



Installation Guide

for

InvisiConnect™ Enterprise Server

Welcome

Thank you for purchasing Metrotek, Inc.'s InvisiConnect™ Enterprise Server solution! This document will help you get started with installing the software and setting up the remote unit. If you have any questions regarding the InvisiConnect™ solution, please feel free to call Metrotek, Inc. Technical Support for assistance.

This document Copyright ©2006 by Metrotek, Inc. and may not be reproduced, in whole or in part without the expressed written consent of Metrotek, Inc. No merchantability is expressed or implied through the use of this document. All rights reserved. For errors, omissions or corrections, please contact Metrotek, Inc., Technical Support at support@metrotekfl.com.

Introduction

This installation guide covers the general setup and configuration of the InvisiConnect™ Enterprise Server (InvisiConnect™) solution by Metrotek, Inc. It will also cover general configurations for applications, but does not cover any specific application except where used as an example. Consult your application's User Guide for more specific information on configuring your application software and/or Metrotek's *Cellular Network Interface User's Guide*, a more comprehensive text for the InvisiConnect™ solution. For InvisiConnect™ specific questions, consult the online help.

This document assumes you have knowledge of installing software, are familiar with your version of the Windows® Operating System and have knowledge of its operation. If you do not think you can install this software on your own or make changes to your system or software, please contact your technical support department or other qualified person to assist you.

The InvisiConnect™ solution components used in this Setup Guide include the InvisiConnect™ software, MP32 programming software, the Cellular Network Interface (CNI) device and a programming cable. Please make sure you have all of these components available before you begin the installation. The software is supplied on CDs. For other media options, please contact Metrotek, Inc. Technical Support.

Remember that this document is only a guide for installing InvisiConnect™ and its components. Once InvisiConnect™ is installed you can use the built-in help to view more detailed program operations.



Table of Contents

Welcome	ii
Introduction.....	ii
Table of Contents	iii
Table of Figures	iv
Knowledge and Prerequisites	2
Knowledge Requirements.....	2
Software Prerequisites.....	2
Hardware Prerequisites	2
Other requirements.....	2
Installation Overview	3
Software Installation	5
Installing InvisiConnect™	5
Installing MP32	9
Configuring InvisiConnect™.....	14
First Run	14
Configuring Network Connections	16
Configuring COM Ports.....	19
Configuring SMS/USSD Options	21
Changing Trace and Alarm log sizes.....	23
Configuring Remote Devices	24
WAS Server Configuration Changes	Error! Bookmark not defined.
WAS Client Configuration Changes	Error! Bookmark not defined.
WAS Server Configuration Changes	26
WAS Client Configuration Changes	27
Programming a CNI with MP32.....	29
Testing Your Configuration	34
InvisiConnect™/CNI Connection	34
InvisiConnect™/Application Connection.....	35
CNI/Device Connection	36
Final Notes	37
Glossary/Terminology	38



Table of Figures

Figure 1 – InvisiConnect™ Installation – Welcome 6

Figure 2 – InvisiConnect™ Installation – Software License Agreement..... 6

Figure 3 – InvisiConnect™ Installation – Choose Destination..... 7

Figure 4 – InvisiConnect™ Installation – Select Program Folder 8

Figure 5 – InvisiConnect™ Installation – Setup Complete 8

Figure 6 – MP32 Installation - Welcome 9

Figure 7 – MP32 Installation – Software License Agreement..... 10

Figure 8 – MP32 Installation - Choose Desired Location 11

Figure 9 – MP32 Installation - Select Program Folder..... 11

Figure 10 – MP32 Installation - Start Copying Files 12

Figure 11 – MP32 Installation – Setup Complete 13

Figure 12 – InvisiConnect™ Configuration – Device Driver Installation 14

Figure 13 – InvisiConnect™ Configuration – WindowsXP Firewall Alert..... 15

Figure 14 – InvisiConnect™ Configuration - Initial Window..... 15

Figure 15 – InvisiConnect™ Configuration – Configuring Connections 16

Figure 16 – InvisiConnect™ Configuration – Add Interface..... 18

Figure 17 – InvisiConnect™ Configuration – COMs for Applications 19

Figure 18 – InvisiConnect™ Configuration – COMs for Applications 20

Figure 19 – InvisiConnect™ Configuration – SMS 22

Figure 20 – InvisiConnect™ Configuration – Logs 23

Figure 21 – InvisiConnect™ Configuration – Remote Device 25

Figure 22 – Configuring WAS – Enable WAS..... 27

Figure 23 – Configuring WAS – Client Configuration 28

Figure 24 – WAS Configuration – Sample Data 29

Figure 25 – CNI Configuration – Initial Window 30

Figure 26 – CNI Configuration – Programming..... 31

Figure 27 – CNI Configuration – Serial Ports..... 32

Figure 28 – CNI Configuration – Cellular Settings..... 32

Figure 29 – CNI Configuration – Confirm Programming..... 33

Figure 30 – InvisiConnect™/CNI Testing –Updates from CNI..... 35

This page intentionally left blank.

Knowledge and Prerequisites

Knowledge Requirements

This document requires basic operating system, hardware and network knowledge in order to properly configure the software and hardware referenced in this document. Specifically, you will need to install software, know some TCP/IP protocol settings and have a basic understanding of data communications such as COM ports. Metrotek, Inc. Technical Support may be able to help in these cases, however configuring your network, application or device is beyond the scope of this document.

Software Prerequisites

InvisiConnect™ should be installed on a computer running Windows98® or later which includes Windows2000® or Windows2003® Server. Regardless of platform, the term “server” is used to identify the computer where InvisiConnect™ is installed and running.

MP32 is the software used to initially program the Cellular Network Interface (CNI) and has the same hardware and software requirements as the InvisiConnect™ software.

It is not necessary to install InvisiConnect™ and MP32 on the same computer since they perform functions that are exclusive to each other, however it is convenient to do so, especially when you are becoming familiar with the hardware and software.

Hardware Prerequisites

InvisiConnect™ will run on the minimum hardware required by the operating system you are using, however, as with any software package, performance is increased dramatically by newer and expanded hardware. You should carefully consider where the software will reside. Also consider that Windows® Server platforms are typically more stable than workstation platforms.

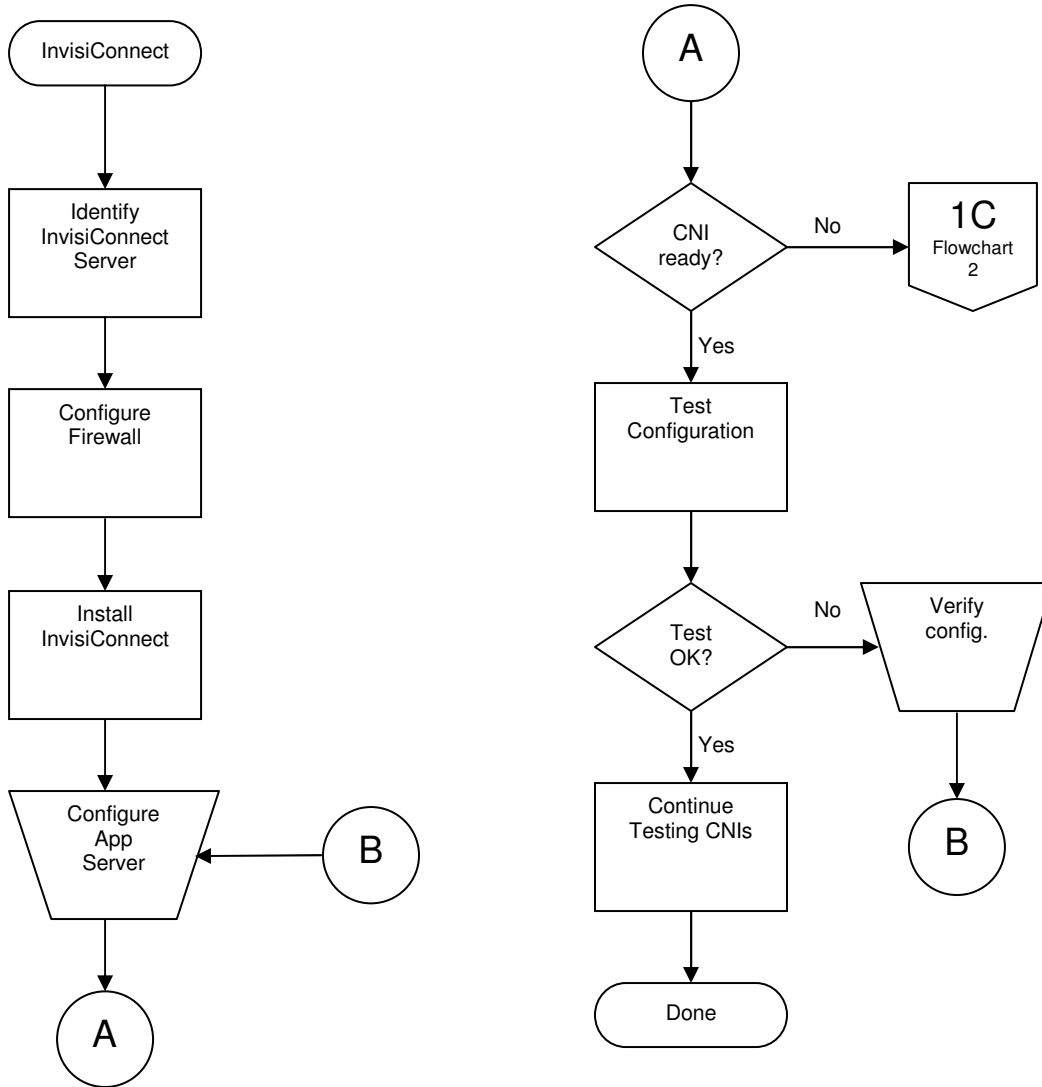
Other requirements

InvisiConnect™ will need a public IP address and port, which can be obtained from your network administrator or your Internet service provider, and a private (internal) static IP address. You may also have to configure your network to allow this IP address and any assigned port through your firewall and route the data to the InvisiConnect™ server on your network.

InvisiConnect™ will need at least one method for sending SMS (Short Message Services) messages. (Refer to the *Cellular Network Interface User's Guide* for more information on the communications process.)

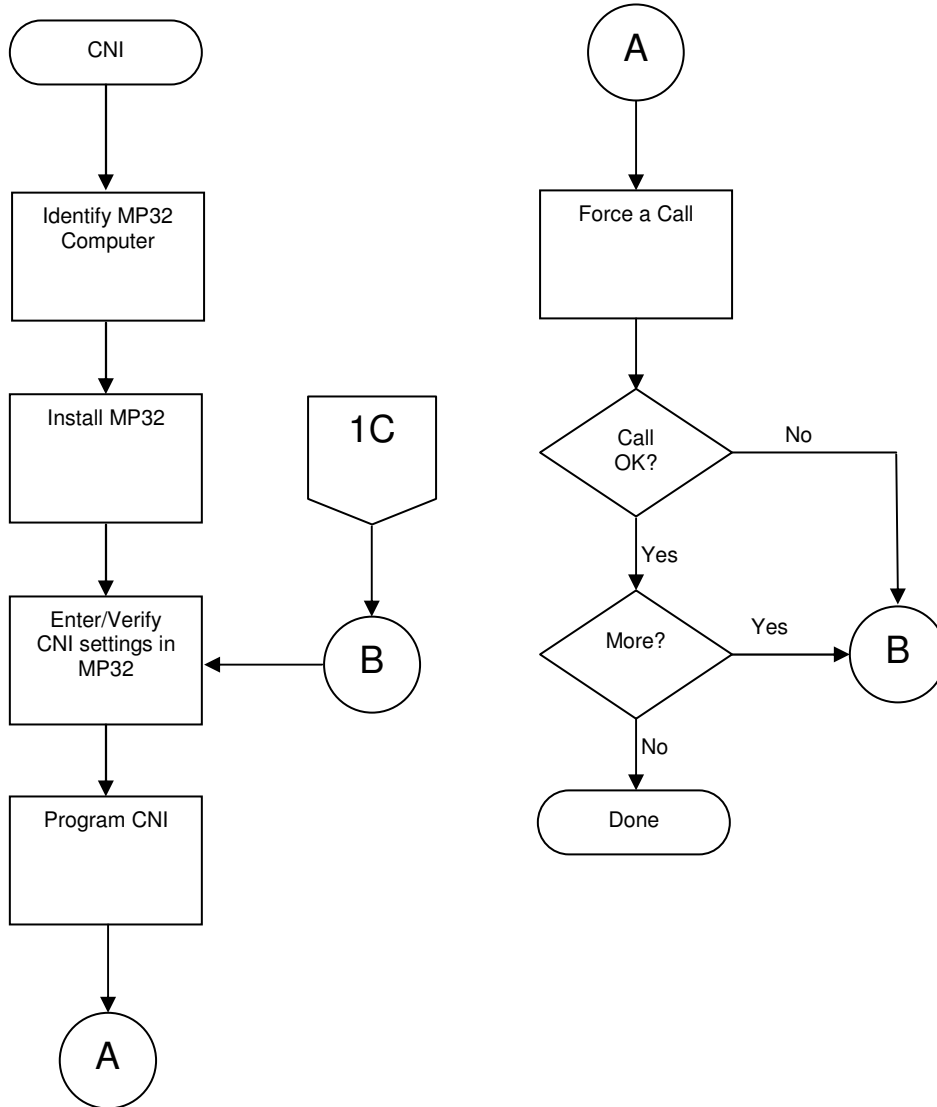
Installation Overview

Flowchart 1 is a flowchart of the processes that are performed when you are installing and configuring InvisiConnect™ on your computer. These steps are covered in more detail later in this guide.



Flowchart 1

Flowchart 2 is a flowchart of the processes that are performed when you are installing MP32 on your computer and programming a CNI. These steps are covered in more detail later in this guide.



Flowchart 2

Software Installation

Once you have identified the computer where you will install the software and you have all the items mentioned earlier, you can begin the installation.

The installation process requires local administrative rights to install the software on the chosen computer. If your account does not have elevated privileges to install software and device drivers do not continue until you can log in with these privileges.

Your license file (filenames *license.bin* and *license.txt*) allows InvisiConnect™ to run and therefore you should always have a backup copy of these files in a secure location in case you need to re-install InvisiConnect™ in the future.

Installing InvisiConnect™

Most installations do not require any changes to the default values provided during the installation. You can change the location of the program or the location of the shortcuts during the installation process. Check to see if your network policies allow the default installation options to be changed first.

