

CETerm | CE3270 | CE5250 | CEVT220

User's Manual

For version 5.7.0 or later

Copyright Notice

This document may not be reproduced in full, in part or in any form, without prior written permission of Naurtech Corporation.

Naurtech Corporation makes no warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Naurtech Corporation, reserves the right to revise this publication and to make changes to it from time to time without any obligation to notify any person or organization of such revision or changes.

Trademarks

CETerm[®], CE3270[™], CE5250[™], CEVT220[™] are trademarks of Naurtech Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Software Version

This user's manual is for version 5.7.x of Naurtech CETerm Industrial Web Browser and Terminal Emulation (TE) application. This manual also applies to CEVT220, CE5250 and CE3270 products.

Table of Contents

Preface	6
Assumptions	6
Conventions used in this Manual.....	6
Additional Documentation.....	7
Online Support Wiki	7
Introduction	8
What's New in version 5.7.....	10
Feature Highlights & Benefits	12
Benefits of Naurtech Terminal Emulators & Industrial Web Browser	19
System Requirements	20
Installation.....	21
Quick Start.....	22
Quick "How To" Tips	23
Automatically submit a barcode (Postamble ENTER)	23
Change the font to fit rows and columns on the screen	23
Configure a session to automatically connect on startup.....	23
Setup Automatic login	23
Remap hardware keys	23
Configure Full Screen mode.....	24
Lock down the device	24
Display Indicators	24
Configure to display International language character sets	24
Enable SSL / SSH security.....	25
Exiting out from the registration dialog	25
Automatic Licensing Registration	25
Evaluation Mode	26
Software Registration	27
Product Version	29
Application Menu	30
Application Toolbar	32
Configuration	33
Connection	33
General.....	36
Network	38
Security.....	40
SSH Secure Shell	40
General.....	41
Encryption.....	48
User Keys	50
Server	51
Proxy	52
IBM Options.....	55
VT Modes	57
VT Options.....	58
VT Extensions	60
Display	62
Hide / Show	65
Colors	67

Cursor	68
Font	70
Printer.....	71
Serial Config	72
Bluetooth Discovery	73
Network Printer	73
Options.....	75
Configure KeyBars and Keys	77
Configure Scripting	86
General Settings.....	86
Editing Scripts	87
Access	89
Info Items.....	90
Manage (Automated Licensing)	92
Touch.....	93
Scanner	95
Symbology	97
Automated Licensing	99
Session Interaction	101
Multiple sessions	101
Password protection.....	102
Connecting / Disconnecting from Host.....	102
Auto-Launch when device boots	103
Auto-Start a host Session.....	103
Network Check on Connect.....	103
Run a Script.....	104
Use barcodes to invoke Operations or Keystrokes	104
Display Indicators (Digital Clock, RF & Battery Strength ...)	105
Display device parameters (Serial #, MAC address, Battery ...)	105
Play a different audio tone / sound on my device	106
Key Remapping and Configuration.....	107
Keyboard Key Remapping	107
Meta Keys.....	109
Configurable KeyBar	111
KeyBar Button Images	113
Remapping Application keys	116
5250 Host key descriptions	119
VT Host key descriptions.....	120
Default VT Keys Escape Sequence Table	122
Creating Context Menus.....	123
Hotkey shortcuts	124
Access Control / Device Lockdown	125
Device Lockdown	125
Full Screen Mode	126
Accessing configuration from Full Screen mode.....	126
International Character Set & Code Pages	127
Code pages for IBM emulations (3270 & 5250)	127
Code pages for VT emulations.....	128
Asia Pacific language character sets	128
Web Browser Sessions	130
Macros	132
Recording	133
Playback	133

Creating a Mini-Macro	134
Printing.....	135
VT printing	135
Legacy Extended commands	135
Printing to a Network / 802.11x WiFi printer.....	135
Hotspots.....	136
Screen Panning	137
SmartPads	138
Text Input Tool.....	139
Command line options.....	141
Online Help	142
Glossary.....	143
Index	147
Appendix A: ID Action Codes (IDA Codes)	151

Preface

All of us at Naurtech Corporation constantly strive to deliver the highest quality products and services to our customers. We are always looking for ways to improve our solutions. If you have any comments or suggestions, please direct these to:

Naurtech Corporation

e-mail: support@naurtech.com

Phone: +1 (425) 837.0800

Assumptions

This manual assumes you have working knowledge of:

- Microsoft Windows user interface metaphor and terminology
- Stylus based touch screen navigation terminology
- Basic knowledge of concepts and terms for computer networking
- Basic operations and requirements of the host telnet server or web applications you want to access using the Naurtech Web Browser and Terminal Emulation application.
- Basic Web Browser terminology
- Basic programming and scripting concepts

Conventions used in this Manual

This manual uses the following typographical conventions:

- User actions and interactions with the application are in bold, as in **[Session] [Configure]**
- Precautionary notes or tips are presented as follows

Tip: Text associated with a specific tip

-  represents new version specific information
- Text associated with configuration examples and samples is presented as follows

```
/*alert*/  
OS.Alert("Script done.");
```

Additional Documentation

This user's manual covers details for installation and configuration of the Naurtech Industrial Web Browser and Terminal Emulation Application. Please refer to the **CETerm Scripting Guide** and the **Naurtech Web Browser Programming Guide** for details about programming and enhancing CETerm. Both these documents may be downloaded from the "Support" section of www.naurtech.com.

Online Support Wiki

Although we strive to keep this manual up to date, you may find our online Support Wiki useful for the latest features, enhancements, best practices, sample scripts, and troubleshooting tips. You can access the Support Wiki from our website:

www.naurtech.com → Support → Support Wiki

Introduction

Naurtech's CETerm is a combined Industrial Web Browser and Terminal Emulation application. CETerm provides mobile access to industrial and line-of-business applications running on web servers, workstations, and mainframes.

The CETerm web browser can work with your web applications whether they are running on a back-office PC or served from a state-of-the-art cloud architecture. The CETerm terminal emulation can access IBM3270, AS/400 (5250), Windows (VT) and Linux (VT) telnet and SSH servers. Also, CETerm can simultaneously run five independent sessions connecting to web or telnet servers. Mixed sessions allow a smooth migration from legacy telnet systems to newer web applications.

CETerm is available for most industrial mobile terminals running Windows CE, Windows Mobile, or Windows Embedded platforms. For some mobile terminals we offer single-emulation products (CE3270, CE5250, and CEVT220) which include the Industrial Web Browser and one type of emulation.

	Web Browser	VT 100/220	5250	3270
CETerm	√	√	√	√
CEVT220	√	√		
CE5250	√		√	
CE3270	√			√

"Device-tailored" CETerm is available for most terminal models from major manufacturers. These versions can use and control the peripherals available on the mobile terminal, such as barcode scanners, imager scanners, RFID readers, magnetic stripe readers and Bluetooth printers.

Single emulation products are only provided for a few terminal models. If you were using one of our single emulation products for your terminal in the past, we now recommend CETerm as it is available for all terminals.

This manual applies to all Naurtech Industrial Web Browser and Terminal Emulation products. Throughout this manual, we refer to CETerm. Except for some emulation specific details, all information provided also applies to our CE5250, CE3270, and CEVT220 products.

NOTE: The **Web Browser Programming Guide** discusses web extensions, HTML meta-tags, and ActiveX controls etc. Please refer to this manual if you are implementing web-based applications to be used with our Industrial Web Browser.

NOTE: All our products provide a fully scriptable platform to automate the data collection workflow and control the terminal and peripheral devices. Please refer to the Naurtech **CETerm Scripting Guide** for details.

Manuals can be downloaded from the Support → Manuals section of www.naurtech.com.

NOTE: The screen shots in this manual are captured from various versions of Windows CE and Windows Mobile platforms. It is possible that CETerm dialogs on your terminal may look slightly different from the depicted image.

What's New is version 5.7

Version 5.7 focuses on features and functionality which allow you to easily customize your applications and integrate with the mobile terminal environment. Several new CETerm Scripting objects have been added that provide this rich extension and customization environment. We implement most new features via scripting to provide the greatest flexibility. In addition, version 5.7 includes several small fixes and enhancements that have been added since the previous major release. Here are some highlights of the new features and enhancements.

- **Signature Capture Object.** CETerm now contains a signature capture object that can create images of signatures or an array of coordinates for a compact representation. The Signature Capture object is accessible via scripting and can be used by both web and terminal emulation sessions. See the CETerm Scripting Manual for complete details.
- **Digital Clock Display.** The current time and/or date can be displayed in any text format on the screen. The clock display can also be used to display information to the user and can be updated via scripting to provide alerts.
- **Extensive Additions to CETerm Scripting.** Once again, most new features are implemented within CETerm Scripting to provide the greatest flexibility. We've added new Automation Objects and events to provide more access to the mobile terminal, its peripherals and CETerm behaviors. As always, we use the industry standard JavaScript language so you won't waste time learning a limited and cumbersome proprietary language. Please see the CETerm Scripting Guide for a full description of the available features.
- **New Scripting Automation Objects.** Here is a list of the new automation objects in CETerm scripting:
 - Device.SignatureCapture - Signature Capture control.
 - Device.SmartCard - Contactless SmartCard (CASIO)
 - Device.GPS - Access and control GPS device.
 - OS.SIP - Soft Input Panel control.
 - OS.Network.ConnectionManager - Network connection control.
 - CETerm.Session(i).Screen - New scrolling controls added.
- **Additional Web Browser Extensions.** Our Industrial Web Browser has been fully featured for years. Recent enhancements are mostly found through CETerm Scripting, but we have added a page progress indicator (Windows CE only) and improved the browser loading indicator. We have added the ability to clear cache elements and save the source (Windows CE only). META key actions can now be accessed and changed from scripting. As expected, you can access all CETerm Scripting objects directly from HTML pages to control the mobile terminal, peripherals, and application behavior. It is truly the most robust platform to build web based Data Collection applications. We continue to support legacy Symbol Pocket Browser and Intermec IBrowse Meta tags as well. The Web Browser is available for all Windows Mobile and Windows CE mobile terminals.
- **Installable Codepages for VT220.** CETerm now supports the installation of single-byte and double-byte code pages for VT220 that are not available from the native Windows "National Language Support" (NLS) on the mobile terminal. These code pages can also be customized for special applications.
- **IBM Emulation Enhancements.** CETerm can now restrict the cursor movement on 5250 emulation to input fields only to eliminate input errors. Also, column separator characters can

be hidden to reduce screen clutter. We have also added support for the TN3270E (enhanced) protocol.

- **More Network Awareness Features.** We continue to strengthen the network awareness of CETerm. Now, “Check Network Before Send” is supported for all emulation types. Using this feature and Network Alerts for lost RF connectivity will virtually eliminate dropped sessions without the added burden and expense of a middleware server. CETerm delivers a simpler operating environment and the lowest cost of ownership.
- **Barcode Scanner Control Improvements.** CETerm integrates the barcode scanner to provide consistent and flexible scanning control. Most mobile terminals now support the full release of the scanner when necessary to share the scanner with other applications. For applications which do not integrate the scanner, CETerm can act as a “scan wedge” and deliver scanner input to those applications.
- **Additional Updates.** In addition to dozens of other enhancements, we added support for new mobile terminal models and current Windows CE versions from all major hardware vendors.

Feature Highlights & Benefits

Multiple host sessions

Supports up to FIVE simultaneous host sessions. Interactive, per-session configuration settings are maintained. Users may connect with any permutation of 3270, 5250, VT host or Web Browser sessions.

Hotkeys and menu context are available to jump between these sessions.

- Simultaneously connect to different hosts
- Multiple Web Browser sessions
- Maintain independent session contexts
- Easily switch between sessions

Industrial Web Browser

Many customers view Windows Mobile / Windows CE mobile terminals as multi-purpose handheld devices, using which they should not only access their legacy telnet host applications, but also web based applications. The integrated Web Browser addresses specialized data collection functionality requirements, such as key remapping, device lockdown, RFID and scanner integration etc that are not possible otherwise.

- Web based applications
- Multiple simultaneous Web Browser sessions
- Multi-purpose mobile terminal applications
- Migration path from green screen to newer web based applications

Scripting Workflow Automation Engine

CETerm includes a full JavaScript engine for both Terminal Emulation and Browser sessions, which allows you to automate and extend the behavior of your data collection application. You can use pre-defined scripts and modify these to customize and your everyday tasks. Several samples for common customization tasks are provided in the Support wiki on our website.

- A rich, scriptable platform to customize and automate business tasks
- Integrated control of scanner and RFID reader allows to differentiate your data collection solutions

Custom Keyboard mapping

Physical keys on the mobile terminal can be re-mapped to invoke any application operation or host key action. Keys can be remapped to:

- another key
- an application operation such as "Print"
- a host specific key such as "F4" or "Field Exit"
- a text string such as "My input string"
- a null operation (to disable the key)

- Remap any hardware key to any application operation
- Works for both TE and Browser sessions
- Minimize user re-training

Full ScreenMode

You can hide the Start Bar, the Application menu and toolbars so that the end user has no control to navigate away from the application. In addition you also get two precious rows of screen real estate as part of your terminal display area.

- Additional rows for display area
- Minimize production downtime by preventing users from changing device configuration and application settings.

Device Lockdown / Access Control

Device Lockdown allows administrators to prevent users from exiting CETerm. You can hide the Windows CE “Start” button, Start bar and also the application menu and tool bars so that the whole device screen is occupied by the CETerm application display.

Administrators can “lock out” users from the operating system so as to prevent users from being able to change the application and device configurations. This also prevents users from running any other application on the mobile terminal. The device may be configured to automatically boot into our application and auto-connect to the host.

- Provides administrators the ability to lock down the mobile terminal so users cannot navigate away from core business processes
- Minimizes support costs
- Simplifies business application workflow

Indicators

Visual Indicators for network RF signal, device battery strength, keyboard state, digital (date and time) clock and browser “page loading” animation can be configured. You can display, position and control these indicators for your Terminal Emulation and Web Browser sessions. You can also configure to receive notification if the RF signal or battery strength falls below a certain threshold. The same information may also be displayed as a Keybar button.

- Visual Indicators are available in full screen locked down configuration. This allows more screen real estate for the host application display area.
- Alert notifications if Indicator strength falls below a configured threshold

Internationalization: Code Pages

All popular Western European languages are supported to display and input language specific special characters. Single byte language code pages are provided. Examples of supported code pages are Swedish, French, German, Italian, Spanish, and Finnish etc. Additional languages, which are represented by single byte code pages, such as Thai, Cyrillic, Greek and Turkish are also supported.

- Support for international customers

Multi-Byte Character set: Asia Pacific language support

Support for multi-byte character set (MBCS) languages, such as Chinese (Traditional and Simplified), Japanese, Korean, Thai etc, is provided only for VT emulation. VT emulations also support the UTF-8 encoding and Single Byte Character Set (SBCS) encoding to support other languages such as Greek and Hebrew. Equivalent support for IBM emulations is not available yet.

- Asia Pacific language support
- UTF-8 encoding support for VT emulations

Network Aware Features

Users can configure to “Check network on Connect” or “Check network on Resume” to ensure network availability prior to establishing a connection if network coverage is lost or if the mobile terminal is resuming from a suspended state. Users can be prompted to return to coverage area if network connectivity is lost while roaming out of coverage.

For web browser sessions, which are stateless and do not require persistent session connectivity, users can also enable “Check Network before Send” to ensure network availability before every data send operation.

- Minimizes user interaction during connection / re-connection attempts
- Maximizes user productivity

Configurable KeyBar & Context Menus

The configurable KeyBar allows users to customize a set of soft buttons to control and invoke any host specific keys or application operation. Users can select from a set of pre-defined KeyBar templates. In addition they can also configure up to six custom templates of their own. Users can navigate between a selected set of KeyBar templates.

A KeyBar can also be made to appear as a Context Menu, which would appear when you tap and hold the stylus on the terminal display screen.

- Can make any host key or application operation available from a KeyBar soft button
- Customize KeyBar buttons to associated with proprietary VT escape sequences

Meta keys

Meta keys are special keys that you can configure to act much like the state keys "Shift", "Alt" and "Ctrl" on a regular keyboard. They are used together with other keys to activate special actions. Meta keys can be assigned to hardware keys for use in key remapping. They are especially helpful on mobile terminals with limited number of physical keys.

- More key remapping options on devices with limited keys
- Allows configuration of less key presses to achieve an action

Auto-start Sessions

Users may launch multiple host sessions when our application gets started. This can simply be enabled via session specific checkbox configuration.

- Eliminates intermediate manual step
- Minimizes retraining. Gives user direct access to familiar host application screen

Automatic login

You can easily automate the login process to your host application. Until now, we had suggested playing back a recorded macro which could be configured to launch automatically when a user session connected to the host application. Since version 5.5 or later, we recommend using scripting instead. An auto-login script can be configured to launch when a session connects, and then if necessary, prompt the user for a user id and password. Sample auto-login scripts are discussed in the Scripting Guide.

- Automates manual steps to enhance usability
- Customized for your host application

HotSpots

A HotSpot is an invisible field on the terminal screen where a user can tap with a stylus to execute a function. A Hotspot thus allows a user to interact with the host application with minimal needs for the special keypads. Instead the user can directly tap on the text in the terminal display to invoke the desired operation.

The pre-defined HotSpots are static. Using a script, you can easily implement dynamic HotSpots for your host application, such that any text on the screen can be made into a HotSpot.

- Leverages the "touch screen" interface of Windows CE to allow enhanced usability
- Minimizes need for host specific keys
- Can be customized for your host application

Dynamic Cursor View modes

Multiple cursor modes are available to support automatic scrolling, so that the cursor / input field is visible. The terminal display window will "track" and follow the cursor. In addition, you can lock a screen display to a specific row and column. These view modes are configurable for each session.

- Automatic scrolling to current cursor location enhances user productivity and usability
- Lock row / column position of display; backward compatibility with pre-existing applications

Legacy Extensions

All our terminal emulations support proprietary protocols used by legacy hardware terminal vendors so as to easily migrate customers to new / upgrade terminals. These include "Intermec Extended Commands", "Symbol IBM PRN", "Telxon VT extensions" and "LXE block mode" for terminal emulation. They include the Symbol Palm Web Client, Symbol Pocket Browser and Intermec iBrowse for Web Browser sessions.

- Seamless migration from legacy DOS / proprietary terminals to Windows CE / Pocket PC terminals

Screen Panning

Screen Panning allows an additional row and column on the display by providing an alternative to horizontal and vertical scroll bars. Imagine the host application screen as a large sheet under the display screen on the handheld device. Screen Panning allows users to "tap", "hold" and "drag" the terminal display screen in any direction to move hidden areas of the host display into view on the handheld device without the use of scroll bars.

- Faster alternative to scrolling
- Easier "Touch screen" usability

Configurable fonts

Users can easily include new fonts for displaying the terminal text. Any fixed-width true type font file (.ttf) may be placed on the mobile terminal and selected for terminal display. VT emulation also allows proportional fonts. Font sizes can easily be increased or decreased from the toolbar with a single stylus tap. Font weight can be changed as well.

- Enhanced readability on both color and monochrome display screens
- Single tap font size change

For Web Browser sessions, the font type, size and other attributes are set in the web page being viewed.

Macro Record and Playback

CETerm has the capability to record input keystrokes for a connected host session and subsequently play the recorded macros for easy, automated navigation through multiple host screens. Only a single macro may be recorded and associated with one host session. This macro may also be auto-launched upon a session connection to get "auto-logon" capability.

- Automates login steps to host application
- Automate host application navigation



Macro playback can sometimes be mis-timed due to network propagation delays and changing host application response times. The recommended approach for automating your tasks is to use a Script.

Automated License Registration

Simplifies the software license registration process by querying a configurable Web server for an XML based registration file. The license file can also reside locally on the mobile terminal.

- Easier deployment as individual CETerm licenses running on mobile terminals do not have to be registered manually

SmartPads

All host applications have specific keyboard requirements. The Smartpad is a floating button pad, which provides support for special emulation host keys. Depending upon the current configured host emulation type, the appropriate Smartpad for that emulation is displayed. The Smartpad supports all the popular 3270, 5250 and VT host keys.

- Access emulation specific host keys

Color Schemes

A color scheme is a collection of colors mapped to a set of terminal text display attributes. Users can select from a pre-defined color schemes or create a custom scheme based upon their preferences. Non-color displays will default to a Black-on-White or White-on-Black scheme.

Color schemes only apply to TE sessions. All color display configuration for web browser sessions is defined by the web page being viewed.

- Enhanced readability in varied lighting conditions

Cold boot persistence

Some Windows CE mobile terminals are diskless and only have volatile memory. These devices lose all installed applications and their registry configuration settings if the device cold boots or completely loses battery charge. You can be setup CETerm to self install and restore all device and application configuration settings. Such setup varies by manufacturer and terminal.

With the new Scripting Engine, cold boot persistence scripts can be written specific for each terminal to reduce this setup into a single key press. Refer to the Support Wiki on our website for details.

- Minimizes support costs and production down time

Host Session password

Any host session may be password protected with the user being prompted for a password when connecting that session.

- Secure host session connection

Device / LU Name support

For IBM emulations (3270 and 5250), logical unit device name resource configuration is supported. This is used during connection negotiations.

- Allows to better management and administration of SNA host resources

Integrated Demo modes

Simulated host terminal screens are integrated within CETerm for evaluation and sales demonstrations. No server component or network connection is required to run demo modes. Simply set the host name to "demo.naurtech.com" and connect.

- Easy demonstrations without need for live host connection

Text Input Tool

For Windows CE mobile terminals without keypads, data entry is usually performed using a stylus with an integrated soft keypad. This requires the user to spell-type text strings. This is a slow and tedious process. The Text Input Tool addresses this issue by allowing users to send text strings to the display window at the current cursor location, without spell typing. A user can preload often used text strings in the Input Tool, highlight the string and “send” the selected string to the session display.

- Optimizes usability and user productivity
- User configurable strings allow for individual customization

VT220 DEC Multinational & NRC support

VT emulations fully support the DEC multinational character sets and National Replacement Character sets (NRC). This support is provided for over a dozen western European languages.

- Supports international character sets for VT host sessions

VT Line Mode / Block Mode

This is a special optimization for VT host sessions. Data is buffered locally within the mobile terminal prior to sending it to the host / telnet server. Line mode optimizes usage of the network bandwidth and host resources.

- Optimized network bandwidth usage for VT emulation sessions

VT Answerback String

This is a configurable text string that certain host applications require to identify the terminal.

- Legacy application compatibility

Hot Keys

Predefined hot keys are available to interact with and invoke emulator operations.

- User productivity

Benefits of Naurtech Terminal Emulators & Industrial Web Browser

Terminal Emulation remains the well-proven, cost-effective solution for host access and automatic data collection solutions that result in the fastest ROI. With the rapid adoption of web-based mobile applications, the Naurtech CETerm Industrial Web Browser has become the new standard to access business processes and data. Our terminal emulator and industrial web browser running on a mobile terminal allows users to automate their business processes and to implement productivity solutions.

Here are some benefits of using Naurtech CETerm:

- It provides a seamless migration path for accessing legacy green screen and newer web based applications. This is especially helpful as legacy and web sessions can be run simultaneously in two independent sessions.
- The CETerm web browser allows you to write custom applications in HTML, giving you full control over the mobile terminal and its attached peripherals. It provides extended capabilities to build web based data collection applications, that cannot be implemented using the built in Pocket IE browser which comes with the Windows CE or Windows Mobile operating system.
- The built-in Scripting engine allows you to customize and automate your workflows for both terminal emulation and web-based applications. It gives users access and control to the state of CETerm, the state of a TE or web browser session, the mobile terminal, and the Windows CE Operating System to allow customization of routine steps or build complex applications.
- The CETerm Web Browser is optimized to seamlessly work with several applications like SAP ITSMobile and Oracle WMS, which require access to their transactions from a barcode RF handheld terminal.
- CETerm does not require any changes to be made to the existing backend / host applications.
- Combined with integrated support for barcode scanners and RFID readers, CETerm TE and Browser provide an efficient solution for data collection and data access.
- Device tailored versions CETerm are available for complete product families of terminals from every major hardware device manufacturer. Naurtech is the only vendor with such a breadth of offering in choosing a hardware platform.
- It supports most legacy proprietary extensions that have been used within the industry. This includes "Extended Commands" from Intermec, proprietary TE extensions from Telxon and Symbol, Block mode from LXE, HTML META tags from Symbol (Pocket Browser) and Intermec (iBrowse). Customers and partners can upgrade hardware terminals to newer models running CETerm without having to change the backend application.
- It is simple to configure, painless to provision, straightforward to deploy, easy to manage.

- Being tailored to the mobile terminal and OS platform, you can implement a higher productivity, higher usability solution. This is because the native client is able to conform to the ergonomics and form factor of the device while interfacing with the attached peripherals.

System Requirements

Following are the system requirements to run Naurtech smart clients.

Windows CE Version	Windows CE 6.0, 5.0 or Windows Mobile 6.5, 6.1, 5.0, Windows Embedded Handheld
Windows XP	XP Embedded
Operating RAM on mobile terminal	8 MB (Recommended 32MB or higher)
Connectivity	TCP/IP enabled LAN, WLAN (802.11B) or WWAN (GPRS), Bluetooth
Desktop connectivity	Windows Mobile Device Center or ActiveSync (3.7 or higher; we recommend ActiveSync 4.5)
Flash / Storage Card	Recommended 4MB

Version 5.7 does not support terminals with older Windows CE and Pocket PC OS platforms. Any terminal running Windows CE 4.2, Windows Mobile 2003 or below is only supported with an earlier versions of our product. Please contact us at support@naurtech.com if you need older versions.

Installation

All Naurtech Web Browser and Terminal Emulation products are packaged as a zip file and distributed electronically. Once you download the product from our website, follow these instructions to install the product to your mobile terminal.

After unzipping the downloaded file on the desktop, you should have the following files in your local directory

```
CExxxx.cab
CExxxx.ini
License.txt
yyyy_readme.txt
Setup.exe
ReleaseNotes.htm
```

where xxxx is the product and platform descriptor for the target CE device. Multiple CAB files may be present for different CPU targets. [e.g CETerm_WM65_ARMV4I.CAB]

where yyyy is a manufacturer and device descriptor for a "device tailored" version of the product. It has specific notes pertaining to the device tailored version.

- Make sure your mobile terminal is connected to your desktop via a USB, serial or wireless 802.11x connection.
- On your Windows desktop, make sure you have the Microsoft Windows Mobile Device Center installed. Older Windows operating systems can have ActiveSync version 4.5. (although you may also use earlier versions up to ActiveSync 3.7). You can get a free downloads from the Microsoft website.
- Make sure your mobile terminal is connected to the desktop via ActiveSync.
- Run Setup.exe on your desktop.
- You will need to read and accept the EULA to proceed. Click the "Install>>" button if you accept the license terms. This will launch the application manager to install the Naurtech product on your mobile terminal.
- Once installed, you will see the application in your [Start] [Programs] menu. For Windows CE OS platform devices, you will also see a shortcut on the desktop.

NOTE: You can select the install location on your mobile terminal from the Setup application. If you want to preserve the application during a device cold boot, you may want to install it on a Compact Flash or Secure Digital Disk, if available on the device.

NOTE: You can also copy the CAB file directly to the terminal and run it directly from there to install the product.

NOTE: CETerm is not a signed application. Certain Windows Mobile devices integrated with phone support may prevent installation. If you receive an error message, contact us at support@naurtech.com and / or the terminal manufacturer.

Quick Start

This section is for advanced users who are familiar with Windows CE devices and generally understand host terminal emulation and web browser terminology. Follow these steps to connect to your host application with minimal configuration setup. For details on various configuration parameters, it is recommended that you read through corresponding sections later in the manual.

- Install CETerm, CE3270, CE5250 or CEVT220 on to the mobile terminal. Follow instruction in the "Installation" section of the manual.
- Make sure the network settings are configured and the device is on the network. If you are connecting over wireless LAN (802.11x), make sure your device is communicating with the Access Point. If you are connecting over a wireless wide area (phone) network, make sure you can access the web.
- From the [**Start**] menu, run Naurtech CETerm, CEVT220, CE5250 or CE3270. On Windows CE platform devices, tap the desktop icon.
- Select [**Session**] [**Configure**] from the application menu and select the "Host Type" that you wish to connect to; i.e. 3270 mainframe, AS/400 5250 server, VT host or HTML for Web browser application.
- Enter the "Host Address" for the host system that you wish to connect to. This may either be a DNS name alias or an IP address of the host system or a URL (Universal Resource Locator such as <http://www.myhostname.com>) for your web based application.
- Update the telnet port number, if your host application is configured to listen on a specific port. If not, just use the default telnet port 23. A telnet port configuration is not required for Web Browser sessions.
- Select [**OK**]
- Select [**Session**] [**Connect**] from the application menu or tap the "Connect" button  on the Toolbar. Upon a successful connection, you should see the host application screen displayed.

NOTE: There are built-in "demo" modes available, which may be used to test the look and feel of CETerm, even if you may not have a live network connection to connect to your host. Simply set the "Host Address" to demo.naurtech.com (default). Select the Host Type and connect on that session. You can progress through pre-captured screens by pressing Enter or one of the function keys.

NOTE: The unregistered download trial of CETerm is fully featured, however it limits your session connection to timed intervals. Once you purchase and register the license, the timeout restrictions go away.

Quick “How To” Tips

Automatically submit a barcode (Postamble ENTER)

All device tailored versions of our Emulators and Web Browser directly interface with the barcode scanner engines. If you would like to configure your barcode scanning such that a key operation such as **[Enter]** or **[Tab]** or **[Field Exit]** etc is automatically appended after a barcode scan, you can set the post-amble in the scanner configuration. For **[Enter]** place a “**\r**” (without quotes), for **[Tab]** place a “**\t**”. For web browser sessions, to submit a form along with a barcode scan, enter “**IDA_DOM_SUBMIT**” in the post-amble. Refer to barcode scanner configuration for a list of pre and post ambles.

Change the font to fit rows and columns on the screen

You can dynamically increase or decrease the font size of the displayed text in either terminal emulation or web browser sessions. This allows you to configure the number of rows and columns such that they fit on the display screen. Select **[Display] -> [Font Up]** or **[Font Down]** from the application menu. You can also use the corresponding buttons on the toolbar. You must be connected to a host session for the settings to take effect.

Configure a session to automatically connect on startup

You can configure any session to automatically connect to the configured host when CETerm starts. To do so, configure your session for a connection. Then enable “Auto Connect” checkbox option from **[Session] -> [Configure] -> [Connection] -> [Advanced]**. Each session can maintain its separate setting.

You can also setup automatic launch of the application upon device boot, by placing a shortcut to the application in the `\Windows\Startup` folder

Setup Automatic login



For automatic login capability, we recommend using a Script rather than a Macro. Scripts offer a more robust solution and are not susceptible to timing related variations (such as network propagation delays or host application response time). Automatic login script sample is provided in the support Wiki and the Scripting Guide.

For versions which predate the scripting functionality, you can use Macros. Refer to the Macros section for more details.

Remap hardware keys

You can re-map any physical keyboard key on the mobile terminal to any host key, text string, application operation or a script. You can also map the key to a NULL operation, which will prevent use of that key. All key remapping is done through CETerm application configuration settings. No additional components are necessary. This remapping may be configured specific to either a session or an emulation type (such as VT, 5250, 3270, HTML etc).

It is sometimes difficult to find out the VK code generated when a physical key is pressed. This is important to know as it is the key code that needs to be remapped to another key. You can use the **[Key Trap]** button on the configuration dialog that monitor and capture the VK key code associated with a specific key (or key combination).

All key remapping configuration settings are performed from the dialog **[Session] -> [Configure] -> [Options] -> [Configure KeyBars and Keys] -> [Select Keymap] / [Edit Keymap]**. Refer to the key remapping section for detailed steps.

Configure Full Screen mode

You can configure CETerm such that the display area occupies the complete screen of the mobile terminal. The “Start” bar, Application menu, toolbar and any KeyBars can all be hidden. To configure full screen mode go to **[Session] -> [Configure] -> [Display] -> [Advanced] -> [Hide/Show]** tab. Enable the checkbox “Hide Menu Bar”, “Hide Keybar” and “Hide Toolbar”. Now go to **[Session] -> [Configure] -> [Options] -> [Advanced] -> [Access Control]** and enable checkboxes “Hide Start Bar”.

You can get back to your configuration dialogs from the full screen mode via a special Context Menu. If you double tap (on Windows Mobile) or tap and hold (on Windows CE) the stylus on the top left vertical edge of the display screen, you will see a context menu appear. Choose the “Configure” option to enter the configuration. Unhide the desired menu(s).

Lock down the device

You can prevent the users from being able to access any application menu or configuration options. To do so, configure CETerm to run in full screen mode. Next enable the checkbox option “Disable App Exit” from **[Session] -> [Configure] -> [Options] -> [Advanced] -> [Access Control]** configuration settings. Also set an access control password here. The user will be prompted for this password if an attempt is made to enter the configuration dialogs. Refer to the Access Control section in this manual for more detailed instructions.

Display Indicators

You can display several informational indicators to display the current status of RF signal strength, battery charge, Keyboard state, date and time etc either as floating icons or as part of KeyBar buttons. To display the Indicators, go to **[Session] -> [Configure] -> [Options] -> [Advanced] -> [Info Items]**. Select the Indicator from the dropdown list.

For the selected Indicator, make sure you enable the “Update” checkbox and the “Enabled” checkbox under “Screen Display”. You can also select the status buttons to be displayed on a Custom KeyBar. Refer to the Indicators section in this manual for more details.

Configure to display International language character sets

We fully support all European language codepages for all terminal emulations. We support multi-byte character set languages, such as Chinese, Japanese, Korean, Hebrew etc for VT emulations only.

For IBM emulations, you can select your language specific codepage table from our support website. Once installed, the codepage will appear as a selectable option under **[Session] -> [Configure] -> [Connection] -> [Advanced] -> [IBM Options]** settings.

For VT emulations, you must have the language specific codepage table installed on the mobile terminal. You can then select the encoding mode and the corresponding codepage from the options under **[Session] -> [Configure] -> [Connection] -> [Advanced] -> [VT Extensions]** settings.

Enable SSL / SSH security



You can encrypt all data exchanged with your host applications by configuring your session connection to use SSL (Secure Sockets Layer) or SSH (Secure Shell Protocol). You can enable either of these from the **[Session] -> [Configure] -> [Connection] -> [Security]** configuration dialog. Additional settings for SSH must be configured. You should review the details under the SSH configuration section.

Exiting out from the registration dialog

When running the software in evaluation mode, you may enter the registration dialog by pressing the “Register” button when you are notified that you are running an evaluation version. At this point you are expected to enter a User ID and a registration key. The device unique License ID is shown in the registration dialog. If you do not yet have your registration key and need to exit back to the splash screen, press the cancel 'X' button or press the Esc key.

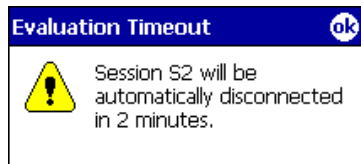
If you have three unsuccessful attempts to register your software license, you will be returned to the splash screen.

Automatic Licensing Registration

Rather than having to type the user id and key to register your software license, you can use the automated license registration. Your registration key(s) are also provided in an XML file format. You can either place this file on a Web server or locally on your mobile terminal. During the first connection attempt, CETerm will automatically try to resolve and complete the registration. You can then configure a reference to this file to automatically register the license. To configure automated licensing, go to **[Session] -> [Configure] -> [Options] -> [Advanced] -> [Manage]**. Under “Server URL” enter the complete URL to the registration license XML file. Please refer to the Automated Licensing section later in this manual.

Evaluation Mode

You can download our Web Browser and Terminal Emulation application from our website at any time. These are fully featured but run in a “trial” mode until the license is registered. In this trial mode, every connected session has a timeout limit following which it will disconnect. You are allowed to connect to at most two sessions simultaneously. You will also receive a warning for the evaluation connection attempts and connected time. The evaluation period expires once the number of host connection attempts is exhausted.



These limitations and warnings are strictly part of the evaluation mode. They are not seen in a registered version of the application. To register the application, you must purchase a legal registration key and register your copy of the software installation. Contact our sales department at sales@naurtech.com for more information.

Software Registration

You can purchase registration keys for our Web Browser and Emulator product by contacting your Systems Integrator / Reseller or Distributor. If you do not know of a reseller who carries our product, feel free to contact us and we will be glad to refer one to you in your geography.

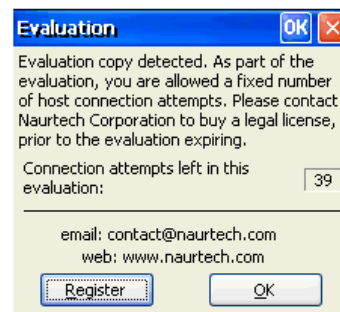
Phone: +001. 425.837.0800
 E-Mail: sales@naurtech.com
 Web: <http://www.naurtech.com>

Once you have received your user id and associated registration key, follow these instructions to register the product.

