings to a file, and open and edit your saved connection files, all in the same program. For more information on Remote Desktop Connection, see topic "RDC Technical Reference".

The client software package can be installed on a computer running any of the following operating systems: Windows 95, Windows 98 and 98 Second Edition, Windows Me, Windows NT® 4.0, Windows 2000 or Windows XP.

Assessment of Partner Impact

First, we acknowledge that introducing Microsoft RDC as the only means of remotely accessing CallPilot 3.0 on 201i IPE late in a product introduction cycle is cause for Nortel and Channel Partner concern. However, because pcAnywhere can cause a crash of CallPilot 3.0 on a 201i IPE and the platform being 80% of all CallPilot shipments, based on our assessment that Microsoft RDC provides equivalent functionality as pcAnywhere, there is a compelling Nortel and Partner business need to begin shipping CallPilot 3.0 on the 201i IPE using RDC.

It is also our assessment that using the information in this document, Channel Partners can quickly introduce Microsoft RDC into their service and support groups that need it.

The following is an assessment in the form of a FAQ:

Q. How is Microsoft RDC different from Symantec pcAnywhere?
A. Microsoft RDC provides similar remote-control capabilities as that of Symantec pcAnywhere. Connectivity can still be controlled and managed from the CallPilot server. A detailed comparison is provided later in this document.

Q. Which personnel need RDC?
A. Persons that remotely administer, check logs, or perform other server-level support and maintenance tasks on a CallPilot 3.0 system not available from CallPilot Manager.

Q. How can the RDC client be acquired?
A. The client is available for download from Microsoft's web page.

Q: Is there any cost for the RDC client?
A: Not at this time. The client is available for download at no charge from Microsoft's web page.

Q. How do personnel learn RDC?
A. This document provides the information they need to be effective with RDC and CallPilot. For additional information, it's recommended visiting Microsoft's web page.

Q: How long will it take to download?
A: Download timeframes depend on internet connection speed. The file is less than 4MB in size so timeframes would be minimal even on a lower bandwidth connection.

Q: How much disk space is required?
A: The application consumes approximately 4MB of disk space. This is significantly less than that of Symantec pcAnywhere.

Q: How much memory does the application use?
A: The application consumes approximately 5-7MB of RAM memory when in use. This is on par with that of Symantec pcAnywhere.

Q: Is the application secure for use over the internet?
A: Yes, but preferred operation is over a VPN or RAS (both of which provide encryption). For complete details, refer to Microsoft's web-site.

Q. How is CallPilot 3.0 ordering affected by this change?
A. Microsoft RDC comes standard with Windows 2003 and CallPilot 3.0. There are no changes to ordering CallPilot 3.0 systems as a result of this change in remote maintenance and support.

Q: Does the Microsoft RDC client conflict with other applications?
A: Nortel has successfully tested the use of Microsoft's RDC client with other CallPilot client applications (Desktop Messaging, Application Builder, etc) and found no interaction issues. There may be some conflicts between the RDC client and other 3rd-party applications. If conflicts do arise, it's recommended they be researched directly via Microsoft's support web-site at http://support.microsoft.com.

Q: Can pcAnywhere still be used on the 703t Tower and1002rp Rackmount platforms?
A: Yes.

Q: Is it safe to use Microsoft RDC to gain access to a CallPilot server during peak traffic times?
A: Yes.

Q: Can Microsoft RDC be used to remotely download and apply approved Microsoft security updates and CallPilot PEPs/Service Updates?
A: Yes. RDC provides remote-control and file transfer capabilities similar to those available with pcAnywhere.

Q: Will pcAnywhere ever be supported on the CallPilot 201i IPE running Windows 2003?
A: Yes, provided an acceptable solution becomes available to address the pcAnywhere/OS/CallPilot video driver conflict that exists today. While no timeline is yet available, this issue is still being pursued with Symantec. A revision to this bulletin will be published as appropriate.

Remote Desktop Connection Overview

Remote Desktop is a feature based on Microsoft's Terminal Server technology. Conceptually it differs significantly from pcAnywhere. With pcAnywhere, the monitor, keyboard and mouse devices from the CallPilot server are remoted. With Remote Desktop, the situation is more akin to logging on to a multi-user mainframe computer. When a Remote Desktop user logs on, a new login session is created that is (by default) distinct from the local console session. Using the Terminal Server technology, there can be multiple simultaneous sessions running on the server – each of those sessions can independently run programs. A login session lasts until it is logged off. If a session is disconnected without logging off, the session will continue to exist and any programs running on that session will continue to run. At a later time, you can reconnect to that session.

Remote Desktop is a feature built into Windows Server 2003 and Windows XP Professional. It is not available for CallPilot servers running Windows NT 4.0. However, the Remote Desktop Client can be run on any version of Windows from Windows 95 on in order to access a server running the Remote Desktop (Terminal) Server. All CallPilot 3.0 and later systems running on Windows Server 2003 can be controlled using the Remote Desktop Client.

Remote Desktop requires network connectivity between the client and the server. This can be a RAS connection running over a modem, or it can be a direct intranet, or VPN connection.

Remote Desktop can perform well over a 28.8 kbps modem. In fact, command line windows and utilities perform dramatically better using Remote Desktop than with pcAnywhere.

References and Related Documents

Information on Microsoft Remote Desktop Connection is available from Microsoft using the following links:

- **Remote Desktop for Administration Overview**
- **Using Remote Desktop for Administration for remote server administration**
- **Remote Desktop Connection – How to**
- **Remote Desktop Connection – Concepts**
- **Remote Desktop Connection – Troubleshooting**

Differences and Limitations as compared with Symantec pcAnywhere

The following table lists known differences and limitations, comparing Remote Desktop Connection with Symantec pcAnywhere.

Difference/Limitation	**Details**
No separate connection user account and password	Unlike pcAnywhere, Remote Desktop Connection uses the same Windows account and password to make the remote connection and log onto the remote server.
Remote Desktop Connection is using IP Port 3389	Remote Desktop for Administration on the remote server is using the Terminal Service Remote Desktop Protocol on port 3389 to provide remote access to the server desktop. Port 3389 must be opened in the connected network path between the local computer and the remote server.
Speed of operation	Using RDC, if Desktop Background is turned ON, speed is noticeably slower than pcAnywhere. It's recommended that this always be turned OFF. Using RDC, Support Tools command-line usage is much faster than pcAnywhere.
No direct modem/COM port connection	pcAnywhere allows for configuring the application to monitor for connections directly on the COM port, bypassing RAS dial-up/authentication. Microsoft RDC only works via LAN, VPN, or RAS dial-up. No support for direct connection to a COM port exists.

Warnings

The following table lists known warnings for Microsoft RDC and Symantec pcAnywhere

Limitation/Warning	**Details**
Conflict with pcAnywhere	If Remote Desktop Connection is utilized to connect to the console session of a remote CallPilot 703t Tower or 1002rp Rackmount server, at some point in time afterward, one may be able to connect but not remotely control that same CallPilot server using pcAnywhere. To clear this issue and again allow for pcAnywhere remote control of the server, the following options exist: • Have a user log into the server locally • Reboot the server
DCOM issue if uninstalling pcAnywhere	Per Symantec design, if the pcAnywhere application is uninstalled, it removes a DCOM registry setting that is required by CallPilot Manager, My CallPilot, Application Builder, and Reporter to communicate with the server. If pcAnywhere is un-installed, obtain file "EnableDCOM.reg" from the ESPL website to re-populate the registry setting.

RDC Technical Reference

The remainder of this document is a technical reference that provides the information needed for personnel to acquire, install, and use the RDC client to access CallPilot 3.0 systems.

Please read this section in its entirety since several important issues and workarounds are described. If not followed, the user will likely encounter the following conditions:

- Errors connecting
- Problems entering passwords
- Confusion on how to share the screen
- Support tools will not work properly
- PEP installs will not work properly
- MAS Trace window will not be visible

The following topics are covered in this section:

- Procedures:
  - Install Remote Desktop Connection Client
  - Enable Remote Desktop feature and Set policy on host
  - Establish a RAS connection
  - Starting the Remote Desktop Client
    - Method 1: Private Session (preferred method)
    - Method 2: Shared Session (only if local console is logged on)

- Advisements:
  - CallPilot Support Tools
  - RAS dial-up required to establish RDC
  - “Double-Hop” remote control
  - Transferring Files in Remote Desktop Connection Session
  - Terminal Server Maximum Connections Exceeded Error
  - Disconnecting the Remote Desktop Connection Session

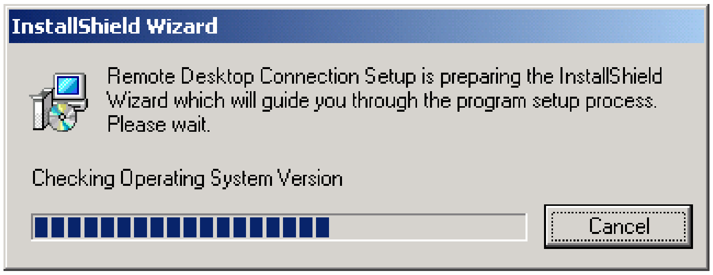
1. Remote Desktop Connection Client Installation

The Remote Desktop Client software is installed by default on Windows XP Professional and on Windows Server 2003. However, the version for Windows Server 2003 is slightly different from the Windows XP version. Obtain the Windows Server 2003 version of the Remote Desktop Connection Client from the following link:

http://www.microsoft.com/downloads/details.aspx?FamilyID=a8255ffc-4b4a-40e7-a706-cde7e9b57e79&DisplayLang=en

This software can be installed on client PCs running Windows 95, Windows 98, Windows ME, Windows NT 4, Windows 2000, or Windows XP using the following procedure:

1.1. Run the executable (msrdpcli.exe). InstallShield will scan the computer to prepare installing the client.

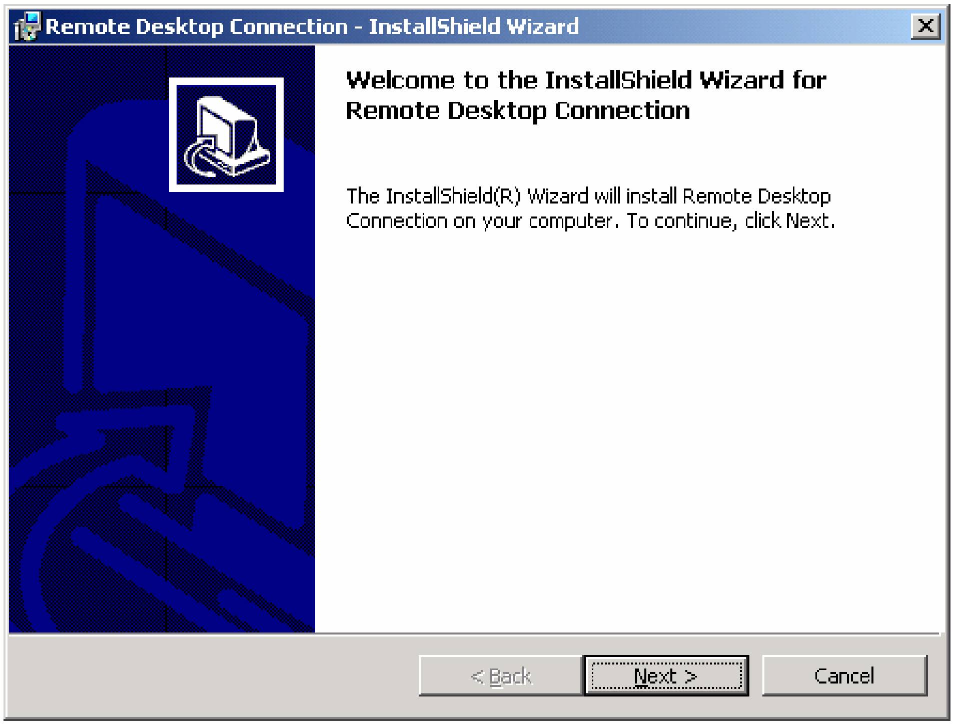


InstallShield Wizard

Remote Desktop Connection Setup is preparing the InstallShield Wizard which will guide you through the program setup process. Please wait.

Checking Operating System Version

1.2. Once complete, the "Welcome" window will appear:

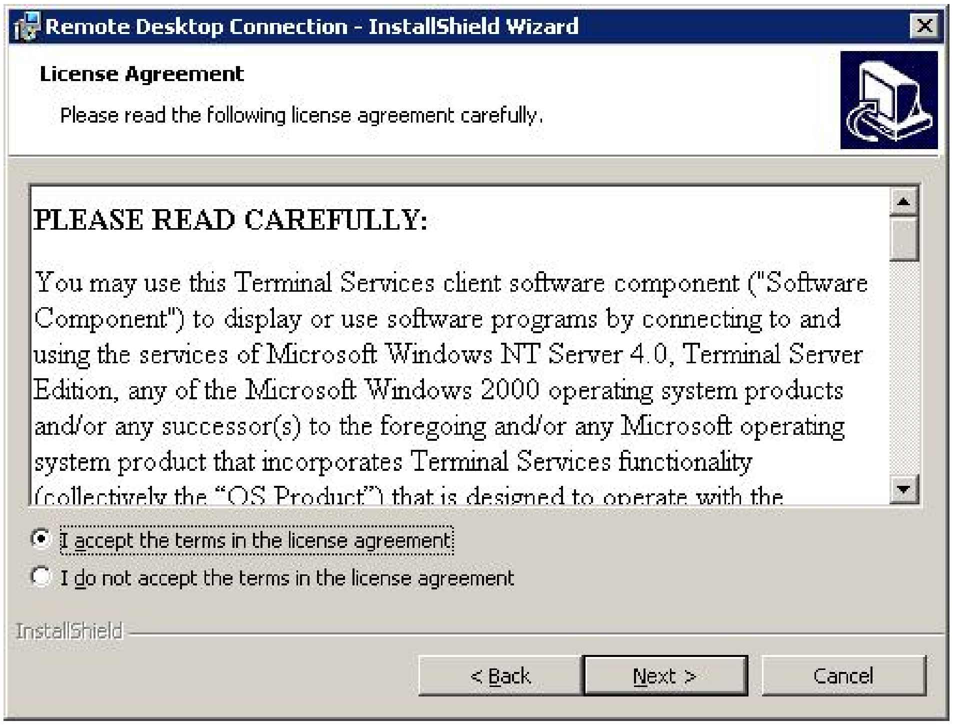


Remote Desktop Connection - InstallShield Wizard

Welcome to the InstallShield Wizard for Remote Desktop Connection

The InstallShield(R) Wizard will install Remote Desktop Connection on your computer. To continue, click Next.

