

ASCII Character Codes

This table lists the values for the ASCII control characters (ASCII decimal values 0 - 31). While the Decimal and Hex values are provided to aid in conversion, note that CRT requires **octal** values.

Ctrl	Dec	Hex	Octal
^@	0	0x00	\000
^A	1	0x01	\001
^B	2	0x02	\002
^C	3	0x03	\003
^D	4	0x04	\004
^E	5	0x05	\005
^F	6	0x06	\006
^G	7	0x07	\007
^H	8	0x08	\010
^I	9	0x09	\011
^J	10	0x0A	\012
^K	11	0x0B	\013
^L	12	0x0C	\014
^M	13	0x0D	\015
^N	14	0x0E	\016
^O	15	0x0F	\017
^P	16	0x10	\020
^Q	17	0x11	\021
^R	18	0x12	\022
^S	19	0x13	\023
^T	20	0x14	\024
^U	21	0x15	\025
^V	22	0x16	\026
^W	23	0x17	\027
^X	24	0x18	\030
^Y	25	0x19	\031
^Z	26	0x1A	\032
^[27	0x1B	\033
^\	28	0x1C	\034
^]	29	0x1D	\035
^^	30	0x1E	\036
^_	31	0x1F	\037

Advanced SSH Options



The Advanced SSH options divide into two tabs. In the **General** tab, you can choose an identity file and select whether you want to use compression on the encrypted session. In the **Port forwarding** tab, you can set up port forwarding.

The General tab options allow you to generate an RSA identity file which can be used for SSH login authentication, as well as to control the compression level of your SSH session. Note that SecureCRT 2.3 made a change in the identity file format, and identity files generated with SecureCRT 2.3 or later will not work with SecureCRT 2.2. Files generated in SecureCRT 2.2 can be read by version 2.3 and later.

There are two options for associating an identity file with an SSH session.

Use Global

Use Session-specific

Create Identity File

The compression options allow turning compression on or off, as well as controlling the level of compression from 1 to 9. 1 provides the best speed and the lowest compression level, while 9 provides the best compression and the lowest performance.

The default settings for compression are **off** and compression level **5**.

Use Compression

The Port Forwarding tab options allow creating and removing configurations that "forward" local ports to a port on a remote host. Please see the discussion of important Port Forwarding Security considerations.

Current Ports list

New button

Delete button

Local Port field

Remote Hostname field

Remote Port field

Save Port Forwarding Field values

Use single SSH connection option

Forward X11 Packets option

Auto Save Preferences

Saves the configuration settings automatically. With this command disabled, settings must be saved by selecting the Save Settings Now command from the **Options** menu.

Automate CRT startup

It's easy to set up a Desktop icon or Start Menu item that opens CRT directly into a specific terminal session. This is done using session configuration information invoked with command line switches.

The steps for automating startup are:

- 1 Choose shortcut command line options
- 2 Create a login script (optional)
- 3 Create a Windows Shortcut for CRT
- 4 Add switches to the Shortcut command line to invoke CRT options

Choose Shortcut Command Line Options

If you have created a session name, use the switch `/S session_name`.

```
CRT.EXE /S database
```

This example starts CRT and connects using the session named 'database'.

Note: If the "Save Session" option is checked in **Quick Connect**, the hostname or IP address will be used as the session name until it is changed.

If you want to use a hostname only, use a command line like the following:

```
CRT.EXE jupiter
```

This starts CRT and connects to the host 'jupiter'.

See Command Line Usage for all available options.

Create a Login Script

Avoid repetitive startup keystrokes by using the **Script Dialog** or a script file to automatically enter startup information such as userid. Using a login script requires that the session be defined with a session name.

To start a session with the user name filled in automatically:

- 1 Check the **Dialog** option on the **Scripts** tab of the **Session Preferences** dialog
- 2 Click on the **Details** button to open the **Script Details** dialog
- 3 Insert the user name in the "send" field. Passwords can also be sent this way. Be aware that placing Password information in the Script Details dialog will store it unencrypted in the CRT configuration file, which is not recommended for security reasons.

Note that the Expect field must contain the characters sent by the host server: i.e. the default "ogin:" string may have to be changed.

Create a Windows Shortcut for CRT

- 1 Use any of several methods to create a CRT shortcut
- 2 Add the `/S`, `/TELNET` or other switches
- 3 Change the icon and name as desired.

Warning: Using the Script Dialog for sensitive information such as userid and password is not recommended. Script Dialog information is stored in the CRT configuration file. The information is "obfuscated" but not encrypted.

CRT License Agreement

End-User License Agreement for CRT 2.4

Copyright (c) 1995-1999 Van Dyke Technologies, Inc.

All Rights Reserved.

AGREEMENT. After reading this agreement carefully, if you do not agree to all of the terms of this agreement, you may not use this software.

This software is owned by Van Dyke Technologies, Inc. and is protected by national copyright laws and international copyright treaties.

1. GRANT OF LICENSE AND PROHIBITIONS. This software is licensed to you. You are not obtaining title to the software or any copyrights. You may not sublicense, rent, lease, convey, modify, translate, convert to another programming language, decompile, or disassemble the software for any purpose. The license may be transferred to another if you keep no copies of the software. Permission must be obtained before mirroring or redistributing the evaluation copies of the software.

2. USE AND EVALUATION PERIOD. You may use one copy of this software on one client computer. A copy of this software is considered in use when loaded into temporary memory (i.e., RAM) and/or installed on a permanent storage device (i.e., hard disk, CD-ROM, etc.). You may also use a copy of the software on a home or portable computer, provided only one copy of the software is in use at a time. You may use an evaluation copy of the software for only thirty (30) days in order to determine whether to purchase the software.

3. MULTI-COMPUTER/NETWORK LICENSES. If this is a multi-computer or network license, you may make, install, and use additional copies of the software up to the number of copies authorized in your registration documentation.

4. LIMITED WARRANTY. THE SOFTWARE IS PROVIDED AS IS AND VAN DYKE TECHNOLOGIES DISCLAIMS ALL WARRANTIES RELATING TO THIS SOFTWARE, WHETHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER VAN DYKE TECHNOLOGIES NOR ANYONE INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THIS SOFTWARE SHALL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH SOFTWARE EVEN IF VAN DYKE TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR CLAIMS. IN NO EVENT SHALL VAN DYKE TECHNOLOGIES' LIABILITY FOR ANY DAMAGES EXCEED THE PRICE PAID FOR THE LICENSE TO USE THE SOFTWARE, REGARDLESS OF THE FORM OF CLAIM. THE PERSON USING THE SOFTWARE BEARS ALL RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE.

5. TERMINATION. This agreement terminates, you lose all rights licensed to you, and you must stop use of the software if you a) violate the terms of this agreement or b) you do not pay the license fee before the end of the evaluation period.

6. GOVERNING LAW. The agreement shall be governed by the laws of the State of New Mexico. Any action or proceeding brought by either party against the other arising out of or related to this agreement shall be brought only in a state or federal court of competent jurisdiction located in Bernalillo County, New Mexico. The parties hereby consent to the personal jurisdiction of such courts.

7. U.S. GOVERNMENT RESTRICTED RIGHTS. This software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software--Restricted Rights clause at 48 CFR 52.227-19, as applicable. Manufacturer is:

Van Dyke Technologies, Inc.
P.O. Box 37457
Albuquerque, NM 87176
USA

e-mail: sales@vandyke.com

CRT Order Form

The pricing below is valid through March 31, 1999. After March 31, 1999, please see <http://www.vandyke.com> for current pricing.

To print the order form, click on Print Topic in the File menu. Payments must be in **U.S. dollars** drawn on a **U.S. bank**.

Send this order form and a check to:

Van Dyke Technologies
P.O. Box 37457
Albuquerque, NM 87176
USA

CRT 2.4 Order Form

1	Computer:	Computer License	@ \$30.00	=	_____
2 to 9	Computers:	_____ Computer Licenses	@ \$27.50 each	=	_____
10 to 24	Computers:	_____ Computer Licenses	@ \$25.00 each	=	_____
25 to 49	Computers:	_____ Computer Licenses	@ \$20.00 each	=	_____
50 to 99	Computers:	_____ Computer Licenses	@ \$17.50 each	=	_____
100 to 199	Computers:	_____ Computer Licenses	@ \$15.00 each	=	_____
200 to 399	Computers:	_____ Computer Licenses	@ \$12.50 each	=	_____
Unlimited Computers (Single Site):			\$4995.00	=	_____

New Mexico Residents only add 5.8125% sales tax + _____
Total Payment _____

- Payments must be in US dollars drawn on a US bank.
- The above pricing is for any mix of Windows 98, Windows 95, or Windows NT.
- Prices are based on the number of computers on which the software is installed.
- Prices are good through March 31, 1999.
- Prices are in US Dollars.

--- Please Print ---

Name: _____ Date: _____

Company: _____

Shipping Address: _____

City, State, Zip: _____

Phone Number: _____

Country:

E-Mail Address:

Would you like to receive update announcements via e-mail?

How did you hear about CRT?

Comments:

Change Keyboard Mapping

Common ways to change keyboard mapping include:

Loading an alternate keymap from the `\keymaps` directory or

`ftp://ftp.vandyke.com/pub/CRT/keymaps`.

Keymaps downloaded from the ftp site should be copied to the local `\keymaps` directory.

Defining custom keymaps using the Keymap Editor.

Defining a Custom Keymap file.

Loading an Alternate Keymap

Keymaps available in the `\keymaps` directory

CRISP.key
doorway.key
vt100.key
vt220.key
vt400.key

Alternate keymaps available from `ftp.vandyke.com`

emacs.key
linux.key

Define Custom Keymaps using the Keymap Editor.

CRT supports Menu Functions, Scrollbar Functions, Telnet Functions, and VT Functions. These functions provide extensive control of CRT and terminal features. Any of the functions can be attached to a key combination, including the operation of CRT's menus. For example, CRT printing can be mapped to a special keystroke like `Ctrl+F12`, or the **Copy & Paste** command (`MENU_COPY_PASTE`) can be mapped to an unused function key.

Menu Functions control CRT menu commands.

Scrollbar Functions control the operation of CRT's vertical and horizontal terminal window scroll bars.

Telnet Functions allow interrupting telnet sessions.

VT Functions allow keystroke assignment.

Define a Custom Keymap file.

Keymap files can be created using an ASCII editor.

Chat Window

Shows or hides the **Chat Window**.

When displayed, the chat window is below CRT's text window and above the status bar. Use Ctrl+Enter to enter a new line in the **Chat Window**. Use Enter to send the text in the chat window to the remote host.

Note: If the window is maximized, you must first restore the CRT window before selecting this option. After selecting this option, the CRT window can be maximized again.

Clear Screen

Clears the current screen. This has no effect on the scrollback buffer.
This command is also available via the right mouse button.

Clear Scrollback

Clears the terminal's scrollback buffer. This has no effect on the current screen. This command is also available by right clicking in the main window area.

Color Schemes

A color scheme is a named set of attributes that defines the colors for the eight combinations of bold, underline and blinking.

Color schemes can be created, edited and deleted through the Color Schemes dialog that is invoked from the Display tab of the Session Preferences Dialog.

The following attributes are defined by a color scheme:

Foreground color - Set the foreground color for all fonts with either normal or bold characteristics.

Background color - Set the background color for all fonts with either normal or bold characteristics.

Note: Selecting the **Advanced** option in the **Color Schemes** dialog allows the foreground and background colors to be controlled individually for each font with the combined characteristics: normal/bold, underline/non-underline, blinking/non-blinking. There are eight different combinations of these characteristics.

