Serial/IP™ Redirector 4.3 User Guide

Table of Contents

1. Getting Started

This chapter provides the basic information you need before installing and using the Serial/IP Redirector.

In This Chapter

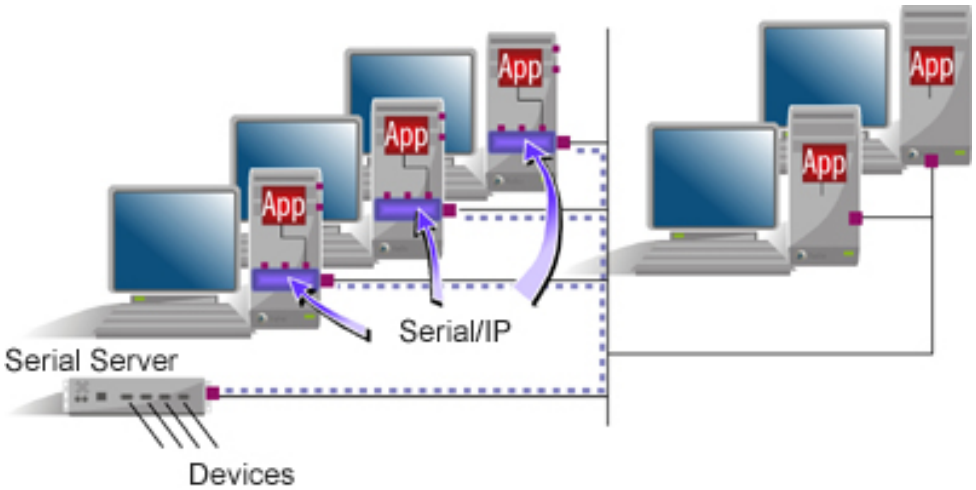
1. Getting Started

1.1 A Brief Review of the Basics

The Serial/IP Redirector from Tactical Software adds "virtual" COM ports to the Windows operating system. Similar to regular COM ports that allow PC applications to use local serial ports, Serial/IP COM ports allow PC applications to use serial ports on a serial server. Because Serial/IP COM ports work like regular COM ports, PC applications do not have to be changed to use a serial server through the Serial/IP Redirector.

The Serial/IP Redirector runs as a kernel-level device driver in the Windows operating system. This means that Serial/IP COM ports are available to PC applications at all times, even if no user is logged in. The Serial/IP Redirector is a high-performance kernel-mode driver with a small "footprint", modest memory requirements and low overhead. The Serial/IP applet in the Windows Control Panel configures Serial/IP COM ports and displays their activity.

Most TCP/IP-based serial servers will work with the Serial/IP Redirector, which detects and uses the specific protocols supported by a serial server. When configuring Serial/IP COM ports, you can use the Serial/IP Configuration Wizard to verify immediately that the Serial/IP Redirector can communicate with the serial server over the network.



The pieces fit together in the following way:

1. You place a serial server on your network and attach devices to its serial ports.

2. Using the manufacturer's instructions, you configure the serial server to make its serial ports available to the network via TCP/IP.

3. You install the Serial/IP Redirector software on each PC that will use devices attached to the serial server.

4. You configure the Serial/IP Redirector to create one or more virtual COM ports.

5. For each Serial/IP COM port, you specify the IP address of a serial server and the TCP port number that provides access to its serial ports.

6. In your PC application, you change settings to use Serial/IP COM ports instead of local COM ports.

7. Thereafter, the PC application can use serial ports on the server instead of local serial ports.

1.2 What You Need to Get Started

Before you install and use the Serial/IP Redirector, you will need the following:

1. **Administrator privileges** when you are installing the software.

2. A **serial server** on your TCP/IP local area network. This server must be configured to provide serial ports to the network using the instructions provided by the manufacturer. Chapter 2 of this document provides general guidance on server configuration and what to look for in the manufacturer's instructions.

3. The **Serial/IP Redirector setup program**. This software will be installed on each PC that uses the serial server.

4. A **license key** to enable the Serial/IP Redirector software. If you are installing the 30-day evaluation software, you don't need a license key because it is built in to the evaluation software. Exception: You do not need a license key if a permanent license for the Serial/IP Redirector software was included with your serial server.

1.3 Solving Problems

If problems are encountered with the Serial/IP Redirector, a number of resources are available to you:

- For problems during installation, see the section Troubleshooting Installation Problems in Chapter 2.
- For problems with application operation, see the section Troubleshooting Application Problems in Chapter 3.
- The Frequently Asked Questions (FAQ) on the Tactical Software web site are searchable and address common technical support issues.
- The Technical Notes on the Tactical Software web site provide more detailed information about Serial/IP Redirector features provided for special special situations, such as DOS applications.
- The Support section of the Tactical Software web site contains a revision history for this product.
- For technical support, please refer to the support information provided by your supplier and the support section of the "readme.txt" file included with the Serial/IP Redirector software. This file is displayed during software installation and is also placed in the installation folder.

2. Installing the Serial/IP Redirector

The Serial/IP Redirector software is installed on a PC by a setup program. Prior to the installation, you must configure your serial server. After the installation, you configure the software to create Serial/IP COM ports and configure them with the IP address (or DNS name) and TCP port numbers of serial servers. This chapter covers these procedures in the order they should be performed.

In This Chapter

How to proceed if the installation is not trouble-free.

2. Installing the Serial/IP Redirector

2.1 Pre-Installation Checklist

The PC running the Serial/IP Redirector must comply with the following requirements:

- Processor: Intel-compatible, Pentium class.
- Operating system: All versions of

  Windows XP
  Windows Server 2003
  Windows 2000
  Windows NT 4.0 SP5 or later
  Windows Me
  Windows 98
  Windows 95
  Microsoft NT/2000 Terminal Server
  Citrix MetaFrame

- Windows Installer 2.0 (already present on most PCs and available at no charge from the Microsoft web site).
- Disk storage: 4 megabytes on the boot drive.
- Network: Microsoft TCP/IP networking software.

Requirements applying to the serial server:

- Must provide access to its serial ports via TCP/IP connections.
- Optionally, support the COM Port Control protocol specified in IETF RFC 2217.

2.2 Configuring the Serial Server

The server must make its serial ports available to the Serial/IP Redirector through a TCP/IP connection from the PC to the serial server. Most serial servers with TCP/IP network interfaces can be configured to comply with this requirement, though the procedure for this will vary according to the manufacturer.

This section describes the necessary configuration operations in general terms. The documentation that accompanies your server should contain specific instructions. If this does not appear to be the case, contact your server supplier for this information.

Please bear in mind that most problems encountered in using a serial server stem from server configuration mistakes. Since this is a likely source of problems, please use care in configuring the server.

The following is the recommended approach to configuring the serial server:

1. Ensure the server is installed on the same TCP/IP network as the PC on which you will later use the Serial/IP Redirector. If this is not the case by default, consider customizing the route table on the PC to make the server reachable.

2. Take note of the IP address (or DNS name) of the serial server. IP addresses take the form xxx.xxx.xxx.xxx, where each xxx has a maximum value of 255. The IP address (or DNS name) will be needed later when configuring the Serial/IP Redirector to use this serial server.

3. Configure the serial server to make one or more of its serial ports accessible at one or more TCP port numbers. *TCP port numbers are not the same as serial port numbers.* The serial server manufacturer will probably recommend a TCP port number range.

   Note: *Do not attempt to guess the TCP port number to use.* Your serial server documentation should contain specific information regarding the TCP port numbers that can be, or must be, used.

4. Optionally, define a "hunt group" of serial ports so that multiple serial ports appear at one TCP port number on the server. Some serial servers support this convenient feature, which automatically selects an unused serial port from a group of serial ports when the Serial/IP Redirector connects to the serial

server.

5. If available, enable the Telnet protocol for incoming TCP/IP connections on the TCP ports (see step 3 above).

2.3 Running the Serial/IP Setup Program

Before running the Serial/IP setup program:

- Ensure that you are logged in as a user with administration privileges.
- Quit all Windows programs that use COM ports.

The Serial/IP setup program takes you through the following steps:

1. If you have previously installed an evaluation copy of the Serial/IP Redirector, or have an existing older version, you will be prompted to run the Uninstall procedure.
2. Display of the end user license agreement, which you must approve to continue the installation.
3. Selection of an installation folder, which defaults to "Program Files\Tactical Software\SerialIP" on your boot drive.
4. Entry of your name, company, and license key. If you do not supply a license key, the installer program automatically uses a license key that will expire 30 days from the current date. You can provide a license key later by using the **Licensing** button in the Serial/IP Control Panel. If the license key is not accepted when you enter it, click here for more information.
5. Selection of installation options. This includes the **Administrator Only** option, which will restrict use of the Serial/IP Control Panel to users with administrator privileges. If you select this option, non-Administrator users can use the Serial/IP Redirector, but they can not open the Serial/IP Control Panel.
6. If selected during the install, display of the Release Notes, which contains important information for your review before proceeding.

The license key activates the Serial/IP Redirector software, sets the maximum number of Serial/IP COM ports that the Serial/IP Redirector can use, and enables optional software features. If the built-in evaluation license key

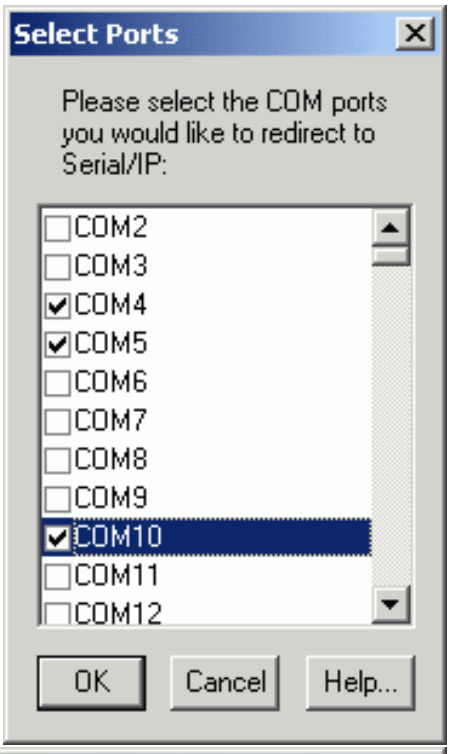
is used, it allows up to 256 Serial/IP COM ports and disables any optional software features.

If the same license key is used on more than one PC, the Serial/IP Redirector will display a window listing the IP address of the PC that has the conflicting license key. An updated license key can be entered in this window, after which the Serial/IP Redirector can continue normal operation. Click here for more information.

At the end of the installation, the setup program automatically runs the Serial/IP Redirector to display the **Select Ports** if needed. This will not occur if the setup program has been able to restore settings used in a previous installation of the same product.

2.4 Selecting Serial/IP COM Ports

The **Select Ports Window** displays a list of COM ports available to become Serial/IP COM ports. COM ports that already exist in the Windows operating system (such as COM1 for a local serial port) are automatically excluded from this list to prevent conflicts.

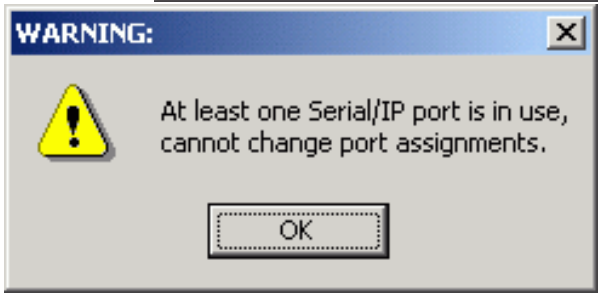


This window appears automatically at the end of the software installation by the Serial/IP setup program. Later, you can use this window to change the selected ports by using the **Select Ports** button in the Serial/IP Control Panel.

In the Select Ports Window you select one or more new COM ports for Serial/IP to create. Because some older client programs do not display COM ports higher than COM4, consider selecting ports in the COM 1-4 range if you will be using such applications.

The list of COM ports goes up to COM256. The number of COM ports that you can select is limited by the license you have purchased. When you have checked the maximum number of COM ports allowed by your license, the other COM ports are greyed and no longer selectable.

Your changes become effective when you click the **OK** button. If running Windows 98/95/Me, it is necessary to restart Windows.



Note: If you attempt to change the ports setting while one or more Serial/IP COM ports are still in use by a PC application, your changes will not be made and you will see a warning message that the port assignments cannot be changed.

2.5 Configuring Serial/IP COM Ports in the Control Panel

Control Panel Overview

The Serial/IP Control Panel window manages the settings for Serial/IP COM Ports.

There are three ways to display the Serial/IP Control Panel:

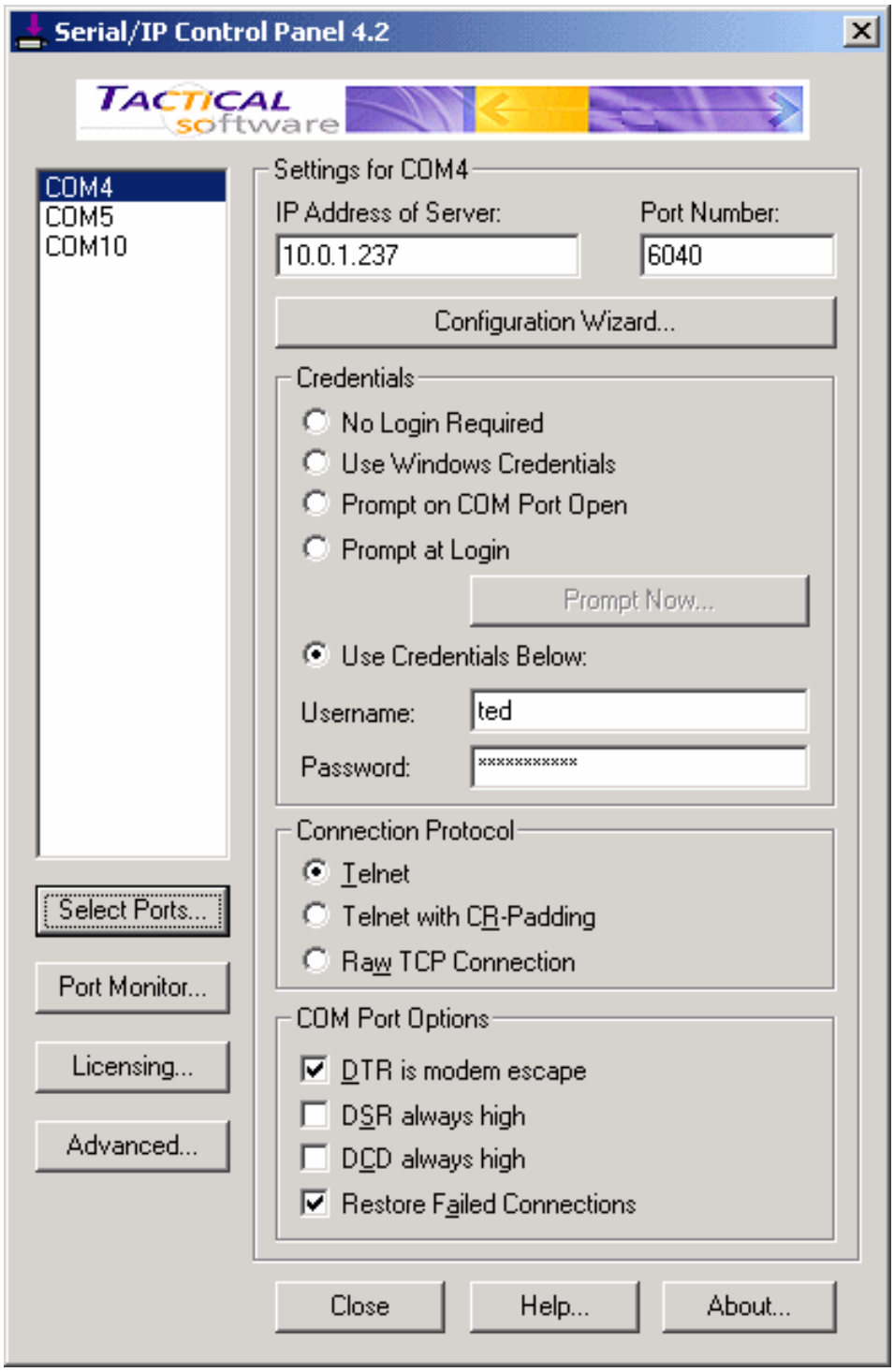
- Open the Serial/IP applet in the Windows Control Panel folder.
- Right-click on the Serial/IP icon in the Windows System Tray and select the **Configure** command.
- In the Window Start Menu, select the Serial/IP program group and select **Control Panel**.

