MICROSOFT® WINDOWS® CE OPERATING SYSTEM FOR WINDOWS- BASED TERMINAL DEVICES VERSION 1.0

IMPORTANT—READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the manufacturer ("Manufacturer") of the special purpose computing device ("SYSTEM") you acquired which includes certain Microsoft software product(s) installed on the SYSTEM and/or included in the SYSTEM package ("SOFTWARE"). The SOFTWARE includes computer software, the associated media, any printed materials, and any "online" or electronic documentation. By installing, copying downloading, or otherwise using the SOFTWARE, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, Manufacturer and Microsoft Licensing, Inc. ("MS") are unwilling to license the SOFTWARE to you. In such event, you may not use or copy the SOFTWARE, and you should promptly contact Manufacturer for instructions on return of the unused product(s) for a refund.

Software LICENSE
The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE is licensed, not sold.

1. **GRANT OF LICENSE.** SOFTWARE includes software already installed on the SYSTEM ("SYSTEM Software") and, if included in the SYSTEM package, software contained on the CD-ROM disk and/or floppy disk(s) labeled "Desktop Software for Microsoft Windows CE" ("Desktop Software"). This EULA grants you the following rights to the SOFTWARE:
   - **SYSTEM Software.** You may use the SYSTEM Software only as installed in the SYSTEM.
   - **Desktop Software.** Desktop Software might not be included with your SYSTEM. If Desktop Software is included with your SYSTEM, you may install and use the component(s) of the Desktop Software in accordance with the terms of the end user license agreement provided with such component(s). In the absence of a separate end user license agreement for particular component(s) of the Desktop Software, you may install and use only one (1) copy of such component(s) on a single computer with which you use the SYSTEM.
   - **Use of Windows CE Operating System for Windows-Based Terminal Devices with Microsoft Windows NT Server, Terminal Server Edition**. If the SOFTWARE is Windows CE operating system for Windows-Based Terminal devices, the following special provisions apply. In order to use the SYSTEM in connection with Windows NT Server, Terminal Server Edition, you must possess (1) a Client Access License for Windows NT Server, Terminal Server Edition and (2) an end user license for Windows NT Workstation or an end user license agreement for Windows NT Workstation for Windows-Based Terminal Devices (please refer to the end user license agreement for Windows NT Server, Terminal Server Edition for additional information). Manufacturer may have included a Certificate of Authenticity for Windows NT Workstation for Windows-Based Terminal Devices with the SYSTEM. In that case, this EULA constitutes an end user license for the version of Windows NT Workstation for Windows-Based Terminal Devices indicated on such Certificate of Authenticity.
   - **Back-up Copy.** If Manufacturer has not included a back-up copy of the SYSTEM Software with the SYSTEM, you may make a single back-up copy of the SYSTEM Software. You may use the back-up copy solely for archival purposes.

2. **DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.**
   - **Speech/Handwriting Recognition.** If the SYSTEM Software includes speech and/or handwriting recognition component(s), you should understand that speech and handwriting recognition are inherently statistical processes; that recognition errors are inherent in the processes; that it is your responsibility to provide for handling such errors and to monitor the recognition processes and correct any errors. **Neither Manufacturer nor its suppliers shall be liable for any damages arising out of errors in the speech and handwriting recognition processes.**
   - **Limitations on Reverse Engineering, Decompilation and Disassembly.** You may not reverse engineer, decompile, or disassemble the SYSTEM Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
   - **Single SYSTEM.** The SYSTEM Software is licensed with the SYSTEM as a single integrated product. The SYSTEM Software installed in Read Only Memory ("ROM") of the SYSTEM may only be used as part of the SYSTEM.
     Single EULA. The package for the SYSTEM Software may contain multiple versions of this EULA, such as multiple translations and/or multiple media versions (e.g., in the user documentation and in the software). Even if you receive multiple versions of the EULA, you are licensed to use only one (1) copy of the SYSTEM Software.
   - **Rental.** You may not rent or lease the SOFTWARE.
   - **Software Transfer.** You may permanently transfer all of your rights under this EULA only as part of a sale or transfer of the SYSTEM, provided you retain no copies, you transfer all of the SOFTWARE (including all component parts, the media, any upgrades or backup copies, this EULA and, if applicable, the Certificate(s) of Authenticity), **and** the recipient agrees to the terms of this EULA. If the SOFTWARE is an upgrade, any transfer must include all prior versions of the SOFTWARE.
   - **Termination.** Without prejudice to any other rights, Manufacturer or MS may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE and all of its component parts.

3. **UPGRADES.** If the SYSTEM Software and this EULA are provided separate from the SYSTEM by Manufacturer and the SYSTEM Software is on a ROM chip, CD ROM disk(s) or floppy disk(s), and labeled "For ROM Upgrade Purposes Only" ("ROM Upgrade "), you may install one copy of the ROM Upgrade onto the SYSTEM as a replacement copy for the SYSTEM Software originally installed on the SYSTEM and use it in accordance with Section 1 of this EULA.

4. **COPYRIGHT.** All title and copyrights in and to the SOFTWARE (including but not limited to any images, photographs, animations, video, audio, music, text and "applets," incorporated into the SOFTWARE), the accompanying printed materials, and any copies of the SOFTWARE, are owned by MS or its suppliers (including Microsoft Corporation). You may not copy the printed materials accompanying the SOFTWARE. All rights not specifically granted under this EULA are reserved by MS and its suppliers (including Microsoft Corporation).

5. **PRODUCT SUPPORT. Product support for the SOFTWARE is not provided by MS, its parent corporation, Microsoft Corporation, or their affiliates or subsidiaries. For product support, please refer to Manufacturer's support number provided in the documentation for the SYSTEM. Should you have any questions concerning this EULA, or if you desire to contact Manufacturer for any other reason, please refer to the address provided in the documentation for the SYSTEM.**

6. **EXPORT RESTRICTIONS.** You agree that you will not export or re-export the SOFTWARE to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export or re-export the SOFTWARE: (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, which as of March 1998 include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any person or entity who you know or have reason to

know will utilize the SOFTWARE or portion thereof in the design, development or production of nuclear, chemical or biological weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.
If the SOFTWARE is labeled "North America Only Version" above, on the Product Identification Card, or on the SOFTWARE packaging or other written materials, then the following applies: The SOFTWARE is intended for distribution only in the United States, its territories and possessions (including Puerto Rico, Guam, and U.S. Virgin Islands) and Canada. Export of the SOFTWARE from the United States is regulated under "EI controls" of the Export Administration Regulations (EAR, 15 CFR 730-744) of the U.S. Commerce Department, Bureau of Export Administration (BXA). A license is required to export the SOFTWARE outside the United States or Canada. You agree that you will not directly or indirectly, export or re-export the SOFTWARE (or portions thereof) to any country, other than Canada, or to any person or entity subject to U.S. export restrictions without first obtaining a Commerce Department export license. You warrant and represent that neither the BXA nor any other U.S. federal agency has suspended, revoked or denied your export privileges.

7. NOTE ON JAVA SUPPORT. The SYSTEM Software may contain support for programs written in Java. Java technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of Java technology could lead directly to death, personal injury, or severe physical or environmental damage.

8. LIMITED WARRANTY.

Limited Warranty. Manufacturer warrants that the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt. Any implied warranties on the SOFTWARE are limited to ninety (90) days. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies. Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet the above Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

No Other Warranties. EXCEPT AS EXPRESSLY PROVIDED IN THE LIMITED WARRANTY SECTION ABOVE, THE SOFTWARE IS PROVIDED TO THE END USER "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK OF THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU.

No Liability for Consequential Damages. MANUFACTURER OR MANUFACTURER'S SUPPLIERS, INCLUDING MS AND ITS SUPPLIERS, SHALL NOT BE HELD TO ANY LIABILITY FOR ANY DAMAGES SUFFERED OR INCURRED BY THE END USER (INCLUDING, BUT NOT LIMITED TO, GENERAL, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION AND THE LIKE), ARISING FROM OR IN CONNECTION WITH THE DELIVERY, USE OR PERFORMANCE OF THE SOFTWARE.

If you acquired this EULA in the United States, this EULA is governed by the laws of the State of Washington.
If you acquired this EULA in Canada, this EULA is governed by the laws of the Province of Ontario, Canada. Each of the parties hereto irrevocably attorns to the jurisdiction of the courts of the Province of Ontario and further agrees to commence any litigation which may arise hereunder in the courts located in the Judicial District of York, Province of Ontario.
If this EULA was acquired outside the United States, then local law may apply.
Should you have any questions concerning this EULA, please contact the Manufacturer of your SYSTEM.

U.S. GOVERNMENT RESTRICTED RIGHTS
The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation/One Microsoft Way/Redmond, WA 98052-6399.

Visara® Windows-based Terminal

Installation Guide and User Reference Manual

P/N 707027-002

Visara® Windows-based Terminal

Installation Guide and User Reference Manual

P/N 707027-002

MTX, Inc
2917 Highwoods Blvd., Suite 100
Raleigh,NC 27604 USA

Toll Free 888-334-4380
Phone 919-250-6000
Internet www.mtx.com

Part Number: 707027-002

Printed in USA

Table of Contents

Preface

FCC Compliance Statement

This equipment generates, uses and can radiate radio frequency energy and may cause interference to radio communications. It has been tested and found to comply with the limits for a Class B computing device pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user, at his own expense, must take whatever measures may be required to correct the interference.

Shielded cables must be used to ensure compliance with the Class A limits.

Warranty

The Visara system unit, the hardware, is warranted to be free from material defects in components and workmanship for 12 months from the date of shipment to the original customer. MTX will, at its option, repair or replace the product if any such defect occurs according to the terms of this limited warranty. MTX' liability under this warranty shall be limited to such repair or replacement. MTX does not warranty damage to or dimming of Cathode Ray Tubes.

This warranty shall be invalid if, in the sole judgment of MTX, the hardware or any hardware component has been subjected to misuse, abuse, neglect, accident, acts of God, external electrical fault, power surges or failure, damage in shipment or improper service or modification by anyone other than a MTX authorized service center. This warranty shall also be invalid if the serial number has been removed, defaced or altered in any way. This limited warranty does not cover other manufacturers' computer hardware, components, accessories or expansion items unless authorized by MTX. The sole and exclusive remedy, under this limited warranty, shall be the repair or replacement of defective parts as provided above.

Under no circumstances shall MTX be liable, under any legal theory, tort, contract or otherwise, in any way for damages, including but not limited to, any loss or inaccuracy of data, business or profits, or any other direct or indirect special, incidental, or consequential damages arising from the use of this product. In no event will MTX be liable for any damages in excess of the amount MTX received for the purchase of the hardware product, even if MTX shall have been informed of the possibility of such damages, or for any claim by any other party. Some states do not allow the exclusion or limitation of incidental or consequential damages. This exclusion may not apply.

There are no express warranties other than those on the face hereof and described above. Except for the foregoing warranties, MTX does not warrant the merchantability or fitness of a product for a particular purpose of the products or performance or non-infringement thereof, and does not make any warranty, express or implied, with respect to the products or anything else. MTX has not authorized anyone to make any representation or warranty other than as provided above. states do not allow limitations on how long an implied warranty lasts. The above limitation may not apply. This warranty gives you specific legal rights and you may have others rights that vary from state to state.

Repairs

MTX will repair or replace any non-obsolete hardware. If under warranty as described herein, such repair or replacement will be provided according to the terms of the warranty. If the hardware is not under warranty, the hardware will be repaired or replaced at the then current labor and material rates. Hardware in need of repair is to be returned, freight and insurance prepaid, to MTX factory or service depot. A Return Merchandise Authorization (RMA) number is required for all returns. MTX will not be responsible for any merchandise lost or damaged in transit. To obtain an RMA number, contact MTX Customer Service with the following information:

- The model and serial number of the item to be repaired
- Purchase date and source
- Description of problem

Pack the item to be returned in the original pacakging if available or packaging of sufficient quality to prevent damage in shipment. The RMA number must be clearly displayed on the outside of the package.

The procedure for obtaining service may vary outside the Continental United States. Contact MTX for further information.

Chapter 1. Overview

The Visara Windows-based Terminal embodies the computing capabilities of both fixed function terminals and PCs and provides:

- access to DOS and Windows applications
- access to mini, midrange and mainframe host computers
- full utilization of PC and Host network-accessible peripheral devices

The Visara Windows-based Terminal is a full-function and powerful desktop device appropriate for all environments.

Advances in network computing enable a Windows-based Terminal device to operate as if application programs are running locally. Powerful, high-speed processors and file servers can simultaneously service many desktops. As new capabilities are added to the server, e.g. CPU power, disk storage, etc., each and every desktop device benefits. This provides a highly effective model for maintenance and operation as administrative services are centrally managed and controlled. And, as a client of powerful servers and hosts, Windows-based Terminals help to minimize desktop device obsolescence.

PC and Host Networks

Visara can access Windows application servers and host computers over either Windows or Netware networks…over local or wide-area networks…to run Windows 3.X, 95/98 and NT applications. HostConnect, a Telnet terminal emulation program permanently stored in Visara, enables server-independent access by a Visara Windows-based Terminal to host data and programs.

Enterprise Networking

Enterprise networks typically require user access to multi-host environments which can consist of mainframe and midrange as well as microprocessor-based servers. The Visara provides simultaneous terminal emulation capabilities for network connection to most host environments including IBM S/390, AS/400, RS/6000 as well as HP, DEC and other ASCII hosts.

Chapter 2: Unpacking the Visara

Unpacking and Setup

The Visara Windows-based Terminal is shipped in a single carton and contains the following components:

- System unit
- System unit stand
- Keyboard
- Mouse
- User Manual

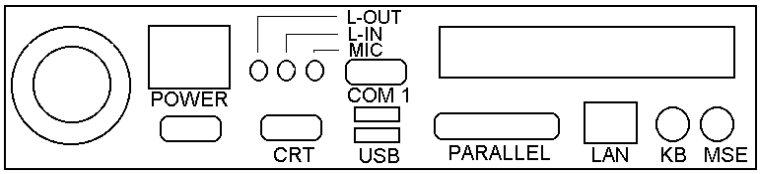
If you purchased the optional monitor, it is shipped in a separate carton. Save the cartons and packing material in the event you need to subsequently store or ship the unit.

Setting up Visara

Clear the work area where you will set up the Visara Windows-based Terminal. The system unit may be positioned horizontally on a flat surface or vertically using the system unit stands. The stands are designed to slip over the side of the system unit. Ensure there is sufficient clearance (minimally 3" / 76mm) behind the unit for the cables and connectors. The system unit is designed to support monitors up to 15 inches or a maximum weight of 30 pounds. **Do not place objects weighing in excess of 30 pounds on the system unit.** Take care not to block the ventilation areas on the system unit. Position the monitor, keyboard and mouse in a comfortable ergonomic position.

Connecting the Cables

Refer to the diagram of the back panel. The icons above the connectors designate their function.



POWER	100-240 VAC input at 47-63Hz
CRT	VGA monitor connector
L-OUT	Audio output jack
L-IN	Audio input jack (not supported)
MIC	Microphone input (not supported)
COM 1	Serial port 1
USB	Universal serial bus connector (not supported)
PARALLEL	Parallel printer port
LAN	Ethernet connector 10/100
KB	Keyboard connector
MSE	Mouse connector

Before connecting power to the system unit, confirm that the power switch on the front is in the off (out) position. Connect the power cord to the Visara system unit before plugging the power cord into an electrical outlet.

Before plugging the monitor into an electrical outlet, connect the video cable from the monitor to the Visara system unit.

Next, connect the keyboard and mouse to the system unit. Be careful that you plug each into the correct connector since they both use the same type of connector.

Connecting to a Network

The Visara is designed to connect to twisted-pair Ethernet networks (10BaseT or 100BaseT). The RJ45 connector on the rear panel is used for this connection. Make your network connection by plugging the RJ45 connector of a category 5 cable (not included), into the RJ45 connector of the system unit.

Power Supply

The Visara Windows-based Terminal has an internal power supply that supports AC input voltages within the range of 100-240 VAC and a frequency range of 47-63Hz. The input connector supports standard appliance power cords and one is typically supplied to match the local power receptacle.

Indicator Lights (LEDs)

There are three lights on the front of the Visara system unit. One is not used.

- **Power**

  The indicator light marked with a “sun” symbol is the power indicator and will be green when the unit is on. If the switch is in the on position and the green light is not lit, check the power cord connections.