Follow these steps and refer to the figures when installing InvisiConnect™ on your system. The installation of InvisiConnect™ WAS Server and InvisiConnect™ WAS Client are identical. The significance between the two functions is a combined result of the configuration and the license files.

To install InvisiConnect™ from a CD:

1. Insert the installation disc into your computer's CD-ROM drive. If AutoPlay is enabled, the setup program will automatically execute. If it does not, navigate to your computer's CD-ROM drive and run *setup.exe* from the root of the disc to begin the setup program.
2. Figure 1. Welcome screen – Click <Next> to continue.

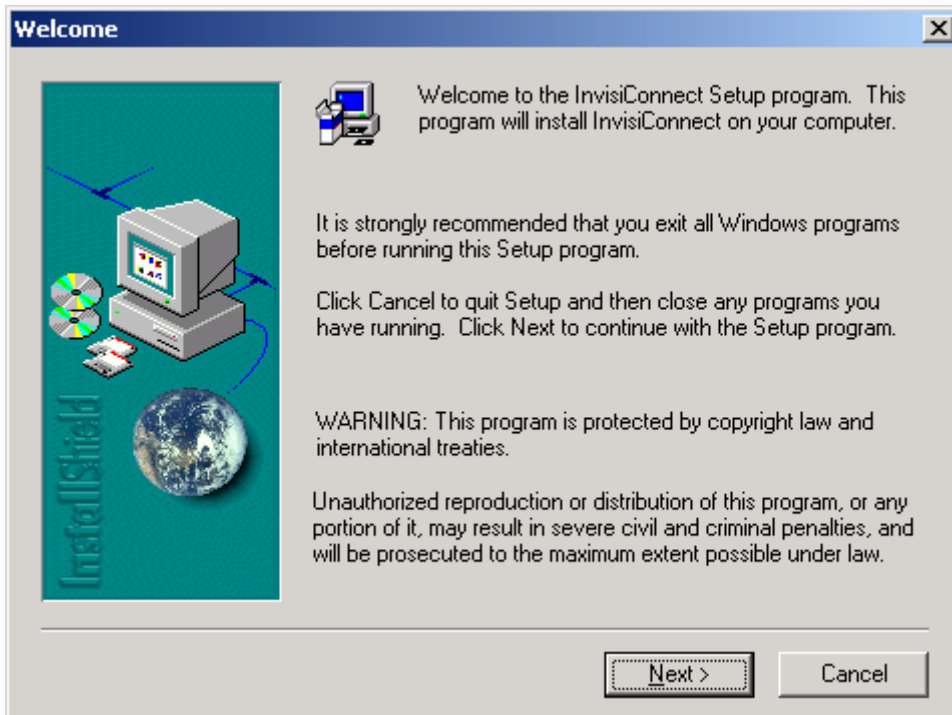


Figure 1 – InvisiConnect™ Installation – Welcome

3. Figure 2. Software License Agreement – Read before continuing then click <Yes> to agree and continue the installation. Clicking <No> will terminate the installation process.

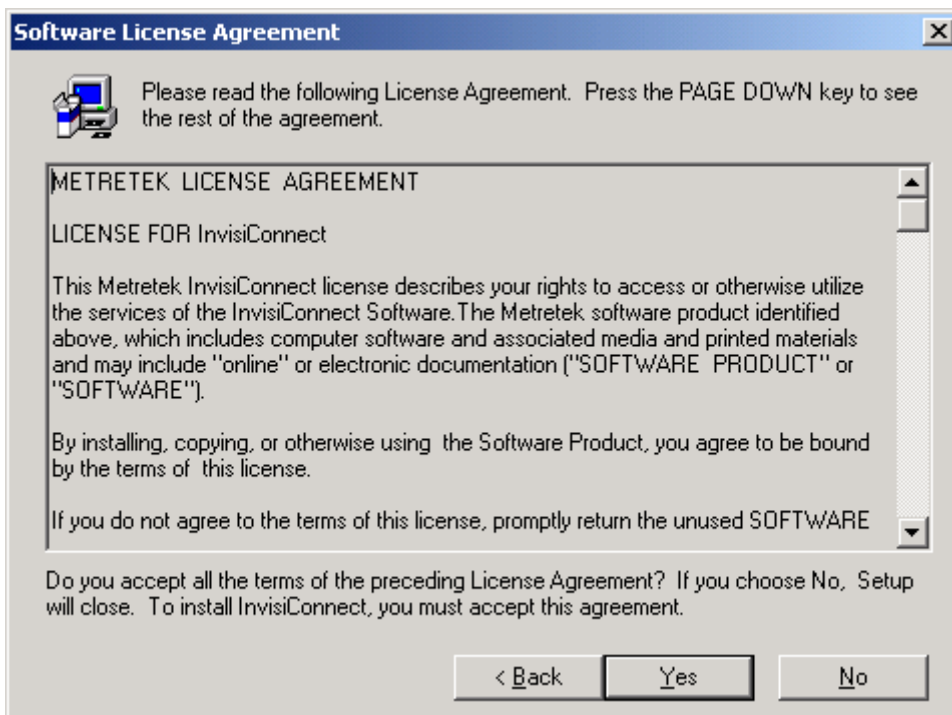


Figure 2 – InvisiConnect™ Installation – Software License Agreement

4. Figure 3. Choose Destination Location - You can choose a destination other than the default location by clicking the <Browse> button and selecting an alternate location for the program. Click <Next> to continue.

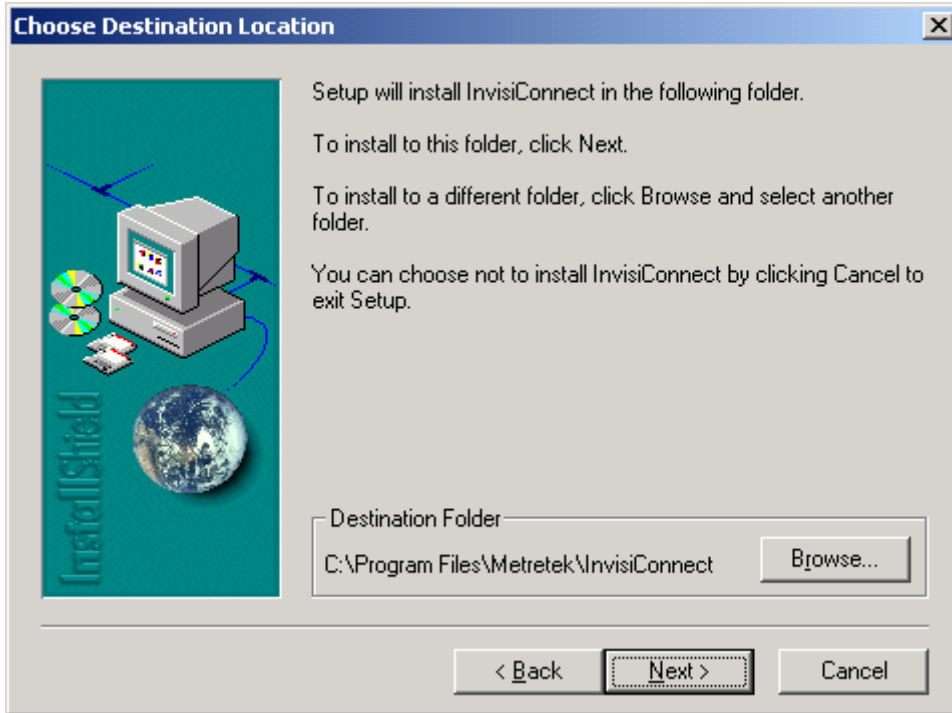


Figure 3 – InvisiConnect™ Installation – Choose Destination

5. Figure 4. Select Program Folder – this is the folder you will select from the Start Menu. If you wish to change the location of the InvisiConnect™ icons on the start menu, make the appropriate changes here. Click <Next> to continue.

Note: You can move the icons to a different location on the start menu after installation, however if you uninstall InvisiConnect™ new location of the icons will not be recognized and they will not be removed automatically.

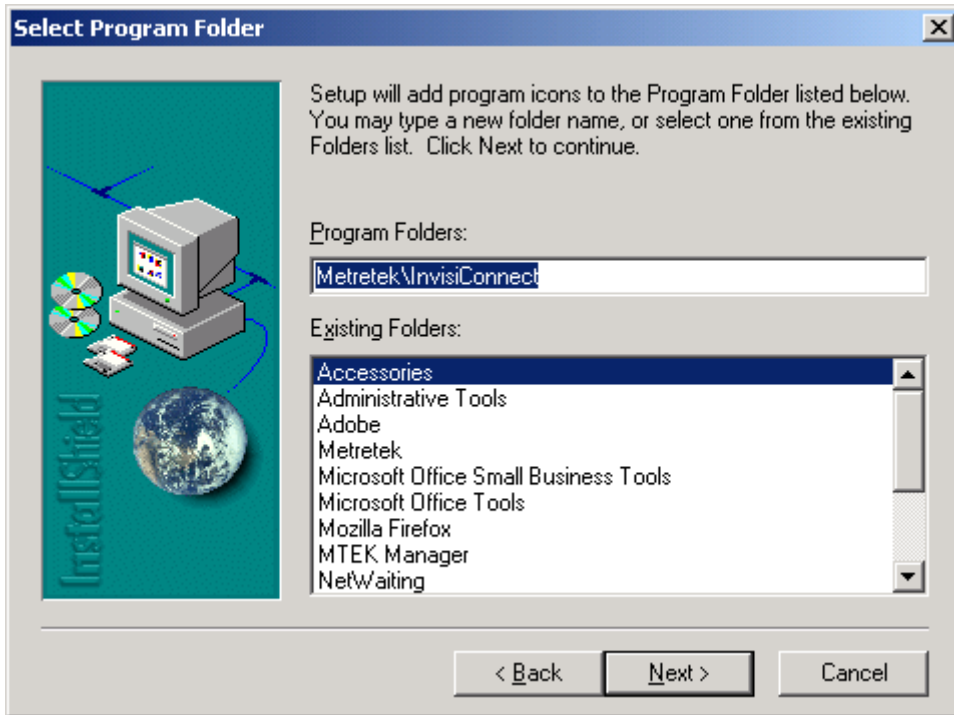


Figure 4 – InvisiConnect™ Installation – Select Program Folder

6. The program will now install using the answers you provided or accepted.
7. Figure 5. Setup Complete – On the final installation screen, click <Finish> to complete the installation process.

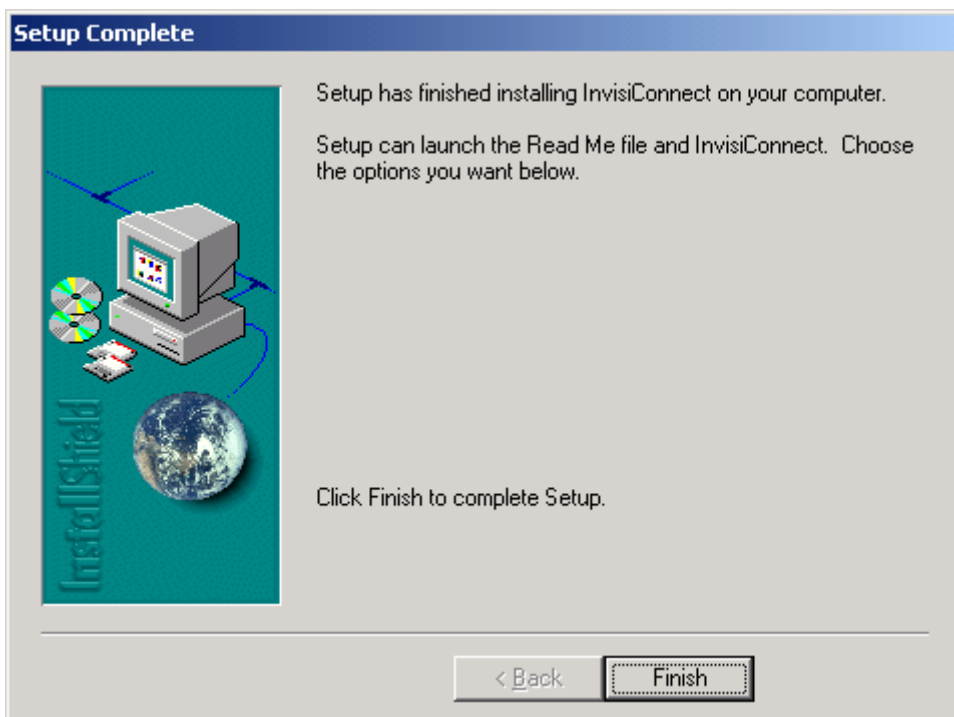


Figure 5 – InvisiConnect™ Installation – Setup Complete

8. The last step is to copy the *license.bin* and *license.txt* files you were given to the InvisiConnect™ installation folder. This will override the default license files which limit the functionality of InvisiConnect™. If you are implementing WAS, make sure you copy the correct files to the computer, i.e. you will have a *license.bin* and *license.txt* file for each installation type, server or client.

Installing MP32

The programming software for the CNI device is called MP32 (Metretek Device Programmer) and is distributed on a CD or Floppy Disks and is available for download. You will only need to install MP32 to configure or reconfigure devices. If you provided the necessary information to Metretek (and purchased programming) then your CNIs will be shipped pre-programmed and most likely have already contacted your server as part of the testing/programming process. The setup for MP32 is similar to the setup for InvisiConnect™.

To install MP32 please do the following:

1. If AutoPlay is enabled on your computer, inserting the CD will start the installation process or if not, run *setup.exe* from the root of the CD. If you have MP32 on Floppy Disks, insert the first disk and run *setup.exe* from it to begin. Alternatively, run *setup.exe* from a folder where you copied the setup files.
2. Figure 6. Welcome - Click <Next> to continue.