1.3. Click “**Next >**” to proceed. The End User License Agreement window will appear:



Remote Desktop Connection - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

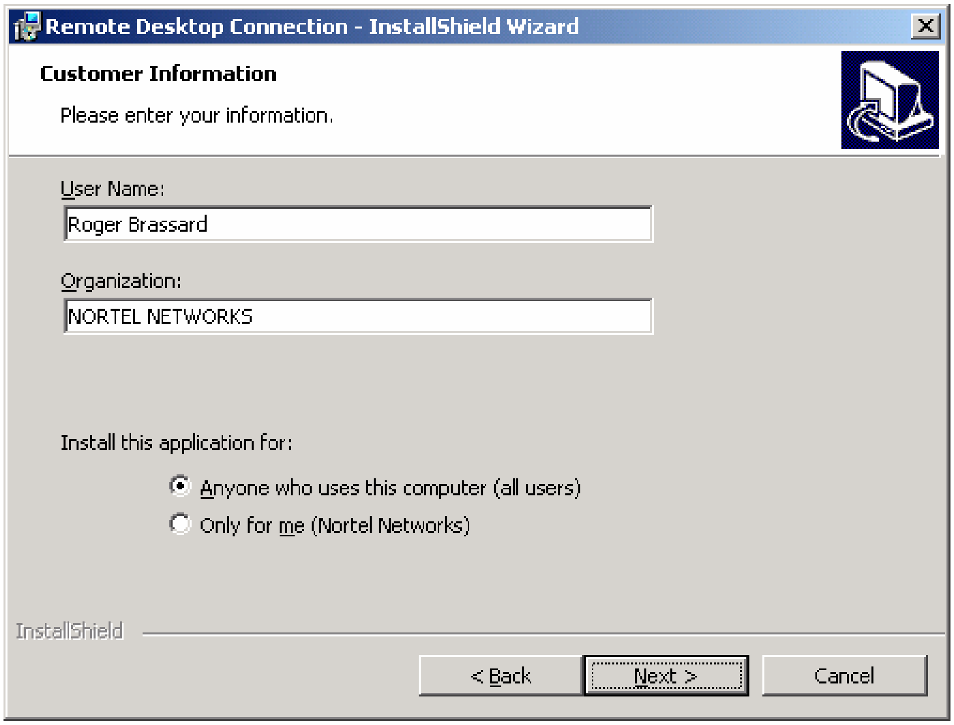
PLEASE READ CAREFULLY:

You may use this Terminal Services client software component ("Software Component") to display or use software programs by connecting to and using the services of Microsoft Windows NT Server 4.0, Terminal Server Edition, any of the Microsoft Windows 2000 operating system products and/or any successor(s) to the foregoing and/or any Microsoft operating system product that incorporates Terminal Services functionality (collectively the “OS Product”) that is designed to operate with the

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

1.4. Accept the License agreement, click “**Next >**”.



Remote Desktop Connection - InstallShield Wizard

Customer Information

Please enter your information.

User Name: Roger Brassard

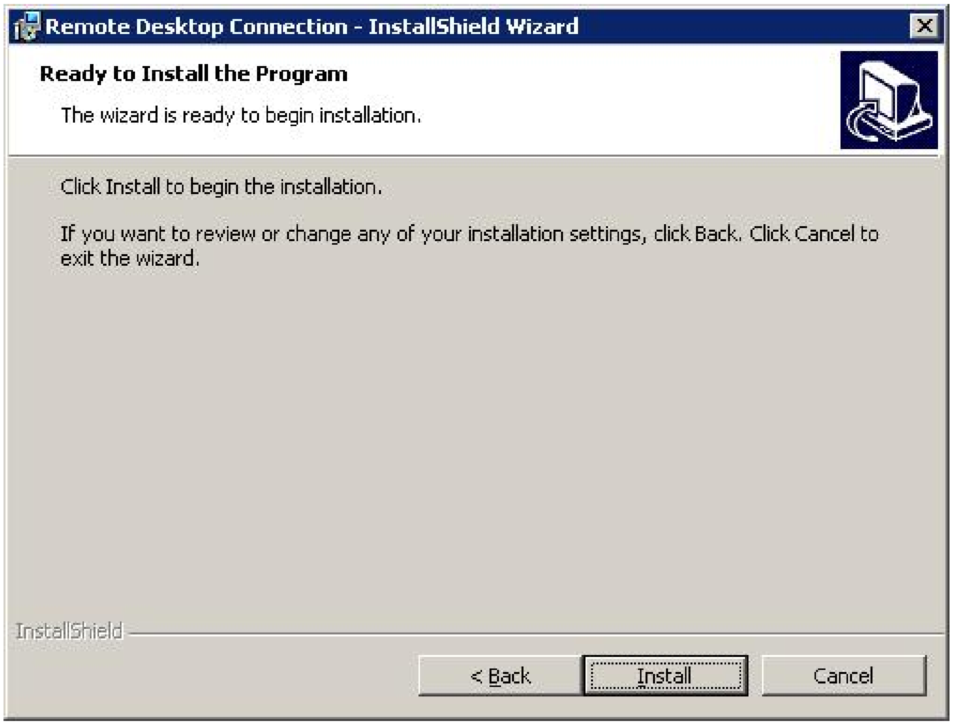
Organization: NORTEL NETWORKS

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Nortel Networks)

1.5. Enter the appropriate User/Organization information and click “**Next >**” to continue.



Remote Desktop Connection - InstallShield Wizard

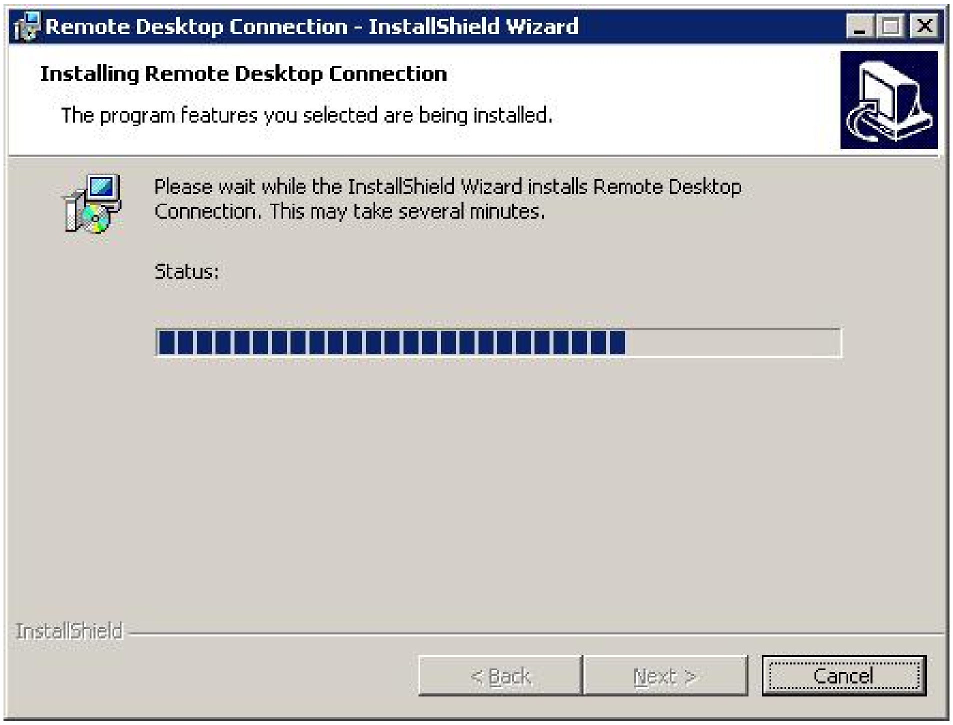
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

1.6. Click “**Install**” to install the client.



Remote Desktop Connection - InstallShield Wizard

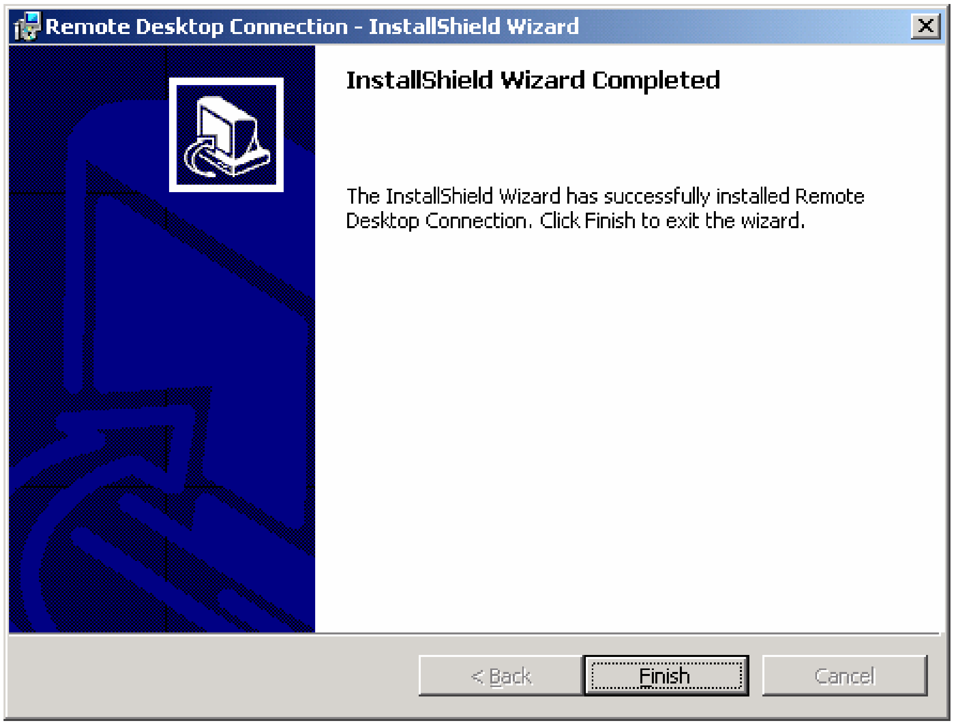
Installing Remote Desktop Connection

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Remote Desktop Connection. This may take several minutes.

Status:

1.7. Once all software has been installed, “Completed” window will appear.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Remote Desktop Connection. Click Finish to exit the wizard.

1.8. Click “**Finish**” to close the wizard window.

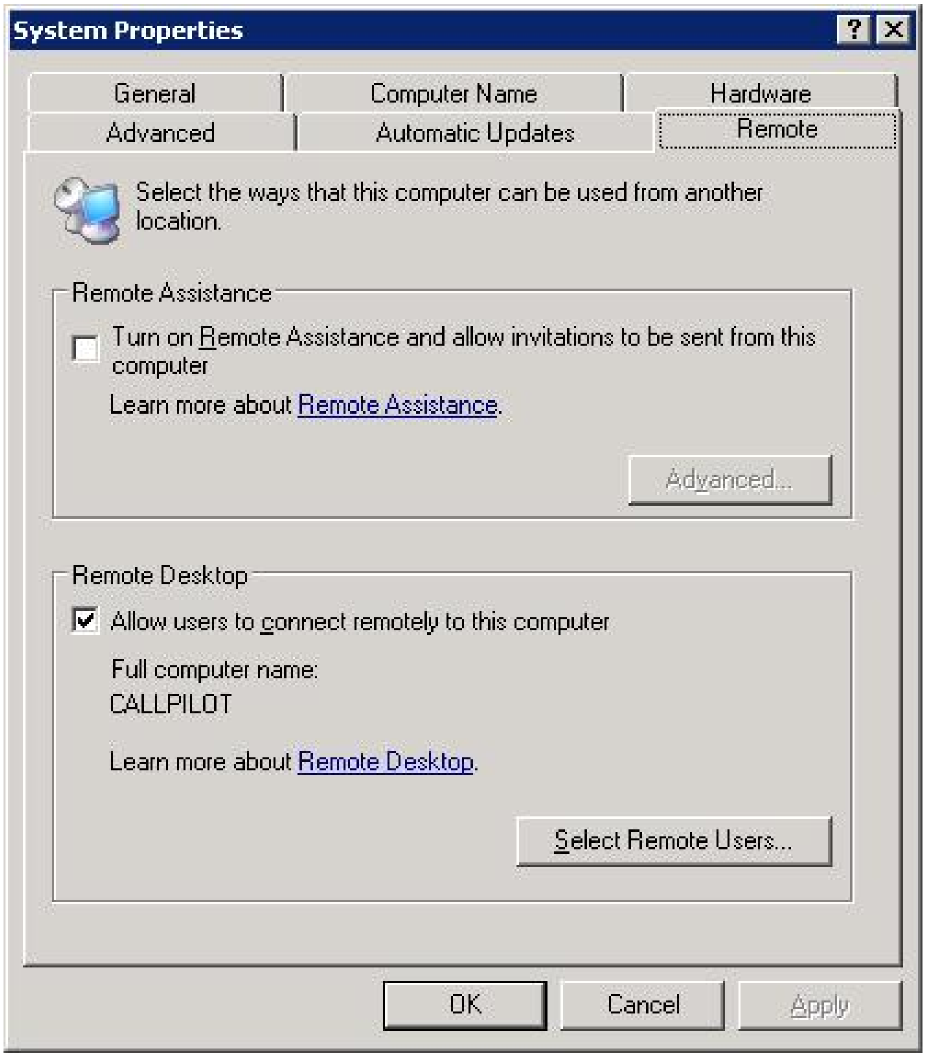
2. Enable Remote Desktop feature and Set policy on host

All CallPilot 3.0 and later servers come with the Remote Desktop server enabled and configured for use by default.