Note: If Administrator-Only Mode was chosen during installation of the Serial/IP Redirector software, only users with administrator privileges can bring up with Serial/IP Control Panel.

At the left side of the Control Panel is a list of the COM ports that you have selected (in the Select Ports window) for use by the Serial/IP Redirector. If you wish to change which ports appear in this list, use the **Select Ports** button.

Each COM port has its own settings. When you click on a COM port, the Control Panel display changes to reflect the settings for that COM port.

Note: When you change settings for a COM port, the changes are effective immediately. There is no separate confirmation dialog to confirm or cancel your changes.



Configuring Serial/IP COM Ports

You configure each Serial/IP COM port as follows:

1. Select a COM port in the list.
2. For **IP Address of Server**, enter a numeric IP address or a DNS name for the serial server.

   Note: If an optional Serial/IP preset file exists, an additional **Preset** pull-down menu will appear in the space above **IP Address of Server** field box. This optional feature is described in Appendix B.

3. For **Port Number**, enter the TCP port number that the serial server uses to provide its serial ports to the network. This TCP port number must be the same as the TCP port number you used when you configured the serial server, as discussed in the previous section Configuring the Serial Server.

4. For **Server Credentials**, the default is **No Login Required**. If your serial server does require a login by the Serial/IP Redirector, the Serial/IP Redirector needs to provide a username and/or password every time an application tries to use the serial server. For details, see More About Login Credentials below.

5. Click the **Configuration Wizard** button and then click the **Start** button that appears in the Wizard window. This important step verifies that the Serial/IP Redirector can communicate with the serial server using the settings you have provided. If the **Log** display does not show errors, click the **Use Settings** button in the Wizard, which makes the recommended settings effective and returns you to the Control Panel to continue with the following steps. For more about the Configuration Wizard, see the next section Using the Configuration Wizard.

6. For **Connection Protocol**, the setting must match the TCP/IP protocol that the serial server supports. The Configuration Wizard is usually able to determine the correct setting. If you wish to make this setting manually, see More About Connection Protocols below.

7. For **COM Port Options**, the settings must match the COM port behavior expected by the PC application that will use this COM port. The Configuration Wizard will recommend a combination of settings. If you wish to make this setting manually, see More About COM Port Options below.

Other Serial/IP Redirector Features Available from the Control Panel

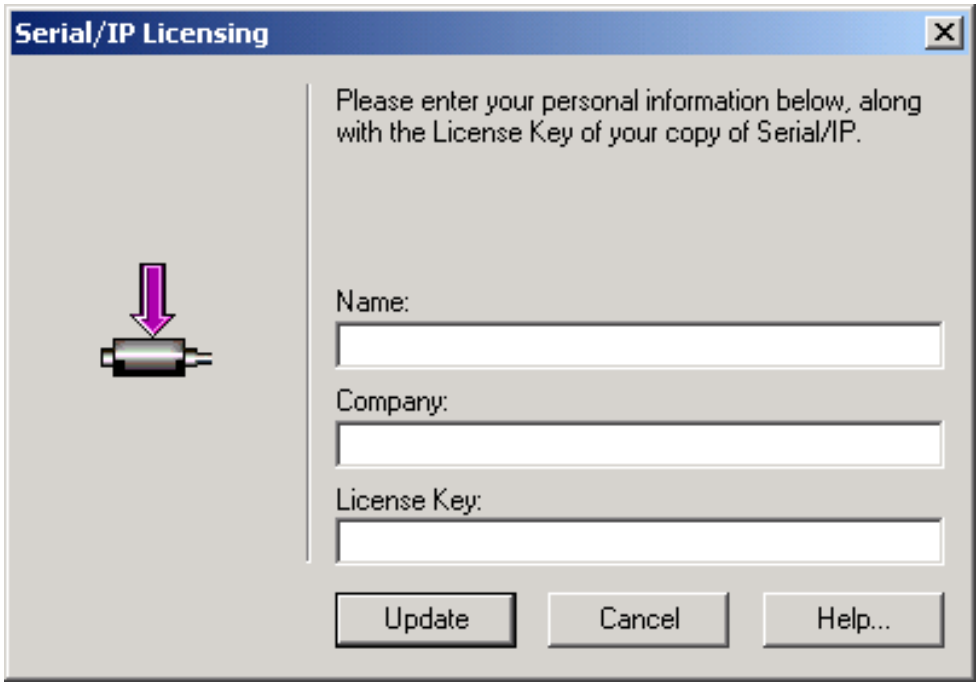
Buttons on the Control Panel take you to the following additional features:

- The **Port Monitor** button displays a tabbed window that shows Serial/IP COM Port activity. For details, see the section Monitoring Serial/IP COM Ports in chapter 3.

- The **About** button displays a window containing the version of the software, the license expiration date (if any), and other notices.

- The **Help** button displays this document with the Adobe Acrobat® Reader® which you can download free of charge.

- The **Licensing** button displays a window that shows the name, company, and license key that enables the Serial/IP Redirector software. This information can be updated in this window.



More About Server Credentials

In addition to the No Login Required setting, there are three ways to specify server credentials:

1. **Use Windows Credentials** • The Serial/IP Redirector will use the user name and password of the current user's Windows login. The user must log off and log back on before this choice is effective. Note: This option is not available in Windows 98/95/Me or multi-user operating systems.

2. **Prompt at Login** • The Serial/IP Redirector will request a user name and password when the current user logs into Windows, and will provide those values to the serial server for any Serial/IP COM port for which this option is selected. The **Prompt Now** button causes the prompt to occur immediately without requiring login. Note: This option is not available for multi-user versions of Windows, such as NT/2000 Terminal Server and Citrix MetaFrame.

3. **Prompt on COM Port Open** • The Redirector will request a user name and password every time the COM port is opened. This allows the use of the Redirector in applications that use dynamic credentials, for example. When the application opens the COM port:
    - The Redirector suspends the application.
    - The Redirector presents a dialog box that identifies the COM port and contains entry fields for user name and password.
    - If the user clicks "OK", the Redirector passes those credentials to the server. If the user clicks "Cancel", or does not click "OK within 60 seconds, the Redirector proceeds as if no credentials are required for this connection.
    - The Redirector waits for its connection to the server to become operational.
    - The Redirector resumes the application.

4. **Use Credentials Below** • The Serial/IP Redirector will use the values you enter in the **Username** and **Password** fields.

If the serial server is configured to *not* require user authentication, the Server Credentials setting must be set to No Login Required. If in doubt, run the Configuration Wizard to determine if the serial server requires user authentication, and test the username and password if it does.

When using Prompt on Port Open, please note:

- If a user is not logged in at the time a COM port is opened, the Redirect proceeds as if "No Login Required" was selected.
- This feature is not available on Windows 98, 95, ME, or multi-user versions of Windows like Terminal Services and Citrix.
- When the Configuration Wizard is run, the Username and Password fields in the Configuration Wizard window are enabled, and those credentials will be used during the Configuration Wizard session. In this case, the credentials are not copied from the Configuration Wizard to the Control Panel when the "Use Settings" button is used.

More About Connection Protocols

There are three options for the connection protocol between the Serial/IP Redirector and the serial server:

1. **Telnet,** which is the correct setting for most serial servers. If this protocol is selected, the Serial/IP redirector will automatically request the use of the Telnet "binary mode" to allow proper operation of applications. If the serial server supports the COM Port Control protocol (RFC 2217), it will automatically be used.

2. **Telnet with CR-Padding** must be set if the serial server uses Telnet software that pads CR/LF characters with null characters.

3. **Raw TCP Connection** is used to communicate with a serial server without any additional protocol. Although this is possible with most servers, it is not recommended because it precludes the use of helpful Telnet protocol features.

More About COM Port Options

These options adjust the behavior of Serial/IP virtual COM ports to meet the needs of certain PC applications.

- **DTR** causes the Serial/IP Redirector to simulate DTR transitions. This setting is usually disabled because it is only useful in the uncommon case that a modem is connected to the serial server.

- **DSR** causes the Serial/IP Redirector to emulate DSR-always-on signal behavior. When this setting is enabled, the DSR signal is raised when the TCP/IP connection to the serial server is established (usually immediately on COM port open), and the DSR signal is dropped when the TCP/IP connection is terminated.

- **DCD** causes the Serial/IP Redirector to emulate DCD-always-on signal behavior. When the setting is enabled, the DCD signal is raised when the TCP/IP connection to the serial server is established (usually immediately on COM port open), and the DCD signal is dropped when the TCP/IP connection is terminated.

- **Restore Failed Connections**. Normally the Serial/IP Redirector will close the TCP connection to the serial server only when the Serial/IP COM port is closed by the PC application. If the TCP connection is closed by the serial server or otherwise fails when this option is disabled, it cannot be re-established until the Serial/IP COM port is closed and reopened. When this option is enabled, a dropped TCP connection will cause the Serial/IP Redirector to automatically attempt to reconnect to the serial server. The first reconnection attempt occurs immediately, with subsequent attempts occurring at 15-second intervals until

the connection is restored or the Serial/IP COM port is closed by the PC application.

When the Configuration Wizard detects support for the COM Port Control protocol in the serial server, it recommends the following settings:

- Emulate DTR (unchecked)
- Emulate DSR always high (unchecked)
- Emulate DCD always high (unchecked)

Adjusting the COM Port options — with the exception of Restore Failed Connections — is not necessary if the serial server supports the COM Port Control protocol. These options should be left "as is" and will be set automatically when the Configuration Wizard detects COM Port Control protocol support in the serial server.

2.6 Using the Serial/IP Configuration Wizard

The Configuration Wizard determines whether the Serial/IP Redirector can communicate with the serial server using the following settings for a Serial/IP COM port:

- IP Address of Server
- TCP Port Number
- Credentials

Additionally, the Configuration Wizard recommends values for the following settings:

- Connection Protocol
- COM Port Options

If the Configuration Wizard has completed successfully, you can accept its recommended settings by clicking the **Use Settings** button. This is usually the fastest way to configure Serial/IP COM ports.

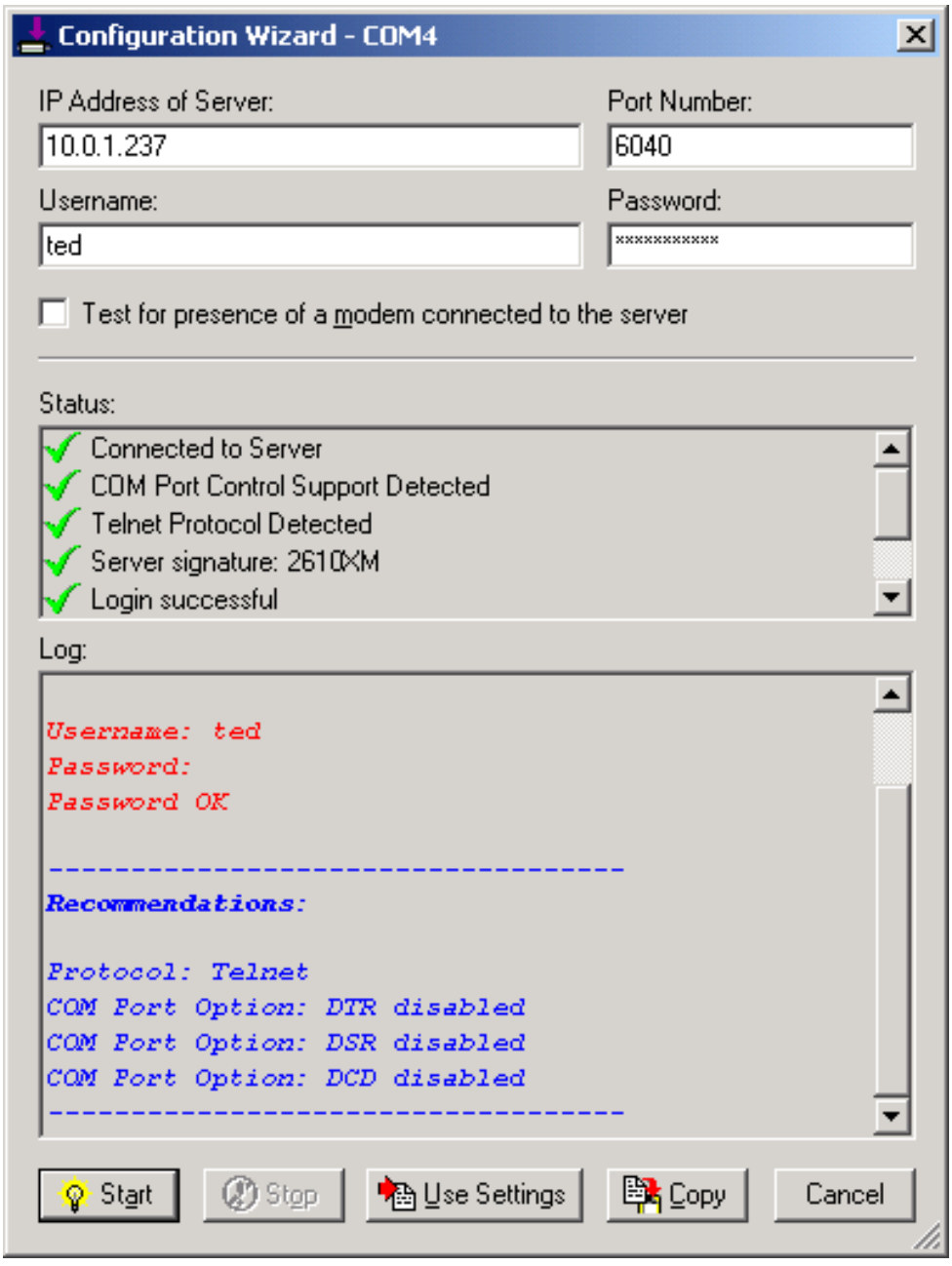
If the Configuration Wizard does **not** complete successfully, you must determine and fix the cause of the problem before proceeding. If the Configuration Wizard is unable to work with your serial server, the Serial/IP COM ports will not work when a PC application attempts to use it.

Activating the Configuration Wizard

1. Open the Control Panel and select a Serial/IP COM port from the list at the left.
2. The Control Panel displays settings for this Serial/IP COM port. If they need to be set, refer to Configuring Serial/IP COM Ports in the Control Panel earlier in this chapter. If you provide initial settings for the following, the Configuration Wizard will use them: **IP Address of Server**, **Port Number**, and **Credentials**.
3. Click the **Configuration Wizard** button to open its window.