Other Attribute options include:

Overstrike bold - Enable display of fonts with bold characteristics using overstrike bold characters. This is selected by default.

Show underline - Show the underline for fonts with underline characteristics. This is selected by default.

Enable blink - Enable blinking on fonts with this characteristic. This is selected by default.

Multiple attributes can be defined by using holding down the Ctrl key and clicking on each attribute desired in the Attributes list box.

Command Line Usage

Standard Session Options

Any combination of the following general command line options can be used.

CRT.EXE Option	Description
<code>/F session_file</code>	Use the specified session configuration file.
<code>/NOMENU</code>	Hide the menu bar.
<code>/NOTOOLBAR</code>	Hide the toolbar.
<code>/NOSAVE</code>	Disable Auto Save Preferences.
<code>/POS x y</code>	Specify the initial position of the CRT window, where <i>x</i> and <i>y</i> specify the upper left corner of the CRT window in pixel coordinates.
<code>/MAX_COLS n</code>	Specify the maximum number of columns. The maximum value for <i>n</i> is 512 and the minimum value is 132.
<code>/FIREWALL</code>	Connects session using current global firewall settings. Replaces <code>/PROXY</code> and <code>/SOCKS</code> options.

For a named session:

```
CRT.EXE [ options ] /S session_name
```

The session name is the label assigned to a terminal session in the name field of the **Connect** dialog. The available session names appear in the session list on the Connect dialog.

For a default Telnet session:

```
CRT.EXE [ options ] /TELNET hostname [ port ]
```

For a default rlogin session:

```
CRT.EXE [ options ] /RLOGIN hostname [ /L username ]
```

For a default serial session:

```
CRT.EXE [ options ] /SERIAL port [ /BAUD baudrate ] [ /PARITY parity ] [ /STOP stopbits ] [ /DATA databits ] [ /DSR | /NODSR ] [ /CTS | /NOCTS ] [ /XON | /NOXON ]
```

Serial Session Options

The following options may be used with a default serial session.

Note: `/SERIAL` and its related options are only available if serial capability is selected during installation.

SERIAL Option	Description
<code>/SERIAL port</code>	Specify the serial port (COM1, COM2, etc). The <i>port</i> parameter is required.
<code>/BAUD n</code>	Set the baud rate. Valid values for <i>n</i> are 110, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200. The default value is 38400.
<code>/DATA n</code>	Set the data bits. Valid values for <i>n</i> are 5, 6, 7 or 8. The default value is 8.
<code>/PARITY p</code>	Set the parity. Valid values for <i>p</i> are <i>NONE</i> , <i>ODD</i> , <i>EVEN</i> , <i>MARK</i> , <i>SPACE</i> . The default is <i>NONE</i> .
<code>/STOP n</code>	Set the stop bits. Valid values for <i>n</i> are 0, 1 or 2 (0 indicates 1 stop bit, 1 indicates 1.5 stop bits, 2 indicates 2 stop bits). The default value is 0 (1 stop bit).
<code>/DSR</code>	DTR/DSR (data-terminal-ready/data-set-ready) are enabled.
<code>/NODSR</code>	DTR/DSR (data-terminal-ready/data-set-ready) are not enabled. This is the default setting.
<code>/CTS</code>	RTS/CTS (request-to-send/clear-to-send) hardware flow control are enabled. This is the default setting.
<code>/NOCTS</code>	RTS/CTS (request-to-send/clear-to-send) hardware flow control are not enabled.
<code>/XON</code>	XON/XOFF software flow control are enabled.
<code>/NOXON</code>	XON/XOFF software flow control are not enabled. This is the default setting.



SSH Session Options

For a default SSH session:

```
SECURECRT.EXE [ options ] /SSH [ /L user ] [ /I identityfile ] [ /C ciphername ] [ /P port ] [ /Z compressionlevel ] hostname
```

The following options may be used with a default SSH session.

Note: `/SSH` and its related options are only available in SecureCRT.

SSH Option

hostname

`/L username`

`/I identityfile`

`/C cipher`

`/P port`

`/Z compressionlevel`

Description

Specifies the hostname of the SSH server. The *hostname* parameter is required.

Specifies the username when connecting to the SSH server.

Specifies the location of the user's identity file. The identity file contains the private key needed to connect to the server using RSA authentication. The absence of this option causes password authentication to be used.

Specifies a cipher for encrypting the session. Valid values for *cipher* are *NONE*, *DES*, *3DES*, *RC4* and *BLOWFISH*. The default is *3DES*.

Specifies the SSH server port. The default value is 22.

Specifies the compression level from 1 (lowest compression/fastest) to 9 (highest compression/slowest).

Connect

Displays the **Connect** dialog with the **Session List** tab selected.

From the **Connect** dialog, you can connect to a remote host by double-clicking on a session in the session list, or by selecting a session and clicking **OK**.

The **Connect** dialog allows you to create, edit, and delete sessions.

The order of the session list can be rearranged by using the Up and Down buttons.

Sessions may be created to use the Rlogin, Telnet, and TAPI protocols. If support for the Serial protocol was chosen at installation then sessions may also be created that connect to serial (COM) ports.

Each session saved includes a comprehensive set of preferences, including protocol-specific settings, emulation, size, font, colors and other options.

Use the Quick Connect tab to make connections without using an existing session.

Note: The Connect menu option is not available when you are connected. New connections can be made using **New Window** and **Quick Connect**.

The option to make a session connect via the Firewall setting is also available with the Telnet and SSH protocols.



SecureCRT users may also create sessions that use the Secure Shell (SSH) protocol.

Copy

Copies the current selection onto the Clipboard. The previous contents of the Clipboard are lost. This operation is also available via the right mouse button.

This command is not available until you have made a selection with the mouse.

Copy & Paste

Copies the current selection onto the Clipboard and immediately sends the selection to the remote host as if it had been typed. This operation is also available via the right mouse button.

This command is not available until you have made a selection with the mouse.

Custom Keymap

A custom keymap can be edited using either a text editor, such as Notepad, or by using the [Keymap Editor](#).

A [Custom Keymap Example](#) has been provided.

Each line of a CRT keymap file has the following format:

```
modifiers    virtual_key    action
```

modifiers:

At least one modifier is required.

- N is None
- E is Extended key
- S is Shift
- C is Control
- A is Alt

N is only used if there is no E, S, C, or A.

E is used to distinguish between keys that occur twice on the keyboard. For example: *insert*, *delete*, and *enter*.

virtual_key:

Here is the list of virtual keys that CRT recognizes. CRT allows either the virtual key name or value in keymap files.:

Virtual Key Name	Value
VK_A .. VK_Z	0x41 .. 0x5A
VK_0 .. VK_9	0x30 .. 0x39
VK_ADD	0x6B
VK_APPS	0x5D
VK_BACK	0x08
VK_CANCEL	0x03
VK_CAPITAL	0x14
VK_CLEAR	0x0C
VK_CONTROL	0x11
VK_DECIMAL	0x6E
VK_DELETE	0x2E
VK_DIVIDE	0x6F
VK_DOWN	0x28
VK_END	0x23
VK_ESCAPE	0x1B
VK_EXECUTE	0x2B
VK_F1	0x70
VK_F2	0x71
VK_F3	0x72
VK_F4	0x73
VK_F5	0x74
VK_F6	0x75
VK_F7	0x76
VK_F8	0x77
VK_F9	0x78
VK_F10	0x79
VK_F11	0x7A
VK_F12	0x7B
VK_F13	0x7C
VK_F14	0x7D
VK_F15	0x7E
VK_F16	0x7F
VK_F17	0x80
VK_F18	0x81
VK_F19	0x82

VK_F20	0x83	
VK_F21	0x84	
VK_F22	0x85	
VK_F23	0x86	
VK_F24	0x87	
VK_HELP	0x2F	
VK_HOME	0x24	
VK_INSERT	0x2D	
VK_MULTIPLY	0x6A	
VK_NEXT	0x22	(page down)
VK_NUMLOCK	0x90	
VK_NUMPAD0	0x60	
VK_NUMPAD1	0x61	
VK_NUMPAD2	0x62	
VK_NUMPAD3	0x63	
VK_NUMPAD4	0x64	
VK_NUMPAD5	0x65	
VK_NUMPAD6	0x66	
VK_NUMPAD7	0x67	
VK_NUMPAD8	0x68	
VK_NUMPAD9	0x69	
VK_PAUSE	0x13	
VK_PRINT	0x2A	
VK_PRIOR	0x21	(page up)
VK_RETURN	0x0D	
VK_SCROLL	0x91	
VK_SELECT	0x29	
VK_SEPARATOR	0x6C	
VK_SHIFT	0x10	
VK_SNAPSHOT	0x2C	
VK_SPACE	0x20	
VK_SUBTRACT	0x6D	
VK_TAB	0x09	
VK_UP	0x26	

action:

Send String and **Run Script** are the two options for acting on a keypress.

Send String If the virtual key is pressed with the corresponding modifiers, the associated string is sent as if typed. The string can include characters represented in octal notation. For example, <Escape>OP, would be represented as: `"\033OP"`. The quotes are required. See the [ASCII Character Code](#) table for octal ASCII codes.

Run Script A script can be run by associating it with a virtual key/modifier combination using the RUN("filename") syntax. For example:

```
RUN ("C:\Program
Files\CRT\scripts\sample.csf")
```

Functions are simply predefined behavior. For example, VT_CURSOR_UP is the VT100 behavior of the *cursor up* key. Depending on the current cursor key mode, this function sends one of two escape sequences even though it is the same key sequence.

CRT Functions include [Menu Functions](#), [Scrollbar Functions](#), [Telnet Functions](#) and [VT Functions](#).

Custom Keymap Example

Here is a keymap file that is an alternate to the built-in VT220 keymap.

```
; VT220.KEY      (for use with a PC-101 keyboard)
; map F1..F4 to send PF1..PF4
N                VK_F1          VT_PF1
N                VK_F2          VT_PF2
N                VK_F3          VT_PF3
N                VK_F4          VT_PF4
; keypad when numlock on
N                VK_NUMPAD0     VT_KEYPAD_0
N                VK_NUMPAD1     VT_KEYPAD_1
N                VK_NUMPAD2     VT_KEYPAD_2
N                VK_NUMPAD3     VT_KEYPAD_3
N                VK_NUMPAD4     VT_KEYPAD_4
N                VK_NUMPAD5     VT_KEYPAD_5
N                VK_NUMPAD6     VT_KEYPAD_6
N                VK_NUMPAD7     VT_KEYPAD_7
N                VK_NUMPAD8     VT_KEYPAD_8
N                VK_NUMPAD9     VT_KEYPAD_9
N                VK_DECIMAL     VT_KEYPAD_PERIOD
; keypad when numlock off
N                VK_INSERT      VT_KEYPAD_0
N                VK_END         VT_KEYPAD_1
N                VK_DOWN        VT_KEYPAD_2
N                VK_NEXT        VT_KEYPAD_3
N                VK_LEFT        VT_KEYPAD_4
N                VK_CLEAR       VT_KEYPAD_5
N                VK_RIGHT       VT_KEYPAD_6
N                VK_HOME        VT_KEYPAD_7
N                VK_UP          VT_KEYPAD_8
N                VK_PRIOR       VT_KEYPAD_9
N                VK_DELETE      VT_KEYPAD_PERIOD
; other keypad
E                VK_RETURN      VT_KEYPAD_ENTER
N                VK_ADD         VT_KEYPAD_COMMA
E                VK_ADD         VT_KEYPAD_COMMA
S                VK_ADD         VT_KEYPAD_MINUS
SE              VK_ADD         VT_KEYPAD_MINUS
; non-keypad cursor keys
E                VK_UP          VT_CURSOR_UP
E                VK_DOWN        VT_CURSOR_DOWN
E                VK_LEFT        VT_CURSOR_LEFT
E                VK_RIGHT       VT_CURSOR_RIGHT
; Find      | Insert      | Remove
; Select | Prev Screen | Next Screen
E                VK_INSERT      VT_FIND
E                VK_HOME        VT_INSERT_HERE
E                VK_PRIOR       VT_REMOVE
E                VK_DELETE      VT_SELECT
E                VK_END         VT_PREV_SCREEN
E                VK_NEXT        VT_NEXT_SCREEN
; F6..F20
N                VK_F6          VT_F6
```

N	VK_F7	VT_F7
N	VK_F8	VT_F8
N	VK_F9	VT_F9
N	VK_F10	VT_F10
N	VK_F11	VT_F11
N	VK_F12	VT_F12
S	VK_F1	VT_F11
S	VK_F2	VT_F12
S	VK_F3	VT_F13
S	VK_F4	VT_F14
S	VK_F5	VT_F15
S	VK_F6	VT_F16
S	VK_F7	VT_F17
S	VK_F8	VT_F18
S	VK_F9	VT_F19
S	VK_F10	VT_F20
S	VK_F11	VT_F11
S	VK_F12	VT_F12

Disconnect

Terminates the current connection.