THERE IS USUALLY NO NEED TO PERFORM THE STEPS SHOWN IN THIS SECTION.

If necessary, Remote Desktop access can be enabled or disabled as follows.

2.1. From the CallPilot server desktop, right-click on **My Computer** and choose **Properties**, then click on the **Remote tab**.



Select the ways that this computer can be used from another location.

Remote Assistance

☐ Turn on Remote Assistance and allow invitations to be sent from this computer

Learn more about Remote Assistance.

Remote Desktop

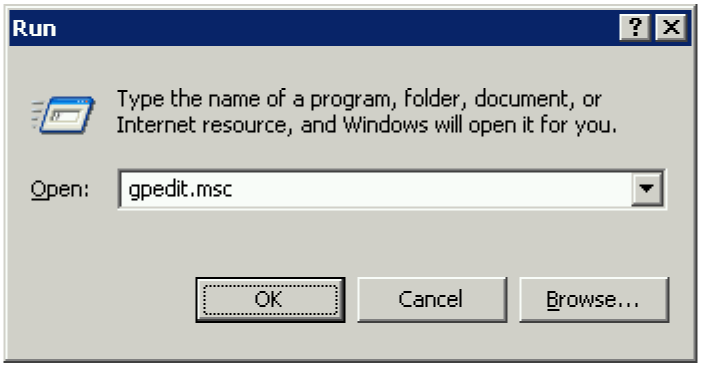
☑ Allow users to connect remotely to this computer

Full computer name:
CALLPILOT

Learn more about Remote Desktop.

2.2. Ensure the “Allow users to connect remotely to this computer” checkbox is selected. Click “**OK**” to close this window.

2.3. There are five (5) options available for remote control settings. To choose among options, you need the Group Policy Snap-in. Open a command prompt window by clicking Start > Run. In the “Open” window type “**gpedit.msc**” and click “**OK**” or press **<Enter>**.

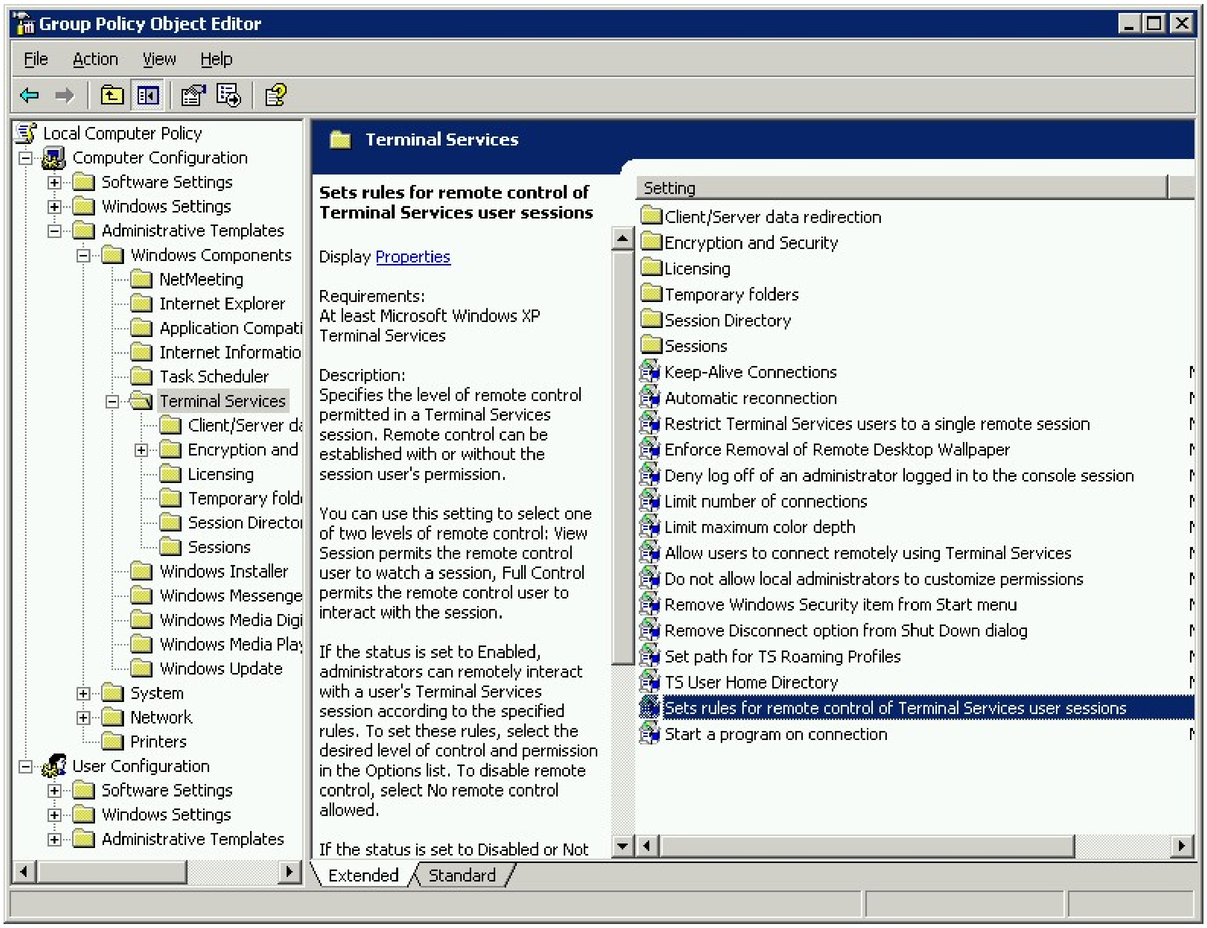


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

2.4. On left side of window, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then select **Terminal Services**.



Sets rules for remote control of Terminal Services user sessions

Display Properties

Requirements:
At least Microsoft Windows XP Terminal Services

Description:
Specifies the level of remote control permitted in a Terminal Services session. Remote control can be established with or without the session user's permission.

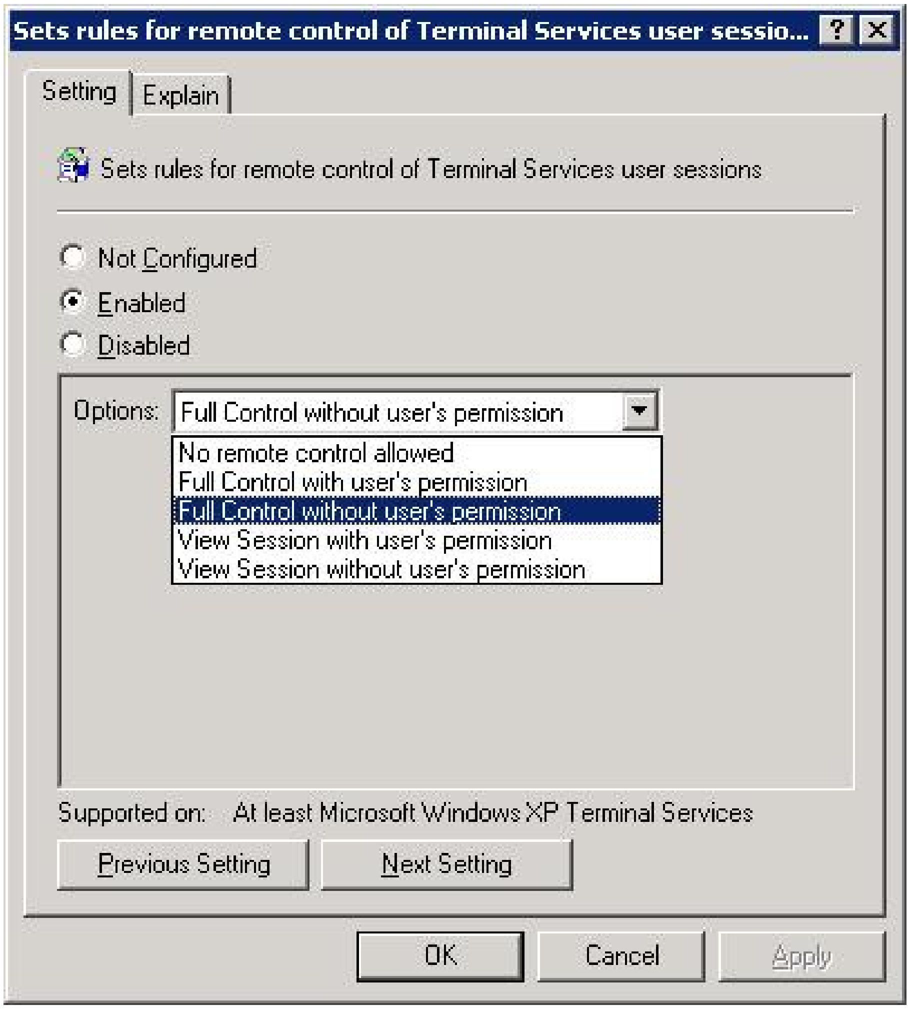
You can use this setting to select one of two levels of remote control: View Session permits the remote control user to watch a session, Full Control permits the remote control user to interact with the session.

If the status is set to Enabled, administrators can remotely interact with a user's Terminal Services session according to the specified rules. To set these rules, select the desired level of control and permission in the Options list. To disable remote control, select No remote control allowed.

If the status is set to Disabled or Not

Setting
- Client/Server data redirection
- Encryption and Security
- Licensing
- Temporary folders
- Session Directory
- Sessions
- Keep-Alive Connections
- Automatic reconnection
- Restrict Terminal Services users to a single remote session
- Enforce Removal of Remote Desktop Wallpaper
- Deny log off of an administrator logged in to the console session
- Limit number of connections
- Limit maximum color depth
- Allow users to connect remotely using Terminal Services
- Do not allow local administrators to customize permissions
- Remove Windows Security item from Start menu
- Remove Disconnect option from Shut Down dialog
- Set path for TS Roaming Profiles
- TS User Home Directory
- Sets rules for remote control of Terminal Services user sessions
- Start a program on connection

2.5. On right side of the window, double-click on “**Sets rules for remote control terminal services user sessions**”. Select “**Enabled**” and five (5) options are available:



Sets rules for remote control of Terminal Services user sessio...

Sets rules for remote control of Terminal Services user sessions

○ Not Configured
● Enabled
○ Disabled

Options: Full Control without user's permission

No remote control allowed
Full Control with user's permission
Full Control without user's permission
View Session with user's permission
View Session without user's permission

Supported on: At least Microsoft Windows XP Terminal Services

2.6. Adjust the set settings as required and click “**OK**” to close the window.

The default and recommended setting for CallPilot is “**Enabled” with Option “Full Control without User’s permission**” selected. This allows for RDC sessions without requiring interaction/consent from a local console user.

2.7. Use **File** > **Exit** to close the “Group Policy Object Editor” window.

3. Establish a RAS connection

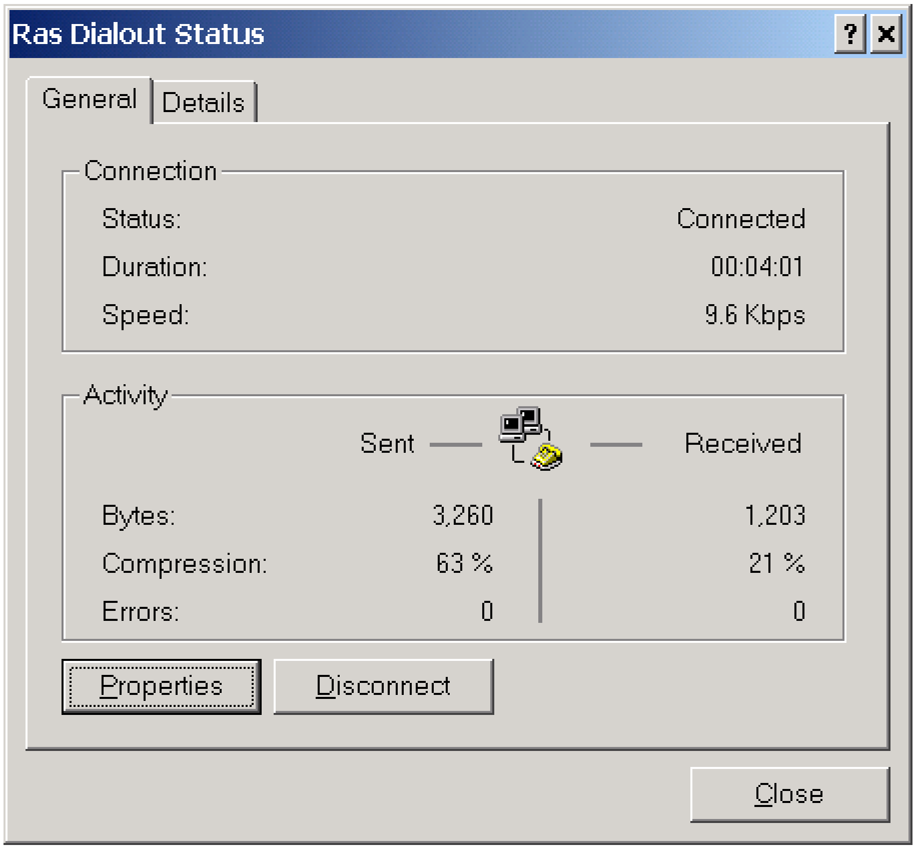
If the CallPilot server is not directly accessible from the Client PC via an intranet or VPN, it will be necessary to establish a Remote Access Service (RAS) connection. This is unchanged from previous CallPilot releases – using Dial-up Networking from the Client Windows PC.