- Launch the product application on your Windows CE / Windows Mobile device
- From the application menu, select [**Session**] [**Connect**]. Alternatively, you may tap the "Connect" button  on the application ToolBar
- If your copy of the product is not yet registered, you will receive the following dialog



Windows Mobile

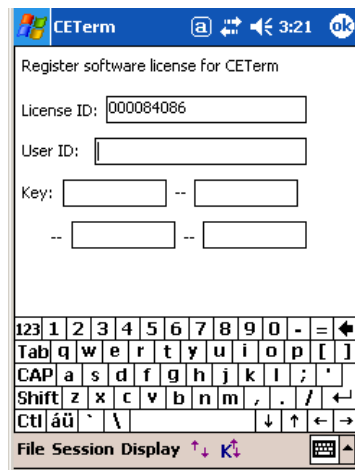


Windows CE

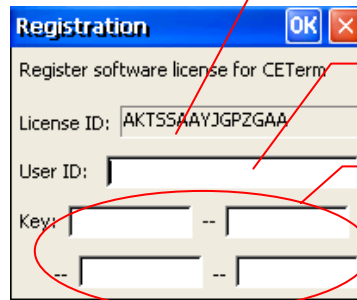
- Tap the "Register" button. This will display your device license ID and prompt you for your User ID and Key to register your software license.
- Verify the license ID of the terminal with the one provided along with your license registration key. These should match exactly.
- Enter the Registration Key using the soft keypad on the mobile terminal. Note that your registration key is provided as 4 hyphenated values such as `aaaa-bbbb-cccc-dddd`. Make sure

you enter these in the correct order as indicated in the picture below. You can also use automated licensing using a license.xml file so you don't have to type your user id or key.

- Tap OK



Windows Mobile



Windows CE

This is a device unique License ID on which your license registration key is based on. It can be your device serial number, MAC address or another unique ID. You would have provided this License ID to Naurtech when purchasing the license.

Enter your User ID, (usually the company name) here

Enter the registration key, which you purchase from Naurtech here. This is a unique key based upon your device license ID.

NOTE: Your registration key is unique to your device License ID. It is case sensitive and must be entered in the correct order.

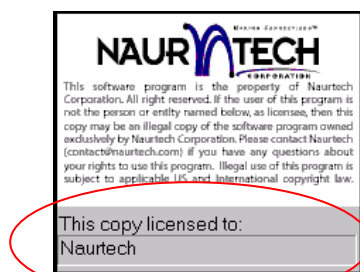
NOTE: The registration key does not include any references to the number zero [0], capital alphabet O, the number one [1] and lowercase letter L [l].

NOTE: If you do not yet have a registration key and would like to exit back to the splash screen, press the cancel button 'X' or the Esc key. On Windows Mobile platform devices, you must enter at least two characters in the User ID field. Tap OK. Repeat this step three times to return to the splash screen.

If your User ID and Key are correct, your product will be registered. If the keys do not match, you will be prompted with a failure message accordingly. Please make sure both the User ID and Key are entered correctly. Both of these are case sensitive. If the problem persists, please send e-mail to support@naurtech.com.

Please keep the product registration key handy. You may be asked to provide this for technical support issues.

Once the product is registered, your User ID will appear on the Splash bitmap and in the File -> About dialog box.



Once the registration is successful, your user id will be displayed under the Splash screen and in the File -> About dialog box.

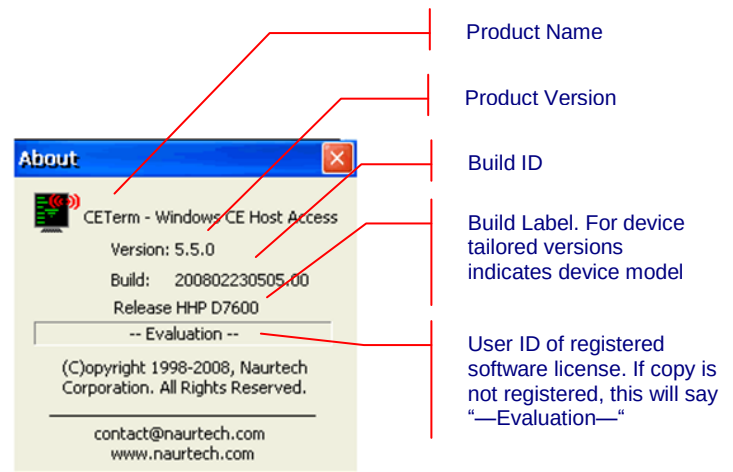
Product Version

You can check the installed version from the “About” dialog. Follow these steps to determine your product version number and licensing registration information.

- Launch the product application on your Windows CE / Windows Mobile device
- From the application menu, select **[File] [About]**. You will see the About dialog as shown below. The product version, build ID, label and license registration information is shown.



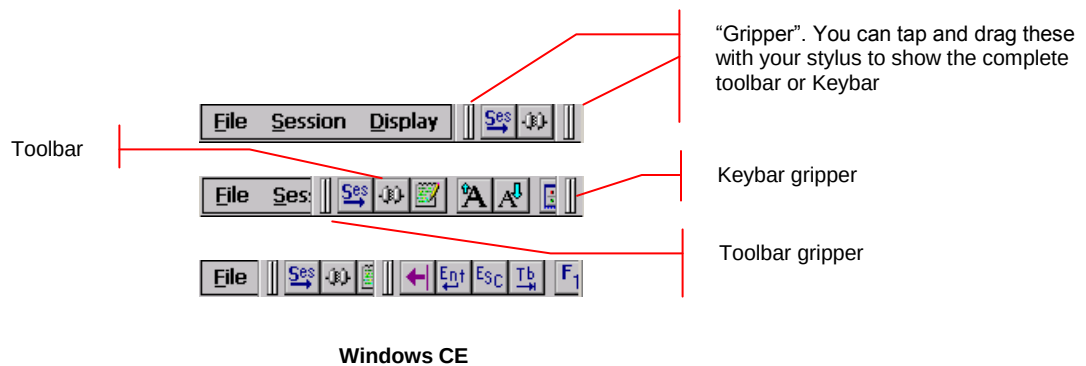
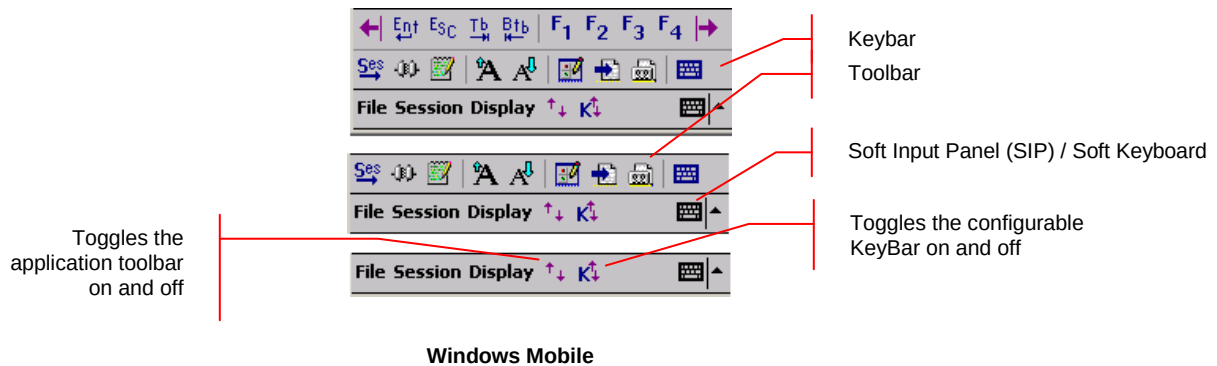
Windows Mobile



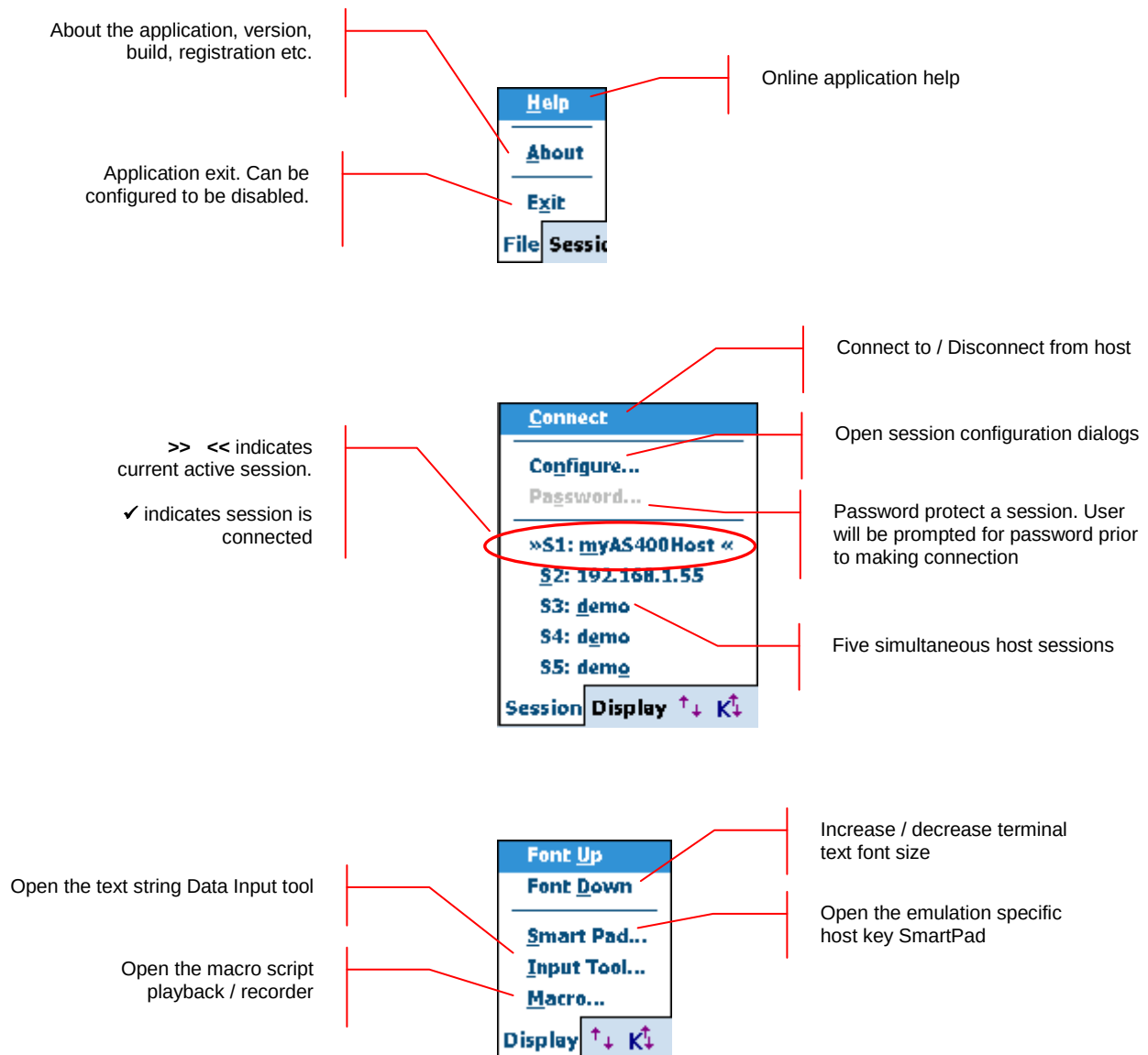
Windows CE

Application Menu

One of the benefits of using Windows CE / Windows Mobile platform devices is that they follow the popular desktop “Windows” usability metaphor. Naurtech Emulators and Web Browser follow the user interface guidelines as recommended by Microsoft. Windows CE uses command bars, which combine menus and toolbars together. The following image shows the application toolbar.



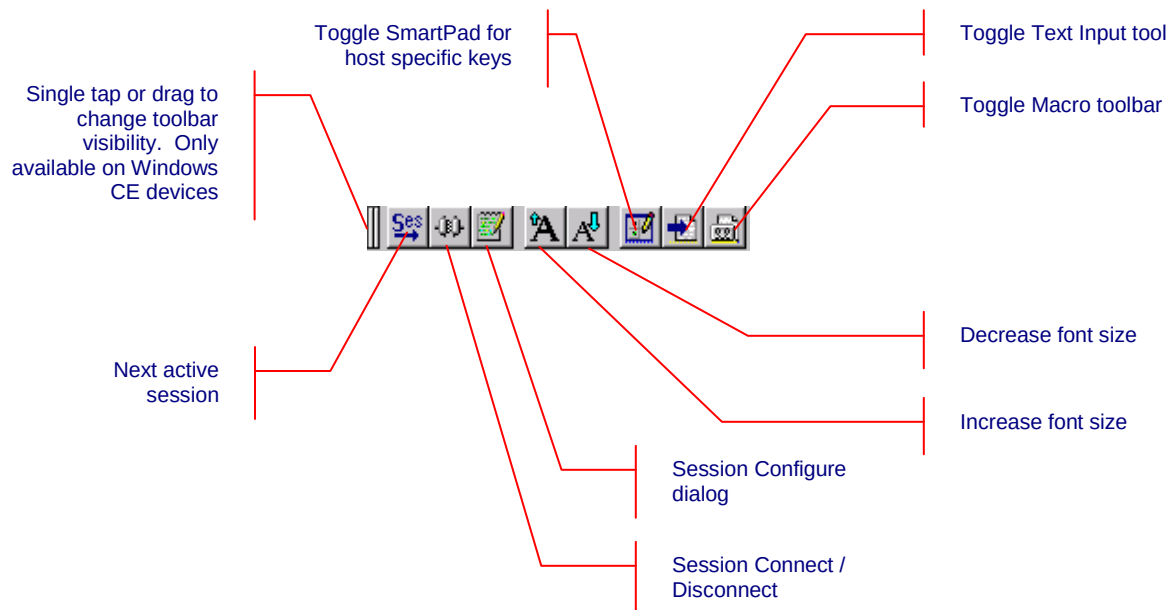
The operations associated with application sub-menu options are shown below



NOTE: You can run up to five host sessions simultaneously. These may be connected in any combination to legacy host or Web server applications

Application Toolbar

An integrated application toolbar is provided for touch screen navigation. For Windows CE platform devices, this toolbar is available next to the Application menu. For Windows Mobile platform devices, you can bring up the toolbar by invoking the toolbar button  next to the application menu. Below is a description of the buttons on the toolbar. You can also tap and hold the toolbar button to get a “toolbar tip” indicating its functionality.



Configuration

This section describes various configuration parameters for session connections. All these parameters are set using the configuration dialogs accessed from the **[Session]** **[Configure]** application menu. Except for "Connection" parameters, you can change or update any parameters at any time, whether the host / browser session is connected or disconnected.

Every configuration setting value is automatically saved to the last configured setting. All configuration attributes are associated with the currently active session. Every session can have a different set of configuration attributes.

NOTE: The positioning of some of the user interface widgets on the dialogs shown might appear slightly different on your mobile terminal. This is because Windows CE devices come in various screen form factors and the placement of the user interface widgets is performed dynamically, based upon the device screen dimensions and characteristics.

Connection

The table below shows the hierarchy of configuration settings for the Connection configuration attributes. Each highlighted title represents a configuration dialog tab or button

Connection			
Host Type			
Host Address			
Terminal Device			
Host Port			
Advanced			
→			
General		IBM Options	VT Options
Auto Connect		IBM Codepage	Answerback Message
Auto Reconnect		Device / LU#	Keyboard
Macro on Connect		Error Row	Send Mode
Confirm Disconnect		Shift all Error Row content	Compatibility
Confirm Exit (Connected)		Suppress Auto Field Advance	User Pref Sup.
Exit on Disconnect		Suppress Backspace At End	VT Extensions
Check Network on Connect		3270 EAB	Multi-byte: Mode
Check Network on Resume		Allow TN3270E	Multi-byte: Code Page
Check Network before Send		Keep Cursor in Input Fields	Two Column DB Characters
Enable Socket Keep-alives		Hide Column Separators	Extensions: Symbol TNVT
		VT Modes	Extensions: Symbol CE VT
Term Type		Background	Extensions: Telxon
Initial Sleep		Columns	
Network		C1 Controls	
Network Check: Timeout		Backspace	
Network Check: Host		Enter Key	
Network Check: Action		Autowrap	
Security		Local Echo	
SSL: Enable SSL			
SSL: Perform Certificate Checks			
SSH: Enable SSH			
SSH: Advanced →			

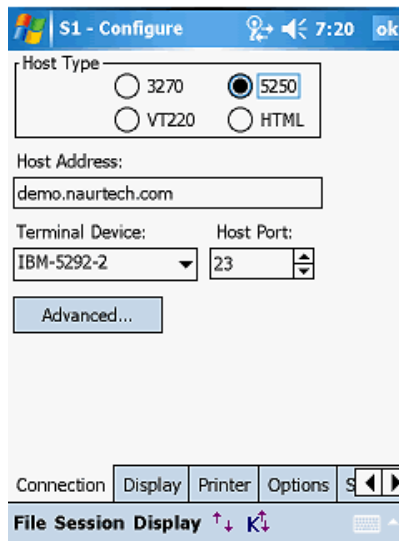
	SSH Advanced: SSH General		SSH Advanced: User Keys
	Enable SSH		User Key
	Prefer SSH-1 Protocol		Clear
	Prefer SSH-2 Protocol		Select
	Auto OK New Host Keys		Import
	Auto OK Changed Host Keys		Delete
	Try Keyboard Auth		Copy OpenSSH Public Text
	Try TIS Auth SSH-1		SSH Advanced: Server
	Auth Username Changeable		Environment
	Skip User Authentication		Command
	Cache Decrypted User Keys		TTY Modes
	Re-Key every 60 Minutes		Forwarding
	Re-Key every 1G of traffic		Delete Server Keys
	Enable Compression		SSH Advanced: Proxy
	Enable Verbose Messages		Type
	Allow IPV4		Host
	Allow IPV6		Port
	Use TCP No-Delay		User
	Send TCP Keep-Alives		Password
	No Pseudo-Terminal on Host		Exclude Hosts
	No Host Shell		Command
	Run Sub-System on Host		
	Try Proxy for Local Host		
	DNS Lookup at Proxy End		
	Local Fwd – Allow All Hosts		
	Remote Fwd – Allow All Hosts		
	Overwrite Existing Log File		
	Omit Passwords from Log		
	Omit Session Data from Log		
	Bug – SSH-1 Ignore		
	Bug – SSH-1 Password Hiding		
	Bug – SSH-1 RSA Auth		
	Bug – SSH-2 HMAC Key		
	Bug – SSH-2 Encryption Key		
	Bug – SSH-2 RSA Signature		
	Bug – SSH-2 ID in PK Auth		
	Bug – SSH-2 Re-Key		
	Username		
	SSH Keep Alive		
	Log Mode		
	SSH Advanced: Encryption		
	Encryption Priority		
	Diffie-Hellman Key Exchange Priority		

Before you can connect to your host or web server application, at a minimum, you must know the type of host you are connecting to and the IP address or URL of the host system. You must also configure the port number on which the host application is expecting connection.

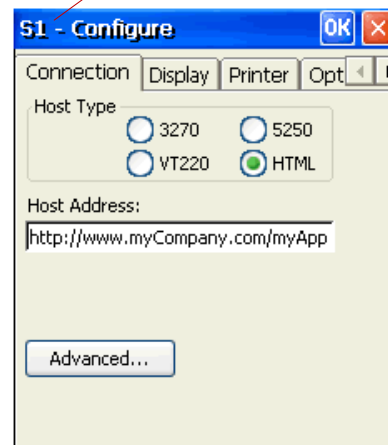
- From the application menu, Select **[Session] [Configure]** or tap the "Configure" button  on the toolbar.
- A "Configure" dialog box will come up.

- Choose the "Connection" tab. This is the first (and default) tab.

The following dialogs show the Connection tab of the host session configuration dialog.



Windows Mobile



Windows CE

Session number being configured

NOTE: The default settings will change depending upon the current selection of "Host Type"; type of emulation of web browser session .

Host Type: This is the type of session required to connect to your host / web server application. Your choices are 3270, 5250, VT220 or HTML. The first three represent terminal emulation sessions. The last option (HTML) represents a Web Browser session. You may select any one emulation type for the session. If you have a single emulation product (CE3270, CE5250 or CEVT220), only that emulation type will be selectable. HTML host session types are available with all products. Other connection configuration options may change dynamically depending upon the Host Type selected.

Host Address: This is the address of a host system or an intermediate gateway managing connections to the host system. Enter the host name or numeric IP address, using up to 64 characters. Default is `demo.naurtech.com`, which connects to a simulated demo host. For HTML browser sessions, the host address should be the URL (Universal resource Locator) of the host application site such as `"http://myIntranetApp.myCompany.com/start.php"`. For HTML sessions, if you are trying to view a page local to your mobile terminal, the URL format should be `"file:///absolutepath/myPage.htm"` where `"absolutepath"` is the absolute path to the web page from the root folder.

Terminal Device: This is the terminal type string that determines a specific terminal to emulate. This setting is applicable only for Terminal Emulation sessions. It does not apply

to Web Browser sessions. For 3270 emulations only model 2 screen geometry is supported. CEVT220 supports VT52, VT100 and VT220 terminal types. Each host emulation type has its own default terminal type.

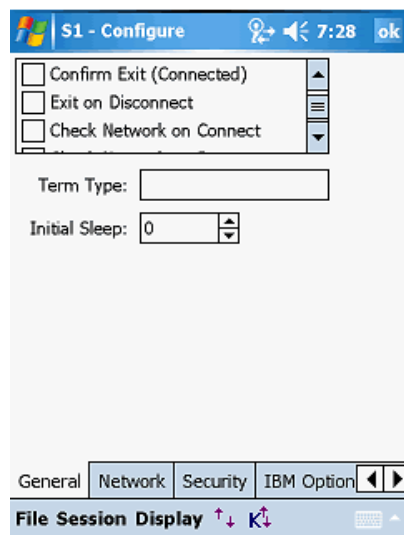
Telnet Port: This is the TCP socket port number to be used to connect to the host system. The default is 23. You may change this to the telnet port on which your host application is listing. This setting does not apply to web browser (HTML) sessions.

Advanced

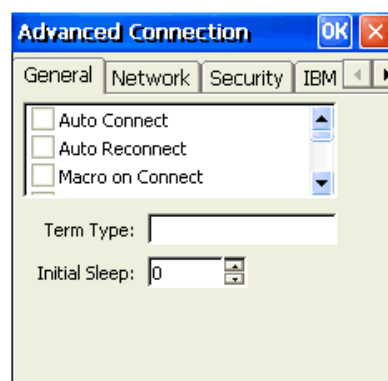
This button opens an advanced connection configuration dialogs.

General

This tab maintains general configuration settings relating to session connection and reconnection.



Windows Mobile



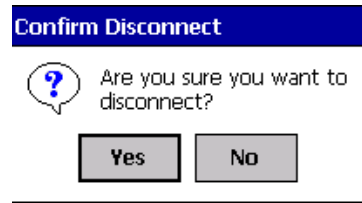
Windows CE

Auto Connect: Checking this box will automatically connect this session when CTerm starts. If you want to automatically connect to your host configured for this session when the application starts, enable this checkbox. You can have more than one session configured for auto connections.

Auto Reconnect: Checking this box will cause the emulator to attempt to reconnect to the host if the connection is lost or closed by the host. This setting has no affect on Web Browser sessions as Browser sessions are stateless and establish a new connection for every data exchange.

Macro on Connect: Check this option if you want to automatically start playback of a pre-recorded macro associated with this session connects. You can use this capability to automate any steps that require to be performed upon session connection; although a CTerm script is recommended instead.

Confirm Disconnect: Check this option if you want to be prompted prior to disconnecting a connected session. The prompt will force a user action before proceeding ahead with disconnection of the host session.



Confirm Exit (Connected): Check this option if you want to be prompted prior to exiting our application if one or more sessions are connected.



Exit on Disconnect: Check this option to exit the application when one or more of the connected sessions disconnects. The disconnection may be triggered by either the user or by the host.

Check Network on Connect: When enabled, the network availability will be automatically checked when an attempt is made to connect / reconnect to the host. The user will be prompted if the mobile terminal is out of RF range or if the network cannot be detected.

Check Network on Resume: On certain mobile terminals, depending on your configuration settings, the OS withdraws power from the WLAN card when the device is suspended. This may be done to prolong battery life. When enabled, this setting ensures presence of a network signal when the device is resuming itself from a "Suspend" state. The user will see a progress bar while CETerm attempts the detect availability of a network. The user will be prompted if the device is not associated, is out of RF range or if the network cannot be detected.

Check Network before Send: This setting is only applicable to Web Browser sessions. It does not affect any of the terminal emulation sessions. When enabled, the network availability will be checked every time before sending any data to the host server. The user will be prompted if the mobile terminal is out of RF range or if the network cannot be detected. Enable this setting if your network coverage is sporadic.

Term Type: Leave this blank unless required. If not empty, this value is reported as the terminal type in the Telnet negotiations. Use this only if your host has a special Telnet server that uses the value to identify devices or special situations.

Initial Sleep: This setting should no longer be used. Instead, use “Check Network on Connect”. This is the time, in seconds, for which CETerm will wait when the application is launched. This setting is useful when CETerm is configured to automatically start following a device cold boot and connection to a host application. The “Initial Sleep” allows the underlying wireless network to initialize prior to the CETerm attempting to establish a connection. The default value is 0, which means no delay.

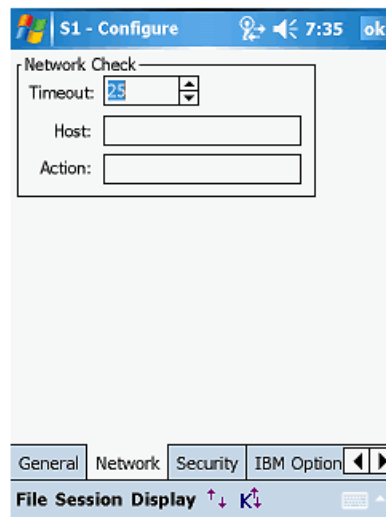
NOTE: This setting has been obsolete by the “Check Network on Connect” setting.

Network

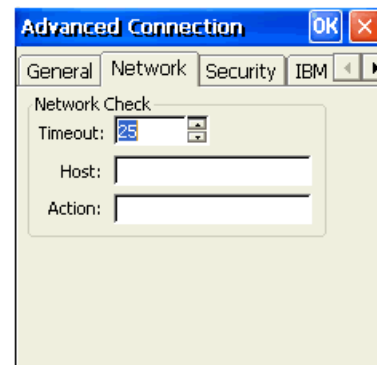
This tab maintains configuration settings to enable detection, presence and availability of the network.

Timeout: This is the length of time for which CETerm will try to find the host by sending multiple ping requests. You can specify a navigation error page in the Action setting to manage RF connection loss. You can also use the Scripting event “OnNavigateError”, to recover when RF is lost during navigation or if web server is not responsive. See the Scripting Guide for details.

Host: This is the URL or IP address of the host server that you would like to check to determine presence of network and availability of the host server. This can be different from the URL or IP address of the host for which your session is configured.



Windows Mobile



Windows CE

NOTE: If this **Network** -> **Host** setting is blank, the network check extracts the hostname from the pending connection URL and sends an ICMP Ping to determine if the path to the host is available. This effectively checks if the RF is available, your mobile terminal is associated, any security protocols are established, and the host is alive. The network check is only performed if the pending URL is a HTTP or HTTPS type. Note that this does not check if your host web server has crashed.

If this **Network** -> **Host** setting is specified, then that host is the target of the ping. This can be useful if you have a network component or alternate host that can be used to query.

Possible problems, if you always navigate to the error page could be:

- Your host or host firewall is configured so that it won't respond to a ping.
- You have a character in the "host" configuration of CETerm. Even a space will be parsed to try to determine the host. Make sure it is empty.

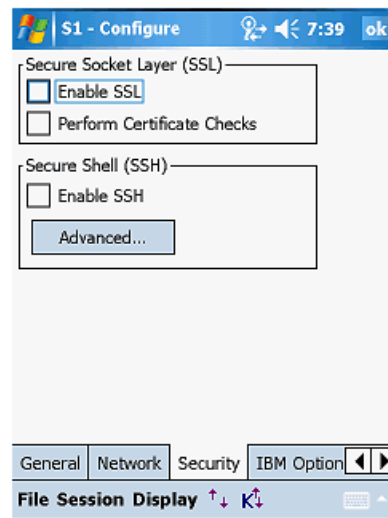
Action: This is the action URL to which the Browser session is redirected if the network is determined to be unavailable. This URL will typically be a device local error page such as `"file:///<myDeviceLocalPath>/myErrorPage.htm"` URL. If you specify an action, the Cancel button is disabled on the Network Check dialog.

Security

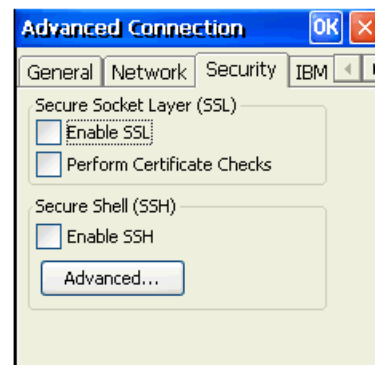
 This tab maintains all advanced connection configuration settings for data encryption and security. Both Secure Shell (SSH) protocol and Secure Sockets Layer (SSL) encryption are provided for all terminal emulations and web Browser sessions. Use `https:` connections to provide SSL for HTML sessions.

Telnet over SSL (Secure Sockets Layer)

SSL or Secure Sockets Layer provides secure encryption of data between a handheld terminal and the host. It is the underlying security protocol used by web browsers. With SSL, they host system can also ask for a password to authenticate. This is sent over a secure encrypted connection.



Windows Mobile



Windows CE

Enable SSL: Check this option to enable SSL data encryption. Once enabled, all data sent to the host application is encrypted. All data received is decrypted

Perform Certificate Checks: Check this option if you want the client to perform checks for valid certificate on the SSL server.

SSH Secure Shell

 SSH, or Secure Shell, is a popular, powerful, software-based approach to network security. Before data is sent by CETerm over a network, it is automatically encrypted (scrambled) by SSH. The data is automatically decrypted (unscrambled) when it reaches

the host. The result is transparent encryption: users can work normally, unaware that their communications are safely encrypted on the network. In addition, SSH uses modern, secure encryption algorithms and can be found within mission-critical applications at major corporations.

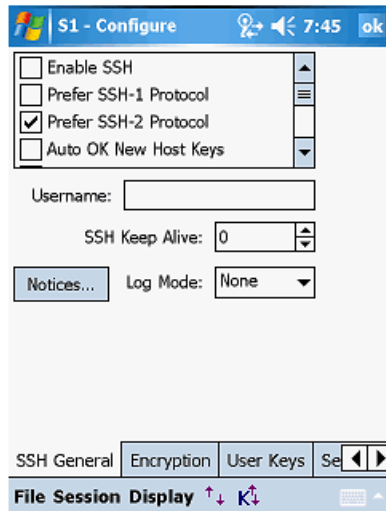
Enable SSH: This option enables the SSH protocol for this CEMTerm session. The default is Off.

Advanced: This button allows configuration of more advanced settings specific to the SSH protocol. By default, these settings will enable connections to most SSH servers. It is recommended that you use the default settings, unless you understand implications of the various settings.

General

This tab is used to configure general settings of the SSH protocol. The list contains check boxes that may be individually selected for the desired option. Please note that some items, whenever applicable, have three selectable states: On, Off and Auto-Sense (Check with "A"). Tapping these options will cycle through the three states.

If checked (On), the option is selected. If unchecked (Off), the option is not selected. If Auto-Sense (Auto OK), CEMTerm will determine and use the most appropriate option setting.



Windows Mobile



Windows CE

Enable SSH: This option enables SSH for the current session. The option is identical to the value on the previous Security tab and is repeated here for convenience.

Prefer SSH-1 Protocol: Enable this option if you would like to connect to your VT host server using SSH protocol version 1. The default setting is Off.

Prefer SSH-2 Protocol: Enable this option if you would like to connect to your VT host using SSH protocol version 2. The default setting is On.

NOTE: If both SSH-1 and SSH-2 options are off, CETerm will first try to connect using SSH2 protocol and then fall back to SSH-1 protocol.

Auto OK New Host keys: Automatically accept the host keys presented by the server. Enabling this option will minimize the amount of interaction that is required on part of a user. The default setting is Off.

WARNING: Enabling this option reduces security because the user does not verify that the server being connected to is the intended destination. For greatest security the user should verify that the server credentials presented match the intended server.

Auto OK Changed Host keys: Automatically accept changed host key presented by the server. Enabling this option will minimize the amount of interaction that is required on part of a user. The default setting is Off.

WARNING-WARNING-WARNING: Enabling this option reduces security because the user does not verify that the server being connected to is the intended destination. A changed host key may indicate a “man-in-the-middle” attack, or it may be that the server administrator has simply changed the server host key. For greatest security the user should verify that the server credentials presented match the intended server.

Try Keyboard Authentication: This option is for SSH-2 protocol only. It is a flexible authentication method using an arbitrary sequence of requests and responses. This method is not only useful for challenge/response mechanisms such as S/Key, but it can also be used for asking the user for a new password when the old one has expired. This option is On by default.

Try TIS Authentication SSH-1: TIS authentication is a simple challenge/response form of authentication available in SSH-1 protocol only. You might use it if you were using S/Key one-time passwords, or if you had a physical security token that generated responses to authentication challenges.

With this option enabled, CETerm will attempt this authentication if the server is willing to try them. You will be presented with a challenge string (which will be different every time) and must supply the correct response in order to log in. If your server supports this, you should talk to your system administrator about precisely what form these challenges and responses take. This option is Off by default.

Auth Username Changeable: The SSH-2 protocol allows change of username during authentication, but does not make it mandatory for SSH-2 servers to accept them. In particular, OpenSSH does not accept a change of username; once you have sent one username, it will reject attempts to try to authenticate as another user.

Enable this option if your server accepts changes to username in its authentication process. This option is Off by default.

Skip User Authentication: When enabled, CETerm will not negotiate user authentication with the SSH server. In most cases this will prevent a connection. This option is Off by default.

Cache Decrypted User Keys: When enabled, CETerm will retain a private copy of any user keys that have been unlocked with a user passphrase. Subsequent requests for the key will be served automatically and will not require the user to re-enter the passphrase. CETerm does not retain the passphrase. The cached key may be used with multiple sessions and will be erased when CETerm exits or if this option is changed to Off. This option is global and is common to all sessions. The default value is Off.

NOTE: While this renegotiation is taking place, no data can pass through the SSH connection, so the session may appear to 'freeze' momentarily. This is a short period when the key exchange is taking place.

Re-Key Every 60 Minutes: A shared session key is used by the encryption protocol. If used too long, the session key may be subject to attack and expose the SSH connection. Although such an attack is unlikely, it is wise to re-exchange the key every so often. This can be initiated either by the client or the server. Enabling this option will trigger CETerm to exchange a new key with the server every 60 minutes. This option is On by default.

Re-Key Every 1G of Traffic: A shared session key is used by the encryption protocol. If used for a large volume of traffic, the session key may be subject to attack and expose the SSH connection. Although such an attack is unlikely, it is wise to re-exchange the key after a significant amount of data. Enabling this option will trigger CETerm to exchange a new key with the server following a total data flow of 1 Gigabyte in either direction. This option is On by default.

Enable Compression: Enabling this setting will compress all data exchanged over the SSH connection. We do not recommend using compression for standard interactive sessions. By default, this setting is Off.

Enable Verbose messages: When enabled, the user is informed of major errors which affect the SSH connection via a popup dialog. Some additional information is presented within the emulation screen. This option is On by default.

Allow IPV4: Enable this option to allow the IPv4 Internet Protocol addressing scheme. The default is On.

Allow IPV6: Enable this option to allow the IPv6 Internet Protocol addressing scheme. The default is Off.

Note: If neither IPv4 or IPv6 options is selected, CETerm will use IPv4. If both are selected, CETerm will first attempt IPv6 and fall back to IPv4 if it is unsuccessful connecting with IPv6.

Use TCP No-Delay (Advanced): Under normal operation, the TCP communication stack performs data packet batching. Enable this option forces the TCP stack to send immediately without batching data packets. This can result

in excessive traffic of short packets. We recommend leaving this option Off. It is Off by default.

Send TCP Keep-Alives (Advanced): Enables the TCP socket keep-alive option. This option is deprecated and should not be used. Use the SSH level keep-alive to prevent session disconnection by a host. This option is Off by default.

No Pseudo-Terminal on Host (Advanced): When connecting to a Unix system, most interactive shell sessions are run in a pseudo-terminal, which allows the VT host system to pretend it's talking to a real physical terminal device and allows the SSH server to catch all the data coming from that fake device and send it back to the client. Occasionally you might find you have a need to not run a session in a pseudo-terminal. Enable this option to prevent CETerm from running a pseudo terminal. The default is Off.