Running the Configuration Wizard

1. If the **IP Address** and **Port Number** have not been provided, enter those settings now. A DNS name can be used instead of an IP address.
2. If the **Username** and **Password** are enabled, this means that **Use Credentials Below** was selected in the Serial/IP Control Panel. If so, ensure that these two settings are correct.
3. Click the **Start** button in the lower left corner of the window. The Wizard will connect to the serial server using the IP address and TCP port number. If this is successful, the Wizard will log in to the serial server if you have provided a valid username and/or password.
4. After a successful connection with the serial server, the **Status** panel shows a summary of server characteristics and the **Log** panel shows the interaction with the serial server. The sample shown at right is an example of a successful run of the Configuration Wizard. To copy the contents of the Status and Log panels to the Windows clipboard, use the **Copy** button.



5. If the Wizard displays errors, you can adjust settings at the top of the window and click the **Start** button again without returning to the Serial/IP Control Panel. See Appendix C Configuration Wizard Messages for detailed information on the meaning of errors and recommendations on resolving them

6. Based on the results of its interaction with the serial server, the Wizard will recommend settings for Connection Protocol and COM Port Options.

7. Click **Use Settings** to make all settings effective for the current Serial/IP COM port. Click **Cancel** to discard settings and return to the Serial/IP Control Panel.

The Configuration Wizard should be used for each Serial/IP COM port by returning to the Serial/IP Control Panel, selecting each COM port, and re-running the Configuration Wizard.

2.7 Troubleshooting Installation Problems

Please note the following suggestions regarding installation problems:

- If your license key is not accepted when you enter it, click here for more information.
- Are you using correct values for both **IP Address of Server** and **TCP Port Number**?
  A common mistake is to assume the TCP port number is the "device number" on the server. TCP port numbers start at a large number, usually 4000 or higher. **Note**: *Any TCP port number less than 1024 is almost always wrong.* See Appendix D Basic Diagnostics for ways to debug this type of problem.
- Are your settings for **Credentials** matching what the serial server expects?
  The Log display in the Configuration Wizard will show authentication problems with serial server login.
- Is the serial server providing a serial port on the expected **TCP Port Number**?
  Serial servers differ in the methods used to make serial ports available to the network on a TCP port.
- Are **errors** appearing in the Log display of the Configuration Wizard?
  For detailed information and tips, see Appendix C Configuration Wizard Messages.

3. Using the Serial/IP Redirector

A PC application employs ports on a serial server when it uses the COM ports that are created and managed by the Serial/IP Redirector.

In This Chapter

3.1 Checking for Special Application Requirements

Nearly all Windows applications can use Serial/IP COM ports and serial servers instead of local COM ports. The exceptions mostly fall into two general categories.

- Does the application require serial line control and/or status?

  Most Windows applications perform only the common read/write operations that all serial servers support. Some applications, however, also require some of the features provided by the COM Port Control protocol specified by IETF RFC 2217. For these applications, the serial server must support the COM Port Control protocol and provide at least the serial port control and status functions that the application requires.

  Generally, applications requiring COM Port Control are of two types:

  1. Applications that must programmatically change serial port settings like baud rates and framing. A common workaround is to manually make these settings on the serial server. If an application must change these settings on the fly, COM Port Control will be required.

  2. Applications that require serial line status signals.

- Is the application a DOS application?

  Some DOS applications are not able to access Windows COM ports (including the virtual COM ports created by the Serial/IP Redirector) without additional software to bridge the gap between DOS and Windows COM ports. If you plan to use the Serial/IP Redirector with a DOS application, refer to the technical note Using Tactical Software Redirectors with DOS Applications.

3.2 Modifying Application Settings

For a PC application to use the Serial/IP Redirector and a serial server, its COM port settings must be changed to use Serial/IP COM ports.

The general procedure is:

1. Find the "settings," or "preferences" or "options" command setting in the application that allows you to specify the COM port to be used by the program.

2. Choose a Serial/IP COM port from the list.

   Note: Some older Windows applications do not recognize COM ports higher than COM4. Some versions of Windows HyperTerminal, for example, have this limitation. If you need to use such an application, create Serial/IP COM ports in the COM 1-4 range.

3.3 Troubleshooting Application Problems

When the Configuration Wizard reports no errors but the PC application doesn't work, the following suggestions may help identify the cause of the problem:

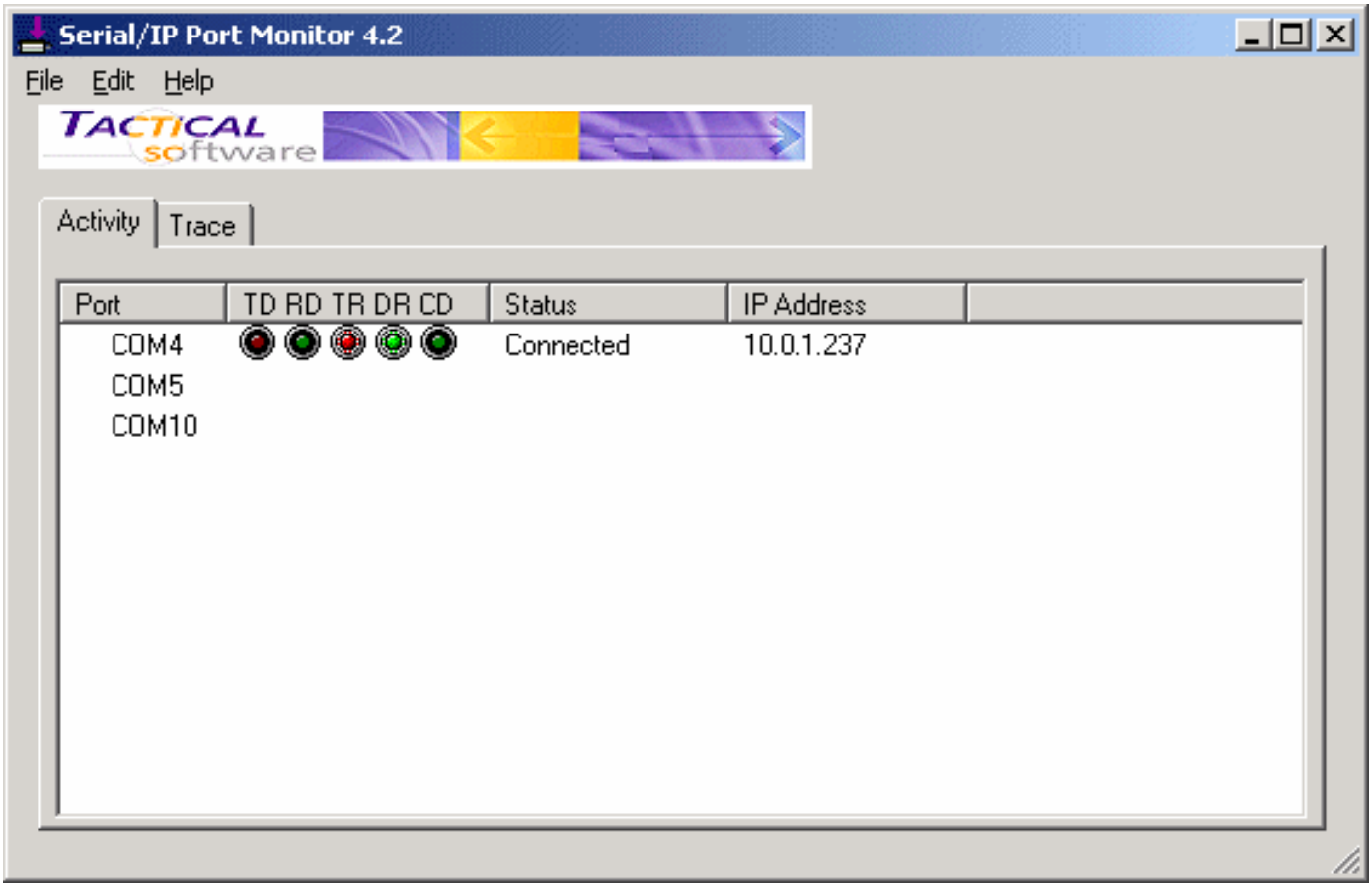
- Use the Serial/IP Activity window to see if the Serial/IP COM port is being used when the application runs. It is surprisingly easy to forget to change all application COM port settings to use Serial/IP COM ports. For details, see the section Monitoring Serial/IP COM Port Activity.

- Use the Serial/IP Trace window to closely inspect the data being read and written by the application. The trace data is fairly self-explanatory, and it can be easy to diagnose a problem from this information. For details, see the section Tracing Serial/IP COM Port Data.

- Double-check if the application must have access to serial line status and control signals of serial ports. This topic is covered in the previous section Checking for Special Application Requirements. If this is a requirement of the application, you will need to use a serial server that supports the COM Port Control protocol.

3.4 Monitoring Serial/IP COM Port Activity

The Serial/IP Activity display summarizes the status of all Serial/IP COM ports. To see this display, click on the Port Monitor button in the Serial/IP Control Panel. Alternatively, right-click on the Serial/IP icon in the Windows system tray and choose **Port Monitor**.



To the right of each COM label is a space that contains the status indicators. The first two indicators always appear when an application has opened a Serial/IP COM port:

- **TD** is "lit" when transmitting data to the serial server.
- **RD** is "lit" when receiving data from the serial server.

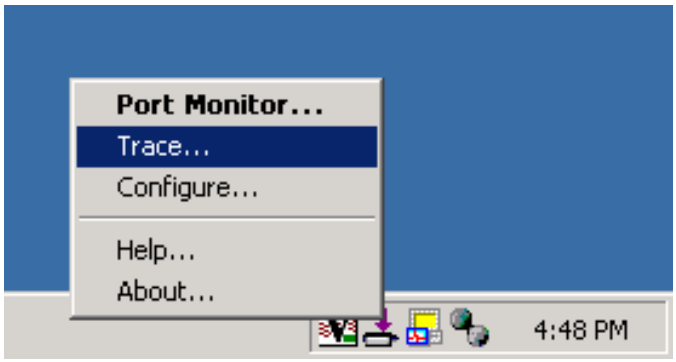
Three more indicators appear only if the serial server supports COM Port Control:

- **TR** (DTR) is the signal to the serial port that the PC application has opened the Serial/IP COM port. The most frequent use of DTR is to signal the serial server to disconnect by lowering the DTR line.
- **DR** (DSR) is the signal to the PC application that a serial device is connected to the serial server and ready to communicate.
- **CD** (DCD) is the signal to the PC application from a device connected to the serial server that it has successfully negotiated a connection with another device.

These indicators only appear when an application has opened a Serial/IP COM port. At other times, the indicator area is blank.

3.5 Tracing Serial/IP COM Port Data

The Serial/IP Trace window can be invaluable in solving difficult configuration problems by showing all interactions between the client application and the remote device. The data displayed can be saved to a file to be examined off-line or sent to others for analysis.



To see the Trace display, right-click the Serial/IP icon in the Windows system tray and choose **Trace**.

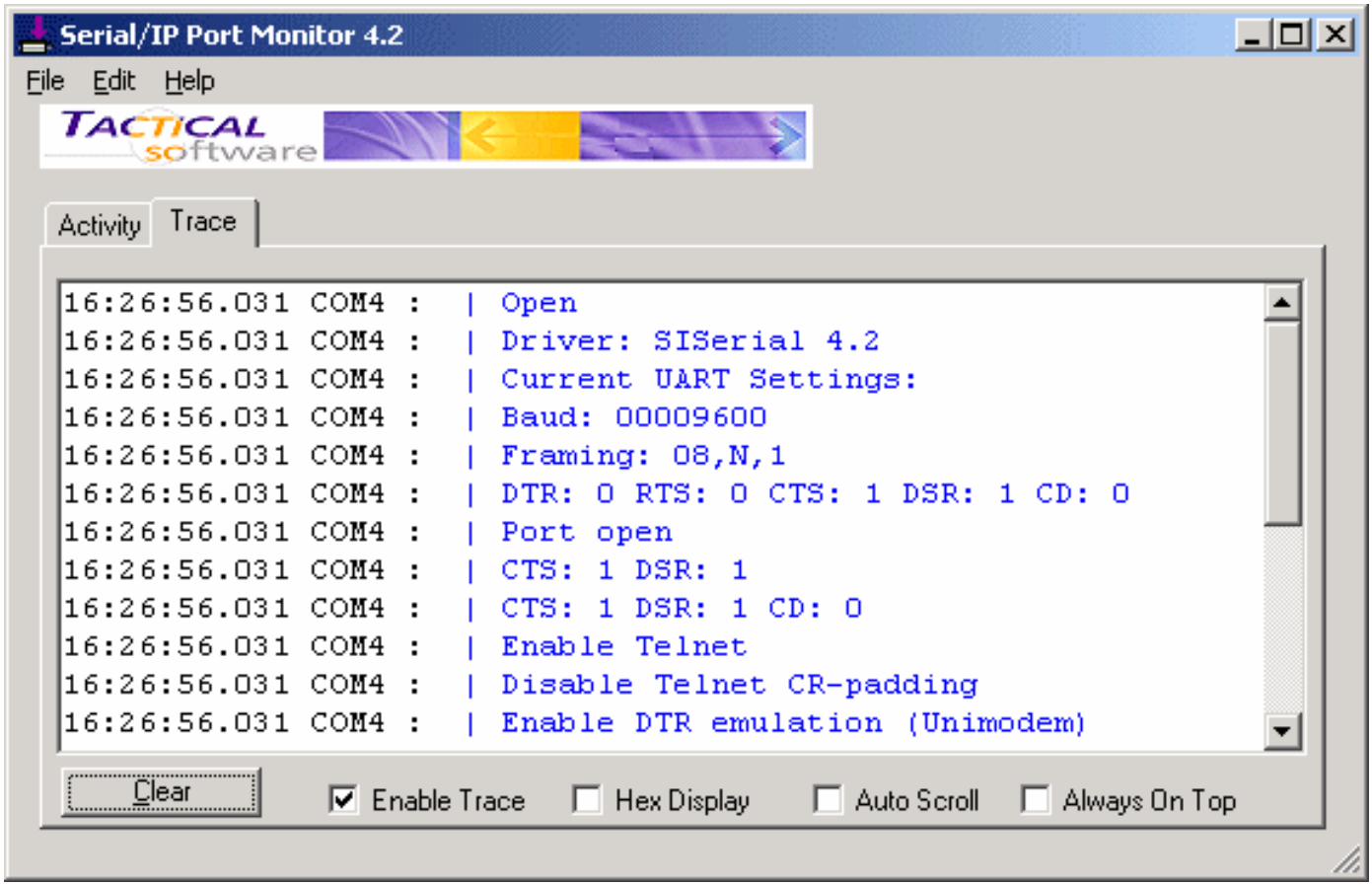
To begin collecting and displaying trace data, check the **Enable Trace** box at the bottom of the window.

Using Tracing

To collect trace data:

1. Log on to Windows.
2. Bring up the **Trace** window and check the **Enable Trace** checkbox.
3. Start the application that uses Serial/IP COM ports.
4. Recreate the problem condition that you are debugging.
5. Allow the Trace window to show and record activity on the Serial/IP COM ports. Activity for all Serial/IP COM Ports will appear.
6. To save the trace data for future review, use the File pull-down menu option and select "Save As." Give the file a name and directory destination. The contents of the display are saved in a *.silog binary file format. Files saved in this format can be opened later in the Serial/IP Port Monitor window with all information preserved.

You can also save files for examination in text editors, such as Windows Notepad, by first running a trace and then by selecting "Copy" from the Edit pull-down menu option. Copy places the text content into the Windows clipboard, where it can then be pasted into any text editor program.



Controls in the Trace Window

The Trace window provides the following controls:

1. **Clear** button.
   This clears the display and resets the trace data collection mechanism.

2. **Enable Trace** checkbox.
   Check this box to begin recording data in a new trace session. Be sure to check this **before** attempting to make a connection with the problem application.