- **Ethernet**

  The light marked by a running man indicates network activity. This light will be yellow or flash yellow when the Visara detects Ethernet network activity. If this indicator does not light check your cable and network connections.

Chapter 3: Starting Visara the First Time

Windows Setup Wizard

The first time the Visara is run the user will be presented with the Windows-Based Terminal setup wizard. The setup wizard welcome screen shows the product ID at this screen, click **Next** to continue the setup function. The setup wizard will then present the Microsoft Windows CE license agreement. You should read this agreement and click **Accept** to continue the setup process.

Depending on your use of DHCP, the setup wizard will present a screen asking if you wish to use the DHCP settings or to configure a manual DHCP address. If your settings are provided by a DHCP server, select DHCP and **Next** to continue. If you will be providing manual settings for the IP address or other settings see the section on Manual configuration below. Once the appropriate information is supplied click finish on the final screen to exit the Setup Wizard. If the **Restart** Message is displayed select **Yes** at the prompt to restart your Visara using the new settings.

Automatic Configuration

The Visara can be configured automatically through the use of a ftp server on the network and the Visara Remote Configuration Utility. Or, these functions can be bypassed and the Visara configured manually. Using a DHCP server will allow use of the Visara without configuring the network parameters such as an IP address or Gateway address. The Remote Configuration Utility is used to configure the connections to other network servers such as telnet terminal emulations. The Visara comes pre-configured to use DHCP and Remote Configuration to allow fully automatic installation without operator intervention. The steps for automatic and manual configuration are covered below:

DHCP

Dynamic Host Configuration Protocol (DHCP) provides a means of automatic configuration of the Visara network parameters such as the IP address and gateway address. The use of DHCP requires the configuration of a DHCP server to provide this information to the Visara at boot time. Your Network Administrator must perform the configuration of the DHCP server.

DHCP Setup

The Visara is factory configured to use DHCP. In order for this feature to operate correctly an active DHCP server must exist on the network and at least one available IP address must be accessible from the DHCP server. To insure that DHCP remains active select DHCP in the Setup Wizard. At boot time the Visara will broadcast a message to the DHCP server requesting network configuration information. If the Visara receives a valid network configuration from the DHCP server it will use this information to configure its TCP/IP settings and become an active node on the Ethernet network. DHCP can be disabled to allow using assigned TCP/IP settings provided by your Network Administrator. To disable DHCP in the Setup Wizard select **"No, I will enter static IP information"** or from the Main Menu do the following:

- From the Visara Main Menu hit F2 on the keyboard to access the Terminal Properties screen**.** Select the **Network** tab and the Network properties window will open.
- Select the radio button to specify an IP address and enter the appropriate IP address information. The Network tab also provides access to advanced network settings for DNS and Wins. Check with your network administrator for the appropriate settings.

For fixed IP addresses and other manual configurations see the section titled **Manual Configuration** in this User Guide.

Remote Configuration of Connections

Remote Configuration allows the Visara to handle Account/User Based connection configurations. Connection configurations determine what servers the user accesses and contains terminal emulation information including Telnet emulation type. Remote Configuration allows the Network Administrator to establish Account/User Based connection configurations that are then downloaded to other Visara units on the network. Configurations can be setup on a user or department basis as desired. The configurations are stored on a central server and are downloaded to the Visara based on the Account name used at Visara boot time. If your Network Administrator has setup the server to support Remote Configurations he will provide you with an account name to use when starting the Visara.

Remote Configuration can be bypassed by clicking **Cancel** on the startup window or it can be disabled. When Remote Configuration is bypassed or disabled the Visara will then use internally stored connection configurations.

Remote Configuration Setup

The Visara is factory configured with Remote Configuration enabled. In order for this feature to operate correctly a configuration must have been previously saved to the appropriate server and the server must be configured to support FTP (a standard file transfer protocol). This setup is performed by your Network Administrator who will provide you with an account name for use when starting the Visara. Enter this account name into the Remote Configuration startup window at boot time and click the **Start** button.

The Remote Configuration function can be bypassed by clicking the **Cancel** button on the Remote Configuration startup window or by pressing the **Esc** key on the keyboard. Remote Configuration can be enabled, disabled or reconfigured from the Admin page of the Terminal Properties window as follows:

- From the Visara Main Menu hit the F2 key to access the Terminal Properties window.
- Select the Admin tab.
- To enable, check the box titled "**Update Configuration at power up**".
- If your adminstrator has provided information for configuring a FTP server, enter that information in the appropriate fields.
- Click on the **Apply** button to save the settings or the **OK** button to save and exit.

For setup information on other Remote Configuration functions, or for using Remote Configuration without DHCP, see **Appendix A**.

Automatic Software Update

The Visara has the ability to update the operating system and applications over the network. This Firmware Update feature can be set to check for updates automatically at every boot time or this function can be run manually when desired.

Firmware Update Setup

The Visara is factory configured with Firmware Update disabled. In order for this feature to operate a server must be configured to support ftp (a standard file transfer protocol) and the update files must be loaded on the ftp server. This setup is performed by your Network Administrator.

- To configure the Visara for Automatic Firmware Update:
- From the Visara Main Menu hit the F2 key to access the Terminal Properties window.
- Select the Firmware tab.
- To enable, check the box titled "**Check for new firmware at power up**".
- To prompt the user before updating check the box **titled "Prompt before downloading new firmware**".
- If your adminstrator has provided information for configuring a FTP server, enter that information in the appropriate fields.
- The "**Check for new firmware now**" button can be used to confirm configuration settings or to check the server for updates. To avoid software conflicts, the Visara only allows actual updates at startup.
- Click on the **Apply** button to save the settings or the **OK** button to save and exit.

Further information on Firmware Update is provided in Appendix B.

Manual Configuration

The first time you start your Visara Windows Terminal, you'll need to enter some basic configuration information. This information is used to identify your Visara to the other computers on the network and visa versa. The configuration information is used each subsequent time you start Visara. Your network administrator will be able to provide this information.

IP Configuration Information

To facilitate this process, collect the following information about your Visara Windows Terminal and network so it will be readily available during configuration. You may not need information for every item.

Visara IP Address	___.___.___.___
Subnet Mask	___.___.___.___
Default Gateway	___.___.___.___
Primary DNS	___.___.___.___
Secondary DNS	___.___.___.___
Primary WINS	___.___.___.___
Secondary WINS	___.___.___.___

Collect the following information about each host computer you will use:
IP Address ___.___.___.___
Terminal type to emulate _____

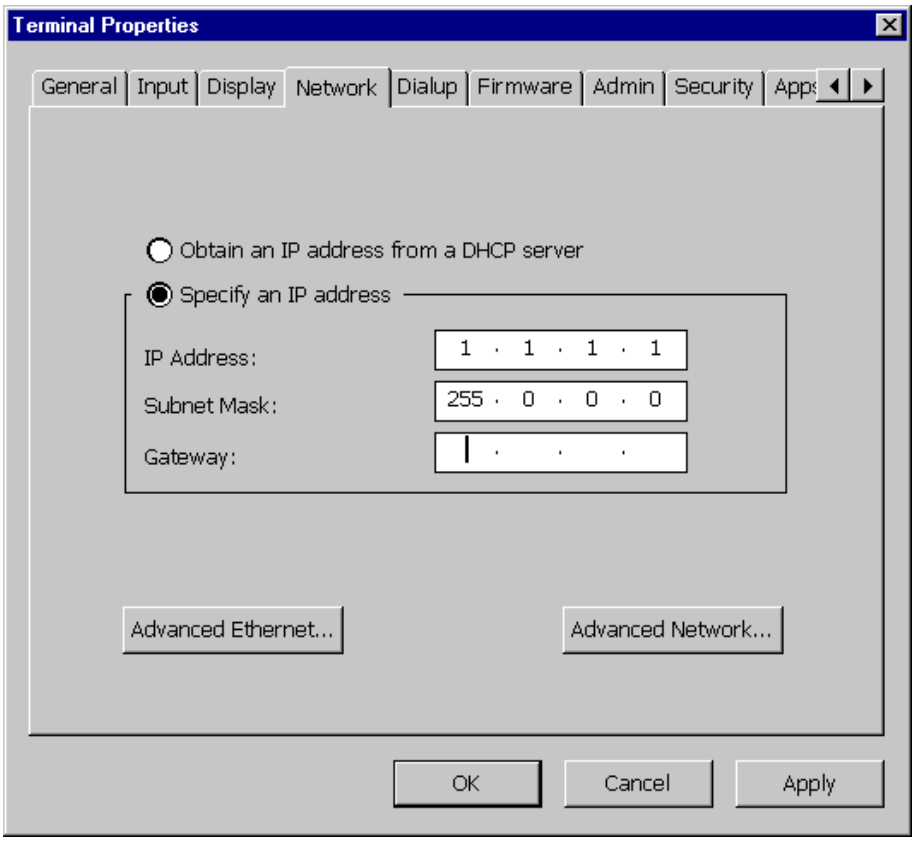
Collect the following information about your Citrix WinFrame or MetaFrame PC applications server:

Server Name _____ or IP Address___.___.___.___

With this information at hand, you are now ready to begin configuring your Visara.

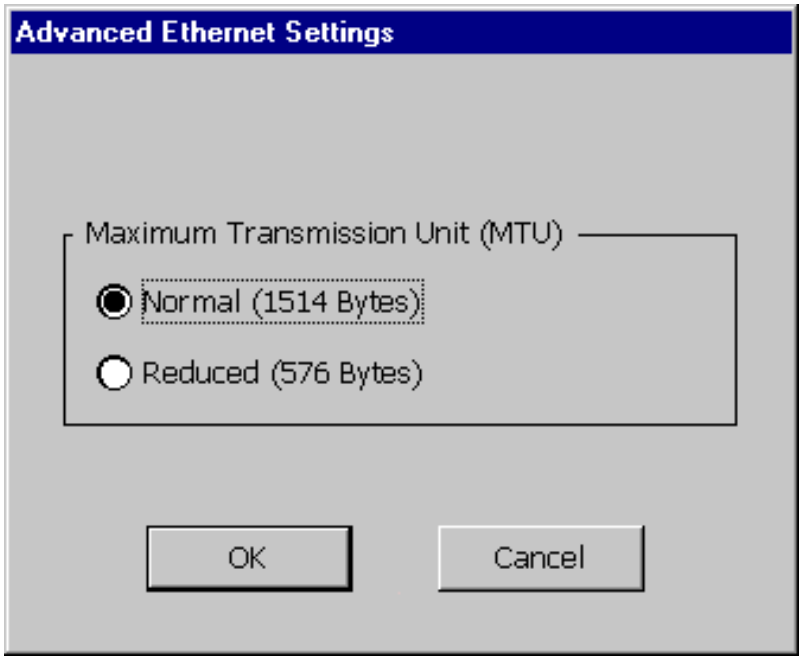
IP Setup Screens

After you have connected the cables and the power supply, turn on the unit by pressing the power button to the ON position (Depressed). If this is the first time the Visara is turned on you will see the Visara Setup Wizard after the completion of the boot process. By proceeding through the steps in the Setup Wizard you will reach the screen titled IP address. If the Visara was configured previously the Remote Configuration Utility window will appear. To disable this window for future boot operations on a manually configured Visara, deselect the check box for Enable Auto-Download of Configuration at Startup and click on the **Apply** button. Click on the **Cancel** button and the Visara Main Menu window will display shortly. At the main menu press the F2 key to access the Terminal Properties Window. Select the Network tab to access the IP address settings.



Advanced Ethernet Settings

The Maximum Transmission Unit (MTU) setting specifies the maximum size of a frame that can be transmitted by TCP/IP over Ethernet. The default is Normal (1514 Bytes). The Reduced setting (576 Bytes) would be used if a host or router on the WAN required the lower setting (example: x.25)



Other Terminal Properties Options

There are nine other Terminal Properties tabs in the Terminal Properties menu:

General

Input

Display

Dialup

Firmware

Admin

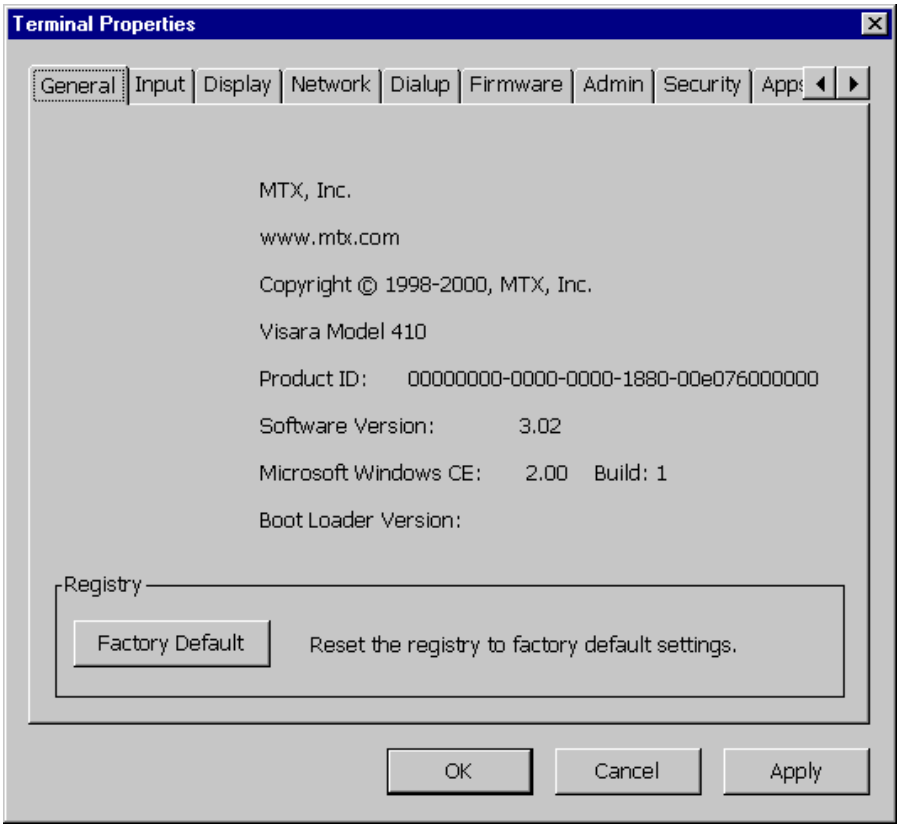
Security

Apps

Hot Keys

General

This tab provides access to copyright and product ID information. The tab also includes a check box that allows resetting the Visara to factory default settings. The Factory Default button will clear the registry and will run the Setup Wizard at the next startup.



Input

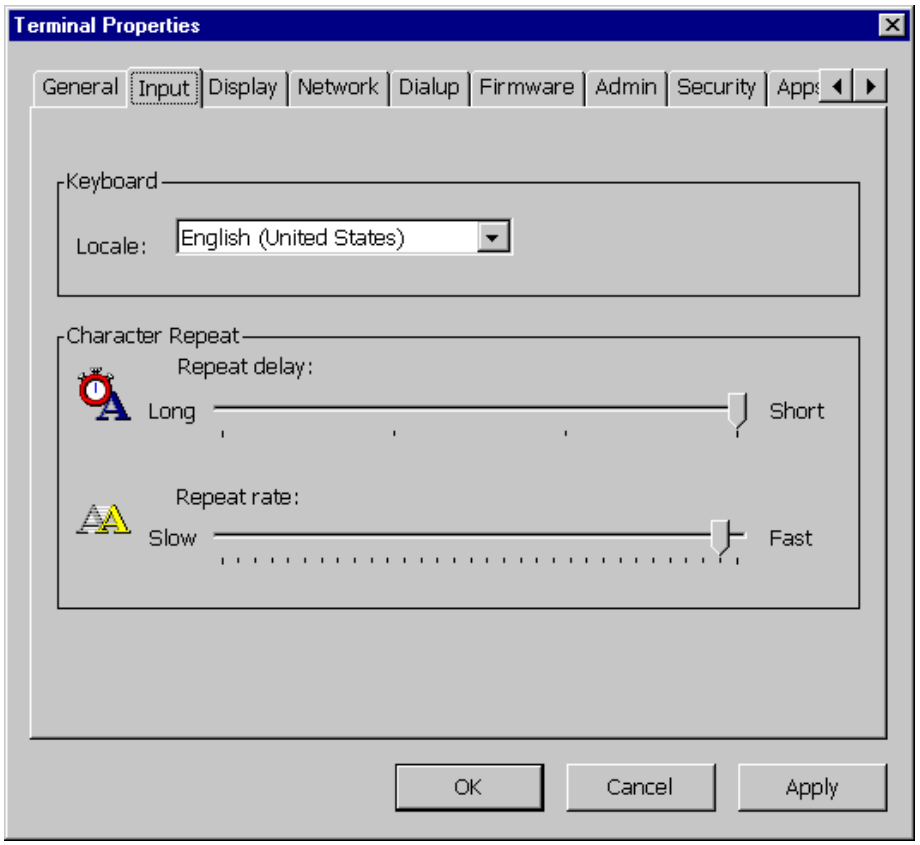
Clicking on the **Input** tab provides access to keyboard settings as described below:

- **Keyboard Locale**

  In the upper section of this window is a drop down box used to identify the keyboard attached to your Visara. Select the appropriate language setting for your keyboard.