This command is only available when you are connected.

Exit

Quits CRT.

If you select **Exit** while connected, CRT asks whether you wish to terminate the current connection.

Find

Displays the standard Windows **Find** dialog.

[Find what](#)

[Match whole word only](#)

[Find Direction](#)

Getting Started - SSH and SecureCRT



SecureCRT is very similar to CRT, so if you have used CRT you will know how to use SecureCRT. See [Getting Started - Telnet with CRT](#) for a quick introduction to telnet and the Quick Connect dialog. Also read [What is SecureCRT?](#) and [Secure Shell Protocol](#).

SecureCRT adds options to the Session Preferences [Session tab](#) that you will need to learn about and look for.

SSH is a secure terminal emulation protocol that allows [authentication](#) using password and RSA methods. See [Setting Up RSA Authentication](#) for more information on authentication.

To initiate an SSH session on a LAN or other remote server, verify that an SSH server is available. SSH servers are not as commonly used as telnet servers.

Here's the fastest, easiest way to connect to an SSH server:

- 1 Click on **File, Quick Connect**
- 2 Select '**ssh**' from the **Protocol** list.
- 3 Type the host (server) name or IP address into the **Hostname or IP** field.
- 4 Change the port if it's different than the default.
5. The rest of the fields should be optional - most servers support 3DES [ciphers](#) and password authentication. You will be prompted for user name and password information if it has not been entered.

SecureCRT can be set to remember passphrases as long as there is one instance of the application is running. This behavior is off by default, and is controlled by the Registry value **Save Passphrase In Shared Memory** in the key

HKEY_LOCAL_MACHINE / Software / Van Dyke Technologies / SecureCRT / SSH

The value is off (0) by default. The option is turned on by using Regedit to change the value from a 0 to a 1.

A very important security note is that while SecureCRT supports the telnet, rlogin and serial protocols, these protocols are **not** encrypted and **not** secure. SecureCRT requires an SSH server connection to secure a connection.

[Port forwarding](#) is a very powerful capability that you may want to investigate. Port forwarding encrypts TCP/IP-based data channels from other Windows applications using SSH between a local PC and an SSH server. There are some [security factors](#) to setting up port forwarding that you should be aware of.

When an SSH session is started with an SSH server, the server sends SecureCRT a [host key](#). Registering the host key allows SecureCRT to match this key to the one provided by the sever the next time you log onto the server. The option controls all instances of SecureCRT on the PC regardless of username or configuration.

Getting Started - Telnet with CRT

Here's the fastest, easiest way to connect to a telnet server:

- 1 Click on **File, Quick Connect**
- 2 Type the host (server) name or IP address into the "Hostname or IP" field.
- 3 Change the port if it's different than the default.

This session will be saved by CRT if the "Save session" option is selected, so that the session configuration can be recalled or modified later. Saving sessions is how you can simplify connecting to a host repeatedly.

Once connected, options include copying and pasting text to and from the Clipboard, and printing to a local or network printer.

If the connection is denied or doesn't work correctly, look at Session Preferences. Two obvious parameters that may be different than the default are the terminal emulation and port value selected.

CRT keeps a default session configuration to avoid defining each session from scratch. The default session is used when connecting via Quick Connect or the browser. The 'Default' session is included in the session list. Default can be moved anywhere in the session list, but must always be present.

The easiest way to configure rows and columns is often to drag the CRT window until the size matches the terminal output. These row and column settings will be saved in Session Preferences.

Global Preferences Dialog

The global preferences dialog includes three tabs: [Options](#), [ANSI Color](#), and [Firewall](#).

Global Preferences, ANSI Color

ANSI Color supports sixteen colors. Eight of these are for normal colors and eight are for bold colors. To change a color, click on the color and select the new color. To change all of the colors in either of the Normal or Bold color categories to their default colors, click on the **Default** button in the respective category.

Global Preferences, Firewall

The **Firewall** dialog allows you to configure CRT to use either a SOCKS firewall or a generic proxy.

To configure the SOCKS firewall, select the appropriate SOCKS version for your firewall and specify the hostname and port (usually 1080) of your SOCKS firewall. SOCKS version 4 and SOCKS version 5 (without authentication) are currently supported.

To configure CRT to use a generic proxy, you must specify the proxy host and port, the proxy prompt, and the connect or open command.

For example, for the TIS Firewall toolkit, the prompt would be

```
tn-gw>
```

and the command would be:

```
c %h %p\r
```

For WinGate, the prompt would be

```
WinGate>
```

and the command would be:

```
%h %p\r\n
```

To enable a session to work with a firewall, you must also choose Connect via firewall from the [Session Tab](#) for that session.



SecureCRT's SSH protocol imposes some special constraints on what firewall software can be used. SSH does work with SOCKS firewalls. SSH does **not** work with generic firewalls that return information after the "connect" command is sent.

SecureCRT allows you to connect through the `plug-gw` proxy. To connect through the TIS `plug-gw`:

- 1 Set the **Firewall** type to **Generic proxy**.
- 2 Set the **Hostname** and **Port** fields to the firewall hostname and port values.
- 3 Leave the **Prompt** field blank.
- 4 Set the **Command** field to

```
CONNECT %h:%p HTTP/1.0\r\n\r\n
```

Any session which uses the `plug-gw` proxy must select the **Connect via firewall** option in the **Session** tab of the **Session Preferences** dialog.

Global Preferences, Options

The ten global options are:

[Copy on select](#)

[Paste on middle button](#)

[Connection closed dialog](#)

[Confirm disconnect dialog](#)

[Hide mouse pointer on keypress](#)

[Disable resize](#)

[Highlight most recent session](#)

[Asynchronous name lookup](#)

[Save window state for each session](#)

[Enable execute escape sequence](#)

Horizontal Scroll Bar

Turns on the horizontal scroll bar.

Note: If the window is maximized, you must first restore the CRT window before selecting this option. After selecting this option, the CRT window can be maximized again.

Host Key



The host key is a unique identifier associated with an SSH server. **Note:** host keys are only used by SecureCRT when making connections using the Secure Shell (SSH) Protocol.

Host keys are used to help verify the identity of an SSH server, and in general an SSH server's host key value should not change. Every SSH server sends its host key each time a connection is initiated. SecureCRT detects this key and checks to see whether a host key for the server has previously been saved. If a previously saved host key does not match a newly received key from the same SSH server then SecureCRT displays a dialog warning of the conflict between the key values. A host key conflict may indicate a security problem with the SSH server.

If no previously saved key is found for an SSH server, SecureCRT displays a dialog stating that the newly detected host key has not been registered. If a new host key or a host key conflict is detected the following choices are available:

Cancel - the host key is not accepted and the connection to the SSH server is closed.

Accept Once - the host key from the server is accepted without being saved.

Accept & Save - accept the host key and save it. The host key detected in future connections to the same SSH server will be compared with the saved key.

Installing CRT and SecureCRT

The downloadable CRT and SecureCRT files are executable files that start a Windows Setup program.

When installing a new version of CRT or SecureCRT on a PC which already has the software installed, always install into the existing directory or folder. This preserves any saved preferences as well as your license data.

For users of 2.0 and older versions, the license data entry has been moved from the entry screen to the **Enter License Data** command on the Help Menu.

After installing, new users of CRT may want to review the **Introduction** and **How To** topics [Getting Started - Telnet with CRT](#), and [How To Automate CRT Startup](#). SecureCRT new users may want to see [Getting Started - SSH and SecureCRT](#) and [How to Set up RSA Authentication](#).

Keymap - Menu Functions

Menu Functions enable mapping CRT commands to a key.

Example: map **Copy & Paste** command (MENU_COPY_PASTE) to a function key not used by the telnet application.

MENU_NEW_WINDOW	MENU_COPY	MENU_SAVE_SETTINGS_NOW
MENU_CONNECT	MENU_PASTE	MENU_WINDOW_NEXT
MENU_QUICK_CONNECT	MENU_COPY_PASTE	MENU_WINDOW_1
MENU_PRINT_AUTO	MENU_SELECT_ALL	MENU_WINDOW_2
MENU_PRINT_SCREEN	MENU_FIND	MENU_WINDOW_3
MENU_PRINT_SELECTION	MENU_CLEAR_SCREEN	MENU_WINDOW_4
MENU_LOG_SESSION	MENU_CLEAR_SCROLLBACK	MENU_WINDOW_5
MENU_RECENT_1	MENU_RESET	MENU_WINDOW_6
MENU_RECENT_2	MENU_TOGGLE_MENU_BAR	MENU_WINDOW_7
MENU_RECENT_3	MENU_TOGGLE_TOOLBAR	MENU_WINDOW_8
MENU_RECENT_4	MENU_TOGGLE_STATUS_BAR	MENU_WINDOW_9
MENU_EXIT	MENU_TOGGLE_CHAT_WINDOW	MENU_WINDOW_0

Keymap - Scrollbar Functions

Scrollbar Functions allow controlling the behavior of the CRT terminal session scroll bars.

SB_LINE_UP	SB_END
SB_LINE_DOWN	SB_COLUMN_LEFT
SB_PAGE_UP	SB_COLUMN_RIGHT
SB_PAGE_DOWN	SB_PAGE_LEFT
SB_BEGIN	SB_PAGE_RIGHT

Keymap - Telnet Functions

Telnet Functions control the interruption of the telnet session.