3. **Hex Display** checkbox.
   Check this box to toggle the recorded data between ASCII text and hexadecimal format. The ASCII display is usually more useful.

4. **Auto Scroll** checkbox.
   Check this box to make the display scroll forward as new session data arrives in real-time.

5. **Always On Top** checkbox.
   Check this box to keep the Serial/IP Port Monitor window always on top of other open applications in Windows.

Events Displayed in the Trace Window

The Trace window displays a series of events, one event per line. Every event is tagged with the current time (shown in hour:minute:second.millisecond format), and the Serial/IP COM port where the event occurred. There are three types of events:

1. **Transmit events.**
   Shown in green and preceded by "»", these indicate that the application software transmitted data to the COM port. The remainder of the line shows the data transmitted, either in ASCII or hexadecimal format, depending upon the current display mode.

2. **Receive events.**
   Shown in red and preceded by "«", these indicate that the application software received data from the COM port. The remainder of the line shows the data received, either in ASCII or hexadecimal format, depending upon the current display mode.

3. **Control events.**
   Shown in blue and preceded by "|", these indicate non-data events. These events can include the setting of session parameters (such as Telnet); opening and closing a port; connecting to the serial server; setting a device control or status line (DTR, DSR, DCD, etc); and the configuration of baud rate and framing parameters.

   Note: The Trace window is updated only once per second to avoid introducing large changes in system timing; as a result, there may be brief delays in the display. It is OK to leave tracing enabled for long periods, though this will impose a minor performance penalty and will use up to 1 megabyte of extra memory.

Appendix A: Advanced Settings

Appendix A Table of Contents

Appendix A: Advanced Settings

A.1. Proxy Servers

A.1. Proxy Servers

Applicable Products

The following Tactical Software products support the Proxy Server feature:

- DialOut/Client Redirector
- Serial/IP Redirector
- COM/IP Redirector

In This Chapter

Appendix A: Advanced Settings

A.1. Proxy Servers

A.1.1 Introduction

The COM/IP, Serial/IP, and DialOut/Client Redirectors support TCP network connections made through proxy servers, which may be controlling access to external networks (such as the Internet) from private networks that lack transparent IP-based routing, such as NAT.

Proxy server support is built into Tactical Software Redirectors because they are drivers that run in kernel mode, while conventional proxy server support runs in user mode and is unavailable to drivers.

Tactical Software Redirectors support the following proxy protocols:

- SOCKS v5
- SOCKS v4
- HTTPS

Tactical Software Redirectors are compatible with the following proxy servers:

- Microsoft ISA (for the SOCKS protocol only)
- Apache on Linux and Windows
- Squid

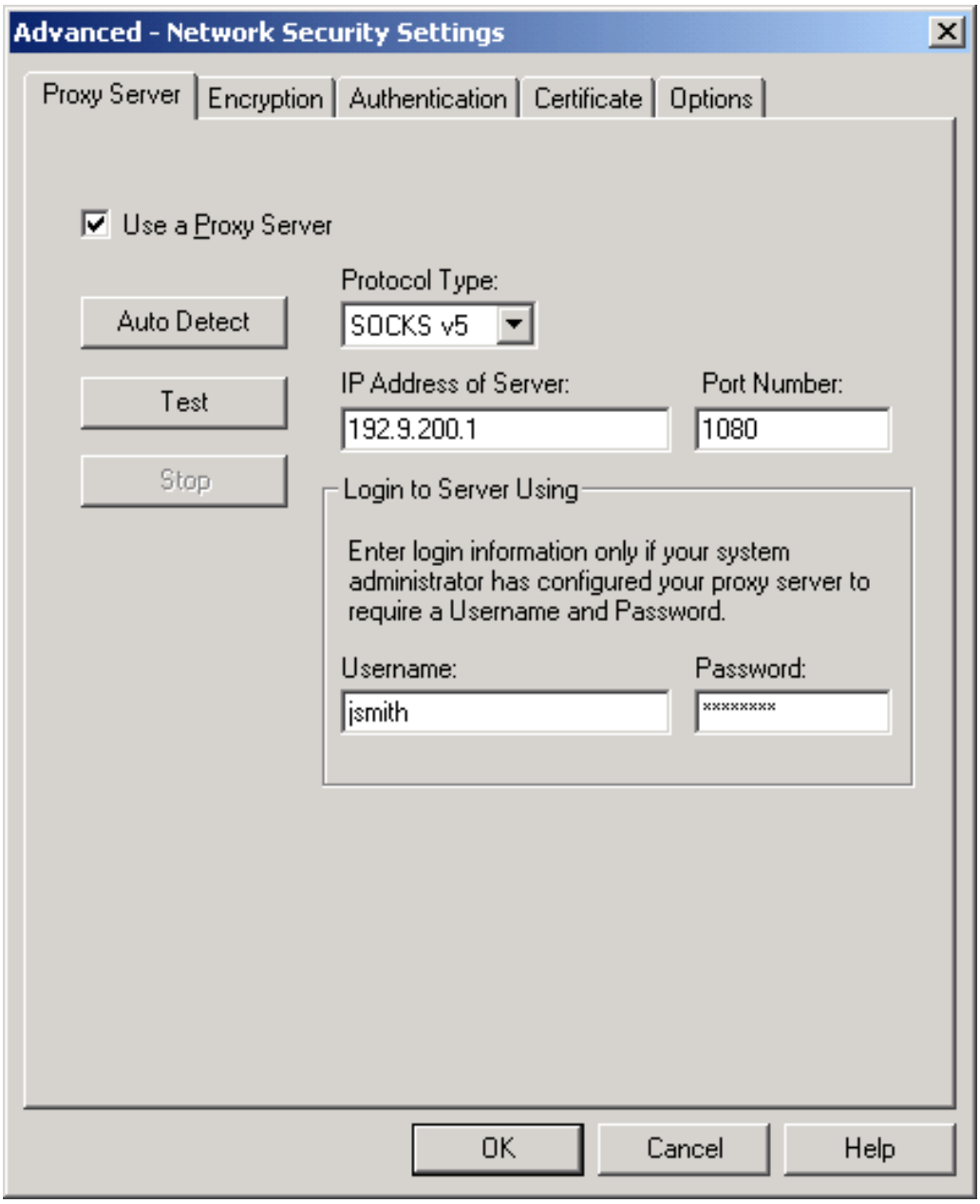
Appendix A: Advanced Settings

A.1. Proxy Servers

A.1.2 Using a Proxy Server

A Tactical Software Redirector is configured to use a proxy server as follows:

1. Select the **Advanced** button in the Tactical Software Redirector's Control Panel window.
2. Select the **Proxy Server** tab if necessary.
3. Select the checkbox **Use a Proxy Server**.
4. If the proxy server requires a login, fill in the **Username** and **Password** fields.
5. The **Protocol Type**, **IP Address**, and **Port Number** are required fields. If you wish to have the software automatically locate the proxy server and sense the correct settings, select the **Auto Detect** button. If the operation is successful, it will fill in the settings for Protocol, IP Address, and Port Number.
6. Select the **Test** button to use the settings to contact the proxy server.
7. Select the **OK** button to apply the settings and return to the Control Panel.



Notes

If the **IP Address of Server** is entered manually, a DNS name can be used.

The **Auto Detect** and **Test** operations will typically take less than 10 seconds. If either of these operations appear to be hung, use **Stop** button to terminate them.

The **Username** and **Password** credentials will be transmitted to the proxy server as plaintext. A **Test** operation will display an error dialog if these credentials are required by the proxy server but not yet entered.

If the proxy server requires a login, the **Auto Detect** and **Test** operations will fail if **Username** and **Password** have not been provided.

If a proxy server is being used, related information will appear in the **Trace** display.

Technical Notes on the Auto Detect Feature

The Auto Detect operation uses the following algorithm:

1. A DNS lookup of “wpad” is attempted.

2. For each IP address returned by the DNS lookup, attempt protocol detection for each supported protocol (SOCKS v5, SOCKS v4, in that order). This is done by attempting a TCP connection to the IANA-defined port for each protocol, then (if successful) attempting proxy operations.

3. If the DNS lookup came back empty, or if no proxy server protocol has been detected, attempt protocol detection on each default gateway in the routing table.

4. If no proxy server protocol is detected, the **Auto Detect** operation is terminated and no settings are automatically entered.

Appendix A: Advanced Settings

A.1.3 Troubleshooting

If operation with a proxy server is not working as expected, the following resources may be of help:

- Verify with the "ping" command (in a DOS prompt window) that the proxy server responds at the expected IP address.
- Use the **Test** button. This conducts additional checks that can not be readily performed otherwise.
- The Frequently Asked Questions (FAQ) on the Tactical Software web site are searchable and address common technical support issues.
- The Technical Notes on the Tactical Software web site may provide relevant supplemental information.
- The Application Notes on the Tactical Software web site may describe the use of SSL/TLS Security features in applications similar to your own.
- The FAQ section of the Tactical Software web site contains a revision history for this product.
- For technical support, please refer to the support information provided by your supplier and the support section of the "readme.txt" file included with the Tactical Software product. This file is displayed by the setup program and is also placed in the installation folder.

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2. SSL/TLS Security

Applicable Products

All Tactical Software products support the SSL/TSL Security feature as an option.

In This Chapter

Configuring the Authentication Feature
Being sure the software is communicating with the expected destination.

Configuring the Certificate Feature
Offering proof of the identity of the local computer.

Troubleshooting
How to proceed if using SSL/TLS Security is not trouble-free.

COM/IP AT Commands
Configuring the SSL/TLS Security features using commands to the COM/IP software modem.

Certificate Authorities
The built-in CA's that are included and used by default.

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.1 Introduction

Tactical Software redirectors use TCP/IP network connections to carry data that PC applications read and write on COM ports. By using a network, redirectors introduce two security concerns:

1. How can the identity of both ends of a connection be guaranteed?
2. Is the data in the transmission secure?

In many cases, these issues are sufficiently addressed by the design of the local area network and restricted physical access to systems and communications equipment.

To meet the greater security requirements of some applications, Tactical Software offers a SSL/TLS Security option that adds SSL/TLS encryption and certificate features to Tactical products. With the SSL/TLS Security option, Tactical products gain data security with encryption and authentication with certificates, matching or exceeding the level of security offered by conventional modem or serial connections.

The SSL/TLS Security features are available only by the use of special Tactical license keys that enable built-in encryption software, which is otherwise not functional in the Tactical product. Once enabled, settings controlling the encryption features become available in the Tactical product's Control Panel and its Advanced Settings window. In the case of the COM/IP Redirector, its built-in software modem also can configure the security-related settings using AT commands.

Important Note Regarding Export

Tactical Software products with the SSL/TLS Security features enabled are subject to regulations of the U.S. government and other authorities. Export or re-export of such products is prohibited without the permission of Tactical Software.

Technical Knowledge Assumed in this Chapter

This User Guide does not attempt to describe security concepts and technology in detail. For users needing this information, Tactical recommends the book *SSL and TLS: Designing and Building Secure Systems* by Eric Rescorla (ISBN 0201615983), a respected tutorial and reference that is widely used in the industry.

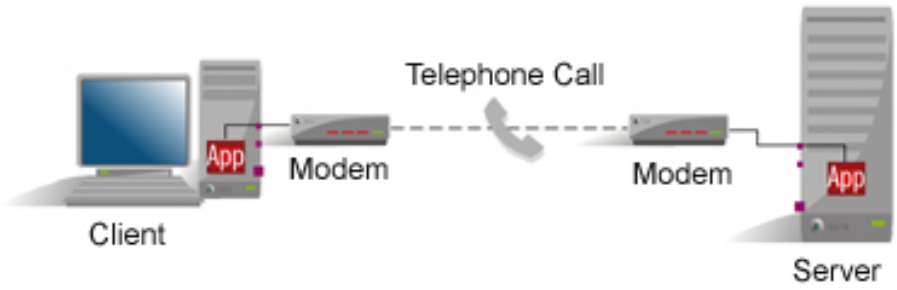
Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.2 Security Issues in Tactical Software Products

Background

A PC application making a modem connection relies on the telephone line for security, as depicted in the following diagram:



The modem connection is considered secure in three respects:

1. Data security is provided by the telephone line. Unauthorized wiretapping is considered difficult or unlikely.

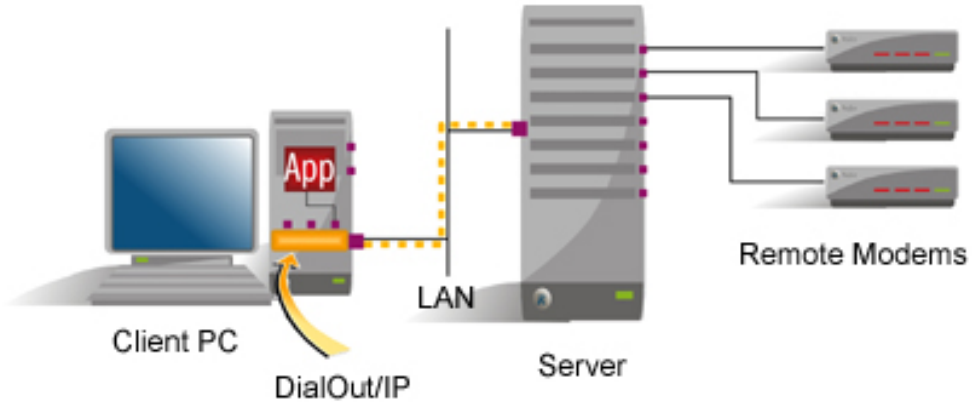
2. The identity of the destination is determined by the telephone number dialed to reach it. It is assumed that the telephone company always connects to the number dialed.

3. The server receiving the call could verify the identity of the caller by caller ID information or by a call-back. Neither of these measures is common in real-world applications.

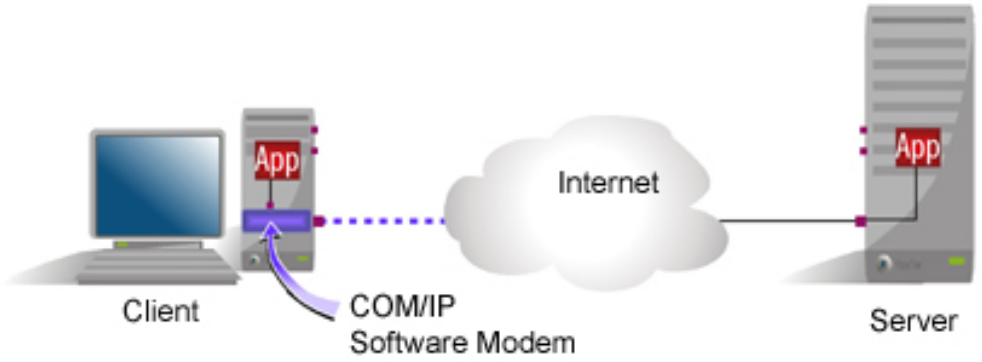
A PC application using a serial connection is even simpler, relying on correct physical wiring to secure the data and establish the identities of the connection endpoints.

Security Issues Introduced by Tactical Software Redirectors

The Tactical Software dial-out and serial redirectors (DialOut/IP, DialOut/EZ, DialOut/Client, and Serial/IP) use a TCP/IP connection to the server that makes the actual modem/serial connection, as illustrated below:



The Tactical Software COM/IP Redirector also introduces a TCP/IP connection, by entirely replacing the modem call with a network connection:



Consequently, three security issues arise:

1. Is data secure between the PC to the server? Network connections can be much easier to "tap" than a telephone line, especially if traversing the Internet or unsecured segments of a corporate network.