- **Character Repeat**

  Use these settings to adjust the keyboard to best suit your typing style. To adjust these settings, drag the sliders to the new settings.



Display

The Display tab allows changing of the Visara display attributes as follows:

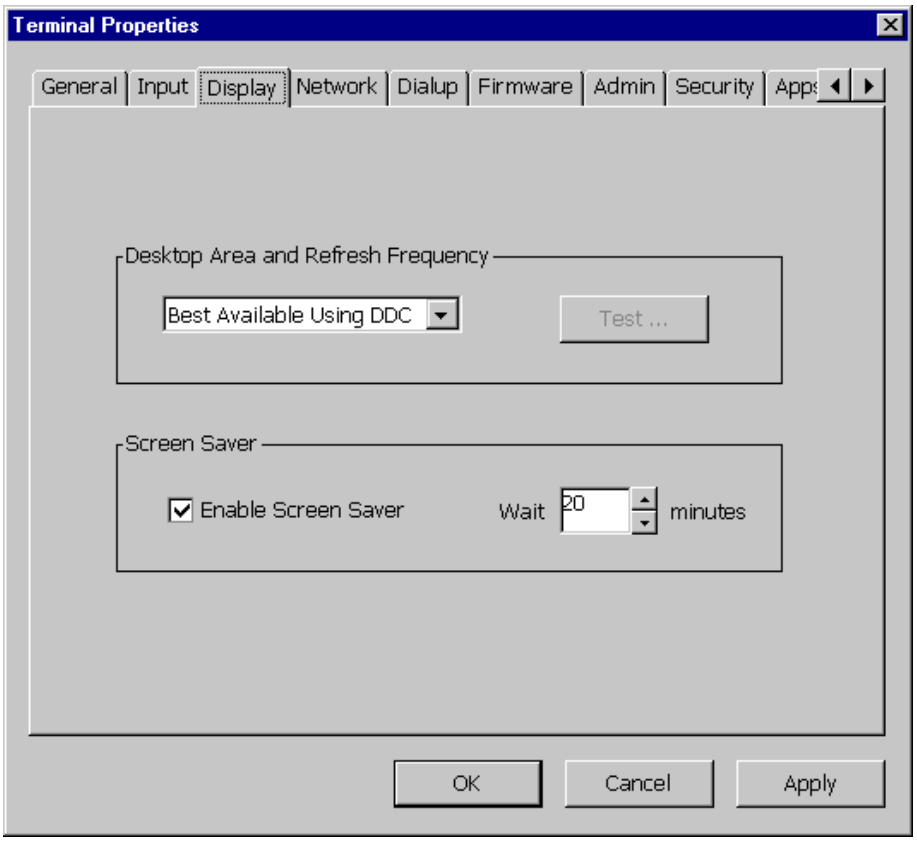
- **Desktop Area and Refresh Frequency**

  This setting allows changing of the Visara screen resolution and vertical refresh frequency. The **Test** button allows the user to insure that the connected monitor can accept the new frequency.

- **Screen Saver**

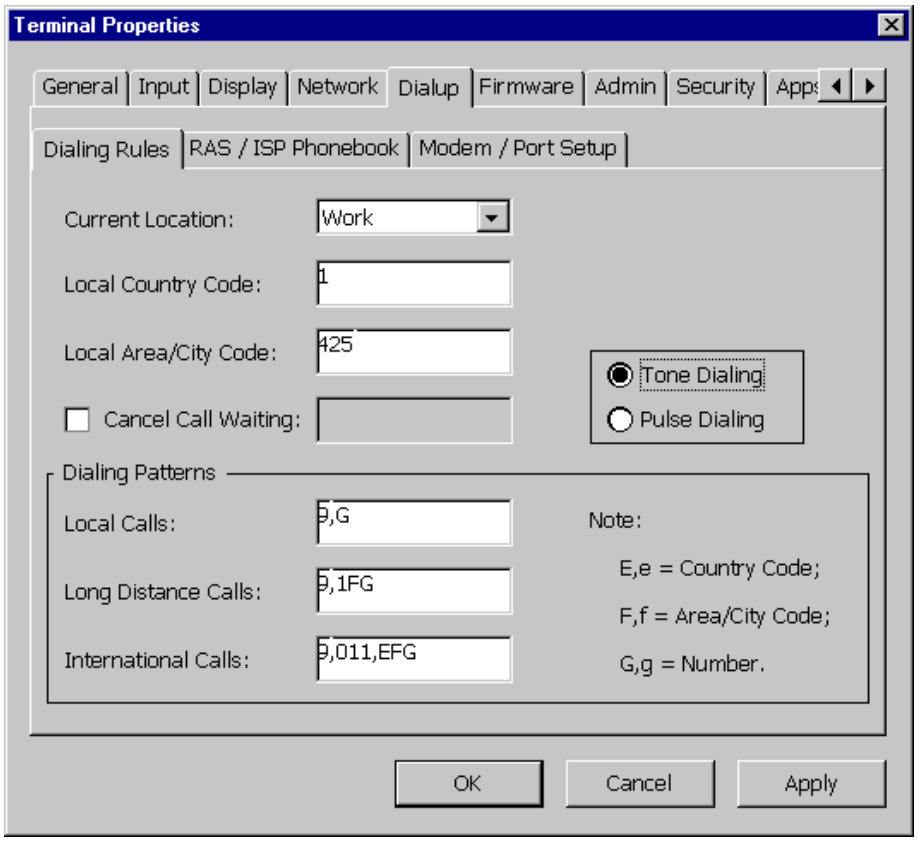
The Visara has a local screen saver function that can be enabled or disabled.

The delay time for invoking the screen saver is also selectable.



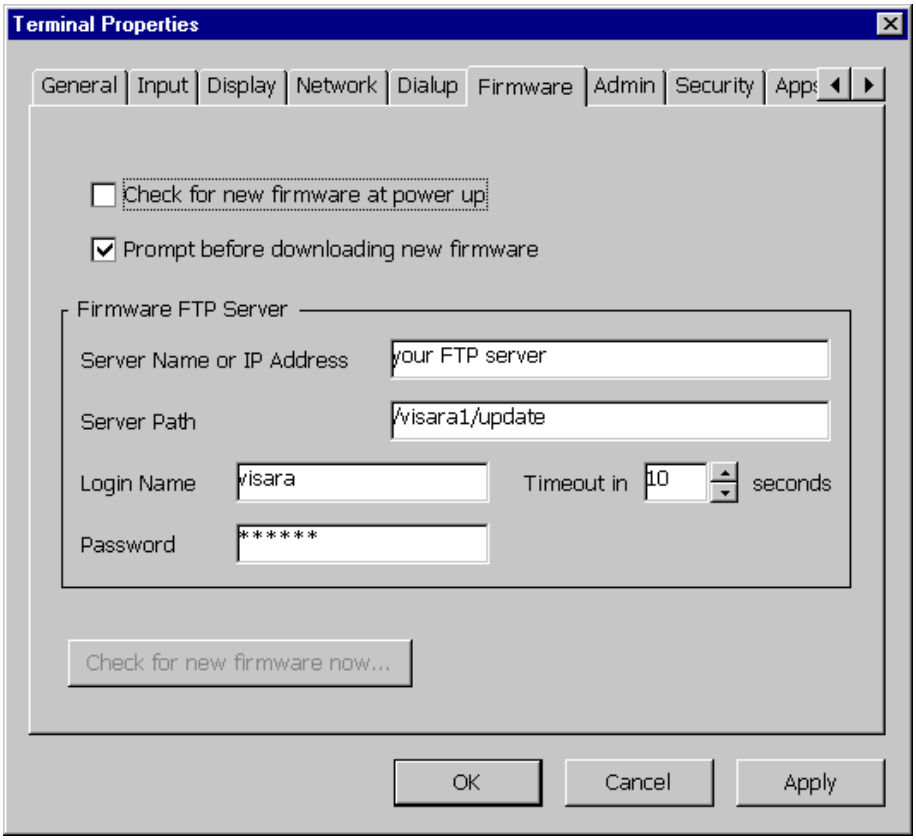
Dialup

The Dialup tab allows the Visara to be configured for remote communications to a RAS (Remote Access Server) or ISP (Internet Service Provider).



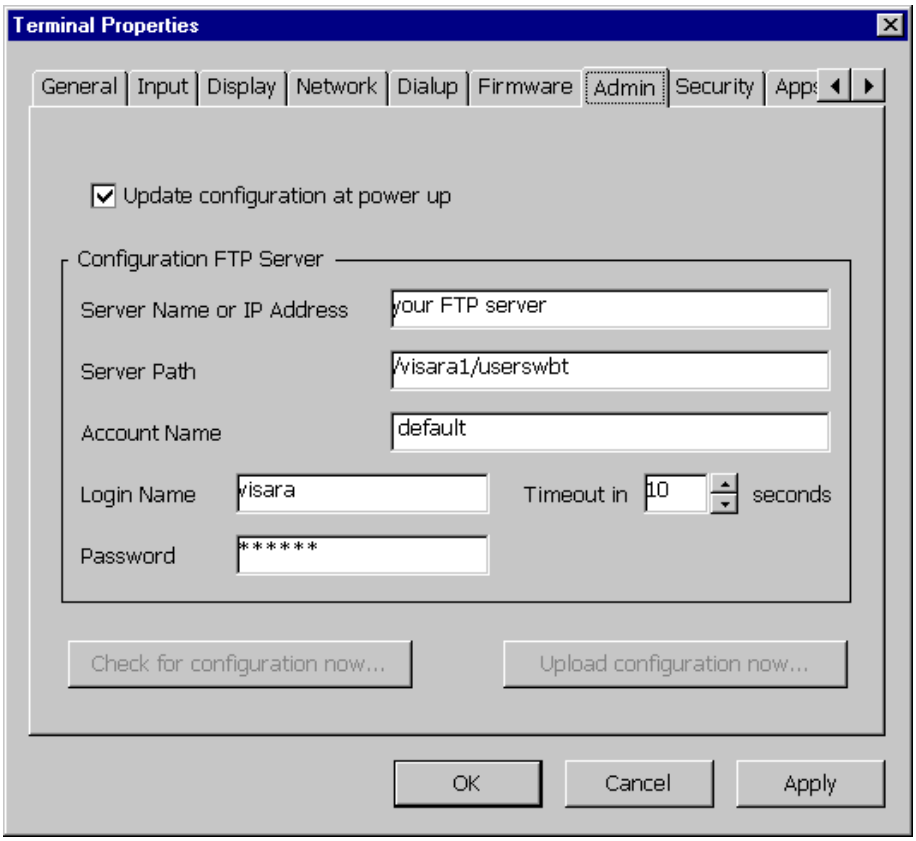
Firmware

The Firmware tab controls the software update feature of the Visara. The Firmware window allows enabling or disabling of the software update function and configuration of the network parameters to access the FTP server.



Admin

The Admin tab controls the Remote Configuration feature of the Visara. The Admin window allows enabling or disabling of the Remote Configuration function and configuration of the network parameters to access the FTP server.



Security

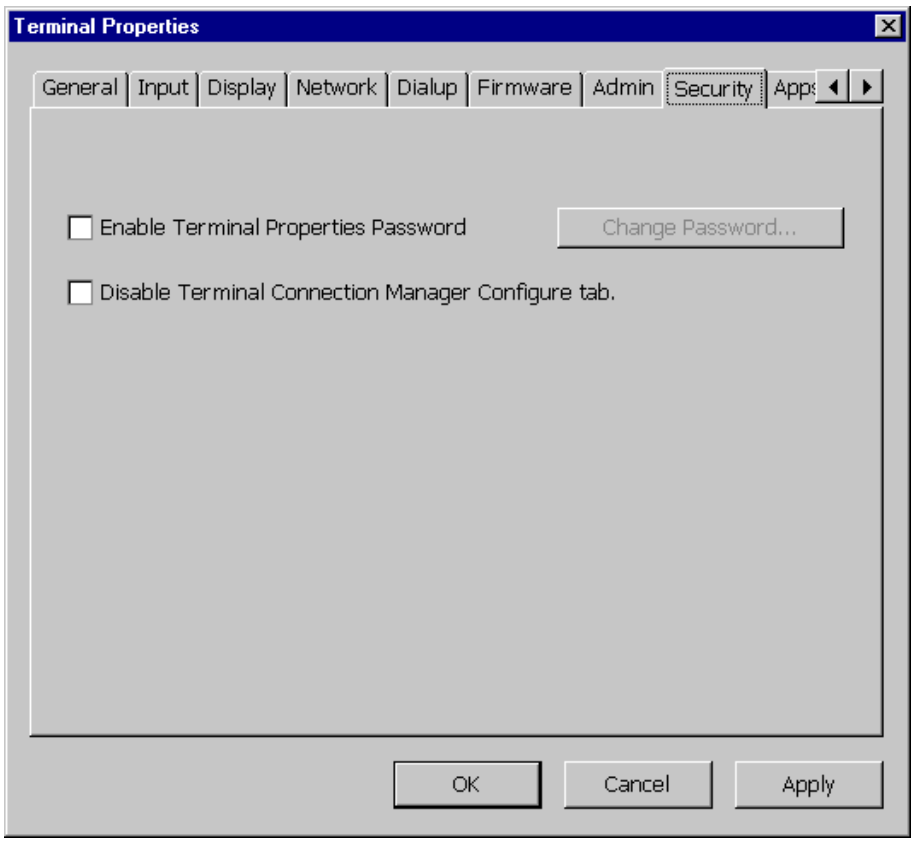
This tab allows an administrator to secure the terminal properties and host configurations in the Visara.

- **Enable Terminal Properties Password**

Enabling this function requires the entry of a password when the [f2] key is pressed. The password can be a maximum of 16 characters (alpha, numeric, special). If the password is incorrect, only the General tab is displayed.

- **Disable Terminal Connection Manager Configure Tab**

Enabling this function will turn off the Configure tab in the Terminal Connection Manager



Apps

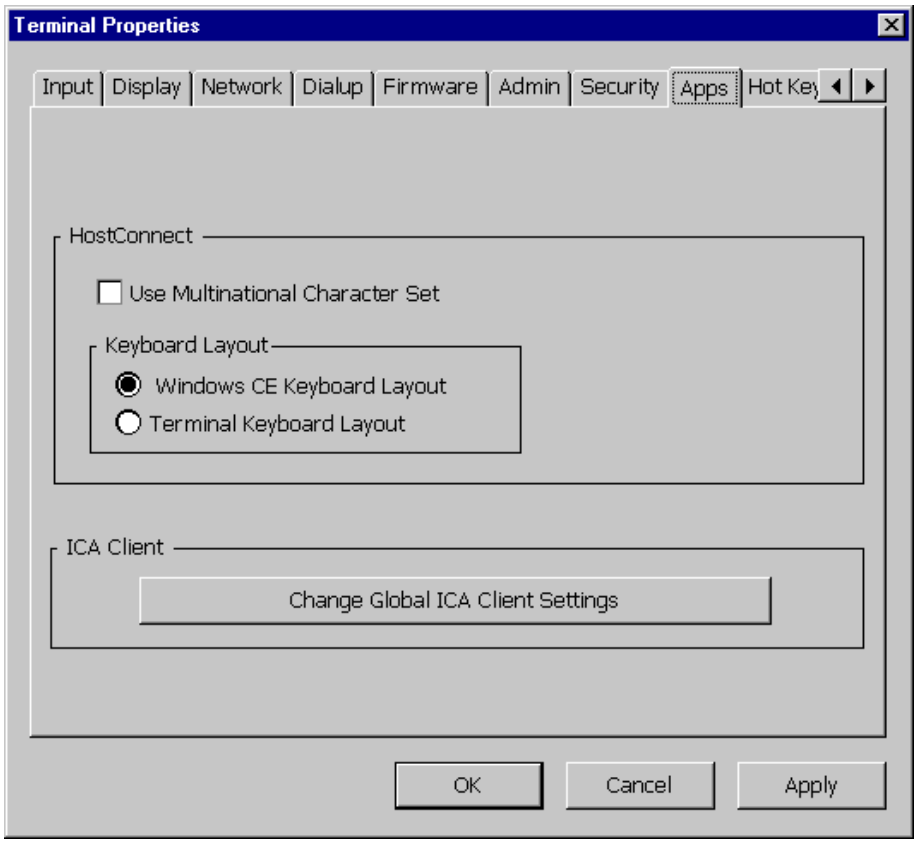
The Apps tab allows setting global session configurations for Host Connect and ICA.