Note: The details of using Dial-up Networking vary depending on which version of Windows Operating System is running on the Client PC. Refer to the CallPilot NTPs, Windows Help, or other Microsoft documentation for details.

The following example is from a client PC running Microsoft Windows 2000 Professional.

Connect to the CallPilot server using Dial-Up Networking. Use the NGenDist or NGenSys accounts since these accounts are enabled for dial-up access. You will need the password for the account.

3.1. Right-click the connection icon in the system tray and choose **Status** (or just double-click the icon). The RAS "Status" window appears.



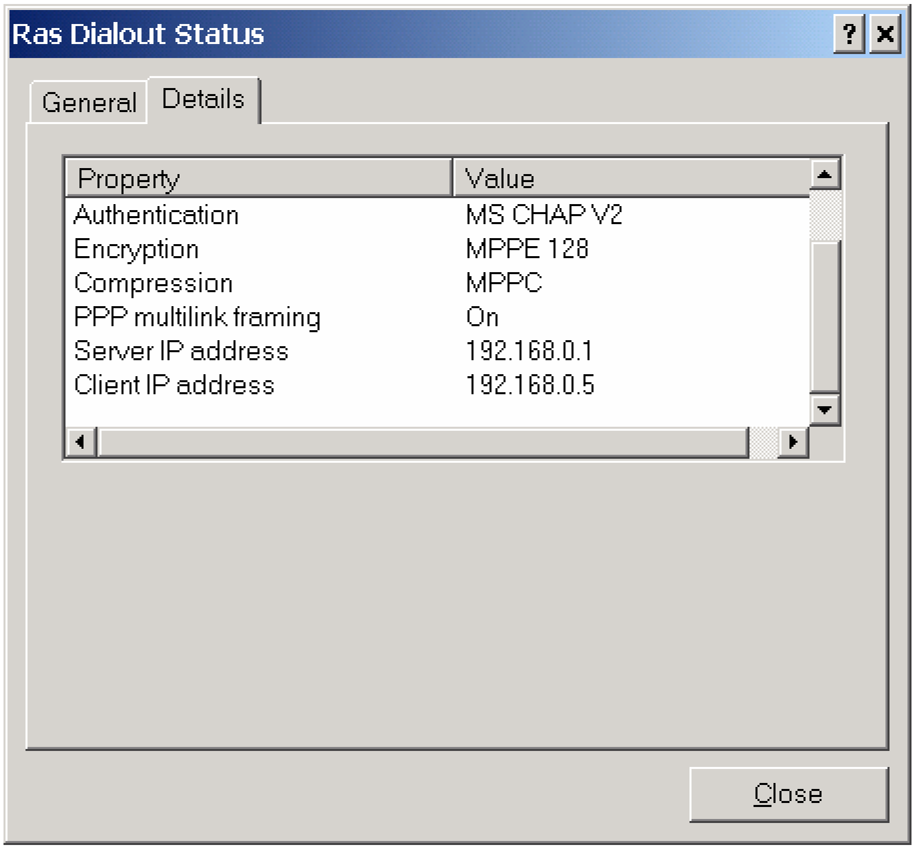
Connection

Status:	Connected
Duration:	00:04:01
Speed:	9.6 Kbps

Activity

	Sent	Received
Bytes:	3,260	1,203
Compression:	63 %	21 %
Errors:	0	0

3.2. To obtain the IP address, select the “**Details**” tab.



Property	Value
Authentication	MS CHAP V2
Encryption	MPPE 128
Compression	MPPC
PPP multilink framing	On
Server IP address	192.168.0.1
Client IP address	192.168.0.5

3.3. From the “Details” tab, note the Server IP address. (192.168.0.1 in this example).

3.4. Close the Dial-Up Networking Status window by clicking “**Close**”.

4. Starting the Remote Desktop Client

4.1. Method 1: Private Session (preferred method)

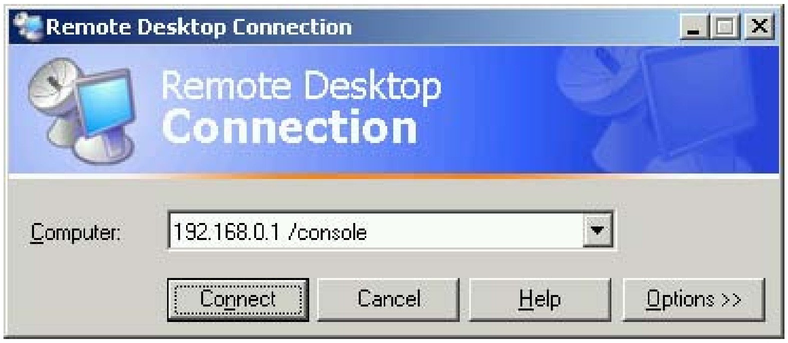
Use this method when needing to perform the following tasks:

- Establish a private login session remotely, not visible from the server console.
- Utilize the CallPilot Support Tools
- Transfer files from local PC to the CallPilot server
- Install a PEP/Service Update that interacts with the CallPilot database

Note: If the local console is already logged in, it will get forcibly logged out (unsaved data will be lost). Your actions will not be visible on the local console.

1. From the client PC, start the Remote Desktop Connection for Windows Server 2003 Client. The usual shortcuts are:

   - Start > Programs > Remote Desktop Connection
   - Start > Programs > Accessories > Communications > Remote Desktop Connection



Computer: 192.168.0.1 /console

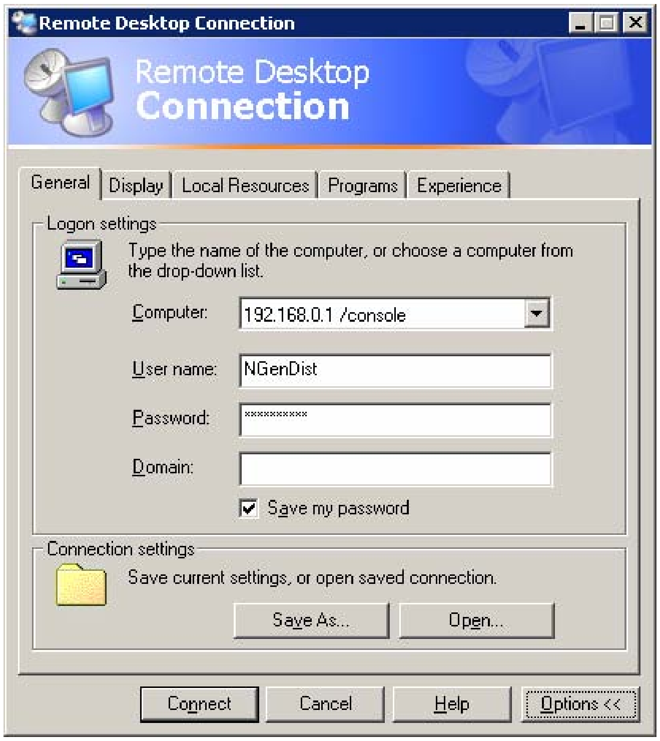
Note: When using the "/console" suffix, this assures a private session connected to the logical console of the CallPilot server.

Note: A space character exists between the last digit of the IP address (or computer name) and the "/console".

For a dial-up RAS connection, use the IP address for the Dial-Up server as shown in the preceding section.

For intranet or VPN connections, you may use the computer name instead of an IP address.

2. Click the “**Options >>**” button:



Remote Desktop Connection

Remote Desktop Connection

Logon settings

Type the name of the computer, or choose a computer from the drop-down list.

Computer: 192.168.0.1 /console

User name: NGenDist

Password: **********

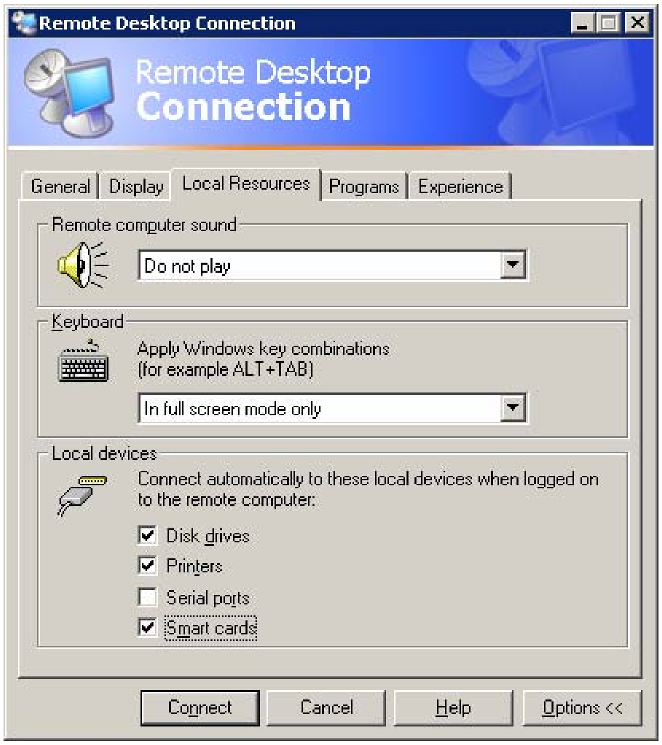
Domain:

☑ Save my password

Connection settings

Save current settings, or open saved connection.

3. Fill in the Computer (name or IP address with a “space” character before “/console”), User name and Password. Click the “**Local Resources**” tab:



Remote Desktop Connection

Remote Desktop Connection

Remote computer sound

Do not play

Keyboard

Apply Windows key combinations (for example ALT+TAB)

In full screen mode only

Local devices

Connect automatically to these local devices when logged on to the remote computer:

☑ Disk drives

☑ Printers

☐ Serial ports

☑ Smart cards

The “Local Resources” tab allows you to specify that the Disk drives and Printers from the client PC are to be made available on the target CallPilot server. Recommended settings:

• Remote Computer Sound:	Leave at remote computer
• Keyboard:	On the remote computer
• Local Devices:	**Note**: Disk Drives must be checked to enable transferring of files (SU/PEP, logs, traces, etc) to and from the CallPilot server.

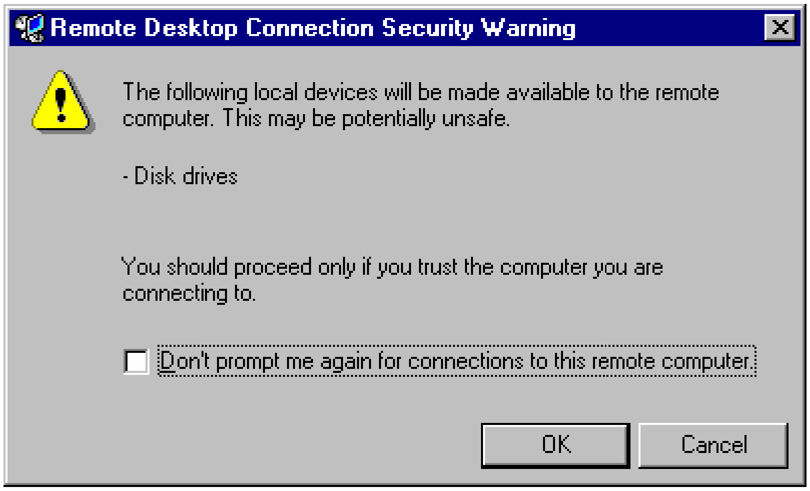
The “Display” tab allows you to specify the screen size and colors for the remote desktop connection. Recommended settings:

• Remote Desktop size:	800x600
• Color Depth:	High Color (16 bit)

The “Experience” tab allows you to specify the connection speed (broadband or modem) that the connection will be optimized for. Recommended settings:

• Performance:	Modem (28.8 Kbps)
• Bitmap caching:	Enabled

4. Click “**Connect**” to create the remote desktop connection. The following “Security Warning” window will appear.



Remote Desktop Connection Security Warning

The following local devices will be made available to the remote computer. This may be potentially unsafe.