2. Is the PC able to verify the identity of the server to which it is connecting?

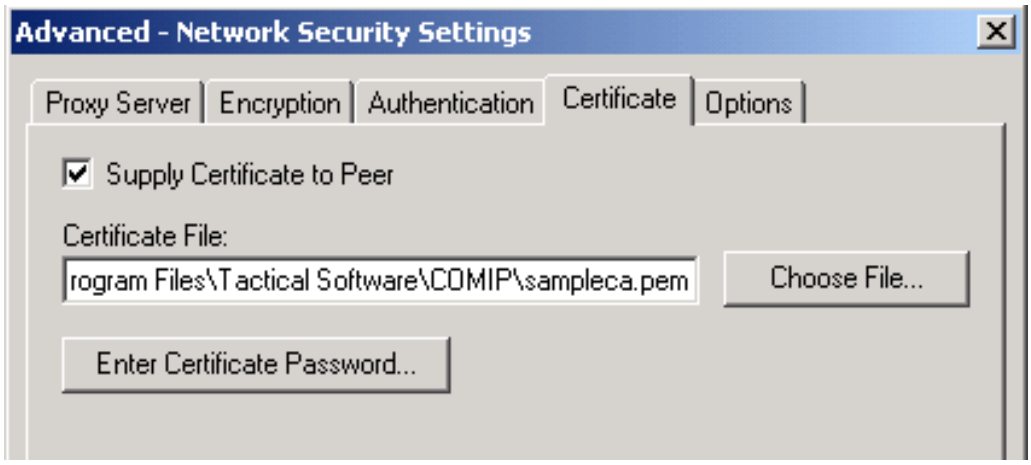
3. Can the PC identify itself to the server?

The SSL/TLS Security option in Tactical Software Redirectors addresses these questions with SSL/TLS encryption (for data security) and SSL/TLS certificates (to verify the identity of computers).

1. In the Tactical Software product Control Panel, click the **Advanced** button to get the **Advanced Settings** dialog window.

2. Select the **Certificate** tab.

3. Select the checkbox **Supply Certificate to Peer**. This enables the other controls in the window.



4. In the **Certificate File** field, enter the filename of a certificate file or use **Choose File** to specify a file.

5. Click **Enter Certificate Password** to provide the password for the certificate in the file. To preserve this password for future sessions, select **Save Password**.

6. Click **OK** to make the changes effective.

For the COM/IP Redirector, the Certificate settings can be configured by the PC application using AT commands.

Saving the Certificate Password

If the Password value is saved, it is placed in the Windows registry in encrypted form. if not saved, the Password is not written to the registry and will be in effect until the Windows operating system is rebooted, after which the Tactical Software product will not be able to use the certificate until the Password is manually entered again.

The Sample Certificate

A sample certificate file named "samplecert.pem" is included with the Tactical Software product and is located in the same folder as the product software. The password for this certificate is "password".

WARNING: The sample certificate should be used for testing only. Using a publicly-distributed certificate leaves a session vulnerable to some types of man-in-the-middle attacks. It is strongly recommended that the sample certificate never be used in a production environment.

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.3 SSL/TLS Security Features

The SSL/TLS Security option adds three features to a Tactical Software product:

- **Encryption** secures the data stream with a cipher and cipher strength that is negotiated when the connection is established. The ciphers and strengths that can be used for connections are user-configurable in the Control Panel. Available ciphers are RC2, RC4, DES, 3DES, and AES. Cipher strengths range from 40 bits to 256 bits. The maximum cipher strength is subject to an upper limit enforced by the product license key provided by the supplier of the software license. Not all ciphers work with all strengths, and this is automatically managed by the software when it negotiates the network connection.
- **Authentication** checks the identify of the peer (the "other end" of the network connection) by validating the certificate supplied by the peer. The specific checks applied to the certificate are user-configurable in the Control Panel. Additionally, the certificate authorities (CA's) used to validate the certificate can either come from a set of built-in CA's (which is the set of CA's used by Internet Explorer 6 and other browsers) or from a user-supplied CA file. Appendix B provides a list of the built-in CA's.
- **Certificate** allows the software to provide a certificate to the network connection peer. An unsecure sample certificate is included with the Tactical Software product. The certificate used in an actual application must be supplied in a user-specified file.

Usage

SSL/TLS Security features are used for various purposes, depending on the Tactical Software product:

Product	Encryption	Authentication	Certificate

COM/IP Redirector	Secure the data stream in the connection to any TCP/IP network peer	Check identity of any TCP/IP connection peer when initiating a connection	Provide private key and prove identity when receiving a connection
DialOut/IP, DialOut/EZ, and Serial/IP Redirectors	Secure the data stream between the user PC and the modem server or serial server	Check the identify of the modem server or serial server	Prove identity by supplying own certificate on demand
DialOut/Server modem server		Check the identity of a user PC requesting a connection	Provide private key and prove identity when receiving a connection

FAQ's

What implementation of SSL/TLS is used?

Security features are implemented with the OpenSSL toolkit 0.9.7b, an implementation of SSL/TLS that has an excellent track record for quality, reliability, and performance.

Why is encryption provided with SSL/TLS instead of SSH?

Tactical Software currently supports SSL/TLS instead of SSH for several reasons. First, widely available SSL/TLS accelerators can be used as a transparent front-end for devices and applications that do not themselves support encryption. Second, as a Secure SHell, SSH has login-related functions that are not usually needed or desired by many Tactical customers. Third, SSH is a tunneling protocol that is potentially less secure because another application could use the SSH connection for unintended purposes.

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.4 What You Need to Get Started

Before you use the SSL/TLS Security features, you will need the following:

1. **Administrator privileges** if the Tactical Software product you are using was installed in "Administrator-Only Mode".

2. A Tactical Software **product license key** that enables the SSL/TLS Security features.

   Note: Unless otherwise arranged with the supplier of the Tactical Software product, evaluation licenses do not enable the SSL/TLS Security features.

3. Optionally, a **certificate authority file** if you use the Authentication feature and will not use the built-in certificate authority file that is provided with the Tactical Software product.

4. A **certificate file** if you are going to use the Certificate feature in an actual application.

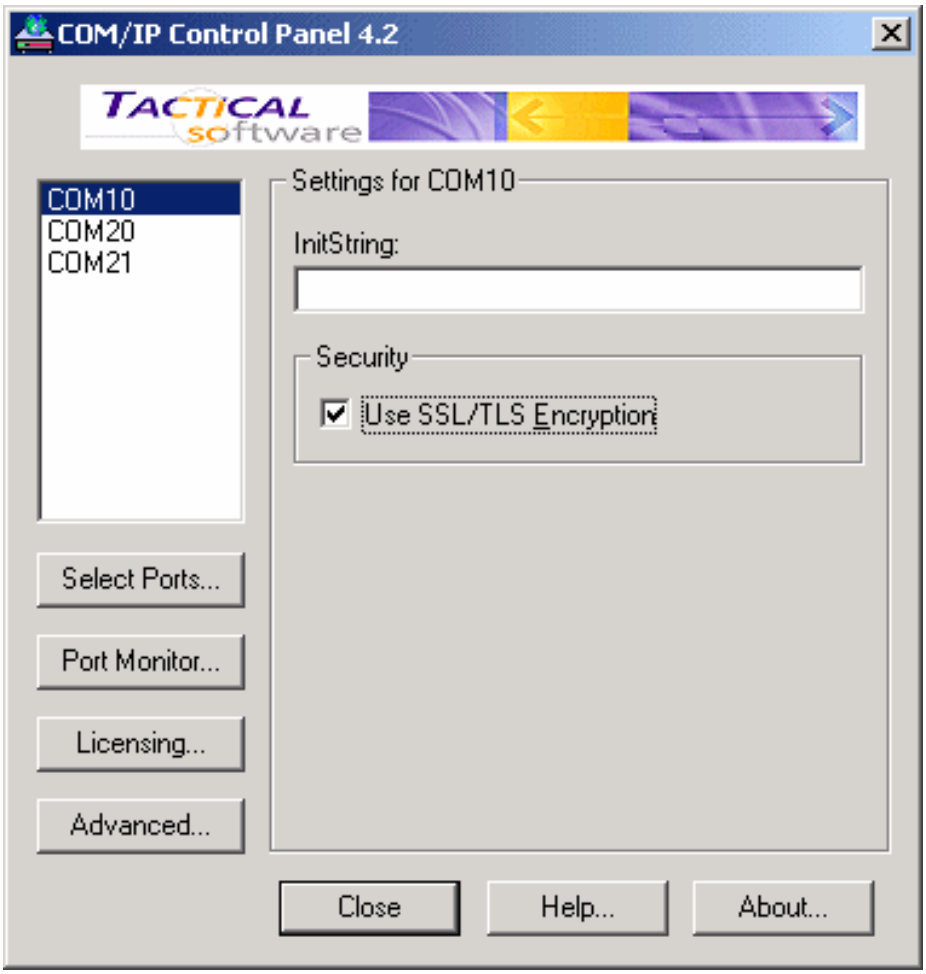
Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.5 Enabling SSL/TLS Security Features

Verifying Availability of the SSL/TLS Security Option

The SSL/TLS Security option is available only if the Tactical Software product has been installed with a license key that enables it.



1. Enter the Control Panel for the Tactical Software product.
2. If the checkbox named **Enable SSL/TLS Encryption** is missing, the license key used to install this copy of the Tactical Software product does not enable the SSL/TLS Security features. To remedy this:
    - Obtain a license key that does enable the SSL/TLS Security features.
    - Use the **Licensing** button in the Control Panel to update the license key.

Using SSL/TLS Security Features

For each COM port that will use SSL/TLS Security features:

1. Select the COM port.
2. Select the **Enable SSL/TLS Encryption** checkbox.

NOTE: This is a per-COM-port setting.

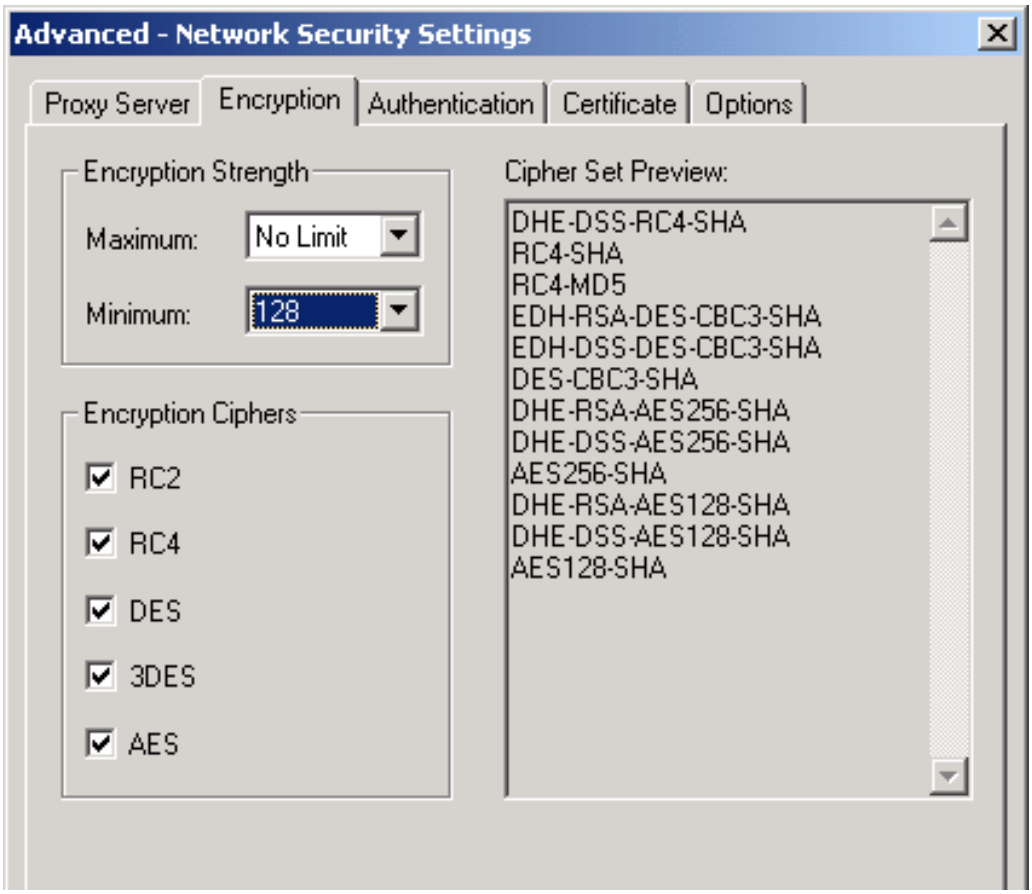
Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.6 Configuring the Encryption Feature

The **Encryption** feature causes the Tactical Software product to negotiate an encrypted connection using one of the available ciphers at the highest available cipher strength. Configuration of the Encryption feature is global, equally affecting all COM ports that have selected Enable SSL/TLS Encryption in the Control Panel.

1. In the Control Panel, click the **Advanced** button to get the **Advanced Settings** dialog window.
2. Select the **Encryption** tab.
3. In the **Encryption Strength** group, select **Minimum** and **Maximum** strengths in their respective dropdown lists. The highest value available for Maximum is limited by the product license key used to install this copy of the software.
4. In the **Encryption Ciphers** group, select one or more cipher suites.



5. Verify that at least one cipher appears in the **Cipher Set Preview** display. These are the available cipher sets that the software can use when negotiating a network connection. Their order of appearance is not significant.

The cipher being used in a connection is displayed in the Port Monitor window.

Available Cipher Sets

Following are all of the cipher sets that the Encryption feature may use:

DHE-RSA-AES256-SHA
DHE-DSS-AES256-SHA
AES128-SHA
EDH-RSA-DES-CBC3-SHA
EDH-DSS-DES-CBC3-SHA
DES-CBC3-SHA
EXP1024-DHE-DSS-DES-CBC-SHA
EXP1024-DES-CBC-SHA
EDH-RSA-DES-CBC-SHA
EXP-EDH-RSA-DES-CBC-SHA
EDH-DSS-DES-CBC-SHA
EXP-EDH-DSS-DES-CBC-SHA
DES-CBC-SHA
EXP-DES-CBC-SHA
EXP1024-RC2-CBC-MD5
EXP-RC2-CBC-MD5
DHE-DSS-RC4-SHA
EXP1024-DHE-DSS-RC4-SHA
EXP1024-RC4-SHA
EXP1024-RC4-MD5
RC4-SHA RC4-MD5
EXP-RC4-MD5

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.7 Configuring the Authentication Feature

The **Authentication** feature causes the Tactical Software product to require and validate an SSL/TLS certificate at the beginning of a network connection. Configuration of the Authentication feature is global, equally affecting all COM ports that have selected Enable SSL/TLS Encryption in the Control Panel.

When the Authentication feature is used, it requests a certificate at the beginning of each encrypted connection. When the certificate is received, it is validated using a two-step process:

1. The contents of the certificate are inspected to ensure that it contains the expected data.
2. If the contents of the certificate meet expectations, the signature attached to the certificate must match the contents and must have been generated by a trusted Certificate Authority.

To configure the Authentication feature:

1. In the Tactical Software product Control Panel, click the **Advanced** button to get the **Advanced Settings** dialog window.

2. Select the **Authentication** tab.

3. Select the checkbox **Require Validated Certificate**. This enables the other controls in the window.

4. In the **Validate Criteria** group, select the checkbox for each certificate field that must be checked when validating a certificate.