TN_BREAK

TN_INTERRUPT_PROCESS

TN_ABORT_OUTPUT

TN_ARE_YOU_THERE

TN_SYNCH

Keymap - VT Functions

VT Functions allow controlling the terminal emulator's keys.-

VT_PF1	VT_KEYPAD_PERIOD	VT_F13
VT_PF2	VT_KEYPAD_ENTER	VT_F14
VT_PF3	VT_CURSOR_UP	VT_F15 (HELP)
VT_PF4	VT_CURSOR_DOWN	VT_F16 (DO)
VT_KEYPAD_0	VT_CURSOR_LEFT	VT_F17
VT_KEYPAD_1	VT_CURSOR_RIGHT	VT_F18
VT_KEYPAD_2	VT_HOLD_SCREEN	VT_F19
VT_KEYPAD_3	VT_PRINT_SCREEN	VT_F20
VT_KEYPAD_4	VT_AUTO_PRINT	VT_FIND
VT_KEYPAD_5	VT_F6	VT_INSERT_HERE
VT_KEYPAD_6	VT_F7	VT_REMOVE
VT_KEYPAD_7	VT_F8	VT_SELECT
VT_KEYPAD_8	VT_F9	VT_PREV_SCREEN
VT_KEYPAD_9	VT_F10	VT_NEXT_SCREEN
VT_KEYPAD_MINUS	VT_F11	
VT_KEYPAD_COMMA	VT_F12	

Keymap Editor

The Keymap Editor allows you to edit [custom keymaps](#). A [custom keymap](#) supports the mapping of almost all keys on the keyboard to a string, [menu function](#), [scrollbar function](#), [telnet function](#), or [VT function](#).

Choose the key that you would like to map in the keyboard section of the dialog. Then, click on the **Map Selected Key** button to map the key. From the **Map Selected Key** dialog, you can choose a general grouping of functions from the Function drop down list. If you choose anything but "Send String" or "Run Script", you will be able to choose the exact function from the drop down list to the right. If you choose Send String, type the string in the edit box to the right of the Function drop down list. If you choose Run Script, enter the path of the script file to be run in the edit box or click the "..." button to browse for the location of the script file. Finally, click the OK button to save the current mapping. Click the **Default** button to reset the key to its **default mapping**.

The **Map Next Key** button will allow you to change the mapping for a key sequence that is entered directly from the keyboard. For example, press the **Map Next Key** button and typing the key sequence Shift+A. will bring up the **Map Selected Key** dialog showing the current mapping for Shift+A. You can then modify the mapping or click Cancel to void any changes made.

The **Save** button will save the keymap at any time.

The **Save As** button will save the keymap that is currently being modified to a specified file.

The **Load** button will load a new keymap.

The **Close** button will exit out of the Keymap Editor. If modifications have not been saved, a dialog is presented asking whether to save the changes or discard them.

Octal values of the [ASCII Control Codes](#) are important for mapping control characters.

License Registration

The following information is for individual licenses. For information on quantity pricing and site licenses, please send e-mail to sales@vandyke.com or see <http://www.vandyke.com>.

Upon receipt of payment we will send you one license key for each copy of CRT paid for. The new license key(s) will have no expiration. The license(s) key will be sent to you via e-mail or postal mail. **Note, no disk will be sent.** All updates to the software will be made available via anonymous ftp.

Four payment methods are available:

Ordering online:

To order online with MasterCard, Visa, American Express, or Discover, visit:

<http://www.vandyke.com/order/online.html>

Ordering by check:

To order by check, fill out and send either the [CRT order form \(click here\)](#) or the [SecureCRT order form \(click here\)](#) and a check to:

Van Dyke Technologies, Inc.
P.O. Box 37457
Albuquerque, NM 87176
USA

Ordering by Credit Card:

The numbers below are for credit card orders only.

The authors of CRT and SecureCRT cannot be reached at these numbers.

Any questions about the status of the shipment of the order, refunds, registration options, product details, technical support, volume discounts, dealer pricing, site licenses, non-credit card orders, etc., must be directed to Van Dyke Technologies, P.O. Box 37457, Albuquerque, NM 87176, USA or sales@vandyke.com.

You can order with MasterCard, Visa, Amex, or Discover from Public (software) Library:

PsL's product number for either version of CRT is **14206**.

PsL's product number for SecureCRT is **15600**.

Phone: 800-242-4775 or 713-524-6394 (extension 14206 for CRT orders,
extension 15600 for SecureCRT orders)

FAX: 713-524-6398

CIS Email: 71355,470

Internet CRT orders: 14206@pslweb.com

Internet SecureCRT orders: 15600@pslweb.com

U.S. Mail: PsL, P.O. Box 35705, Houston, TX 77235-5705

PsL is open from 8:30am-5pm CST Monday - Friday (except holidays).

PsL will notify us the day of your order and we will send you the license key(s) directly.

Log Session

Selecting this command toggles whether the current session is logged to a file. By default, logging is off.

If you turn logging on, you will be prompted for a filename. The default filename may be specified via the [Files tab](#) of the [Session Preferences Dialog](#).

Login Script Files

Login scripts are managed in the **Scripts** Tab of the **Session Preferences** dialog. Use the Dialog option for simple login procedures using fields like login ID and password. Scripting of conditional statements, timing, and prompts requires file-based scripting.

If the 'File' option is checked, use the associated edit box to enter the login script filename.

If both Dialog Login Script and File Login Script are checked, the Dialog Login Script will be executed followed by the File Login Script.

For information on the scripting language, see [Scripting Language](#). Four sample scripts are installed with CRT. They are located in the \scripts directory. login4.csf is a sample script that demonstrates all of the functions currently available in the scripting language.

By default, File Login Script is not selected.

Medium Toolbar

Selects medium-sized buttons for the Toolbar.

Menu Bar

Hides the CRT menu bar.

If the menu bar is hidden, select **Toggle Menu Bar** from the CRT System menu to display the menu bar. The System menu is located at the left end of the CRT title bar.

New Window

Opens another CRT Window.

Open Session File

CRT stores a set of named sessions in the session file. Under most circumstances, a user will use only one session file. This command allows the user to change the current session file.

This command is not available when you are connected.

Other Support Issues

We are very interested in hearing from our users. If you have a general question about CRT, send e-mail to:

`crt-questions@vandyke.com`

If you have a feature that you would like to see added to CRT, then send e-mail to:

`crt-features@vandyke.com`

For the latest information on CRT and Van Dyke Technologies, Inc., check out our home page:

`http://www.vandyke.com`

To receive announcements of new versions of CRT via e-mail, send e-mail to:

`crt-announce-request@vandyke.com`



To receive announcements of new versions of SecureCRT via e-mail, send e-mail to:

`SecureCRT-announce-request@vandyke.com`

If **Answerback** is selected, the specified string is sent in response to the remote host sending the answerback command (Ctrl+E).
By default, **Answerback** is not selected.

If **Display tab as** is selected, the text in the associated edit field is displayed whenever a tab from the remote host is received. By default, **Display tab as** is not selected.

If **Enable 80/132 column switching** is selected, CRT will resize the window when the VT escape 80/132 column mode escape sequence is received.

By default, **Enable 80/132 column switching** is selected.

If **Enable cursor key mode switching** is not selected, CRT will ignore the VT escape sequence which changes the cursor key mode.

By default, **Enable cursor key mode switching** is selected.

If **Enable keypad mode switching** is not selected, CRT will ignore the VT escape sequence which changes the keypad mode.
By default, **Enable keypad mode switching** is selected.

If **Enable line wrap mode switching** is not selected, CRT will ignore the VT escape sequence which changes the line wrap mode.
By default, **Enable line wrap mode switching** is selected.

Force **Local echo** of user input. By default, **Local echo** is not selected.

If **SCO line wrap** is selected, SCO ANSI line wrap is emulated. By default, **SCO line wrap** is not selected. This option should be cleared when connecting to SCO UNIX.

If SGR escape sequence is received with an argument of zero, ANSI color is reset. By default, **SGR zero resets ANSI color** is selected. This option should be cleared when connecting to SCO UNIX.

Selecting this option causes the high-order bit of each byte received from the remote host to be ignored.

If **Terminal type** is selected, instead of sending the emulation (VT100, VT220, or ANSI) as the terminal type, the specified string is sent.

By default, **Terminal type** is not selected.

If **Disable pass through printing** is selected, all pass through printing commands are ignored.
By default, **Disable pass through printing** is not selected.

Specifies the anti-idle string that is sent when a **time out** value other than 0 is set.

A non-zero **time out** specifies the interval in seconds to wait between sending the anti-idle string.
The default value is 0 which disables the **time out** string.

If **Initial position** is selected, CRT will be started with its upper left corner at the specified x,y location. This option is only used when CRT is started with the `/S session_name` option.

By default, **Initial position** is not selected.

If **Direct pass through printing to port** is selected, when the pass through escape sequence is received, the characters received are not interpreted and sent directly to the selected printer port.

By default, **Direct pass through printing to port** is not selected.

If **Title bar** is selected, you may specify the text that appears in the title bar.

By default, **Title bar** is not selected and the session name is displayed in the title bar.

If **Use raw mode** is selected, all printer data is sent directly to the printer.
By default, **Use raw mode** is selected.

If **Use raw mode** is selected, all printer data is sent directly to the printer.
By default, **Use raw mode** is not selected.

Specify the characters that are used as word delimiters.

Selecting this option forces CRT to be in "character at a time" telnet mode. Required in rare cases where telnet negotiation between the client and server does not occur correctly.

Warning: For most users, this option should be not be selected.

If **Send SGA** is selected, CRT will send Telnet sites the `DO SGA` command immediately after connecting. Most Telnet sites expect this command to be sent when a Telnet client connects.

By default, **Send SGA** is selected.

Selecting this option initiates telnet negotiation by sending the telnet SGA command. Most telnet servers expect this from the telnet client.

Warning: For most users, this option should be selected.

If **Will LFLOW** is selected, CRT will enable local flow control when connecting to Telnet sites that support LFLOW.
By default, **Will LFLOW** is selected.

Invoke the **RSA Key generation wizard** to generate a new identity file.

Use Global uses the named identity file for all SSH sessions **except** those with a defined **session-specific** file.

Session-specific defines an identity file to be used for the current session.

Current shows the current list of forwarded ports.

Delete removes the highlighted port from the **Current** list of forwarded ports.

Forward X11 Packets enables X11 clients to connect to the local X server if the server is running. This option causes the DISPLAY environment variable to be set when the SecureCRT session successfully connects to the remote host.

The **port number** of the local port to be forwarded.

Clears the **Local Port** and **Remote Port** fields, and fills in the **Remote Hostname** with the hostname of the current session.

The hostname or IP address of the remote host.

The **Remote Port** number that the **Local Port** is to be forwarded to. Defaults to the same port number entered for the local port.

Saves the contents of the **Local Port**, **Remote Hostname** and **Remote Port** fields to the forwarded ports list.

Use single SSH connection directs all SSH traffic through one connection instead of multiple connections. This option is selected by default.

Use compression applies a variable compression algorithm to the SSH data stream to increase performance for slow connections.

Close the dialog.

Create a copy of the selected session.

Delete the selected session.

Move the selected session **down** one position in the session list.

Edit the the selected session.

Create a **new** session with factory default settings.

Connect to selected host.

The **session list** consists of the Default session and zero or more named sessions.

The Default session is a template for creating new sessions. Named sessions can also be created with New and Clone.

If **Show dialog at startup** is on, this dialog will displayed when CRT is started.

Move the selected session **up** one position in the session list.

Network connection where data stream is encrypted.

The label assigned to a terminal session in the name field of the **Session List - New** dialog.
The available session names appear in the **Session List** on the **Connect** dialog.

Connection where security precautions have been taken to prevent unauthorized access.

Usually a trusted connection exists within a private network



Trusted connections on the Internet require encryption with the Secure Shell protocol and SecureCRT.
Note that SecureCRT's telnet sessions are not secure.

Authentication means verifying that you are the person you claim to be. Usually done when first logging onto a server or network. Passwords are the most common means of authentication. SecureCRT's strongest authentication method uses RSA public-private key pairs.

An encryption method (technically a mathematical algorithm) that is used to encode information between client and server. Used to encrypt passwords or data sent between SecureCRT and the SSH server.