No Host Shell (Advanced): Enabling this option will force CETerm to not run a shell or command after connecting to the remote host server / host. This option may be used only when using the SSH connection for port forwarding, and your user account on the server not having the ability to run a shell. This option is only applicable with SSH protocol version 2, since the SSH version 1 protocol assumes you will always want to run a shell. The default is Off.

Run Sub-System on Host (Advanced): If enabled, attempts to run an SSH-2 subsystem on the host. By default, this option is Off

Try Proxy for Local Host: If using a proxy connection, this option enables the use of the proxy even for connections to localhost. By default, this option is Off

DNS Lookup at Proxy End: If Off, CETerm will perform DNS lookup on the handheld. If On, CETerm will perform DNS lookup on the proxy host. If Auto-Sense, CETerm will choose the DNS lookup location based on the proxy type. By default, this option is Auto-Sense.

Local Fwd – Allow All Hosts: If enabled, this option allows hosts other than the handheld to connect to local ports that are forwarded to the server. This may be useful for a peripheral device to connect to the server. By default, this option is Off.

Remote Fwd – Allow All Hosts: If enabled, this option allows hosts other than the server to connect to remote ports that are forwarded to the handheld. By default, this option is Off

Overwrite Existing Log File: Enable this option if you want to automatically overwrite the existing log and start capturing a new log. If unchecked, log data will be appended to the end of the existing log. The default option is Auto-Sense, in which case the user is prompted when logging starts and the file exists.

Omit passwords from Log: When checked, password fields are removed from the log of transmitted packets. This includes any user responses to challenge-response authentication methods such as 'keyboard-interactive'. Note that this setting will only omit data that CETerm knows to be a password. If you start another login session within your CETerm SSH session, for instance, any

password used will appear in the clear in the packet log. This option is Off by default.

Omit Session data from Log: When checked, all 'session data' is omitted; this is defined as data in terminal sessions and in forwarded channels (TCP, X11, and authentication agent). This will usually substantially reduce the size of the resulting log file. This option is Off by default.

NOTE: Not all SSH servers work properly. Various existing servers have bugs in them, which can make it impossible for a client like CETerm to talk to them unless it knows about the bug and works around it. Since most servers announce their software version number at the beginning of the SSH connection, CETerm will attempt to detect which bugs it can expect to see in the server and automatically enable workarounds.

The following configuration options are provided to navigate around these known bugs in the various SSH server implementations.

Bug – SSH-1 Ignore: Within the SSH-1 protocol, the client or server can send an "ignore message" at any time. Either side is required to ignore the message whenever it receives it. Within CETerm, this capability is used to hide the password packet in SSH-1, so that a listener cannot tell the length of the user's password. CETerm also uses "ignores messages" for application level keepalives. Certain SSH-1 servers lock up in using "ignore messages".

If this option is not enabled, CETerm will assume that the SSH-1server does not have this bug.

If this option is enabled, CETerm session connection will succeed, but keepalives will not work and the session might be more vulnerable to eavesdroppers than it could be.

If the option is auto-sensed, CETerm will detect the bug and stop using "ignore messages". The default option is Auto-Sense.

Bug – SSH-1 Password Hiding: When talking to an SSH-1 server which cannot deal with ignore messages, CETerm will attempt to disguise the length of the user's password by sending additional padding *within* the password packet. This is technically a violation of the SSH-1 specification, and so CETerm will only do it when it cannot use standards-compliant ignore messages as camouflage. In this sense, for a server to refuse to accept a padded password packet is not really a bug, but it does make life inconvenient if the server can also not handle ignore messages.

If this 'bug' is auto-sensed, CETerm will have no choice but to send the user's password with no form of camouflage, so that an eavesdropping user will be easily able to find out the exact length of the password. If this is enabled when talking to a correct server, the session will succeed, but will be more vulnerable to eavesdroppers than it could be.

This option only applies to SSH-1 servers. The default option is Auto-Sense.

Bug – SSH-1 RSA Auth: Some SSH-1 servers cannot deal with RSA authentication messages at all. If Pageant is running and contains any SSH-1 keys, CETerm will automatically try RSA authentication before falling back to passwords, so these servers will crash when they see the RSA attempt.

If this bug is auto-sensed, CETerm will go straight to password authentication. If this option is enabled when talking to a correct server, the session will succeed, but of course RSA authentication will be impossible.

This option only applies to SSH-1 servers. The default option is Auto-Sense.

Bug – SSH-2 HMAC Key: Versions 2.3.0 and below of the SSH server software from *ssh.com* compute the keys for their HMAC message authentication codes incorrectly. A typical symptom of this problem is that CETerm can fail at the beginning of the session, saying 'Incorrect MAC received on packet'.

If this bug is auto-sensed, CETerm will compute its HMAC keys in the same way as the buggy server, so that communication will still be possible. If this option is enabled when talking to a correct server, communication will fail.

This option only applies to SSH-2 servers. The default option is Auto-Sense.

Bug – SSH-2 Encryption Key: Versions below 2.0.11 of the SSH server software from *ssh.com* compute the keys for the session encryption incorrectly. This problem can cause various error messages, such as 'Incoming packet was garbled on decryption', or possibly even 'Out of memory'.

If this bug is auto-sensed, CETerm will compute its encryption keys in the same way as the buggy server, so that communication will still be possible. If this option is enabled when talking to a correct server, communication will fail.

This option only applies to SSH-2 servers. The default option is Auto-Sense.

Bug – SSH-2 RSA Signature: Versions below 3.3 of OpenSSH require SSH-2 RSA signatures to be padded with zero bytes to the same length as the RSA key modulus. The SSH-2 draft specification says that an unpadded signature **MUST** be accepted, so this is a bug. A typical symptom of this problem is that CETerm mysteriously fails RSA authentication once in every few hundred attempts, and falls back to passwords.

If this bug is auto-sensed, CETerm will pad its signatures in the way OpenSSH expects. If this option is enabled when talking to a correct server, it is likely that no damage will be done, since correct servers usually still accept padded signatures because they're used to talking to OpenSSH.

This option only applies to SSH-2 servers. The default option is Auto-Sense.

Bug – SSH-2 ID in PK Auth: Versions below 2.3 of OpenSSH require SSH-2 public-key authentication to be done slightly differently: the data to be signed by the client contains the session ID formatted in a different way. If public-key authentication mysteriously does not work but the Event Log thinks it has successfully sent a signature, it might be worth enabling the workaround for this bug to see if it helps.

If this bug is auto-sensed, CETerm will sign data in the way OpenSSH expects. If this option is enabled when talking to a correct server, SSH-2 public-key authentication will fail.

This option only applies to SSH-2 servers. The default option is Auto-Sense.

Bug – SSH-2 Re-Key: Some SSH servers cannot cope with repeat key exchange at all, and will ignore attempts by the client to start one. Since CETerm pauses the session while performing a repeat key exchange, the effect of this would be to cause the session to hang after an hour (unless you have your rekey timeout set differently). Other, very old, SSH servers handle repeat key exchange even worse, and disconnect upon receiving a repeat key exchange request.

If this bug is auto-sensed, CETerm will never initiate a repeat key exchange. If this option is enabled when talking to a correct server, the session should still function, but may be less secure than you would expect.

This option only applies to SSH-2 servers. The default option is Auto-Sense.

Username: This is the field where you can specify what user name you want to login as, when connecting through your SSH server. Configuring a username will prevent you from having to explicitly type this on every connection. The default is blank.

SSH Keep Alive: This is the time interval, in seconds, that CETerm will use for triggering SSH level keep-alive frames. Note SSH Keep-Alives are different from TCP protocol Keep Alives. A value of 0 implies not to use SSH Keep-Alives. The default value is 0.

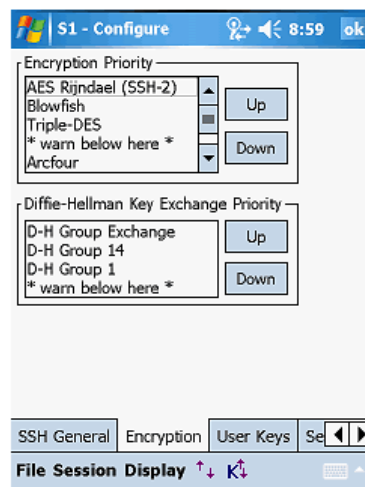
Log Mode: CETerm can maintain a log of all data interaction and exchange performed over the SSH connection. This can be helpful in troubleshooting connection failures. Use this setting to configure the type of log that CETerm should save. The amount of information saved in the log varies with the configured log mode setting. The log file is created in the root directory with the following name format: `/ssh_log_&h.raw` where `&h` is replaced by the hostname. The default mode is None.

- None
- Info
- Debug
- SSH Data
- SSH Raw

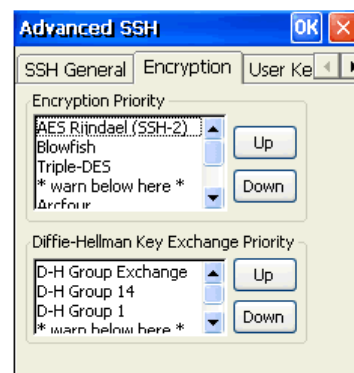
Notices: This button displays SSH specific copyright notice.

Encryption

CETerm supports a variety of different encryption algorithms, and allows you to prioritize which one you prefer to use. Use this configuration tab to set a priority preference for the SSH encryption algorithms.



Windows Mobile



Windows CE

Encryption Priority: Highlight the preferred encryption algorithm and use the up and down buttons to position it in the list box to specify a priority preference order. When you make an SSH connection, CETerm will search down the list from the top until it finds an algorithm supported by the server, and then use that. By default, CETerm list the following encryption algorithms in priority order:

- AES Rijndael (SSH-2)
- Blowfish
- Triple-DES
- * warn below here *
- Arcfour
- * ignore following *
- DES

If the encryption algorithm which CETerm finds is below the 'warn below here' line, you will see a warning box when you make the connection:

The first cipher supported by the server
is single-DES, which is below the configured
warning threshold.

Do you want to continue with this connection?

This warns you that the first available encryption is not a very secure one. Typically you would put the “* warn below here *” line between the encryptions you consider secure and the ones you consider substandard. By default, CETerm supplies a preference order intended to reflect a reasonable preference in terms of security and speed.

In SSH-2, the encryption algorithm is negotiated independently for each direction of the connection, although CETerm does not support separate configuration of the preference orders. As a result you may get two warnings similar to the one above, possibly with different encryptions.

Any algorithms below the “* ignore following *” selection are not used and ignored by CETerm.

NOTE: Single-DES is not recommended in the SSH-2 draft protocol standards, but one or two server implementations do support it.

Diffie-Hellman Key Exchange Priority: Key exchange occurs at the start of an SSH connection (and occasionally thereafter, depending upon your settings in the SSH General tab); it establishes a shared secret that is used as the basis for all of SSH security features. It is therefore very important for the security of the connection that the key exchange is secure.

Key exchange is a cryptographically intensive process; if either the client or the server is a relatively slow machine, the slower methods may take several tens of seconds to complete.

NOTE: If connection startup is too slow, or the connection hangs periodically, you may want to try changing these settings. If you don't understand what any of this means, it's safe to leave these settings alone.

CETerm supports a variety of SSH-2 key exchange methods, and allows you to choose which one you prefer to use. This configuration is similar to encryption algorithm cipher selection. CETerm currently supports the following varieties of Diffie-Hellman key exchange:

D–H Group exchange: with this method, instead of using a fixed group, CETerm requests that the server suggest a group to use for key exchange; the server can avoid groups known to be weak, and possibly invent new ones over time, without any changes required to CETerm's configuration. We recommend use of this method, if possible.

D–H Group 14: a well-known 2048-bit group.

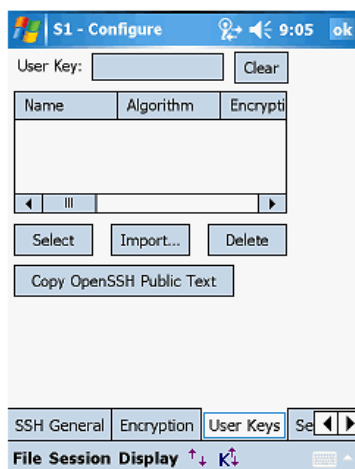
D–H Group 1: a well-known 1024-bit group. This is less secure than group 14, but may be faster with slow client or server machines, and may be the only method supported by older server software.

If the first algorithm CETerm finds is below the “* warn below here*” line, you will see a warning box when you make the connection, similar to the one discussed in the previous (encryption priority selection) configuration.

User Keys

This configuration tab manages the User Keys to be used for authentication with the SSH server. User Keys are used for public key authentication. Public key authentication requires a key-pair consisting of a public key and a private key. The public key can be known by everybody whereas the private key is a closely held secret and is usually encrypted with a corresponding passphrase.

The public key is copied to the server and the private key is imported into CETerm. The private key is stored in CETerm in the encrypted form. The server and CETerm use the keys to authenticate the login request.



Windows Mobile



Windows CE

User Key: This is the key which has been selected for use with the current session. It can only be selected from the keys which have been imported into CETerm.

Clear: This will remove any currently selected key for the session. Without a key, the SSH connection will attempt to use password or other authentication mechanisms.

Select: This button selects the highlighted key in the table to be used as the User Key for this session.

Import: Tap this button to import a key into CETerm. CETerm can import keys generated for OpenSSH and ssh.com servers and some SSH client tools.

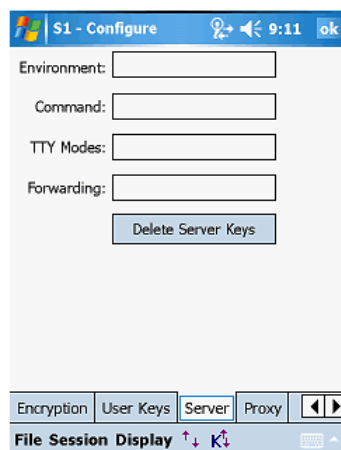
Delete: Tapping this button will delete the highlighted key from the table and remove it from CETerm settings.

Copy OpenSSH Public Text: Tapping this button will copy the public text for the highlighted key into the device cut-and-paste clipboard and display the text in a popup window. This text is commonly put in the “authorized_keys” file in the user’s home directory on the server.

The table contains a list of keys that have been imported into CETerm. These keys are shared by all CETerm sessions. Each key has a “Name” which is assigned by the user when the key is imported. Also shown is the “Algorithm” the key supports, the “Encryption” used for the key, and the “Comment” field of the key.

Server

The configuration attributes on this tab allow you to configure server options.



Windows Mobile



Windows CE

Environment: This setting specifies environment variables to be set on the SSH server. Not all servers will accept new environment variables. The format of the variables is a list of semicolon delimited name-value pairs:

```
name="value";name2=!a=b;c="d"!
```

Each value is delimited by quoting characters. Typically that character will be the double-quote (“). If the value contains double-quote characters, any other printable character may be used, including the single-quote or exclamation mark. Note that the value for name2 contains equal signs, double-quotes, and a semicolon and is delimited by the exclamation mark (!).

Whatever character is used at the start of the value must be used at the end. The default setting is blank.

Command (Advanced): This represents a special command or subsystem to invoke on the SSH server in lieu of an interactive shell. This is typically used for non-interactive host sessions. For most users this will be blank.

TTY Modes (Advanced): This setting can be used to add TTY Modes to be sent to the SSH server. The format of the variables is a list of semicolon delimited name-value pairs:

```
mode="value";mode2="value2"
```

Each value is delimited by quoting characters. See Environment above for details on quoting.

Forwarding (Advanced): This setting defines port forwarding or tunnels supported by this connection. Each tunnel is defined in the following format:

```
[4,6,A][L,R,D][sourcehost:]sourceport=desthost:destport;...
```

Where brackets indicate optional items,

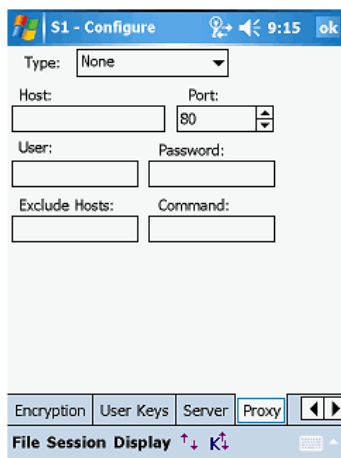
4 – use IPV4, or 6 – use IPV6, or A – autodetect

L – local port forwarded, R – remote port forwarded, D – dynamic (proxy) port
For most users this will be blank.

Delete Server Keys: Tapping this button will erase all “known hosts” server keys stored within CETerm. The user must re-accept all keys during future host key negotiations.

Proxy

The Proxy tab allows you to configure CETerm to use various types of proxy servers in order to make network connections. The settings affect the primary network connection from your CETerm SSH session, but also any extra connections made as a result of SSH port forwarding.



Windows Mobile



Windows CE

Type: This option allows you to configure what type of proxy you want CETerm to use for its network connections. The choices are:

- *None:* No proxy is used.
- *SOCKS 4 or SOCKS 5:* proxy through a SOCKS server.
- *HTTP:* proxy through a web server supporting the HTTP CONNECT command
- *Telnet:* Many firewalls implement a less formal type of proxy in which a user can make a Telnet connection directly to the firewall machine and enter a command such as connect myhost.com 22 to connect through to an external host. Selecting 'Telnet' allows you to tell CETerm to use this type of proxy.

The default setting is None.

Host: This is the DNS name or IP address of the proxy server. The default is blank.

Port: This is the port on which the proxy server is listening. Set this to match the port on the proxy server for connections. The default is 80.

User: If your proxy server requires authentication, enter the username. The default is blank.

Password: If your proxy server requires authentication, enter the password. The default is blank.

WARNING: This password is stored in plain text within CETerm.

NOTE: Authentication is not fully supported for all forms of proxy. Username and password authentication is supported for HTTP proxies and SOCKS 5 proxies.

With SOCKS 5, authentication is via CHAP if the proxy supports it otherwise the password is sent to the proxy in plain text.

With HTTP proxy, the only currently supported authentication method is 'basic', where the password is sent to the proxy in plain text.

SOCKS 4 can use the 'Username' field, but does not support passwords.

You can specify a way to include a username and password in the Telnet proxy command

Exclude Hosts: Typically you will only use a proxy to connect to non-local parts of your network. For example, your proxy might be required for connections outside your company's internal network. Use this setting to enter ranges of IP

addresses, or ranges of DNS names, for which CETerm will avoid using the proxy and make a direct connection instead.

This setting may contain more than one exclusion range, separated by commas. Each range can be an IP address or a DNS name, with a * character allowing wildcards. For example:

`*.somehost.com`

excludes any host with a name ending in `.somehost.com` from proxying.

`192.168.88.*`

excludes any host with an IP address starting with `192.168.88` from proxying.

`192.168.88.*, *.somehost.com`

This excludes both of the above ranges at once.

Command: If you are using the Telnet proxy type, the usual command required by the firewall's Telnet server is `connect`, followed by a host name and a port number. If your proxy needs a different command, you can enter an alternative here.

In this string, you can use `\n` to represent a new-line, `\r` to represent a carriage return, `\t` to represent a tab character, and `\x` followed by two hex digits to represent any other character. `\\` is used to encode the `\` character itself. Also, the special strings `%host` and `%port` will be replaced by the host name and port number you want to connect to. The strings `%user` and `%pass` will be replaced by the proxy username and password you specify. To get a literal `%` sign, enter `%%`.

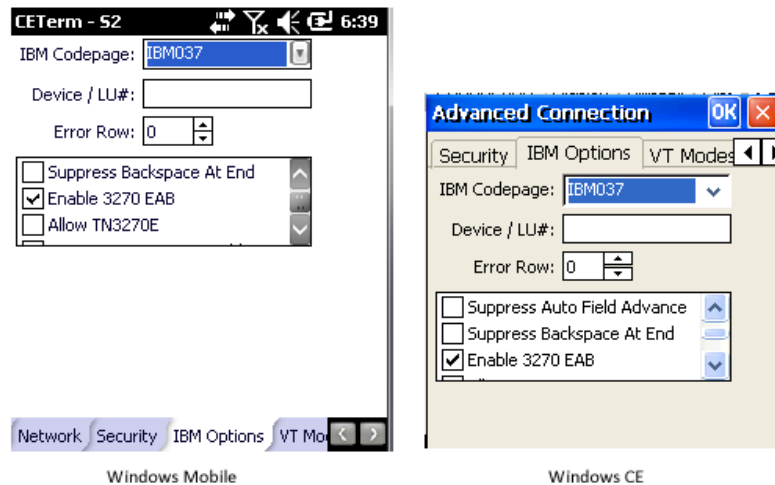
If the Telnet proxy server prompts for a username and password before commands can be sent, you can use a command such as:

```
%user\n%pass\nconnect%host%port\n
```

This will send your username and password as the first two lines to the proxy, followed by a command to connect to the desired host and port. Note that if you do not include the `%user` or `%pass` tokens in the Telnet command, then the 'Username' and 'Password' configuration fields will be ignored.

IBM Options

This tab maintains all advanced configuration attributes relating to IBM (3270 or 5250) terminal emulations.



IBM Codepage: All popular Western European and Eastern European codepages are supported for IBM emulations. By default, only the US English code page (IBM037) is selectable. Codepages for other languages are available from the support section of our website. You can download a codepage from our website for the desired language (CAB file) and install it on your mobile terminal. Once installed, you will then be able to select your language codepage from this list. IBM codepages for popular languages are available for download from the support Wiki on our website. If you have a need for an unlisted code page, please contact us at support@naurtech.com

Device / LU#: The device name / LU# represents a dedicated LU name or number on the server that you want to connect through. Device names are used within IBM SNA world to optimize management of host connection resources. A device name may be associated with a "LU pool" or a specific LU. Device names may also be allocated when connecting to an IBM host through an intermediate gateway. Default is blank.

Error Row: In 5250 emulation sessions, the host application can send an error message for display on the terminal. The host application controls the row on which this error message is displayed. Setting this Error Row value displays the error message on this row. Default is 0 implying no change in the row on which the error message is displayed. Valid error row values are between 1 and 24.

Shift all Error Row content: Typically, a 5250 host application displays an error message on an error row. This error message is only displayed during an actual error. Certain legacy applications require the error row to always be displayed, irrespective of an error message being present on it. Enabling this attribute will force the error row to always be displayed.

Suppress Auto Field Advance: On IBM emulations (5250 and 3270), a host application can define attributes on an input field to automatically advance the cursor to the next field, if the existing field is full. Enabling this flag will ignore this automatic field advance. This support is provided for compatibility with some legacy applications.

Suppress Backspace at End: This setting applies only to terminals with a phone style keypad running IBM emulation. Normally, when entering data using a phone style keypad, the keyboard driver generates a Back Space following each character that it is cycling through; To input "B", you press ABC twice and the keyboard driver generates 'a', 'BS' 'b'. When this setting is enabled, CETerm will not Back Space if the present cursor location is at last char of an input field. This is because cursor did not advance when the previous char was input, due to the cursor being at the end of a field. This will allow overwriting of the last character for phone style keypad rather than deleting a previous character.

Enable 3270 EAB: This is an optional 3270 terminal emulation parameter. If checked, this will allocate an Enhanced Attribute Buffer. EAB support allows for advanced display features such as color and highlighting. This attribute does not apply to 5250 host sessions.

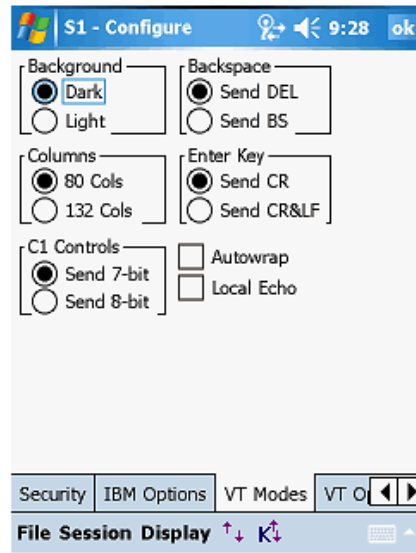
Allow TN3270E: This checkbox setting, when enabled will allow CETerm to negotiate the session connection using the TN3270 Enhanced (TN3270E) protocol. The connection to the host application is generally made through a TN3270E server which allows access to certain resources and functions not available via traditional TN3270 (Telnet 3270) protocol. Enable this checkbox only if you are connecting to your 3270 host application through a TN3270E server.

Keep Cursor in Input Fields: When enabled, this setting will constrain the cursor location to input fields on the screen. This feature reduces keyboard "input inhibit" conditions and speeds data entry.

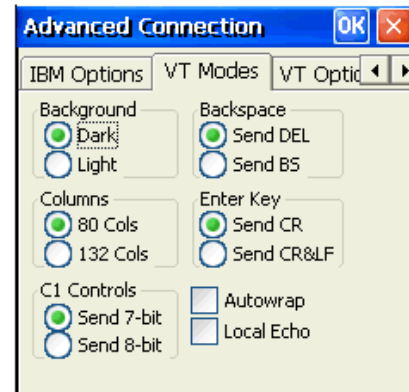
Hide Column Separators: When enabled, this setting will reduce screen clutter by hiding the column separator dots. Hiding the separators can improve screen clarity in harsh viewing conditions.

VT Modes

This tab shows standard VT input and display attribute preferences.



Windows Mobile



Windows CE

Background: This option controls the background shade for VT host sessions.

Backspace: This option configures the backspace key to send either the Delete character or the Backspace character.

Columns: This option specifies the number of columns for the VT host session to be 80 or 132.

Enter Key: This option configures the Enter key to send either a carriage return or a carriage return and line feed.

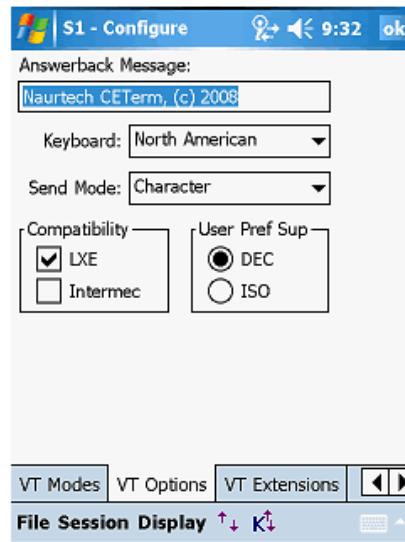
C1 Controls: This option selects 7-bit or 8-bit ASCII control sequences for the host session.

Autowrap: Check this option to enable automatic wrapping of text once it reaches the maximum column width.

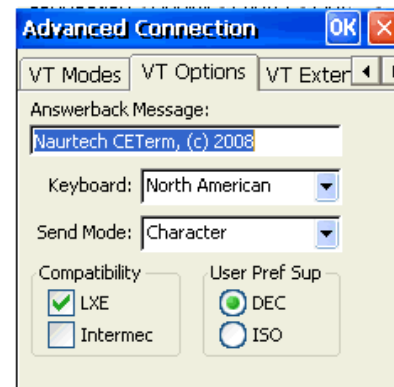
Local Echo: Check this option to echo typed text locally on the terminal.

VT Options

This tab shows additional VT options including support for proprietary protocol extensions.



Windows Mobile



Windows CE

Answerback Message: Host applications may query the VT terminal for a text message answerback response. This response may be used to identify the terminal. Configure the answerback text string as per your VT host application requirement. Default is a Naurtech copyright message string.

Keyboard: Select the keyboard character locale for DEC multinational and National Replacement Character set support. You can select from:

- North American
- British
- Flemish
- Canadian (French)
- Danish
- Finnish
- German / Austrian
- Dutch
- Italian
- Swiss (French)
- Swiss (German)
- Swedish
- Norwegian
- French / Belgian

- Spanish
- Portuguese
- Canadian (English)

Default is "North American".

Send Mode: Check this option to select buffering of text prior to being sent to the host.

Character: This is the default VT behavior. Every character is sent to the host application as soon as it is typed. There is no local buffering.

Line buffered: When enabled, all typed characters are buffered locally until a function key, editing key, Enter, or other non-character is typed. It then sends the buffered keys to the host.

Local Edit (Block): This is an ANSI mode, which allows a host application to define entry fields on a screen. All typing is stored locally until a function key or Enter is typed. The contents of the screen are then returned to the host, depending on the modes set by the host application.

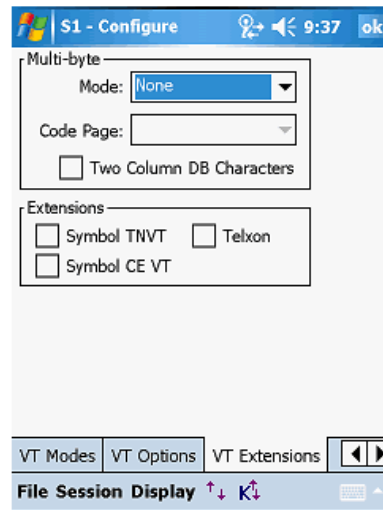
Both Line buffered and Local Edit modes optimize usage of network bandwidth and host resources. However compatibility with these modes is dependent upon the VT host applications.

Compatibility: Hardware vendors Intermec Technologies and LXE have proprietary implementations of block mode support for VT host sessions. Check the appropriate box for block mode compatibility.

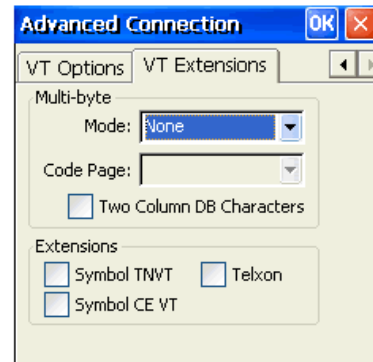
User Preference Supplemental: This is the user preferred supplemental character set. Default is DEC

VT Extensions

This tab shows proprietary extensions for international multi-byte character sets and legacy VT extensions.



Windows Mobile



Windows CE

Multi-byte: This group box wraps all configuration settings for international languages such as Chinese Traditional, Chinese Simplified, Japanese, Korean, Thai, Hebrew, Greek and others. This support is only available for VT emulation sessions.

Mode: This selects one of the several multi-byte modes to support single-byte and double byte character sets. Select the type of character set encoding. You can select from:

None: Use standard VT international character sets or National Replacement Character (NRC) Sets.

DBCS: Double Byte Character Set. Selecting this encoding will process double-byte characters based on the selected code page. Note that 8-bit VT commands are illegal in DBCS mode.

SBCS: Single Byte Character Set. Selecting this encoding will process single-byte characters based on the selected code page. Note that 8-bit VT commands are illegal in SBCS mode.

UTF-8: Selecting this encoding will process the data stream as Unicode in the UTF-8 encoding. Note that most 8-bit VT commands are illegal in UTF-8 mode.

Code Page: When DBCS or SBCS modes are selected, this setting allows selection of the appropriate code page. Only the code pages available on the mobile terminal will be listed. If none are available, the mode will be forced back to None.

All our emulators display international character sets using Windows CE

Font Linking. This makes it possible to link one or more fonts, called *linked fonts*, to another font, called the *base font*. Once you link fonts, characters that do not exist in the base font are displayed from the linked fonts. For example, linking a Japanese font to a Latin font gives you the ability to display Japanese characters when using a Latin font.

Font linking is typically used to enable Roman fonts to display non-Roman characters. To extend font linking on your mobile terminal, you can examine the following registry setting to determine the mappings of linked fonts to base fonts.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\FontLink\SystemLink
```

You can add additional links by creating additional registry values:

```
"base font face name" = "path and file to link to," "face name of the font to link"
```

Example: In this example, the Japanese-specific font MSGothic is linked to the base Tahoma font. When searching for a character, the Tahoma font is searched first followed by the MSGothic font. This enables support for a larger variety of characters without switching fonts.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\FontLink\SystemLink]
```

```
"Tahoma"=\\Windows\\msgothic.ttc,MS PGothic
```

Two Column DB Characters: This setting only applies when displaying characters requiring double byte character sets. When enabled, it forces interpretation that the double byte character consumes two columns in screen buffer. For some languages, this helps with character alignment.

Extensions: This group box wraps all VT protocol extensions that are proprietary to legacy emulations. These are provided to easy migration from legacy terminals to newer Windows CE terminals.

Symbol TNVT: Enable extensions from Symbols 3000 series and Telxon TE such as enabling the scanner, setting fixed screen mode, reporting the IP address, exiting the program, and sending special control characters.

Symbol CE VT: Enable extensions in Symbols VT220 CE TE, such as reporting the MAC address, enabling the scanner, sounding tones, and setting block or character modes.

Telxon: These are similar to the Symbol TNVT extensions.

Display

This table below shows the hierarchy of configuration attributes for the Display related settings.

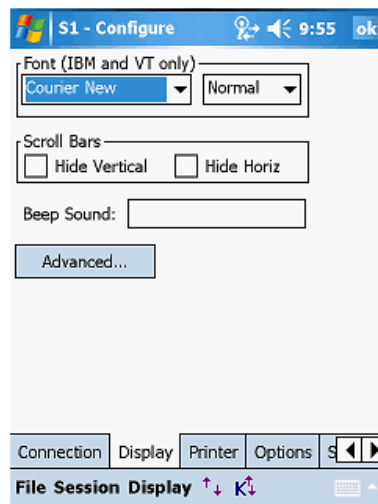
Display		
Font		
Type		
Weight		
Scroll Bars		
Hide Vertical		
Hide Horizontal		
Beep Sound		
Advanced		
→	Hide / Show	Font
	Hide All Bars *	Allow Proportional Fonts
	All Bars at Bottom *	Force Proportional Characters
	Hide Menu Bar	Force Fixed Width Characters
	Hide Keybar	Width Factor
	Hide Toolbar	
	Hide OIA (IBM only)	
	Hide SIP button **	
	Lock SIP on Hide **	
	Disable Browser Auto SIP *	
	Auto-Fit to Browser Screen *	
	Display Browser Errors *	
	Show Macro on Play	
	Show Start Bar on Exit	
	Colors	
	Scheme	
	Attribute	
	Intense	
	Select Color...	
	Cursor	
	Cursor Options	
	Full Block	
	Underline	
	Half Block	
	Automatic Scrolling	
	None	
	Center Cursor	
	Visible Cursor	
	Locked	
	Row	
	Col	

* Option only available on Windows CE OS platform terminals

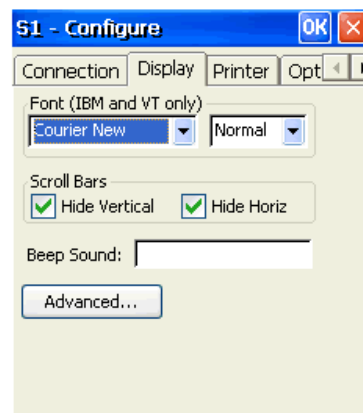
** Option only available on Windows Mobile OS platform terminals

The terminal display may be configured to optimize screen real estate and readability. These options may be configured for connected or non-connected host sessions. Hot keys are available to toggle the options on and off.

- From the application menu, Select [**Session**] [**Configure**] or tap the "Configure" button  on the toolbar.
- A "Configure" dialog box will come up.
- Choose the "Display" tab



Windows Mobile



Windows CE

Font: This group allows configuration for a selectable font and its weight.

The font name is a fixed-width True Type font that is used to display the terminal text. To enhance readability, you may install additional fixed-width True Type fonts on the mobile terminal by copying the associated .TTF file to the \Windows or \Windows\fonts directory. Your font will automatically appear in this list and may be selected from this font selection option.

NOTE: Except in special cases, only fixed pitch true type fonts will be visible in this dropdown list. If VT emulation has proportional fonts enabled, then you will also see proportional fonts

The font weight selects the boldness level used to display the terminal text. The following shows the selectable options.

Default
Thin
Light

Normal
Medium
Bold
Xbold
Heavy

NOTE: The appearance of these weights is dependent on the selected font and the display resolution. In some cases, only 2 or 3 different weights can be seen.

Scroll Bars: This group of attributes configures hide and show settings for the horizontal and vertical scroll bars.

Hide Vertical: Checking this box will hide the vertical scroll bar. Pressing the hotkey **[Ctrl] [Shift] [V]** or the toolbar button  will alternate between the hide and visible states.

Hide Horiz : Checking this box will hide the horizontal scroll bar. Pressing the hotkey **[Ctrl] [Shift] [H]** or the toolbar button  will alternate between the hide and visible states.

NOTE: For Web Browser sessions, the visibility of scroll bars may be overridden by the HTML page contents. Also, changes to these settings may not take effect until the next page is loaded.

Beep Sound: This is an optional beep sound configuration. It controls the sound of the standard terminal bell or beep. For devices that support .wav files, you can enter any .wav file available in the standard sound locations on the device. For mobile terminals that support tone generators, you can specify a custom tone. The custom tone has the following format:

vvFFFttt or vvFFFtttvvFFFttt or vvFFFtttvvFFFtttvvFFFttt, etc.

where

vv	Volume	is the volume of the beep. The range is 00-10 where 0 is off and 10 is loudest.
FFF	Frequency	is frequency in 10 Hertz units. A value of 200 is 2000 Hertz, 300 is 3000 Hertz.
ttt	Time	is the length of the beep in 10ms units. A value of 050 is ½ second. 100 is one second.