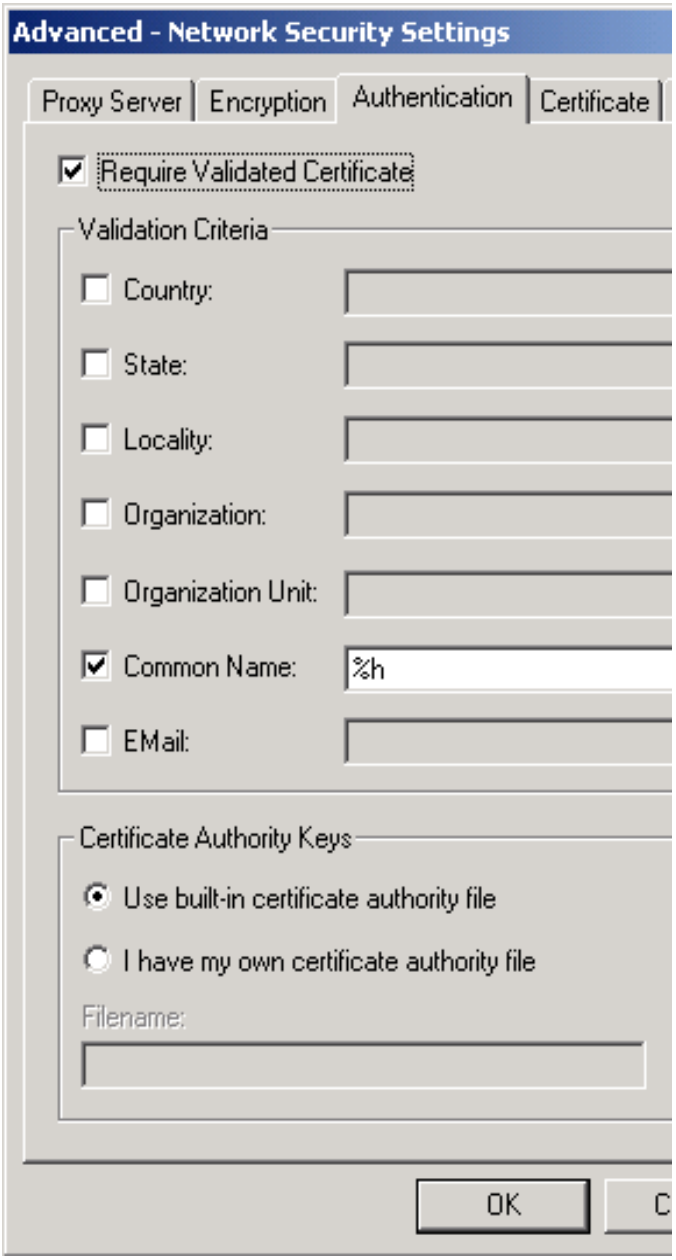
5. For each field, enter the data that the field must match.

   Entering **%h** causes a match to the hostname used to connect to the peer.

   Entering **%a** causes a match to the IP address of the peer.

   Otherwise, the match is to the entry as literal text.

   Note: The %h and %a entries are typically only useful for matching the Common Name field.



6. In the **Certificate Authority Keys** group, select the radio button that corresponds to the source of the CA keys to be used. Built-in CA keys are those used by Internet Explorer 6, and are summarized in Appendix B. Alternatively, a file containing CA keys can be specified in **Filename**. A sample CA file named "sampleca.pem" is included with the software and is located in the software installation folder.

7. Click **OK** to make the changes effective.

For the COM/IP Redirector, the Authentication settings can be configured by the PC application using AT commands.

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.8 Configuring the Certificate Feature

The **Certificate** feature lets the Tactical Software product use a user-supplied certificate. Configuration of the Certificate feature is global, equally affecting all COM ports that have selected Enable SSL/TLS Encryption in the Control Panel.

A certificate is mandatory in two situations:

1. If the software is initiating a connection, the network connection peer may request a certificate for authentication purposes.
2. If the software is accepting a connection, it extracts its private key from the certificate when an incoming connection request occurs.

The Certificate feature is mainly useful for two of the Tactical Software products:

- The COM/IP Redirector must use the Certificate feature if receiving incoming connections.
- DialOut/Server modem server must use the Certificate feature to receive incoming connections from any Tactical Software redirector that is using encryption.

To configure the Certificate feature:

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.9 Troubleshooting

If problems are encountered with SSL/TLS Security features, the following resources may be of help:

- The Activity display in the Port Monitor window shows the cipher and strength being used for encrypted connections.
- The Trace display in the Port Monitor windows shows additional information related to SSL/TLS when a connection is encrypted.
- The Frequently Asked Questions (FAQ) on the Tactical Software web site are searchable and address common technical support issues.
- The Technical Notes on the Tactical Software web site may provide relevant supplemental information.
- The Application Notes on the Tactical Software web site may describe the use of SSL/TLS Security features in applications similar to your own.
- The FAQ section of the Tactical Software web site contains a revision history for the product.
- For technical support, please refer to the support information provided by your supplier and the support section of the "readme.txt" file included with the Tactical Software product. This file is displayed by the setup program and is also placed in the installation folder.

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.10 COM/IP AT Commands

In the COM/IP Redirector, the settings for the SSL/TLS Security features can be modified programmatically by issuing "AT+S" commands to the COM/IP Redirector's AT command processor. For each COM port, settings are initially those set in the Control Panel, then subject to change for each COM port via AT commands. Changes remain in effect separately for each COM port until the software modem for that port is reset or the next time the Windows operating system is rebooted, at which time the settings currently applied in the Control Panel are in effect.

The **AT+S** command has three modes:

- Set parameters: **AT+S<*cmd*>=<*value*>**
- Query current parameters: **AT+S<*cmd*>?**
- Query allowable settings: **AT+S<*cmd*>=?**

As detailed later in this section, the semantics of the last mode are context-dependent.

There are six commands associated with **+S**:

- Encryption Protocol: **AT+SPROTO**
- Cipher Set: **AT+SCS**
- Negotiated Cipher Set: **AT+SNS**
- Certificate Authentication: **AT+SCA<*field*>**
- Certificate Presentation: **AT+SCP**
- Certificate Password: **AT+SCPW**

None of these commands have any effect on the settings saved in the GUI. Furthermore, the next time the COM/IP modem is reset (via ATZ, AT&F, or a reboot), the settings specified by these commands revert to the settings specified in the Control Panel.

Encryption Protocol (AT+SPROTO)

This command allows the application to query and set what encryption protocol is to be used, currently either TCP (i.e., no encryption) or TLS. The following example sets encryption to TLS then turns it back off:

```
AT+SPROTO=TLS
OK
AT+SPROTO=TCP
OK
```

The application may also query the current protocol in effect, for example:

```
AT+SPROTO?
TLS
```

The application may also query the list of currently supported protocols, for example:

```
AT+SPROTO=?
TCP,TLS
OK

AT+SPROTO=?
RC4-MD5(128)
OK
```

Cipher Set (AT+SCS)

This command allows the application to query and set the list of ciphers to be used in the next SSL/TLS negotiation. It is of the format:

```
AT+SCS=<min-key-length>,<max-key-length>,
        <cipher1>,<cipher2>,...,<cipher n>
```

The parameters accepted are as follows:

min-key-length: minimum cipher key strength to be negotiated. Values are 40, 56, 64, 128, or 168.

max-key-length: maximum cipher key strength to be negotiated. Values are 40, 56, 64, 128, 168, or zero. Zero denotes no upper limit.

cipher1-n: the list of cipher families to be negotiated. Only those ciphers specified will be included in the cipher set. Ciphers supported are: RC2, RC4, DES, 3DES, and AES.

For example, to specify that 56-128 bit ciphers from RC4 and DES may be negotiated, the application sends the

following command:

```
AT+SCS=56,128,RC4,DES
```

Entries may be omitted from the list, in which case the defaults from the GUI are used. For example, to set 40-56 bit ciphers using the current families specified in the GUI, the application sends the following command:

```
AT+SCS=40,56
```

To use the current cipher strengths from the GUI, but only use RC4, the application sends the following command:

```
AT+SCS=,,RC4
```

The application may query the current settings using the command below, which shows the output when the key lengths are restricted to 40-56 for RC2 and RC4:

```
AT+SCS?
40,56,RC2,RC4
OK
```

The application may query the final cipher set using the command below, which shows the output when the key length are restricted to 40-56 for RC2 and RC4:

```
AT+SCS=?
EXP1024-RC2-CBC-MD5
EXP1024-DHE-DSS-RC4-SHA
EXP1024-RC4-SHA
EXP1024-RC4-MD5
EXP-RC2-CBC-MD5
EXP-RC2-CBC-MD5
EXP-RC4-MD5
EXP-ADH-RC4-MD5
EXP-RC4-MD5
OK
```

Negotiated Cipher Set (AT+SNS)

This command may be used in only one mode: to query the cipher and strength negotiated on the last SSL/TLS session. For example, for a session that negotiated 128-bit RC4:

```
AT+SNS?
RC4-MD5(128)
OK
```

If the SSL/TLS Security features are not enabled in the software or there has not been any SSL/TLS session

negotiated on the last TCP connection, the command processor simply emits “OK”.

Certificate Required (AT+SCR)

This command allows the application to set and query whether the remote endpoint must present a valid certificate at the beginning of the SSL/TLS session. It is of the format:

```
AT+SCR=[0,1]
```

If the application specifies 0, no certificate checking is performed. If the application specifies 1, then certificate checking is performed in accordance with the following two commands. If the application specifies no value, the current setting returns to the default as specified in the Control Panel.

The application may also query the current status of certificate checking, for example:

```
AT+SCR?
1
OK
```

The application may also query the range of values, for example:

```
AT+SCR=?
0,1
OK
```

Certificate Authority Keys (AT+SCK)

This command allows the application to specify the path to the file that contains the public keys of the Certificate Authority that is to be used to authenticate a certificate. It is of the format:

```
AT+SCK=<fully-qualified-filename>
```

The *<fully-qualified-filename>* specifies the file that contains the certificate keys (in PEM format). If the specified file does not exist or is not accessible, then “ERROR” is output and the original value is retained. If no file is specified, the setting refers to the default as specified in the GUI.

The application may query the current setting by using the command in the following example:

```
AT+SCK?
C:\Program Files\Tactical Software\COMIP\sampleca.pem
OK
```

Certificate Authentication (AT+SCA)

This command allows the application to set and query the certificate validation parameters. It is of the format:

```
AT+SCA<field>=<matching-text>
```

The <*field*> is the field within the certificate, and may be one of the following values:

C: Country

S: State

L: Locality

O: Organization

OU: Organizational Unit

CN: Common Name

EM: Email Address

The <*matching-text*> is a literal string with the addition of three tokens: *%h* which means the hostname of the remote peer, %i which means the IP Address of the remote peer. If the <*matching-text*> is omitted, then the field is not validated (note that once a field is set via this command, the only way to revert the setting back to the GUI specification is to reset the modem via ATZ or AT&F, which reverts *all* of the settings). For example, to validate the Organization as “Tactical Software”, and the Common Name as the hostname of the server, the application sends the following commands:

```
AT+SCAO=Tactical Software
OK
AT+SCACN=%h
OK
```

The application may query the current setting of each field, as shown in the example below:

```
AT+SCAO?
Tactical Software
OK
AT+SCACN?
%h
OK
```

The application may also query the contents of each field of the certificate presented from the peer in the last SSL/TLS session. For example:

```
AT+SCEM=?
admin@tacticalsoftware.com
OK
AT+SCACN=?
server.tacticalsoftware.com
```

OK

Certificate Presentation (AT+SCP)

This command allows the application to set and query the filename of the SSL/TLS certificate. It is of the format:

AT+SCP=<*fully-qualified-filename*>

The <*fully-qualified-filename*> specifies the file that contains the certificate (in PEM format). If any passwords for the private key have been specified previously, they are cleared. If no file is specified, then no certificate will be made available to the remote peer. If the specified file does not exist or is not accessible, then "ERROR" is output and the original value is retained.

The application may query the current setting by using the command in the following example:

AT+SCP?
C:\Program Files\Tactical Software\COMIP\sample.pem
OK

Certificate Password (AT+SCPW)

This command allows the application to specify a password to decrypt the private key of the certificate specified in the AT+SCP command above. It is of the format:

AT+SCPW=<*password*>

If the application omits the password, then any saved passwords for the certificate are cleared, for example:

AT+SCPW=
OK

If the application specifies a password, it is used to decrypt the private key of the certificate. If the password specified is incorrect, "ERROR" is output and any previous password cleared. For example:

AT+SCPW=bad-password
ERROR
AT+SCPW=raining-cats-and-dogs
OK

The application may only query the *status* of the password, which may return one of the following status codes:

VALID: the password has been specified and is valid for the current certificate.

INVALID: a password has not been specified and the current certificate requires one.

NONE: there is no certificate currently specified.

For example:

```
AT+SCPW?
NONE
OK
AT+SCP=c:\sample.pem
OK
AT+SCPW?
INVALID
OK
AT+SCPW=raining-cats-and-dogs
OK
AT+SCPW?
VALID
OK
```

Appendix A: Advanced Settings

A.2. SSL/TLS Security

A.2.11 Certificate Authorities

The following organizations are the certificate authorities in the file "ca.pem" that is used by default in the Authentication option:

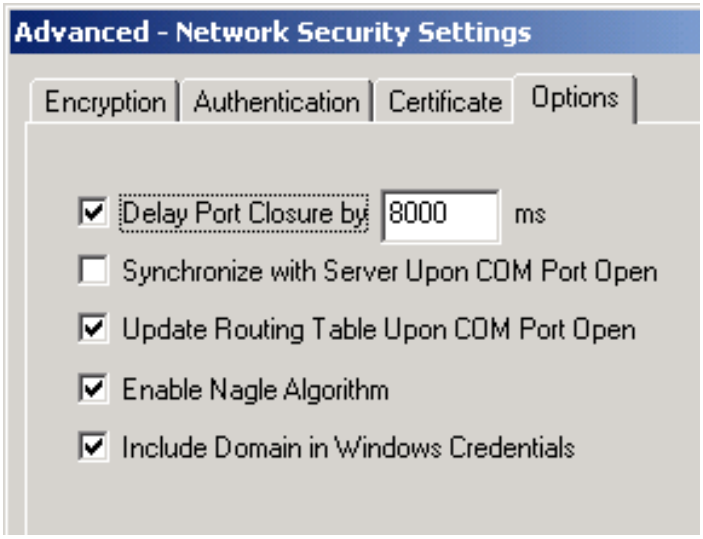
ABA.ECOM, Inc.
Administracion Nacional De Correos
Belgacom
C&W HKT SecureNet CA Class B
C&W HKT SecureNet CA SGC Root
Certiposte
Certisign Certificadora Digital Ltda.
Certplus
Colegio Nacional de Correduria Publica Mexicana, A.C.
Deutsche Telekom AG
Digital Signature Trust Co.
EUnet International
Entrust.net
Equifax
Equifax Secure Inc.
FNMT
First Data Digital Certificates Inc.
Fundacion FESTE
GTE Corporation
GlobalSign nv-sa
IPS Seguridad CA
Japan Certification Services, Inc.
NetLock Halozatbiztonsagi Kft.
PTT Post
RSA Data Security, Inc.

SIA S.p.A.
Saunalahden Serveri
SecureNet
Swisskey AG
TC TrustCenter for Security in Data Networks GmbH
Thawte Consulting
The USERTRUST Network
ValiCert, Inc.
VeriSign, Inc.
ViaCode
Xcert EZ by DST

Appendix A: Advanced Settings

A.3. Options

A.3. Options



The **Options** tab of the **Advanced Settings** window provides control of infrequently used settings. This tab is present only in the redirector products, and only the applicable settings appear in each product.

Delay COM Port Closure • All Redirectors

Products: All redirectors.

Default value: 8000 (8 seconds)

This setting changes the number of milliseconds that the COM port will be considered open after an application closes it. This feature minimizes the effect of a COM port being "handed off" between two processes.