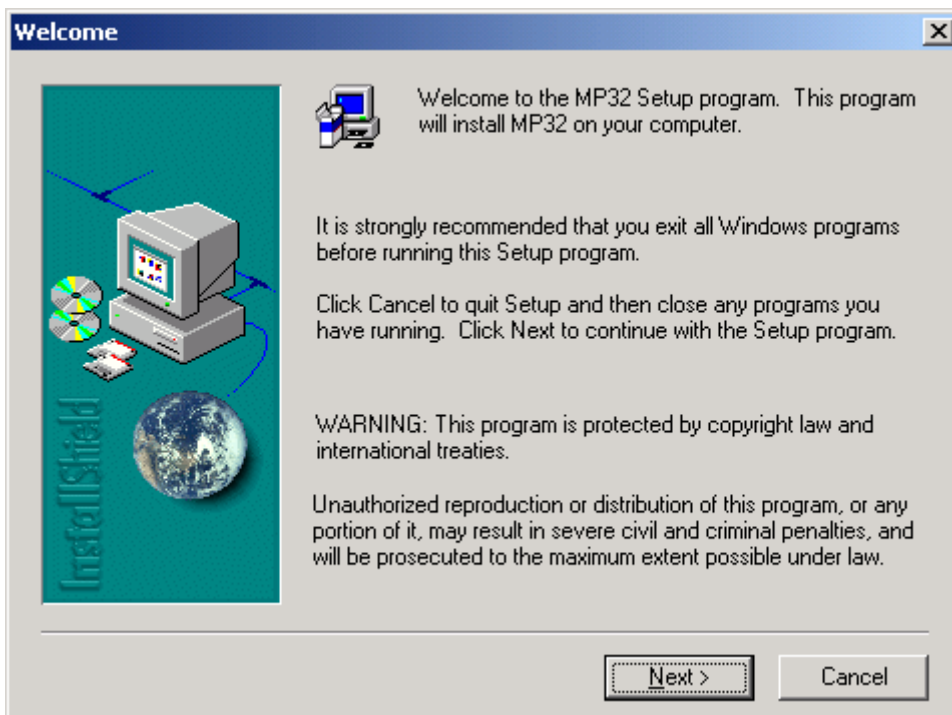


Figure 6 – MP32 Installation – Welcome

3. Figure 7. Software License Agreement – Read before continuing then click<Yes> to continue the installation.

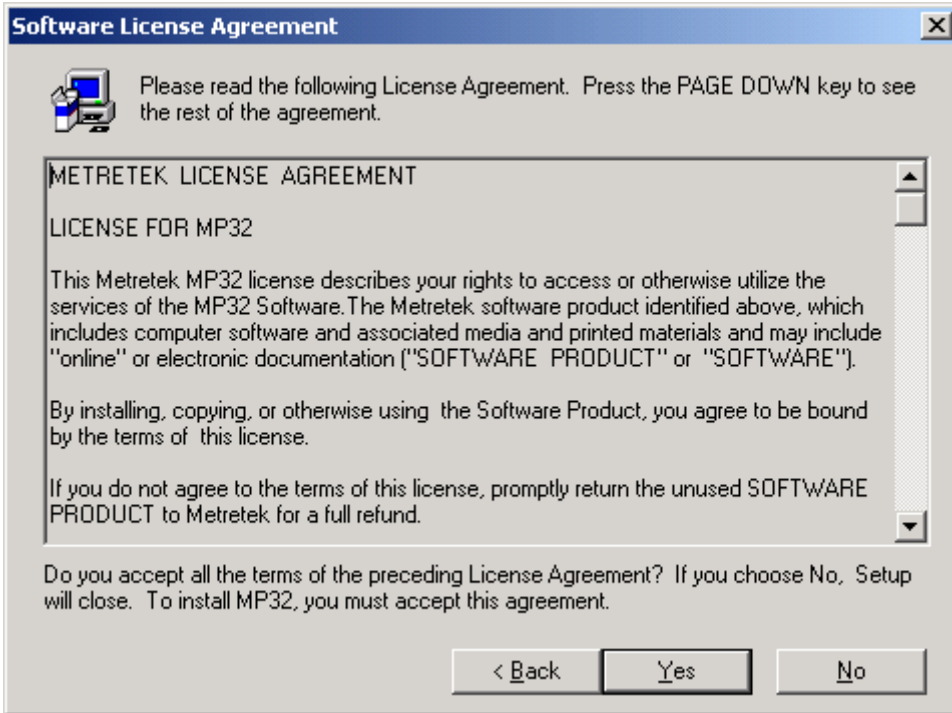


Figure 7 – MP32 Installation – Software License Agreement

4. Figure 8. Choose Destination Location - You can choose a destination other than the default location by clicking the <Browse> button and selecting an alternate location for the program. Click <Next> to continue.

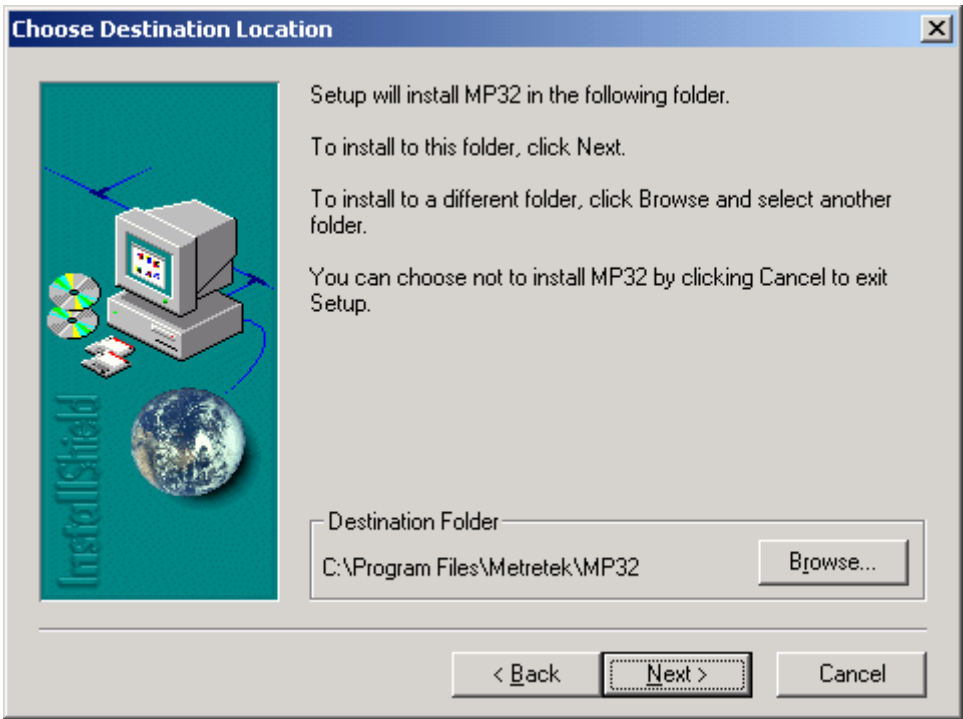


Figure 8 – MP32 Installation - Choose Desired Location

5. Figure 9. Select Program Folder – this is the folder you will select from the Start Menu. If you wish to change the location of the InvisiConnect™ icons on the start menu, make the appropriate changes here. Click <Next> to continue.

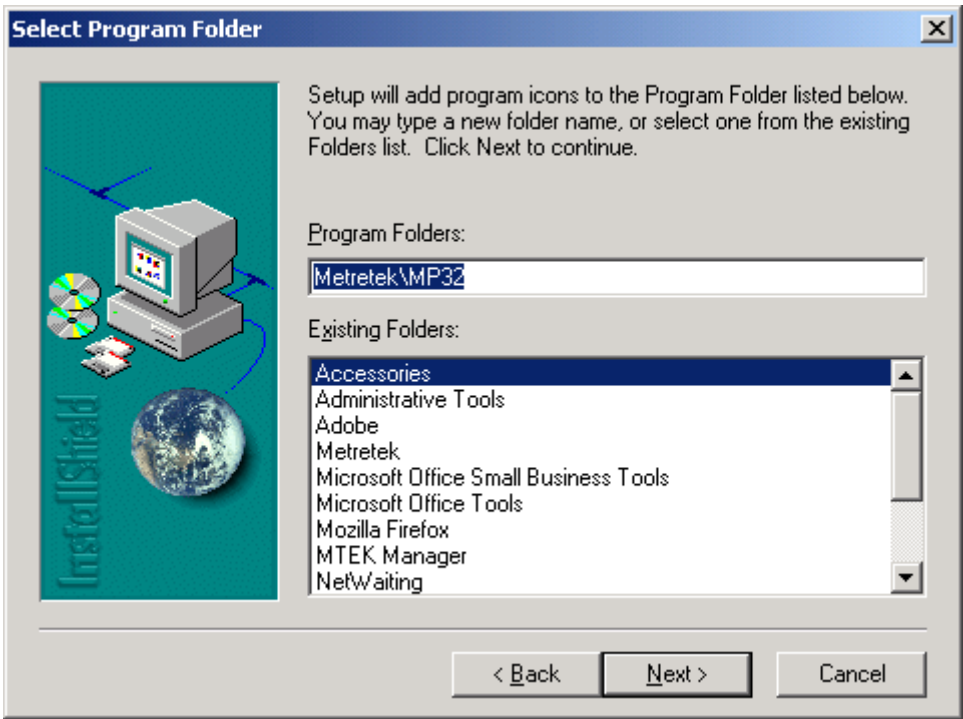


Figure 9 – MP32 Installation - Select Program Folder

6. Figure 10. Start Copying Files – The setup program is now ready to copy files to your computer. Click the <Next> button to begin copying files. The program will install using the answers provided.

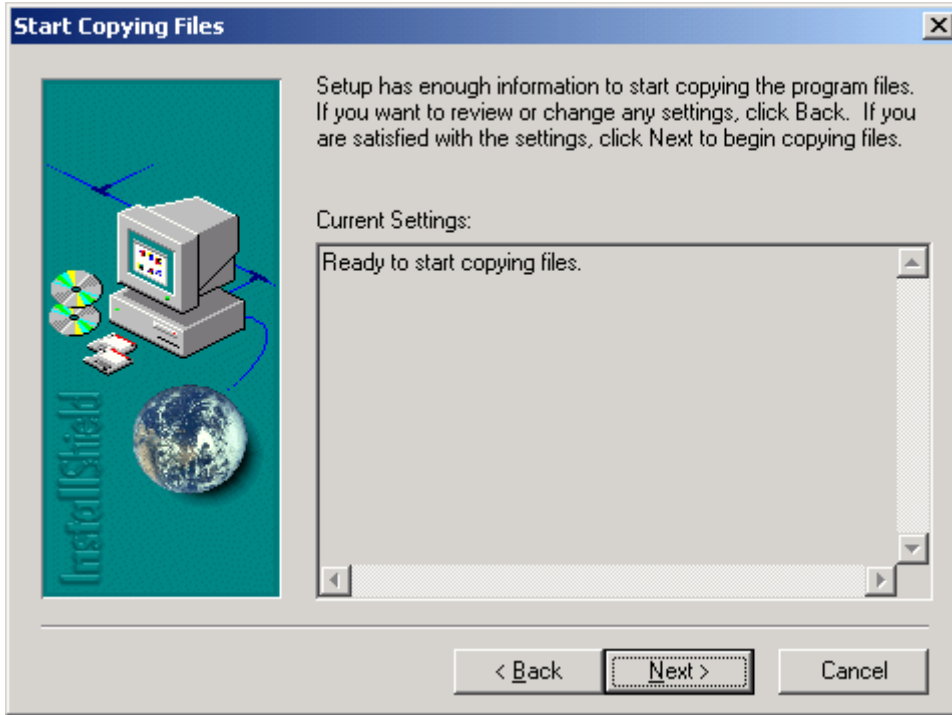


Figure 10 – MP32 Installation - Start Copying Files

7. Figure 11. Setup Complete – On the final installation screen, click <Finish> to complete the installation process. You are now ready to configure your system.

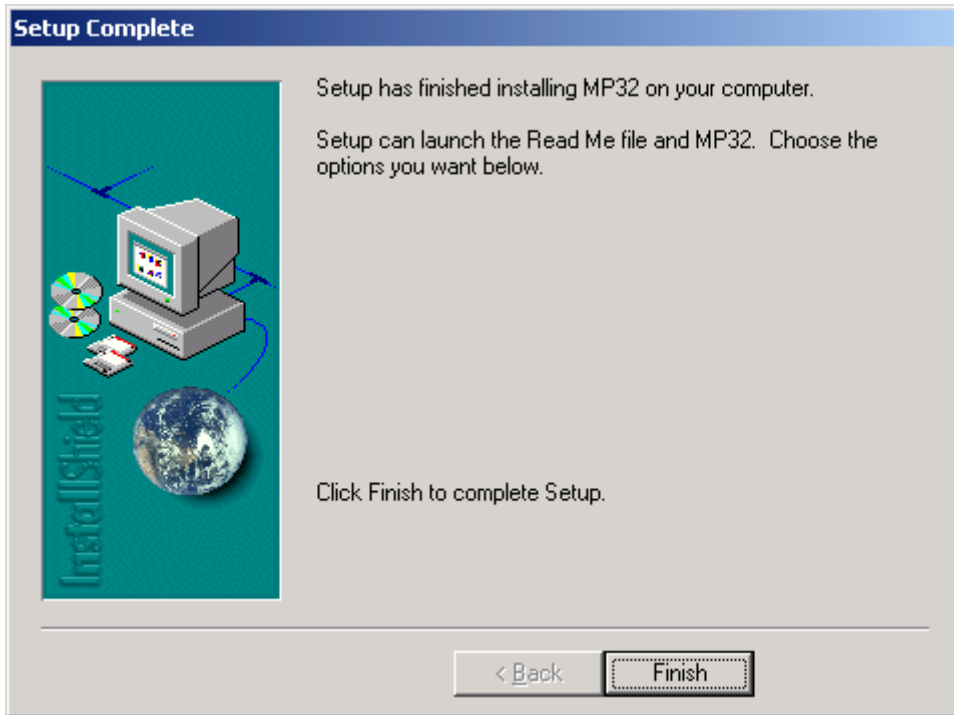


Figure 11 – MP32 Installation – Setup Complete

Configuring InvisiConnect™

This portion of the guide will help you install InvisiConnect™ as a WAS Server or as a stand alone product, therefore you should complete this section prior to configuring a WAS Client. After you have installed InvisiConnect™ you can view or print the complete manual by selecting *InvisiConnect Help Manual* from the program folder.

First Run

When InvisiConnect™ is launched for the first time on a computer, you will receive a warning (Figure 12) that device drivers need to be installed. Click <OK> to continue if you have logged on the computer with an account that has rights to install software and device drivers, otherwise, log off and use another account that has these elevated privileges and launch InvisiConnect™ again to complete the installation process.