Computer that provides telnet or rlogin services to terminals
A host can be on a local or wide-area network, or on the Internet.

Identity files are two files containing the public-private key pair used to connect to an SSH server using **RSA authentication**. **Identity** contains the public and private key pair and is used by SecureCRT. **Identity.pub** contains only the public key and is for appending to the `authorized_keys` file.

An **insertion attack** is an attempt to gain access to an SSH session by inserting packets into the encrypted data stream.

Ports identified in a local Windows system file that maps ports to service names and named aliases. Allows you to refer to a port in SecureCRT by the service name or alias without using the port number.

Example: Enter 'smtp' in **Local** or **Remote Port** field instead of '25'.

Using a local port to connect to a remote host using **SSH** to secure the connection.

This method can be used for telnet, SMTP, POP and IMAP protocols.

Example: **Port forwarding** allows reading mail on an IMAP server with an encrypted data channel.

Display a blinking cursor. This is selected by default.

Define, edit or delete a **color scheme**.

Select an existing **color scheme** for a terminal session.

Choose a color for the cursor.

By default, this option is not selected.

Choose a cursor style of type **block**, **short block**, **underline** or **vertical bar**. The default cursor style is **block**.

If a **narrow font** is selected then it will be used if CRT switches to 132 column mode.

The **normal font** is displayed by CRT in 80-column mode.

If **Up** is selected, CRT will search from the current selection or cursor position back through the scrollbar. If **Down** is selected, the search will be from the current selection to the bottom of the scrollbar.

Enter the text that you would like to search for in the scrollbar.

If **Match whole word only** is selected, CRT will search for the string, specified in the [Find what](#) edit box. A match will be found only if the string found is the same string surrounded by space, tab, carriage return or a line feed.

By default, **Match whole word only** is not selected.

Displays the **Advanced Emulation Options** dialog with mode, mode switching and other options.

If **ANSI Color** is checked, CRT will recognize ANSI color sequences sent by the remote host.

Number of **Columns** displayed in the terminal window.
The default value is 80.

If **Cursor key mode** is selected, the arrow keys send application sequences to the remote host.

If **Cursor key mode** is not selected, the arrow keys send ANSI cursor sequences to the remote host.

By default **Cursor key mode** is not selected.

Terminal **emulations** supported by CRT.

Select the keymap to use: Default, VT100, VT220, or Custom.

Select the custom keymap file to use.

If **Numeric keypad** option is selected, the numeric keypad sends the characters shown on each key to the remote host.

If **Application keypad** option is selected, the numeric keypad sends application sequences to the remote host.

By default, the **Numeric keypad** option is selected.

If **Line wrap** is selected, lines longer than the current display are wrapped to the next line.
By default **Line wrap** is selected.

If **New line mode** is selected, LF's, FF's, and VT's move the terminal cursor to the first column of the next line; and when the enter key is pressed, both a CR and LF are sent.
By default **New line mode** is not selected.

Number of **Rows** displayed in the terminal window.
By default, this is 24.

Number of rows in the **Scrollback** buffer.
The default value is 500.

If **Synchronize viewable columns** is selected, the viewable columns will be kept in sync with the number of logical columns.

With this option on, the number of logical columns will change whenever the number of viewable columns changes, and visa versa. If the number of logical columns is greater than can be displayed, the horizontal scroll bar can be turned on from the view menu to access the additional logical columns.

With this option off, the number of logical columns is independent of the number of viewable columns. When the window is resized, the logical number of columns is unaffected. Correspondingly, when the number of columns specified on the emulation tab of the preferences dialog is changed, the number of viewable columns is unaffected.

By default, **Synchronize viewable columns** is selected.

If **Synchronize viewable rows** is selected, the viewable rows will be kept in sync with the number of logical rows.

With this option on, the number of logical rows will change whenever the number of viewable columns changes, and visa versa. If the number of logical rows is greater than can be displayed, the horizontal scroll bar can be turned on from the view menu to access the additional logical columns.

With this option off, the number of logical rows is independent of the number of viewable rows. When the window is resized, the logical number of columns is unaffected. Correspondingly, when the number of columns specified on the emulation tab of the preferences dialog is changed, the number of viewable columns is unaffected.

By default, **Synchronize viewable rows** is selected.

If **Disable ZModem** is on, CRT will ignore the character sequence that starts ZModem transfers.

Specify the filename for session log files.

If **Truncate file** is on and the session log file already exists, the file will be truncated.

If **Append to file** is on and the session log file already exists, the new session log will be appended to the existing file.

Otherwise, a new file is created.

If **Prompt for filename** is on, the user is prompted for the session log filename when the log is started.

If **Raw log** is selected, every character received by CRT including terminal escape sequences will be written to the session file.
By default, **Raw log** is selected.

Specify the directory for files being downloaded via ZModem.

If **Start Log Upon Connect** is selected, then Log will be started whenever a connection is made.
By default, **Start Log Upon Connect** is not selected.

Specify the initial directory displayed in the ZModem upload list dialog.

The firewall server's hostname or IP address.

Port used by firewall software. For SOCKS 4 and 5 the default port is 1080

Choose the firewall type.

If **Asynchronous name lookup** is selected, resolution are done asynchronously. If your Winsock supports this option, CRT will be able to respond to menu commands, paint messages, etc. when a connection is being initiated.

By default, **Asynchronous name lookup** is selected.

If **Confirm disconnect dialog** is selected, a dialog is displayed when **Disconnect** is selected from the menu or toolbar.
By default, **Confirm disconnect dialog** is selected.

If **Connection closed dialog** is selected, a dialog is displayed when the connection is closed by the remote host or when the connection is aborted.

By default, **Connection closed dialog** is selected.

If **Copy on select** is selected, selections are copied to the Clipboard automatically.
By default, **Copy on select** is not selected.

If **Disable resize** is selected, the window cannot be resized by the resize frame. In addition, maximize is disabled.
By default, **Disable resize** is selected.

With the option selected, **Enable Execute Escape Sequence** allows the remote system to execute commands on the local computer. Unless this support is required, it should not be selected.

If **Hide mouse pointer on keypress** is selected, the mouse pointer is hidden while the user types. The mouse pointer is shown again when the mouse is moved.

By default, **Hide mouse pointer on keypress** is selected.

If **Highlight most recent session** is selected, the most recently used session in the **Connect** dialog is highlighted.
By default, **Highlight most recent session** is selected.

If **Paste on middle button** is selected, clicking the middle mouse button sends the current contents of the Clipboard to the remote host as if it had been typed.

By default, **Paste on middle button** is not selected.

Saves the position, size and state of the CRT window for each session separately.
By default, **Save window state for each session** is not selected.

Displays the **Advanced Telnet Options** dialog with options for telnet sessions.

Select the **Baud rate** for the device. The default value is 38400.

Causes the session to connect using the current firewall settings.

Select this option to use the **DTR/DSR** (data-terminal-ready/data-set-ready) signals with the connected device. By default, this is not selected.

The number of communication **Data bits**. The default value is 8.

The **Hostname** or **IP** address of the remote host.

Load session settings from a built-in profile.

Specifies the **Name** of the session as it will appear in the **session list**.

Choose the **Parity** setting supported by the connected device. The default setting is **None**.

The **port** number of a service on a remote server. For telnet the default **port** number is 23. For SSH the default **port** number is 22.

Specifies the **Protocol** for connecting to remote systems. The following choices may be available: **telnet**, **rlogin**, **serial** and **SSH**. The **serial** protocol is available only if selected when CRT was installed. By default, the protocol is Telnet.



SSH is only available in SecureCRT.

Use **RTS/CTS** (request-to-send/clear-to-send) hardware flow control. By default, this option is selected.

Choose **Identity File** and **Port Forwarding** options.

Port Forwarding allows a local port to be forwarded to a remote server with RSA encryption.

Identity Filename supports selecting global or session-specific identity files to provide RSA public key encryption.



SecureCRT supports three types of authentication for connecting to SSH servers: **Password**, **RSA**, and **TIS**. With **Password** authentication the user's password is encrypted and sent to the server. **RSA** authentication uses public/private key encryption to authenticate the connection. **TIS** authentication uses the TIS firewall server to provide a challenge phrase / response combination. SSH servers must be configured to offer TIS authentication. The first time you use **RSA** authentication, SecureCRT will prompt you for the location of your identity file (which contains your private key) upon making the connection. **Password** authentication is the default.

Change Passphrase allows you to change the authentication passphrase for your identity file.



The **cipher** is the encryption algorithm that is used to encrypt the data channel for the session. The **cipher** selected must also be supported by the destination SSH server. An error will be reported upon connection if the chosen **cipher** is not supported by the server. The default **cipher** is **3DES**. Note: setting **cipher** to **None** causes the session to be unencrypted and offers no security. Some SSH servers reject the use of password authentication if the cipher is set to **None**.

The **password** used to login to the SSH server. The **password** field is only enabled if **Password authentication** is selected.

The serial **port** (COM1, COM2, etc.) used by the session.

The number of **stop bits** sent after each character. The default value is 1.

The **Alternates** button allows defining and choosing from a list of phone numbers.

Move successful number to top automatically places the last successful number at the top of the **Alternates** list. The default is **off**.

New Phone Number enables adding phone numbers to the phone number list, and changing existing phone numbers.

The **phone numbers** list shows the set of numbers available to choose from. The list can be sorted and edited using the **Up**, **Down**, and **Delete** buttons.

Area code specifies the national area code number.

Configure brings up a standard modem configuration dialog.

Country code specifies the international code by country (if needed).

Dial using specifies which modem will be used.

Phone number specifies the number to be dialed for the TAPI connection.

Auto Redial allows selecting the number of redial attempts and the timeout period between redial attempts.

Redial Attempts is the number of times CRT will try redialing the numbers in the phone number list. The range of valid values is 0 to 999.

Redial Seconds is the number of seconds the dialer pauses after processing the numbers in the dialing list.

The **username** used to connect to the remote host.

Use **XON/XOFF** software flow control. By default, this option is not selected.

Select the function key to program.

Enter the text for the function key to send.

When the **Map Next Key** button is pressed, the **Map Next Key** dialog will appear. Enter the key sequence to be mapped.

If a key on the keyboard portion of the dialog is selected; **Map Selected Key** will display a dialog to choose a mapping for the selected key.

TBD

If **Audio bell** is selected, the system default sound is sounded.
By default, **Audio bell** is selected.

If **Blinking cursor** is selected, the terminal cursor will blink.
By default, **Blinking cursor** is selected.

If **Clear on disconnect** is selected, the CRT window will be cleared when the remote connection is disconnected.
By default, **Clear on disconnect** is not selected.

If **Close on disconnect** is selected, the CRT window will be closed when the remote connection is disconnected.
By default, **Close on disconnect** is not selected.

If **CUA copy and paste** is selected, Ctrl+C, Ctrl+V, Ctrl+A, and Ctrl+F are accelerators for Edit/Copy, Edit/Paste, Edit/Select All, and Edit/Find, respectively.

Warning: If the remote system uses Ctrl+C, Ctrl+V, Ctrl+A and Ctrl+F, do not use this option. For most UNIX and VMS systems, this option should not be selected.

Selects emacs mode. If **Alt sends escape** is selected, `Alt+<key>` sends `<esc><key>`
By default, **Alt sends escape** is not selected.

If **Jump scroll** is selected, text is scrolled multiple lines at a time when more than a screenful of text is received.
By default, **Jump scroll** is selected.