- **Host Connect**

The Host Connect settings provide global settings for the Host Connect character set and keyboard mapping.

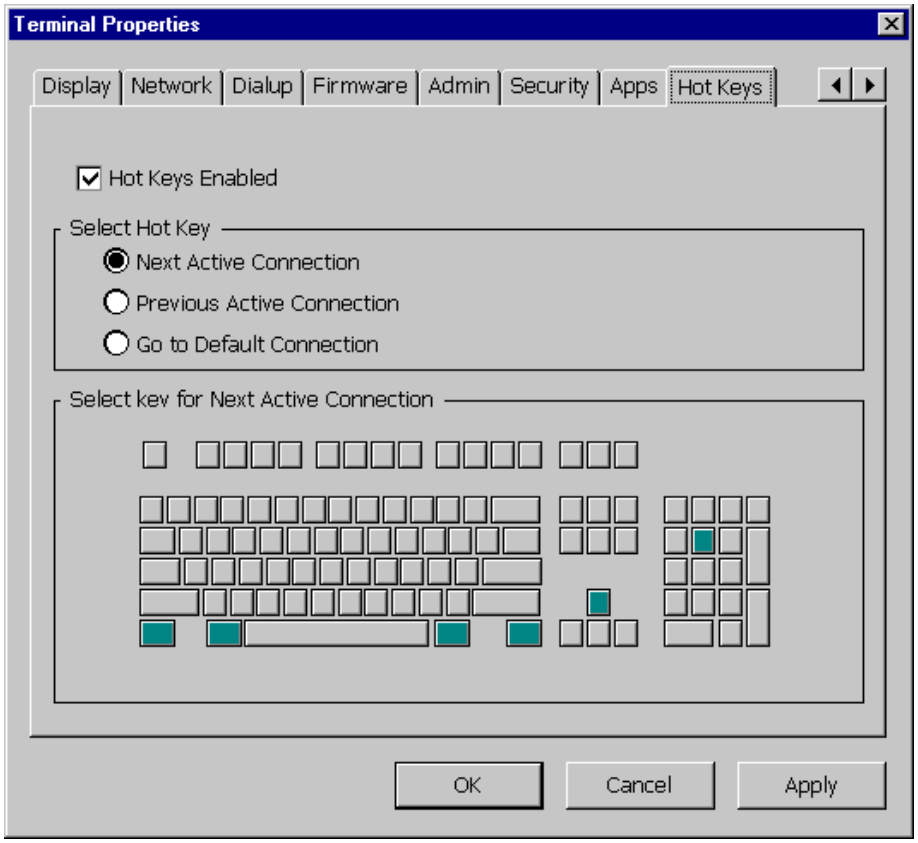
- **ICA**

This button provides access to the global settings for the ICA sessions and is covered in the Citrix ICA section of this manual.



Hot Keys

The Hot Keys tab allows the modification of the key sequence used to switch between connections. The functions of Next, Previous or Default Connection can be mapped from the standard key sequence to a user defined sequence. The key sequence must include one or more of the modifier keys Shift, Alt or Control plus one other key. The sequence is set by selecting or deselecting keys using the mouse.



After configuration, exit the Terminal Properties menu by clicking OK. Reboot the Visara to load the new settings. Once the Visara network configurations are made the Visara is ready to operate as a node on the Ethernet Network. If using manual configurations, all that remains is to configure the connections that will be used to communicate with other servers on the network. These connections configurations are divided into HostConnect Telnet connections, Microsoft RDP connections, Citrix ICA connections and Dialup connections. This configuration is accomplished from the Main Menu.

Chapter 4: Terminal Connection Manager

The Terminal Connection Manager acts as the Main Menu for the Visara terminal functions. In this manual the term "Terminal Connection Manager" and "Main Menu" are used interchangeably.

Use the Main Menu to setup and control your connections and to modify existing connections. This menu is used to manage Microsoft's Remote Desktop Clients (RDC), HostConnect Telnet sessions and Citrix ICA and RAS/ISP Dialup Connections.

Initially, the Main Menu will have no connections configured unless the Remote Configuration function is used. As you create new connections using the Configure tab and setup buttons at the bottom of the window, the new connections appear in the window and display selected information about each connection.

The Visara Main Menu is always active. Once a connection is started, the Main Menu is normally hidden beneath the active connection. When the last active connection is closed, the Main Menu is once again visible. You can also gain access to the main menu through a hot-key sequence of Ctrl + Alt + End.

Navigating Through Open Sessions

The Visara terminal sessions are displayed full screen. In order to switch between sessions and the main menu a series of Hot Key sequences are used to control the active window. A Hot Key sequence requires that all keys in the sequence be in the key down position at the same time. These Hot Key sequences are defined below:

104 Enhanced Keyboard:

Ctrl + Alt + End	Return to Main Menu
Ctrl + Alt + ↓	Go to next session
Ctrl + Alt + ↑	Go to previous session
F2 (from Main Menu)	Go to Terminal Properties
Ctrl + Alt + Home	Go to default session

122 Keyboard:

Ctrl + Alt + End	Return to Main Menu
Alt + Jump	Go to next active session
Alt + Shift + Jump	Go to previous active session
Alt + Shift + Home	Go to default session
F2 (from Main Menu)	Go to Terminal Properties

Configured Connections

The Main Menu shows the connections you have set up and information about each connection.

- Connection Name
- Connection Type
- Status

Connection Control Buttons

Each tab on the Main Menu provides buttons used to start, end, add, delete and edit connections. The Startup button can also be used to configure a connection as the Default Connection or to configure the connection to automatically start at system startup. Double clicking a connection in the Connections tab will start that connection. Double clicking a connection in the configure tab will allow editing of that connection.

Chapter 5: HostConnect Connection Configuration

Connection Types

HostConnect is the application which provides simultaneous connections to a variety of host systems using the Telnet protocol over TCP/IP on an Ethernet network. HostConnect provides TN5250 emulation for access to IBM AS/400 systems, TN3270 terminal emulation for connection to IBM Mainframe systems, and ASCII terminal emulation for connection to RS/6000, DEC, HP and other ASCII host computers. In addition, HostConnect supports the TN5250E and TN3270E protocols, giving you access to advanced features such as device-name selection, sign-on bypass and printing.

Host sessions can be configured to start automatically each time Visara is started or you can start sessions as needed from the HostConnect Desktop or the menu bar in an emulation session. HostConnect session types include:

- **TN5250**

  TN5250 is a full featured emulation of the IBM 5250 twinax terminal and includes support for Field Attributes, Text Assist and other unique 5250 functions.

- **TN3270**

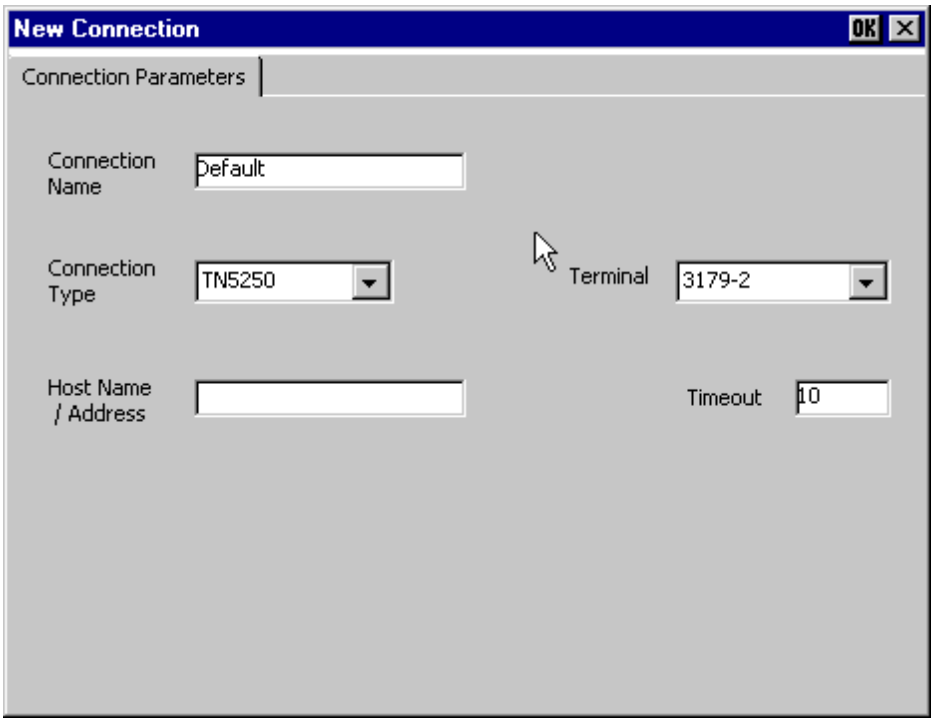
  Emulating the IBM 3278 coax terminal, it includes full terminal emulation support for 3270 keys and the screen attributes of a 3278 terminal session.

- **ASCII**

  HostConnect also provides Telnet IBM 3151, VT100, and 220 terminal emulation in a graphical window. It contains substantial enhancements to the standard VT functions, including local printer support and color command support. These features can be selected either from the pull-down menus or VT command sequences.

Configuring Host Connections

New Connection



Create a new HostConnect connection by clicking the add button in the Configure tab of the main menu, then select HostConnect from the popup window. The New Connection window will be displayed. The following configuration items are also available from the Edit Connection button for existing connections.

Connection Name

Choose a name to identify each connection you configure. The name can be up to sixteen characters long. When you start the connection, the name you chose will be shown in the title bar of the open Session Window.

Connection Type

The connection type is dependent upon the host system to which you will connect. AS/400 hosts typically use TN5250 or TN5250E. IBM mainframes use TN3270 and TN3270E. UNIX and most non-IBM computers use ASCII emulation. To select a Connection Type, click on the down arrow at the right of the drop-down list box and choose the proper Connection Type for your host.

Host Name / Address

The Visara supports Domain Name Services (DNS) names to make connections with network servers. The Host Name/Address field therefore supports DNS names of the host system with which a connection is to be established. For example, the Library of Congress TN3270 server name is "LOCIS.LOC.GOV". This field also supports the IP address of the host system with which a connection is to be established. The Library of Congress IP address for example, is 140.147.254.3.

Terminal Type

HostConnect supports various models of 3270, 5250 and ASCII terminals as described below:

- **5250 Terminals**

  HostConnect supports emulation of a variety of 5250 terminal models, including 132-column mode and Text Assist. If the TN5250E protocol is selected and supported by the host, advanced features such as device-name selection and sign-on bypass are available. In addition, HostConnect supports a printer emulation under TN5250E.

  Emulation of the following 5250 terminal models is included in HostConnect. All models support Text Assist:

Model	Screen Size
3179-2	24 by 80
3180-2	27 by 132
3196	24 by 80
3477-FC	27 by 132
3477-FG	27 by 132
3487-HA	27 by 132
3487-HC	27 by 132
5251-11	24 by 80
5291-1	24 by 80

- **5250 Printer**

  For 5250 printer emulation select connection type TN5250E and terminal type 3812. For additional printer setup information see the section titled Additional Connection Capabilities.

- **3270 Terminals**

  HostConnect supports emulation of a variety of 3270 terminal models and includes support for extended highlighting, extended color, and alternate screen sizes. In addition, if the TN3270E protocol is selected and supported by the host, more advanced features such as device-name selection and reporting and access to the SNA Bind information are enabled.

  Emulation of the following 3270 color and mono terminal models is supported:

Model	Screen Size	EAB
3278-2	24 by 80	Yes
3278-3	32 by 80	Yes
3278-4	43 by 80	Yes
3278-5	27 by 132	Yes

- **3270 Printer**

  For 3270 printer emulation, select connection type TN3270E and Terminal type 3287. For additional printer setup information see the section titled “Additional Connection Capabilities”.

- **ASCII Terminals**

  HostConnect supports emulation of several ASCII terminal models and includes support for double-high and double-wide characters, smooth scrolling and extended highlighting.

  Emulation of the following ASCII terminal models is supported:

Model	Features
VT100	basic ASCII terminal
VT220	double-high and double-wide characters, smooth scrolling and extended highlighting
IBM 3151	

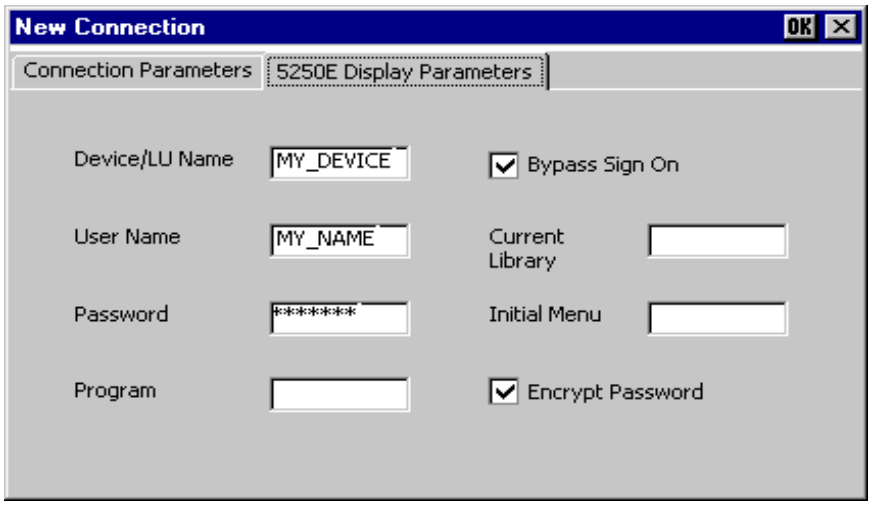
Timeout

The number of seconds HostConnect will wait for a host connection to be established. If a connection is not established within that time, the message “timed out” will be displayed. The default is 10 seconds.

Depending upon the Connection Type you select, additional configuration capabilities may be available.

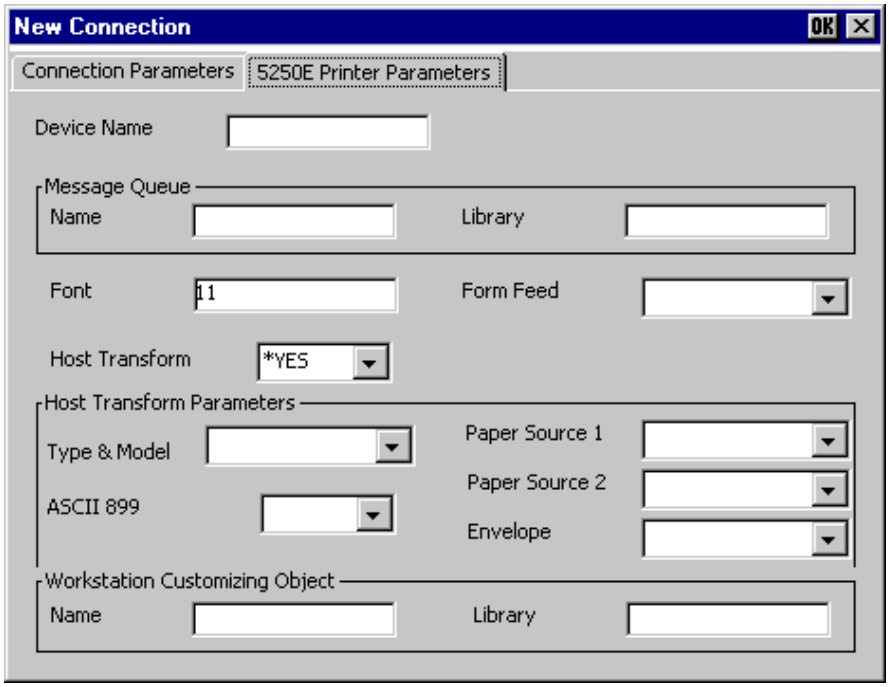
Additional Connection Capabilities

Display Parameters, TN5250E



The 5250E Display Parameter screen allows entry of the session Device or LU Name. If **Bypass Sign On** is also selected, the screen provides input fields to support this function. The **Bypass Sign On** is by default disabled. If you enable Bypass Sign-On, you must enter a User Name and Password. Optionally, you may enter Program, Current Library and Initial Menu. These fields are the same as those displayed on your sign on screen. Optionally you may choose to encrypt your password. When enabled the password is encrypted when transmitted over the network under TN5250E. This is disabled by default.