Figure 12 – InvisiConnect™ Configuration – Device Driver Installation

1. If you are running InvisiConnect™ on a computer with a firewall, such as WindowsXP SP2 or Windows2003 Server, you may receive a warning. You must allow the application to run, or you will not be able to use InvisiConnect™. Refer to your firewall's documentation for more information on how to allow application exceptions.



Figure 13 – InvisiConnect™ Configuration – WindowsXP Firewall Alert

2. If your network policies impose firewall rules as a Group Policy, contact your network administrator to make the necessary changes.
3. InvisiConnect™ will automatically start after the device drivers are installed and will look similar to Figure 14.

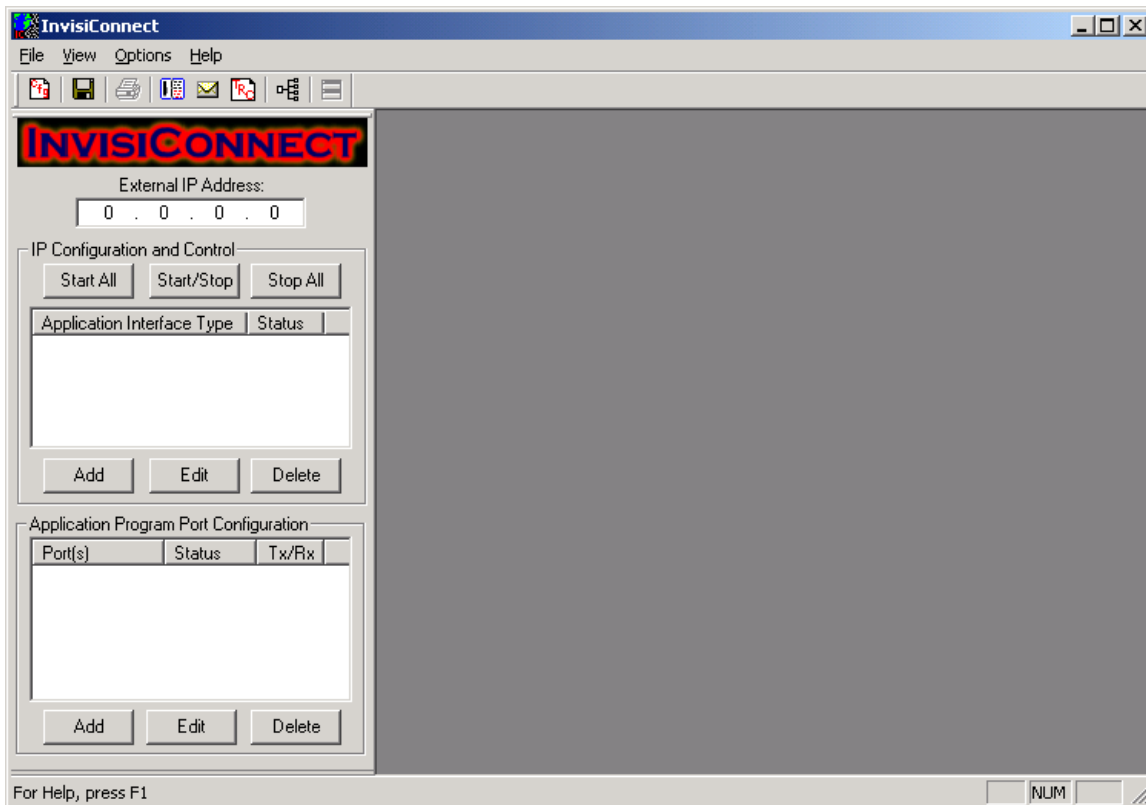


Figure 14 – InvisiConnect™ Configuration - Initial Window

Configuring Network Connections

Refer to Figure 15 for the location of the following configuration changes.

1. Enter your external (public) IP address here. This address is the one that is available to public and the CNI. Hint: It will not start with 10.x.x.x, 172.16.x.x to 172.31.x.x or 192.168.x.x as these are part of the private addresses set aside for internal networks. Failing to enter the appropriate value here will cause an authentication failure when the CNI contacts the server.
2. Click on the <Add> button in the *IP Configuration and Control* section of InvisiConnect™.

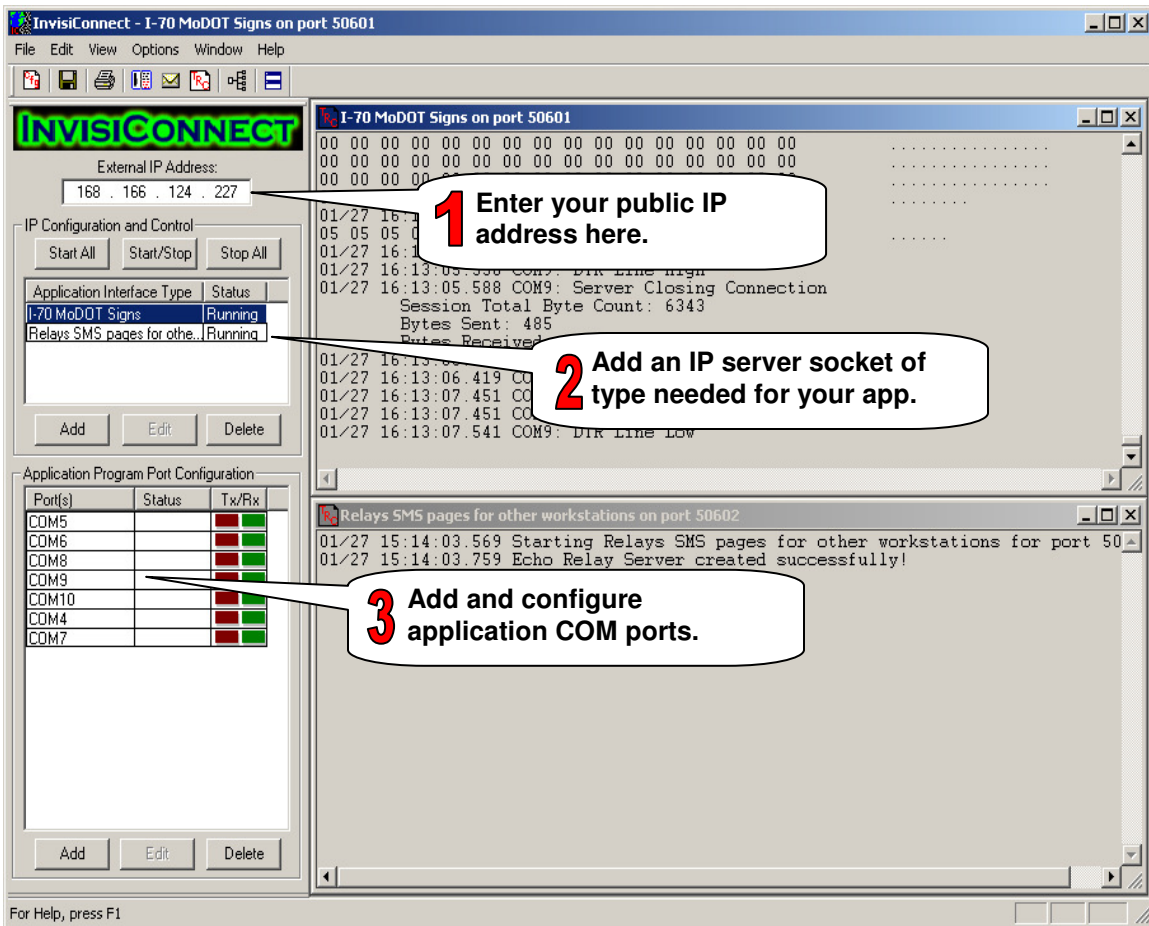


Figure 15 – InvisiConnect™ Configuration – Configuring Connections

- a. Select the type of connection. The most common option is to use **Standard AT Modem** because it allows more configuration options with the COM port. Figure 16 – InvisiConnect™ Configuration – Add Interface shows the defaults when this is selected.

The types of connections available are:

- **Direct Serial Application Interface**
Some applications may be expecting to communicate directly with the remote device without the use of a modem. In essence the application program still believes that the remote device is directly connected to the computer.
- **DNS / Application Server Application Interface**
In this mode InvisiConnect™ and the CNI allow the host application to run as a server and all of the remote devices as clients, no matter which direction the requests are coming from. Each remote device acting as a server must have its own unique IP address. However, the application may only know the remote device in the form of a domain name, such as "RemoteDevice135.net".
- **Discreet IP / Application Server Application Interface**
This interface is very similar to the DNS / Application Server but is designed for applications that only use IP addresses, such as "42.145.90.45", to contact the remote devices. Therefore there is no need to translate a domain name into an IP address.
- **Echo / Relay / API Server Application Interface**
In this approach InvisiConnect™ can forward an SMS message on behalf of another computer that is also running InvisiConnect™ through its own SMTP server or cellular modem. The Echo / Relay / API Server use the UDP protocol. If there is a firewall between InvisiConnect™ and the Internet it will need to be configured to allow UDP to pass through.
- **MODSMOD Modem**
Your application program may be expecting to communicate with the remote device using the Metretek Protocol. In this case select "MODSMOD Modem". In this mode, InvisiConnect™ will intercept commands issued by the server application and send them to the device.

- b. Select a different IP port number if desired. In any case, your network must route traffic (data) on this port to the computer running InvisiConnect™.
- c. Enter a description for the interface. Identifying an interface by entering a description will make it easier when setting up InvisiConnect™. The description you enter will be displayed in the appropriate trace window when it is started.

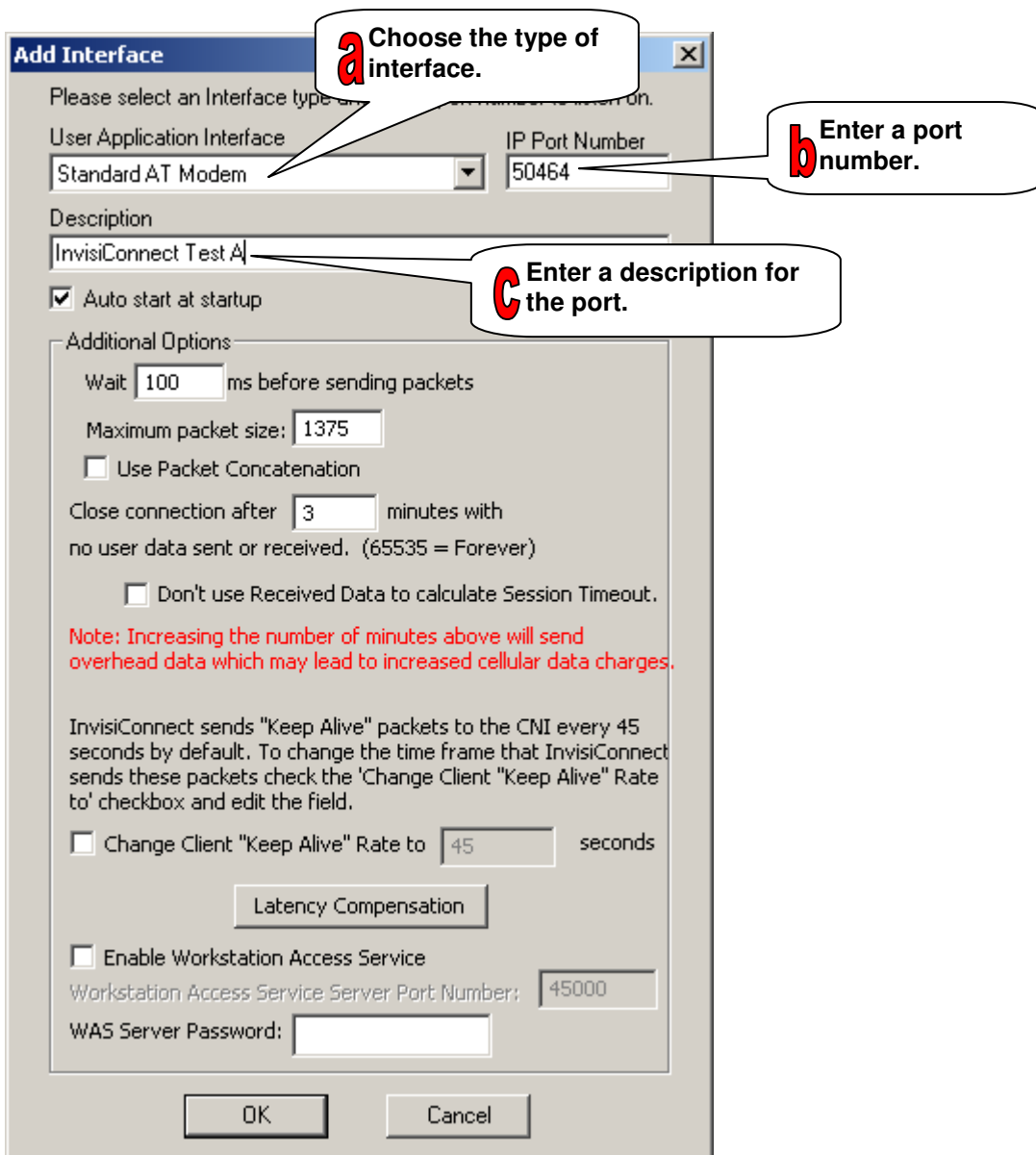


Figure 16 – InvisiConnect™ Configuration – Add Interface

- 3. Click on the <Add> button in this section to add a COM port. You can also add a range of COM ports using the same settings. This topic is covered in the next section.

4. During the initial setup and testing of InvisiConnect™ it is recommended that you not start the Workstation Access Service (WAS) which is discussed later in this guide.
5. Continue with the next section Configuring COM Ports.

In most cases, the defaults for the remaining settings will work. If you are experiencing trouble with the communications, contact Metretek, Inc.'s Technical Support or your network administrator for assistance.

Configuring COM Ports

This section can be repeated for as many COM ports needed to communicate with your program. Typically one or possibly two COM ports are needed to communicate. You may wish to duplicate the number of physical modems (by adding virtual COM ports) your program had available in InvisiConnect™ to make the new environment closely resemble your previous setup. The number of COM ports (and RUIDs) you can create in this section is limited by your license files, so it is important that you use your license files instead of the default files which will limit InvisiConnect's™ functionality.

1. Click on <Add> in the Application Program Port Configuration section to add a COM (communications) port to InvisiConnect™. Refer to Figure 17 to complete the following steps.
2. Unless you are specifically using a physical modem to communicate between InvisiConnect™ and your program, you need to make sure **Use Hardware Com Port(s)** is unchecked.
3. Select a COM port to use. Do not use a port already in use by hardware! This port must match the COM port in your application. Make sure that your application supports the port number. Some applications will not support ports past COM4.