If **Backspace sends delete** is selected, the delete character is sent when the backspace key is pressed.
By default, **Backspace sends delete** is not selected.

If **Delete sends backspace** is selected, the backspace character is sent when the delete key is pressed.
By default, **Delete sends backspace** is not selected.

AltGr and Alt+Ctrl are equivalent. Therefore, in emacs mode, users with international keyboards that require the use of AltGr should select this option.

If **Scroll to bottom on keypress** is selected, CRT automatically repositions the screen to the bottom of the scrolling region when keyboard input is received.

By default, **Scroll to bottom on keypress** is selected.

If **Scroll to bottom on output** is selected, CRT automatically repositions the screen to the bottom of the scrolling region when output is received.

By default, **Scroll to bottom on output** is selected.

If **Scroll to clear screen** is selected, the current screen is saved in the scroll buffer prior to processing the clear screen operation.
By default, **Scroll to clear screen** is selected.

If **Visual bell** is selected, the screen is momentarily switched to reverse video.
By default, **Visual bell** is not selected.

If **Dialog login script** is selected, the login script specified by the **Details** dialog is used to automate the login process.
By default, **Dialog login script** is not selected.

If **File Login Script** is selected, enter the filename of the login script to automate the login process in the associated edit box. If both **Dialog Login Script** and **File Login Script** are selected, then the **Dialog Login Script** will be executed and the **File Login Script** will not be executed.

By default, **File Login Script** is not selected.

localhost is the name used by a TCP/IP packet for the same computer where the message originated. The localhost IP address is 127.0.0.1.

Page Setup

Displays the **Page Setup** dialog to adjust the printer margins and printer font.

Paste

Sends the current contents of the Clipboard to the remote host as if it had been typed.

This operation is also available via the right mouse button.

This command is not available if the Clipboard is empty.

Paste as Quotation

Sends the current contents of the Clipboard to the remote host as if it had been typed. Each line sent will be preceded by the string ">".

This operation is also available via the right mouse button.

This command is not available if the Clipboard is empty.

Port Forwarding Security



Security Considerations

It is important to understand that the client data is only encrypted between the machine that SecureCRT is running on and the SSH server that SecureCRT is connected to. Any data moving from the SSH server across the network to another server is **not** encrypted.

Two configurations are presented below to illustrate different machine/network configurations and their effect on security. Your evaluation of the connection between Servers A and B is the critical factor in deciding whether the aggregate security meets your needs.

Configuration 1

SecureCRT forwards POP3 mail to a remote mail server which is a different machine than the SSH server.



- Between the Windows PC and Server A the data is encrypted.
- Between Server A and Server B the data is not encrypted.
- Since the SSH server and mail server are on different machines your data can be viewed on this connection.

In Configuration 1, the connection between Servers A and B could be:

- on the Internet - an unsecure network.
- on an internal LAN - a network which may or may not deliver a satisfactory level of security.

Configuration 2

SecureCRT forwards POP3 mail to a remote mail server which is running on the same machine as the SSH server.



Between the Windows PC and Server A the data is encrypted.



Since there is no network traffic between the SSH server and Mail server, security is increased over Configuration 1.

Port Forwarding in SecureCRT



Port forwarding is a powerful tool that allows you to secure TCP/IP traffic using SecureCRT's SSH protocol support. This means that you can encrypt application data using protocols such as IMAP, POP3 and SMTP. For example, if you receive your e-mail from an Internet Service Provider (ISP), you could encrypt the communication between your workstation running the email client and the ISP's SSH server. SecureCRT also supports X11 forwarding, which allows X Windows traffic between the X server and X client to be encrypted.

Port forwarding works by forwarding data from a local port to the remote host/port. For example, to secure POP3 traffic through your mail client, set up **port forwarding** with the

- local port=110
- remote hostname set to the mail server's hostname
- remote port=110.

Configure the mail client to use 127.0.0.1 as the POP3 server's IP address.

Hostname and port configuration needs to be done in both SecureCRT and the client application (e.g., e-mail). After connecting with this session, POP3 traffic is encrypted to the SSH server as long as SecureCRT is running. If the connection to the ssh server is broken or closed, the forwarded ports will no longer be forwarded, and the client applications may receive an error when they try to connect to the local port.

In general, with any port forwarded by SecureCRT for an application, the application needs to be reconfigured to use the localhost or loopback address 127.0.0.1 as its application server address.

To set up port forwarding, follow these steps:

- 1 Click on **File / Connect** and select the SSH session for which you would like to use forwarded ports.
- 2 Click on the **Edit** button to bring up the **Session Preferences** dialog and click on the **Advanced** button on the **Session** tab. Select the **Port Forwarding** tab.
- 3 To add a new forwarded port, click on **New**, fill in the local port, remote hostname and remote port, then click **Save**.
Note that after you enter the local port and hit the Tab key, the remote hostname and remote port are automatically filled in from the existing session information. Ports may be defined either by their port number or by their service name.
X11 Forwarding is configured in the same way, with the added step of selecting the **Forward X11 Packets** option.
- 4 Connect with this session to start port forwarding, then run the client application.

For X11 Forwarding, the local X Server must be running before the SecureCRT session is started.

If you are using Xhost authority access on the local X11 server, you will need to add the localhost or loopback address 127.0.0.1 to your server's Xhost list

There are important network factors in understanding Port Forwarding Security.

Print

The **Print** command consists of four sub menus:

Auto Print	Print each line as it is received
Screen	Print the current screen
Selection	Print the current selection
Cancel	Cancel Auto Print

Auto Print sends terminal output to the printer from a specified starting point to the point where **Auto Print** is canceled. **File, Auto Print** starts directing output to the printer. **Auto Print** is completed when **Auto Print** is cleared. The **Cancel** command terminates **Auto Print**. Selecting **Cancel** may send the print job to the printer.

Print Selection

Prints the text that is currently selected.

Print Setup

Displays the standard printer setup dialog.

Quick Connect

Connects to a remote server by selecting a protocol and supplying the protocol-specific information needed to make the connection (hostname, port, username, etc).

Quick Connect allows connections to be made without having a defined session. Each connection made using **Quick Connect** is saved as a session in the **session list** if the option **Save session** is selected. By default, this option is selected

By default, the **Quick Connect** dialog is displayed when CRT is started. To turn off this feature, clear the option **Show Quick Connect on startup** .

Receive ASCII

Toggles on and off saving all data from the remote host in a file of your choosing. Selecting **Receive ASCII** begins saving data and opens a file dialog to name and locate the file. Clearing **Receive ASCII** stops the flow of data to the file.

Reconnect

Reestablishes the previous connection. This option is not available until CRT has made and disconnected at least one session.

Reporting Problems

Please send e-mail regarding bug reports to crt-bugs@vandyke.com.

Please describe the problem in as much detail as possible. In your e-mail message, please include the following information:

- The version of CRT you are using (as shown in the About dialog box)

- The TCP/IP package and version

- The operating system and version

We try to respond to all bug reports within 2 business days.. In addition, we will try resolve the problem as quickly as possible.

Reset

Resets the terminal, including:

- Clears the scrollbar buffer
- Clears the screen
- Resets the emulator

Save Settings Now

Save the configuration settings now.

Script, Cancel

Cancels the currently executing script.

For information on creating and using scripts, see [Login Script Files](#) and [Scripting Language](#).

Script, Run

Selects a script to execute.

For information on creating and using scripts, see [Login Script Files](#) and [Scripting Language](#).

Scripting Language

Login script files are set up in the **Login** Tab of the **Session Preferences** dialog.

The CRT scripting language is used to create login and other script files. CRT's scripting language is a C-like language and includes the built-in functions listed below. Four sample CRT scripts are provided in the \scripts directory. login4.csf demonstrates the functions currently available in the scripting language.

Statement

```
statement;  
  
if ( expression ) {  
    statement;  
} else {  
    statement;  
}
```

identifier:

goto identifier;

Description

A statement is either an empty statement (;), or a call to an internal function followed by a semi-colon.

The expression must evaluate to TRUE or FALSE.

Example:

```
if ( ! expect( "ogin", 3 ) ) {  
    send("\r");  
    expect( "ogin" );  
}
```

Wait 3 seconds for the string "ogin". If it is not found, send a carriage return and wait forever for the string "ogin"

Declares identifier as a label. The only use of a label is as a target of the goto statement.

Control may be transferred unconditionally by means of the goto statement.

Operator

!

Description

logical negation operator

Function

```
Expect("string")  
Expect("string", n)  
  
Send("string")  
Prompt()  
  
Prompt("string", n)
```

ShowWindow(n)

```
MessageBox("string")  
Disconnect()  
CloseWindow()
```

Description

Wait forever until string is read from the remote host.

Wait until string is received from the remote host or until *n* seconds have passed. If the string is received, Expect returns TRUE.

Sends string to the remote host.

Displays a dialog with an edit box, an OK button and a Cancel button. When the user clicks OK, Prompt() returns the string contained in the edit box

Displays a dialog with an edit box, an OK button and a Cancel button, with *string* as the message. When the user clicks OK, Prompt() returns the string contained in the edit box. *n* can have the following values

0 - Allows the typed string to be displayed in the edit box

1 - Displays all typed characters as asterisks (*)

Where *n* is one of the following:

1 - Restore Window

2 - Minimize Window

3 - Maximize Window

Display a dialog with a message string and an OK button.

Disconnect the current session from the remote host.

Close the current CRT window.

Secure Shell (SSH) Protocol



The SSH protocol allows remote server connections using an encrypted data channel with support for password and RSA authentication. **The SSH protocol is only available in SecureCRT.**

Secure Communications

SSH provides secure communication over an insecure channel by encrypting the data channel using the cipher algorithm selected for the session by the user. The cipher selected must also be supported by the destination SSH server. An error will be reported upon connection if the chosen cipher is not supported by the server.

Note: setting cipher to None causes the data channel to be left unencrypted and offers no security. SecureCRT displays a 'key' icon on the Windows Taskbar and Alt+Tab panel when a cipher is being used, and a plain icon when data is unencrypted.

The default cipher is 3DES.

Authentication

SecureCRT supports three types of authentication for connecting to SSH servers: password, RSA, and TIS.

Password authentication transmits the user's password to the server to authenticate the connection. The transmitted password is protected from network eavesdropping, due to the cipher encryption of the data channel. For this reason, some SSH servers reject the use of password authentication if the cipher is set to "None".

RSA authentication - uses a public/private key pair to authenticate the connection. The general mechanism behind RSA authentication is that the RSA server "challenges" the client to decrypt a message encoded using the user's public key stored on the server.

Upon connecting, the RSA server generates a random value, encrypts the value using the user's public key and sends the encrypted challenge to the client. The client authenticates the connection by successfully decrypting the challenge using the user's private key.

The security of the mechanism requires that no one but the owner have access to the private key. The private key is stored locally in an identity file. The first time you connect to an SSH server using RSA authentication, SecureCRT will prompt you for the location of this file. Also, prior to using RSA authentication, the public key must be made available to the SSH server.

TIS Firewall authentication uses the TIS firewall server to provide a challenge phrase / response combination. SSH servers must be configured to offer TIS authentication.

See Setting Up RSA Authentication about generating identity files and other setup issues. Port forwarding is another feature based on SSH security.

SecureCRT License Agreement

End-User License Agreement for SecureCRT 2.4
Copyright (c) 1995-1999 Van Dyke Technologies, Inc.
All Rights Reserved.

AGREEMENT. After reading this agreement carefully, if you do not agree to all of the terms of this agreement, you may not use this software.