Printer Parameters, TN5250E



When TN5250E and terminal type 3812 are selected on the Connection Parameters screen a new tab, 5250E Printer Parameters, will be displayed. The 5250E Printer Parameter screen provides fields for entering additional settings for the printer emulation. Once the settings are entered correctly the TN5250E printing will be automatically configured on the AS/400 system. OS/400 versions prior to V4R3 may require certain PTFs. Check with IBM to determine what PTFs you may require to support TN5250E printing. Some fields are required as defined below:

- **Device Name**

  This field entry is required. The name is arbitrary but must be unique. The name will usually be supplied by the System Administrator.

- **Message Queue**

  Not required. This field will identify the message queue where operational messages are sent.

- **Font**

  This field entry is required. The default value is **11**.

- **Form Feed**

  Not required. Identifies the type of forms used.

- **Host Transform**

  This field entry is required. The default value is ***YES**.

- **Host Transform Parameters**

  The Type and Model field is required. This field identifies the attached printer type. If your printer type is not listed use a printer type with a compatible printer command set. The other fields are not required.

- **Workstation Customizing Object**

  Not required. Allows customization of the printer command stream.

Display Parameters, TN3270

Attention Key Action and System Request Key Action. You can override the default action for the Attention or System Request Key while connected to a host system. This would be necessary if the host stops responding to HostConnect and the host also ignores the default Telnet commands it receives when those keys are pressed.

Display Parameters, TN3270E

Enter your device or LU name

Printer Parameters, TN3270E

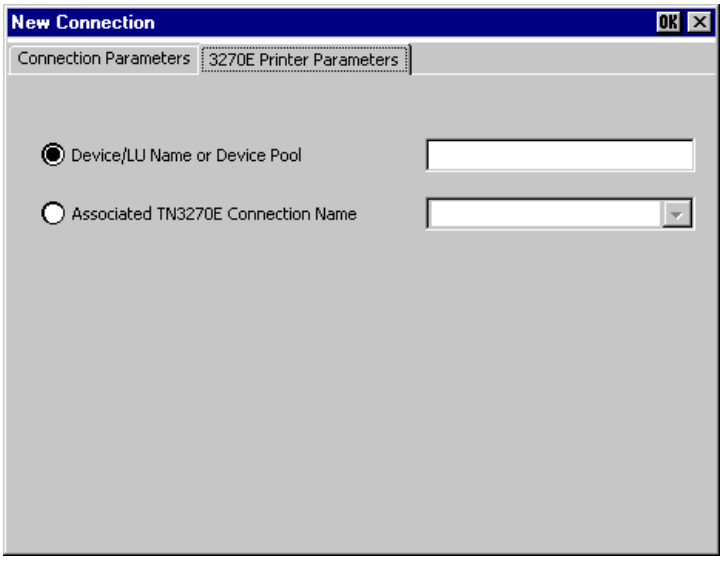
When TN3270E and terminal type 3287 are selected on the Connection Parameter screen, a new tab, 3270E Printer Parameter, will be displayed. The 3270E Printer Parameter screen provides the following options:

- **Device/LU Name or Device Pool**

  Select this option to allow entry of a device name, LU name or device pool in the corresponding field.

- **Associated TN3270E Connection Name**

  Select this option to define a “paired” printer device with a predefined TN3270E terminal. The pulldown field will list all TN3270E terminals that are configured on the Visara Terminal Connection Manager.



Chapter 6: HostConnect Terminal Emulation Session

HostConnect is a Telnet terminal emulation program stored in Read Only Memory (ROM) in the Visara. This enables the Visara to operate as an Ethernet-attached terminal to an IBM mainframe, AS/400 or any ASCII host without having to rely on a remote server in order to start and load emulation software. A Session Window will be visible for each host connection or session that is open. The Session Window consists of a Title Bar, a Menu Bar, the Display area and a Status Area. When you start a connection from the Main Menu, the newly opened Session Window becomes visible and obscures the Main Menu, as well as any other open Session Windows. To open additional sessions on the same host, click on **Session** on the menu bar, then click on **New** in the drop down menu. A subsequent but identically configured session will open on the same host. To switch between new sessions started in this way click on Window in the menu bar then select next or previous.

To move between open sessions on any and all hosts use the Hot Key sequence Ctrl + Alt + ↑ or Ctrl + Alt + ↓ (Alt + Jump or Alt + Shift + Jump for 122 keyboard) to scroll through the open sessions. Ctrl + Alt + End will return to the Main Menu.

Title Bar

The title bar is on the top of the screen and identifies the open session by name. The name is that which was chosen when the connection was configured. If more than one session on the same host and of the same configuration is in use, a dash and an incremental numeral are also displayed to show the number of open connections/sessions.

Session Menu Bar

Items on the Menu Bar are used to customize the session environment, copy or paste text, record or play a macro, open or close sessions, etc. Each option and its use is described below:

Session

Open new sessions; close currently open sessions.

- **New**

  Open additional sessions on the current host using the same configuration information as the current session. The second and all subsequent sessions display the session name on the title bar with the same name as the original session suffixed with incremental numbers.

- **Close**

  Close the current session window. A confirmation window asking, “Are you sure you want to do this?” will be displayed. Click OK to close the window or Cancel to keep the window open.

- **Print Screen Local**

  Send a copy of the currently-displayed host screen to the local (Visara-attached) printer.

- **Print Screen Host**

  Send a copy of the currently-displayed host screen to the default system (host-attached) printer.

- Offline

  Take an ASCII (VT emulation) session offline or put it back online.

Edit

Provides the ability to copy text between terminal emulation sessions.

- **Copy**

  Copy highlighted text from a Session Window into the clipboard. This function can also be performed by clicking on the **Copy** Icon located on the Session Menu Bar.

- **Paste**

  Copy the contents of the clipboard into a Session Window starting at the cursor position. This function can also be performed by clicking on the **Paste** Icon located on the Session Menu Bar. The Paste function will normally initialize a Pop-Up window with termination options for the paste operation. This Window can be disabled by deselecting the **Always Ask** check box on the Pop-Up window. The Paste Options can always be accessed by clicking on the **Options** Icon located on the Session Menu Bar.

Macro

Use this option to record a series of repetitious or lengthy keystrokes which can later be played simply by highlighting the name of the macro and clicking Play.

- **Record**

  Ensure that the cursor is positioned on the screen where you will begin recording your keystrokes. Click Record and a window will open to enter the name of your macro. Choose a name that describes the function the macro will perform and click OK. An accelerator key (F1 - F24) can also be assigned to the macro. Type the keystrokes you wish to record. A counter is displayed to indicate the number of keystrokes that can be recorded. The total buffer size is 5000 bytes. You can Pause recording by clicking Pause. During this time, any keystrokes you type are not recorded in the macro. To resume recording click Resume. When you finish recording click OK.

- **Play**

  Select this option from the Macro dropdown menu to display the list of Macros you have recorded. Highlight the macro you wish to play and click play. A Macro can be deleted by highlighting it and clicking **Delete** to clear the contents of the Macro and remove the Macro from the list.A macro can also be played back with an accelerator key. Press the Alt + F5 (if using the 104 keyboard) or the Play key (if using the 122 keyboard) followed by the assigned Function (F1 - F24) key.

Options

View or change settings that are common across all sessions or across all sessions of the same type as the currently open session.

- **Audible Alarm**
  Select or deselect the audible alarm.

- **Cursor Preferences**
  Choose between blinking or non-blinking; underline, block or half-block text cursor.

- **Attribute Map**
  View or modify the color displayed for any host-defined attribute.

- **Hotspots**
  View or modify your custom hotspot definitions.

- **Keyboard Map**
  View or modify the mapping between any keyboard key and its associated host key.

- **TN5250 (104 key USA keyboard)**

  HostConnect TN5250 uses a combination of keystrokes with host key functions. These defaults are identified in the keyboard map and the table below. You can remap many of these host functions. Changes to the table and keymap can be made or identified by utilizing the keymap function.

5250 Function	Default Keystroke(s)	Host environment
Attention	<Esc>	Standard
Backspace	<Backspace>	Standard
Backtab	<Shift> - <Tab>	Standard
Begin Bold	<Alt> - <B>	Word Processing
Begin Underline	<Alt - <U>	Word Processing
Beginning of Line	<Alt> - <←>	Word Processing
Bottom of Page	<Alt> - <↓>	Word Processing
Carriage Return	<Alt> - <Enter>	Word Processing
Center	<Alt> - <C>	Word Processing
Clear	<Pause>	Standard
Delete	<Delete>	Standard
Down	<↓>	Standard
Down Double	<Alt> - <↓>	Standard
Duplicate	<Shift> - <Insert>	Standard
End Bold or Underline	<Alt> - <J>	Word Processing
End of Line	<Alt> - <→>	Word Processing
Enter	(right) <Ctrl>	Standard
Erase EOF	<End>	Standard
Erase Input	<Alt> - <End>	Standard
F1 - F12	<F1> - <F12>	Standard
F13 - F24	<Shift> - <F1> through <Shift> - <F12>	Standard
Field Exit	<Enter>	Standard
Field Minus	(keypad) <->	Standard
Field Plus	(keypad) <+>	Standard
Half Index Down	<Alt> - <H>	WorProcessing
Half Index Up	<Alt> - <Y>	Word Processing
Help	<Scroll Lock>	Standard
Hex Mode	<Alt> - <F7>	Standard
Home	<Home>	Standard
Insert	<Insert>	Standard
Insert Symbols	<Alt> - <A>	Word
Left	<←>	Standard
Left Double	<Alt> - <←>	Standard
New Line	<Shift> - <Enter>	Standard
Next Stop	<Alt> - <N>	Word Processing
Next Text Column	<Alt> - <D>	Word Processing
Page Down	<Page Down>	Standard
Page End	<Alt> - <P>	Word Processing
Page Up	<Page Up>	Standard
Page CR Mode	<Alt> - <F12>	Standard

Print Screen	<Print Scrn>	Local Function
Required CR	<Enter>	Word Processing
Required Space	<Alt> - <Spacebar>	Word Processing
Required Tab	<Alt> - <Tab>	Word Processing
Reset	(left) <Ctrl>	Standard
Right	<→>	Standard
Right Double	<Alt> - <→>	Standard
Roll Down	<Shift> - <↓>	Standard
Roll Up	<Shift> - <↑>	Standard
Stop	<Alt> - <S>	Word Processing
SysReq	<Alt> - <Print Scrn>	Standard
Tab	<Tab>	Standard
Tab Advance	<Alt> - <T>	Word Processing
Top of Page	<Alt> - <↑>	Word Processing
Test Request	<Alt> - <Scroll Lock>	Standard
Up	<↑>	Standard
Up Double	<Alt> - <↑>	Standard
Word Underline	<Alt> - <W>	Word Processing

- **TN3270 (104 key USA keyboard)**

  HostConnect TN3270 uses a combination of keystrokes with host key functions. These defaults are identified in the keyboard map and the table below. You can remap many of these host functions. Changes to the table and keymap can be made or identified by utilizing the keymap function.

3270 Function	Default Keystroke(s)	Host environment
Alt Cursor	<select from menu>	Local Emulation
Attention	<Esc>	Standard
Backspace	<Backspace>	Standard
Backtab	<Shift> - <Tab>	Standard
Clear	<Pause>	Standard
Cursor Select	<Not Available>	Standard
Cursor Blink	<select from menu>	Local Emulation
Delete	<Delete>	Standard
Dev Cancel	<Not Applicable>	Standard
Down	<↓>	Standard
Dup	<Shift> - <Insert>	Standard, * displayed
Enter	(right) <Ctrl>	Standard
Erase EOF	<End>	Standard
Erase Input	<Alt> - <End>	Standard
F1 - F12	<F1> - <F12>	Standard
F13 - F24	<Shift> - <F1> through <Shift> - <F12>	Standard
Field Mark	<Alt>-<Page Down>	Standard, * displayed
Home	<Home>	Standard
Ident	<Not Applicable>	Standard
Insert	<Insert>	Standard
Key Click	<Not Available>	Standard
Left	<←>	Standard

Left Double	<Alt> - <←>	Standard
New Line	<Shift> - <Enter>	Standard
PA1	<Alt>-<F1>	Standard
PA2	<Alt>-<F2>	Standard
PA3	<Alt>-<F3>	Standard
Print Screen	<Shift>-<Print Scrn>	Standard
Reset	(left) <Ctrl>	Standard
Right	<→>	Standard
Right Double	<Alt> - <→>	Standard
SysRequest	<Print Scrn>	Standard
Tab	<Tab>	Standard
Test	<Not Applicable>	Standard
Up	<↑>	Standard

- **Paste Options**

  View or modify the options for pasting from the clipboard to a Session window.

Connection

View or change settings which are common across all sessions of the same type (5250, 3270 or ASCII) as the currently open session; save or restore those settings.

- **Save**

  Save the session options in the currently open Session Window as the default for all sessions of the same type.

- **Restore**

  Restore the saved session options to the currently open Session Window.

- **Font Size**

  View or modify the selected font size.

- **Reverse Screen**

  Enable or disable the display of the screen with foreground and background colors swapped.

- **Ruler Cursor**

  Select whether the ruler is disabled, locked in position, follows the text cursor or is key activated.. Choose between horizontal, vertical and cross ruler styles.

- **Show Hotspots**

  Enable or disable the display of hotspot text areas as the mouse is moved over them.

- **Show Attributes**

  Enable or disable the display of field attributes in the Session Display Area as two-digit hexadecimal codes.

- **Attribute Type**

  Select which type of field attributes are displayed when Show Attributes is enabled. This option currently only applies to 3270 sessions.

- **Type Ahead**

  Available in TN5250 and TN3270 this capability dynamically allocates RAM to enable continual typing while the HostConnect session is waiting for information from the host. Type Ahead must also be activated on the host.

Window

Use Next or Previous to scroll through the open connections to the same host.

Help

Access the HostConnect version and Copyright information.

Font Select

The Session Menu Bar has a pull down Tab for font size selection. The default selection is **Auto.** This setting selects the largest font that will fit full screen on the Display Area. Other settings can be selected as desired.

Display Area

The Session Display Area is the vertical center of the screen between the Session Menu Bar and the Status Area where all host application data is displayed.

Status Area

The Session Status Area is at the bottom of the Session Window. It provides status information about the session. It may be referred to as the User Information Area (UIA) or Operator Information Area (OIA). Each session type displays status differently.

5250 Status Area

The 5250 status area consists of seven indicators on the left side of the status bar as follows:

- Displays a circle when the session is connected to a host system; this is sometimes called “System Available”.
- Displays an X when input is inhibited, usually because the session is waiting for data from the host system. If instead, input is inhibited due to a user error, a four-digit error code may also be displayed inside the Session Display Area.
- Displays an envelope when your session has a message waiting.
- Displays a caret “^” when Insert mode is active.
- Displays a “d” character in script when Diacritic mode is active.
- Displays a “>>” pair of characters when type-ahead is activated.
- Displays an arrow when keyboard-shift is in effect.

The current row/column position of the text cursor appears to the right of the last indicator followed by a message area.

3270 Status Area

The 3270 status area consists of seven indicators on the left side of the status bar as follows:

- Displays a Red circle when the session has initiated a connection to a host system, but has not yet received a response. The circle turns yellow when a response from the host is received, and connection negotiation is in progress. The circle turns green when the connections established; this is sometimes called “System Available”.

- Displays an X when input is inhibited, usually because the session is waiting for data from the host system. If instead, input is inhibited due to a user error, a four-digit error code may also be displayed inside the Session Display Area.
- When indicator #2 shows that input is inhibited, indicator #3 displays the cause: an hourglass if the session is waiting for data from the host system; a question mark if input is inhibited due to a user error. Also, when input is not inhibited (i.e. indicator #2 is blank), indicator #3 will display a "stick man" when the session is connected to the host SSCP (System Service Control Point) rather than the normal LU-LU connection.
- Displays a caret "^" when Insert mode is active.
- Displays a "d" character in script when Diacritic mode is active.
- Displays ">>" characters when type-ahead is activated.
- Displays an arrow when keyboard-shift is in effect.