An example of the setting can be 05300100. This will play a one second beep of 3000 Hz at half volume. Don't forget the leading zeros.

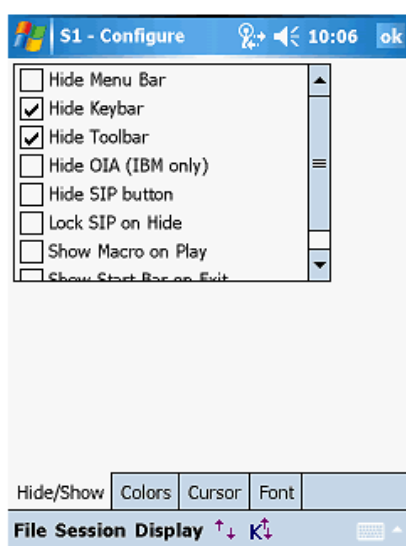
Advanced: This button opens an advanced display configuration dialogs.

Hide / Show

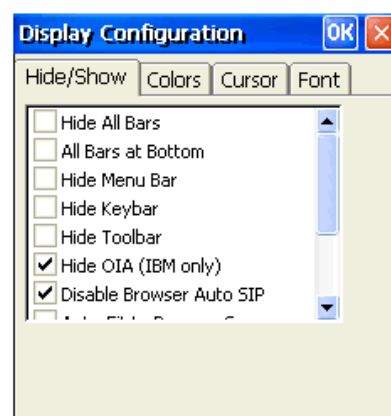
This tab holds attributes to control the visibility of various application and display widgets.

Hide All Bars: This configuration option is only available on Windows CE OS platform devices. Since the Toolbar and Keybar are part of the application menu, on Windows CE devices, enabling this option hides all three.

All Bars at Bottom: Checking this box will move the menu to the bottom of the screen. Pressing the hotkey **[Ctrl] [Shift] [B]** will alternate the location between the top and bottom of the screen. This option is only available for Windows CE OS platform devices. It is not available on terminals running Windows Mobile OS.



Windows Mobile



Windows CE

Hide Menu Bar: Checking this box will hide the application menu. This is the main application menu with **[File] [Session] [Display]** options.

Hide Keybar: Checking this box will hide the configurable Keybar. The Keybar is a set of configurable buttons that can be associated with application operations.

Hide Toolbar: Checking this box will hide the application toolbar. The toolbar is the main application toolbar.

NOTE: Hiding the application Menu, Toolbar and Keybar will give you additional rows of screen real estate and assist in locking down the mobile terminal.

Refer to the section “Accessing Configuration from Full Screen Mode” to restore the application menu.

Hide OIA (IBM Only): Checking this box will toggle hiding of the OIA or the Operator Information Area. This option applies only to IBM 3270 and 5250 emulations. Pressing the hotkey **[Ctrl] [Shift] [O]** will alternate between the hide and visible states.

Hide SIP Button : This configuration setting is only available for Windows Mobile OS platform devices. Checking this box will hide Windows Mobile SIP (Soft Input Panel) button.

Lock SIP on Hide: Checking this box will cause the SIP (Soft Input Panel) to be locked down when closed. This configuration setting is only available for Windows Mobile OS platform devices.

 **Disable Browser Auto-SIP:** On Windows CE platform terminals, when running web browser sessions, the Soft Input Panel (SIP) automatically pops up if the cursor input focus is in an input text box. This may not necessarily be the desired behavior for your web application. Enabling this setting prevents the SIP from popping up when focus set to text box in Windows CE browser.

 **Auto-Fit to Browser Screen:** This setting is only available for Windows CE OS platform terminals. When enabled, this setting turns on auto-fit formatting for Windows CE Browser similar to as is available on Windows Mobile Browser. The Web Browser will try to display the page in one column with no horizontal scroll.

 **Display Browser Errors:** When enabled, this setting will allow display of JavaScript errors on web pages when displayed in a Browser session on a Windows CE OS platform terminal. For equivalent functionality on a Windows Mobile terminal, you need to manually set a registry value.

Show Macro on Play : By default, the macro toolbar bar is not visible when a macro is being played back. Checking this option will make the macro toolbar visible during playback.

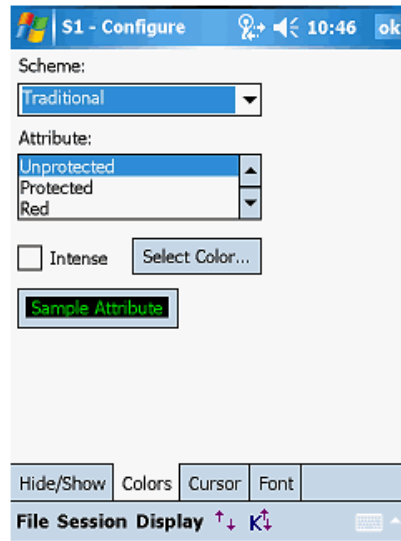
NOTE: It may be necessary to make the macro toolbar visible so that CETerm receives application focus to ensure the “played back” keystrokes are sent to CETerm.

If you run an auto-login macro and do not get focus back to your telnet host server application, you should enable this flag. Doing so will ensure you receive focus back in CETerm

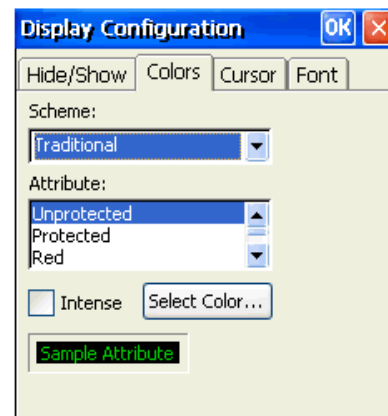
Show Start Bar on Exit: Normally, CETerm restores the state of the Start Bar to however it was found when it was launched. Enabling this setting forces the Start Bar to be made visible if the user exits our application, ignoring the original state of the Start Bar.

Colors

: CETerm provides predefined color schemes to enhance readability of the terminal text on the terminal. In addition, a (customizable) "Custom" color scheme is also provided. The Custom scheme may be configured to suit the user's preferences.



Windows Mobile



Windows CE

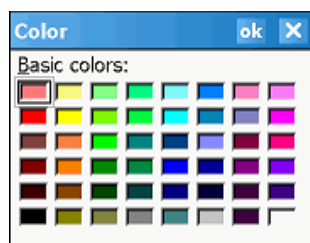
Scheme: To select a predefined color scheme, choose one from the "Scheme" drop down box. The sample box will change to reflect the current selected attribute foreground and background colors. The following pre-defined color schemes are available.

Traditional	The traditional IBM terminal "green screen" color scheme
Black on White	Used primarily on mobile terminals with non-color LCD displays
White on Black	Inverse of Black on White
Factory	Scheme optimized for factory lighting and color displays
Custom	User configurable scheme

Attribute: This lists display attributes for which colors may be changed as part of creating a "Custom" color scheme. Under VT emulation, the attributes correspond as follows.

VT Attribute	IBM Attribute
Normal	Unprotected
Bold	Intense version of Unprotected
Blinking	Protected
Blinking and Bold	Intense version of Protected

Select Color: : This button invokes the "Color" dialog to select a color for an attribute



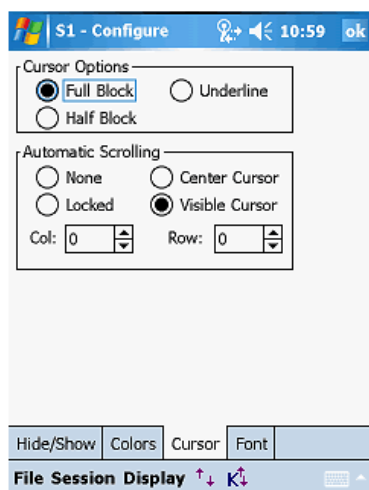
Intense: This check box, when selected, applies the custom color to the "intense" version of the selected attribute. This option applies to 3270 and VT emulations.

Sample Attribute: This is a sample box that shows the foreground and background color of the currently selected attribute. To create a custom color scheme, select the attribute from the attribute list box.

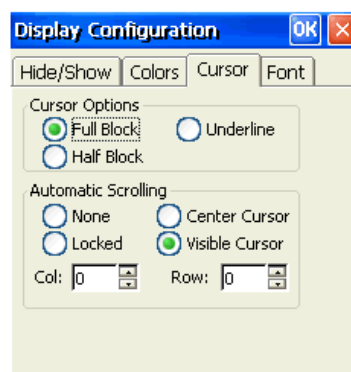
- Choose the attribute, whose color is to be changed
- Tap the **Select Color...** button.
- You will see a "Color" dialog.
- Select the desired color for the attribute. Press OK
- The Sample box will change to reflect the newly selected color.
- For updating colors associated with the "Intense" mode of an attribute, check the "Intense" box then select the desired color.

Cursor

: Cursor options are provided for easy visual identification of current input field. Automatic scrolling parameters offer settings to configure the row and column positions for the current visible cursor position.



Windows Mobile



Windows CE

You may configure cursor type and auto-scrolling options for the terminal.

Cursor Options: This option allows you to change the cursor appearance. Three options are available:

Full Block: The cursor appears as a full character block ()

Half Block: The cursor appears as a bottom half block ()

Underline: The cursor appears as an underscore line ()

Automatic Scrolling: This option enables automatic scrolling so the current cursor position is always visible. This option is particularly helpful when the host screen too large to fit in the terminal display screen. The following auto-scrolling options are available

None: No automatic scrolling is preferred.

Center Cursor: : In this mode the cursor is always as close as possible to the center of the screen. When scrolling limits are reached, the cursor will move toward the edge of the terminal display.

Visible Cursor: : In this mode the cursor is always visible. The display is scrolled vertically and horizontally to prevent the cursor from moving out of view.

Locked: In this mode you can specify a starting row and column position at which to lock the cursor. This would force every new screen to automatically start its top left edge at the specified row and column position.

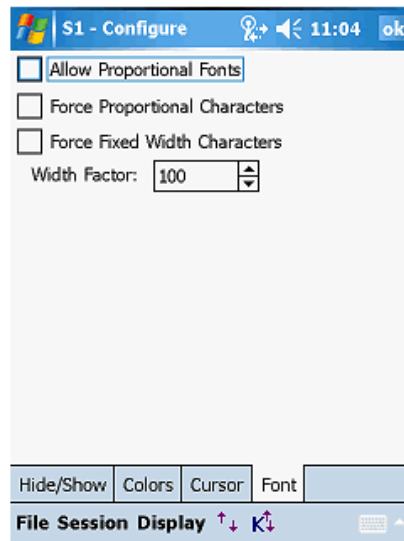
Col: This is the column number for the top left position of display. It is applicable only with the “Locked” scrolling option

Row: This is the row number for the top left position of display. It is applicable only with the “Locked” scrolling option

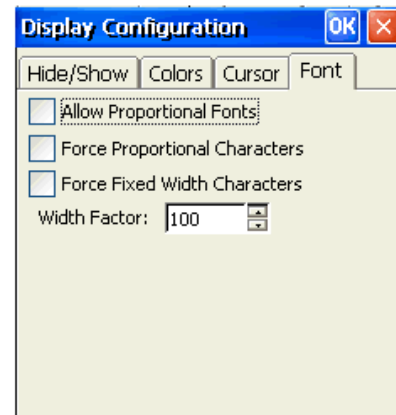
NOTE: Only the starting position of the display text is locked. The user can still use scroll bars, touch stylus, buttons, and remapped keys to scroll the screen. If no scrolling is desired, you must hide or unmap these other controls.

Font

: This tab holds advanced font settings for enhanced readability and international language character glyphs.



Windows Mobile



Windows CE

Allow Proportional Fonts: Traditionally, only fixed pitch fonts have been used with terminal emulation. This option, when enabled, will allow proportional fonts in the font selection box. Some Asian language fonts are only available with proportional spacing. Usually, the Asian fonts are “linked” to the Tahoma font, which is also proportional. To display all characters, this box can be checked and the Tahoma font selected. Proportional fonts can also be used to improve readability of the display if the host application does not require column alignment of the screen (see Force Fixed Width Characters).

Force Proportional Characters: This option is enabled to force the display to draw with proportional spacing even when the selected font is fixed pitch. This setting may be required when a proportional Asian font is linked to a fixed pitch font such as Courier New and Courier New is the selected font. This setting overrides “Force Fixed Width Characters”.

Force Fixed Width Characters: This option will force the display to draw proportional fonts with a fixed width spacing. This can result in irregular displays where the narrow characters (e.g., 'i') appear scrunched to the left of their "cell" and the wide characters (e.g., 'm') to overlap their neighbors on the right. This setting is used to force a display into traditional column alignment and may be needed with host applications that display tables or character based graphics.

When forcing to fixed width, a "nominal" width must be computed for the font and it is narrower than the widest characters. The next parameter can be used to spread out the characters.

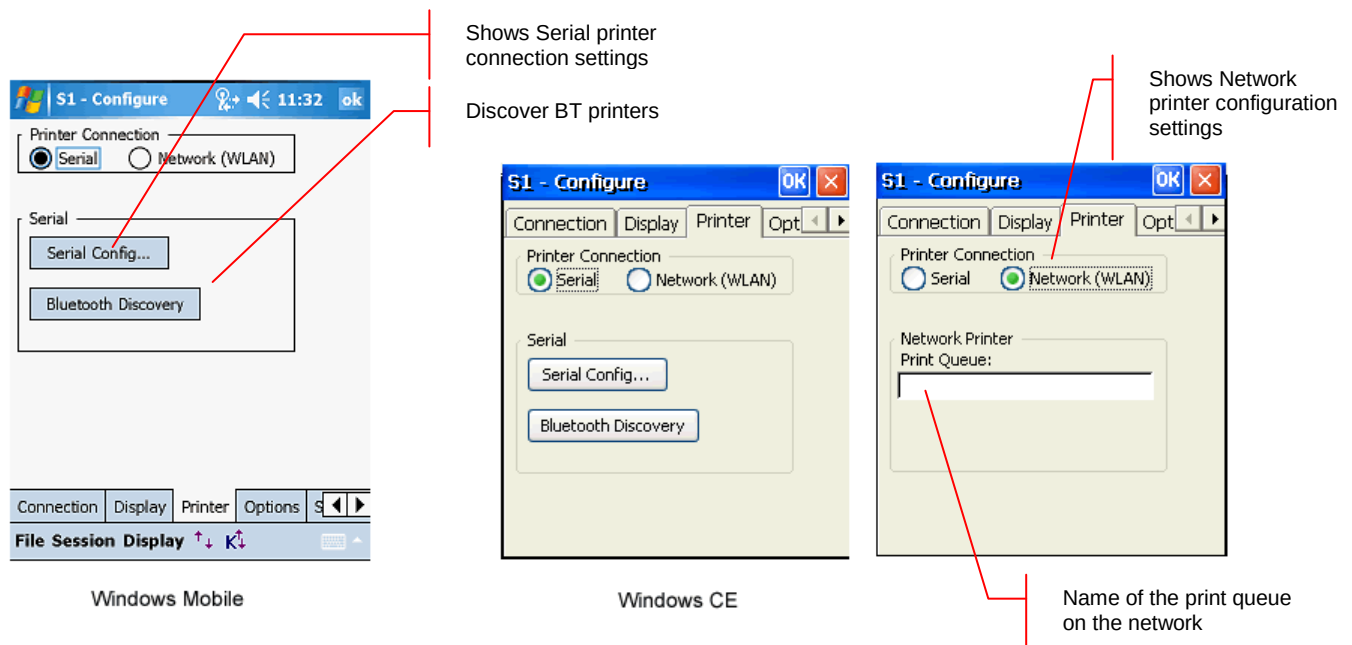
Width Factor: This applies to a factor to the "nominal" width used when forcing proportional fonts to fixed width. A value of 100 is 100% of the "nominal" width. Values larger than 100 spread out the characters and values smaller than 100 squeeze them together. You may use "Force Fixed Width" and the "Width Factor" with fixed-pitch fonts to get more readable displays.

Printer

This table shows the hierarchy of settings for configuration a tethered or networked printer.

Printer		
Serial		
Network (WLAN)		
→	Network Printer	
	Print Queue	
Serial Config		
→	Serial Port Config	
	COM Port	
	Baud Rate	
	Data Bits	
	Parity	
	Stop Bits	
	Timeout	
	DTR Control	
	RTS Control	
	CTS Out	
	DSR Out	
	XOnOff Xmit	
	XOnOff Recv.	
Bluetooth Discovery		
→		

Host applications may print to serial, IrDA, Bluetooth or 802.11B network attached printers. You can configure the printer from the "Printer" options tab.



Printer Connection: Select the type of connection used to access the printer. This may be serial or a Network connection.

Serial: Select this button for printers attached via a serial port, IrDA or Bluetooth protocols

Network (WLAN): Select this button to print to a Windows print queue or directly to a network attached printer.

Serial Config

This button opens a serial port configuration dialog.

The 'Serial Port Config' dialog box contains the following settings:

- COM Port:** BT Printe
- Baud Rate:** 9600
- Data Bits:** 8
- Parity:** None
- Stop Bits:** 1
- Timeout:** 10
- DTR Control:** Enable
- RTS Control:** Enable
- CTS Out:** ☐
- DSR Out:** ☐
- XOnOff Xmit:** ☒
- XOnOff Recv:** ☒

COM Port: This is the serial communications port to which the printer is attached. Choices depend on the mobile terminal. Users may select from COM, IrDA, Bluetooth, None, or one of the Virtual COM (VCOM0 - 9) ports. The default value varies with the hardware device. The None value can be selected to act as a “sink”. Printing to the “None” device will always succeed. For printing to an infrared printer, select IrDA port. If IrDA is selected, all settings except Timeout are ignored. Use the VCOMx ports for custom connections such as virtual Bluetooth ports.

Baud Rate: The baud rate at which the communication device operates. It varies from 110 to 256K bits per second. Default is 9600.

Data Bits: The number of bits in the bytes transmitted and received. Default is 8.
The number of bits in the bytes transmitted and received. Default is 8.

Parity: The parity scheme to be used to communicate with the printer device. Default is “None”.

Stop Bits: The number of stop bits to be used. Default is 1.

Timeout: The amount of time to wait prior to aborting a connection if the printer is not responding.

DTR Control: The DTR (data-terminal-ready) flow control. Default is “Disable”.

RTS Control: The RTS (request-to-send) flow control. Default is “Disable”

CTS Out: The CTS (clear-to-send) signal monitoring for output flow control. If box is checked and CTS is turned off, output is suspended until CTS is asserted again.

DSR Out: The DSR (data-set-ready) signal monitoring for output flow control. If this member is TRUE and DSR is turned off, output is suspended until DSR is asserted again

XOnOff Xmit: When checked, use XON/XOFF flow control during transmission.

XOnOff Recv: When checked, use XON/XOFF flow control during reception.

Bluetooth Discovery

This button triggers the automatic discovery of Bluetooth devices (printers). It requires the COM Port setting under Serial Port configuration to be “BT Printer” or “BT COM”. A list of discovered Bluetooth devices is provided in a selection list. Select your Bluetooth printer from the list. On certain terminals, you may have to enable Bluetooth service through the control panel.

Network Printer

Configuration settings for a network printer

Print Queue: This is the Windows print queue name or the hostname of a printer.

The Windows print queue uses Windows print protocols and assumes that the queue is available on the network. You may be prompted for username and password if the print queue is secured. Also, you should receive notification when the print job completes.

The print queue uses the following naming convention:

Name or IP address of the print server	\\MyPrintServerName\PrintQueueName
	\\192.168.1.223\PrintQueueName

To print directly to a network connected printer, enter the hostname or IP address of the printer. By default this will connect to port 6101 and send all print content directly to this port. Optionally, you can specify a different port.

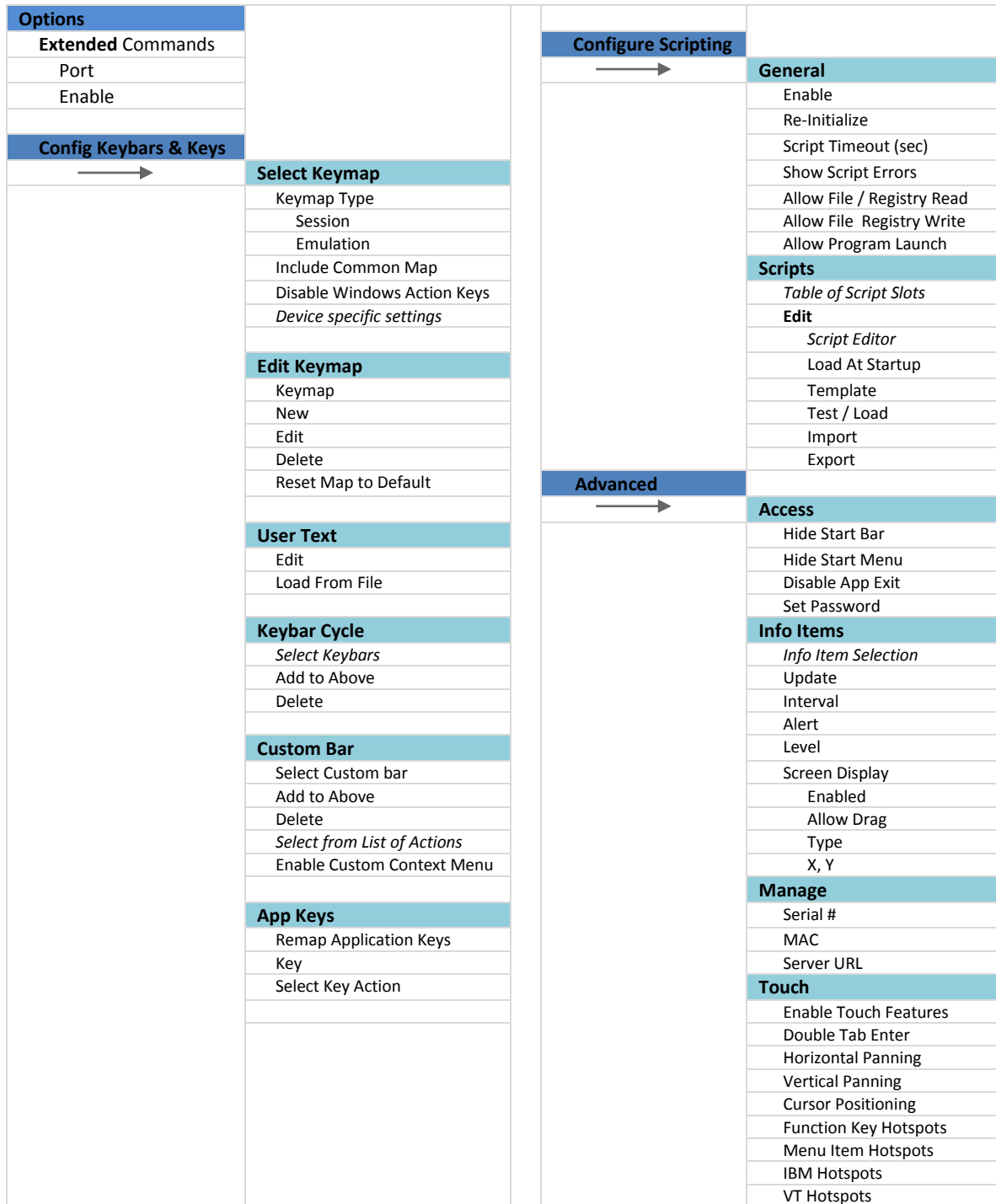
The hostname uses the following naming convention:

hostname:port

where hostname is either a symbolic name or an IP address and port is a number.

Options

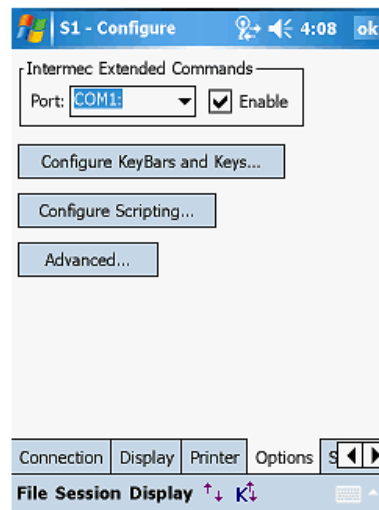
The diagram below shows the hierarchy of configuration attributes for the Options tab.



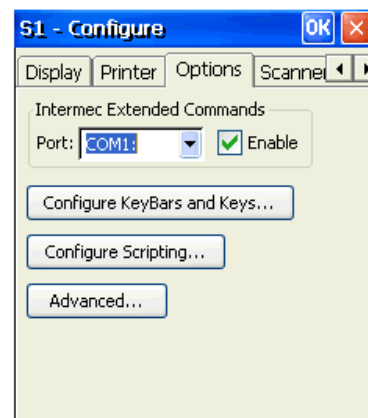
The Options tab includes configuration for key remapping, Scripting, device access control, Indicators, Automatic licensing and touch screen features.

All key remapping is configured right on the mobile terminal. Configuration dialogs are accessible through the “Configure Keybars and Keys...” button.

 The Scripting capability has been enhanced even more with this version. New automation objects have been added and existing ones enhanced. You can import, edit, test and run scripts right on the mobile terminal. Scripts provide a powerful mechanism to automate workflows. All scripting is configuration is accessible through the “Configure Scripting” button. Please refer to a separate Scripting Guide which describes the CETerm Scripting functionality and usage in detail.



Windows Mobile



Windows CE

Intermec Extended Commands: This setting is part of the “Legacy Support”. It enables proprietary extensions from Intermec for controlling peripheral devices. “Extended Commands” are extensions to the terminal emulation protocol data stream (3270, 5250 or VT) that allow host applications to control serial printers, card readers etc. All our emulators support Extended Commands for bi-directional communication with peripherals such as Serial printers and Magnetic Card Readers for all three terminal emulations.

Port: Intermec Extended Commands are sent to this port to access and control peripheral devices.

Enable: Checking this box will enable support for Intermec Extended commands

Configure KeyBars and Keys:

This button invokes configuration tabs for key remapping and Custom Keybar configuration.

Configure Scripting: This button invokes configuration tabs for all Scripting related settings.

Advanced: This button invokes configuration tabs for access control and touch screen attributes.

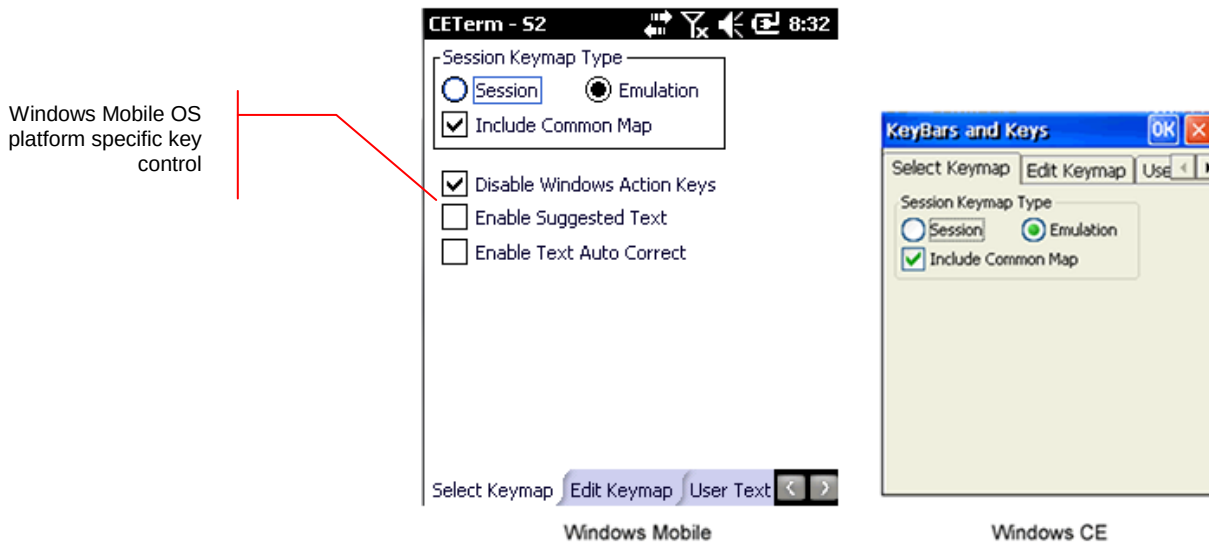
Configure KeyBars and Keys

The “Config KeyBars and Keys...” button is used to remap mobile terminal hardware keys, configure custom KeyBars and associate device application keys with operations (only on Windows Mobile terminals)

Select Keymap

A “Keymap” is a collection of remap bindings which associate keys with corresponding actions. Most hardware keys can be remapped to perform any action such as simulating a function key, entering a string of text, sending a custom VT escape sequence or running a Script. Keys that control screen brightness, sound volumes, and other Windows CE actions, often cannot be remapped. The two main steps for key remapping are selecting the type of Keymap to use, and editing the Keymap.

NOTE: Certain settings which are specific to the Operating System platform or to the mobile terminal are only visible in the device tailored versions of CETerm for that OS and / or device.



Select Keymap Type: Selects “how” the configured Keymap bindings will apply to connected host sessions. The available choices are:

Session: The key remapping configured in this session will be associated with this host session only (say S1, if S1 is being configured). When you choose this selection, the key remap bindings will not be available in another session (say S2 or S3 etc).

Emulation: The key remapping configured is associated with a particular type of emulation or host connection; such as 3270, 5250, VT or HTML. This Keymap can be shared with other host sessions running the same host type connection. As an example, if sessions S1 and S3 are configured for 5250 emulations and S2 is configured for a Web Browser session, then all 5250 Keymap configurations will be available to all 5250 sessions (S1 and S3). These will not be available to session S2 as it is not a 5250 emulation session.

Include Common Map: CETerm provides a predefined set of key remap bindings which are common to all sessions by default. When checked, the Common keymap will be added to the session or emulation keymap. You can also modify the Common keymap binding separately.

Device Specific Key remap configurations: Certain mobile terminals, like the Honeywell Dolphin series and the Compsee MAT terminals may have device specific key remap bindings which can be loaded. These key remaps are based on popular legacy overlays for various emulations. You can enable inclusion of these key remaps using the device specific configuration attributes.

These settings will only be visible when running the device tailored versions of CETerm on applicable mobile terminals.

Disable Windows Action Keys: The Windows Mobile Operating System includes an OS Shell to manage its special user interface. For devices running Windows Mobile, the OS shell intercepts certain function keys like the F6 and F7 for volume up / down controls thus preventing their use in any application (like CETerm). By enabling this setting, CETerm prevents the OS Shell from intercepting these keys.

This setting is specific to the OS platform and is only visible in CETerm running on Windows Mobile platform devices.

Enable HHP TE Keypad Mode: This is a device specific setting only available on certain Honeywell Dolphin terminals. When checked, it loads the emulation specific legacy key remap to match overlays designed for Honeywell (HHP) Dolphin terminals.

 **Enable Suggested Text:** When checked, you will be offered suggestions for complete words from its predictive dictionary when typing data into an input field. This setting is only available on Windows Mobile OS platform terminals.

 **Enable Text Auto Correct:** When checked, the input being typed will be automatically corrected for spelling. This setting is only available on Windows Mobile OS platform terminals.

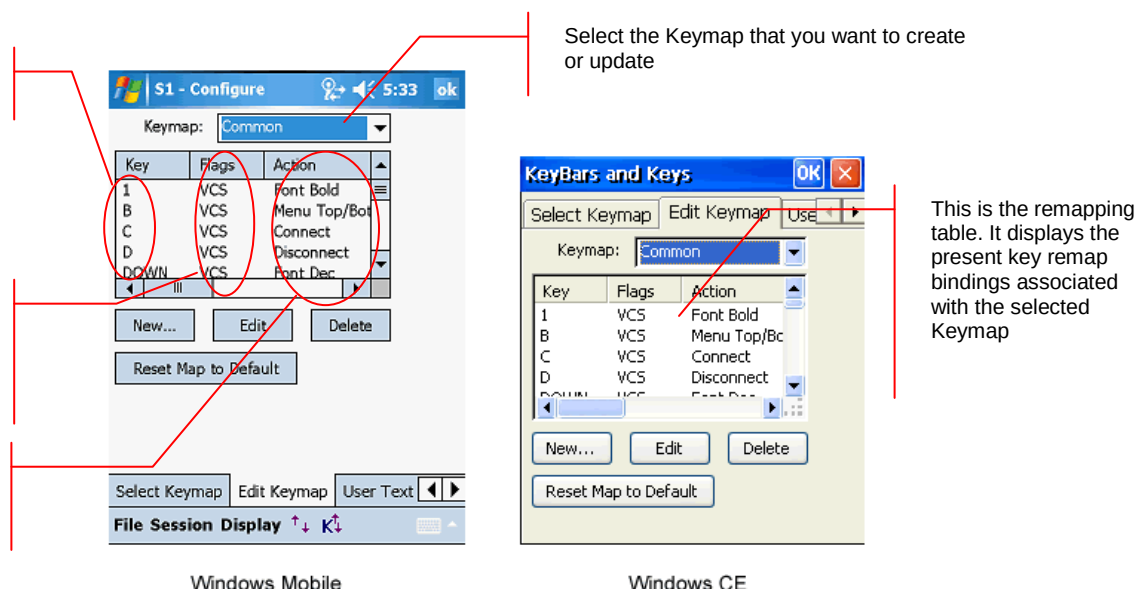
Edit Keymap

You can add, modify and remove key remap bindings using this configuration tab. The current bindings for the default selected Keymap are visible in the table.

Key: These keys are being remapped

Flags: These are the modifier / state keys which must be pressed along with the hardware key being remapped

Action: This is the new action operation, which the remapped key will now invoke



Keymap: Select the Keymap you wish to edit. You may select the session specific map for the current session (Session #), an emulation Keymap (3270, 5250, HTML, or VT), the Base Keymap, or the Common Keymap. When you select the Keymap which you want to configure, the table is automatically populated with existing configured bindings for that Keymap.

Key: This column shows the ASCII character or "Virtual Key" symbol for the remapped physical key. If a symbol is not available, the key may be shown as a hexadecimal value.

Flags: This column shows the type of key and any modifier keys, which represent the key combination for this binding. The physical key along with the configured modifier key must be pressed to invoke this Keymap.

V indicates a Virtual Key.

A indicates "Alt" is pressed with the key.

C indicates "Ctrl" is pressed with the key.

S indicates "Shift" is pressed with the key.

As an example, the third entry in the table of the image above shows a key combination of (C)ontrol + (S)hift + C for a session "Connect" action.

NOTE: If you have Meta Keys configured, you may see additional state key options.

Action: This column shows the action that the key remapping invokes. If the key is associated to invoke a "Text #" action, the current text is shown.

New: This button opens a **New Key** dialog to add a new key remap binding to the selected Keymap. Make sure that you have correctly selected the Keymap to which you want to add a new binding.

Edit: This button allows modification of the highlighted key binding from the list. Tapping this button will open an **Edit Key** dialog. Alternatively you may double-tap the entry in the list to modify it.

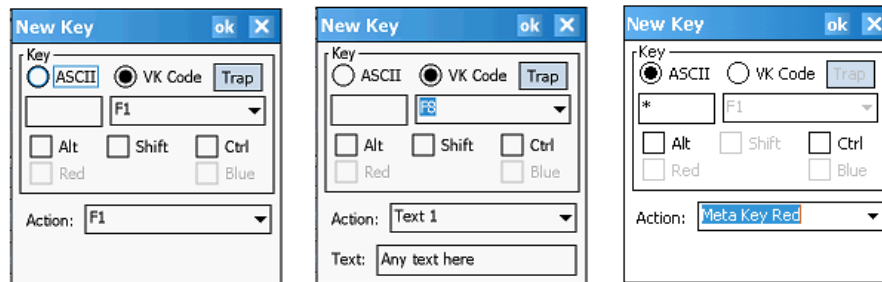
Delete: Pressing this button will delete the current highlighted key remapping from the list.

Restore Map to Default: Tap this button to reset the current map to the default contents.

NOTE: If you have enabled device specific key remaps to be included under the "Select Keymap" tab, you must tap "Restore Map to Default" button to include the default key remap bindings for the selected emulation. You will see the table being populated with the new key remap bindings for that emulation.

The same is true if you are disabling the use of device specific key remap bindings.

New / Edit Key Dialog This dialog is used to edit existing Keymap bindings and add new ones. If a new or edited Keymap binding conflicts with an existing binding, you will be given a choice to apply or reject the new binding. Note that this dialog may vary in its configuration attributes depending upon specific device tailored versions of CETerm, which may include default key remap bindings for legacy support.