This software is owned by Van Dyke Technologies, Inc. and is protected by national copyright laws and international copyright treaties.

1. EXPORT LAW. This Software is subject to export control. The software cannot be transmitted, exported, or reexported without written consent of the Bureau of Export Administration, United States Department of Commerce.

2. GRANT OF LICENSE AND PROHIBITIONS. This software is licensed to you. You are not obtaining title to the software or any copyrights. You may not sublicense, rent, lease, convey, modify, translate, convert to another programming language, decompile, or disassemble the software for any purpose. The license may be transferred to another if you keep no copies of the software. Permission must be obtained before mirroring or redistributing the evaluation copies of the software.

3. USE AND EVALUATION PERIOD. You may use one copy of this software on one client computer. A copy of this software is considered in use when loaded into temporary memory (i.e., RAM) and/or installed on a permanent storage device (i.e., hard disk, CD-ROM, etc.). You may also use a copy of the software on a home or portable computer, provided only one copy of the software is in use at a time. You may use an evaluation copy of the software for only thirty (30) days in order to determine whether to purchase the software.

4. MULTI-COMPUTER/NETWORK LICENSES. If this is a multi-computer or network license, you may make, install, and use additional copies of this software up to the number of copies authorized in your registration documentation.

5. LIMITED WARRANTY. THE SOFTWARE IS PROVIDED AS IS AND VAN DYKE TECHNOLOGIES DISCLAIMS ALL WARRANTIES RELATING TO THIS SOFTWARE, WHETHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER VAN DYKE TECHNOLOGIES NOR ANYONE INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THIS SOFTWARE SHALL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH SOFTWARE EVEN IF VAN DYKE TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR CLAIMS. IN NO EVENT SHALL VAN DYKE TECHNOLOGIES' LIABILITY FOR ANY DAMAGES EXCEED THE PRICE PAID FOR THE LICENSE TO USE THE SOFTWARE, REGARDLESS OF THE FORM OF CLAIM. THE PERSON USING THE SOFTWARE BEARS ALL RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE.

6. TERMINATION. This agreement terminates, you lose all rights licensed to you, and you must stop use of the software if you a) violate the terms of this agreement or b) you do not pay the license fee before the end of the evaluation period.

7. GOVERNING LAW. The agreement shall be governed by the laws of the State of New Mexico. Any action or proceeding brought by either party against the other arising out of or related to this agreement shall be brought only in a state or federal court of competent jurisdiction located in Bernalillo County, New Mexico. The parties hereby consent to the personal jurisdiction of such courts.

8. U.S. GOVERNMENT RESTRICTED RIGHTS. This software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software--Restricted Rights clause at 48 CFR 52.227-19, as applicable. Manufacturer is:

Van Dyke Technologies, Inc.
P.O. Box 37457
Albuquerque, NM 87176
USA

e-mail: sales@vandyke.com

SecureCRT Order Form

The pricing below is valid through March 31, 1999. After March 31, 1999, please see <http://www.vandyke.com> for current pricing.

To print the order form, click on Print Topic in the File menu. Payments must be in **U.S. dollars** drawn on a **U.S. bank**.

Send this order form and a check to:

Van Dyke Technologies
P.O. Box 37457
Albuquerque, NM 87176
USA

SecureCRT 2.4 Order Form

This software is subject to export control. This software cannot be transmitted, exported, or reexported without written consent of the Bureau of Export Administration, United States Department of Commerce.

Please answer all questions.

[] **Yes** [] **No** Is the computer the software will be installed on located within the United States?

[] **Yes** [] **No** Do you acknowledge affirmatively that you understand that the requested software is subject to export controls under the Export Administration Act and that you cannot export or reexport the software without a license?

[] **Yes** [] **No** Do you certify that you are not on any of the United States Government's lists of export-precluded parties or otherwise ineligible to receive this transfer of cryptographic software subject to export controls under the Export Administration Act?

[] **Yes** [] **No** Do you warrant that you are not under the control of a foreign person of foreign government ?

I am: (please check one)

[] a United states citizen physically located in the United States; or

[] a Canadian citizen physically located in Canada or the United States; or

[] a person lawfully admitted to the United States for permanent residence, temporary residence under the legalization program, admitted as a refugee, or granted asylum under the Immigration & Naturalization Act, who is physically located in the United States; or

[] none of the above.

--- Please Print ---

1	Computer:	Computer License	@ \$99.00	=	_____
2 to 9	Computers:	_____ Computer Licenses	@ \$85.00 each	=	_____
10 to 24	Computers:	_____ Computer Licenses	@ \$70.00 each	=	_____
25 to 49	Computers:	_____ Computer Licenses	@ \$65.00 each	=	_____
50 to 99	Computers:	_____ Computer Licenses	@ \$57.50 each	=	_____
100 to 199	Computers:	_____ Computer Licenses	@ \$50.00 each	=	_____
200 to 499	Computers:	_____ Computer Licenses	@ \$42.50 each	=	_____
500 to 999	Computers:	_____ Computer Licenses	@ \$35.00 each	=	_____

Quantities over 999, please send email to: sales@vandyke.com

New Mexico Residents only add 5.8125% sales tax + _____
Total Payment _____



Payments must be in US dollars drawn on a US bank.



NT.

The above pricing is for any mix of Windows 98, Windows 95 or Windows



Prices are based on the number of computers on which the software is installed.



Prices are good through March 31, 1999.



Prices are in US Dollars.

--- Please Print ---

Signature: _

Name: _____ Date: _____

Company: _____

Shipping Address: _____

City, State, Zip: _____

Phone Number: _____

Country:

E-Mail Address:

Would you like to receive update announcements via e-mail?

How did you hear about SecureCRT?

Comments:

Select All

Selects all text that is visible as well as all text in the scrollbar.
This operation is also available via the right mouse button.

Send ASCII

Allows any file to be sent to the remote host as if it had been typed. Opens a file dialog to choose the file to be sent.

Session Preferences Dialog

This section describes the **Session Preferences** dialog. The dialog has eight tabs or sections.

Session

Emulation

Display

Options

F Keys

Files

Scripts

Advanced

Session Preferences, Advanced

From the last tab of the [Session Preferences Dialog](#), you may specify:

Advanced Options

[Title Bar](#)

[Initial Position](#)

[Word delimiter characters](#)

Anti-Idle

[Anti-Idle Time out](#)

[Anti-Idle Send](#)

The anti-idle string can contain one or more `\ooo` sequences, where `ooo` represents the octal representation of a character. Anti-idle strings follow the same rules as strings sent from a [Function Key](#).

For example, the following sequences can be used.

`\r` sends carriage return (CR)

`\n` sends linefeed (LF)

`\b` sends a backspace

`\e` sends an escape.

`\t` or `tab` pastes the current Clipboard contents into the active session window

`\p` pauses 1 second

Printing Options

[Disable pass through printing](#)

[Use raw mode](#)

[Direct pass through printing to port](#)

Session Preferences, Display

From the third tab of the [Session Preferences Dialog](#), you may specify display colors, fonts and cursor characteristics for a session. The available options are:

[Color scheme](#)

[Normal font](#)

[Narrow font](#)

[Cursor style](#)

[Cursor Color](#)

[Blinking Cursor](#)

Session Preferences, Emulation

From the second tab of the [Session Preferences Dialog](#), you can specify:

- The emulation,
- The number of rows and columns displayed in the terminal window,
- The number of rows saved in the scrollback buffer,
- Whether or not to [Synchronize Viewable Rows](#) and [Synchronize Viewable Columns](#), and
- The emulation modes.

You may specify either a built-in or [custom keymap](#). There are three built-in keymaps: Default, VT100, and VT220. When the VT100 Keymap is selected, the keypad will emulate the VT100 keypad. When The VT220 Keymap is selected, the VT220 keypad and VT220 function keys are emulated.

The easiest way to configure rows and columns is often to drag the CRT window until the size matches the terminal output. These row and column settings will be saved in Session Preferences.

The emulation modes are:

- [Cursor Key Mode](#)
- [Line Wrap](#)
- [New line mode](#)
- [Numeric or Application Keypad Mode](#)

The advanced emulation dialog includes the following options:

- [Enable 80/132 Column Switching](#)
- [Enable Cursor Key Mode Switching](#)
- [Enable Keypad Mode Switching](#)
- [Enable Line Wrap Mode Switching](#)
- [Local Echo](#)
- [Strip 8th Bit](#)
- [SGR Zero Resets ANSI Color](#)
- [SCO Line Wrap](#)
- [Terminal Type](#)
- [Answerback](#)
- [Display Tab As](#)

Session Preferences, F Keys

From the fifth tab of the Session Preferences Dialog, you can map Fn, Ctrl+Fn, Shift+Fn, and Alt+Fn to send an arbitrary string or issue one of a set of commands

The string to be sent can include \ooo, where ooo represents the octal representation of a character.

In addition, the following commands can be issued.

- \r sends carriage return (CR)

- \n sends linefeed (LF)

- \b sends a backspace

- \e sends an escape.

- \t or \t\b\v pastes the current Clipboard contents into the active session window

- \p pauses 1 second

Note that combinations like Ctrl+Shift+Fn are not supported.

Session Preferences, Files

From the sixth tab of the [Session Preferences Dialog](#), you can specify:

[ZModem upload directory](#)

[ZModem download directory](#)

[Disable ZModem option](#)

[Log filename](#)

[Prompt for filename option](#)

[Start log upon connect](#)

[Truncate/Append option for log file](#)

[Raw log](#)

Session Preferences, Options

From the fourth tab of the [Session Preferences Dialog](#), you can specify the following options:

[Backspace sends delete](#)

[Delete sends backspace](#)

[Audio bell](#)

[Visual bell](#)

[Close on disconnect](#)

[Clear on disconnect](#)

[Jump scroll](#)

[Scroll to clear screen](#)

[Scroll to bottom on output](#)

[Scroll to bottom on keypress](#)

[CUA Copy and Paste](#)

Emacs Modes

[Alt sends escape](#)

[Preserve Alt-Gr](#)

Session Preferences, Scripts

From the seventh tab of the [Session Preferences Dialog](#), you can specify details to automate the login process. There are two ways to supply the information for an automated login:

[Dialog](#)

[File](#)

The [File](#) option is explained further in [Login Script Files](#) and [Scripting Language](#).

Session Preferences, Session

The following options are available in the Session tab of the [Session Preferences Dialog](#):

[Name](#)

[Protocol](#)

[Load Profile](#)

The remainder of the session tab settings vary depending on the protocol selected:

Telnet protocol

[Hostname or IP](#)

[Port](#)

[Connect via firewall](#)

Advanced telnet options:

[Will LFLOW](#)

[Force character at a time mode](#)

[Send SGA \(port 23 only\)](#)

[Send SGA](#)

Rlogin protocol

[Hostname or IP](#)

[User name](#)

Serial protocol -

Note: The serial protocol is only available if selected when CRT is installed.

[Port](#)

[Baud rate](#)

[Data bits](#)

[Parity](#)

[Stop bits](#)

[DTR/DSR](#)

[RTS/CTS](#)

[XON/XOFF](#)

TAPI Protocol

[Dial using](#)

[Country code](#)

[Area code](#)

[Phone number](#)

TAPI Configuration options - This button brings up a Standard Windows Modem Properties dialog.

[Alternate phone number options](#)

[Add / Replace new phone number](#)

[Reorder phone numbers](#)

[Move successful number to top](#)

[Auto-redial options](#)

[Number of redial attempts](#)

[Seconds between redial attempts](#)



SSH protocol - Note: The SSH protocol is only available in SecureCRT.