The current row/column position of the text cursor is shown to the right of the last indicator followed in left to right order by:

- The IP address of the host system.
- Name for a TN3270E connection or terminal type.
- A message area.

ASCII Status Area

The ASCII status area consists of eight indicators used as follows:

- Displays the terminal type.
- Displays whether ANSI or VT52 control sequences are in use.
- Displays the number of characters per text line.
- Displays an icon indicating whether or not the session is connected to a host system.
- Displays whether or not Auto-Wrap is enabled.
- Displays whether or not the host system has reversed the screen.
- Displays a caret "^" when Insert mode is active.
- Displays an arrow when keyboard-shift is in effect.

The current row/column position of the text cursor to the right of the eighth indicator and four status LEDs, between indicators #7 and #8 (VT100 only)

Chapter 7: Microsoft RDP Client

Introduction

The Microsoft RDP (Remote Desktop Protocol) Client is an integral part of the Windows-based Terminal. The RDP client enables a Visara Windows-based Terminal to connect to a Microsoft Windows NT TSE server to run PC applications. This thin client model provides a high performance, cost-effective, and secure way to deploy, manage, and access business-critical applications throughout an enterprise.

Overview

The RDP client launches remote control sessions on the Microsoft Windows NT TSE server. These RDP are applications that are displayed on your Visara Windows-based Terminal. You can connect to the Microsoft server and run RDP sessions through a local TCP/IP network connection. The Visara is connected to the network that contains Microsoft server using its built-in Ethernet connection.

Creating a New Connection

Connections are created from the Main Menu Configure tab. Select Add and then Microsoft Remote Desktop Client in the New Connection Window. Click OK to access the WTS Connection Wizard. Follow the steps as outlined in the WTS Connection Wizard.

Starting a Connection

Once a connection is configured, highlight the connection in the Connections tab of the Main Menu and click the Connect button to begin the session or, double click on the connection in the Connections tab of the Main Menu.

Chapter 8: Citrix ICA Client for Windows CE

Introduction

The Citrix ICA Client for Windows CE enables a Visara Windows-based Terminal to connect to a Citrix MetaFrame or WinFrame server to run PC applications.

MetaFrame is Citrix's thin-client/server system software for Microsoft's Windows NT 4.0 Terminal Server Edition. WinFrame is Citrix's original thin-client/server software. Both MetaFrame and WinFrame are based on Citrix's Independent Computing Architecture (ICA) and provide a high performance, cost-effective, and secure way to deploy, manage, and access business-critical applications throughout an enterprise.

This document contains procedures for using the Citrix ICA Client for Windows CE on a Visara Windows-based Terminal. Topics covered include:

- ICA Windows CE Client overview
- Creating a new connection
- Connecting to a Citrix server
- Editing connection properties
- Global ICA Windows CE Client settings
- Printing to a local printer

Overview

The ICA Windows CE Client launches remote control sessions, called ICA sessions. *ICA sessions* are applications running on a Citrix server that are displayed on your Visara Windows-based Terminal. You can connect to the Citrix (MetaFrame or *WinFrame)* server and run ICA sessions through a local TCP/IP network connection. The Visara is connected to the network that contains Citrix servers using its built-in Ethernet connection.

You can configure and run two types of ICA sessions: Citrix server connections and published applications.

Citrix server connections allow you to control a session on a Citrix server from your Visara. Citrix server connections let you access the desktop of a specific Citrix server; you can run any applications available in any order.

Published applications are specific applications set up by an administrator. With published application connections, you access only the specified application and do not need to know the address of a specific server to create the connection.

Creating a New Connection

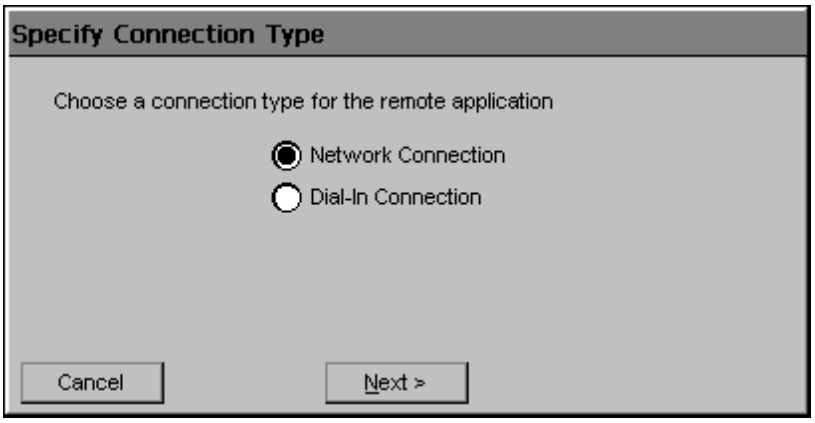
The following procedure describes how to create a network connection to a Citrix server.

Creating a Network Connection

To create a network connection:

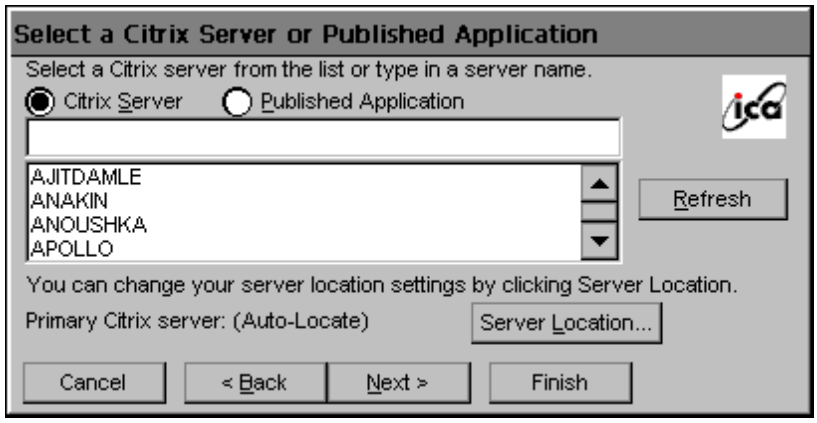
1. On the Visara Main Menu Configure Tab, click on the Add button and select **ICA Client** in the New Connection window.

2. Click **OK** and the Specify Connection Type window will appear:



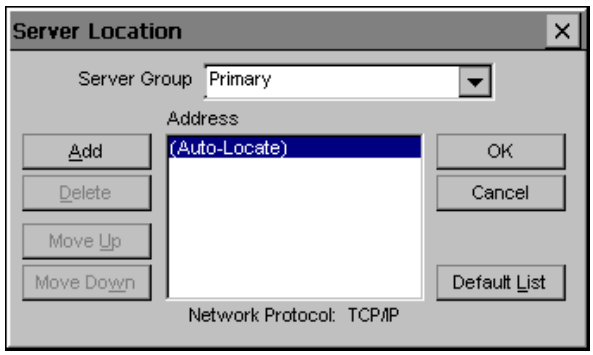
3. Click **Network Connection**. Click **Next** to continue. If your Visara is connected to the network the ICA software will search for, and produce a list of, applicable servers located on the network.

4. The **Select a Citrix Server or Published Application** screen appears:



If your Visara is not on the same network as the Citrix server you want to connect to, the server or published application list will not be displayed. If, for example, you are on the other side of a router from the server, the server and published application list will not contain that server. In this case, click **Server Location** and go to Step 5. Otherwise, scroll through the list and select the Citrix server or published application or type the name of the Citrix server or published application in the edit field. Click **Next** to continue. Go to Step 6.

5. The **Server Location** screen appears:

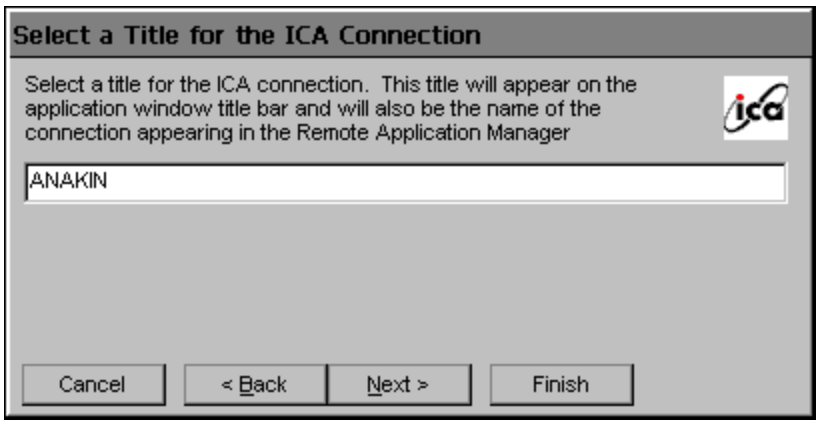


Visara uses the information entered in the **Server Location** dialog to locate available Citrix servers and published applications. The default value entered in the **Address** field is **Auto-Locate**. To use **Auto-Locate**, your Visara and the Citrix server you want to connect to must be on the same local network.

If you are on another network (for example, if you are on the other side of a router or across the Internet) you must enter the IP address or DNS name of a Citrix server on the network that contains the Citrix server you want to connect to.

Click **Add** and enter the IP address or DNS name of any Citrix server on the remote network. Click **OK**. The **Select a Citrix Server or Published Application** screen reappears. Scroll through the list and select the name of the Citrix server or published application you want to connect to. Click **Next** to continue.

6. The **Select a Title for the ICA Connection** screen appears:



By default, the Citrix server or published application name appears in the edit field. You can accept this name or enter another. The name you choose will be the name of the entry in the **Current Client Connections** list and will appear in the title bar of the ICA session window. Click **Finish**.

Once you have created a connection entry, the name appears in the list of connections in the **Visara Main Menu**

Connecting to a Citrix Server

To start a previously defined connection

In the Visara Main Menu, Connections tab, double click on the menu entry for any connection you previously defined or highlight the entry and click the Connect button.

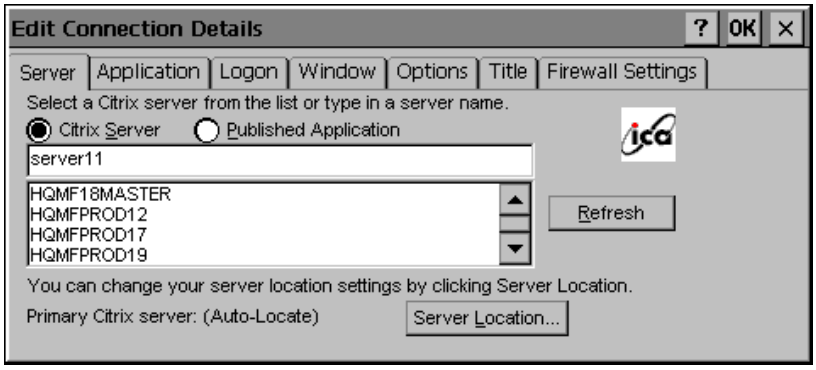
Editing Connection Properties

To edit an existing connection's properties

1. In the **Visara Main Menu** dialog box, click the **Configure** tab.

2. Click the name of the connection entry that you want to change.

3. Click **Edit** to display the **Edit Connection Details** dialog box.



4. Make the desired changes.

5. Click **OK** to save your changes.

The **Edit Connection Details** dialog box contains the following tabs:

The **Server** tab (network connection entries only), where you can set the server or published application name to which to connect. There is also a button to display the **Server Location** dialog box where you can set Business Recovery options.

The **Dial-in** tab (dial-in connection entries only), where you can set the area code, country code, and telephone number to dial. You can use the settings on this page in the same way as when you first set up the connection entry, See "Creating a New Connection Entry" for more information.

The **Application** tab, where you can specify an application to run after connecting to a Citrix server, See " To specify an Application to Run after Connecting to a Citrix Server" for more information.

The **Logon** tab, where you can set the user name, password, and domain to use to log in to the Citrix server automatically, See "To specify Logon Information" for more information.

The **Window** tab, where you can set the number of colors used for the ICA Client window, See "Changing the Window Properties" for more information.

The **Options** tab, where you can control the connection between the Citrix server and the Visara and configure sound support, See "To Set Connection Options" for more information.

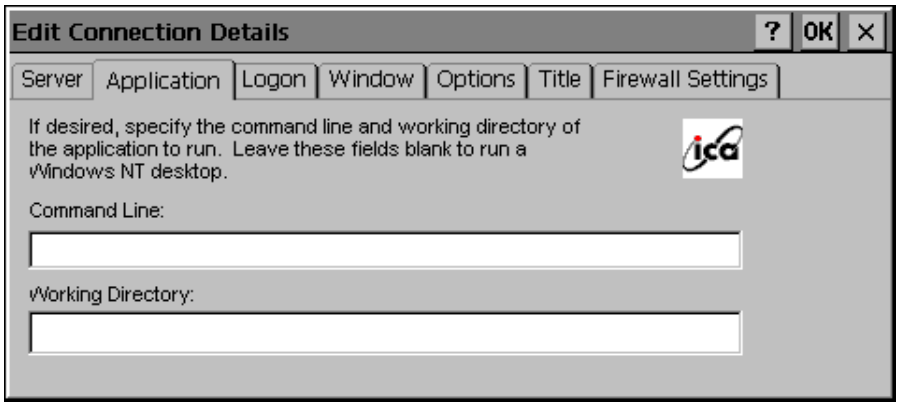
The **Title** tab, where you can change the name of the connection. The name appears in the list in the **Connection Manager** dialog box.

The **Firewall Settings** tab, where you can configure the client to use a SOCKS proxy and alternate address remapping, See "To configure Firewall Settings" for more information.

To specify an application to run after connecting to a Citrix server

Use the **Application** tab to specify an application to run after connecting to a Citrix server. If you specify an application, you do not see the Windows desktop when you connect and the connection is closed when you exit the application.

Note: This tab does not apply to connection entries for published applications. Any values entered are ignored.



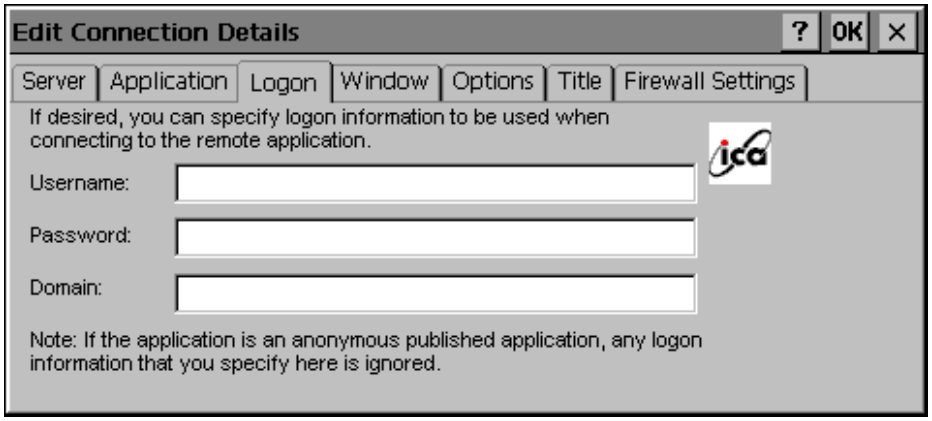
In the **Command Line** field, enter the path and name of an application to run on the server once the logon to the Citrix server is successful. Leave this field blank to run a Windows NT desktop on the Citrix server. **Working Directory** lets you associate a directory with the application specified in the **Command Line** field. Enter the drive and path of the working directory in the **Working Directory** field.

For example, if the application Notepad.exe is in the C:\WTSRV directory on the Citrix server, type **C:\WTSRV\Notepad.exe** in the **Command Line** field. If you use Notepad to work on documents in the C:\My Documents directory, type **C:\My Documents** in the **Working Directory** field. When you log on to the Citrix server, Notepad begins. In Notepad, if you click the **File** menu, the directory C:\My Documents is displayed. Click **Ok** to save your changes.