- Disk drives

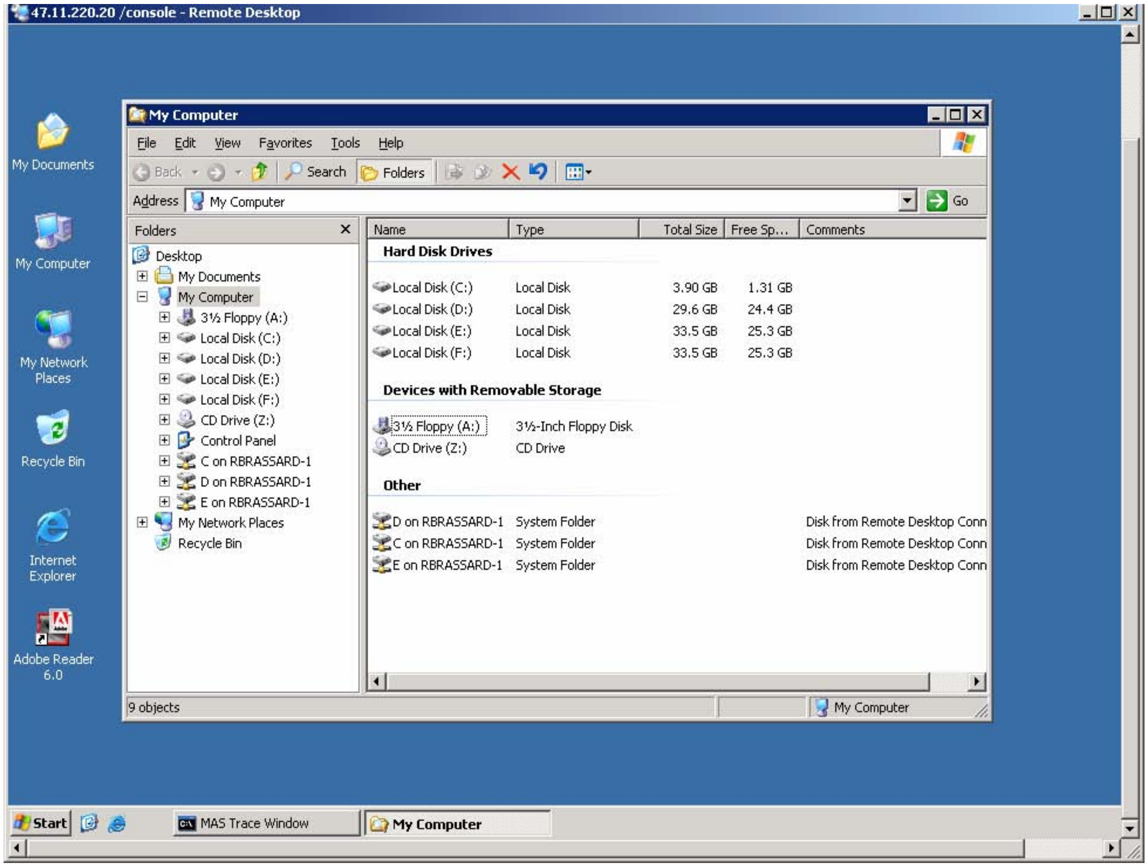
You should proceed only if you trust the computer you are connecting to.

☐ Don't prompt me again for connections to this remote computer.

5. Click “**OK**” to continue

6. A remote desktop session will be started in a window on the client PC.

   Example of RDC session (with an open “My Computer” window):



Name	Type	Total Size	Free Sp...	Comments
Hard Disk Drives				
Local Disk (C:)	Local Disk	3.90 GB	1.31 GB	
Local Disk (D:)	Local Disk	29.6 GB	24.4 GB	
Local Disk (E:)	Local Disk	33.5 GB	25.3 GB	
Local Disk (F:)	Local Disk	33.5 GB	25.3 GB	
Devices with Removable Storage				
3½ Floppy (A:)	3½-Inch Floppy Disk			
CD Drive (Z:)	CD Drive			
Other				
D on RBRASSARD-1	System Folder			Disk from Remote Desktop Conn
C on RBRASSARD-1	System Folder			Disk from Remote Desktop Conn
E on RBRASSARD-1	System Folder			Disk from Remote Desktop Conn

You can maximize the window to make it full screen. The CallPilot “MAS Trace Window” should be visible on the taskbar. By default, this is a private session which cannot be seen from the CallPilot local console. All disk drives from the client (including floppy and CD drives) will be mapped to the CallPilot server. Files can be transferred by copying them using Windows Explorer.

If the RAS connection drops, the Remote Desktop Connection will be disconnected. You can dial back in to re-establish the RAS connection. Then reconnect using Remote Desktop Client in the same way. You will see any windows you left open.

4.2. Method 2: Shared Session (only if local console is logged on)

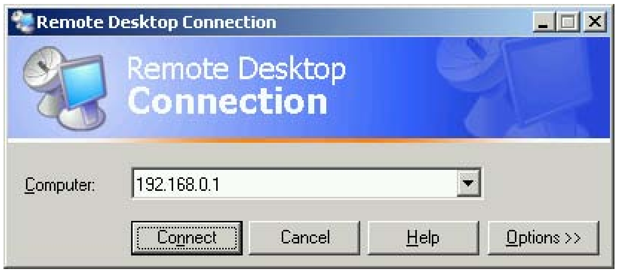
Use this method when one or more of the following conditions are true:

- Need a “shared” login session where you are able to see exactly what is on the local console and all tasks are visible from the server console. (i.e. during mentoring sessions, or investigating an existing alarm message displayed on the console, etc.)
- When no transfer of files between the local PC to the CallPilot server will occur

You can choose to start a shared session as follows:

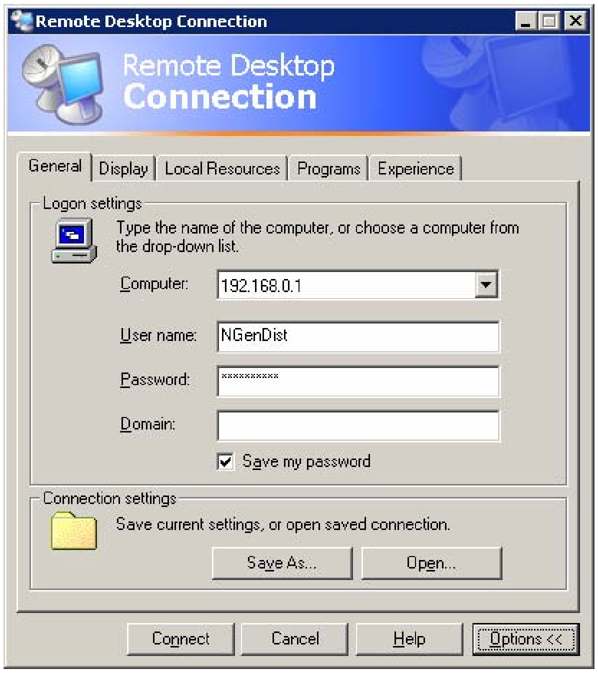
1. From the client PC, start the Remote Desktop Connection for Windows Server 2003 Client. The usual shortcuts are:

   - Start > Programs > Remote Desktop Connection
   - Start > Programs > Accessories > Communications > Remote Desktop Connection



Computer: 192.168.0.1

2. Click the “**Options >>**” button:



Type the name of the computer, or choose a computer from the drop-down list.

Computer: 192.168.0.1

User name: NGenDist

Password: **********

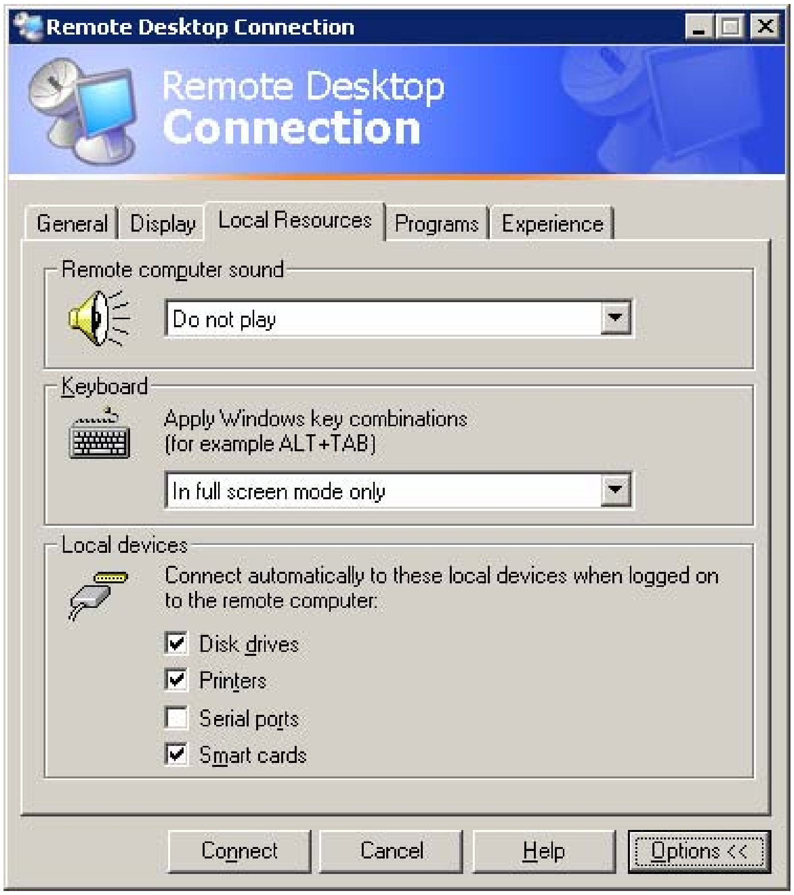
Domain:

☑ Save my password

Save current settings, or open saved connection.

3. Fill in the Computer (name or IP address), User name and Password.

   For a dial-up RAS connection, use the IP address for the Dial-Up server as shown in the preceding section. Click the "**Local Resources**" tab:



Remote computer sound

Do not play

Keyboard

Apply Windows key combinations
(for example ALT+TAB)

In full screen mode only

Local devices

Connect automatically to these local devices when logged on to the remote computer:

☑ Disk drives
☑ Printers
☐ Serial ports
☑ Smart cards

The "Local Resources" tab allows you to specify that the Disk drives and Printers from the client PC are to be made available on the target CallPilot server. Recommended settings:

• Remote Computer Sound:	Leave at remote computer
• Keyboard:	On the remote computer
• Local Devices:	**Note:** Disk Drives must be checked to enable transferring of files (SU/PEP, logs, traces, etc) to and from the CallPilot server.

Note: Disk drive sharing is needed to be able to transfer files to and from the CallPilot server. While file transfer is not possible in a "shared" session, it's recommended this setting still be selected.

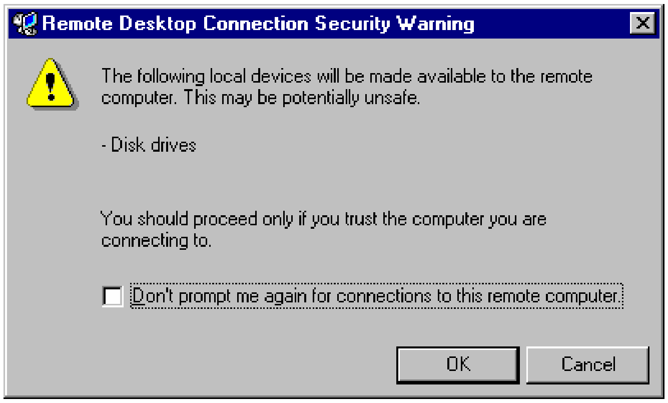
The “Display” tab allows you to specify the screen size and colors for the remote desktop connection. Recommended settings:

Remote Desktop size:	800x600
Color Depth:	High Color (16 bit)

The “Experience” tab allows you to specify the connection speed (broadband or modem) that the connection will be optimized for. Recommended settings:

Performance:	Modem (28.8 Kbps)
Bitmap caching:	Enabled

4. Click “**Connect**” to create the remote desktop connection.



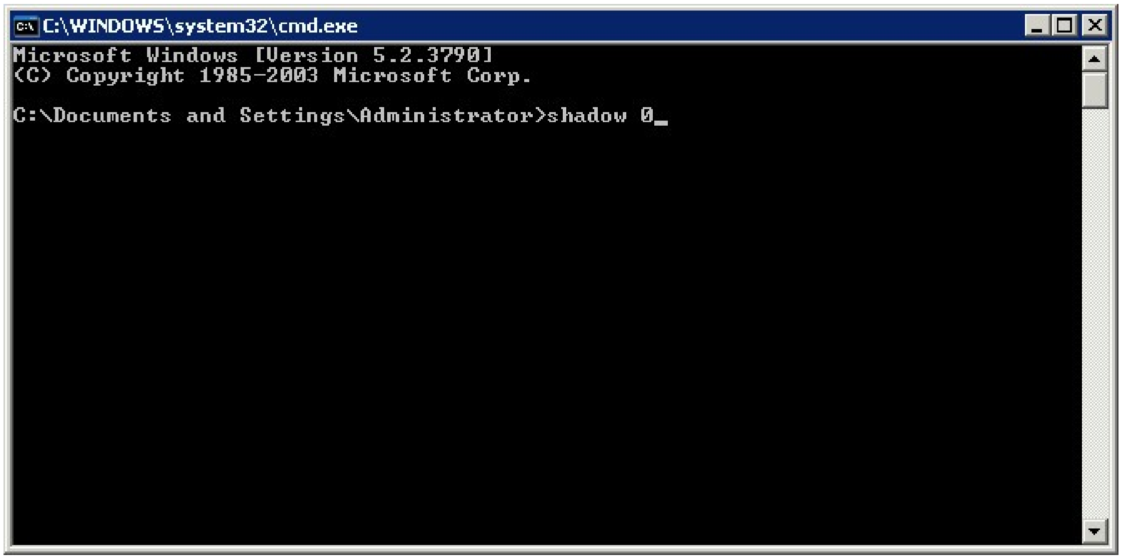
The following local devices will be made available to the remote computer. This may be potentially unsafe.