[Advanced SSH Options](#)

[Hostname or IP](#)

[Port](#)

[Connect via firewall](#)

[User name](#)

[Cipher](#)

[Authentication](#)

[Password](#)

[Advanced](#)

Set Up RSA Authentication



RSA authentication uses a public-private key pair to authenticate and log in to an SSH Server. It offers a higher level of authentication security than **password authentication** by requiring both the private key and the passphrase that protects the private key to complete authentication.

Setting up RSA Authentication for a SecureCRT session is a multi-step process. Identity Files are created with the RSA Key Generation Wizard. The identity file is defined for global or session-specific use in the SSH Advanced Dialog. Then the public key is added to the SSH server's `authorized_keys` file.

- 1 In the **Connect** dialog, select an SSH session and click **Edit** (or create a session by clicking **New**).
- 2 Click the **Advanced** button on the **Session** tab and select **Create Identity File** on the **Identity Filename** Tab.
- 3 Follow the instructions in the RSA Key Generation Wizard to create your identity files. The identity filename will be inserted in the current **Use session-specific** or **Use global** field in the SSH Advanced Dialog.
- 4 Connect to the remote SSH server using SSH and password authentication.
- 5 Append the contents of the public key file created with the RSA Key Generation Wizard to the file `~/.ssh/authorized_keys` on the remote host. The default name of the public key file is `identity.pub`. Create the `~/.ssh/authorized_keys` file if it does not already exist. If you want multiple authorized keys, append the contents of the public key file to the `authorized_keys` file. The simplest way way to do this is typically

```
%cat identity.pub >> ~/.ssh/authorized_keys (note that the name of the identity file can be different than the example)
```

- 6 Now you can change the session to use **RSA authentication**. Disconnect from the remote server if you have not already done so. In the **Connect** dialog, select the SSH session and click **Edit**. Change the **Authentication** setting from **Password** to **RSA**. Click **OK** to save the changes and click **OK** again in the Connect dialog to open the connection. If you supplied a passphrase when you created your key, you will be prompted to enter it before you are connected.

Note on placing public keys: The format of the `authorized_keys` file requires that each entry consist of a single long line. If you use Copy and Paste to add a public key to the `~/.ssh/authorized_keys` file, make sure that the entry contains no additional newline characters.

Note on passphrases: SecureCRT can be set to remember passphrases as long as there is one instance of the application is running. This behavior is off by default, and is controlled by the Registry value **Save Passphrase In Shared Memory** in the key `HKEY_LOCAL_MACHINE / Software / Van Dyke Technologies / SecureCRT / SSH`

The option is turned on by using the Windows Regedit utility to change the value from a 0 to a 1. The option controls all instances of SecureCRT on the PC regardless of username or configuration.

Note on identity files: SecureCRT 2.3 made a change in the identity file format. Version 2.3 and later will read 2.2 identity files, but an identity file generated with 2.3 or later will not work with version 2.2.

Small Toolbar

Selects small-sized buttons for the Toolbar.

Start ZModem Upload

Send the ZModem **receive** command. This ZModem **receive** command is currently hard-wired to be `rz<CR>`. You can also start a ZModem upload by manually running the ZModem **receive** command on the remote machine.

Status Bar

Shows or hides the status bar.

When displayed, the status bar is below CRT's text window. Informational text, such as brief menu descriptions, is displayed in the status bar.

System Menu Options

The CRT system menu adds three options to the standard window size, move and close commands. It is found by clicking on the small CRT icon at the left end of the CRT title bar.

These commands are useful if you are running CRT as a bare terminal window without menus and toolbars.

Toggle Menu Bar turns the menu bar on or off depending on its current state.

Save Settings Now saves the configuration settings - works exactly as the **Save Settings Now** command on the **Options** menu.

Always on Top keeps the CRT window on top of other application windows whether it is active or not.

System Requirements

System Requirements for CRT:



Minimum of a 386 based machine with 8 megabytes of RAM.



Windows NT® - version 3.51 or greater.



Windows 98 or Windows 95.



Windows 3.1 - operating in enhanced mode with Win32s (version 1.30d or later).



Windows for Workgroups - operating in enhanced mode with Win32s (version 1.30d or later).



winsock.dll (compliant with version 1.1 of the Winsock standard).



TCP/IP stack. Under Windows® 98, Windows 95 and Windows NT®, it must be a 32-bit TCP/IP stack.



System Requirements for SecureCRT:



Minimum of a 486 based machine with 8 megabytes of RAM.



Windows NT® - version 3.51 or greater.



Windows® 98 or Windows 95



winsock.dll (compliant with version 1.1 of the Winsock standard).



TCP/IP stack. Under Windows® 98, Windows 95 and Windows NT®, it must be a 32-bit TCP/IP stack.

Terminal Session Security

Session security depends on several factors, including whether the connection you're using to the host is a trusted connection. If it is not, consider whether private or confidential information will be sent and received. A standard CRT telnet session on the Internet will transmit user ID, password and other sensitive or private information in an easily readable format.

For maximum security, don't put passwords in the CRT **Script** dialog or script file. Script dialog information is stored in the CRT configuration file, which may not be secure.
















Maximum security and privacy on the Internet and local networks requires the use of Secure Shell Protocol (SSH) and SecureCRT. Note that SecureCRT does do telnet, but SecureCRT telnet sessions are **not** encrypted.

Toolbar

Shows or hides the **toolbar**.

When displayed, the **toolbar** is above CRT's text window. Move the mouse cursor over an icon to view the action associated with the icon.

Below is a list of the actions associated with the icons.

Icon	Action
	Opens another CRT Window
	Displays the Quick Connect dialog.
	Displays the Connect dialog.
	Terminates the current connection
	Copies the current selection onto the Clipboard
	Sends the current contents of the Clipboard to the remote host as if it had been typed
	Displays the standard Find dialog
	Prints the current screen
	Prints the current selection
	Toggles Auto Print
	Opens <u>S</u> ession <u>P</u> references dialog.
	Displays the <u>K</u> eymap <u>E</u> ditor dialog
	Displays Help topics

Trace Options

The **Trace Options** command determines whether the server initialization negotiation is displayed. **Trace Options** applies to Telnet, SSH, and SOCKS servers. If selected, the session negotiation is echoed to the screen. This option displays the option negotiation for Telnet sessions, the login negotiation for SSH sessions, and the initialization negotiation for SOCKS firewalls. This can be useful in determining a Telnet server's capabilities and in monitoring the status of SSH login sequence.

Vertical Scroll Bar

Turns on the vertical scroll bar.

Note: If the window is maximized, you must first restore the CRT window before selecting this option. After selecting this option, the CRT window can be maximized again.

Welcome

This help system documents both CRT version 2.4 and SecureCRT(TM) version 2.4.

- Look for this icon for information on features and subjects specific to SecureCRT.

If you do not find the information you need here, please e-mail any questions you have to the following address:

`crt-questions@vandyke.com`.

We will try to respond within 1-2 business days.

SecureCRT is a trademark of Van Dyke Technologies, Inc.

What is CRT?

CRT is a 32-bit terminal emulator designed for Internet and intranet use with support for both the telnet and rlogin protocols. It supports Windows NT 3.51, NT 4.0, Windows 98, Windows 95, and Windows 3.1 with Win32s libraries installed.

CRT is highly customizable and easy to use. Remote sites can be easily accessed simply by entering a hostname.

SecureCRT has all of the features and functionality of CRT, but also includes support for the Secure Shell (SSH) protocol.

- Look for this icon for information on features and subjects specific to SecureCRT.

General features

- Named sessions allow the user to have different preferences for different hosts
- Simple mechanism for automating logins
- Telnet protocol support, including to a specific port
- Rlogin protocol support
- Serial (COM port) support (not available for Windows 3.1)
- Easy reconnect on connect abort and close
- Printing support: auto print, print selection and screen, cancel print job
- Easy installation

Advanced/Convenience features

- "Open URL" feature in context menu (right mouse button)
- Keyboard accelerator (Ctrl+Tab) to easily cycle between CRT windows
- Support for use from the command line or web browsers
- Each session can be logged to a file
- Anti-idle support.
- Searchable scrollbar buffer
- User-defined number of savelines (scrollback)
- Emacs mode maps Alt+<key> to Esc+<key>
- Easy access to CRT features through graphical toolbar
- User-defined word delimiter characters for double click
- Optional chat window provides an editable type-ahead buffer

Emulation

- Quality VT100, VT102, VT220, and ANSI emulation
- VT line drawing
- User-defined foreground and background colors for all eight combinations of the attributes (blink, underline, bold)
- Configurable number of rows and columns
- 80/132 column switching
- Ability to select separate fonts for both 80 and 132 column modes
- Double width and double height fonts
- Optional ANSI color and customizable ANSI colors.
- xterm extensions for mouse support and changing title bar
- 4 cursor styles and support for customizing cursor color
- National Replacement Characters sets (British, Dutch, Finnish, French, French Canadian, German, Italian, Norwegian/Danish, Spanish, Swedish, Swiss)

Keyboard mapping

- VT100 and VT220 keyboard emulation
- Support for user-defined custom keymaps
- Custom Keymap editor allows easy mapping of key combinations to:
 - Execute menu functions
 - Run scripts
 - Send string sequences
 - Call additional CRT functions
- Support for mapping key combinations based on NumLock state

Firewall support

- SOCKS version 4 and version 5 (telnet and SSH only)
- Generic telnet proxy firewall support

Scripting

- A simple expect/send dialog can be used to easily automate login commands
- Support for file-based scripts:
 - Scripts can be run automatically at login
 - Run a script at any time from the menu
 - Map a key combination to run a script using the Keymap editor

File transfer

- ZModem file transfer (upload and download)
- Transfer list dialog allows selection of multiple files for ZModem upload

Clipboard support

- Copy and paste, including an "Auto Copy" option
- Column select feature (Alt+Left click)

What is SecureCRT?

▪ SecureCRT is an enhanced version of CRT that includes support for the [Secure Shell \(SSH\) protocol](#), along with CRT's standard telnet, rlogin and serial terminal emulation. SecureCRT can be used to provide a single application for both secure and non-secure sessions, and includes all the options and customization capabilities of CRT. SSH is a secure protocol that replaces existing terminal protocols such as telnet and rlogin. SSH must be supported by both the client and the server.

General Features

- Use SSH to securely log in to any SSH server.
- Easy public key generation with [RSA Key Generation Wizard](#).
- RSA public key [identity files](#) can be global or session-specific.
- Variable SSH compression allows tuning session performance on slow dialup connections.
- [Port forwarding](#) allows encrypting the network traffic of insecure protocols like SMTP, POP and IMAP.
- X11 forwarding allows forwarding X Windows packets through the SSH session, which makes possible the encryption of the data between the client and server.
- Support for [named services](#) simplifies selecting ports used in [Port forwarding](#).
- And all the features of [CRT](#)!

Encryption ciphers

- DES
- 3DES
- RC4
- Blowfish

Authentication methods

- Password
- RSA public-private key pairs
- TIS

What's New in SecureCRT 2.4

Port forwarding

- **Use single SSH connection** option. Selecting this option for applications like web browsing may increase performance.

Please see `readme.txt` in the SecureCRT directory for additional information on minor changes and bug fixes.

Window, Close All

Closes all sessions.

Window, Next

Brings the next CRT window to the foreground.

ZModem Upload List

Displays the file list dialog. One or more files can be selected for ZModem upload.

The upload does not occur until the ZModem **receive** command is run on the remote machine.