For the DialOut and Serial/IP Redirectors, the connection to the modem or serial port on the server is not disconnected until the specified amount of time has elapsed after the COM port is closed. Similarly, for the COM/IP Redirector, any active network connections are not dropped until the delay occurs.

Update Routing Table Upon COM Port Open

Products: All redirectors except COM/IP.

Default setting: Enabled.

When enabled, the product adds a host route to the IP Address of the server (and to the IP Address of the License Manager if a Site Edition) each time a COM port is opened. This action helps ensure that Dial-Up Networking does not interfere with network connections of the redirector.

Enable Nagle Algorithm

Products: All redirectors except COM/IP.

Default setting: Enabled.

When enabled, the redirector uses the Nagle algorithm to coalesce small TCP/IP packets in the connection to the server. This incurs a minor latency impact on the data stream, which is irrelevant to nearly all applications.

Include Domain in Windows Credentials

Products: All redirectors except COM/IP and DialOut/Client.

Default setting: Enabled.

When enabled, the current domain is pre-pended to the username sent as a result of "Use Windows Credentials".

Synchronize with Server Upon COM Port Open

Products: All redirectors except COM/IP.

Default setting: Enabled for the Serial/IP Redirector on Windows NT/2000/XP, disabled otherwise.

When enabled, the redirector defers the completion of COM port open until the server is ready to accept the data stream.

If the Redirector is unable to fully set up the connection (e.g., the TCP connection fails or the Redirect is unable to log in) then the application that opened the COM port will receive an error code from its attempt to open the COM port.

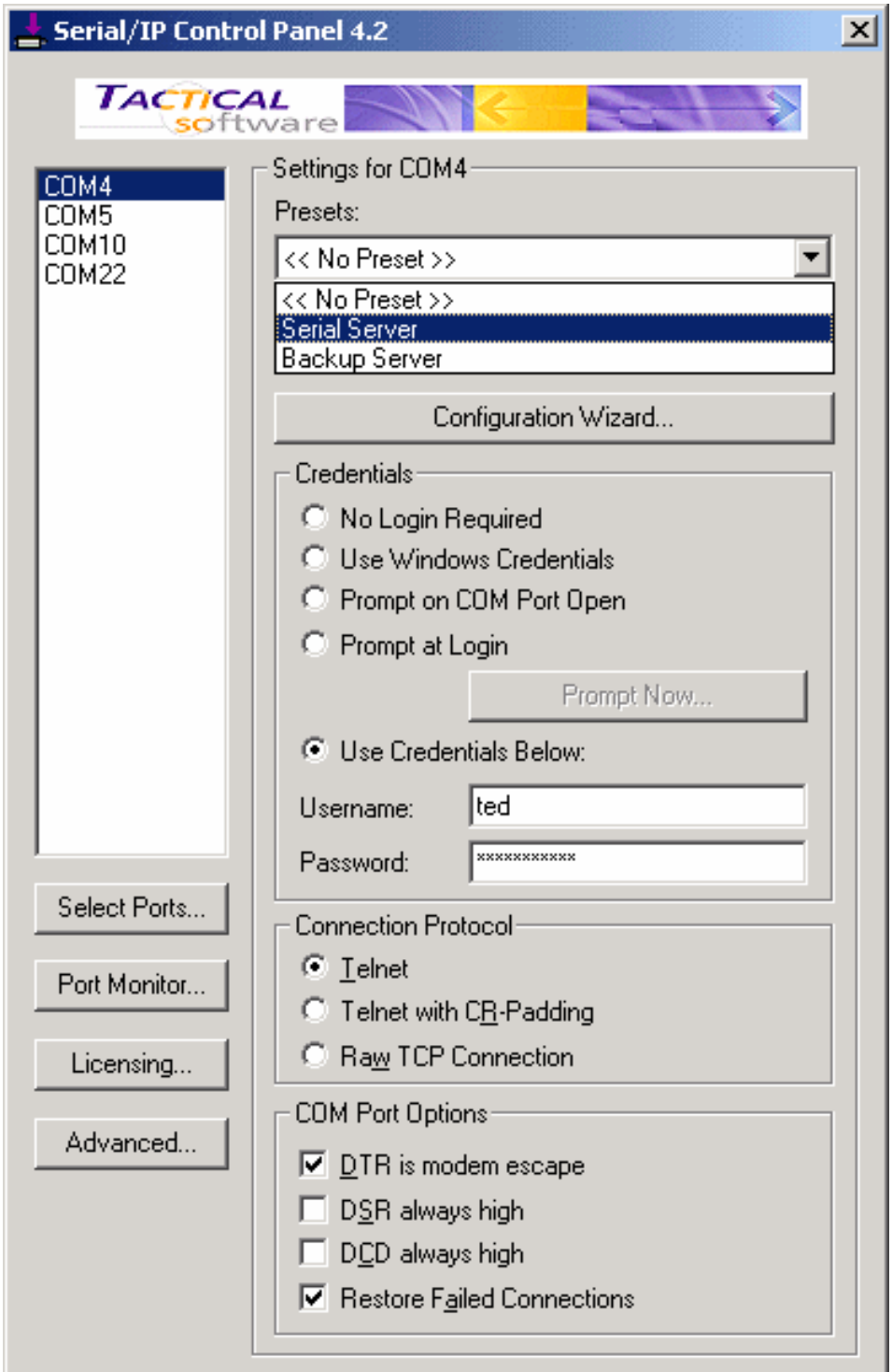
Appendix B. Using a Presets File

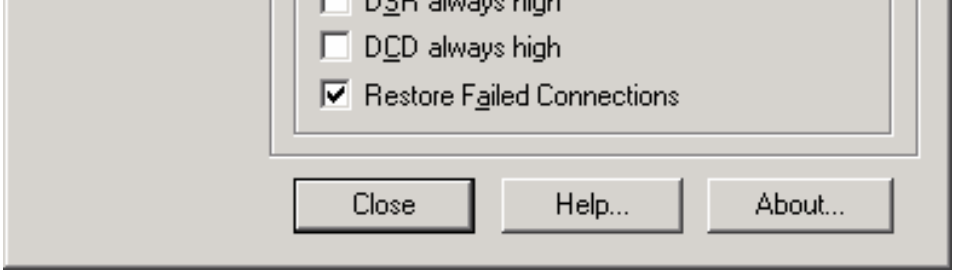
Presets are a convenient way to quickly change the settings that are associated with a COM port. Rather than retype an IP address, TCP port number and all the other configuration settings, you can keep them in a comma-delimited text file and then use an optional Presets pull-down menu to access them conveniently.

The Presets file is a text file containing the preset values. It must be named "presets.txt" and must reside in the same folder where the Serial/IP Redirector software is installed, typically:

```
C:\Program Files\Tactical Software\SerialIP\
```

Note: The Presets pull-down menu will appear in the Serial/IP Control Panel only if the presets.txt file exists.





The Preset File Format

The text file format for Serial/IP is as follows:

```
<Label>,<IP Address>,<TCP Port Number>,<Auth Option>,
        <Connection Protocol>,<COM Port Options>,...
```

Where:

Field	Value	Description
Label	Descriptive text string	Will appear in the Presets drop-down box in the Control Panel
IP Address	xxx.xxx.xxx.xxx or DNS name	Sets value of **IP Address**
TCP Port Number	A valid TCP port number	Sets value of **Port Number**
Auth Option	noauth	Selects **No Login Required**
	authwindows	Selects **Use Windows Credentials**
	authloginprompt	Selects **Prompt at Login**
	authmanual	Selects **Use Credential Below**
	authportopenprompt	Selects **Prompt on COM Port Open**
Connection Protocol	telnet	Selects **Telnet**
	crpad	Selects **Telnet with CR-Padding**
	raw	Selects **Raw TCP Connection**
COM Port Option	dun / nodun	Selects/deselects **DTR is modem escape**
	dsr / nodsr	Selects/deselects **DTR**
	dcd / nodcd	Selects/deselects **DCD always high**
	reconnect / noreconnect	Selects/deselects **Restore Failed Connections**

No extra spaces are allowed except in the **Label** field.

Preset File example:

```
Server 1,10.0.0.1,6000,noauth,telnet,nodun,nodsr,nodcd,reconnect
```

```
Server 2,10.0.0.4,6001,authmanual,raw,dun,dsr,dcd,reconnect
```

Appendix C. Configuration Wizard Messages

Status Panel

The following messages may appear in the Status panel:

Server connection failure.
The Wizard window here shows a simple communication problem. In this case, the Wizard indicates that it cannot connect to the IP address and TCP port number set for this Serial/IP COM port.

Normal progress messages.
When the Wizard's work proceeds normally, the messages summarize the interaction with the server. These messages include:

- Connected to Server
- COM Port Control Support Detected
- Telnet Protocol Detected
- Server signature: `<server name>`
- Session Completed

License mismatch messages.
If your license for Serial/IP is restricted for use with specific serial server hardware, Serial/IP will issue the following message if the license does not match the server:

> **Client not licensed for this server**
> See the About box for more information about the Serial/IP license, or contact your supplier for more information.

Communications error messages.
If the Wizard encounters a problem with the server, the Status panel will contain one of the following messages:

- Error connecting to `<server IP address>`
- Error sending data.

If such errors appear:

1. Verify that your serial server is at the IP address you expect.

2. Verify your server configuration is providing devices for access at the TCP port number you expect.
   Note: In many cases the Port Number is determined when the serial server is configured. There is no "correct" value that works for every type of serial server.

User authentication error messages.
If the Wizard encounters a problem related to user authentication (credentials), the Status panel will contain one of the following messages:

- Server expecting username
- Server expecting password
- Username and/or password incorrect
- No login/password prompts received from the server
- Server requires username/password login
- "Prompt at Login" selected but no credentials present
- "Windows Credentials" selected but no credentials present

If such errors appear, one of the following conditions is present:

1. The Configuration Wizard detects a username prompt but the Username field is empty.

2. The Configuration Wizard detects a password prompt but the Password field is empty.

3. The user entered a username and/or password, but the Configuration Wizard does not see any recognizable prompts. The most common cause is that the serial server's user authentication is not enabled; therefore the username and password should be left blank.

4. The Configuration Wizard detects the server repeatedly requesting the username and/or password. A username and/or password must be entered for a successful connection.

5. The “Prompt at Login” option was selected but no credentials were entered. Return to the Control Panel and select “Prompt Now”. Once credentials are entered, this error should not appear.

6. The “Use Windows Credentials” option was selected but no credentials were stored. The user must logoff/on after selecting to use ‘Windows Credentials” in order for the credentials to be stored.

Log Panel

If the Status panel indicates an error, the Log panel will one or more messages that provide more details. These messages include:

- Bad IP address
- Server disconnected prematurely
- Internal error

The Log panel can also contain error messages showing error codes that sometimes relate to specific causes. They include:

CONNREFUSED
Most likely cause: The TCP port number is incorrect, or the serial server is not properly configured to accept connections at that port number.

NETUNREACH, TIMEDOUT, or HOSTUNREACH
Most likely cause: The IP address number is incorrect.

NAMETOOLONG, AFNOSUPPORT
Most likely cause: The IP address as entered is a malformed hostname.

ADDRNOTAVAIL
The specified address is not available.

NETDOWN
The network has failed or the specified IP address is incorrect.

CONNABORTED, CONNRESET, NOTCONN, SHUTDOWN, EDISCONN
The server has disconnected from the network. This may be caused either by a server failure, an incorrect IP address and/or TCP port number, or by a misconfigured server.

All errors containing Internal error, contact tech support
These message indicate serious errors conditions that require the attention of your company's technical support resource.

Appendix D. Basic Diagnostics

Windows utilities and administration commands can serve as basic independent diagnostics that help debug problems relating to Serial/IP Redirector installation or configuration of the serial server.

Use "ping" to Check the Network Connection

Ensure that the PC is connected to the server using the Microsoft TCP/IP networking software supplied with Windows. Open a DOS command prompt window and type in the **ping** command, using the server's network address or domain name in place of the xxx.xxx.xxx.xxx:

```
C:\ ping xxx.xxx.xxx.xxx
```

The output should indicate that ping has reached the server. If not, the Serial/IP Redirector will not be able to use the server until the problem is resolved. Contact your system administrator for help.

Use "route" to Check the Routing Table

If there is more than one default route, the Serial/IP Redirector may not be able to determine a correct static route to the server and will display a warning dialog. Follow this process:

Check the PC's route table for multiple default routes. Open a DOS command prompt and use the **route print** command:

```
C:\ route print ...
(multiple lines of output showing the routes
in effect)
```

The output will indicate if there is only one default route. In the command's output, the default routes appear at the top and show a Network Address value of 0.0.0.0. If the PC has more than one default route, the Serial/IP Redirector may not be able to access a server that is not on the same subnet.

In Windows XP, NT and 2000, make sure you are logged into an account with administrator privileges. Use the Windows NT User Manager or check with your system administrator if you are not sure of the status of your current account.

Use "telnet" to Check the Serial Server

Type the **telnet** command from the DOS prompt to establish a connection to one of the ports on the server. This, in turn, opens a Telnet window session.

Note: You can run the telnet command from a DOS prompt, or by using the **Run** command in the Start menu. If your server has a name on your network, you may be able to use the server´s name instead of the numeric address.

Verify the Creation of Serial/IP COM Ports in Windows

If you are running Windows 98, Me or NT, you can verify the presence of the virtual COM ports created by the Serial/IP Redirector from any system port list. Use the following procedure:

1. Run System in the Windows Control Panel.
2. Select the Device Manager tab.
3. Expand the Ports (COM & LPT) entry.
4. Entries should appear corresponding to those checked in the Select Ports window.

Note: Windows XP/2000/2003 will not show the ports in this way, but the ports will be available as choices when installing modems or other devices (excepting printers).

Serial/IP Redirector User Guide

Appendix E. Inbound Connections

Overview

As typically used for outbound connections through a serial device server, the application software uses the Serial/IP Redirector's client functions to communicate with the networked serial device:

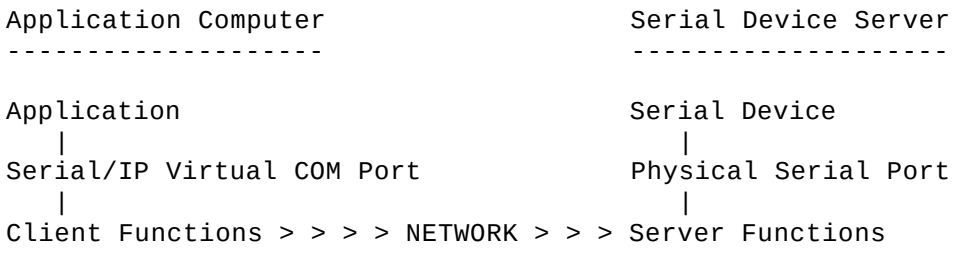


Figure 1. Client initiates connection to device.

The Serial/IP Redirector can also be configured to accept inbound connections that are initiated by a serial device server that supports client functions. This allows the application computer to wait for a networked serial device to connect instead of polling it:

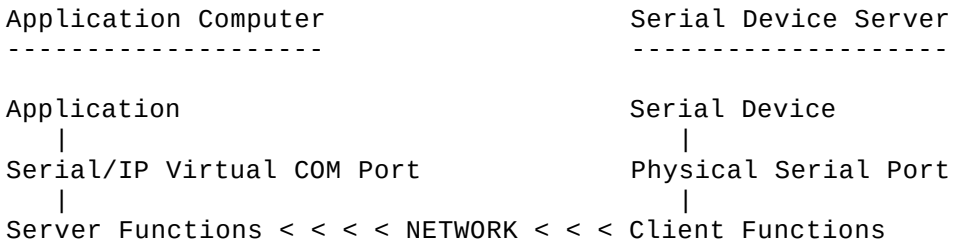


Figure 2. Device initiates connection to client.