ASCII: When creating new keys, always use the "Virtual Key" (VK) mode unless the VK code cannot be determined. VK codes may not be known usually for non-standard hardware keys. If you know that the key you want to remap generates an ASCII character but you cannot determine the VK code, then use the "ASCII" mode and enter the character that is generated. Enter the desired character in the box below.

VK Code: Use the VK code for this key remap binding. Select the virtual key from the dropdown list or enter a hexadecimal value in the form "0x5a".

Trap: If you are not sure about the VK code associated with a physical key (or key combination) which you would like to remap, simply tap this button. CETerm will then monitor the next key (or key combination) you press and automatically enter the associated VK code for that key (or key combination). This feature helps you ensure that you are remapping the correct VK code associated with the physical key.

We recommend always using the Trap button to let CETerm determine the VK code of the physical key that you want to remap.

Alt: If checked, "Alt" must be pressed with the key for this key remap.

Shift: If checked, "Shift" must be pressed with the key for this key remap.

Ctrl: If checked, "Ctrl" must be pressed with the key for this key remap.

!ASC - This option is only available for Meta key configuration. It means "Ignore Alt, Shift and Control" states. When checked, the Meta key will be effective regardless of the Alt, Shift, or Control states. Usually this option is checked to allow the most flexible key combinations.

Toggle - This option is only available for Meta key configuration. When enabled the Meta key will "toggle its state" each time the key is pressed. Otherwise, the state is set when pressed and cleared when the key is released. Usually, this option is checked.

NOTE: Some keyboards require the "key up" action of a key before another key can be pressed. For these keyboards, the "toggle" option *must* be checked, otherwise no other key can ever "see" the Meta state.

One-shot - This option is only available for Meta key configuration. Enabling this setting will force the Meta key state to reset after the next key is pressed, whether or not the next key was part of a Meta key translation. If this option is unchecked, the Meta state remains set until the Meta key is pressed again. Usually, this option is checked.

Action: Select the desired action from the list. This is the action that the key will be remapped to.

Text: This edit field is visible only if a "Text #" action is selected. You may edit the associated text directly. It can include an IDA code (see Appendix), a Script, an escape sequence or simple ASCII user string.

User Text

All user text strings may be edited via this tab. Text strings may contain special escape sequences for VT or sequences of actions:

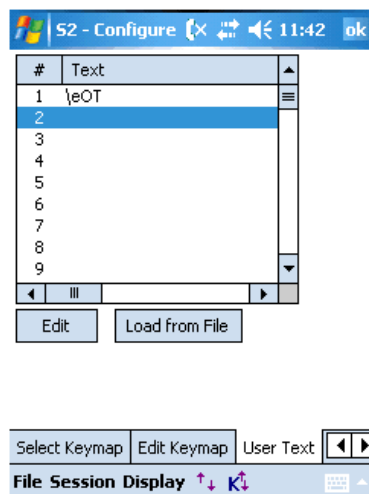
<code>\r</code>	- return
<code>\t</code>	- tab

```

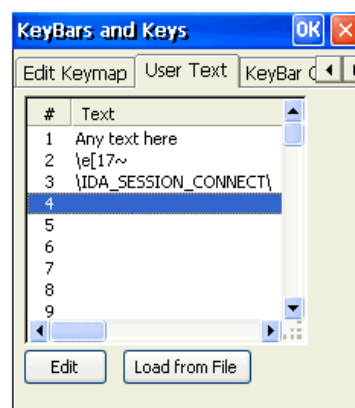
\e          - ESC for VT sequences
\x5a       - hexadecimal value
\IDA_action\ - invoke action

```

NOTE: The \IDA_action\ text is a standard invented and used by Naurtech. This allows users to invoke almost any application operation or event. Please refer to the Appendix to lookup a specific IDA_action code.



Windows Mobile



Windows CE

Edit: Highlight a user text entry in the list and tap this button to open the edit mode. Alternatively you may tap (not double-tap) the entry a second time to open the edit mode. Once opened, enter the user text desired. The images above show some samples.

Load from File: Tap this button to select a text file from which you can load user text entries. The text file can have up to 64 entries. Each entry, delimited by a CRLF, is imported into a separate user text slot.

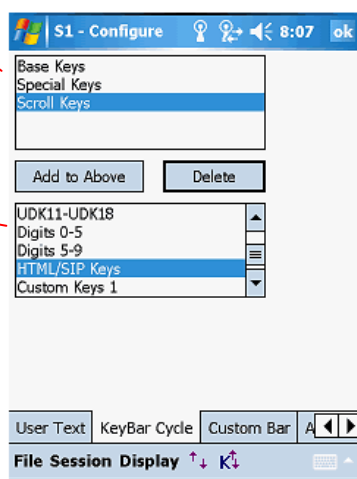
The file *replaces* the current text contents that may already be present in the table.

Keybar Cycle

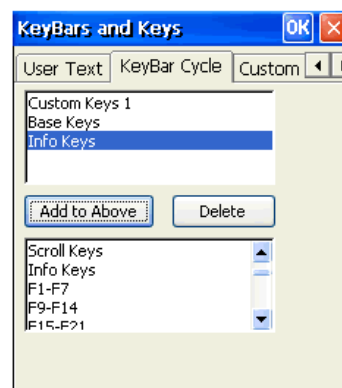
A KeyBar configuration consists of both the KeyBar Cycle and any Custom or template KeyBars. A KeyBar is a set of soft button keys visible at one time. The KeyBar Cycle is a collection of KeyBars that can be visible. The user "cycles" through the collection of KeyBars by tapping the arrow buttons on either end of the current KeyBar. Each key on the KeyBar is associated with a host or emulator operation. Users are allowed a maximum of eighteen KeyBars, six of which can be customized. The same KeyBar may be added multiple times to the KeyBar Cycle.

Order in which the KeyBars will "cycle". Can include pre-defined KeyBars and Custom KeyBars

This is the complete list of available KeyBars. You can select from these predefined KeyBars



Windows Mobile



Windows CE

Add to Above: Tapping this button will add the highlighted KeyBar from the bottom listbox to the top (selected) list of KeyBars. Users will be able to cycle through only the selected KeyBars in the application. A KeyBar which has already been added to the selected list cannot be added again.

Delete: This button removes the highlighted Keybar from the selected list of KeyBars (top listbox)

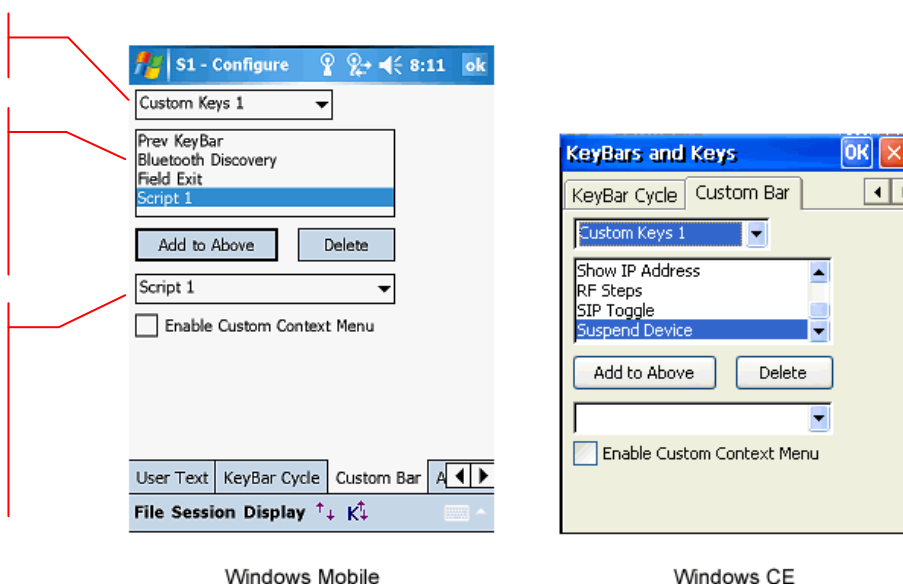
Custom Bar

If a Custom KeyBar ("Custom Keys 1" through "Custom Keys 6") is selected in the KeyBar Cycle, it can be configured by tapping the "Custom Bar" tab.

Select the Custom KeyBar that you want to configure

This is a list of keys that will appear on the Custom KeyBar Cycle. The order of keys in this list dictates the order of appearance on the Custom KeyBar

This is a list of all the available "action" keys and operations, which can be selected. A "Separator" places a vertical separation line. The "Empty" key leaves an empty space on the KeyBar.



Windows Mobile

Windows CE

Select Custom KeyBar: Select the "Custom Keys N" Custom KeyBar for which you would like to configure the keys. This is a dropdown list with all the available Custom KeyBars.

Add to Above: Tapping this button will add the highlighted key from the bottom listbox to the top (selected) list of KeyBar keys.

Delete: This button removes the highlighted Keybar key from the selected list of keys (top listbox)

Enable Custom Context Menu: The keys on "Custom Keys 6" KeyBar can also appear on the Context Menu. Enable this checkbox to enable the context menu, which may be invoked by tapping and holding the stylus anywhere in the terminal display area. Any operation configured in Custom Keys 6 will appear on this context menu. This option does not work for any other Custom Bars other than "Custom Keys 6".

You can add up to a total of 9 key buttons on each Custom Bar (Fewer on some devices). The entry for "Previous KeyBar" cannot be removed and must exist in each KeyBar to allow for "cycling" between KeyBars. Typically, the last key should be "Next KeyBar" for cycling to the next KeyBar.

One powerful feature of CTerm is the ability to associate KeyBar keys with User Text strings and Scripts. Key entries "Text 1" through "Text 20" or "Script 1" through "Script 20" may be associated with KeyBar keys as well. The "x" in Text x or Script x

corresponds to the respective User Text or Script slot. Thus if you have a text string configured in the User Text, this string can be submitted to the host application by tapping on the "Text X" key in a Custom KeyBar.

Tapping this key will send the complete text string to the current cursor location. For VT terminal sessions, escape sequences can be added to the User Text string. This allows users to configure custom escape sequences as required by their host applications. Escape sequences can be entered into the User Text in the following format:

```
\e = Escape
\n = Newline
\r = Enter or Return
\t = Tab
\xDD = Hexadecimal value
```

Scripts loaded in specific script slots (Script x) can be associated with a Custom KeyBar button.

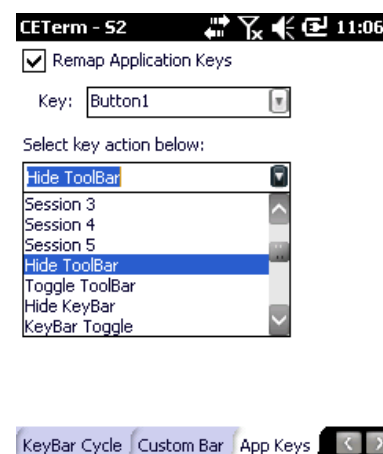
App Keys

Windows Mobile devices have hardware buttons that launch specific applications. These "Application Keys" are typically configured using an applet in the Control Panel. You can re-map these keys to invoke emulator or host operations. The App Keys dialog is used to configure the Application button remapping.

NOTE: This functionality is only associated with Windows Mobile platform devices.

NOTE: If "Record" is one of the default application key actions, you may need to change it in

[Start] [Settings] [Buttons] so that the application keys can be remapped



Remap Application Keys: Checking this box will allow remapping of the application keys

Key: This is a list of all the hardware application keys available on the mobile terminal. This list will vary depending on the device. Select the Application key that you would like to remap.

Select key action below: This is a list of actions and operations that you can associate with the Application Key selected above. After selecting the Key to remap, select the desired action. Only one action may be associated with a Key.

Configure Scripting

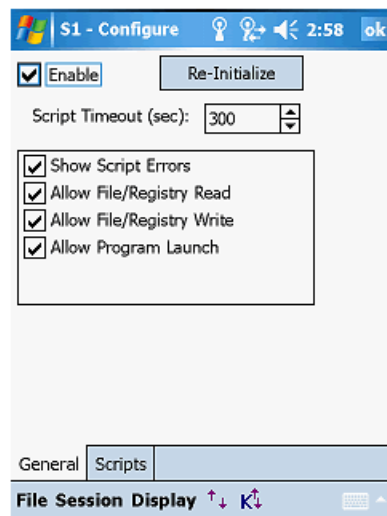
The “Configure Scripting...” button is used to create, import, edit, test and associate scripts. The Scripting capability in CETerm provides a platform to automate workflows with powerful JavaScript scripting and Workflow automation objects. It provides a "solutions platform" to automate and customize business tasks.

Scripts can be launched by pressing keys, or triggered by events such as specific host data detected on the screen or successful barcode scanner input etc. Scripts can be edited and tested directly on the mobile terminal. Scripts can also interact with the Web Browser and native JavaScript. A script can be as simple as an automated login or as complex as reformatting a TE session with a Web Browser interface.

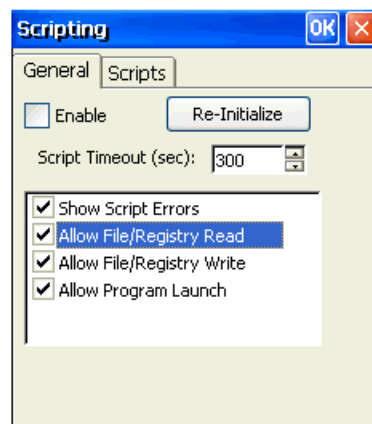
👉 With version 5.7, a lot of work has gone into making the scripting functionality even more powerful. Several new automation objects have been added. Interfaces of existing ones have been enhanced. A separate **CETerm Scripting Guide** available from our website discusses these in detail. Please refer to it.

General Settings

The General tab maintains settings for enabling, running, permissions and testing scripts. All settings on this tab apply to all scripts configured in the Scripts tab.



Windows Mobile



Windows CE

Enable: This is the main setting to enable or disable the scripting capability. This checkbox should be set for the Scripting engine to be loaded and initialized inside CETerm. The default value is unchecked.

Re-Initialize: This button can be used if you have made changes to the permissions or your scripts and you wish to re-load these changes. The re-initialization does not take place until the dialog is closed.

Script Timeout: This setting is provided to limit the duration of script execution. This limit is useful when developing new scripts and as a safeguard against a script with an “infinite loop”. A value of 0 will disable the timeout. During execution, a script can modify the timeout value and reset the timer to allow additional execution time. The default value is 300 seconds; about five minutes.

Show Script Errors: Enable this checkbox if you want CETerm to display errors if these are encountered in testing your scripts. Only syntax errors are detected.

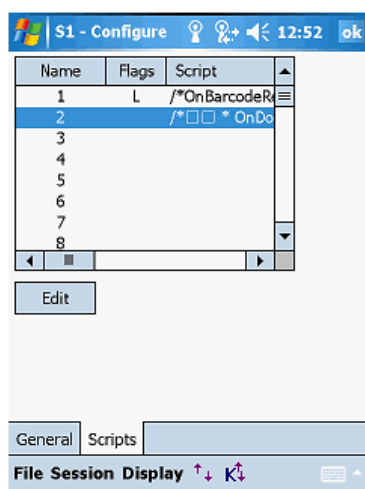
Allow File/Registry Read: Enable this checkbox if you want to allow scripts running in CETerm to have the ability to read data from the mobile terminal registry.

Allow File/Registry Write: Enable this checkbox if you want to allow scripts running in CETerm to have the ability to write and modify data in the mobile terminal registry.

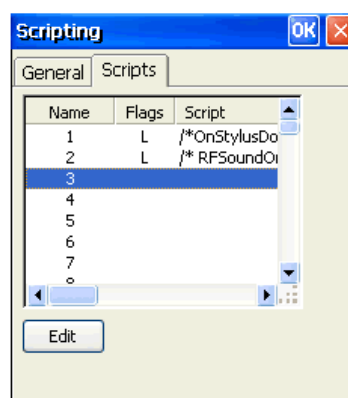
Allow Program Launch: Enable this checkbox if you want scripts running in CETerm to have the capability to launch external programs.

Editing Scripts

Scripts are edited on the **Scripts** tab. There are 64 script slots. The size of a script in each slot is limited to about 260,000 characters (about one-half megabyte under Windows CE). Scripts can also be loaded dynamically from files. A script slot will usually contain function definitions, which will be loaded into the engine, or executable statements such as function calls which may be bound to a key, toolbar, or menu.

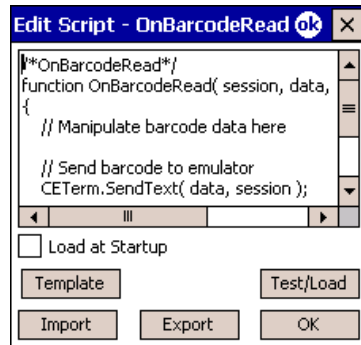


Windows Mobile



Windows CE

After selecting a script slot and tapping the **Edit** button, an Edit Script dialog will appear. The edit dialog allows **Import** and **Export** of scripts. For initial script development it may be easier to edit on your desktop PC, copy the script to the mobile terminal, and **Import** the script. Smaller changes are easily made on the device.



The checkbox **Load at Startup** should be checked for all scripts that contain function definitions that you want to have available in the script engine. The checkbox should **not** be checked for slots that contain scripts that are bound to keys or other activations. **Load at Startup** should be checked for all event handler definitions. All scripts with **Load at Startup** will be loaded into the script engine when it starts with CETerm startup, or when **Re-Initialize** has been pressed on the **General** tab.

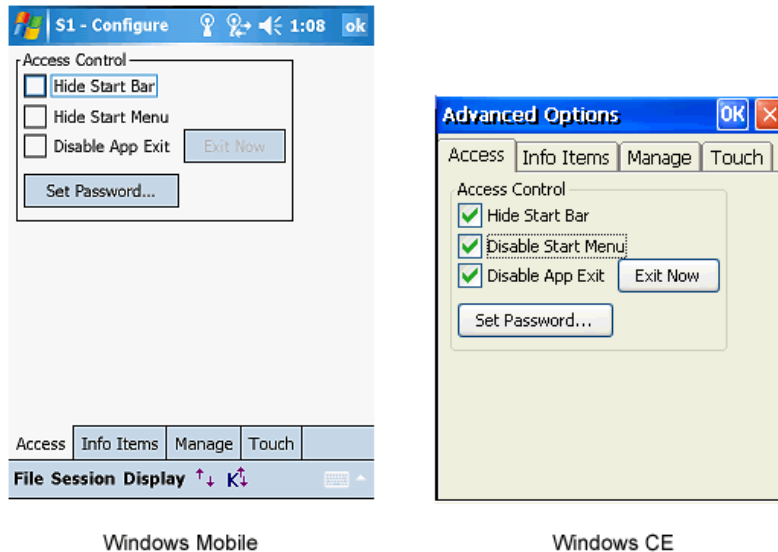
After importing or editing a script, you may want to tap the **Test/Load** button. If the script engine was previously enabled, the script will be executed. If the current script is a function definition, it will be checked for correct syntax and will be made available to the script engine. If the current script contains executable statements or is a function call, it will simulate activating the script. In general, you do not want to use **Test/Load** for executable statements.

Remember to tap **Test/Load** or **Re-Initialize** (with **Load at Startup** checked) after making changes to a script, if you want those changes loaded into the script engine. Also, **Test/Load** will not work if you have just checked **Enable** but not yet accepted the configuration changes.

The **Template** button displays a list of script templates which correspond to the scripting event handlers. Select a template and tap **OK** to have it replace the current contents of the script being edited. The template scripts show some of the ways to use CETerm Automation Objects.

Access

The following configuration tab is invoked from the Advanced button. It maintains all settings for configuration Access control and Operating System lockout.



Hide Start Bar: When checked, the Windows CE or Windows Mobile “Start” bar will be hidden. This option prevents users from launching other applications on the mobile terminal. For Windows Mobile platform devices, it also removes the smart minimize control (little “x” on the top right of the Start bar which may be used to “close” the application) and allows the terminal screen to occupy the full display area of the device. This also provides an additional row, which may be used by the terminal display.

Hide Start Menu / Disable Start Menu: When checked, the “Start” button will be hidden (for Windows Mobile devices) or disabled (for Windows CE devices). The Start bar however will still be present. This setting prevents users from launching other applications yet provides the visual status controls (volume, WLAN, battery, clock, etc) on the Start bar.

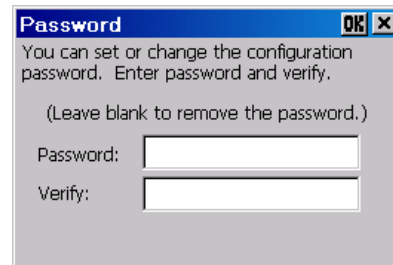
Disable App Exit: When checked, this option disables the application exit button. This prevents the users from exiting out of our application.

Exit Now: This button is enabled only when the “Disable App Exit” option is checked. It allows the administrator to save the configuration and exit when “Disable App Exit” is checked. Typical use would be for an administrator to set all configuration settings including a configuration access control password and exit the application using this button. Subsequently, users will not be able to exit the application and a password will be required to access the configuration options.

Set Password: This button prompts the user for a configuration password. When set, users are prompted for this password prior to viewing or modifying the session configuration. This capability prevents users from changing the configuration settings in controlled environments.



Windows Mobile

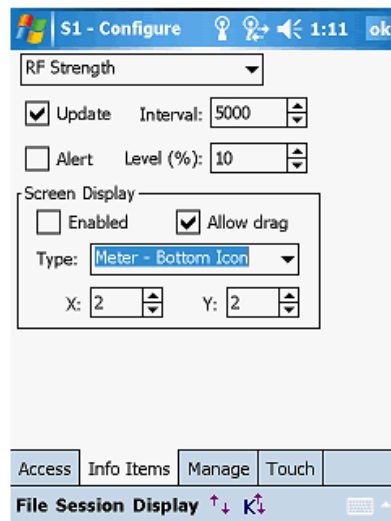


Windows CE

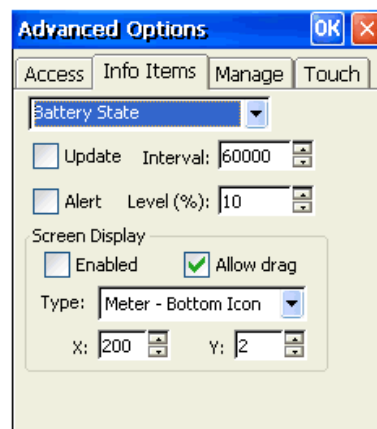
NOTE: To remove the password, clear the password fields and press OK..

Info Items

The Info Items tab holds attributes related to configuration and display of various Indicators. Indicators may be displayed in both terminal emulation or Web Browser sessions to give visual status for RF signal strength, battery level etc. Indicators may also be controlled and managed using scripts. These Indicators attributes should not be confused with the “Information buttons” in a Configurable KeyBar.



Windows Mobile



Windows CE



Indicator: This is the type of Indicator for which the various configuration settings will be applied. Selection includes:

- Battery State
- RF Strength
- Keyboard Mode (Available on specific mobile terminals only)
- Digital Clock
- Browser Loading
- Browser Progress

Update: Enabling this check box will force a repaint update of the Indicator status. This setting should be enabled if the Indicator is displayed on the screen.

Interval: This is the frequency of update in milli-seconds.

Alert: Enabling this check box will configure an alert notification message if the Indicator strength falls below a certain threshold level.

Level: This is the threshold level, in percentage, below which a notification prompt is generated if Alert notification is enabled.

Screen Display: This group box lists all attributes, which are related to the display of the configured Indicator on the screen.

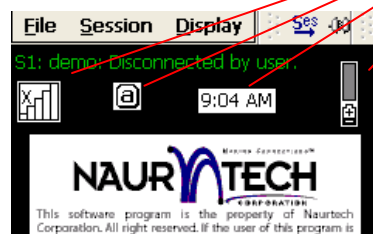
Enabled: This check box should be enabled to show the Indicator in this session.

Allow Drag: Enable this checkbox if you want the user to have the ability to tap-hold and drag the Indicator icon to different locations on the screen.

Type: Select the type of Indicator icon of your preference. These are designed for minimal use of screen real estate in the orientation, which best conforms to your host application.

X & Y: These are the top-left starting co-ordinates of the Indicator icon

You can tap the Indicator icon on for detailed status popup information. You can also control the configuration and display of the Indicators from HTML META tags for Web Browser sessions. Please refer to the Web Browser Programming Reference for details.

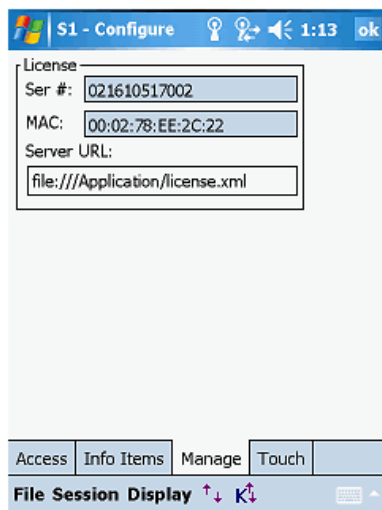


RF Signal; Keyboard Mode; Digital Clock and Battery Strength Indicators.

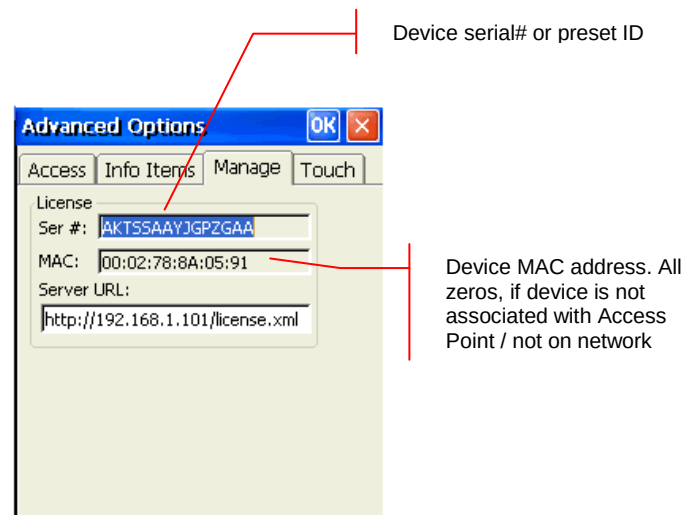
- Double tap to get detailed status in popup dialog.
- Tap, hold and drag to screen location
- Automatic update of strength icons
- Can also be displayed as a Keybar button
- Configure notification

Manage (Automated Licensing)

The Manage tab maintains all configuration attributes to manage the licensing, configuration and deployment of the application. It provides information related to license registration and maintains attributes for automated licensing.



Windows Mobile



Windows CE

Server URL: This is the URL to the XML based license registration file. It may be local to the mobile terminal or may reside on a web server. Exact format of the URL should be:

XML file on the device:

```
file:///license.xml
file:///Flash FX/license.xml
```

XML file on a Web server:

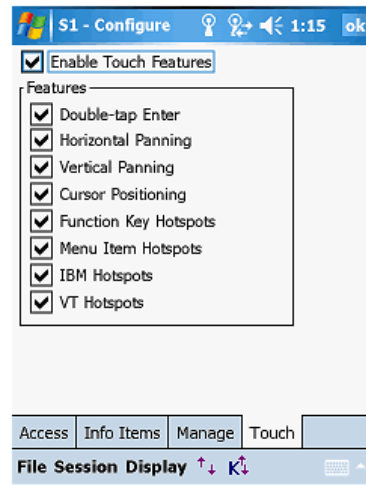
```
http://MyWebServerAlias/license.xml
http://x.y.z.w/license.xml
```

Please refer to the Automated Licensing section for more details.

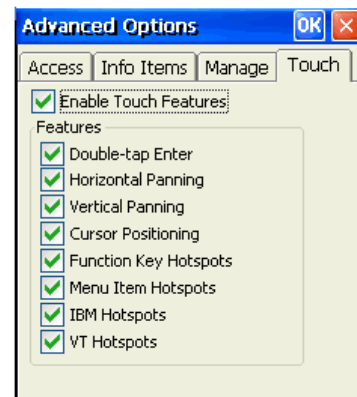
NOTE: If you have spaces in your URL path, you may need to escape these using %20 escape sequences. Note that the capability of the XML parser available on your terminal varies with the platform and version of the Windows CE OS running on it.

Touch

This tab provides attributes to control touch screen interactions.



Windows Mobile



Windows CE

Enable Touch Features: This is a global setting for all touch features. When checked, touch screen features are enabled. You must also individually enable the granular touch features for these to work. When un-checked, no touch features are enabled.

Double-tap Enter: When checked, a double-tap action with the stylus will simulate pressing the Enter key

Horizontal Panning: When checked, allows panning in the horizontal direction

Vertical Panning: When checked, allows panning in the vertical direction.

NOTE: Using the **screen panning** functionality, you can “tap-hold and drag” the terminal display screen with a stylus, to scroll to areas of the host screen which were not visible.

Cursor Positioning: When checked, a single stylus tap moves the cursor to the location of the tap (IBM emulation only).

Function Key Hotspots: When checked, enables Hotspot functionality for function keys. When enabled, you will be able to just tap on the function key text (such as **F7 = Prev** **F8 = Next** etc) on the terminal display to invoke the corresponding function key

NOTE: A Hotspot is a text on the terminal display where a user can tap with a stylus to execute a function. This allows a user to interact with a host application with minimal needs for special host keys.

A simple example might be the use of PF Keys. An operation associated with a PF key might be displayed on the terminal screen as "PF1 = Help". CETerm automatically detects this as a Hotspot and will send a PF1 key to the host when you tap on the "PF1" text on the terminal display. Refer to the Hotspots section for further details.

Menu Item Hotspots: Check this attribute to enable Hotspot functionality for menu items. When enabled, you will be able to just tap the menu item number on the terminal display to invoke the corresponding menu item operation. An example of this would be a menu such as:

```
1. Shipping
2. Receiving
3. Inventory
```

The user can just tap on "1." to invoke a "Shipping operation.

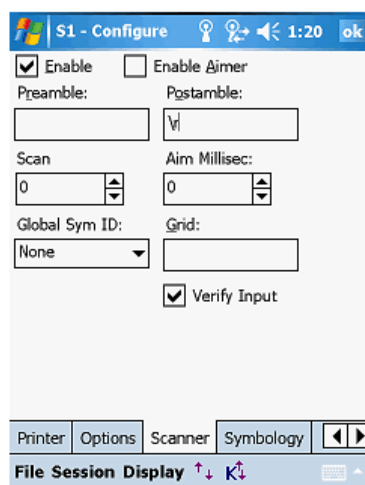
IBM Hotspots: 3270 and 5250 applications have several keywords, which are commonly used across many applications. Check this attribute to enable these commonly used keywords as Hotspots. Examples are "Enter", "More" and "Bottom". IBM Mouse and light pen activation must have IBM Hotspots enabled.

VT Hotspots: VT host applications have several keywords, which are commonly used across many applications.

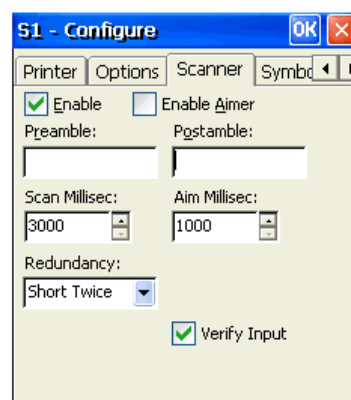
Scanner

Device tailored versions of our Emulators and Web Browser provide integrated support for barcode scanners. Scanner options may be configured and updated from the "Scanner" tab.

- From the application menu, Select [Session] [Configure] or tap the "Configure" button on the toolbar.
- A "Configure" dialog box will come up.
- Choose the "Scanner" tab



Windows Mobile



Windows CE

Enable: Checking this box will enable control of the barcode scanner. The scanner should be disabled if you must use a separate scanner wedge application. For all device tailored versions, we recommend that you let CETerm control the barcode scanner. Default is enabled.

Enable Aimer: Some mobile terminals support an "Aimer" option with their barcode scanner that appears as a laser pointer prior to scanning a barcode. Checking this box enables such an aimer pointer. This setting is only visible if the barcode scanner supports the functionality. Default is unchecked.

Preamble: This is a prefix ASCII string that will be pre-pended to any scanned data. Default is blank.

Postamble: This is a suffix ASCII string or control command that will be sent after completion of a successful scan. Default is blank.

Some of the more commonly used preamble and postamble codes are listed in the following table. You can join multiple codes with printable text in any combination.

String	Description
\t	Tab
\r	Return or Enter
\n	New line
\\	Backslash character
\xYY	where YY is a hexadecimal digit between 00 and FF to represent a character value
%A	ASCII label type (Symbol or HHP only)
%C	Custom label type, see config
%D	Date
%H	Device manufacturers labeltype as hex value
%I	AIM identifier letter of symbology, will be "*" if unsupported.
%M	AIM modifier digit of symbology, will be "*" if unsupported.
%L	Labeltype, custom (if defined) or same as %H
%T	Time stamp
%%	Percent sign character
\IDA_action\	where IDA_action is a Naurtech proprietary symbolic value that represents an action. Please refer to the IDA table in the appendix for a complete list. The table below lists some of the popular IDA actions.

IDA Code	Key / Action
IDA_ENTER	Enter key action
IDA_NEWLINE	Newline key action
IDA_ERASE_EOF	Erase to end of field key action
IDA_ERASE_INPUT	Erase input key action
IDA_FIELD_EXIT	Field exit key action
IDA_FIELD_PLUS	Field+ key action
IDA_HOME	Home key action
IDA_DOWN	Down arrow key action
IDA_UP	Up arrow key action
IDA_LEFT	Left arrow key action
IDA_RIGHT	Right arrow key action

Redundancy: This configuration describes the redundancy or linear security level used during decoding. Default is "Short Twice".

Scan Millisec: This attribute controls the scan duration. If a barcode is not read within this time, the scanner will shut off and a failure tone is sounded. The default value is 0 which is unlimited. Some scanners do not timeout regardless of this setting.

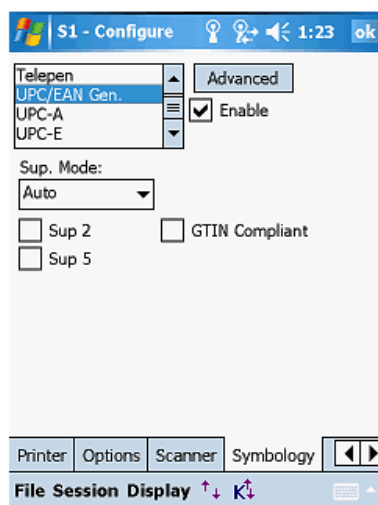
Aim Millisec: This attribute controls the duration of the aimer pattern prior to scanning of a barcode.

Verify Input: When using IBM 5250 emulation and if Verify Input is checked, the input field at the cursor location will be checked to determine if there is sufficient space for the scanned data. If there is no input field or there is insufficient space, a warning will be displayed and the data will be discarded.

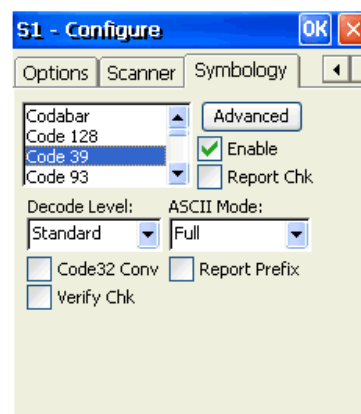
Symbology

Depending upon the mobile terminal and built-in scanner, our Emulators and Web Browser support about twenty different barcode symbologies. Individual symbologies may be enabled, disabled and configured.

- From the application menu, Select [**Session**] [**Configure**] or tap the "Configure" button on the toolbar.
- A "Configure" dialog box will come up.
- Choose the "Symbology" tab



Windows Mobile



Windows CE

The list box on the top left contains a list of barcode symbologies supported by the scanner. This list of symbologies varies with every mobile terminal. Configuration parameters associated with each symbology are displayed with the selection of a symbology. These configuration parameters vary depending upon the symbology selected.

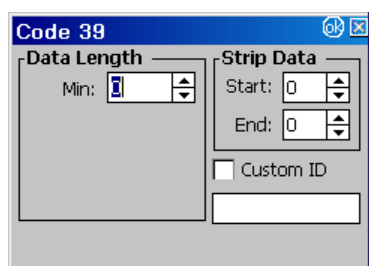
Enable: Check this box to enable the selected symbology for decode. If desired, you may enable a subset of symbologies from the complete list. On certain devices, barcode symbology initialization can take a couple of seconds. To minimize this initialization time on such devices, it is recommended that you can

enable only those symbologies that are being used for scanning and disable all other symbologies.

Report Check: Check this box to report (or return) the check digit as part of the barcode data.

NOTE: Each symbology has a separate set of configuration parameters associated with it. Selecting the symbology from the list will make these visible for configuration and update. Please refer to the individual barcode symbology references in the documentation for the handheld device.

Advanced: This button opens advanced configuration dialog for the selected barcode symbology. All settings configured and updated in this dialog are associated with the currently selected symbology.