- Disk drives

You should proceed only if you trust the computer you are connecting to.

☐ Don't prompt me again for connections to this remote computer.

5. Click “**OK**” to continue.
6. Then, within the Remote Desktop session, start a command prompt and enter the command “**shadow 0**”:
   - Start > Run, then in the “Open” box enter “**cmd**” and click “**OK**”.
   - Within a command prompt window, type “**shadow 0**” and **<Enter>**



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>shadow 0_
```

This will put your private session on hold and will start a shared session, allowing the local and remote consoles to share/view the same thing. All your remote actions will be visible on the local console. Both the local and remote mouse and keyboard are active. The screen resolution of the Remote Desktop Connection will be adjusted to match the resolution of the local console. The disk drives shared from the client PC are not visible after you enter the “shadow 0” command.

The CallPilot desktop background will be visible during a shared session. This can slow performance if you are connected over a modem. You can turn off the background using Control Panel > Display > Desktop tab (set it to None). Once completed with your shared session, remember to set the background back to its original setting:

Start > Settings > Control Panel > Display > Desktop tab

(browse to path: C:\windows\system32\CP3BackSplashs\ CPBAKxxxx.bmp where xxxx = platform number)

To cancel shadowing of the CallPilot console and return to the original session, hold the **CTRL** key while pressing the ***** key on the numeric keypad. The shared disk drives will again be visible. You can toggle back and forth using shadow 0 and CTRL num *.

Note: If no numeric keypad exists (e.g. using a laptop), use the Function and * keys.

Note: If you logout while in a shared session, console shadowing will end and you will revert to your initial private session. The local console session will be logged out.

Note: PEP installs and CallPilot support tools may not work properly when you are in an un-shadowed session not connected to the console.

Note: While in a “shadow 0” session, you will be unable to see your local drives on the remote server.

Note: If the local console is not already logged on when the “shadow 0” command is used, the system will return the following error within the Command prompt window:

Remote Control Failed. Error 7050
Error [7050]:The requested session cannot be controlled remotely. This may be because the session is disconnected or does not currently have a user logged on.

You can still connect to the console session by logging out from your RDC session, then reconnecting using the /console option (Method 1).

5. CallPilot Support Tools

Certain support tools and operations (including PEP installs) will work properly only when run from the logical console. MMFS and database operations can only be done from the logical console session. These tools must be run using either Method 1 (a private session connected to the console) or by using Method 2, after entering “shadow 0” (i.e. a shared session connected to the console). Once you cancel console shadowing, support tool operations may not work unless you re-shadow.

If you wish to use support tools without the customer being able to see on the console, use Method 1 to create a private session. This will log out any local user. Note that you can start and stop Remote Desktop sessions without dropping the RAS dial-up connection.

Note: PEP installs that perform database or MMFS operations may also require use of a session connected to the console.

Note that there is no way to send the "CTRL-ALT-DEL" key combination. If you need to reboot the CallPilot 3.0 server, use "Start - Shutdown". (Although this method of restarting caused problems with the database on earlier CallPilot software releases, it does not cause any problems on CallPilot 3.0)

To disconnect finally, you log out from the NGenDist session. This will close any programs you started and terminate the Remote Desktop Client. You can then hang up the RAS connection.

6. RAS dial-up required to establish RDC

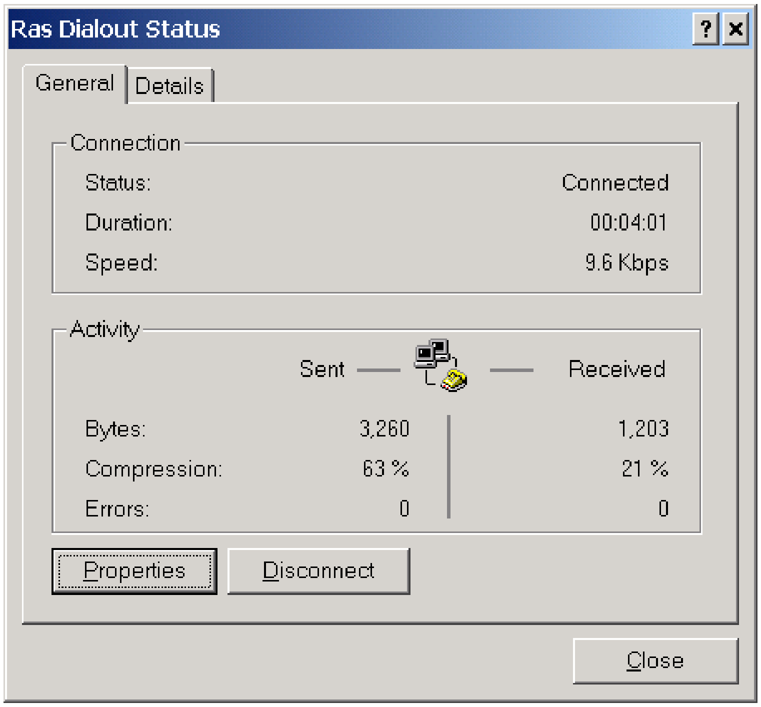
Unfortunately it is not possible to use Remote Desktop directly through a modem. RAS dial-in must be working for this form of remote access to work.

7. “Double-Hop” remote control

A common support scenario is for one technician to dial in to a customer’s CallPilot server, then another technician controls the first technician’s computer (e.g. via intranet or VPN), thereby gaining access to the dial-up remote control session on CallPilot. For this to work, the intermediate computer’s Dial-Up Networking TCP/IP Settings must have the setting “Use default gateway on remote network” unchecked.

This can be modified using the following procedure:

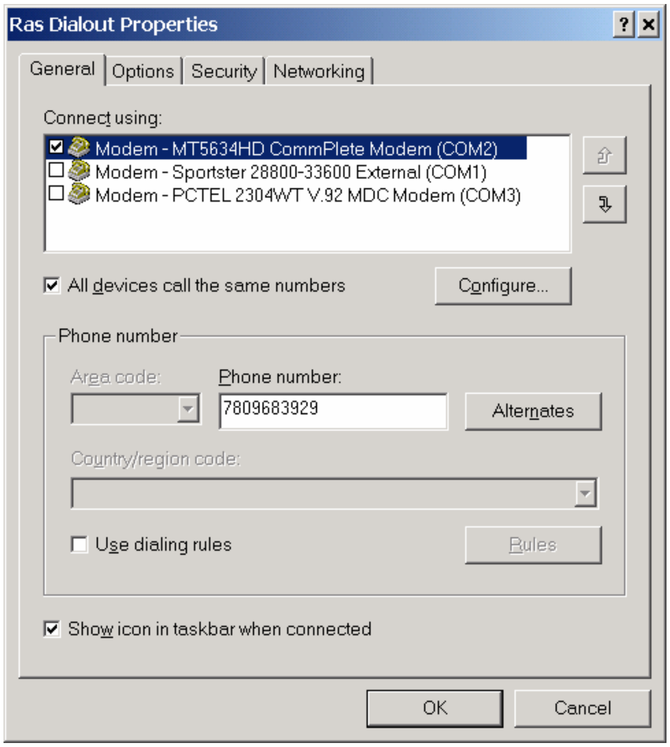
7.1. Double-click the Dial-up Networking connection icon in the system tray. The “Status” window will appear.



Status: Connected
Duration: 00:04:01
Speed: 9.6 Kbps

	Sent	Received
Bytes:	3,260	1,203
Compression:	63 %	21 %
Errors:	0	0

7.2. Click the “**Properties**” button. The “Properties” window will appear.



Connect using:

☑ Modem - MT5634HD CommPlete Modem (COM2)
☐ Modem - Sportster 28800-33600 External (COM1)
☐ Modem - PCTEL 2304WT V.92 MDC Modem (COM3)

☑ All devices call the same numbers

Phone number

Area code:

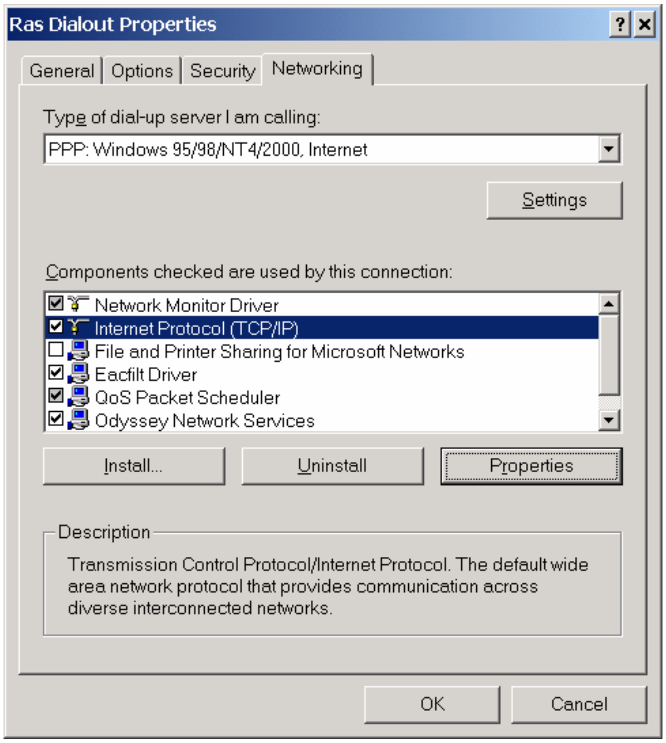
Phone number: 7809683929

Country/region code:

☐ Use dialing rules

☑ Show icon in taskbar when connected

7.3. In the “Properties” window, select the **Networking** tab.



Type of dial-up server I am calling: PPP: Windows 95/98/NT4/2000, Internet

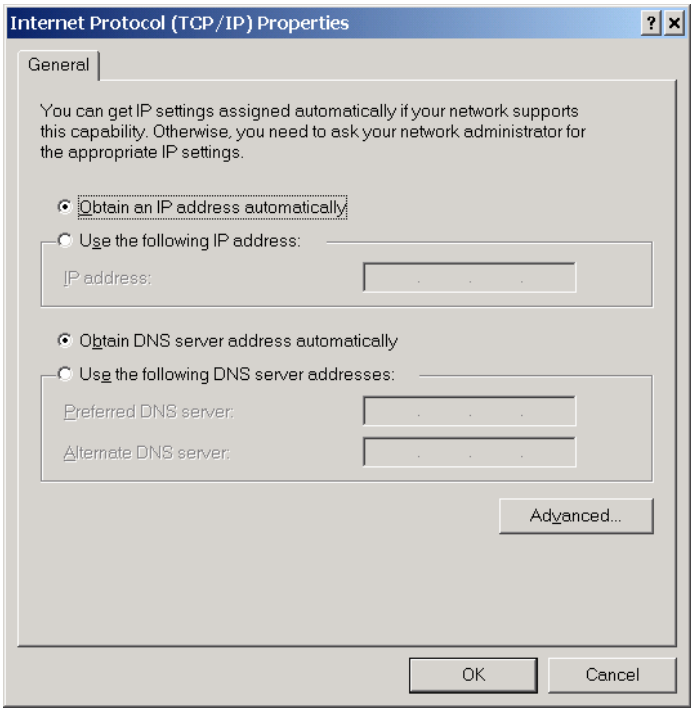
Components checked are used by this connection:

☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)
☐ File and Printer Sharing for Microsoft Networks
☑ Eacfilt Driver
☑ QoS Packet Scheduler
☑ Odyssey Network Services

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

7.4. Highlight the Internet Protocol (TCP/IP) component and click the “**Properties**” button. **DO NOT** un-check “Internet Protocol (TCP/IP).



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

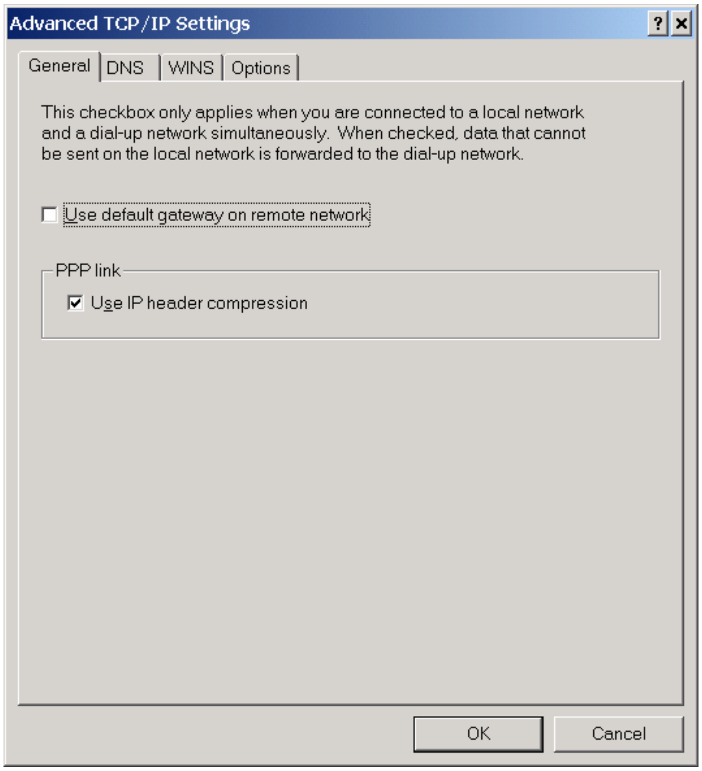
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

7.5. In the Internet Protocol (TCP/IP) Properties window, click the “**Advanced**” button.



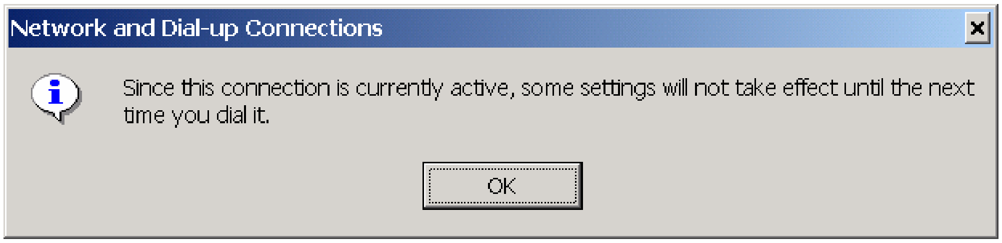
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

☐ Use default gateway on remote network

PPP link

☑ Use IP header compression

7.6. In the Advanced TCP/IP settings, uncheck the setting ""Use default gateway on remote network". Click OK to close all windows. The following “warning” will appear.


Network and Dial-up Connections

Since this connection is currently active, some settings will not take effect until the next time you dial it.

7.7. Disconnect and re-connect to the remote server. The modified “Default gateway” setting will now be active.

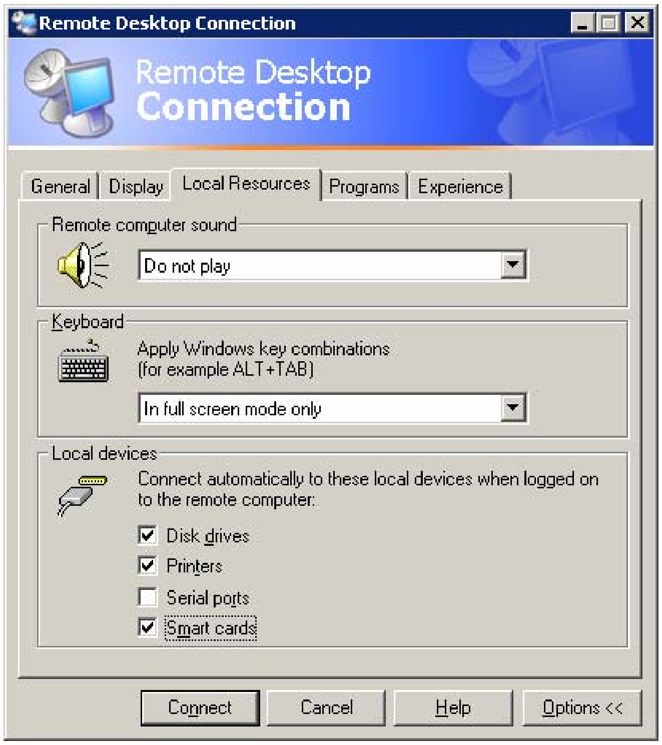
Note: It is possible to use pcAnywhere to control a PC that is in turn connected into a CallPilot server via Remote Desktop Connection. However, the right keyboard shift key does not seem to work in this scenario, nor does the CAPS LOCK key. You must use the left shift key only to input upper case characters. This is especially important when typing passwords. (This problem was noted using pcAnywhere 10.5 and 11.01).

Note: Double-Hop remote control is also possible using two Remote Desktop Connections if the intermediate PC is running an OS that includes the Remote Desktop Connections Server. This works fine, however it can be a little confusing if both sessions are in full-screen mode. Refrain from maximizing the Remote Desktop windows to see them nested.

8. Transferring Files in Remote Desktop Connection Session

Before a file can be transferred between a local computer (the computer that is launching the Remote Desktop Connection and making the remote support connection session) and the remote CallPilot server, the local disk drives must be made available during the Remote Desktop Connection logon session.

As noted in sections 4.1 and 4.2, ensure the "Local devices" settings include the local "Disk Drives" to enable file transfer while in a Remote Desktop Connection session:



Remote Desktop Connection

Remote Desktop Connection

Remote computer sound

Do not play

Keyboard

Apply Windows key combinations (for example ALT+TAB)

In full screen mode only

Local devices

Connect automatically to these local devices when logged on to the remote computer:

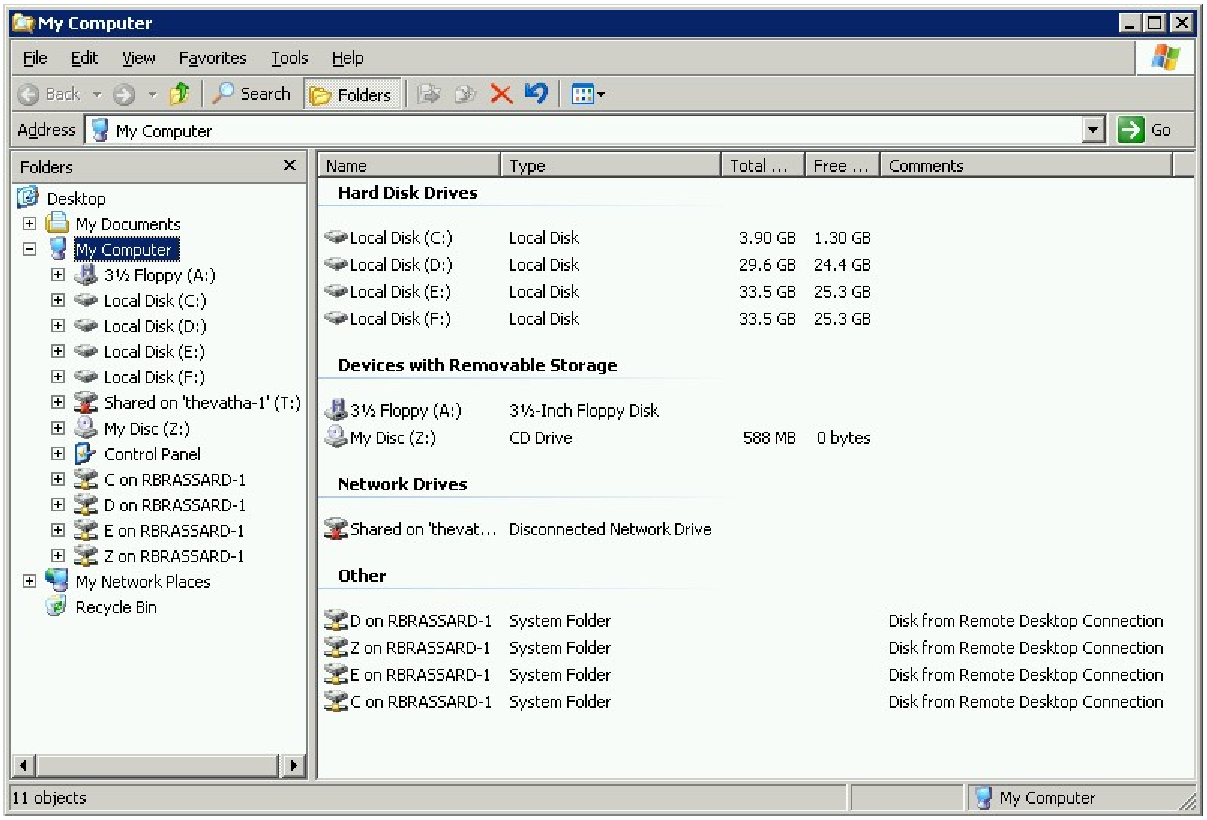
☑ Disk drives

☑ Printers

☐ Serial ports

☑ Smart cards

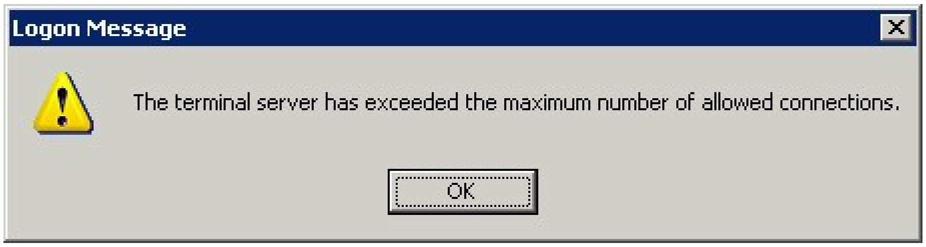
While in a session, moving files between the local computer and the remote CallPilot server can be done within an Explorer window. If the "Local devices" setting for Disk Drives was checked during the initial connection, the local drives will be displayed in the "Other" section as indicated in the following example:



Name	Type	Total ...	Free ...	Comments
Hard Disk Drives				
Local Disk (C:)	Local Disk	3.90 GB	1.30 GB	
Local Disk (D:)	Local Disk	29.6 GB	24.4 GB	
Local Disk (E:)	Local Disk	33.5 GB	25.3 GB	
Local Disk (F:)	Local Disk	33.5 GB	25.3 GB	
Devices with Removable Storage				
3½ Floppy (A:)	3½-Inch Floppy Disk			
My Disc (Z:)	CD Drive	588 MB	0 bytes	
Network Drives				
Shared on 'thevat...	Disconnected Network Drive			
Other				
D on RBRASSARD-1	System Folder			Disk from Remote Desktop Connection
Z on RBRASSARD-1	System Folder			Disk from Remote Desktop Connection
E on RBRASSARD-1	System Folder			Disk from Remote Desktop Connection
C on RBRASSARD-1	System Folder			Disk from Remote Desktop Connection

9. Terminal Server Maximum Connections Exceeded Error

CallPilot supports a maximum of two (2) remote sessions and one (1) console session concurrently. If these limits are exceeded, when trying to start a Remote Desktop session you might receive the following error:



The terminal server has exceeded the maximum number of allowed connections.

If this occurs, it is still possible to make a connection without the need for local intervention. Just use Method 1 as described in section 4.1 to connect. This will force any local user to logout and will allow you to connect.

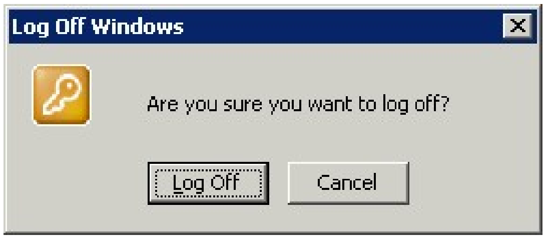
10. Disconnecting the Remote Desktop Connection Session

You should not terminate a Remote Desktop Connection by simply clicking “X” on the Remote Desktop Window. This will disconnect your session, but the session will continue to exist on the CallPilot server. Any programs you were running will continue to run. You can connect again and see the same session.

If you are finished with remote support, you should LOG OFF your session. This can be done using Start > Logoff, or Start > Shutdown >Logoff.

To log off and end the Remote Desktop Connection session:

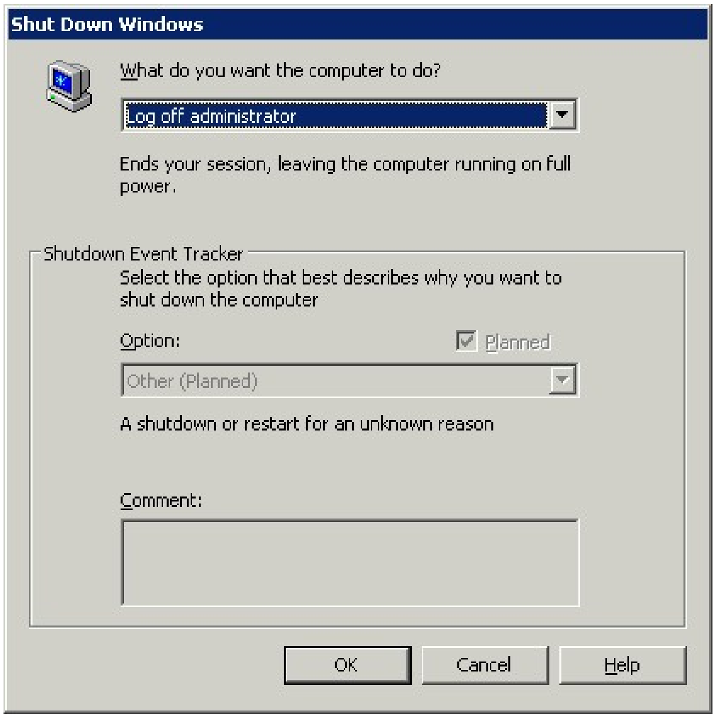
10.1. In the Remote Desktop Connection window, click **Start**, and then “**Log Off <username>**”.   The following confirmation window will appear. Click “**Log Off**” to exit the Remote Desktop Connection session.



Log Off Windows

Are you sure you want to log off?

10.2. Alternatively, in the Remote Desktop Connection window, click **Start**, and then “**Shutdown**”. When the “Shut Down Windows” dialog appears, select “**Log Off <username>**”, from the “What to do” box and then click “**OK**”.



Shut Down Windows

What do you want the computer to do?