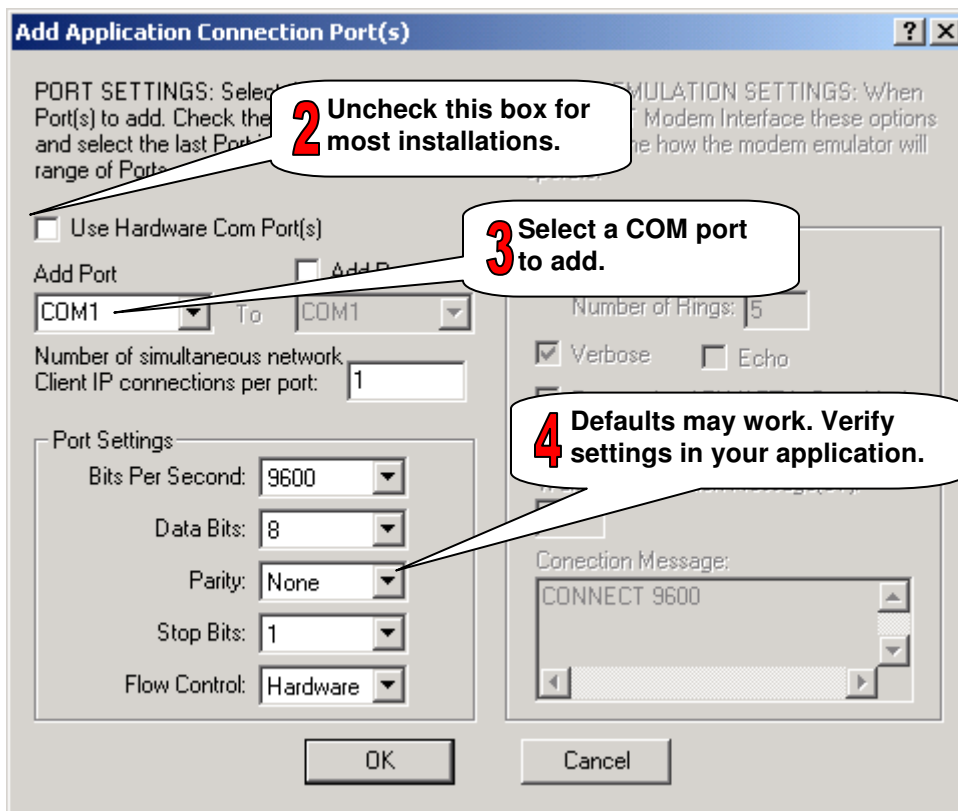


Figure 17 – InvisiConnect™ Configuration – COMs for Applications

4. In the *Port Settings* section, make any adjustments necessary so they match the application settings. Note that these settings are only necessary between the application and InvisiConnect™. Remember, these ports are not used to connect to the device or the CNI.
5. Now you can configure the specific modem settings for this port. Refer to Figure 18. Note that these options are only available if you chose *Standard AT Modem* for the type of connection. These settings should reflect what your application expects regarding communications. If you have any questions about the AT command set, refer to your application or modem user guide for explanations.
 - a. Auto Answer is on by default and in most cases should remain on. Set the number of “rings” before InvisiConnect™ will “pick up” the line.
 - b. Some applications do not properly interpret Verbose modem results. Uncheck this box to only send decimal values or check it to send text values.
 - c. Some applications do not expect to see the baud rate with the connection message. You can edit this field to remove or change the message.
Note: changing to or from Verbose mode affects the output.
 - d. Checking Echo will reflect any output back to the application. In most cases, enabling this settings will result in duplicated data being returned because the device will normally send any responses the application is expecting. Refer to your application’s user guide to determine if this setting is necessary.

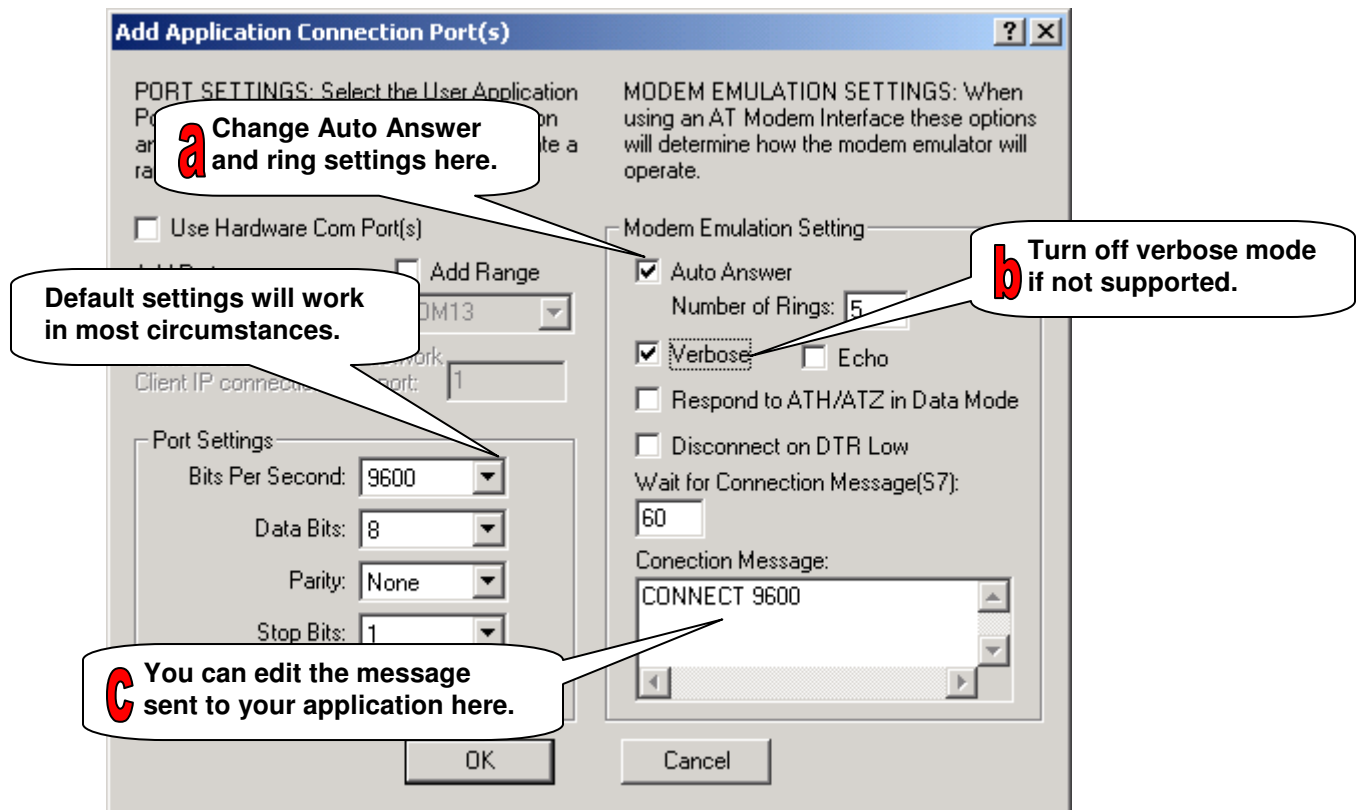


Figure 18 – InvisiConnect™ Configuration – COMs for Applications

- e. The remaining settings are for advanced configurations as the default settings will work in most cases.

6. Once you have completed the changes, click the <OK> button to save the configuration for this port. Repeat these steps to add (or you can edit) more ports.

Configuring SMS/USSD Options

You will need to configure SMS (Short Message Services) to initiate any communications with the CNI. (Configuring the CNI to accept SMS messages is covered later in this document.) Refer to Figure 19 for configuring SMS.

1. Select SMS/USSD Configuration from the Options menu in InvisiConnect™ to display a settings page similar to Figure 19.
2. Initially, the checkbox for Enable SMS/USSD is unchecked. Check it to continue configuring the service.
3. There are three options available in the SMS/USSD Send Method section for sending SMS messages to the CNI.

They are described as follows:

- a. Use *SMTP Mail Server* option. This uses a mail server (SMTP) to send the message. If you are using only one carrier, enter the carrier's SMS domain information in the SMS/USSD suffix field, eliminating the need to append the same information in the device configuration.

This option requires the mail server to be configured to accept SMS messages and forward them appropriately. You would populate the fields with the mail settings provided by your mail administrator.
- b. Select *Use Attached Cellular Modem* if you have a cellular modem attached directly to the workstation running InvisiConnect™. The settings you would enter here would come from the modem's setup guide. This method will not require you to enter a carrier's domain suffix information to send messages since there is no message conversion process.
- c. Select *Use Relay Server* to send the messages to a server that will then forward the message to its destination. You would normally enter an internal IP address and port number of the relay server, however you can also use an external IP address and port if the server is not on your network. If the relay server requires a password, you would also enter it in the appropriate field. This method does not require you to enter a carrier's domain suffix information to send messages since there is no message conversion process.

NOTE: Implementing a relay server requires a CNI with special firmware. Contact Metrotek if you need assistance implementing this option.

Metrotek's recommended order of preference is to implement (b) *Use Attached Cellular Modem*, then (c) *Use Relay Server* and finally (a) *Use SMTP Mail Server*.

- d. Enter the IP address and port number of the relay server and a password if required.
 - e. Enter the public IP address for the InvisiConnect™ server here if you are implementing more than one server. This allows each server to globally override the callback IP address for any message sent from it. Entering a server's IP address here will temporarily override the CNI's programmed values allowing it to connect to a different server. Once the call is complete, the CNI will use its default settings unless instructed by another SMS.
4. Click <OK> to accept the settings and return to the main window.

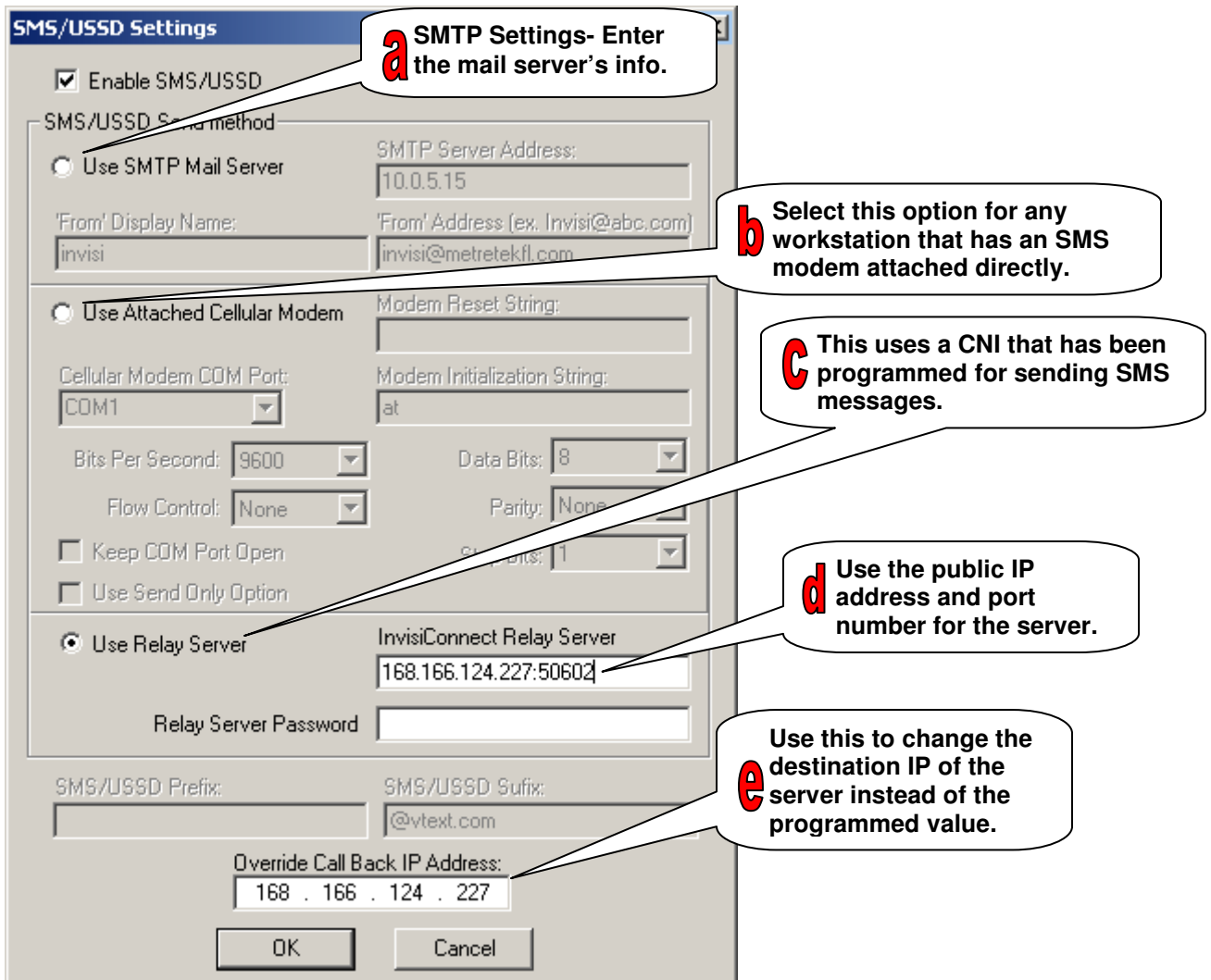


Figure 19 – InvisiConnect™ Configuration – SMS

- 5. On the main InvisiConnect™ window, click the <Start/Stop> button to start the services. If you receive any errors in the right pane of the window, repeat the above steps to help with troubleshooting the error.

Changing Trace and Alarm log sizes.

It is advisable that you increase the size of the trace files. Click <Options> on the main menu and then select <Trace & Alarm File Configuration> to make these suggested changes: Refer to Figure 20 when configuring the suggested changes.

- Set the Maximum Alarm File Size to at least 2048k
- Set the Maximum Trace File Size to at least 2048k
- Change the Output Window Buffer Size to at least 512k
- Leave the checkboxes in their original state.
- When you have completed these changes, click <OK> to return to the program.

You may wish to increase the log files to an even larger number depending on how much data you wish to capture in them. Refer to the Help in InvisiConnect™ for more information about log files and names.