Alternatively, the connection may be initiated by an application on another computer (#2) that is also running the Serial/IP Redirector. This allows the applications to communicate with COM ports but use the network instead of a serial cable:

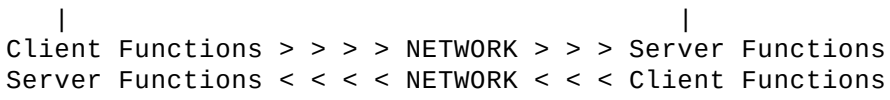


Figure 3. Both computers can initiate connections.

Accepting Inbound Connections Only

If a Serial/IP COM port is configured to only accept connections:

- User Credentials are disabled.
- The Configuration Wizard is unavailable.
- Deferred Port Open is disabled.
- While waiting for an inbound connection, data sent to the COM port by the application is discarded.
- If more than one Serial/IP COM port is configured to accept connections on the same TCP port number, arriving connections will go to the lowest numbered COM port that is available.
- CE_FRAME is not pulsed while the connection is down.

Initiating Outbound and Accepting Inbound Connections

If a Serial/IP COM port is configured to both initiate and accept connections:

- User Credentials are enabled, but used only for outbound connections.
- The Configuration Wizard is available for testing outbound connections only.
- Deferred Port Open is disabled.
- While there is no active connection, data sent to the COM port by the application is discarded.
- CE_FRAME is not pulsed while the connection is down.
- If Restore Failed Connections is enabled, it functions for outbound connections only. A failed inbound connection must be re-initiated by the other device/computer, and the Serial/IP Redirector will accept it.
- If Restore Failed Connections is disabled, the Serial/IP Redirector only initiates connections when the Serial/IP COM port is opened, then begins waiting for an inbound connection after the COM port is closed.

Tactical Software End-User License Agreement

THIS TACTICAL SOFTWARE END USER LICENSE AGREEMENT (this "Agreement") IS A BINDING AGREEMENT BETWEEN TACTICAL SOFTWARE, LLC ("Tactical") AND THE INDIVIDUAL, COMPANY, ORGANIZATION OR OTHER ENTITY ("Licensee") ACQUIRING THE LICENSE TO USE THE SOFTWARE PRODUCT (AS DEFINED IN SECTION 1) PURSUANT TO THIS AGREEMENT. IN THE EVENT LICENSEE IS AN ENTITY, LICENSEE AND THE INDIVIDUAL REVIEWING AND ACCEPTING THE TERMS OF THIS AGREEMENT ON BEHALF OF LICENSEE, EACH REPRESENT AND WARRANT THAT SUCH INDIVIDUAL IS AUTHORIZED TO ACT ON BEHALF OF LICENSEE TO REVIEW AND ACCEPT THIS AGREEMENT AND TO BIND LICENSEE TO THE TERMS AND CONDITIONS HEREOF. IF THE INDIVIDUAL REVIEWING THIS AGREEMENT DOES NOT HAVE SUCH AUTHORITY, THEN THE SOFTWARE PRODUCT MAY NOT BE INSTALLED OR USED BY LICENSEE.

BY INSTALLING OR OTHERWISE USING THIS SOFTWARE PRODUCT, LICENSEE AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, LICENSEE MAY NOT CONTINUE THIS INSTALLATION OR OTHER USE AND MUST DELETE ANY PORTION OF THE SOFTWARE PRODUCT ALREADY INSTALLED, IF ANY.

1. LICENSE TYPE AND LICENSE GRANT

(a) Tactical grants to Licensee a non-exclusive, non-transferable, limited license for an evaluation period (the "Evaluation Period"), the term of which shall be determined by Tactical, to use:

(i) the Tactical software installed or otherwise accessed by Licensee (the "Software Product") for internal evaluation of the Software Product only; and

(ii) the documentation accompanying the Software Product (the "Documentation").

Such Evaluation Period shall begin on the day the Software Product is installed.

(b) Upon Tactical's receipt of the applicable license fee for the Software Product, Tactical grants to Licensee a non-exclusive, non-transferable license, for the applicable license term (the "License Term") set forth in the License Certificate (as defined below), to use:

(i) the Software Product for internal use only; and

(ii) the Documentation.

The type of license granted to Licensee and certain restrictions regarding Licensee's use of the Software Product are set forth on the License Certificate which Tactical sends to Licensee if Licensee elects to license the Software Product (the "License Certificate"). The License Certificate is incorporate herein and is deemed to be a part of this Agreement, and Licensee shall be bound by the restrictions set forth therein.

(c) The Software Product is being "used" on a computer when it is resident in memory (i.e., RAM) or when the executable or other files of the Software Product are installed on the hard drive or other storage device of the computer.

2. CERTAIN RESTRICTIONS

(a) Licensee may not, and Licensee may not permit others, to (i) reverse engineer, decompile, or disassemble the Software Product, or otherwise attempt to derive the source code of the Software Product, except to the extent (if at all) expressly permitted under any applicable law. If applicable law expressly permits such activities, any information so discovered or derived shall be deemed to be the confidential proprietary information of Tactical and Licensee must promptly disclose such information to Tactical.

(b) Any attempt by Licensee to transfer any of Licensee's rights, duties or obligations hereunder is void. Licensee shall not rent, lease or loan the Software Product.

(c) Licensee may not, and Licensee may not permit others, to (i) copy, modify, translate, or create derivative works from, the Software Product or the Documentation, or (ii) remove any proprietary notices in, or labels on, the Software Product or the Documentation, including copyright, trademark or patent notices.

3. BACKUP COPY

Licensee may make a reasonable number of copies of the Software Product solely for backup or archival purposes. Licensee may not make any copies of the Software Product, except as expressly provided in this Section, or as permitted in Section 1 (but only to the extent necessary to use the Software Product in accordance with the license granted in Section 1), and any such copy must include all copyright and other intellectual property and proprietary notices that are in the original copy of the Software Product.

4. SOFTWARE PRODUCT

(a) The Software Product includes any updates, upgrades, fixes, and other supplements to the original Software Product provided to Licensee by Tactical, if any, and Licensee's use of any such updates, upgrades, fixes, and other supplements shall be subject to the terms, conditions, and restrictions of this Agreement.

(b) Tactical reserves the right at any time to alter features, capabilities, functions, release dates, general availability or any other characteristics of the Software Product as Tactical deems appropriate in its sole discretion.

5. TITLE

The Software Product and the Documentation are licensed, not sold. Title, ownership rights, and intellectual property rights in and to the Software Product and the Documentation remain with Tactical. The Software Product and the Documentation are protected by the copyright and other intellectual property rights laws of the United States and international copyright treaties and international law.

6. NO VIRUSES, WORMS OR TROJAN HORSES

As of the date Licensee first downloads the Software Product or first receives a copy of the Software Product from Tactical, to Tactical's knowledge, the Software Product does not contain any virus, worm, or Trojan horse which would cause damage to Licensee's software or data.

7. INTELLECTUAL PROPERTY WARRANTIES

Tactical represents and warrants to Licensee that Tactical owns or has all necessary rights, authorizations and licenses to enable Tactical to license the Software Product and Documentation in accordance with the provisions of this Agreement and that the Software Product and Documentation do not infringe or otherwise violate the copyright rights of any third party.

8. WARRANTY; LIMITATIONS

(a) Notwithstanding anything to the contrary in this Agreement, the Software Product is delivered to Licensee for the Evaluation Period “AS IS”, without any warranty of any kind, whether express or implied. Without limiting the generality of the foregoing, the Limited Warranties (as defined in Section 8(d)) do not apply during the Evaluation Period.

(b) Tactical warrants that the Software Product will perform substantially in accordance with the Documentation for a period of ninety (90) days from date Licensee acquires its initial copy of the Software Product (by download, delivery of physical media containing the Software Product, or other method of delivery).

(c) In addition, Tactical warrants that the storage media on which the Software Product is delivered directly from Tactical to Licensee shall be free from defects for a period of ninety (90) days from date Licensee acquires its initial copy of the Software Product on such storage media directly from Tactical. In the event that such media does not conform to such warranty, Licensee shall return such non-conforming media to Tactical, and Tactical’s entire liability and Licensee’s exclusive remedy shall be, at Tactical’s expense, to replace such non-conforming media.

(d) EXCEPT AS EXPRESSLY PROVIDED IN SECTION 6, 7, 8(B), and 8(C) (collectively, the "Limited Warranties"), THERE ARE NO WARRANTIES, CONDITIONS OR REPRESENTATIONS, EXPRESS OR IMPLIED BY STATUTE, USAGE, CUSTOM OF TRADE OR OTHERWISE WITH RESPECT TO THE SOFTWARE PRODUCT OR DOCUMENTATION, INCLUDING BUT NOT LIMITED TO, WARRANTIES OR REPRESENTATIONS OF WORKMANSHIP, MERCHANTABILITY, SUITABILITY OR FITNESS FOR A PARTICULAR PURPOSE, DURABILITY, OR NON-INFRINGEMENT. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, TACTICAL DOES NOT WARRANT THAT THE SOFTWARE PRODUCT WILL MEET ALL OF LICENSEE’S NEEDS OR THAT OPERATION OF THE SOFTWARE PRODUCT WILL BE ERROR-FREE. THIS LIMITED WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT.

9. REMEDY

In the event of a breach of any of the Limited Warranties (other than the Limited Warranty set forth in Section 8(c)), Tactical’s entire liability and Licensee’s exclusive remedy shall be, at Tactical’s option and expense, to either (a) refund the amount of the license fee actually paid by Licensee for the non-conforming Software Product (in which event this Agreement shall terminate), (b) repair the non-conforming Software Product by providing a patch, work-around or other reasonable solution, or (c) replace the non-conforming Software Product. The Limited Warranties do not apply in the event that non-conformance of the Software Product with a Limited Warranty results from accident, abuse, or misapplication (including use of the Software Product together with a software operating system or software and hardware environment which does not meet the specifications set forth in the Documentation). Any replacement Software Product will be warranted for the remainder of the original warranty period or thirty (30) days from the date on which the replacement Software Product is delivered, whichever is longer.

10. LIMITATION OF LIABILITY

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL TACTICAL BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER RELATING TO THE SOFTWARE PRODUCT, THE DOCUMENTATION, OR THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF TACTICAL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW A LIMITATION ON CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE. IN NO EVENT

WILL TACTICAL BE LIABLE FOR ANY DAMAGES WHATSOEVER IN EXCESS OF THE AMOUNT PAID TO TACTICAL FOR THE SOFTWARE PRODUCT THAT IS THE SUBJECT MATTER OF THE CLAIM OR THAT IS DIRECTLY RELATED TO THE CAUSE OF ACTION.

11. TERM AND TERMINATION

(a) This Agreement shall become effective upon installation of the Software Product and shall terminate automatically and immediately upon breach of this Agreement by Licensee, if any. Licensee may terminate this Agreement for convenience by removal of the Software Product from all Licensee's systems upon fifteen (15) days prior written notice to Tactical.

(b) Licensee agrees that, in the event of any termination of the license of the Software Product (including termination resulting from the termination of this Agreement), Licensee shall, within fifteen (15) days following such termination, purge all copies of the Software Product and the Documentation from all computers and storage media on which Licensee has maintained them, destroy all copies of the Software Product and the Documentation, and promptly certify in writing to Tactical that the same have been purged and destroyed.

(c) Termination of this Agreement shall not relieve either party of any payment or other obligation under this Agreement which was to have been performed by such party prior to the termination. All provisions of this Agreement which by their nature are intended to survive the termination of this Agreement (including the provisions of Sections 2, 5, 8(c), 9, 10, 11(b), this 11(c), 12, 13, and 14) shall survive such termination.

12. DISPUTE RESOLUTION

(a) If any dispute arises between Tactical and Licensee pertaining to this Agreement which Tactical and Licensee are unable to resolve amicably, such dispute shall be submitted to arbitration before a single arbitrator selected in accordance with the then-prevailing Rules of Commercial Arbitration of the American Arbitration Association. The arbitration proceeding shall take place in Manchester, New Hampshire or such other location as Tactical and Licensee may mutually agree.

(b) The arbitrator shall not contravene or vary in any respect any of the terms or provisions of this Agreement. The award of the arbitrators shall be final and binding upon Tactical and Licensee, and judgment upon any award rendered therein may be entered and enforced in any court of competent jurisdiction, including the New Hampshire Superior Court.

(c) Neither this arbitration provision nor a pending arbitration shall prevent either party from obtaining injunctive relief for any matter at any time.

13. EXPORT

Licensee acknowledges and accepts responsibility for complying with all import and export statutes, regulations, treaties and other laws, both foreign and domestic, (collectively, the "Export Laws") and agrees to not use or otherwise export or re-export, directly or indirectly, the Software Product except in accordance with the Export Laws. In particular, but without limitation, the Software Product may not be exported or re-exported, directly or indirectly,

(a) into (or to a national or resident of) any U.S. embargoed country, as such list may be revised from time to time (including without limitation Afghanistan, Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria), or

(b) to anyone on the U.S. Treasury Department list of Specially Designated Nationals or the U.S. Bureau of Industry and Security Denied Persons List or the U.S. Bureau of Industry and Security Unverified List, or

(c) for any end-use that is prohibited by United States law and the laws of the jurisdiction in which the Software Product was obtained.

Licensee represents and warrants that Licensee is not located in, under control of, or a national or resident of any such country or on any such list and that no U.S. federal agency has suspended, revoked, or denied Licensee's import or export privileges.

14. MISCELLANEOUS

(a) If any provision of this Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable, and shall not affect the other provisions of this Agreement.

(b) This Agreement shall be governed by and construed under New Hampshire law, without regard for its conflicts of law provisions. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.

(c) This Agreement constitutes the entire agreement between Tactical and Licensee regarding the subject matter hereof and supersedes all prior or simultaneous representations, discussions, negotiations, and agreements, whether written or oral.

(d) Licensee may assign this Agreement only to any entity to which it transfers all or substantially all of its assets, provided the assignee agrees to be bound by the terms of this Agreement. Otherwise, Licensee may not assign or have assumed, voluntarily, by operation of law, in bankruptcy or otherwise, any rights or delegate any duties under this Agreement without Tactical’s prior written consent, and any attempt to do so without such consent will be null and void. This Agreement will bind and inure to the benefit of the parties and their respective successors and permitted assigns.

(e) This Agreement may be amended or supplemented only by a writing that is signed by duly authorized representatives of both parties. No term or provision hereof will be considered waived by either party, and no breach excused by either party, unless such waiver or consent is in writing signed on behalf of the party against whom the waiver is asserted. No consent by either party to, or waiver of, a breach by either party, will constitute a consent to, waiver of, or excuse of any other, different, or subsequent breach by either party.

15. U.S. GOVERNMENT LICENSES

The Software Product and Documentation are provided with "restricted rights". Use, duplication or disclosure of the Software Product or the Documentation by the Government is subject to restrictions as set forth in Subparagraph 252.227-7015 (Technical Data - Commercial Items) of the Department of Defense Federal Acquisition Regulations Supplement ("DFARs") and other sections of DFARS applicable to commercial software, or Subparagraphs 52.227-19(c)(1) and (c)(2) (Commercial Computer Software - Restricted Rights) of Title 48 of the Code of Federal Regulations ("FARs") and other sections of FARS applicable to commercial software, as applicable.

Tactical Software, LLC
670 North Commercial Street
Manchester, New Hampshire, USA 03101