Data Length Min: This is the minimum length, in characters, for the decoded barcode. Specifying a minimum length will require every scanned barcode to be at least the minimum length. Possible values depend on the symbology. Default is usually 0 which implies no minimum length.

Data Length Max: This is the maximum length, in characters, for the decoded barcode. Specifying a maximum length will require every scanned barcode to be at most the maximum length. Possible values depend on the symbology. Default is usually 0 which implies no maximum length.

Strip Data Start: This is the number of characters to be stripped from the beginning of the decoded barcode. Default is 0, which does not strip any characters.

Strip Data End: This is the number of characters to be stripped from the end of the decoded barcode. Default is 0, which does not strip any characters.

Custom ID: Checking this box will enable the Custom ID when used with the %L pre-ambble or post-ambble code. A %C in a pre-ambble or post-ambble will insert the custom ID regardless of the setting of this box. The custom ID text may be configured in the edit box.

NOTE: Custom ID field may be used when you have a requirement to add different pre-ambbles or post-ambbles for two or more barcode symbologies. For example you may need to add a prefix "UPC" to all UPC-A barcodes and a prefix "C128" to all Code 128 barcodes. In such a case, you can set a custom id of

“UPC” for UPC-A symbology and a custom id “C128” for Code 128 symbology. Placing a “%C” in either the pre-amble or post-amble would then add the corresponding string based upon the symbology of the barcode decoded.

Automated Licensing

The automated licensing capability simplifies setting of license registration keys. When the user attempts to connect a session, a license file can be queried to provide the license registration key. This license file can reside locally on the mobile terminal or on any web server. It is referenced using a URL configured under **[options] [Advanced] [Manage]** tab. CETerm will only query the license file if the running instance of CETerm is currently un-licensed and if a URL has been specified in the CETerm configuration.

The license URL is saved with all other CETerm configuration variables. If a master configuration is created from this device, then all cloned devices will request their key on their first connection attempt. The license URL may also be specified directly in a registry value that is preloaded into the device during a cold-boot restore or from a generic default configuration package.

In the simplest case, the URL refers to a license.xml file, which is a static XML page that can be returned by any web server. The XML is parsed to extract the key. Here is a sample of the XML document:

```
<?xml version='1.0'?>
<CETerm>
  <!-- Licenses for Motorola (Symbol) MC9090 terminals -->
  <license>
    <id>1E00040099409997</id>
    <user>End User Company</user>
    <key>42AA330245FE55D245C60460D22C05B0</key>
  </license>
  <license>
    <id>290006000B401680</id>
    <user> End User Company </user>
    <key>D4A1189D796B0CFD969361ED72B77AB5</key>
  </license>

  <!-- Licenses for Intermec CV60 terminals -->
  <license>
    <id>00:A0:F8:6D:81:5D</id>
    <user> End User Company </user>
    <key>9C5D0D771BA849386D33A989AFECECDB</key>
  </license>

  <!-- Licenses Honeywell Dolphin 9500 terminals -->
  <license>
    <id>000056627</id>
    <user> End User Company </user>
    <key>9C53837701784938222A989AF345CDB</key>
  </license>
</CETerm>
```

There may be any number of <license> elements in the file served to the mobile terminal. Note that there are no hyphen separators in the <key> element. The product element, <CETerm> in this case, must match the Naurtech product in use. The license URL may reference a file residing on a web server or on the mobile terminal. The following syntax may be used to specify the license file:

If license file is residing locally on the mobile terminal:

```
file:///license.xml
```

If license file is residing on a web server:

```
http://MyWebServerAlias/license.xml  
http://192.168.5.221/license.xml
```

Tips:

You can easily concatenate registration keys from multiple `license.xml` files into a single `license.xml` file. All that is required is an editor like Notepad. Make sure you copy all tags between <license> and </license> from the source license.xml file into the license.xml which holds all the concatenated keys. Please refer to the support wiki on our website for articles related to this issue.

Here are some common error codes:

0x80070490	License not found in XML document, check your XML. Validate that the license ID of your terminal is present in the license.xml file.
0x800c0006	XML document not found, check your URL path and location of license.xml file on the server or mobile terminal.
0x80040154	XML or SAX Parser not found on device. Unsupported or missing Microsoft components.
0x80004005	General failure. Catch all error code.

The following steps should be followed to install the new “automated licensing” capability:

1. Install the new version of CETerm on your terminal. This should be version 5.0 or higher. Run it

2. On the mobile terminal, go to the Manage tab
[Session] -> [Configure] -> [Options] -> [Advanced] -> [Manage]

Enter the URL to web server where CETerm should look for the license.xml file

The license.xml file should have a license ID and corresponding registration key for *this* device. Tap OK, all the way out.

3. Configure and Connect to your host. If there are no errors, license registration is transparent. You can validate registration by looking at the About box

File -> About

You should see your registered company userid.

If you prefer to configure the server URL directly using a device / application management tool, you can directly write the following key into the device registry.

```
[HKEY_LOCAL_MACHINE]
[Software]
[Naurtech]
[CETerm]
    ConfigServerURL = SZ:http://192.168.1.101/license.xml
```

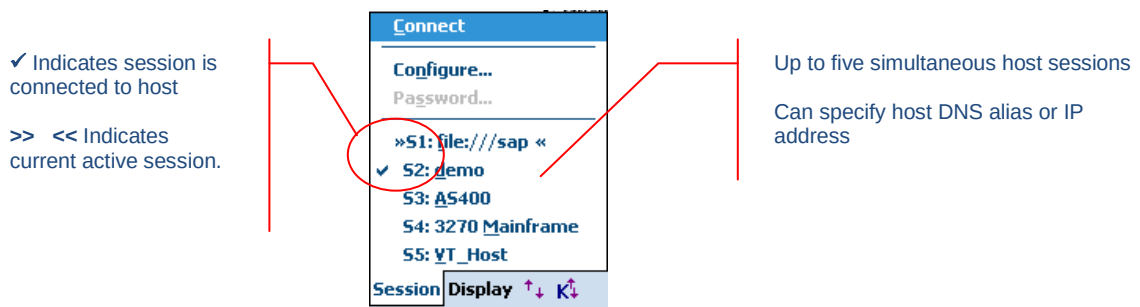
NOTE>> The product name "CETerm" in the registry key example above will change to respective product names for CE3270, CE5250 and CEVT220.

Session Interaction

CETerm allows up to five simultaneous host sessions. Any one or all of these sessions may be simultaneously connected to a host, but only one session is in the foreground at any time. This is the active session and it receives all user interaction. Connected sessions in the background maintain their host session connections and update their (hidden) screen content.

Multiple sessions

You can run up to five independent sessions simultaneously. You can navigate between these sessions either from the application menu or by using the "Next live session" hotkey. The current active session is indicated in the application **[Session]** menu as shown below. Host addresses configured for each of the host sessions are indicated as part of the session names.



Tip: To jump to the next connected host session; use the hotkey **[Ctrl] [Shift] [J]**

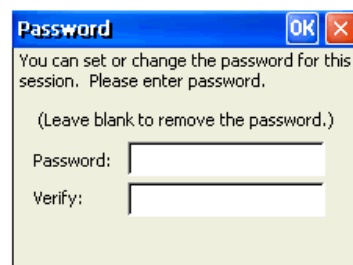
Password protection

All sessions may be password protected for security. You can set a password for a host session by first configuring the session and connecting to the host.

- Once connected, from the application menu select **[Session] [Password]**. This will prompt with a password dialog.
- Enter the password.
- Next time you attempt to connect this session, you will be prompted to enter the session password. If the password is incorrect, session will not connect.



Windows Mobile



Windows CE

Note: If you forget your session password and can no longer access your session, please contact us at support@naurtech.com

Connecting / Disconnecting from Host

To connect to a host, configure the session parameters and select "Connect" from the application menu. Only disconnected sessions may be connected. Once connected, you may disconnect the host session by selecting "Disconnect" from the application menu. You must configure the host session prior to attempting a connection. You cannot change the host address once the session is connected. These are grayed out for connected sessions.

- From the application menu select **[Session] [Connect]** to connect or **[Session] [Disconnect]** to disconnect. You may also tap the "Connect / Disconnect" button  on the toolbar.

Auto-Launch when device boots

You can configure our application to automatically launch when the mobile terminal boots. This can simply be done by placing a shortcut in the `\Windows\StartUp` folder on the device.

- Make sure CETerm is installed correctly and you can see an icon on the Start Menu
- On the mobile terminal, run Windows file explorer **[Start] [Programs] [Windows Explorer]**
- Navigate to the `\Windows\Desktop` folder
- Highlight the shortcut “Naurtech CExxxx”, where xxxx is the product specified
- Select **[Edit] [Copy]** from the Windows Explorer menu
- Navigate back to the `\Windows\StartUp` folder
- From the Windows Explorer menu, select **[Edit] [Paste]**

NOTE: You can also follow these steps from the mobile device explorer running on your desktop, if your device is connected via active sync to it.

Auto-Start a host Session

You can configure sessions to automatically connect to the host when the emulator starts. You can enable this from the advanced connection configuration setting.

- From the application menu, select **[Session] [Configure]**
- In the "Connection" tab, select the **Advanced** button. This will open the advanced connection settings dialog
- Select the "General" tab
- Enable the "Auto Connect" checkbox
- Hit OK all the way out of the dialogs

Network Check on Connect

When CETerm is configured to automatically launch during a device boot and then connect to your host application, the underlying network may not have completed initialization before our application attempts to use the network. You can enable the setting **[Session] [Configure] [Advanced] [Check Network on connect]** to cause CETerm to detect the network availability prior to attempting a host connection.

As an alternative, you can also introduce a delay during the startup process. *This is the older approach to resolving the issue and is no longer recommended.*

A delay causes our application to wait until the underlying wireless TCP/IP network is available. The delay will allow time for the mobile terminal to make an RF association with the access points and perform the needed network initialization. The length of this initial delay will vary from one network to another. It is recommended that you change the “Initial Sleep” delay settings to match your network requirements.

- From the application menu, select **[Session] [Configure]**

- In the "Connection" tab, select the **Advanced** button. This will open the advanced connection settings dialog.
- Enter a value in the "Initial Sleep" edit box. The default is 0 meaning no delay. This value is in seconds.

Wherever possible, you may consider using the "Check Network on Connect" attribute to achieve a more optimal equivalent result.

Run a Script

Please refer to the Naurtech CETerm Scripting Guide for detailed description.

Use barcodes to invoke Operations or Keystrokes

For all our Emulators and Web Browser, you can scan a barcode with special content to simulate Keystrokes. In fact, any application operation can be invoked via ID action (IDA) codes with this approach. The barcode can be any symbology, but "Extended Code 39" is a good choice. Extended Code 39 is also called the "Full ASCII" mode of Code 39. By using two-character sequences, it can represent the needed backslash and underscore characters.

With Extended Code 39 symbology, the scanner is often configured to require a '*' as a start and stop character. Make sure your generated barcodes are compliant with your scanner configuration whether you use Code 39 or some other symbology.

The content of the barcode is in the form: ***\IDA_name*** where **name** is the "Symbolic Name" of the IDA action. These values are unique to our application.

There is a "Free 3 of 9 Extended" font available for Microsoft Windows operating systems, which may be used to represent text into Extended Code 39 barcode. You can download this from the Naurtech support knowledgebase.

Note that if an IDA action is decoded at the start of a barcode, all additional characters are ignored. Also, there is no "stripping" of characters and no pre- or post-amble are sent. Any barcode length restrictions may still be imposed by the symbology configuration. Here are some samples containing special host key and application operation barcodes

Action	Barcode Content	Extended Code 39 barcode
F2	*\IDA_PF2*	
Tab	*\IDA_TAB*	
Session Connect	*\IDA_SESSION_CONNECT*	
Field Exit	*\IDA_FIELD_EXIT*	

Please contact technical support for more information on available ID action (IDA) codes.

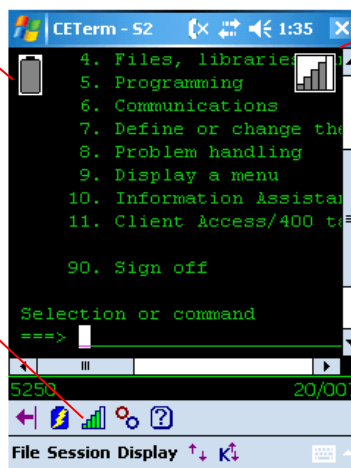
Display Indicators (Digital Clock, RF & Battery Strength ...)

You can display visual Indicators, such as a digital clock and / or RF and Battery strength in your TE or Web Browser sessions. For optimal usage of the precious screen real estate, you can select an Indicator icon of your preference. You may drag the Indicator or lock it at a specific location. Double tapping on the indicator will display a popup dialog with details information. You can also configure a low threshold percentage. If the Indicator strength falls below this threshold, you will receive a notification. To configure:

- From the application menu, select **[Session] [Configure] [Options]** tab
- Select the **Advanced** button and then the **[Info Items]** tab.
- To enable an Indicator, select it from the list and enable the “Update” and “Enabled” checkboxes.

Battery Strength Indicator.

Indicators displayed on a Custom KeyBar



RF Strength Indicator.

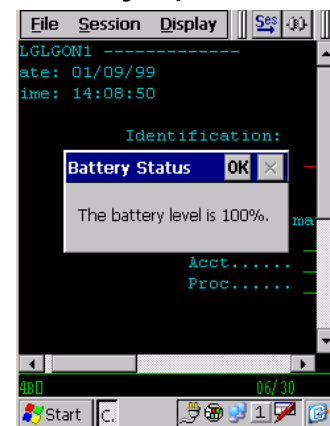
- Double tap to get detailed status in popup dialog.
- Tap, hold and drag to screen location
- Configure notification message if strength falls below a specific threshold

You can also include the RF and Battery strength Indicators on the Configurable KeyBar so these appear as status buttons.

Display device parameters (Serial #, MAC address, Battery...)

You can remap a hardware key to display device specific information such as serial number, MAC address, IP address and Battery level. This is done via popup messages. The steps for this configuration are equivalent to key remapping. The only difference is in the selection of the “Action”.

1. Navigate to **[Session] -> [Configure] -> [Options] -> [Config Keybar and Keys] -> [Edit Keymap]**
2. Select the **Common** Keymap from the Keymap dropdown list
3. Hit **[New]** to add a new key remapping



4. Select the key in the **Virtual Key** dropdown that you would like to associate with the device setting.
5. In the **Action** list box, select device setting for which you want to associate a popup message. The following table show the possible action selections

Action	IDA code
Show IP Address	IDA_POPUP_IPADDRESS
Show MAC address	IDA_POPUP_MACADDRESS
Show Battery	IDA_POPUP_BATTERY
Show Time	IDA_POPUP_TIME
Show Serial #	IDA_POPUP_SERIALNUMBER

6. You may want to add the same remapping to the base (unconnected) keymap as well

NOTE: The device specific information, which may be queried, is dependent upon the device. All information may not be available on all devices

Play a different audio tone / sound on my device

Audio tones can be played in either TE or Browser sessions using a Script. A trigger event can be configured to invoke a script. The script handler can be implemented to sound a beep or play a wave file. This mechanism can be used in either web browser or TE sessions. This functionality is discussed in the Scripting Guide.

For TE sessions, CETerm also includes built in support for Extended Commands used in many legacy host applications. Users can use the "Tone" extended command to cause the system to play a specified tone. This is supported through the "extended commands". The syntax is:

```
#T<volume><frequency><length>
```

```
<volume>      is specified in columns 4-6. Range is between 000 and 255
<frequency>   is specified in columns 7-9. Range is between 000 and 030
<length>      is specified in columns 10-12. Range is between 001 and 010
```

You can also play any "system sound" or a .wav file on CE devices that support .wav files. To play any .wav file on the mobile terminal the syntax is the same except that the "Volume", "Frequency", and "Length" parameters are used directly to construct a filename. You may use any 9 characters for the sound name / filename. Do not put in the (.wav) extension, it is assumed. More than 9 characters are ignored. If you have a shorter filename, insert leading spaces so that the filename ends at the 9th character.

If the requested sound does not exist on the device, a default sound will play. For development purposes you may want to use a standard system sound and then find or create your custom "alert sound" later. You can look for .wav files in the \Windows directory for standard sounds.

If only one unique sound is needed, it will be easier to configure that sound in the "Beep Sound" under **[Session]->[Configure]->[Display]**. The normal VT Bell character will activate this sound

Key Remapping and Configuration

CETerm provides functionality for remapping keys for both TE and Browser sessions. Users can choose one or more of the following mechanisms for key remapping and input.

- Remap physical hardware keys on the mobile terminal. Details for this functionality are discussed in the “Keyboard Key Remapping” section below.
- Remap hardware keys or KeyBar buttons and associate these with a Script. Details for this functionality are discussed in the “Naurtech CETerm Scripting Guide”. You can download this from our website.
- Configure Windows CE application keys. Details for this functionality are discussed in the “Keyboard Key Remapping” section below.
- Configure “Meta Keys” which may be used in conjunction with other keys to create unique key combinations to remap application operations or host key actions.
- Configure one or more soft KeyBars. Users may select from predefined templates or customize their own KeyBars. Details for this functionality are discussed in the “Configurable KeyBar” section below
- Configure a Context Menu KeyBars. Details for this functionality are discussed in the “Context Menu” section below.

Keyboard Key Remapping

CETerm can be configured to map any physical keyboard key (except state keys like “Ctrl”, “Alt” etc) on the device to any host action, application operation, user text, IDA code, macro or Script.

Users can directly configure the key remap bindings using on-device dialogs. The typical approach should be to use "emulation specific" maps, which apply to all sessions using the same emulation type, such as VT220. In special cases, it may be necessary to define a map, which applies only to one session. In this case you should define and use the "session specific" map.

Session specific maps are more work to configure because they must be defined individually for each session.

To simplify configuration of keys that are common to all sessions and emulations, there is a "Common" map, which can be "added" to the "Emulation" or "Session" maps by checking the "Include Common Map" box. The Common map can be edited.

Lastly, there is the situation when a session is not connected to the host. In this disconnected state, all sessions share a common key mapping which is independent of the session emulation type. This mapping is called the "Unconnected" or "Base" map. The Base map can be edited or an external Base can be selected.

Please refer to the configuration section of this manual for details on creating customized key remap bindings.

Remap a hardware key

You can configure CETerm to re-map any physical keyboard key on the mobile terminal to any of the following:

- Another key
- An application operation such as "Jump to Next Session" or "Print"
- A host specific key such as "F4" or "Field Exit"
- An escape sequence such as "Esc[15~"
- A text string such as "My input string"
- A NULL or no operation which will prevent use of that key
- A Script

This remapping may be configured specific to either a session or an emulation type (such as VT, 5250, 3270 etc). Follow these steps to remap a hardware key:

1. From the application menu, select **[Session] [Configure]**
2. Go to the "Options" tab and click the "Configure Keybars and Keys..." button
3. Go to the "Select Keymap" tab. Select the custom keymap to be specific to this particular session or an emulation type (3270, 5250 or VT). Generally it is recommended that you use an "Emulation" keymap type. The "Unconnected Keymap" is used when the session is not connected to the host.
4. Go to the "Edit Keymap" tab. Say you want to customize the following key remap:

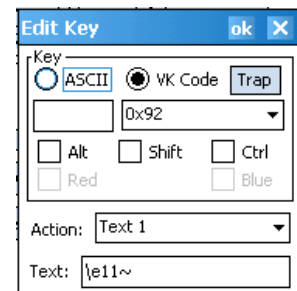
Key Sequence	New key remapping
F1	"W" key
Ctrl + 1	"Next live session"
F5	"Esc[13~" escape sequence
F8	"Erase Input"
F9	"my custom input" text string
Up Arrow	Disable this key

5. From the "Keymap" dropdown list, select the type of keymap you want to customize. For an emulation keymap, (selected in 3 above) select the "VT Keymap" for all VT sessions or "5250 Keymap" for all 5250 sessions, "3270 Keymap" for all 3270 sessions. There might be some predefined entries, which will appear in the keymap table for each keymap selection. For details on the keymap table columns, please refer to the Options section under Configuration.

6. Select the "New..." button. You will be prompted with a New key dialog. This is identical to the "Edit" key dialog

6.1 Select the key type to be "Virtual Key".

6.2 From the dropdown list, select the key you want to remap. In our remap example, you want to remap the F1 key so that when it is pressed a "W" is generated instead. (F1 → "W"). Select the key to be "F1".



NOTE: If you do not know the VK of the physical key (or key combination) that you want to remap, simply tap the "Trap" button. This forces CETerm to monitor the VK code of the next key / key combination which you press and display the captured VK code in the edit box. If a well defined VK code is not recognized, CETerm places the actual hexadecimal value.

6.3 Check any modifier state key checkboxes. In our custom remap example, none of these will be checked for the F1 → "W" key remapping. The "Ctrl" checkbox will be checked for the remap Ctrl + 1 → "Next live session"

6.4 In the "Action" dropdown, Select the new action that the key is being remapped to. In our remap example (F1 → "W"), this should be a "W"

6.5 Click OK. This remap will be displayed in the table.

6.6 To remap a key to an Escape sequence or text string, select the Action "Text n" (where n is the number between 1 and 65). This will result in an edit box appearing, where you can specify the custom text string. Text strings may contain special escape sequences for VT or sequences of actions:

Text String	Description
\r	Return
\t	Tab
\e	ESC for VT sequences
\x5a	Hexadecimal value
\IDA_action\	Invoke ID action

The \IDA_action\ text is proprietary to CETerm. This allows users to invoke almost any application operation or event programmatically. Please contact us if you have a specific need and are looking for a particular IDA_action reference

6.7 To remap a key to a CETerm script, select action "Script n" where "n" is the script slot number in which the script or call to a script function is implemented.

Follow steps 6.1 through 6.5 to remap other keys. To disable a key, you can map it to a "Null" Action.

7. Click OK. Connect to the host application and invoke the remapped keys to test the remap.

Meta Keys

Meta keys are special keys that set and clear a Meta state. They act much like the state keys "Shift", "Alt" and "Ctrl" on a regular keyboard. Similar to these normal state keys, Meta keys are used together with other keys to activate special actions. Meta keys are named with colors. Typically these can include: Red, Green, Blue, and Yellow. For device tailored versions of CETerm, whenever possible, Meta key colors are synonymous with physical keys on these devices.

Meta keys can be assigned to hardware keys in much the same way that other key mapping is configured in CETerm. After Meta keys are assigned to hardware keys, they can be used in other key re-mapping assignments. For example, after the Blue Meta key is assigned, you may create the mapping where Blue + '1' switches to Session 1, etc.

Defining Meta Keys

Meta keys are defined in the Edit Keymap tab of the key remapping. Simply select the "Meta" keymap. There is one basic restriction for the Meta keymap. There may only be one key for each Meta state. Typically this means a key for each of Red, Green, and Blue.

When defining (or editing) a Meta key, there are three special attributes:

"!ASC" - This checkbox means "Ignore Alt, Shift and Control". When checked, the Meta key will be effective regardless of the Alt, Shift, or Control states. Usually this option is checked to allow the most flexible key combinations.

"Toggle" - This checkbox means to "toggle the state" of a Meta key each time the key is pressed. Otherwise, the state is set when pressed and cleared when the key is released. Usually, this option is checked. Some keyboards require the "key up" action of a key before another key can be pressed. For these keyboards, the "toggle" option *must* be checked, otherwise no other key can ever "see" the Meta state.

"One-shot" - This checkbox means that the Meta state is reset after the next key is pressed, whether or not the next key was part of a Meta key translation. If this option is unchecked, the Meta state remains set until the meta key is pressed again. Usually, this option is checked.

Using Meta Keys for Remapping

When Meta keys are available for key remapping, you will see corresponding checkboxes on the "New Key" / "Edit Key" dialogs. Meta state flags may also appear in the "Flags" column of the keymap. The flags meanings are:

- V - Virtual Key remap
- A - Alt state
- C - Ctrl state
- S - Shift state
- R - Red meta state
- G - Green meta state
- B - Blue meta state
- Y - Yellow meta state

To require a Meta state for a key, simply check the corresponding checkbox.

NOTE: You should define the corresponding Meta key in the Meta keymap before creating key remap bindings that use the Meta key.

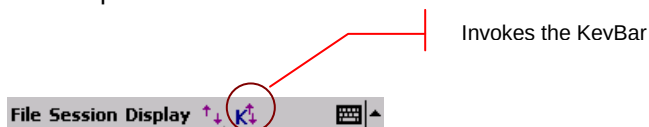
Configurable KeyBar

Most Windows Mobile and Windows CE devices have a limited keypad. They often rely upon the Soft Input Panel (SIP) to "spell type" data. However, the SIP usage can be cumbersome and it does not provide any special host keys such as those needed in a terminal emulation program or special keys to simplify web page navigation in a Browser.

The configurable KeyBar functionality allows users to customize a set of soft keys to invoke any host specific keys or application operations. Users can select from a set of pre-defined KeyBar templates. In addition, they can also configure up to six Custom KeyBars of their own. Users can navigate or "cycle" within a selected subset of KeyBars.

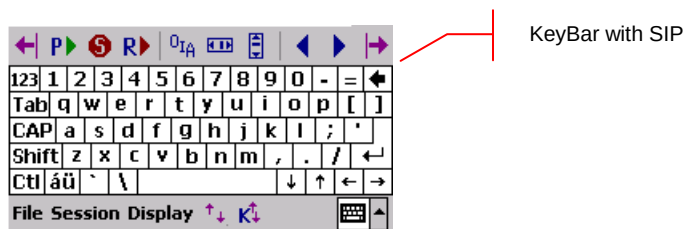
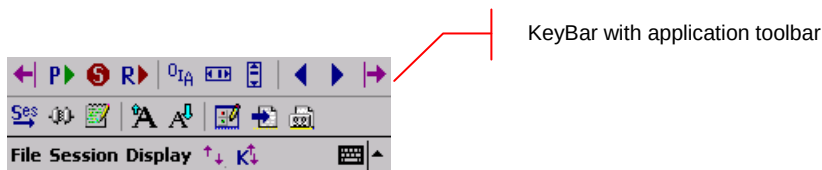
For Windows CE devices, the KeyBar appears next to the application Menu and Toolbar. These can be dragged and placed in separate rows, if so desired.

For Windows Mobile devices, the KeyBar appears as a toolbar. You can toggle it on or off by pressing the KeyBar icon next to the application menu. The session screen automatically adjusts to provide the maximum possible screen real estate.

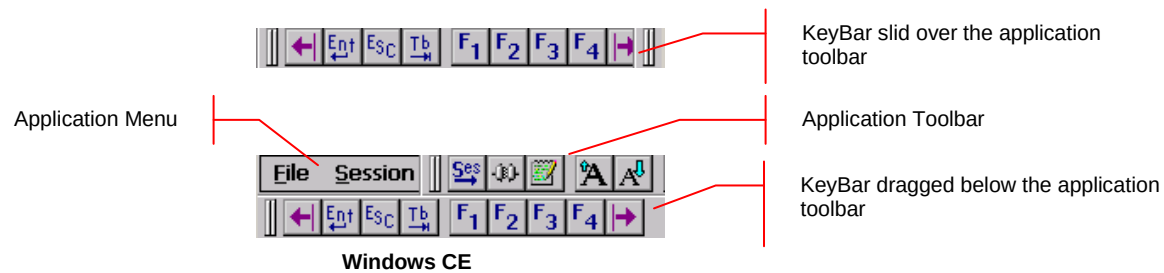


To configure the KeyBar, please refer to the Options section under Configuration. Take some time to customize the KeyBar and become familiar with its use. It will be time well spent.

When enabled, the KeyBar appears on "top" of either the application menu, application toolbar or SIP, depending upon their visibility state. Tap the arrow button on either end to cycle backward or forward through the configured KeyBars.



Windows Mobile



There are several pre-defined KeyBars that are provided with the application. These serve as emulation specific or operation specific templates. You may use these in addition to the customized KeyBars. The following table shows these pre-defined KeyBar templates.

KeyBar Name	KeyBar Buttons	KeyBar Name	KeyBar Buttons
Base Keys		IBM 2	
Special Keys		IBM 3	
Info Keys		VT 1	
Scroll Keys		VT 2	
F1 - F8		VT 3	
F9 - F16		UDK11 - UDK18	
F17 - F24		Digits 0 - 5	
IBM 1		Digits 5 - 9	
HTML / SIP keys			

KeyBar Button Images

The following table shows bitmaps and associated action text for some of the more popular actions and operations that can be associated with the configurable keys.

Bmp	Action Description
	Previous KeyBar
	Next KeyBar
	(Empty) no action
	? character
	Enter key
	Escape key
	Tab key
	Field Backspace (Back Tab key)
	Insert Toggle
	Delete key
	Backspace key
	Left arrow key
	Right arrow key
	Up arrow key
	Down arrow key
	OIA Toggle
	Jump to Session 1 (S1)
	Jump to Session 2 (S2)
	Jump to Session 3 (S3)
	Jump to Session 4 (S4)
	Jump to Next Session (active)
	Macro Play
	Macro Stop
	Macro Record
	Program Exit (emulator)
	Print Screen
	F1 function key
	F2 function key
	F3 function key
	F4 function key
	F5 function key
	F6 function key
	F7 function key
	F8 function key
	F9 function key
	F10 function key
	F11 function key
	F12 function key
	F13 function key

	F14 function key
	F15 function key
	F16 function key
	F17 function key
	F18 function key
	F19 function key
	F20 function key
	F21 function key
	F22 function key
	F23 function key
	F24 function key
	PA1 key
	PA2 key
	PA3 key
	Erase EOF
	Erase Input
	Attn
	Reset
	Clear
	DUP
	Newline
	IBM Home
	System Request
	Field Mark
	Field Exit
	Field +
	Field -
	Roll Up
	Roll Down
	IBM Help
	IBM Print
	Find
	Insert Here
	Remove
	Select
	Previous
	Next
	Hold
	Cancel

	Answerback
	DEL (VT)
	Linefeed
	VT PF1
	VT PF2
	VT PF3
	VT PF4
	Numpad 0
	Numpad 1
	Numpad 2
	Numpad 3
	Numpad 4
	Numpad 5
	Numpad 6
	Numpad 7
	Numpad 8
	Numpad 9
	Numpad Enter
	Numpad Minus
	Numpad Comma
	Numpad Period
	VT CSI M (custom)
	VT CSI N (custom)
	VT CSI O (custom)
	VT CSI P (custom)
	VT CSI Q (custom)
	VT CSI R (custom)
	VT CSI S (custom)
	VT CSI T (custom)
	VT SAP0135 (custom)
	ASCII 0
	ASCII 1
	ASCII 2
	ASCII 3
	ASCII 4
	ASCII 5
	ASCII 6
	ASCII 7
	ASCII 8
	ASCII 9
	ASCII +
	ASCII -
	UDK F6
	UDK F7
	UDK F8

	UDK F9
	UDK F10
	UDK F11
	UDK F12
	UDK F13
	UDK F14
	UDK F15
	UDK F16
	UDK F17
	UDK F18
	UDK F19
	UDK F20
	Text 1 (User Text)
	Text 2 (User Text)
	Text 3 (User Text)
	Text 4 (User Text)
	Text 5 (User Text)
	Text 6 (User Text)
	Text 7 (User Text)
	(Text 8 (User Text)
	Text 9 (User Text)
	Text 10 (User Text)
	Text 11 (User Text)
	Text 12 (User Text)
	Text 13 (User Text)
	Text 14 (User Text)
	Text 15 (User Text)
	Text 16 (User Text)
	Text 17 (User Text)
	Text 18 (User Text)
	Text 19 (User Text)
	Text 20 (User Text)
	VScroll Toggle
	HScroll Toggle
	HScroll Left (Page)
	HScroll Right (Page)
	VScroll Top (Page)
	VScroll Down (Page)
	Scroll Upper Left quadrant
	Scroll Upper Right quadrant
	Scroll Lower Left quadrant
	Scroll Lower Right quadrant
	Scroll Center quadrant
	Scroll Cursor Center
	Scroll Cursor Visible
	HScroll Left (End)

	HScroll Right (End)
	VScroll Top (End)
	VScroll Down (End)
	Home page (HTML)
	Go Back (HTML)
	Go Forward (HTML)
	Page refresh (HTML)
	SIP Up (HTML)
	SIP Down (HTML)
	Red / Blue Meta key press state info
	Yellow / Green Meta key press state info
	Device Serial Number
	Device MAC address

	Device IP address
	Battery charge level
	Time
	Enables barcode scan trigger
	Scanner enabled status
	Battery strength meter
	RF Strength meter (tower)
	RF Strength meter (steps)
	Run Script 1
	Run Script 2
	Run Script 3 (and so on until Run Script 20)

Create a Custom KeyBar

- In the KeyBar Cycle tab, add a Custom Bar to the KeyBar Cycle
- In the Custom Bar tab, select the Custom Bar that you want to configure
- Select the Key or operation that you want to appear on this custom bar
- Tap "Add to Above". The selected key / operation will appear in the list.
- Delete unwanted keys by selecting them and tapping "Delete".

You can add up to a total of 9 key buttons on each Custom Bar (Fewer on some devices). The entry for "Previous KeyBar" cannot be removed and must exist in each KeyBar to allow for "cycling" between KeyBars. Typically, the last key should be "Next KeyBar" for cycling to the next KeyBar.

With this version you can also add informational / status buttons for Meta key states, RF and Battery strength, scanner status etc. These status buttons can be interspersed with normal Keybar action buttons and are configured the exact same way.

One powerful capability of the KeyBar is the ability to associate keys to a User Text. Key entries "Text 1" through "Text 20" are tied to the corresponding twenty entries in the User Text configuration. Any text string configured in User Text slot can be submitted to the host application by tapping on the "Text X" Keybar button in a Custom KeyBar. Tapping this key will send the complete text string to the current cursor location. For VT terminal sessions, escape sequences can be added to the User Text.

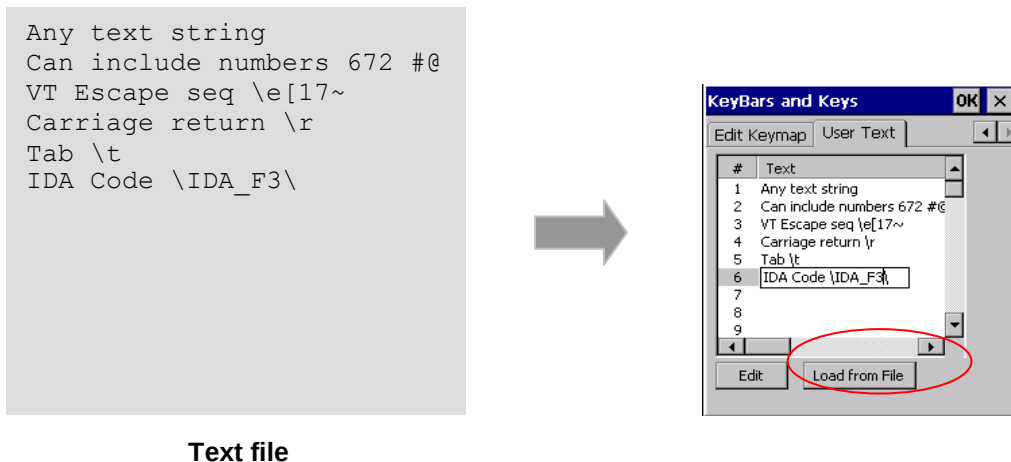
Escape sequences can be entered into the User Text in the following format:

```
\e = Escape
\n = Newline
\r = Enter or Return
\t = Tab
\xDD = Hexadecimal value
```

Customize User Text

User Text is any arbitrary text that may be configured so that this does not have to be spell typed using either the hardware keys or the soft input panel on the mobile terminal. You can associate the user text strings with either button keys on the Configurable Keybar or hardware keys. User text strings can be any escaped text string, escape sequence or Naurtech ID action (IDA) codes. Please refer to the “User Text” section under Options configuration.

Text strings do not have to be created on the mobile terminal. You can create an ASCII text file (sing any editor such as Notepad), copy this file to the mobile terminal and “load” your text strings from this file. Each text entry should be on a separate line. An example is shown below.



Text file

The user text entries are automatically assigned a numeric order value. This is for representation only. This order numbering value is not part of the user text. Once configured the user text entries are referenced as **Text n** within CETerm configuration, where **n** is the assigned slot number. In our example above, text entry **Text 4**, within CETerm, will be associated with the text string “Carriage return \r”

You can also edit the text strings directly on the mobile terminal by highlighting and tapping the User Text slot.

Remapping Application keys

Most Windows Mobile devices have hardware application keys (buttons) that may be associated with installed applications. These keys may be used to launch associated applications. It is possible to remap these buttons to perform application or emulation actions. This remapping is valid only while the CETerm is running.

Follow these steps to remap your device application keys to host keys or application operation.