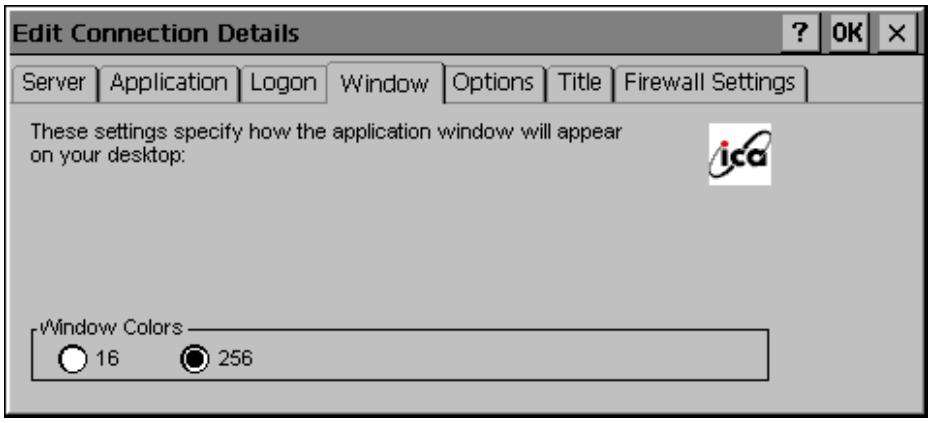
To specify logon information

Type a valid username, password and domain. If you leave these fields blank, you are prompted for your username, password and domain when the ICA Client connects to the Citrix server.

Click **Ok** to save your changes

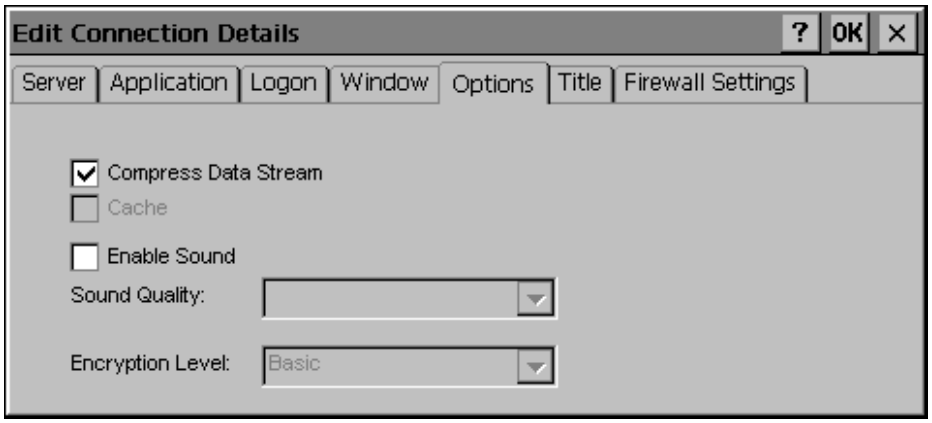


To specify the Window properties for a connection entry



In the **Window Colors** field, select 16 or 256 colors. Click **Next** to continue.

To set connection options



Click **Compress Data Stream** to reduce the amount of data transferred between the Visara and the Citrix server hosting the session. (If your connection is bandwidth-limited, enabling compression may increase performance. If your Visara is on a high-speed LAN, you may not need compression.)

The **Cache** feature is not supported in this release.

Click **Enable Sound** to enable sound support. Remote applications will be able to play sounds on your client. From the pull-down list, select a sound presentation quality level. Full sound support requires external speakers.

High provides the greatest audio quality but should only be used when bandwidth consumption is not a concern.

Medium results in less bandwidth consumption than when using **High**. Compression of sound data provides greater bandwidth efficiency but reduces sound quality somewhat. This value is recommended for most LAN-based connections.

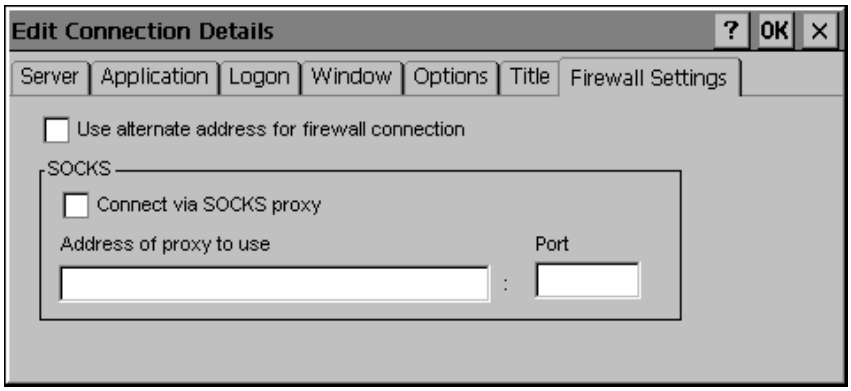
Low offers the most efficient use of bandwidth but also decreases sound quality severely. This value is recommended for low-bandwidth connections, including most modem connections.

The **Encryption Level** feature is not supported in this release.

Click **Ok** to save your changes.

To configure Firewall Settings

If you are using a SOCKS proxy server to limit access to your Citrix servers, you must configure the Visara ICA Client to connect to Citrix servers through a SOCKS proxy server. You can configure a default SOCKS proxy for all connections or use only a SOCKS proxy with a specific connection file.



To configure a SOCKS proxy server

1. Click **Connect via SOCKS proxy**.

2. In the **Address of proxy to use** box, enter the SOCKS proxy server's IP address.

3. In the **Port** box, enter the proxy server's port number (if different than 1080).

4. Click **OK** to save your changes.

Configuring Alternate Address Translation

If the Visara is outside a firewall that uses address remapping, you must configure the Visara ICA Client to use the alternate address returned by the master ICA Browser. This is necessary even if you are not using a SOCKS proxy server.

☞ **Note:** You must also use the ALTADDR utility to manually set the alternate address for each Citrix server, See the Command Reference appendix of either the *MetaFrame Administrator's Guide* or the *WinFrame System Guide* for more information.

☞ **Note**: If you set alternate address translation for all connection entries, it cannot be disabled for specific connection entries.

Global ICA Windows CE Client Settings

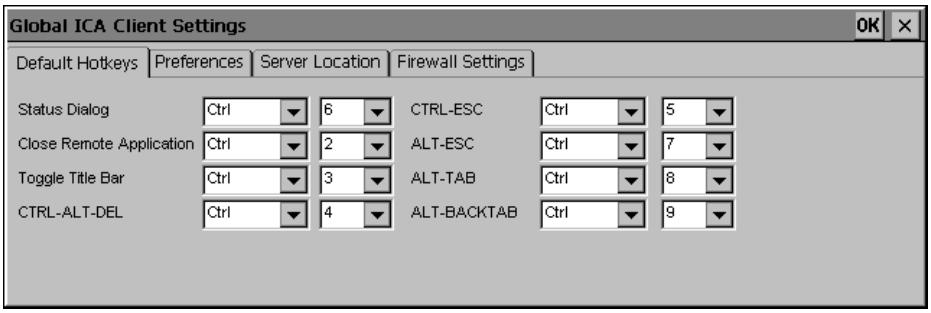
The **Global ICA Client Settings** dialog box lets you define the default settings for all remote application entries. You can override some of these global settings by choosing your own values when creating a new connection or by using the **Connection Manager Configure** dialog box. The **Global ICA Client Settings** dialog box contains four tabs: **Default Hotkeys**, **Preferences**, **Server Location** and **Firewall Settings**.

To access the Global ICA Client Settings dialog box

1. Hit the F2 key from the Main Menu.
2. Select the Apps tab in the Terminal Properties screen.
3. Click on the Change Global ICA Client Settings button.

Default Hotkeys

The ICA Windows CE Client provides hotkeys that can be used during ICA sessions to control various functions. Some hotkeys control the behavior of the ICA Windows CE Client itself while others emulate



standard Windows hotkeys.

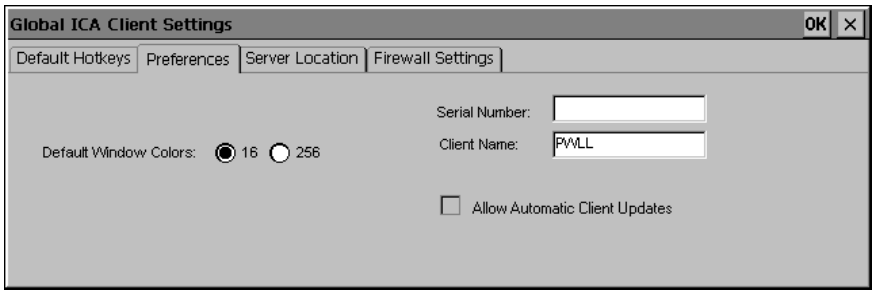
Use the pull-down boxes in the **Default Hotkey** tab to customize the default hotkey key sequences.

The following table describes ICA Windows CE Client hotkeys. The first column lists the hotkey's name or the name of a standard Windows hotkey. The second column lists the key sequence used to produce the hotkey in your ICA session, and the third column describes the hotkey's behavior.

Function	Key Sequence	Description
Status Dialog	CTRL+6	Displays ICA Windows CE client connection status.
Close Application	CTRL+2	Disconnects the ICA Windows CE Client from the Citrix server and closes the client window on the local desktop. Using this hotkey leaves the ICA session running in a disconnected state on the Citrix server. If you do not want to leave your session running in a disconnected state, log off instead.
Toggle Title Bar	CTRL+3	Alternately hides and displays the client window title bar. Use the title bar to drag the client window to different positions on the local desktop. Remove the title bar to maximize your work space.
CTRL-ALT-DEL	CTRL+4	Displays the **Windows NT Security** dialog box for the remote desktop.
CTRL-ESC	CTRL+5	On *WinFrame* servers, this hotkey displays the remote Task List. On MetaFrame servers, the remote Windows NT **Start** menu appears.
ALT-ESC	CTRL+7	This hotkey cycles the focust hrough the minimized icons and open windows of applications run in your ICA session.
ALT-TAB	CTRL+8	This hotkey cycles through applications that have been opened in the ICA session. A popup box appears and displays the programs as you cycle through them. The selected application receives keyboard and mouse focus.
ALT-BACKTAB	CTRL+9	Like the ALT+TAB hotkey, this key sequence cycles through applications that have been opened in the ICA session but in the opposite direction. The chosen application receives keyboard and mouse focus.

Preferences

Use the **Preferences** tab to change the default window color and other settings.



The **Preferences** tab contains the following fields:

Serial Number. This is the serial number of your ICA Client software. This field is only necessary when you are using the ICA Windows CE Client with a product such as *WinFrame* Host/Terminal, which requires each client to have a Citrix PC Client Pack serial number in order to connect to the server. If a serial number is required, you must enter it exactly as it appears on the Serial Number card. The **Serial Number** field is not used by MetaFrame servers.

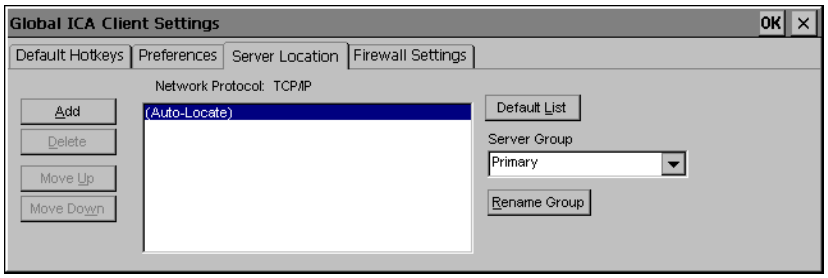
Default Window Colors. In the Window Colors field, select 16 or 256 colors. If the window options specified exceed the capabilities of the hardware, the maximum size and color depth supported by Visara are used instead.

Client Name. This text box allows you to change the client name of your client device. The Citrix server uses the client name to uniquely identify resources (such as mapped printers) associated with a given client device. The client name should be unique for each computer running a copy of a Citrix ICA Client. If you do not use unique client names, device mapping and application publishing may not operate correctly. The default value is the MAC address (unique ethernet interface board ID) of the Visara.

Allow Automatic Client Updates. This feature is not supported in this release.

Server Location

The ICA Windows CE Client uses the information entered in the **Server Location** tab to locate available Citrix servers and published applications.



The default value entered in the list is **Auto-Locate**. **Auto-Locate** automatically searches your network for the Citrix server that maintains the list of available Citrix servers and published applications. To use **Auto-Locate**, your Visara and the Citrix server or published application you want to connect to must be on the same local network.

If you are on another network (for example, if you are on the other side of a router or across the Internet) you must enter the IP address or DNS name of a Citrix server on the network that contains the Citrix server or published application you want to connect to. Visara uses this server to locate the list of available Citrix servers and published applications on the network.

Use the **Add** and **Delete** buttons to add or delete Citrix servers from the **Address** list. Use the **Move Up** and **Move Down** buttons to order the list of Citrix servers used for server location. The higher the server appears in the list, the higher its priority for server location.

You can define a list of servers to contact to determine the master browser. Up to three groups of Citrix servers can be defined to which you want to contact: a primary and two backups. The client attempts to contact all the servers within the Primary group using directed packets; the first server to respond is then queried for the address of the master ICA Browser. If none of the servers respond, the client attempts to contact all the servers within the Backup 1 group. If there is still no response, the client attempts to contact all of the servers in the Backup 2 group. This process is repeated each time the user attempts to make an ICA connection.

These options can be set for a particular connection entry or all connection entries. If both are set, the settings for the connection entry are used.

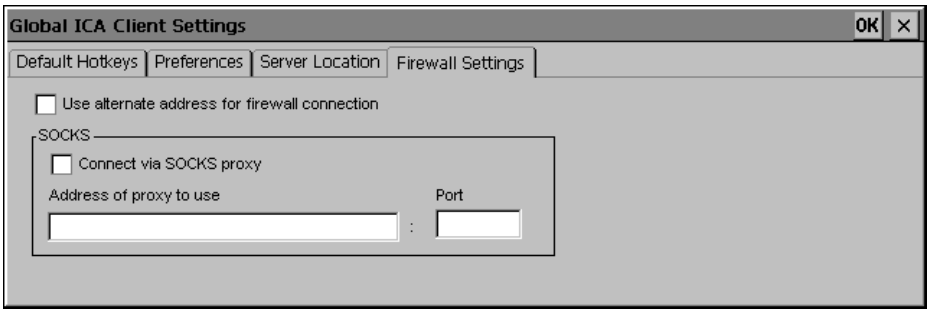
To set Business Recovery options for all connection entries

1. Click **Add** to add a server to the selected group. The **Add Server Address** dialog box appears.
2. Type the name or address of a Citrix server and then click **OK**.
3. Add more servers as necessary.
4. Click **OK** to save your changes.

Firewall Settings

If you are using a SOCKS proxy server to limit access to your Citrix servers, you must configure the Visara ICA Client to connect to Citrix servers through a SOCKS proxy server. You can configure a default SOCKS proxy for all connections or use only a SOCKS proxy with a specific connection file.

To configure a default SOCKS proxy server



1. Click **Connect via SOCKS proxy**.
2. In the **Address of proxy to use** box, enter the SOCKS proxy server's IP address.
3. In the **Port** box, enter the proxy server's port number (if different than 1080).
4. Click **OK** to save your changes

Note: If you configure a default SOCKS proxy server, you must specify at least one server in the **Server Location** tab for server and published application browsing to work.

Configuring Alternate Address Translation

If the Visara is outside a firewall that uses address remapping, you must configure the Visara ICA Client to use the alternate address returned by the master ICA Browser. This is necessary even if you are not using a SOCKS proxy server.

To use alternate address translation for all connection entries:

1. Click **Use alternate address for firewall connection**.

2. Click **OK** to save your changes

Printing to a Local Printer

You can print to a printer attached to the LPT port of your Visara.

To print to a local printer in MetaFrame

1. After login to the Citrix server, click **Start** on the taskbar; point to **Settings**; click **Printers** on the submenu.

2. In the **Printers** window you should see an icon for a network printer with a name similar to ***clientname#port***, where ***clientname*** is the name you have assigned to your Visara (on the Global ICA Client Settings Preference Tab) and ***port*** is the printer port on your Visara, for example LPT1.

3. If no client printer is available, double-click the **Add Printer** icon in the **Printers** window to run the **Add Printer Wizard**.

4. Click **Network printer server,** then click **Next**.

5. Double-click **Client Network**, and double-click **Client**.

6. Select the printer from the list displayed, and click **OK**. Note, Device LPT2 is not supported.

7. Printer ports available on the Visara have a name similar to ***clientname#port***.

8. Select the manufacturer and printer type for the printer to be installed and click **OK**.

9. If you want this printer to be your default printer, click **Yes,** then click **Next**.

10. Click **Finish** to complete the process.

To print to a local printer in *WINFRAME*

1. In the **Main** program group double-click the **Print Manager** icon. In the **Printer Manager** window you should see an icon or open dialog box, for a network printer with a name similar to ***clientname#port***, where ***clientname*** is the name you have assigned to your Visara and ***port*** is the printer port on your Visara, for example COM1 or LPT1.
2. If no client printer is available, select **Create Printer…** from the **Printer** menu.
3. The **Printer Name** should be pre-configured with the client name from the **ICA Global Preferences** in Terminal Properties.
4. Select your printer from the **Driver** pull down field.
5. The **Print To** field should be set for **Client\LPT1:**, click **OK**.
6. If you want this printer to be your default printer, select it in the **Default** menu at the top of the **Printers** window.