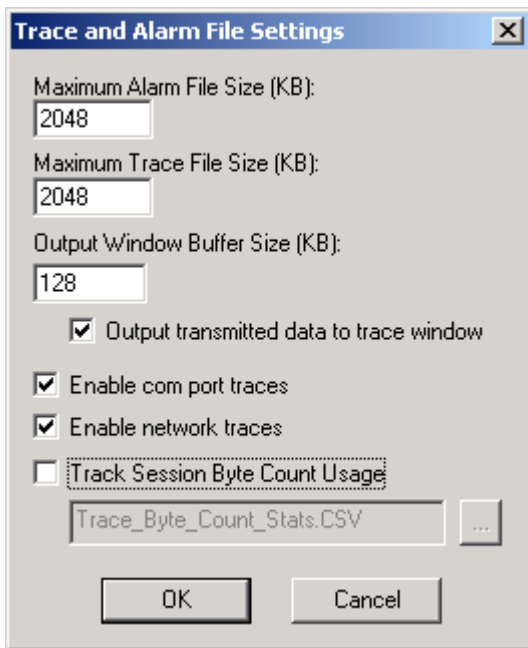


Figure 20 – InvisiConnect™ Configuration – Logs

Configuring Remote Devices

This section is where you configure InvisiConnect™ so the program knows which device(s) it will communicate with. The devices are primarily the CNI units deployed remotely, although during setup and MP32 programming, they should be local.

1. Select *Change Remote Configuration* from the *Options* menu item to open a settings dialog box similar to Figure 21. (Note that this figure has already been populated with devices.)
2. Click the <Add Remote> button to add a remote device to the list. The device name can be up to six (6) hexadecimal characters so you should consider a logical naming scheme to allow you to identify the device by its name.

NOTE: InvisiConnect™ will automatically add the CNI to the RUID database if it does not exist when the CNI calls the server. However, InvisiConnect™ will not populate all of the fields automatically so some intervention may be required.

3. Enter the phone number of the CNI here. Depending on the carrier, you may also need to enter the APN and login information. If you chose to use SMTP for your SMS solution and you are using multiple carriers, you should append the carrier’s SMS domain information to this field.
4. Set the IP and Port for the device to call back. Entering an IP address here will override any other callback IP addresses either programmed into the CNI or entered in the SMS/USDD settings window. While this is a temporary override, the CNI will always receive this information in an SMS until it is cleared, effectively making it a semi-permanent solution. This will not affect the CNI settings on another InvisiConnect™ server.
5. You can return to these steps to add or configure more devices at any time. It is suggested that you configure one or two devices for testing to make sure your configuration is correct.

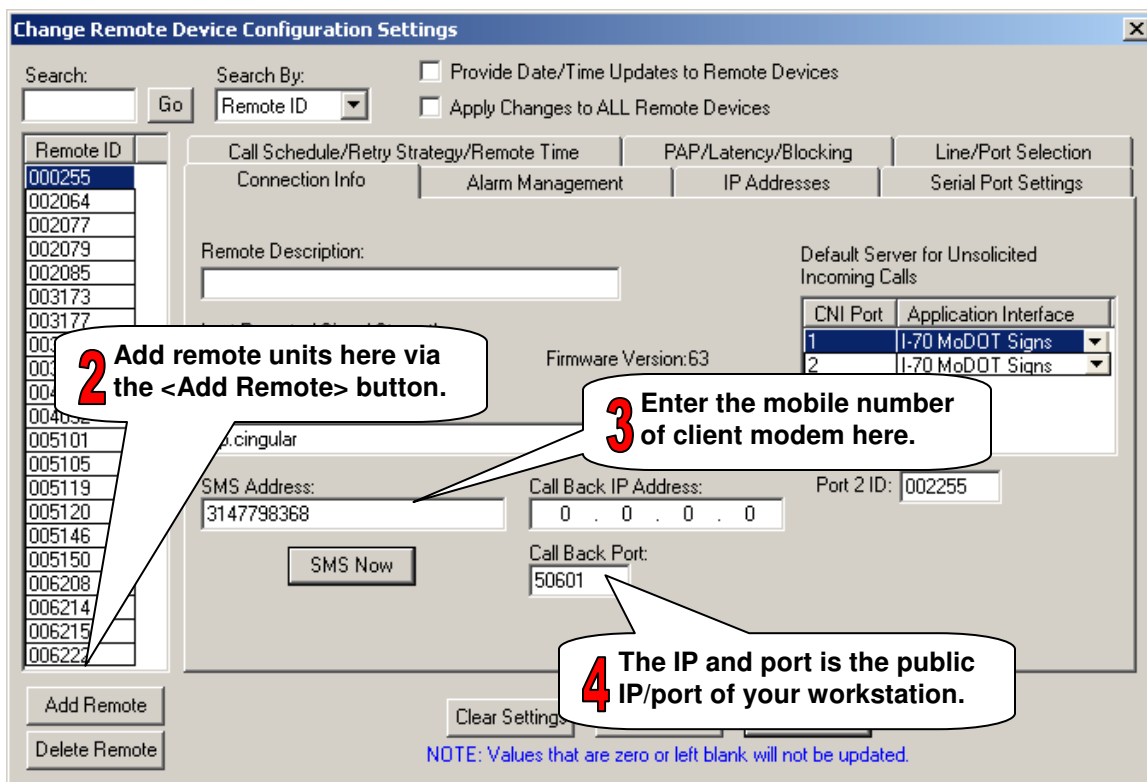


Figure 21 – InvisiConnect™ Configuration – Remote Device

Configuring Workstation Access Services (WAS) Client

InvisiConnect™ needs access to the global Internet. If the computer is located behind a corporate firewall then the remote devices must be allowed through to the InvisiConnect™ Server's IP address. If many computers need to have access to the remote devices then this would require numerous "holes" through the firewall. To minimize this risk the Workstation Access Service feature allows all computers within a local network to interface to one and only one computer that is visible to the outside world. This feature only applies to the Direct Serial Server MODSMOD Modem and the AT Modem Server.

If you are not using InvisiConnect™ as a WAS Server, you can safely skip this section.

This service can be configured any time after the InvisiConnect™ solution is in place. To reduce troubleshooting, your application and device should already be configured to use InvisiConnect™ and should be able to communicate with each other prior to implementing WAS.

Some portions of this section were previously published as *Application Note #0606: Workstation Access Service*.

InvisiConnect™ Enterprise Server (IES) software, release 4.6.23 and later, now functions as an application data routing server for other InvisiConnect™ powered workstations as well as InvisiConnect™ CNI cellular client modems. This means any number of workstations running your application program can connect to your field CNIs via InvisiConnect™ Enterprise Server, thus making system expansion and remote control easy to set up without firewall or network configuration changes. This new service is called Workstation Access Service or WAS.

The Workstation Access Service (WAS) allows other computers (in addition to the server) to connect to devices using one primary installation of InvisiConnect™ which is configured as the WAS Server. These additional computers will not have to be configured with each device since they will use the server's configuration and resources to communicate to each device and CNI, eliminating additional configuration errors and troubleshooting as well as possible data loss.

WAS Server Configuration Changes

1. On the computer running as the InvisiConnect™ WAS Server, edit the interface used to communicate with your CNI. Refer to Figure 22.
2. In the interface configuration window, check the box to enable WAS.
3. Change the port number if desired.
4. Setting a password is optional; however you may wish to implement a password for this service for increased security.
5. Click <OK> to save the changes.
6. The InvisiConnect™ WAS Server is now configured to accept requests from WAS Clients.
7. Record the WAS Server's local IP address and the WAS Service port number you selected. You will need this information to configure the WAS Client.

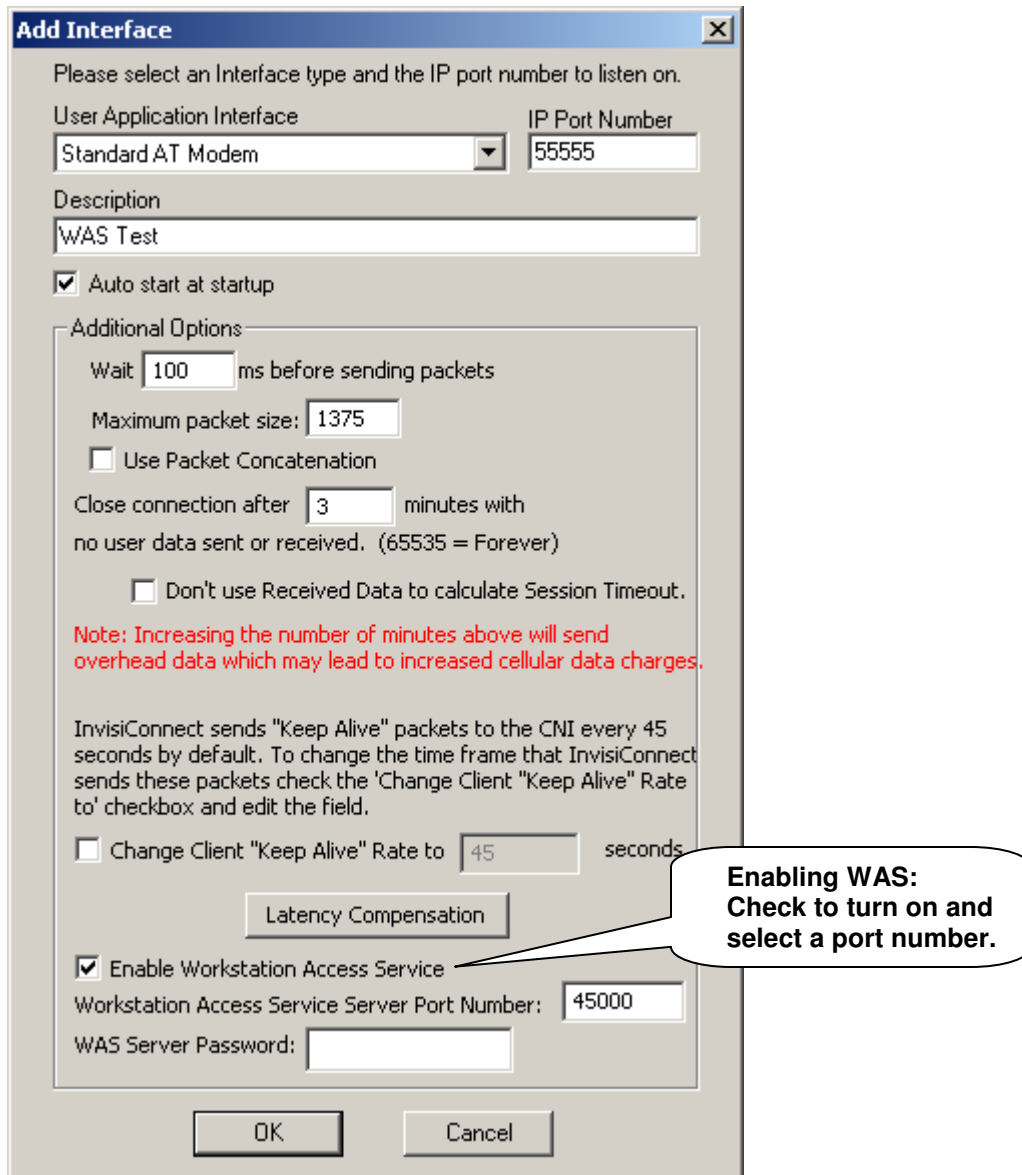
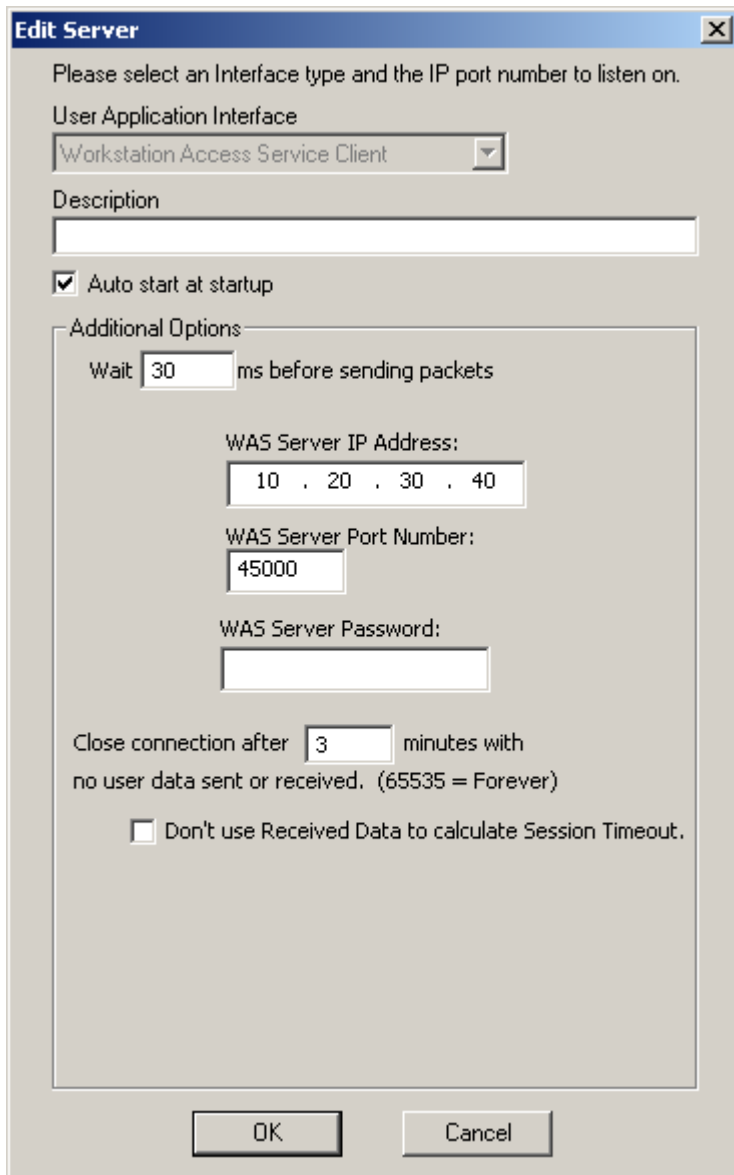


Figure 22 – Configuring WAS – Enable WAS

WAS Client Configuration Changes

1. On the WAS client computer, add a Workstation Access Service Client interface. This interface will connect to the WAS Server created in the previous steps.
2. Enter an optional description to identify the interface.
3. Enter the local IP address of the WAS server and the WAS port number you entered on the WAS Server. If you enabled a password, you should also enter it here. See Figure 23.
4. Timing and latency issues on your network may require you to increase the wait time. For testing purposes, you may want to change this number to 200 to help eliminate as many potential problems as possible. Later you can adjust this value to improve performance.