1. From the application menu, select **[Session] [Configure]** to open the configuration dialog.
2. Select the **[Options]** tab
3. Select **[Config Keybars and Keys]** button. This will open another tabbed dialog.
4. Select the **[App Keys]** tab
5. Enable the checkbox "**Remap Application Keys**". If this check box is not enabled, device application keys will not be remapped
6. From the "**Key**" dropdown box, select the device application key that you wish to remap to an emulation host key or CETerm application operation
7. From the list box "**Select key action below:**" select the action association
8. To remap other device application keys, repeat steps 6 and 7.

NOTE: If any of the device application keys is associated with the Windows Mobile "Record" application, then this association must be changed. Otherwise, the remap configuration for that key may not work. You can use the "Buttons" applet to change this association.

- From the "Start" menu, select "Settings". This will launch the device control panel
- Select the [Personal] tab
- Run the "Buttons" application
- Under the button assignment list box, look for the device application button, which has an association with "Record". Highlight this button
- From the "Button assignment:" dropdown list, select anything but "Record" to change the device application key association
- Now proceed with the application key remapping procedure described above.

3270 Host key descriptions

ATTN

The Attention key interrupts the host application.

SYS_REQ

The System Request key gives context to the System Software such as the SSCP (System Services Control Point)

CLEAR

The Clear key causes a CLEAR Attention Identifier key to be sent to the host and the host responds according to the host application.

RESET

The Reset key resets the terminal. Depending upon the current state, it removes the host application from a keyboard inhibit state, terminates the System Request functions and exits terminal from insert mode.

ERASE INPUT

This key clears all unprotected input fields and moves the cursor to the beginning of the first input field.

ERASE to END OF FIELD (EOF)

This key erases all data in an input field from the current cursor location to the end of the input field

DELETE

The Delete key deletes data from an input field. When you press this key, the character at the cursor location is deleted, and all characters to the right of the cursor shift one position to the left.

INSERT

This key toggles the insert mode on and off. In insert mode, characters are inserted at the current cursor location if space is available. The characters to the right of the cursor are shifted one character position to the right.

HOME

This key repositions the cursor to the first input location of the first input field.

TAB or NEXT

This key moves the cursor forward to the next input field. When the cursor is not on an input field it moves to the next input field from the current cursor location.

BACKTAB or PREVIOUS

This key moves the cursor back to the previous input field. When the cursor is not on an input field, the cursor moves to the previous input field from the current cursor location. This key is equivalent to [Shift] [Tab].

ENTER

The Enter key submits control to the host application.

NEW LINE

This function moves the cursor to the first input field on the next line.

PA1, PA2, PA3

The PA1 through PA3 keys communicate with the host application. Their use is defined by the host application.

PF1 - PF24

The Program Function keys PF1 - PF24 communicate with the host application. Their use is defined by the host application.

5250 Host key descriptions

ATTN

The Attention key interrupts the host application.

SYS_REQ

The System Request key gives context to the System Software such as the SSCP (System Services Control Point)

CLEAR

The Clear key causes a CLEAR Attention Identifier key to be sent to the host and the host responds according to the host application.

RESET

The Reset key resets the terminal. Depending upon the current state, it removes the host application from a keyboard inhibit state, terminates the System Request functions and exits terminal from insert mode.

ERASE INPUT

This key clears all unprotected input fields and moves the cursor to the beginning of the first input field.

ERASE to END OF FIELD (EOF)

This key erases all data in an input field from the current cursor location to the end of the input field

FIELD MINUS

This key causes the cursor to advance to the next field and a minus sign is inserted in the last position of a signed numeric-only field.

FIELD PLUS

This key causes the cursor to exit an input field and insert null characters from the current cursor location to the end of the field.

FIELD EXIT

This key behaves similar to the Field Plus key. It causes the cursor to exit an input field and insert null characters from the current cursor location to the end of the field.

ROLL UP

The Roll Up key sends a request to the host computer to roll up the information on the display.

ROLL DOWN

The Roll Down key sends a request to the host computer to roll down the information on the display.

DUP

This DUP key is used to insert DUP characters in a field for host processing.

FIELD MARK

The Field Mark key is used to insert a Field Mark character in a field for host processing.

DELETE

The Delete key deletes data from an input field. When you press this key, the character at the cursor location is deleted, and all characters to the right of the cursor shift one position to the left.

INSERT

This key toggles the insert mode on and off. In insert mode, characters are inserted at the current cursor location if space is available. The characters to the right of the cursor are shifted one character position to the right.

HOME

This key moves the cursor to the first input location of the first input field.

TAB or NEXT

This key moves the cursor forward to the next input field. When the cursor is not on an input field it moves to the next input field from the current cursor location.

BACKTAB or PREVIOUS

This key moves the cursor back to the previous input field. When the cursor is not on an input field, the cursor moves to the previous input field from the current cursor location. This key is equivalent to **[Shift] [Tab]**.

ENTER

The Enter key submits control to the host application.

NEW LINE

This function moves the cursor to the first input field on the next line.

PA1, PA2, PA3

The PA1 through PA3 keys communicate with the host application. Their use is defined by the host application.

PF1 - PF24

The Program Function keys PF1 - PF24 communicate with the host application. Their use is defined by the host application.

VT Host key descriptions

The following legend is used to indicate escape sequence values associated with various keys:

Bold Orange Indicates 7 bit ASCII mode

Bold blue Indicates 8 bit ASCII mode

HOLD

The Hold key has no current action.

ENTER

The Enter or Return key transmits either a carriage return (CR) character or a carriage return and line feed (LF) character, depending on the VT configuration.

COMPOSE CHAR

The Compose Character key does not transmit a code. Pressing the Compose character key starts a compose sequence which is used to generate characters that cannot be typed directly from the keyboard. Because accented characters are accessible from the SIP, this key is not implemented.

TAB

The TAB key transmits a tab character .

DELETE

This key transmits a DEL character.

FIND

This key transmits the escape sequence **ESC [1 ~** or **CSI 1 ~**

INSERT HERE

This key transmits the escape sequence **ESC [2 ~** or **CSI 2 ~**

REMOVE

This key transmits the escape sequence **ESC [3 ~** or **CSI 3 ~**

SELECT

This key transmits the escape sequence **ESC [4 ~** or **CSI 4 ~**

PREV SCREEN

This key transmits the escape sequence **ESC [5 ~** or **CSI 5 ~**

NEXT SCREEN

This key transmits the escape sequence **ESC [6 ~** or **CSI 6 ~**

PF1 – PF4

The numeric keypad keys PF1 through PF4 transmit the following escape sequences

Key	ANSI Mode	VT 52 Mode
PF1	SS3 P or ESC O P	ESC P
PF2	SS3 Q or ESC O Q	ESC Q
PF3	SS3 R or ESC O R	ESC R
PF4	SS3 S or ESC O S	ESC S

The 5 keys F1-F5 on a VT terminal are local function keys and do not send codes. When a mobile terminal has physical keys for F1-F5, we send PF1-PF4 for the corresponding F1-F4 and send a custom escape sequence for F5, which depends on the device.

Default VT Keys Escape Sequence Table

The following table shows the default association of escape key sequence with action for VT emulation within CETerm. There are no spaces in the key code sequence. Both 7 bit and 8 bit escape sequences are shown.

Key	7 Bit Escape Sequence		8 Bit Escape Sequence	
	Code	Hex	Code	Hex
Line Feed	<10>	0A	<10>	0A
Enter	<13>	0D	<13>	0D
Backspace (Delete)	<127>	7F	<127>	7F
Backspace	<8>	08	<8>	08
Tab	<9>	09	<9>	09
Back Tab	<Esc>[Z	1B 5B 5A	<155>Z	9B 5A
Up Arrow	<Esc>[A	1B 5B 41	<155>A	9B 41
Down Arrow	<Esc>[B	1B 5B 42	<155>B	9B 42
Left Arrow	<Esc>[D	1B 5B 43	<155>C	9B 43
Right Arrow	<Esc>[C	1B 5B 44	<155>B	9B 44
VT PF1	<Esc>OP	1B 4F 50	<143>P	8F 50
VT PF2	<Esc>OQ	1B 4F 51	<143>Q	8F 51
VT PF3	<Esc>OR	1B 4F 52	<143>R	8F 52
VT PF4	<Esc>OS	1B 4F 53	<143>S	8F 53
F5*	<Esc>[M	1B 4F 4D	<143>M	8F 4D
F6	<Esc>[17~	1B 5B 31 37 7E	<155>17~	9B 31 37 7E
F7	<Esc>[18~	1B 5B 31 38 7E	<155>18~	9B 31 38 7E
F8	<Esc>[19~	1B 5B 31 39 7E	<155>19~	9B 31 39 7E
F9	<Esc>[20~	1B 5B 32 30 7E	<155>20~	9B 32 30 7E
F10	<Esc>[21~	1B 5B 32 31 7E	<155>21~	9B 32 31 7E
F11	<Esc>[23~	1B 5B 32 33 7E	<155>23~	9B 32 33 7E
F12	<Esc>[24~	1B 5B 32 34 7E	<155>24~	9B 32 34 7E
F13	<Esc>[25~	1B 5B 32 35 7E	<155>25~	9B 32 35 7E
F14	<Esc>[26~	1B 5B 32 36 7E	<155>26~	9B 32 36 7E
F15 / Help	<Esc>[28~	1B 5B 32 38 7E	<155>28~	9B 32 38 7E
F16 / Do	<Esc>[29~	1B 5B 32 39 7E	<155>29~	9B 32 39 7E
F17	<Esc>[31~	1B 5B 33 31 7E	<155>31~	9B 33 31 7E
F18	<Esc>[32~	1B 5B 33 32 7E	<155>32~	9B 33 32 7E
F19	<Esc>[33~	1B 5B 33 33 7E	<155>33~	9B 33 33 7E
F20	<Esc>[34~	1B 5B 33 34 7E	<155>34~	9B 33 34 7E
Find	<Esc>[1~	1B 5B 31 7E	<155>1~	9B 31 7E
Insert Here	<Esc>[2~	1B 5B 32 7E	<155>2~	9B 32 7E
Remove	<Esc>[3~	1B 5B 33 7E	<155>3~	9B 33 7E
Select	<Esc>[4~	1B 5B 34 7E	<155>4~	9B 34 7E
Previous Screen	<Esc>[5~	1B 5B 35 7E	<155>5~	9B 35 7E
Next Screen	<Esc>[6~	1B 5B 36 7E	<155>6~	9B 36 7E

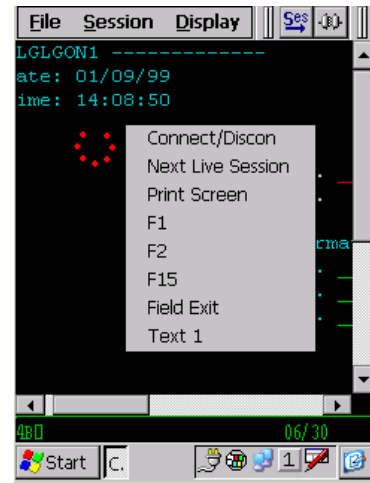
* F5 key is undefined by VT specifications. It can be remapped to any escape sequence.

Creating Context Menus

If configured, you can tap and hold your stylus anywhere within the terminal display area of your mobile terminal to invoke a context menu. This menu can be customized with specific entries.

Configurable KeyBar **Custom Keys 6** is associated with the Context menu. Any actions associated with **Custom Keys 6** shows up in the context menu when it is enabled. To enable the context menu

1. Navigate to [Session] -> [Configure] -> Options tab -> [Configure KeyBars and Keys] -> [Custom Bar]
2. Enable the **Enable Custom Context Menu** checkbox
3. Add the desired key operations which you want to appear in the Context Menu to Custom KeyBar **Custom Keys 6**
4. To trigger the Context Menu, tap and hold the stylus anywhere on the terminal display area. Appearance of a red dotted circle, as shown in the screenshot, indicates that the Context Menu is being invoked. Hold the stylus until the menu appears.



NOTE: If you have a User Text entry in the context menu, it appears as “Text x” where x is the user text entry order number. The actual value of the User Text is not shown since this can be too long to display.

NOTE: A special context menu is invoked when the user taps and holds the stylus in to top left vertical edge of the display screen. This special context menu is never disabled and offers predefined actions. If you are running CETerm session in full screen (with application menu and toolbars hidden), you can use this special context menu to get back into configuration dialogs.

Hotkey shortcuts

All emulation and browser sessions have several predefined hot keys. You should be able to see these configured in the “Common” Keymap table. These may normally be used with devices that have a keypad. The following table lists the default hotkeys. On some devices, **[Ctrl] [Shift]** may be replaced by **[Alt]** or **[Alt] [Shift]**

Hotkey	Description
[Ctrl] [Shift] [C]	Connect to the host
[Ctrl] [Shift] [D]	Disconnect a connected host session
[Ctrl] [Shift] [M]	Hides or displays the command menu bar
[Ctrl] [Shift] [B]	Display the command menu bar at the bottom
[Ctrl] [Shift] [K]	Configure host session
[Ctrl] [Shift] [Up]	Increase font size
[Ctrl] [Shift] [Down]	Decrease font size
[Ctrl] [Shift] [!]	Toggle between bold and normal font
[Ctrl] [Shift] [P]	Display or Hide SmartPad
[Ctrl] [Shift] [I]	Display or Hide Text Input Tool
[Shift] [Up]	Scroll up one row
[Shift] [Down]	Scroll down one row
[Shift] [Left]	Scroll left one column
[Shift] [Right]	Scroll right one column
[Ctrl] [Shift] [X]	Exit the emulator

Access Control / Device Lockdown

In certain workflow scenarios, there is a need to prevent users from being able to change the application configuration. Further there may be a requirement to prevent users from exiting the application or launching other applications on their Windows CE or Windows Mobile device. The Access Control features address these needs. Refer to the Options configuration section for details on configuring these features.

Access control functionality allows for the following:

- Administrators can protect access to session configuration settings with a password. This can be used to prevent users from changing the application configuration
- Prevent users from invoking another application. This is done by disabling the Start menu button.
- Prevent users from exiting the application.

Please refer to the Quick reference and configuration sections of this manual for details on configuring this functionality.

Device Lockdown

You can lock down your mobile terminal by configuring the following three options. These will prevent the user from exiting CETerm, launching any other application, or changing the configuration.

- Hide the Application Menu, Toolbars and KeyBars
 - Hide the Start button / Start bar
 - Disable application exit
 - Set a configuration access password
1. Navigate to **[Session] -> [Configure] -> [Display] -> [Advanced] -> [Hide/Show]**
 2. Enable checkboxes **Hide Menu Bar**, **Hide Tool Bar**, **Hide KeyBar**. Hit OK.
 3. Navigate to **[Session] -> [Configure] -> [Options] -> [Advanced] -> [Access Control]**
 4. Check **"Hide Start Bar"** checkbox
 5. Check **"Disable App Exit"** checkbox
 6. Tap the **"Set Password"** button and enter a configuration access password. Hit OK
 7. Tap the **"Exit Now"** button in the Advanced Options dialog.

- Launch CETerm. You will be in full screen mode, with no access to any application menu or Start Bar

NOTE: On Windows CE, “Hide Start button” will disable the Start button but leave the start bar. Under Windows Mobile, it will remove the button and also remove the “Smart Minimize” (x) button. You can also select “Hide Start Bar”, which will remove the whole start navigation bar.

Full Screen Mode

You can configure our Emulators and Web Browser such that all device and application control menus are hidden and the whole display area is occupied by the terminal screen. This is the full screen mode. To set up the full screen mode, you need to do the following:

- Hide application menu
- Hide application Toolbar and KeyBars
- Hide Start bar

To configure full screen mode follow these steps

1. Go to [Session]->[Configure]->[Display]->[Advanced]->[Hide/Show]
2. Enable the checkboxes “Hide Menu Bar”, “Hide KeyBar” and “Hide Toolbar”.
3. Hit OK
4. Go to [Session]->[Configure]->[Options]->[Advanced]->[Access Control]
5. Enable the checkbox “Hide Start Bar”
6. Hit OK all the way out

Your display area will be completely occupied by the terminal display window.

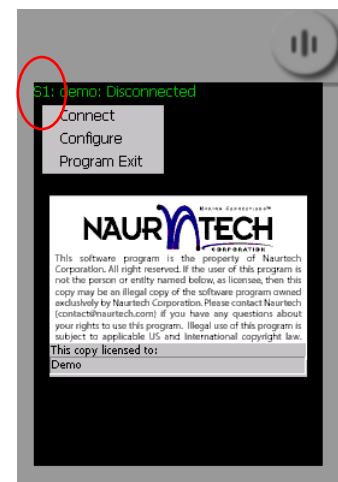
Accessing configuration from Full Screen mode

When configured in full screen mode, the whole screen is occupied by the terminal display. The user does not have access to the Windows CE Start button. The application menu and toolbars are all hidden.

You can still access configuration dialogs via a special Context Menu. If you tap and hold the stylus very near the top left vertical edge of the display screen, you will see a context menu appear. If the Start bar is visible, then tap and hold on the top left edge just below the Start bar. Your choices will be “Connect”, “Configure” and “Program Exit”.

Choosing Configure will bring up the configuration dialog. If you have configured an access control password, you will be required to enter this, prior to gaining access to the configuration dialogs.

The screenshot on the right shows the top left area, which will invoke the special context menu. This is circled in red.



International Character Set & Code Pages

Support for international languages can be provided in two categories.

- (1) localizing the application
- (2) input and display of language specific characters

Localization means that application dialogs; menus and other widgets are translated into the specific language. Currently, CETerm provides all its menus and dialogs only in English. However, it has rich support for the display and processing of host applications in international languages. Support for international language is provided for both Terminal Emulation and Web Browser sessions.

For IBM emulations (3270 and 5250), this support is provided via code pages. International language support for VT emulations is provided through the National Replacement Character set, MBCS (Multi Byte Character set Encoding), SBCS (Single Byte Character set Encoding) and UTF-8 encoding

A codepage is a list of selected character codes in a certain order. Codepages are usually defined to support specific languages or groups of languages, which share common writing systems. For example, codepage 1253 provides character codes required in the Greek writing system. The order of the character codes in a codepage provides the appropriate character code for an application when a user presses a key on the keyboard. When a new codepage is loaded, different character codes are provided to the application.

Codepages can be changed on-the-fly by the user, without changing the default language system in use on the mobile terminal. Language specific fonts are required to be installed on the device, to correctly display the character glyphs for the codepage language.

Code pages for IBM emulations (3270 & 5250)

In order to display European language character set for IBM (3270 and 5250) emulations, you will need to install the corresponding language code page. You can download a CAB file associated with your code page from the support section of our website and install this on your mobile terminal. The code page will then appear as a selection in the list under **[Session] -> [Configure] -> [Advanced] -> [IBM Options]**. By default, only IBM037 codepage (US English) is enabled.

The following is a list of available code pages. If you have a need for a codepage, which is not available on this list, please contact us at support@naurtech.com

Language	Codepage *	Codepage CAB
US English	037	IBM01140.CAB
Austrian	273	IBM01141.CAB
German	273	IBM01141.CAB
Danish	277	IBM01142.CAB
Norwegian	277	IBM01142.CAB

Finnish	278	IBM01143.CAB
Swedish	278	IBM01143.CAB
Italian	280	IBM01144.CAB
Spanish	284	IBM01145.CAB
UK English	285	IBM01146.CAB
French	297	IBM01147.CAB
Belgian	500	IBM01148.CAB
Icelandic	861	IBM861.CAB
Poland Romania Hungary	870	IBM870.CAB
Greek	875	IBM875.CAB
Swiss	871	IBM01149.CAB
Turkish	1026	IBM01026.CAB
Thai	838	IBM838.CAB
Multinational	256	IBM256.CAB
Cyrillic	1154 / 1381	IBM1154.CAB

For VT emulations, you need to install the correct codepage on the device and select this language option from **[Session] -> [Configure] -> [Advanced] -> [VT Extensions]**

Code pages for VT emulations

For VT emulations, we support native Windows CE codepages, which are already installed on the mobile terminal.

Asia Pacific language character sets

International character sets for Asian languages such as Chinese (Simplified and Traditional), Japanese, Korean, Thai etc. are supported for VT emulations only. This allows users to view the host text in the international language character set. This functionality for VT emulation also supports European language character sets. All application menus and dialogs still remain in English.

Follow these steps to configure your terminal to be able to display Asia-Pacific language character set:

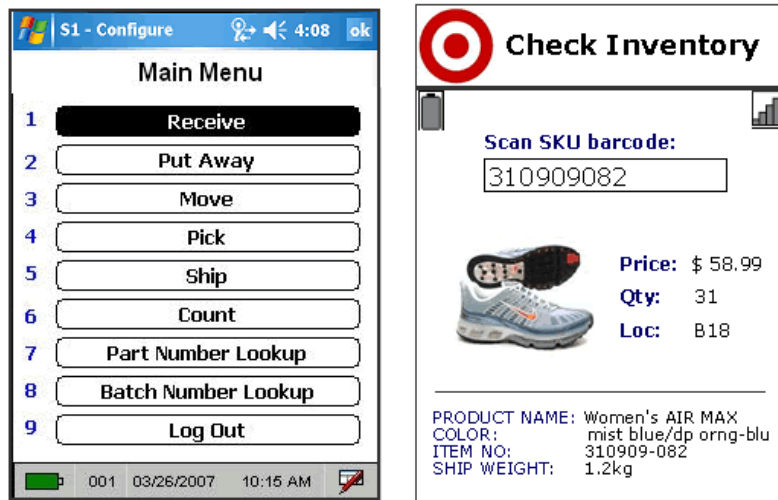
1. Go to **[Session] [Configure] [Connection]**
2. Make sure that the Host Type selected is VT220
3. Go to **[Advanced] [VT Extensions]** under the Connection configuration



4. Select the encoding mode. This indicates the type of encoding which is sent by the host for display of the international language character set. For VT emulation, your choices can be SBCS (Single Byte Character Set), DBCS (Double Byte Character Set), or UTF-8 encoding. If you are unsure, speak to your VT host application administrator.
5. Depending upon your encoding selection, the “Code Page” combo box will dynamically populate itself with all code pages available on your mobile terminal. These code page numbers are well defined. Code page for the desired language must be pre-installed on the device. Not all mobile terminals contain double-byte code pages. UTF-8 does not require a codepage.
6. Hit OK all the way out and Connect to your host

Web Browser Sessions

One of the value propositions for upgrading to Windows CE or Windows Mobile handheld devices is the multi-application versatility and graphical user interface. These devices provide a migration path from legacy host applications, using text based terminal emulation to web-based applications with rich content. Previously the only solution to this mixed use was to run both a terminal emulator and the Pocket IE browser as two separate applications. This scenario can be a recipe for disaster in a controlled access environment for data collection applications.



With CETerm, you can run browser sessions along-side terminal emulation sessions in any combination, all as part of the same application. A user can have both terminal emulation and web applications together within a single application. You get the data collection solution features, access control, and peripheral support for your web based application. Here are some of the benefits of the Naurtech CETerm Web Browser:

- **Full Screen readability and Context Menus.** You can hide the “Start” bar and application menu to maximize usage of your screen real estate giving you the full 320 x 240, ¼ VGA screen for display. “Tap and hold” Context Menus are available for application control
- **Operating System Lockout.** The address and navigation bars are inaccessible within the HTML browser sessions. The application may be configured to prevent users from exiting the application, launching any other application, or browsing to unauthorized websites. This locks down the device completely.
- **SIP Control.** The Soft Input Panel (SIP) popup can be fully controlled.
- **Tab Key.** Within Pocket IE, you are not able to use the Tab key to jump from one input field to the next. A TAB will not work in a barcode post-amble to jump to the next field after filling the current field. This results in compromised usability. The Naurtech browser fully supports

Tab and Back Tab navigation with native HTML text objects. Tabs also work in the barcode post-ambles.

- **Device and Peripheral Control.** Full control over barcode scanner and other peripherals (MSR, Smart Card Reader etc.) for browser based applications. Using HTML meta-tags, you can programmatically invoke any application operation from a web page.
- **Parse scanner decoded data.** Web applications can have the ability to validate, manipulate and parse the barcode scan data. A single 1D or 2D barcode can automatically be read into multiple input fields within a web form.
- **Associate Keypad hardware keys.** Touch screen navigation may not be suitable in every ADC solution. Therefore CETerm provides the ability to associate a menu option, URL, text string or any application operation to a hardware key
- **Single Application.** You do not need to run two separate applications for legacy TE and web based applications. Eliminates the need to support two separate applications
- **Multiple HTML Sessions.** You can run multiple simultaneous web applications and quickly switch between them. With other browsers, you can only have one web application active
- **Invoke Java Script functions.** Using embedded HTML meta-tags, you can invoke java script functions on the HTML page, based on various triggers such as page load, input selection, button press etc.
- **Full support of Symbol and Intermec meta-tags.** We fully support Symbol and Intermec proprietary HTML meta-tags. In addition there are many Naurtech meta-tags that allow for further device configuration, control and notification.

Please refer to the Connection configuration section for details on how to configure a connection to a web server.

Refer to the Web Browser Programming Reference Guide for details on using CETerm to access your web applications. This is available for download from our website.

Macros

Macro functionality was originally provided in CETerm to automate navigation across multiple host screens within a session. We no longer recommend using Macros and instead suggest using a script over a Macro since scripts are more flexible and offer a level of functionality not available with Macros. Macros remain part of CETerm for backward compatibility.

Note that Macros may only be used with terminal emulation session. To automate workflow in Web Browser sessions, you should use scripts.

CETerm provides a Macro toolbar to control all macro operations. To use macros, you must first “record” the steps which you are trying to automate. After recording a macro you can play this recorded macro any number of times.

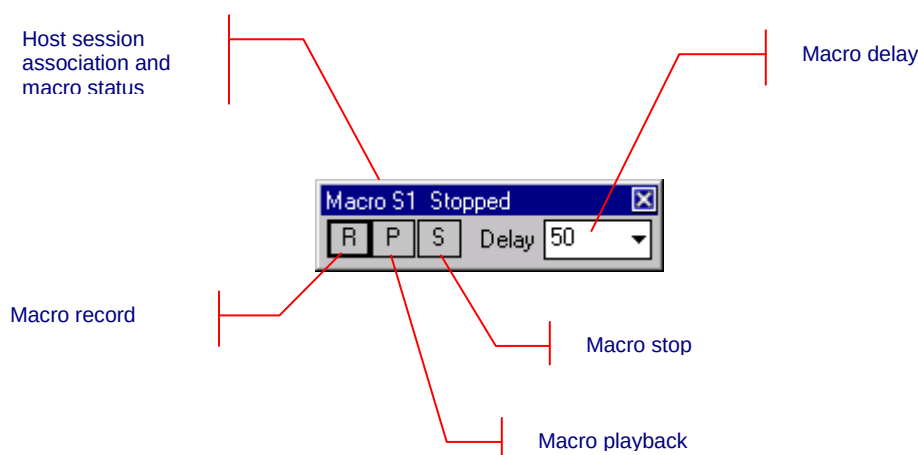
Because user input and host response is specific to the host application, macros are specific to the host application in use. In addition, macros are sensitive to the network propagation delay, which may vary with every connection to the host. CETerm uses a complex algorithm to record and playback a macro to account for various network and host application delays.

Each macro is associated with a specific host session. Only one macro may be recorded for each session. Re-recording a macro for a session will overwrite the previously recorded macro.

You can invoke the Macro toolbar from the application menu by selecting **[Display] [Macro]**.

You may also tap the "Macro " button  on the toolbar.

Tip: You may use the Macro hotkey **[Ctrl] [Shift] [S]** to invoke this operation



Macro Status: The macro toolbar window title displays the host session association and current status of the macro. Macro status may be “Stopped”, “Recording” or “Playback”.

Delay: Due to parameters such as network propagation delays, host application response times may vary slightly with every host session connection. This slight variation in response times can contribute to the failure of a macro during playback. The “Delay” attribute is a forced delay inserted during playback between sending recorded keystrokes and receiving host application

responses. Increase the delay timing when interacting with slower host systems or over a slower network. The maximum delay that may be entered is 1600 milliseconds (1.6 seconds)

Recording

Prior to recording a macro it is helpful to rehearse the desired actions. To record a macro, follow these steps.

- Configure and connect a terminal session to the host application
- Invoke the macro toolbar
- Tap the “Record” button  to start recording the macro. Focus will shift to the terminal application. The Macro toolbar title status will change to “Recording...”. You can interact with the host application as you would normally by entering text and host keys and getting response screens.
- During the recording phase, all inputs are saved. Once you are done navigating the host screens, you can stop recording by tapping the “Stop” button 
- The macro is automatically saved for the current active session. No explicit save is required.

Playback

You must successfully record a macro prior to playing it back. Macro playback must be invoked at the exact same point, within the host application, at which the recording started. Attempting a macro playback at any other point will most likely fail except for trivial text entry. To playback a macro, follow these steps.

- Connect to the host application on the session for which the macro was recorded. Navigate to the starting point within the host application at which the macro was recorded. This may be the opening screen if the macro is used to auto-login.
- Invoke the macro toolbar
- Tap the “Playback” button  to start playing the macro. Focus will shift to the terminal application. The Macro toolbar title status will change to “Playback...”. The macro toolbar will hide. You will see the cursor relocate and keystrokes automatically being typed. The host application will respond. The macro playback engine will appropriately wait until all host response is received and then type subsequent recorded keystrokes to navigate across additional host screens.
- It is recommended that you review your recorded macro to ensure that it successfully runs to completion.

WARNING: Playback of macros is sensitive to the host screen and associated keystrokes. Do not press any extraneous keys or the macro playback might fail. Macro playback should be started at the point where recording started.

By default the Macro toolbar will not be visible when you are playing a macro. If you want the macro toolbar to be visible when the macro is playing, please check the “Show Macro on Play” checkbox under **[Session] [Configure] [Display] [Advanced] [Hide/Show]**.

Creating a Mini-Macro

Within CETerm, most application operations have an associated ID Action (or IDA) code defined. These IDA codes can be chained to create a sequence of events, which is called a mini macro. This sequence of events can be remapped to any key.

You can use the User Text configuration to define a sequence of IDA operations which will get executed in serial order. This is a mini-macro. To create your mini macro:

1. Navigate to **[Session] -> [Configure] -> [Options] -> [Config KeyBars and Keys] -> [User Text]**
2. Enter your IDA sequences for **Text n** entries, where **n** is an index number between 1 and 64. The syntax is demonstrated via examples below.
3. Now you can remap **Text n** to any application, hardware or KeyBar key. Note that there are KeyBar buttons only for Text 1 through 20

Text 1 = `\IDA_SESSION_S1\\IDA_SLEEP_5000\\IDA_SESSION_CONNECT\`

In the example above, Text 1 will trigger the following operations in order:

- It will switch to session S1
- Wait for 5 seconds (5000 milliseconds)
- Attempt to connect to the configured host on this session

Text 2 = `\IDA_SESSION_DISCON_ALL\\IDA_PROGRAM_EXIT\`

In the example above, Text 2 will trigger the following operations in order:

- Disconnect all connected host sessions
- Exit CETerm application

You can join several IDA actions to create an elaborate macro to automate application navigation steps. Please contact us at support@naurtech.com for more information on IDA codes to create mini macros.

Printing

CETerm supports printing to a printer connected via a serial port, infrared (IrDA), Bluetooth, or over a WiFi (802.11x) network

VT printing

VT terminal emulation in CETerm and CEVT220 support all VT printing commands. You can invoke VT pass-through printing to any configured printer.

For serial attached printers, make sure that your printer is attached to the serial port via a serial cable and the serial port configuration is correct. Please refer to your printer manuals for serial port configurations required by your printer.

For IrDA printing, make sure that there is a clear path between the IrDA port on the handheld and the IrDA port on the printer.

For Bluetooth printer device, you must have a terminal that is Bluetooth enabled. For some of our device tailored CETerm versions which support automatic device discovery, you will be prompted with a list of “discovered” Bluetooth devices within range to which a print job may be redirected..

For network printing, make sure you have the correct printer queue or IP address defined for your printer configuration.

To print, issue print commands from the host application.

Legacy Extended commands

Legacy Extended Commands, such as those from Intermec are special commands implemented by the host application to control and interact with peripherals attached to the handheld device. Such commands are used to “extend” the connection protocol and send as part of the protocol data stream. These are generally used to transmit and receive data on the serial (RS-232) port of the device. Refer to reference documents from Intermec for details on their command set.

Extended commands can be used under 3270, 5250, and VT emulations. They can be used to print receipts or read from an attached scale or magnetic stripe reader.

Printing to a Network / 802.11x WiFi printer

You can either use the network printer queue or directly print to an IP printer over 802.11x. All Network printer configuration is set from:

```
[Session] -> [Configure] -> [Printer] -> Network (WLAN)
```

To print to a Windows print queue follow the syntax:

```
\\MyNetworkPrintQueueName\MyPrinter
```

Prior to printing, you may be prompted to provide a username and password.

To directly route data to an IP port use the syntax:

IPAddress:port

For example if the printer IP address is 192.168.1.10 and is listening on port 2345, then you can:

1. Select "Network (WLAN)" printer connection option under **[Session]->[Configure]->[Printer]**.
2. Set the Print Queue value to be **192.168.1.10:2345**
3. If you have DNS enabled, you may also use a hostname instead of the IP address

Hotspots

A Hotspot is an area on the terminal screen where a user can tap with a stylus to execute a function. This allows a user to interact with a host application without using physical keys or the KeyBar. A simple example might be the use of PF Keys. An operation associated with a PF key might be displayed on the terminal as "PF1 = Help". All Naurtech emulators automatically detect this as a Hotspot and will send a PF1 key to the host when you tap on the PF1 text on the terminal display. To invoke a hotspot, tap anywhere on the text of that hotspot. Hotspots are not user configurable.

All predefined Hotspots are static, meaning that the underlying text to be recognized cannot be changed to customize for your host server application. To implement dynamic Hotspots, so that you can customize the terminal text which will be recognized and also control the action which corresponds to such a Hotspot, use Scripting. Please refer to the CETerm Scripting Guide for details.

Hotspots are supported for 3270, 5250 and VT emulations. The emulations share some forms of Hotspots, such as function keys and menus, but others depend on the type of emulation.

The following table lists some text strings that are recognized as Hotspots

Hotspot String	Sends
PFx=	Function key x. where x is between 1..9
PFxx=	Function key x. where x is between 10..24
xx.	Menu option xx. where xx is any one or two digit number
Fxx=	Function key x. where x is between 1..24
<Fxx>=	Function key x. where x is between 1..24
Enter	Sends Enter key
"X. Menu choice"	Selects menu choice X
Double Tap	Sends Enter key
+	Roll Up key (5250 only)
-	Roll Down Key (5250 only)
More	Roll Down AID (5250 only)
Bottom	Roll Down AID (5250 only)

NOTE: Prior to using a “menu choice” HotSpot, the cursor must be in the input field where the menu choice is submitted. (Applies to IBM emulation only.)

TIP: HotSpots are sensitive to the stylus calibration on the mobile terminal. To get accurate HotSpot taps, make sure your stylus is correctly calibrated.

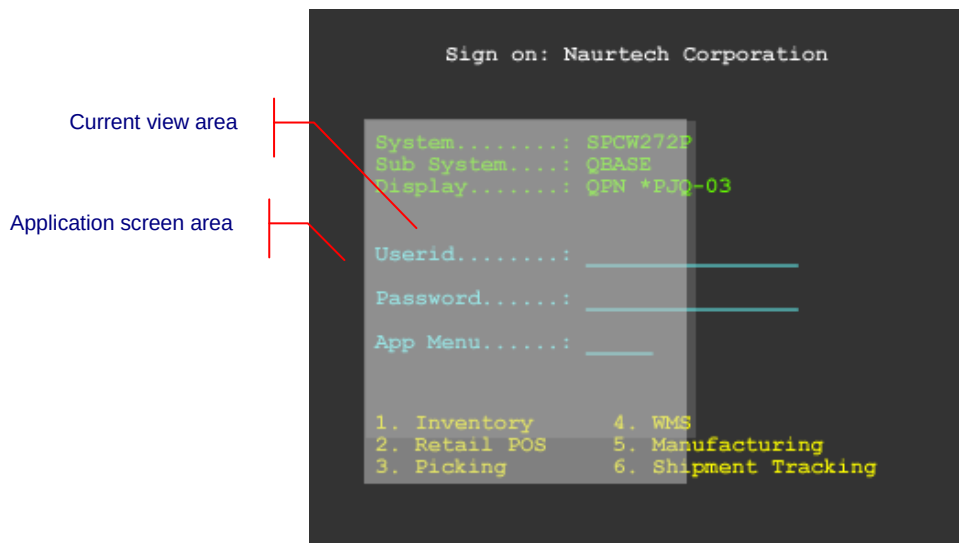
Screen Panning

Several host applications have been designed for the desktop screen form factor. These applications typically have 24 rows x 80 columns. When viewing these applications from a handheld device, only a portion of the host screen is visible because of the smaller display of the handheld device. Horizontal and vertical scroll bars are typically used to set the viewport location. As an alternative to scroll bars, the screen can be positioned by “dragging” the stylus.