Appendix A: Remote Configuration

Remote Configuration Of Connections

Remote Configuration allows the Visara to handle Account/User Based connection configurations. This is a very powerful feature for management of the Visara configurations from a central location and allows pre-configuration of the Visara connections prior to installation. These connection configurations are downloaded to the Visara at startup.

Connection configurations determine what servers the user accesses and the type of connection used for access. Account/User Based connection configurations allow the user to use any Visara on the network while retaining their connection configuration. Configurations can be setup on a user or department basis as required. The configurations are stored on a central server and are downloaded to the Visara based on the Account name used at Visara boot time. This feature can be disabled to use internally stored connection configurations.

Remote Configuration Setup

Use of Remote Configurations is pre-configured as active on a new Visara. In order for this feature to function correctly a configuration must have been previously saved to the appropriate server directory and the server must be configured to support FTP (a standard file transfer protocol). When using DHCP, the Remote Configuration Utility will default to the DHCP server for the Remote Configuration information and will try to down load the configuration information from that server. In order to minimize setup requirements, one Visara can be configured and the configuration settings then uploaded to the appropriate server and directory.

Server Setup for Remote Configuration

The server used to store the Remote Configuration files must support FTP file transfers and FTP must be enabled. In addition, the Visara default username and password for FTP transfers must be setup on the server by the System administrator. Using the default Username and password along with the default directory structure will allow Plug and Play installation of new Visaras into the Network. The Visara defaults are:

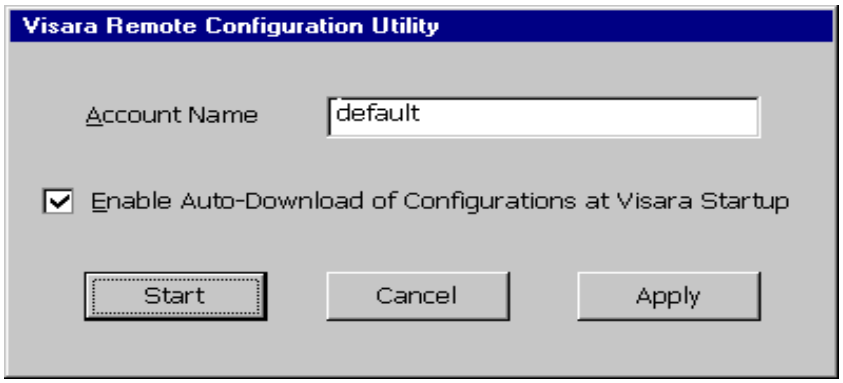
Username	visara
Password	visara
Directory	/visara1/userswbt

To access the configuration file the Visara will append the account name to the directory structure. Therefore, a user using the account name *sales* would have a full directory path of visara1/userswbt/sales. When establishing the FTP directory and uploading the configuration be certain to append the account name to the directory path.

The default settings can be changed but this will require entering the new settings into each Visara when a new configuration is to be downloaded. We recommend setting up the FTP username visara with read only access. When uploading settings, the system administrator can use another username and password to upload configurations to the appropriate directories. The upload utility will not establish new directories, these must be pre-established by the system administrator prior to uploading.

Uploading Configuration Files

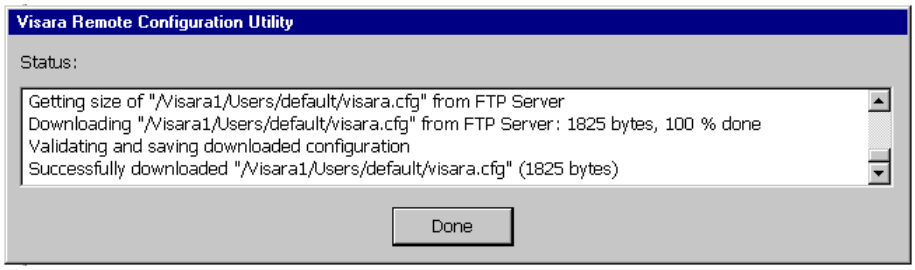
The ability to upload a Visara's configuration files provides a convenient method of managing the connection configurations for all Visaras on the network. A system administrator can configure one Visara unit and then make that same configuration available to all units through the Remote Configuration capability. Once a Visara has been configured the upload capability can be started through the Admin tab on the Terminal Properties page. After starting the Visara perform the following:



Click Cancel on this Remote Configuration Utility window to access the Visara Main Menu. Use the Configure tab on the Main Menu to setup the appropriate connections. Use the F2 key to access the Terminal Properties Page and select the Admin tab.

To upload the current connection configuration from the Visara to the server, insert the correct FTP Servers DNS name or IP address and insert the path name for the directory path on the server. Note, the last entry in the directory path must be the account name that will be used by the user when starting the Visara and the directory path must already exist on the server. The Login Name and Password fields provide the Username and Password for the FTP function on the FTP server. When the server settings are correct click the "**Apply**" button to begin the "**Upload**".

The Remote Configuration status window will open providing FTP status on the transfer.



Configuration and Upload, Step By Step

1. Connect all Visara cables and turn on the power.

2. The Visara Remote Configuration Utility dialog box will display.

3. Click **Cancel,** the Visara Remote Configuration Utility startup window will close. Configure using the Setup Wizard if not previously configured and the Main Menu will appear.

4. Create the connection(s) which will be used by this Account (see Chapter 3, Terminal Emulation Configuration)

5. Use the F2 key to access the Terminal Properties page and select the 1. Admin tab.

6. The Admin window will display with the Configuration FTP Server settings.

7. Check the FTP Server settings to be certain they match the server address and path for your FTP server.

8. Append the correct Account name to the Server Path. This is the name the user will use as an account name at startup.

9. Click **Apply**.

10. Click the "**Upload configuration now**" button to perform the upload function.

11. In the Status window, watch for the message, Successfully uploaded "/Visara1/userswbt/<Account Name>/Visara.cfg" (### bytes)

12. When this message appears the Cancel button will change to Done.

13. Click **Done** and you will return to the Terminal Properties page.

14. Select the Admin Tab again. Remove the Account name from the Server path. Click **Apply**.

To test your settings use a new Visara with the account name and FTP server settings you have established. The FTP status window will provide FTP transfer status and a successful download message upon completion.

Running Remote Configuration at startup

At startup of a new Visara, the first window to open after the Setup Wizard will be the Remote Configuration Utility startup window. This window provides a means to specify the account name or user configuration files to download. The window also allows for disabling of the Remote Configuration feature.

When using DHCP for IP address assignments it is possible to attain a true Plug and Play environment for Visara installation. Simply setup the DHCP server as the FTP server for Remote Configuration download. Upon startup the user will enter the account name into the Remote Configuration startup window and click on the start button. The Remote Configuration Utility will assume the DHCP server is the FTP server and begin the download function. The startup window will close and the download is performed. If the download cannot be completed successfully a status will be displayed in the Remote Configuration status window.

If DHCP is not being used or you wish to setup an alternate server as the configuration download server then the server DNS name or IP address must be entered. This is done from the Admin tab on the Terminal Properties Page. This window also allows entry of the directory path to the configuration file. In download operations the account name from the Startup window is appended to this path to complete the directory path to the location of the configuration file (**visara.cfg**).

Appendix B: Firmware Update

Network Update of Application or Operating System

Firmware Update allows the Visara to be updated over the network connection through FTP download of Boot Code, applications or the operating system. This feature allows the administrator to maintain and update all the Visara systems on the network from a central location.

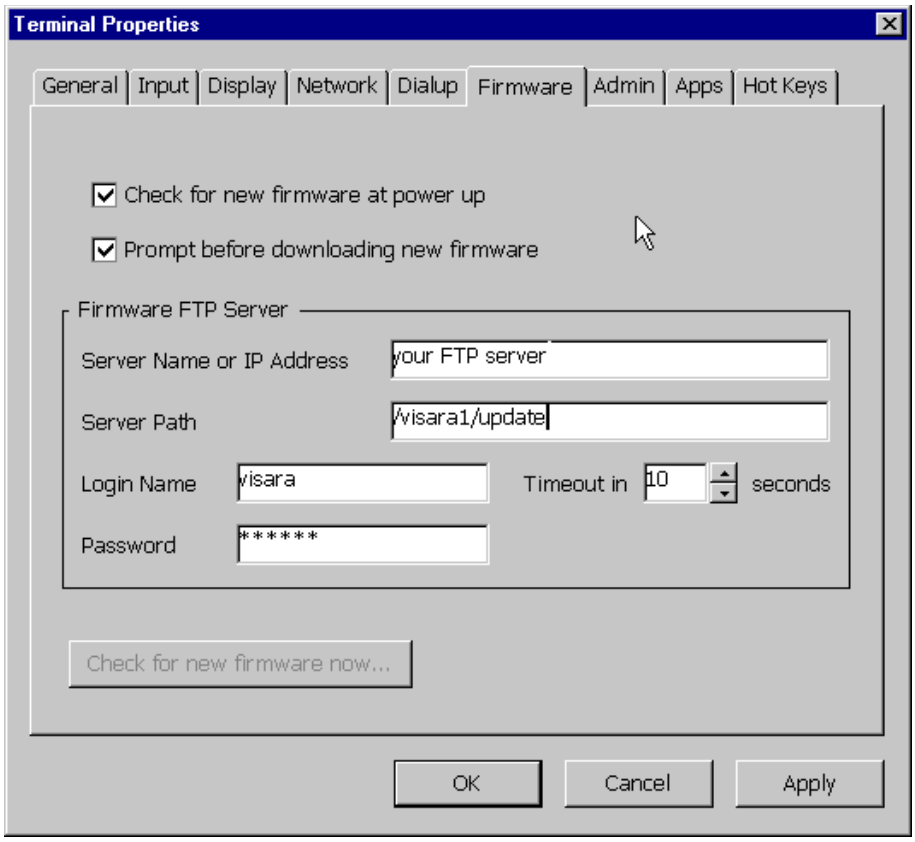
The Firmware Update function can be set to run automatically or it can be run only when required. Automatic updating requires no operator intervention. The settings for the Firmware Update function are handled by Remote Configuration and can be setup through this utility.

Firmware Update Setup

Firmware Update is pre-configured as inactive on a new Visara. In order for this feature to function correctly the appropriate server directory and the server must be configured to support FTP (a standard file transfer protocol). When using DHCP, the Firmware Update function will default to the DHCP server and if enabled will try to down load the update information from that server. In order to minimize setup requirements the administrator should consider the use of the Visara default parameters or use the Remote Configuration utility to setup additional units.

Server Setup for Firmware Update

The server used to store the Firmware Update files must support FTP file transfers and FTP must be enabled. In addition, the Visara default username and password for FTP transfers should be setup on the server by the System administrator. An alternate server and FTP settings can be used but each Visara will need to be configured with these new settings. The settings can be verified or changed from the Firmware tab of the Terminal Properties page.



The FTP defaults are:

Username	visara
Password	visara
Directory	/visara1/update

The default settings can be changed but this will require entering the new settings into each Visara when a new configuration is to be downloaded. We recommend setting up the FTP username visara with read only access.

Running Firmware Update at startup

At startup of a new Visara, the Firmware Update feature is disabled. The feature can be enabled through Remote Configuration or through the Firmware tab on the Terminal Properties page. When enabled, Firmware Update runs immediately after the Remote Configure utility at boot time. When enabled, the Visara will check the configured server for an ASCII text file that identifies any updates loaded on the server. If the Visara is configured to prompt the user prior to updating the software it will do so, otherwise it will proceed with the update operation. After any updates the Visara will reboot.

Firmware Update can consist of three different sets of software:

Boot Flash Code: Initializes hardware

Operating System: Windows CE O/S

Applications: HostConnect, Remote Config, Firmware Update

The file **visara.txt** contains version numbers that are used to indicate what software is available for download.

Appendix C: Dialup

Connecting the Visara to a RAS or ISP

The Visara can be connected to a server or to the Internet using a standard Hayes-compatible modem.

Dialing Rules

This tab specifies the settings for the location from which the Visara will call from.

Current location: Select the location where the Visara is calling from.

Local country code: Enter the local country code where the Visara is calling from.

Local area/city code: Enter the area code where the Visara is calling from.

Cancel call waiting: Enable this check box if your phone line supportsthe Call Waiting feature.

Dialing Patterns: Type the number (normally 8 or 9) required to accessand outside line.

Tone/Pulse Dialing: Select the type of dialing.

RAS / ISP Phonebook

This tab contains sub-tabs that pertain to the host connection (RAS or ISP) information such as telephone number, outside line, dialup userID and password, etc.

- **Devices**

  Select the Connection type to the host: modem or direct. Depending on the Connection Type, the Device Name field indicates a Hayes-compatible modem or a serial cable connected to COM1 of the Visara.

- **Dial Info**

  Enter the host phone number: country code, area/city code and telephone number.

Use Default Dialing rules**:**	Select this option if you have configured the Dialing Rules tab.
Force Long Distance Call:	Select this option if you want to disregard the Dialing Rules and only use the numbers entered on the Dial Info tab.
Force Local Call:	Select this option if you want to disregard the Dialing rules and only use the numbers entered in the Telephone field.

- **Dial Options**

Manual Dial**:**	Select this option if the telephone number is to be entered manually by the user.
Use Terminal Window before dialing**:**	Select this option if there is a need to send commands directly to the modem before dialing.
Use Terminal Window after dialing**:**	Select this option if there is a need to send commands directly to the modem after dialing or to interact with the remote host.
Wait for Dial tone:	This option is enabled by default. Clear this option if you have to dial the phone manually.
Wait for Credit Card Tone:	This option is disabled by default. It specifies how many seconds to wait for a credit tone dial before continuing dialing.

Cancel Call if not connected within x seconds:	This option is enabled by default.
Extra Modem Commands**:**	Enter modem initialization commands here. Example: m0 to turn off the modem speaker.

- **User Info**

User Name**:**	Enter a valid user name that will be used to automatically login to the RAS Server or ISP.
Password**:**	Enter a valid password that will be used to validate the user on the RAS Server or ISP.
Domain**:**	Enter a valid domain name for the RAS Server.

- **IP Addresses**

Use Server-assigned IP address:	The Visara uses the IP address received from the host.
Specific IP:	Enter a specific IP address to be used by the Visara for this dialup connection..
Use Server-assigned DNS and WINS Server addresses**:**	The Visara uses the IP addresses for the DNS and WINS Servers assigned by the host.
Primary/Secondary DNS and WINS Server addresses:	Enter specific IP addresses for the DNS and WINS to be used by the Visara for this dialup connection.

- **TCP/IP Options**

Use software compression:	Enables the data to be compressed in order to speed up transmission.
Use IP header compression:	Optimizes data transfer between the Visara and the host.
Use default gateway on remote network:	If selected, then IP traffic is routed to the WAN connection.

Framing Protocol

- PPP: Select this option to use point-to-point protocol to the remote host.
- SLIP: Select this option to use serial line interface protocol to the remote host.
- RAS (Async NetBEUI): Select this option if dialing a RAS Server running Windows NT3.1 or Windows for Workgroups 3.11

Authentication

- Accept any authentication including clear text: Select this option if you are not concerned with passwords or dialing a non-Microsoft host.
- Accept only encrypted authentication: Select this option if dialing a non-Microsoft host and do not want clear text passwords to be seen on the communications line.
- Accept only Microsoft encrypted authentication: Select this option if dialing a Microsoft host and the Microsoft MS-CHAP authentication is to be used.

Modem / Port Setup

This tab pertains to the settings for the communications port COM1. If connected to a modem, the default settings (Baud Rate = 19200, Parity = None, 8 Data bits, 1 Stop bit,) should be sufficient.

- **Flow Control**:

Hardware:	Uses RTS/CLS handshake to control the flow of data between the modem and Visara. The cable between the modem and the Visara needs to support hardware flow control. This is the default setting.
Software:	Uses XON/XOFF handshake to control the flow of data between the modem and Visara.
None:	There is no handshake between the modem and the Visara.