The screenshot shows a dialog box titled "Edit Server" with a close button (X) in the top right corner. The main text reads: "Please select an Interface type and the IP port number to listen on." Below this, there is a section for "User Application Interface" with a dropdown menu currently set to "Workstation Access Service Client". A "Description" text box is empty. A checked checkbox labeled "Auto start at startup" is present. An "Additional Options" section is enclosed in a rounded rectangle and contains: a "Wait" field set to "30" followed by "ms before sending packets"; "WAS Server IP Address:" with a field containing "10 . 20 . 30 . 40"; "WAS Server Port Number:" with a field containing "45000"; "WAS Server Password:" with an empty field; "Close connection after" followed by a field set to "3" and "minutes with no user data sent or received. (65535 = Forever)"; and an unchecked checkbox labeled "Don't use Received Data to calculate Session Timeout." At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 23 – Configuring WAS – Client Configuration

5. Add a COM port for the new interface. This is what the application will use so verify the settings with those expected in the application.
6. Click <OK> to save the settings, then in the main window, start the interface.
7. Launch the application and make sure it is set to use the COM port of the WAS client you just created. If your application can perform a “modem query” you can have it do that to test the connection.

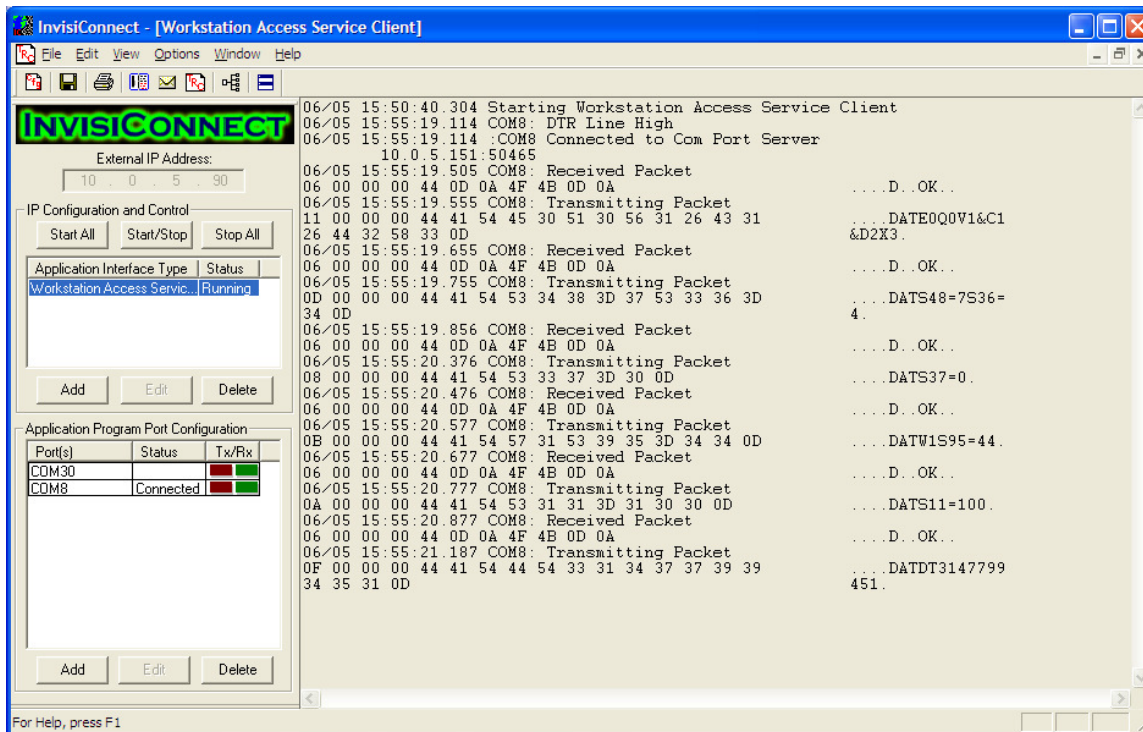


Figure 24 – WAS Configuration – Sample Data

8. Figure 24. All data routed through the WAS Server and all CNI client modems are managed by the InvisiConnect™ WAS server. This includes the SMS paging function. The WAS Client can be used on any workstation that has the ability to connect to the InvisiConnect™ WAS server, whether wired, wireless, internal or external connection.

Note that an external connection to the WAS server will most likely need additional firewall configuration to allow access to the server.

9. Once you have established a connection to the WAS server, the COM port status will change to “Connected” to confirm the connection and you will see the Transmit/Receive indicators illuminate as data is transferred.

This completes the InvisiConnect™ configuration for a WAS client. If your installation requires programming a CNI, continue with the next section, otherwise you can continue with Testing Your Configuration.

Programming a CNI with MP32

MP32 is the tool used to program a CNI. The first time you launch MP32 you are reminded about the Admin account’s password but you will not see this reminder on subsequent executions. Figure 25 will be the normal startup window after login. At this time, the CNI should be readily available and have the data/programming cable attached to it.

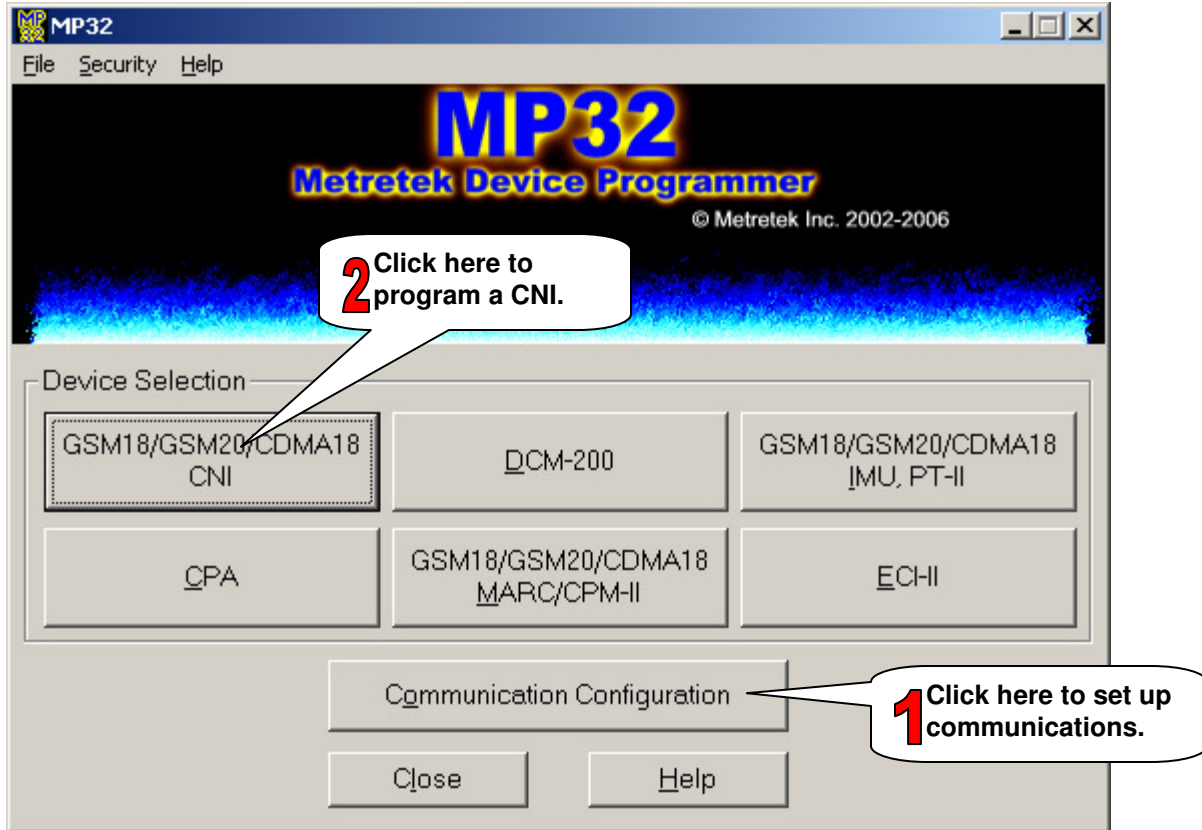


Figure 25 – CNI Configuration – Initial Window

1. Typically, you would attach the programming cable to COM1 of your computer. Click on the button labeled <Communication Configuration> to make changes or to verify which COM port you are using.
2. To begin programming a CNI, click on the <GSM18...> button indicated in Figure 25 and a window similar to Figure 26 will open.
3. If the CNI has already been programmed, you may wish to retrieve the settings by clicking on the <Read> button. Note that there is no visual feedback on the CNI that the configuration is being written or retrieved; instead, observe the bottom portion of the configuration window for status messages.
4. If you need to program the CNI with new settings, follow these guidelines: Note that having a configuration file (perhaps from another working and tested CNI) will reduce the programming errors; simply change the necessary values to match the new CNI.

- f. Enter a Device ID (RUID) here. Remember each RUID has to be unique so InvisiConnect™ can differentiate one CNI from another.
- g. Enter the public IP address and port of the InvisiConnect™ server. If you are not using the port shown, hold the <CTRL> key down and double-click the port number box to edit it.
- h. There are some options for how the CNI reacts to the call. Use these checkboxes to alter the CNI's behavior. Remember that placing a checkmark in any of the boxes other than Originate Calls will keep the cellular connection alive which will drain the battery. If your CNI is on AC power, you can disregard this warning.
- i. Using a port range will sequentially cycle through the numbers in the range each time a new connection is made to the server.
- j. If you have a module for an additional alarm on the CNI you can set the IP and port number for that alarm here.
- k. These settings are the defaults and are adequate for a typical installation.
- l. The debounce time is a threshold time in which duplicate keystrokes are treated as a repeat. Any duplicate packets within this period will be ignored.

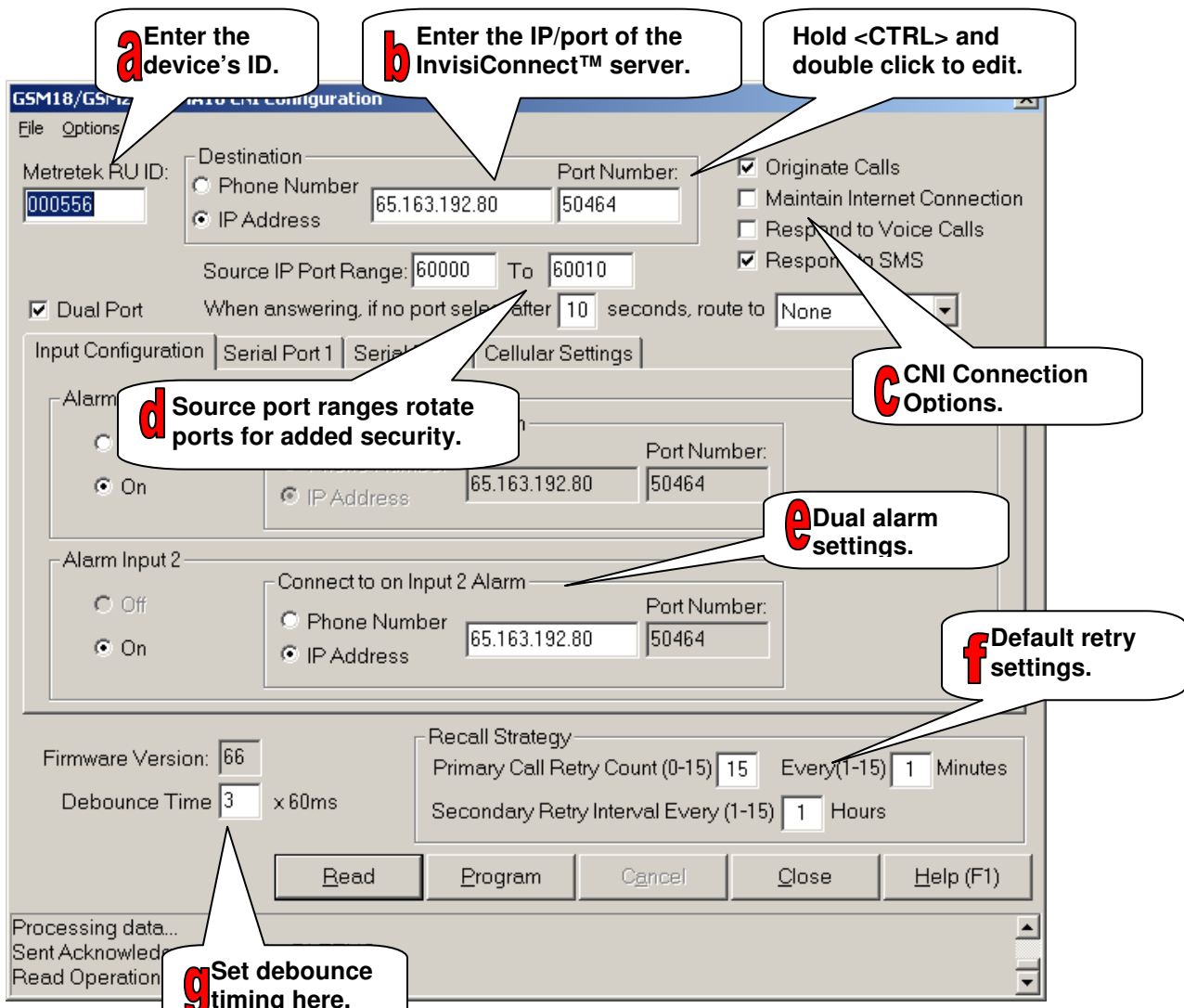


Figure 26 – CNI Configuration – Programming

5. The Serial Port 1 and Serial Port 2 tabs are where you configure the settings for each port so the CNI can communicate with your device. If you are experiencing problems communicating with your device, check these settings as well as the device settings. The configuration pages for each port are identical and the defaults are shown in Figure 27. Note that each serial port should have a unique RUID to distinguish between each device connected to the CNI.
6. The Cellular Settings tab shown in Figure 28 is where you will configure settings required to allow the CNI to initiate communications with the InvisiConnect™ server. The cellular carrier you have chosen should supply this information. The sample settings shown here show T-Mobile as the carrier.