Imagine the host application screen as a large sheet under the display on the handheld device. Screen Panning allows users to “tap, hold and drag” this sheet in any direction to move hidden areas of the host display into view on the handheld device without the use of scroll bars.

Follow these steps to use panning:

- Connect to a host application using the Naurtech emulator
- With the stylus, “tap and hold” anywhere on the terminal screen. Be careful not to tap on a HotSpot, if you do not also want a HotSpot action
- Drag the stylus, without lifting, to drag hidden areas of the screen into view



You can independently enable horizontal panning, vertical panning or both. This configuration is available under **[Display] -> [Advanced] -> [Touch features]**

 You can also dynamically reformat an application designed for a larger screen so that only specific fields from the larger screen are “scraped” and displayed in a new screen. This is done by implementing a screen reformat script which is customized for your host application. Please contact us at support@naurtech.com for a detailed discussion.

SmartPads

SmartPads are only applicable to Terminal Emulation sessions only.

Depending upon the terminal emulation type, certain keys may be required to navigate within the host application. The SmartPad is a soft keypad that provides access to all emulation specific keys. You can invoke the SmartPad only if the session is connected. The correct SmartPad appears for the emulation type of the current active session.

You can invoke the SmartPad from the application menu by selecting **[Display] [SmartPad]**.

You may also tap the "SmartPad " button  on the toolbar.

Tip: You may use the SmartPad hotkey **[Ctrl] [Shift] [P]** to invoke this operation

The SmartPad provides a quick and convenient access to all host keys when needed. SmartPads are not configurable dynamically. SmartPads for 3270, 5250 and VT host emulations are shown below.

SmartPad [3270]							
F1	F2	F13	F14	Eof	Srq		
F3	F4	F15	F16	Rst	Attn		
F5	F6	F17	F18	Clr	NI		
F7	F8	F19	F20	Hm	BSp		
F9	F10	F21	F22	Tb	BTb		
F11	F12	F23	F24	Ins	Del		
Pa1	Pa2	Pa3	ElIn	Esc	Ent		

SmartPad [5250]							
F1	F2	F13	F14	ElIn	Eof	Hlp	Prt
F3	F4	F15	F16	Srq	Attn	FEx	Sel
F5	F6	F17	F18	Clr	NI	F+	F-
F7	F8	F19	F20	Hm	BSp	Dup	Mark
F9	F10	F21	F22	Tb	BTb	RUUp	RDn
F11	F12	F23	F24	Ins	Del		
Pa1	Pa2	Pa3		Rst	Ent		

SmartPad [VT]							
Hld	Ent	PF1	ESC	BS	LF		
Cmp	Tab	PF2	F6	F7	F8		
Brk	DEL	PF3	F9	F10	F11		
CAN	ANS	PF4	F12	F13	F14		
Fnd	Ins	Rem	Hlp	Do	F17		
Sel	Prv	Nxt	F18	F19	F20		

NOTE: We recommend using the Configurable KeyBar with Custom bars to access frequently needed keys and conserve display space. The SmartPad functionality is provided for backward compatibility and will be phased out in later versions.

Text Input Tool

For Windows CE devices without a keyboard, data entry is usually performed using a stylus with the integrated soft keypad. This requires the user to spell-type text strings. This is a slow and tedious process. The Text Input Tool addresses this issue by sending complete text strings to the display window at the current cursor location. A user can record a set of often used text strings in the input tool.

You can invoke the Text Input Tool from the application menu by selecting **[Display] [Input Tool]**. You may also tap the "Input Tool" button  on the toolbar. On Pocket PC devices, the Text Input Tool may be made visible or hidden by alternatively selecting the toolbar button or hotkey.



Tip: You can also invoke the Text Input tool by using the hotkey **[Ctrl] [Shift] [I]**.

You can build your recorded list of text strings by pasting text from the clipboard (For example *[Edit][Copy]* in pocket word) directly into the Text Input Tool edit box. You can also directly type a text string into the edit box using the system soft keypad. Lastly, you can initialize this list from an ASCII text file.

Paste: Tapping the Paste button will copy any text from the clipboard into the edit box.

Add: Tapping the Add button adds any text in the edit box to the list. Blank strings are not added.

Del: Tapping the Del button deletes the currently selected text string from the list.

Clear: Tapping the Clear button clears the edit box.

File: Tapping the File button opens a dialog to select a text file that will be read to initialize the list. Each text string to be added to the list must be on a separate line delimited by a CRLF. The following file shows a sample input text file

```
78438-8889-9494
Any text string here
Username
```

We recommend that you create a file for initializing the list on your desktop PC and then copy it to the mobile terminal.

Send: The Send button sends the text in the edit box to the current cursor location on the terminal display.

Enter: Is equivalent to the Enter key.

Tab: Is equivalent to the Tab key.

BTab: Is equivalent to the “back tab” or [Shift] [Tab] action.

Esc: Is equivalent to the ESC key.

Each entry in the list is preceded by an index value in the form “1. “ (Not shown in the image above.) This index, including the first space after the period, is stripped before sending. You can edit an existing list entry by selecting it, making your changes, then pressing Add. It will replace the existing entry contents with the new value. If there is no leading index value, for example on a new entry, then Add will append a new list entry.

To create an entry, which begins with text similar to an index, first create a dummy entry, then edit it to include your desired text. For example, to create an entry with the contents “1. My text”, first enter the text “new” and press Add. Assume that this becomes the third entry. Select the entry from the list and change “3. new” to “3. 1. My text”, then press Add again.

The index values are used to identify the text sent with the “Input n” keys on the KeyBar. Be careful when deleting entries. Doing so may change the text sent via an Input key. A better choice is to use the User Text feature.

Special characters can also be entered in the text. This can be especially useful under VT emulation when custom escape sequences are required. The following special characters are available:

Operator	Meaning
\e	ESC character/action
\n	Newline character/action
\r	Enter character/action
\t	TAB character/action
\xDD	Hexadecimal value of byte

NOTE: The Input Tool functionality is similar to that provided by User Text. It is recommended that you use the User Text rather than the Input Tool

Command line options

CETerm supports a command line switch to invoke one or a sequence of IDA commands. The specific IDA commands can be used to invoke a desired action as the application launches. It may even be used to run a script which can be implemented to customize a desired behavior. Please refer to the list of IDA commands in the Appendix. Here are some examples:

The following command line example will start CETerm, switch to Session 1 and connect the session. If CETerm is already running, this will switch it to Session 1 and connect the session if it is not already connected.

```
CETerm.exe IDA_SESSION_S1 IDA_SESSION_CONNECT
```

To switch a running CETerm to Session 2, otherwise do nothing, use the command line syntax:

```
CETerm.exe IDA_SESSION_S2 IDA_NONE
```

IDA_NONE is a special code to prevent CETerm from starting if it is not already running. This is useful when you want an external tool to activate a CETerm action but don't want to start CETerm if not already running.

NOTE: The older command line option `-Sx` to launch CETerm with a specific session to be active should no longer be used. Although it is still supported, its usage is not recommended.

To run a script loaded in script slot 1, use the command line syntax:

```
CETerm.exe IDA_SCRIPT_1
```

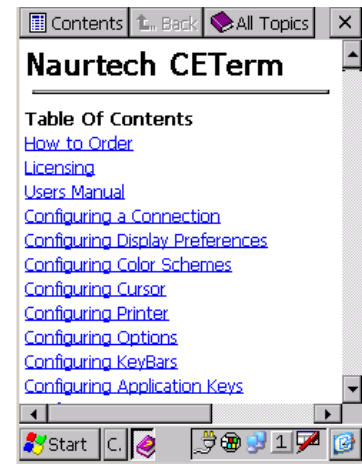
Online Help

Online help available on the mobile terminal. This is provided through the Online Help feature of the Windows CE operating system.

You can access online help from the application menu by selecting **[File] [Help]**. Alternatively, you can invoke the device help from **[Start] [Help]** and then select "Naurtech CETerm"

You can navigate within the Online help via the Pocket Browser.

NOTE: The title in the help file, even for single emulation products (CE3270, CE5250 and CEVT220) is always indicated to be "CETerm". All content in the help file applies to CETerm and all single emulation products.



NOTE: Although the online help is provided on the device, it is limited. For detailed explanation of features, configuration and functionality please refer to this Users Manual, the Scripting Guide or the Web Browser Programming Reference.

Glossary

3270

A well defined protocol used to communicate and control IBM mainframe display terminals.

5250

A well defined protocol used to communicate and control AS/400 display terminals.

802.11

An IEEE specification that provides interoperability between mobile clients and wireless LAN access points.

Access Point (AP)

Generally, a hardware product that bridges a Local Area Network (LAN) to a Radio Frequency (RF) network.

ASCII

A standard for assigning numerical values to the set of letters in the Roman alphabet and typographic characters.

Baud Rate

The number of bits per second transmitted between two devices.

Bar Code

A machine readable graphic image, using predefined patterns of linear bars or polygon elements to encode, typically, all of the ASCII character codes.

Clear To Send (CTS)

A serial (RS-232) signal used to control the exchange of data between the computer and a serial device. A hardware handshaking signal sent by the data communication equipment (DCE) to the data terminal equipment (DTE), which informs the DTE device it may send a message to the DCE device.

COM1, COM2, COM3, and COM4

Logical names for serial ports.

Cursor

A small rectangle or line, sometimes blinking, that indicates where characters will appear when typed.

DTR

Data Terminal Ready. An serial hardware handshaking signal sent from the data terminal equipment (DTE) indicating that it is ready for communication with the data communication equipment (DCE).

Emulation

Referred to in context of "Terminal Emulation" or "TE" where a software application is used to emulate a hardware terminal.

Emulator

The actual software program, CETerm, CE3270, CE5250, or CEVT220 that runs on a handheld device to emulate a hardware terminal.

Extended Binary Coded Decimal Interchange (EBCDIC)

An 8-bit character set, typically used in IBM mainframe environments.

Gateway

A computer device residing between a terminal device and an mainframe host to "load balance" and manage the host traffic. The term is also interchangeable used to refer to a computer device which serves as a link between two or more wide area networks.

Host Address

An address that identifies the host computer. Typically this is a numeric IP address or host name.

Host Application

An application program that runs on the host computer and is accessed from a hardware terminal or emulator.

Hot Key or HotKey

A key combination that is associated with a specific application operation.

HTML

An authoring language that defines the structure and layout for a web document / web page for view in a Web Browser.

HTTP

The underlying protocol used by the web. It defines how messages are formatted and transmitted between web servers and web Browsers.

Icon

A small graphic image displayed on the computer screen that visually represents a program applications.

IP address

An Internet Protocol address that identifies a specific computer or device on a TCP/IP network. It is represented as a 32-bit entity in dot notation such as 192.168.1.255

Local Area Network (LAN)

A group or set of physically connected computers / devices.

Logical Unit (LU)

An entity defined by IBM to represent a software element within an IBM SNA architecture. It represents a mainframe resource used to connect a terminal device

Mainframe

A large, powerful computer, which runs applications to serve many connected terminals or terminal emulation software clients.

Network Propagation Delay

The delay introduced in interactive computer communications due to routing, administration and management of data over networks.

Operator Information Area (OIA)

A single row area, typically used on IBM 3270 and 5250 terminals, that indicates the status of the terminal and the current cursor location.

Pocket PC

A version of the Windows CE graphical operating system for handheld devices. Also referred to as Windows Mobile OS.

Radio Frequency (RF)

Term used to indicate information exchange between computer devices where some or all of the communication uses radio transceivers.

Random Access Memory (RAM)

Fast computer memory used to store applications and data.

Reboot

A process to reset and restart a computer device.

Registry

A database residing in memory that is managed by the operating systems and shared by all applications on a computer device.

Response time

The time elapsed between submission of a query and receipt of a response

RTS

Request to Send. A serial handshaking signal that data terminal equipment (DTE) uses when it wants to send information to data communication equipment (DCE).

Scanner

A peripheral that enables a computer to read barcodes

Symbology

A well defined pattern of barcodes used to represent different characters. There are many different types of barcode symbologies, each having their own special characters and features.

Scrollbar

A graphical user interface component that is used to scroll horizontally or vertically within a window.

Serial port

A communication port used to attach a peripheral device, such as a printer.

Session

A logical interaction between a terminal device or terminal emulation application and a connected host application.

Stop bit

A data bit used in serial transmissions to signal the end of a character and indicate that the channel is idle.

Soft Input Panel (SIP)

A software key input application, typically available on Pocket PC devices

Telnet

An Internet communications protocol that enables a computer to function as a remote terminal.

Terminal

A device through which data or information can be entered or displayed interactively.

Terminal Type

A specific type or category of terminal. Generally it defines the capabilities of the terminal or terminal emulation client to the host application.

TN3270

A well defined Telnet protocol which defines the connection and interaction process for terminals to communicate with IBM 3270 mainframes.

TN5250

A well defined Telnet protocol which defines the connection and interaction process for terminals to communicate with IBM AS/400 servers.

Toolbar

A common graphical application component, consisting of a visible row of buttons which, when tapped by a stylus, cause the program to perform some action.

URL

The global address of a web page, document or any resource on the Web.

VT

Specifies a range of unintelligent visual terminals which are controlled using well defined protocols.

Windows CE

A graphical operating system for handheld devices

Wireless Wide Area Network (WWAN)

A wireless network extending over greater distances greater than a few miles.

Index

A

Access Control · 89
Action · 79
Aim Millisec · 96
Alert · 91
All Bars at Bottom · 65
Allow Drag · 91
Allow File / Registry read write · 87
Allow Program launch · 87
Answerback Message · 58
App Keys · 85
Application Menu · 30
Auto Connect · 23, 36
Auto Launch · 103
Auto Login · 15, 23
Auto Reconnect · 36
Auto Start · 103
Auto-fit to Browser screen · 66
Automated licensing · 92, 99
Automatic scrolling · 69
Auto-start sessions · 14
Autowrap · 57

B

Barcode keystrokes · 104
Battery State · 91
Baud Rate · 73
Beep Sound · 64
Block Mode · 18, 59
Bluetooth · 73
Browser Loading · 91
Browser Progress · 91
Build ID · 29

C

Center Cursor · 69
Certificate Checks · 40
Check Network before Send · 37
Check Network on Connect · 37, 103
Check Network on Resume · 37
Code Page · 13, 55, 127
Color scheme · 17, 67
Colors · 67
COM Port · 73

Command line options · 141
Configuration · 33
Confirm Disconnect · 37
Confirm Exit · 37
Connection · 33, 35
Context Menu · 84, 123
CTS Out · 73
Cursor · 68
Cursor Locked · 69
Cursor Options · 69
Cursor positioning · 93
Custom color scheme · 68
Custom ID · 98
Custom KeyBar · 84

D

Data Bits · 73
Data Length Max · 98
Data Length Min · 98
DBCS · 60
Delay · 132
Demo modes · 17
Device Lockdown · 13, 125
Device LU# / Name · 17, 55
Device parameters · 105
Device specific keymap · 78
Digital Clock · 10, 91
Disable App Exit · 89
Disable Browser Auto-SIP · 66
Display · 62, 63
Display Browser errors · 66
Double-tap Enter · 93
DSR Out · 73
DTR Control · 73

E

EAB · 56
Edit Keymap · 78
Editing Scripts · 87
Enable Aimer · 95
Enable Touch Features · 93
Error row · 55
Evaluation mode · 26
Exit Now · 89
Exit on Disconnect · 37
Extended Commands · 76

F

Fixed width characters · 70
Flags (Keymap) · 79
Font · 63, 70
Font size · 23
Full Screen · 12, 24
Full screen configuration · 126
Full screen mode · 126

H

Hide All Bars · 65
Hide Column Separators · 56
Hide Horizontal Scroll Bar · 64
Hide KeyBar · 65
Hide Menu Bar · 65
Hide OIA · 66
Hide SIP Button · 66
Hide Start Bar · 89
Hide Start Menu · 89
Hide Toolbar · 65
Hide Vertical Scroll Bar · 64
Host Address · 35
Host key descriptions - 3270 · 118
Host key descriptions - 5250 · 119
Host key descriptions - VT · 120
Host Type · 35
Hotkeys · 124
HotSpots · 15, 93, 136
HTML Browser · 12
HTML session · 130

I

IDA Action · 104
IDA App Keys · 116
IDA Configurable Keybar · 111
IDA Custom Keybar · 111, 115
IDA Sound · 106
IDA Tone · 106
IDA User Text · 116
Include Common Map · 78
Indicators · 13, 24, 91, 105
Industrial Web Browser · 130
Info Items · 90
Initial Sleep · 38
Install · 21
Installable Codepages · 10
Intermec Extended Commands · 135
Interval · 91

K

Keep cursor in input fields · 56
Key · 27
Key remap · 23
Keybar Cycle · 82
Keyboard Mode · 91
Keymap · 77

L

Legacy TE support · 15
Level · 91
License ID · 27
License registration · 25, 27
Line buffered · 59
Load at Startup · 88
Local Echo · 57
Lock down · 24
Lock SIP · 66

M

Macro on Connect · 36
Macro Status · 132
Macros · 16, 132
MBCS · 128
Meta Keys · 14, 109
Mini-Macro · 134
Multi-byte · 60
Multiple sessions · 12, 101

N

Network Action · 39
Network Awareness · 14
Network Host · 38
Network Printer · 72, 73
Network timeout · 38

O

Online help · 142
Options · 75

P

Panning Horizontal · 93
Panning Vertical · 93

Parity · 73
Password · 102
Playback · 133
Postamble · 23, 95
Preamble · 95
Print Queue · 73
Printer Connection · 72
Product version · 29
Proportional Characters · 70
Proportional Fonts · 70

R

Recording · 133
Redundancy · 96
Re-Initialize · 86, 88
Remap keys · 107
Report Check · 98
RF Strength · 91
RTS Control · 73
Run a script · 104

S

SBCS · 60
Scan Millisec · 96
Scanner · 95
Screen Display · 91
Screen Panning · 15, 137
Script timeout · 87
Scripting · 12, 86
Security · 40
Select color · 68
Select Keymap · 77
Send Mode · 59
Serial Config · 72
Serial Printer · 72
Server URL · 92
Session password · 17
Set Password · 89
Setup · 21
Shift error row content · 55
Show Macro on Play · 66
Show Script errors · 87
Show Start-Bar on exit · 66
Signature Capture · 10
Single Emulation Products · 8
SmartPad · 16, 138
Splash · 28
SSH Encryption · 48
SSH Secure Shell · 40

SSL & SSH · 25
SSL Secure Sockets Layer · 40
Stop Bits · 73
Strip Data End · 98
Strip Data Start · 98
Suggested text · 78
Suppress Auto field advance · 56
Suppress backspace at end · 56
Symbol CE VT · 61
Symbol TNVT · 61
Symbology · 97
System requirements · 20

T

Telnet Port · 36
Telxon · 61
Template · 88
Terminal Device · 35
Terminal Type · 38
Text auto-correct · 78
Text Input tool · 139
Timeout · 73
TN3270E · 56
Toolbar · 32
Touch · 93
Trap · 81
Two column DB characters · 61

U

Update · 91
User ID · 27
User Preference · 59
User Text · 81
UTF-8 · 60

V

Verify Input · 97
Visible Cursor · 69
VT Backspace · 57
VT C1 Controls · 57
VT Code Page · 61
VT Columns · 57
VT Enter key · 57
VT Host key descriptions · 120
VT Keyboard · 58
VT keys escape sequences · 122
VT printing · 135

W

Web Browser sessions · 130
Width Factor · 71
Windows Action Keys · 78

X

XOnOff Recv · 73
XOnOff Xmit · 73

Appendix A: ID Action Codes (IDA Codes)

The following table lists all supported ID Action codes, which may be used with our Terminal Emulation and Web Browser sessions. Some IDA codes can only be used in restricted circumstances, such as IDA_URL.

Symbolic Name	Friendly Name	Description
IDA_BEL	Bell	
IDA_BS	Backspace	
IDA_HT	Horizontal Tab	
IDA_TAB	Tab	
IDA_LF	Linefeed	
IDA_VT	Vertical Tab	
IDA_FF	Form Feed	
IDA_CR	Carriage Return	
IDA_SOH	Start Of Heading	
IDA_EOT	End Of Transmission	
IDA_STX	Start Of Text	
IDA_ETX	End Of Text	
IDA_ENQ	Enquiry	
Printable ASCII		
IDA_SPACE	<Space>	
IDA_EXCLAMATION_MARK	!	
IDA_DOUBLE_QUOTE	"	
IDA_NUMBER_SIGN	#	
IDA_DOLLAR_SIGN	\$	
IDA_PERCENT	%	
IDA_AMPERSAND	&	
IDA_SINGLE_QUOTE	'	
IDA_LEFT_PAREN	(	
IDA_RIGHT_PAREN	)	
IDA_ASTERISK	*	
IDA_PLUS	+	
IDA_COMMA	,	
IDA_HYPHEN	-	
IDA_PERIOD	.	
IDA_SLASH	/	
IDA_0	0	
IDA_1	1	
...	...	
IDA_9	9	
IDA_COLON	:	
IDA_SEMICOLON	;	
IDA_LESS_THAN	<	
IDA_EQUAL	=	
IDA_GREATER_THAN	>	
IDA_QUESTION_MARK	?	
IDA_AT	@	
IDA_A	A	
IDA_B	B	
...	...	
IDA_Z	Z	
IDA_LEFT_BRACKET	[	
IDA_BACKSLASH	\	
IDA_RIGHT_BRACKET	]	

Symbolic Name	Friendly Name	Description
IDA_CARET	^	
IDA_UNDERSCORE	_	
IDA_BACKTICK	`	
IDA_a	a	
IDA_b	b	
...	...	
IDA_z	z	
IDA_LEFT_BRACE	{	
IDA_PIPE		
IDA_RIGHT_BRACE	}	
IDA_TILDE	~	
IDA_DEL	DEL	
C1 ASCII Controls		
IDA_IND	Index	
IDA_NEL	Next Line	
IDA_HTS	Horizontal Tab Set	
IDA_RI	Reverse Index	
IDA_SS2	Single Shift 2	
IDA_SS3	Single Shift 3	
IDA_DCS	Device Ctrl Str	
IDA_PU1	Private Use One	
IDA_PU2	Private Use Two	
IDA_CSI	Ctrl Seq Intro	
IDA_ST	String Term	
IDA_OSC	OS Command	
IDA_PM	Private Message	
IDA_APC	App Program Command	
Internal Actions (TE only)		
IDA_UPDATE_CURSOR	Update Cursor	
IDA_INHIBIT_UPDATE	Inhibit Update	Don't update display
IDA_UNINHIBIT_UPDATE	Uninhibit Update	Allow display update
IDA_UPDATE	Update	Force display update
IDA_INHIBIT_SEND	Inhibit Send	VT buffer characters
IDA_UNINHIBIT_SEND	Uninhibit Send	VT stop buffering
IDA_SEND_PENDING	Send Pending Chars	VT send buffered chars
Program Actions		
IDA_PROGRAM_ABOUT	Program About	Display About dialog
IDA_PROGRAM_EXIT	Program Exit	Exit program
IDA_PROGRAM_HELP	Program Help	Display Help
IDA_PROGRAM_MINIMIZE	Minimize application	Only applicable for Windows CE
IDA_PROGRAM_FOREGROUND	Bring application to foreground	
IDA_PROGRAM_EXITSILENT	Exit application without prompts	
IDA_SUSPEND_DEVICE	Suspend Device	Enter suspend state
IDA_BLUETOOTH_DISCOVERY	Bluetooth Discovery	Start discovery
IDA_DEVICE_WAKEUP		
IDA_WARMBOOT	Warm Boot	Warm boot device
IDA_COLDBOOT	Cold Boot	Cold boot device
IDA_MENU_TOPBOTTOM	Menu Top/Bottom	Toggle menu location
IDA_MENU_TOGGLEHIDE	Menu Toggle	Toggle menu visibility
IDA_TOOLBAR_TOGGLE	ToolBar Toggle	Toggle toolbar visibility
IDA_START_TOGGLEHIDE	Start Menu Toggle	Toggle Start visibility
IDA_MENUBAR_TOGGLEHIDE	MenuBar Toggle	Toggle menu bar visibility
IDA_MENUBAR_ACTIVATE	Activate Menu	
IDA_SESSION_TOGGLECON	Connect/Disconnect	Toggle session connection

Symbolic Name	Friendly Name	Description
IDA_SESSION_CONFIGURE	Configure	Configure session
IDA_SESSION_CONNECT	Connect	Connect session
IDA_SESSION_DISCONNECT	Disconnect	Disconnect session
IDA_SESSION_NEXT_LIVE	Next Live Session	Switch to next live session
IDA_SESSION_PASSWORD	Password	Session password dialog
IDA_SESSION_PREV	Prev Session	Switch to previous session
IDA_SESSION_NEXT	Next Session	Switch to next session
IDA_SESSION_DISCON_ALL	Disconnect All	Disconnect all sessions
IDA_SESSION_S1	Session 1	Switch to session 1
IDA_SESSION_S2	Session 2	Switch to session 2
IDA_SESSION_S3	Session 3	Switch to session 3
IDA_SESSION_S4	Session 4	Switch to session 4
IDA_SESSION_S5	Session 5	Switch to session 5
IDA_TOOLBAND_HIDE	Hide Toolbar	Hide full Toolbar
IDA_TOOLBAND_TOGGLEHIDE	Toggle Toolbar	Toggle Toolbar visibility
IDA_KEYBAR_HIDE	Hide KeyBar	Hide KeyBar
IDA_KEYBAR_TOGGLEHIDE	KeyBar Toggle	Toggle KeyBar visibility
IDA_KEYBAR_LEFT	Prev KeyBar	Switch to previous KeyBar
IDA_KEYBAR_RIGHT	Next KeyBar	Switch to next KeyBar
IDA_KEYBAR_SEPARATOR	--Separator--	Separator for KeyBar
IDA_KEYBAR_NONE	(Empty)	No action placeholder
IDA_HSCROLL_HIDE	HScroll Hide	
IDA_HSCROLL_VISIBLE	HScroll Show	
IDA_HSCROLL_TOGGLEHIDE	HScroll Toggle	
IDA_HSCROLL_PLUSON	HScroll Right One	
IDA_HSCROLL_MINUSONE	HScroll Left One	
IDA_HSCROLL_PLUSHALF	HScroll Right Page	
IDA_HSCROLL_MINUSHALF	HScroll Left Page	
IDA_HSCROLL_PLUSEND	HScroll Right End	
IDA_HSCROLL_MINUSEND	HScroll Left End	
IDA_VSCROLL_HIDE	VScroll Hide	
IDA_VSCROLL_VISIBLE	VScroll Show	
IDA_VSCROLL_TOGGLEHIDE	VScroll Toggle	
IDA_VSCROLL_PLUSONE	VScroll Up One	
IDA_VSCROLL_MINUSONE	VScroll Down One	
IDA_VSCROLL_PLUSHALF	VScroll Up Page	
IDA_VSCROLL_MINUSHALF	VScroll Down Page	
IDA_VSCROLL_PLUSEND	VScroll Up End	
IDA_VSCROLL_MINUSEND	VScroll Down End	
IDA_FONT_PLUS	Font Inc	Increase font size
IDA_FONT_MINUS	Font Dec	Decrease font size
IDA_TOGGLE_FONT_BOLD	Font Bold	
IDA_SMARTPAD_OPEN	SmartPad Show	
IDA_SMARTPAD_CLOSE	SmartPad Hide	
IDA_SMARTPAD_TOGGLEHIDE	SmartPad Toggle	
IDA_SLEEP_10	Sleep 10msec	
IDA_SLEEP_50	Sleep 50msec	
IDA_SLEEP_200	Sleep 200msec	
IDA_SLEEP_1000	Sleep 1sec	
IDA_SLEEP_5000	Sleep 5sec	
IDA_SLEEP_20000	Sleep 20sec	
IDA_SLEEP_100000	Sleep 100sec	
IDA_SCAN_TRIGGER	Scan Trigger	Soft trigger scanner
IDA_SCAN_TRIGGER_OFF	Turn scan trigger off	

Symbolic Name	Friendly Name	Description
IDA_SCAN_ENABLE	Enable scanner	
IDA_SCAN_DISABLE	Disable scanner	
IDA_SCAN_SUSPEND	Suspend scanning	
IDA_SCAN_RESUME	Resume scanning	
IDA_MACRO_OPEN	Macro Show	Show Macro Tool
IDA_MACRO_CLOSE	Macro Hide	Hide Macro Tool
IDA_MACRO_TOGGLEHIDE	Macro Toggle	Toggle Macro Tool hiding
IDA_MACRO_RECORD	Macro Record	Start Macro record
IDA_MACRO_STOP	Macro Stop	Stop Macro record
IDA_MACRO_PLAY	Macro Play	Replay Macro
IDA_PRINT_SCREEN	Print Screen	Print current screen
IDA_PRINT_LINE	Print current line	
IDA_PRINT_CANCEL		
IDA_OIA_HIDE	OIA Hide	Hide IBM OIA bar
IDA_OIA_VISIBLE	OIA Show	Show IBM OIA bar
IDA_OIA_TOGGLEHIDE	OIA Toggle	Toggle OIA bar visibility
General IBM and VT Actions		
IDA_PF1	F1	(Not VT PF1)
IDA_PF2	F2	(Not VT PF2)
IDA_PF3	F3	(Not VT PF3)
IDA_PF4	F4	(Not VT PF4)
...	...	
IDA_PF24	F24	
IDA_HOME	Home	
IDA_DOWN	Down	
IDA_UP	Up	
IDA_LEFT	Left	
IDA_RIGHT	Right	
IDA_ENTER	Enter	
IBM Actions		
IDA_IBM_HOME	IBM Home	
IDA_DELETE	Delete	
IDA_INSERT_ON	Insert On	
IDA_INSERT_OFF	Insert Off	
IDA_INSERT_TOGGLE	Insert Toggle	
IDA_ATTN	Attn	
IDA_CLEAR	Clear	
IDA_CURSOR_SELECT	Cursor Select	
IDA_DUP	DUP	
IDA_ERASE_EOF	Erase EOF	
IDA_ERASE_INPUT	Erase Input	
IDA_FIELD_MARK	Field Mark	
IDA_NEWLINE	Newline	
IDA_PA1	PA1	
IDA_PA2	PA2	
IDA_PA3	PA3	
IDA_RESET	Reset	
IDA_SYSREQ	Sys Request	
5250 Specific Actions		
IDA_FIELD_EXIT	Field Exit	
IDA_FIELD_PLUS	Field +	
IDA_FIELD_MINUS	Field -	
IDA_FIELD_ADVANCE	Field Advance	
IDA_FIELD_BACKSPACE	Field Backspace	

Symbolic Name	Friendly Name	Description
IDA_FIELD_SUB	Field SUB	
IDA_HELP	IBM Help	
IDA_ROLL_DOWN	Roll Down	
IDA_ROLL_UP	Roll Up	
IDA_ROLL_LEFT	Roll Left	
IDA_ROLL_RIGHT	Roll Right	
IDA_BACKSPACE	Backspace	
IDA_PRINT	IBM Print	
VT Actions		
IDA_ANSWERBACK	Answerback	
IDA_FIND	Find	
IDA_INSERT_HERE	Insert Here	
IDA_NEXT	Next	
IDA_PREVIOUS	Previous	
IDA_REMOVE	Remove	
IDA_SELECT	Select	
IDA_VT_PF1	VT PF1	Numpad PF1 key
IDA_VT_PF2	VT PF2	Numpad PF2 key
IDA_VT_PF3	VT PF3	Numpad PF3 key
IDA_VT_PF4	VT PF4	Numpad PF4 key
IDA_NUMPAD_0	Numpad 0	
IDA_NUMPAD_1	Numpad 1	
IDA_NUMPAD_2	Numpad 2	
IDA_NUMPAD_3	Numpad 3	
IDA_NUMPAD_4	Numpad 4	
IDA_NUMPAD_5	Numpad 5	
IDA_NUMPAD_6	Numpad 6	
IDA_NUMPAD_7	Numpad 7	
IDA_NUMPAD_8	Numpad 8	
IDA_NUMPAD_9	Numpad 9	
IDA_VT_COMMA	Numpad Comma	
IDA_VT_ENTER	Numpad Enter	
IDA_VT_MINUS	Numpad Minus	
IDA_VT_PERIOD	Numpad Period	
IDA_UDK_F6	UDK F6	VT User Defined Key F6
IDA_UDK_F7	UDK F7	VT User Defined Key F7
...	...	
IDA_UDK_F20	UDK F20	VT User Defined Key F20
IDA_VT_HELP	VT Help	
IDA_VT_DO	VT Do	
IDA_ADD	Add	
IDA_MULTIPLY	Multiply	
IDA_DIVIDE	Divide	
Custom VT Sequences		
IDA_VT_SAP0135	VT SAP0135	0x00 0x35
IDA_VT_CSI_M	VT CSI M	ESC [M
IDA_VT_CSI_N	VT CSI N	ESC [N
IDA_VT_CSI_O	VT CSI O	
IDA_VT_CSI_P	VT CSI P	
IDA_VT_CSI_Q	VT CSI Q	
IDA_VT_CSI_R	VT CSI R	
IDA_VT_CSI_S	VT CSI S	
IDA_VT_CSI_T	VT CSI T	
Windows App Keys		
IDA_APPKEY_K1	App Key 1	

Symbolic Name	Friendly Name	Description
IDA_APPKEY_K2	App Key 2	
...		
IDA_APPKEY_K16	App Key 16	
IDA_SCROLL_UPPERLEFT	Scroll Upper Left	
IDA_SCROLL_UPPERRIGHT	Scroll Upper Right	
IDA_SCROLL_LOWERLEFT	Scroll Lower Left	
IDA_SCROLL_LOWERRIGHT	Scroll Lower Right	
IDA_SCROLL_CENTER	Scroll Center	
IDA_SCROLL_CURSOR_CENTER	Scroll Cursor Center	
IDA_SCROLL_CURSOR_VISIBLE	Scroll Cursor Visible	
IDA_COPYALL	Copy All	Copy screen to clipboard
IDA_PASTE	Paste	Past clipboard
Script Actions		
IDA_SCRIPT_1	Script loaded in slot 1	
IDA_SCRIPT_2	Script loaded in slot 2	
...		
IDA_SCRIPT_64	Script loaded in slot 64	
IDA_USTRING_0	Text 1	Send user text 1
IDA_USTRING_1	Text 2	Send user text 2
...	...	
IDA_USTRING_63	Text 64	Send user text 64
IDA_SIP_HIDE	SIP Hide	
IDA_SIP_SHOW	SIP Show	
IDA_SIP_TOGGLEHIDE	SIP Toggle	
IDA_SIP_LOCKDOWN	SIP Lockdown	
IDA_SIP_UNLOCK	SIP Unlock	
IDA_SIP_UP	SIP Up	
IDA_SIP_DOWN	SIP Down	
IDA_SIP_FORCEDOWN	SIP Forcedown	
IDA_IM_KEYBOARD	IM Keyboard	
IDA_IM_LOCKED	IM Locked	
HTML Actions		
IDA_URL_HOME	URL Home	
IDA_URL_BACK	URL Back	
IDA_URL	URL	Defines start of URL
IDA_URL_REFRESH	Refresh page	
IDA_DOM_SUBMIT	Force a form submission	
Special Actions		
IDA_VIBRATE_100	Vibrate 100ms	
IDA_VIBRATE_200	Vibrate 200ms	
IDA_VIBRATE_500	Vibrate 500ms	
IDA_VIBRATE_1000	Vibrate 1sec	
IDA_VIBRATE_2000	Vibrate 2sec	
IDA_VIBRATE_5000	Vibrate 5sec	
IDA_BEEP_OK	Beep	
IDA_BEEP_WARN	Beep Warn	
IDA_BEEP_LOUD	Beep Loud	
IDA_POPUP_IPADDRESS	Show IP Address	
IDA_POPUP_MACADDRESS	Show MAC Address	
IDA_POPUP_BATTERY	Show Battery	
IDA_POPUP_TIME	Show Time	

Symbolic Name	Friendly Name	Description
IDA_POPUP_SERIALNUMBER	Show Serial #	
IDA_POPUP_DEVICEID	Show Device ID	
IDA_POPUP_RFINFO	Show RF info	
IDA_KBD_CAPSLOCK	Force caps lock	
IDA_KBD_NUMLOCK	Force numeric lock	
IDA_INFO_RFMETER	Show RF Meter indicator	
IDA_INFO_RFTOWER	Show RF Tower indicator	
IDA_INFO_RFSTEPS	Show RF Steps indicator	
IDA_INFO_BATTERY	Show RF Battery indicator	
IDA_INFO_SCANNER	Show Scanner status	
IDA_INFO_KBDMODE	Show Keyboard mode	
IDA_INFO_REDBLUE	Show Red / Blue key status	
IDA_INFO_GREENYELLOW	Show Green / Yellow key status	