Log off administrator

Ends your session, leaving the computer running on full power.

Shutdown Event Tracker

Select the option that best describes why you want to shut down the computer

Option: ☑ Planned

Other (Planned)

A shutdown or restart for an unknown reason

Comment:

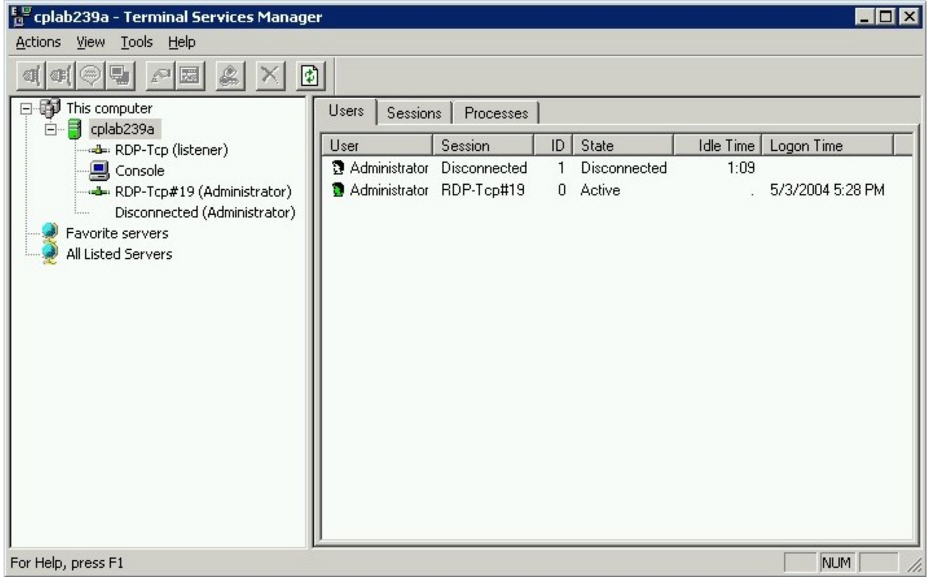
11. View/Disconnect concurrent or previous “stale” sessions

Microsoft Windows Terminal Services Manager provides the administrative user the ability to see different sessions that are active or in-active on the server.

This tool can be used to logoff and/or disconnect any leftover sessions that are no longer needed. It can also be used to send messages to other sessions for messaging between users.

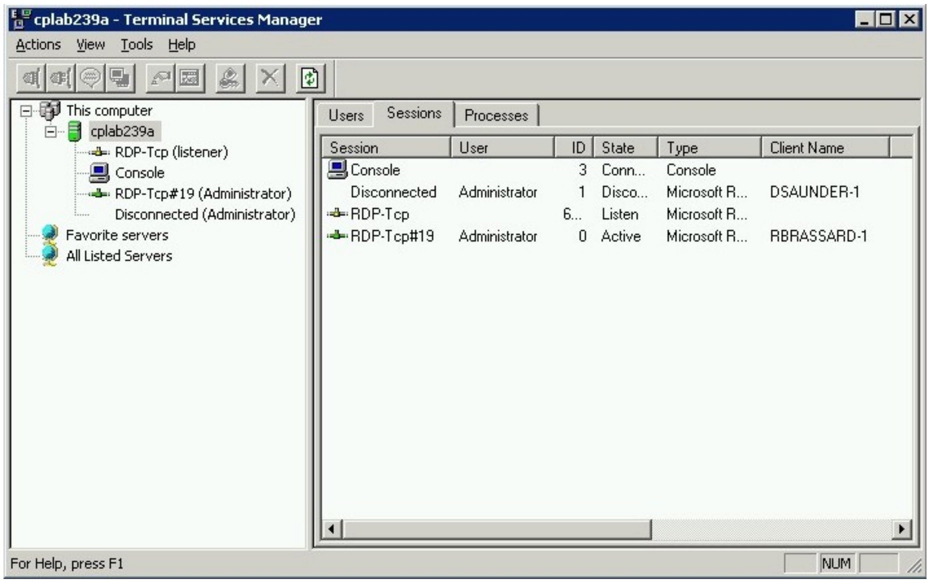
The tool is available using: Start > Programs > Administrative Tools > Terminal Services Manager. Similar functionality is also available from the Users tab of the Task Manager.

Example of Windows Terminal Services Manager (Users):



User	Session	ID	State	Idle Time	Logon Time
Administrator	Disconnected	1	Disconnected	1:09	
Administrator	RDP-Tcp#19	0	Active	.	5/3/2004 5:28 PM

Example of Windows Terminal Services Manager (Sessions):



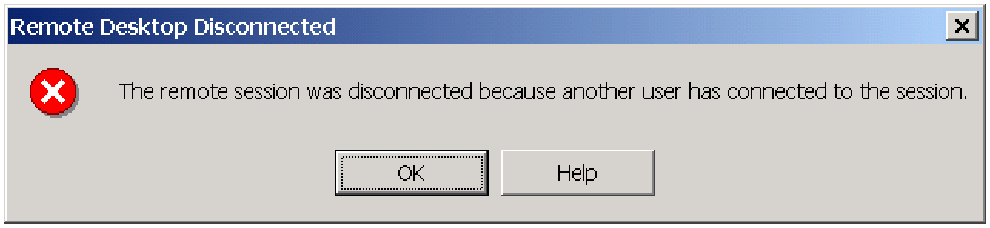
Session	User	ID	State	Type	Client Name
Console		3	Conn...	Console	
Disconnected	Administrator	1	Disco...	Microsoft R...	DSAUNDER-1
RDP-Tcp		6...	Listen	Microsoft R...	
RDP-Tcp#19	Administrator	0	Active	Microsoft R...	RBRASSARD-1

12. Troubleshooting

The following provides troubleshooting information/workarounds for scenarios that might be encountered while using Microsoft RDC.

12.1. Session disconnected unexpectedly

If while in a private console session (e.g. using "192.168.0.1 /console") another user takes away the console (either local to the server, or another remote RDC session), the following message is displayed:



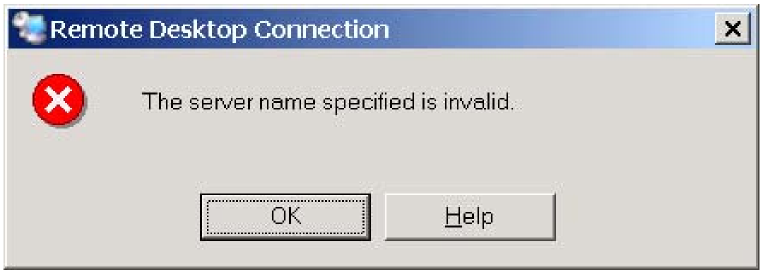
Remote Desktop Disconnected

The remote session was disconnected because another user has connected to the session.

Tip: Contact the site to arrange for access, or use a "shared" session (Method 2) and then message the other user via Windows Terminal Services Manager or Task Manager.

12.2. Receive "The server name specified is invalid" message when trying to connect using "/console" switch, Method 1.

If using an older version of Microsoft Remote Desktop Connection client, and enter a server name of "192.168.0.1 /console", the following message is displayed:



Remote Desktop Connection

The server name specified is invalid.

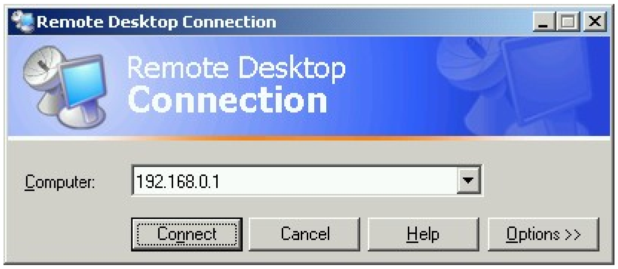
Tip: Upgrade to the newer Windows 2003 RDC client (this document references version control 5.2.3790.0).

Workaround: If the RDC client can't readily be upgraded, the following alternative steps may also be used:

a. Open a command prompt window on your client PC

b. Enter "**mstsc /console**" and press **<Enter>**. The RDC window is now visible.

c. Enter the IP address of the server into the “Computer” field.



Computer: 192.168.0.1

12.3. Unable to transfer files to the remote CallPilot server

If unable to see local client PC files/folders from within the RDC client session, either or both of the following conditions may apply.

Scenario #1: If the Local Devices/Disk Drives option was not checked within the Options window before connecting to the remote server, the local files/folders will not be visible from within the RDC client.

Scenario #2: If connected to the CallPilot server using a shared session (“shadow 0”), files will not be visible and therefore cannot be transferred.

Workaround: When transferring files between the CallPilot server and RDC client PC, use Method-1 “Private” session.

12.4. Connection to server is extremely slow

When using RDC, the access speed is diminished if the Desktop Background setting is turned ON.

Workaround: If using Method-1 (Private session using the “/console” switch), prior to connecting, under Options, in the “Experience” tab, ensure that “Desktop Background” in unchecked.

If using “Method-2 (Shared session using “shadow 0” command), after connecting, and logging onto the server, right-click on the **Desktop**, select **Properties**, then select the **Desktop** tab. In the Background selection box, choose “**None**”.
Click “OK” to close the window.

12.5. “Shadow 0” session fails with error “Remote Control Failed. Error 7050”

If the local console is not already logged on when the “shadow 0” command is used, the system will return the following error within the Command prompt window:

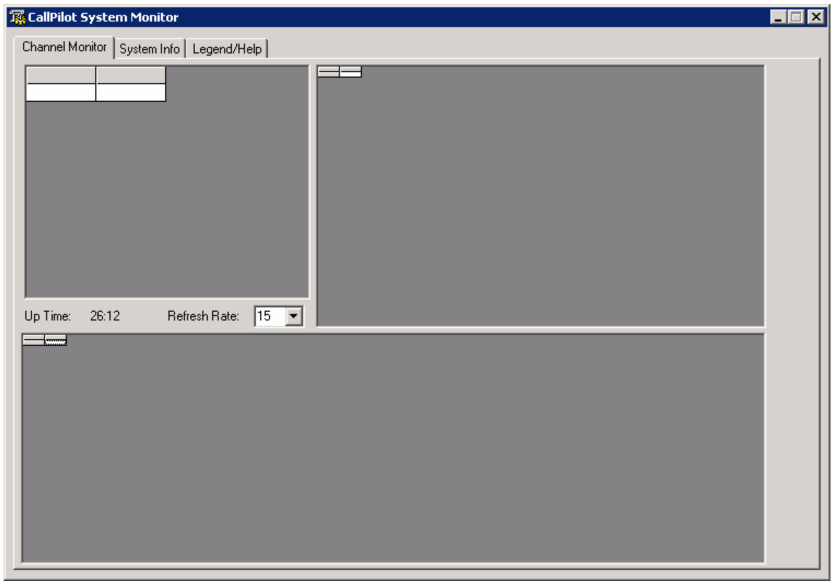
Remote Control Failed. Error 7050
Error [7050]:The requested session cannot be controlled remotely. This may be because the session is disconnected or does not currently have a user logged on.

Workaround: Connect to the console session using the “/console option” (Method 1). This method does not require a user be logged on already.

12.6. System Monitor and/or Support Tools do not return valid/legible information.

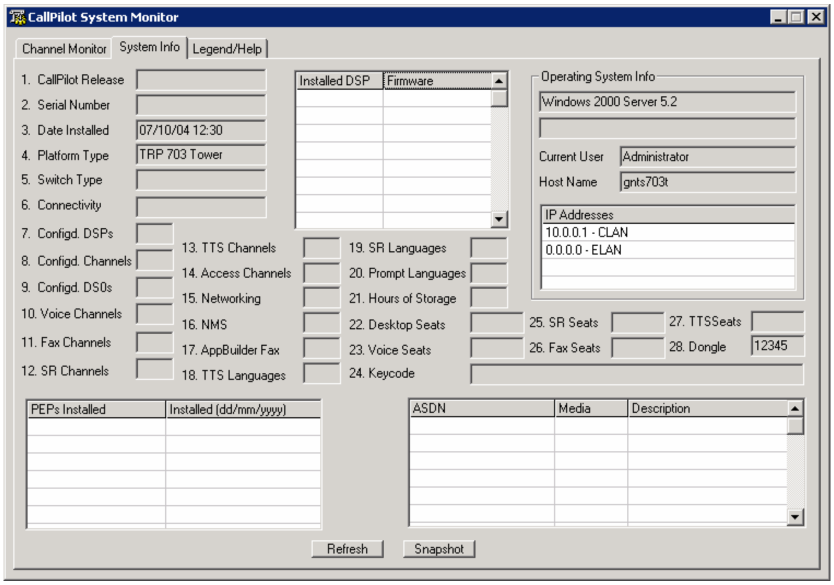
If you connect to the CallPilot server using Method-2 but without issuing the required “shadow 0” command, and then attempt to run various Support Tools/Diagnostics that access the database, each may return invalid results.

For example, when Launching System Monitor:



Up Time: 26:12

Refresh Rate: 15



3. Date Installed: 07/10/04 12:30

4. Platform Type: TRP 703 Tower

Operating System Info: Windows 2000 Server 5.2

Current User: Administrator

Host Name: gnts703t

IP Addresses:
10.0.0.1 - CLAN
0.0.0.0 - ELAN

28. Dongle: 12345

Workaround: Use as documented Method-1 or Method-2 (with the required “shadow 0” command) when connecting to the CallPilot server.

* Nortel, the Nortel logo, the Globemark, and CallPilot are trademarks of Nortel.