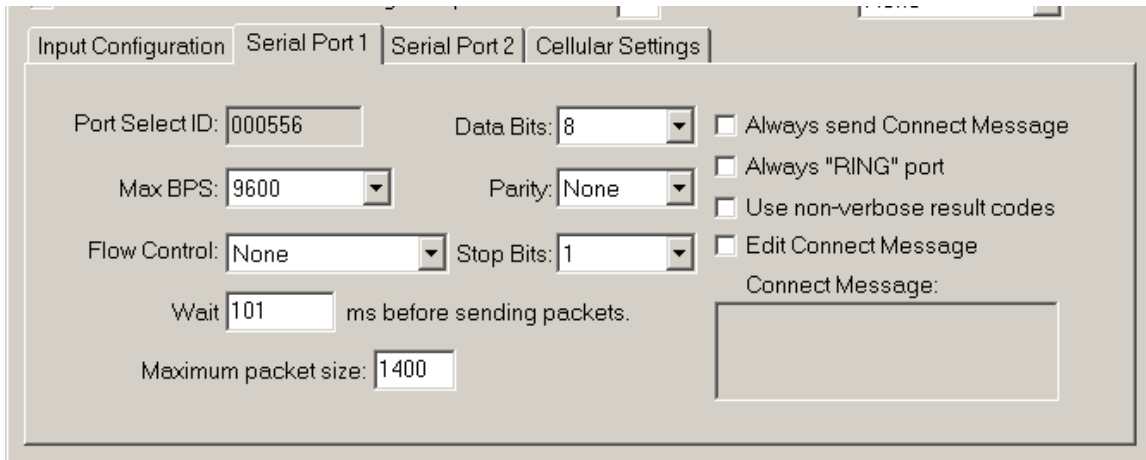


Figure 27 – CNI Configuration – Serial Ports

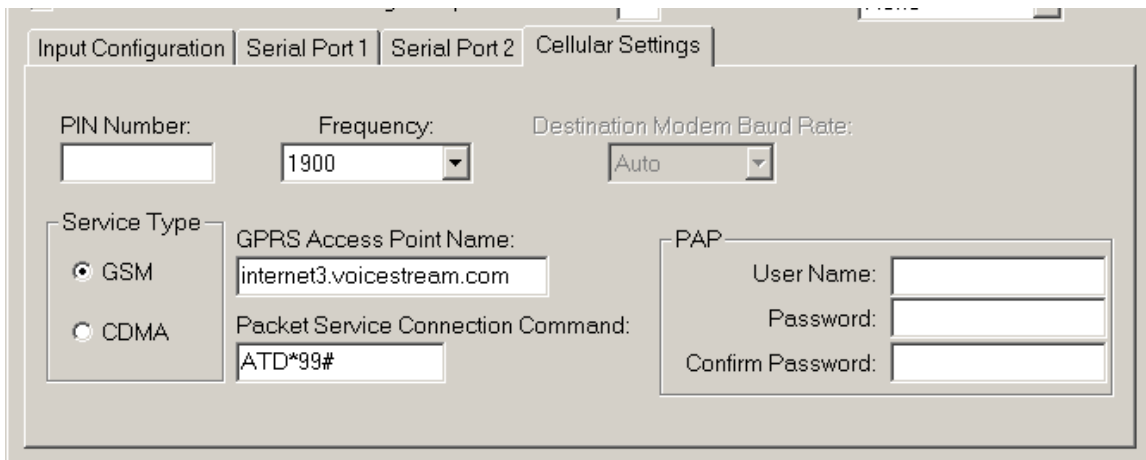


Figure 28 – CNI Configuration – Cellular Settings

7. Upon entering the information, click the <Program> button to program the CNI with the settings. You will be prompted to confirm the operation as in Figure 29. Once programmed, you can now test the connection between the CNI and InvisiConnect™.

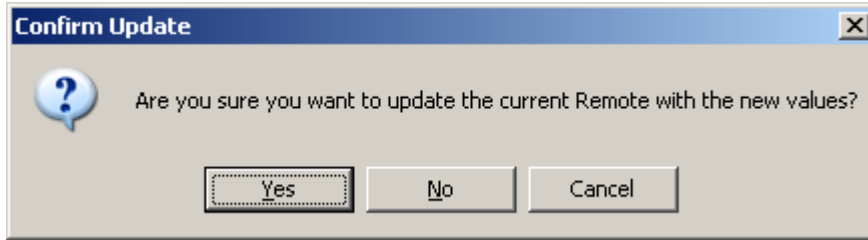


Figure 29 – CNI Configuration – Confirm Programming

8. At this point it is highly recommended that you save the configuration file for this CNI. Use the Save or Save As options under the File menu. Hint: Once you have tested a CNI, use its configuration file as a template to program another CNI, changing only what is necessary.
9. If you are finished programming your CNI, click the <Close> button to exit the programming page and then click on <Close> again to exit MP32.

Testing Your Configuration

At this point it is assumed that your Application is configured to use the InvisiConnect™ COM port that was created (either on the server or client) and configured earlier in this documentation and the Device is physically (and properly) connected to the CNI using appropriate cabling. You can still test portions of the setup without connecting a device, however you will not be able to use your application to query the device since it not connected to the CNI.

There are three parts to the testing phase. These connections need to be confirmed:

- The connection between the InvisiConnect™ server and the CNI communications needs to be tested.
- The connection between the application and InvisiConnect™ needs to be tested.
- And finally, the connection between the CNI and the device needs to be tested. This test is probably the most difficult to accomplish, especially if the device is already deployed.

InvisiConnect™/CNI Connection

This is the easiest connection to test since it does not involve your application or device. These steps send an SMS to the CNI, which will then respond and initiate a call.

1. Power on the CNI. Verify you have a cellular signal by viewing the green LED's activity which indicates signal strength – the faster it is blinking, the stronger the signal.
2. Start InvisiConnect™, verify its configuration and that the interface is running. If you are on a WAS client, make sure the WAS server is also running. Note that the interfaces are automatically started upon launching InvisiConnect™.
3. There are two different procedures to test the CNI/InvisiConnect™ connection.
4. The first procedure is helpful if you have not entered the CNI's information into the RUID database.
 - a. Momentarily short the *J2 Call* jumper on the CNI board to initiate a call from the CNI itself. Remember this will enter the RUID into the InvisiConnect™ database if it does not already exist.
 - b. Remember to observe the LED activity on the CNI and the data in the trace window in InvisiConnect™.
5. Upon successful completion of this procedure, you can now initiate a call from InvisiConnect™. Note that you may have to add the carrier specific domain information to the phone number as described above to ensure the CNI receives the SMS page.
 - a. Select Remote Configuration from the Options menu or click on the Remote Configuration button.
 - b. Select the device you wish to test from the list.
 - c. Click the <SMS Now> button.
 - d. Observe the CNI's LED activity and the trace window in InvisiConnect™ to verify the connection.
6. Figure 30. If you have the Remote Configuration window open when the CNI connection is established, you will receive updated information in the Connection Info tab such as the Last Reported Signal Strength and CNI port information identifying the Application Interface of the Default Server. Hint: This is why it is a good idea to descriptively name your interfaces.

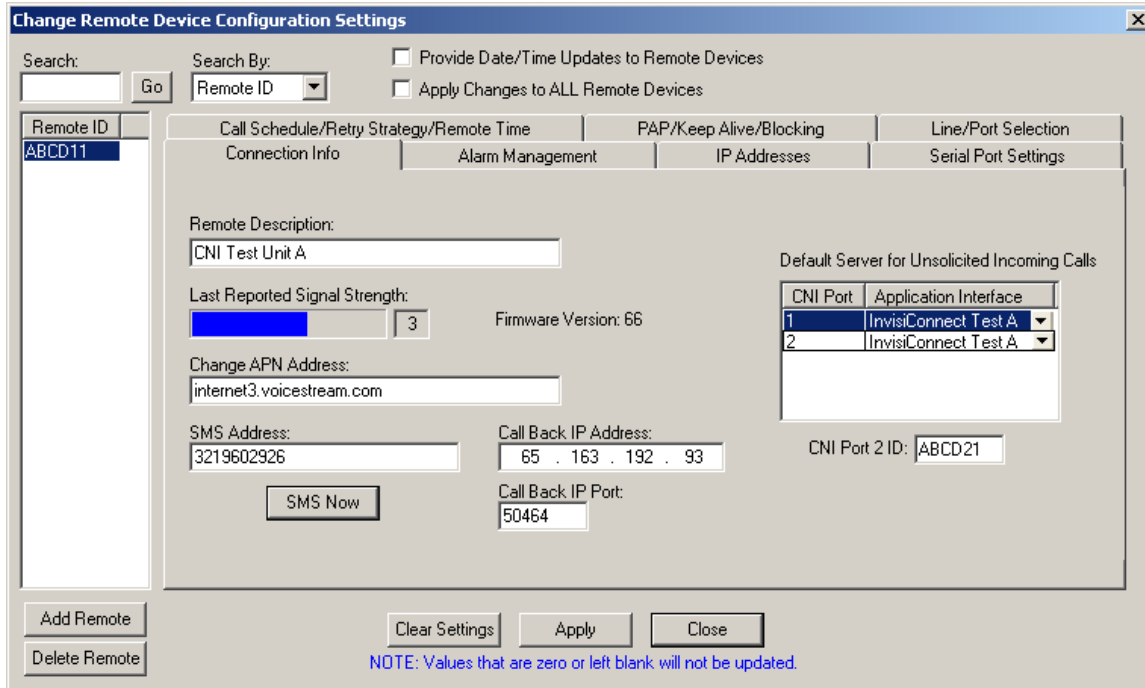


Figure 30 – InvisiConnect™/CNI Testing –Updates from CNI

- Once the CNI connects with InvisiConnect™ you have confirmed the settings are correct between them and can continue with testing the other components.

InvisiConnect™/Application Connection

This connection test only requires that the application use an InvisiConnect™ COM port. Once the application has been configured to use an InvisiConnect™ COM port, you can attempt to make a connection. Note that some applications will require you to make changes in more than one location.

Please note these steps are generic and should work in most cases. For specific instructions, refer to your application's setup guide.

- Start InvisiConnect™, verify its configuration and that the interface is running. If you are on a WAS client, make sure the WAS server is also running. Note that the interfaces are automatically started upon launching InvisiConnect™.
- Start your application and verify it is using the same COM port as the one you configured in InvisiConnect™.
- Configure a new device (or reconfigure an existing device) with the phone number of the CNI.
- Instruct the application to dial the device.
- Once a connection has been established, use your Application to view data and/or send commands.
- Observe the trace window in InvisiConnect™ and the LED activity on the CNI to verify the connection.
- Once the application connects to the CNI you have confirmed the settings are correct between them and can continue with testing the other components.

Note that if there is no device connected to the CNI, you will not get the expected results of any commands you send from the application. This procedure is only to test the communications connections, not transfer data.

CNI/Device Connection

This procedure will help test the connection between the CNI and the Device. Refer to your device's user guide and the CNI User Guide to make the necessary hardware connections. For reference, the CNI User Guide has an example of how to connect a Metretek Gas Volume Corrector to a CNI board.

1. Your device should already be configured to answer a call.
2. Start InvisiConnect™, verify its configuration and that the interface is running. If you are on a WAS client, make sure the WAS server is also running. Note that the interfaces are automatically started upon launching InvisiConnect™.
3. Launch your application that normally communicates with the device and make sure it is properly configured and communicating with InvisiConnect™.
4. Make sure the CNI is powered up, configured and connected the device.
5. Instruct the application to dial the device.
6. Observe the trace window in InvisiConnect™ and the LED activity on the CNI to verify the connection.
7. Once a connection has been established, use your Application to view data and/or send commands to the device.
8. The device should respond as when it was connected via a phone line and you should be able to perform any functions available to you from the application.
9. Now you can use your application as you normally would to call, configure and retrieve data from the device.

Congratulations! Upon successful completion of this testing phase, your InvisiConnect™ solution is properly configured and operating! Continue testing CNIs and different devices.



Final Notes

We at Metrotek are continually improving our products and software and are constantly improving InvisiConnect™ as both technology and our customers' needs change. To help us improve InvisiConnect™, we ask that you contact us at support@metrotekfl.com with any questions or concerns you have about this product. If you have a suggestion for an improvement, we would like to hear about that too!

And since we are continually improving our products, minor version updates are typically free of charge to existing InvisiConnect™ customers.

Remember there are specific settings in InvisiConnect™ that allow you to “tweak” the communications process if you get inconsistent communications. Of course, Metrotek Technical Support is available to assist with your setup.

Glossary/Terminology

1XRTT (1X) – Single Carrier Radio Transmission Technology. Sometimes referred to as a "2.5G" standard.

APN – Access Point Name. A way of verifying that you are allowed to transmit and receive data.

Application – Your software that is used to collect data from your device.

Binary – A base₂ numbering system and is the operating mode for all electronics. Valid numerals are 0 and 1, which are often referred to by their Boolean values of True/False or On/Off. A single value is also called a "bit."

Carrier – The cellular provider, such as Cingular, Verizon or T-Mobile. Each carrier has chosen to use either CDMA or GSM for digital communications.

CDMA – Code Division Multiple Access. One method of cellular radio communications.

CNI – Cellular Network Interface. The remote portion of the InvisiConnect™ solution that is connected to your device.

CSD – Circuit Switched Data. Typically analog cellular communications are in this form.

Device – The physical device used to collect data.

Firewall – Hardware or software that inspects network traffic and either grants or denies traffic based on its type, source and/or destination information.

GSM – Global System for Mobile communications. Another method of cellular radio communications.

Hexadecimal – Or simply "hex" is a base₁₆ numbering system typically used in computer programming. Valid numerals are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F.

InvisiConnect™ - The software that provides the connection through the CNI to your device, which translates the data between your application and your device.

NAT – Network Address Translation. This is used to open a socket from one network to another, typically from the Internet to an internal network. InvisiConnect™ requires the CNI be able to connect to it either directly or through NATting.

OTA – Over the Air.

Remote Unit – See CNI.

Server – The computer (hardware and operating system) where InvisiConnect™ is installed and running.

Socket – A networking term, which is comprised of an IP address, a port and a protocol.

WAS – Workstation Access Service. The feature in InvisiConnect™ that allows another computer (client) to connect to a central installation of InvisiConnect™ that has all of the settings and configurations. This allows changes to be made in only one location rather than many, reducing errors.