

## **Entire Connection**

### **Installation**

Version 4.5.2

April 2009

This document applies to Entire Connection Version 4.5.2 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © Software AG 1984-2009. All rights reserved.

The name Software AG, webMethods and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA, Inc. Other company and product names mentioned herein may be trademarks of their respective owners.

## Table of Contents

1	Installation .....	1
2	Supported Communication Methods .....	3
	TN3270(E) .....	4
	Telnet VTxxx .....	4
	BS2000 TCP/IP .....	4
	HLLAPI .....	5
	Serial, VTxxx .....	6
	VT100 Protocol Converter .....	6
3	Possible Setup Scenarios .....	9
	Asynchronous Communication with IBM Host Systems .....	11
	Communication via TCP/IP Networks .....	13
	Terminal Emulation for UNIX Systems .....	14
4	Installing Entire Connection .....	15
	Prerequisites .....	16
	Installing Entire Connection for the Administrator .....	17
	Silent Installation .....	18
	Program Folders .....	19
	Environment Variables .....	21
	Upgrading Entire Connection .....	21
	Installing Entire Connection on a Client Workstation .....	21
	Uninstalling Entire Connection .....	22
5	TN3270 SSL/TLS Support .....	23
	SSL Functionality Supported in Entire Connection .....	24
	Establishing an SSL TN3270 Session .....	24
	Configuring SSL for Entire Connection .....	25
	Checking Server Certificates in Entire Connection .....	26
	Client Authentication .....	27
	More About Certificates .....	28
6	.key Files for Protocol Converters .....	31
	.key Files Provided with Entire Connection .....	32
	Sample .key File .....	32
	Entries with Special Meanings .....	34
	Mnemonic Names .....	35



# 1 Installation

---

The following topics provide all information required for installing Entire Connection.

- **Supported Communication Methods**
- **Possible Setup Scenarios**
- **Installing Entire Connection**
- **TN3270 SSL/TLS Support**
- **.key Files for Protocol Converters**



## 2 Supported Communication Methods

---

▪ TN3270(E) .....	4
▪ Telnet VTxxx .....	4
▪ BS2000 TCP/IP .....	4
▪ HLLAPI .....	5
▪ Serial, VTxxx .....	6
▪ VT100 Protocol Converter .....	6

## TN3270(E)

---

Entire Connection supports TCP/IP TN3270 and TN3270E communication for display sessions. It also supports TCP/IP TN3270E communication for host printer sessions.

You can use any network adapter that is supported by any TCP/IP stack software which provides the WinSock 2 interface. This mode supports extended attribute bytes (EABs).

The TCP/IP stack software must be installed and active in order to activate terminal emulation.

For IBM host printer emulation, it is necessary to define generic, specific or associated printers on the Telnet server. See your Telnet server documentation for details.

See also: communication parameters for TN3270(E) in the *Overview of Object Properties*.

## Telnet VTxxx

---

Entire Connection supports VT100, VT220 and VT320 communication with any network adapter that is supported by any TCP/IP stack software which provides the WinSock 2 interface.

The TCP/IP stack software must be installed and active in order to activate terminal emulation.

See also: communication parameters for Telnet VTxxx in the *Overview of Object Properties*.

## BS2000 TCP/IP

---

This communication method emulates the standard 9750 terminal which is a 24 by 80 characters display without colors. Local printing is not supported. In addition to the standard 9750 terminal features, the following features of the 975x family are supported:

- 80 FTZ per line
- 20 P-keys
- 24 F-keys
- reverse video
- full 9756-type memory support for P-Registers



In Natural environments, the color terminal type 9763 (7 bit) is also supported. As a prerequisite, Natural Version 3 or above must be installed. By default, Natural uses the terminal type 9750 (monochrome). To activate the terminal type 9763, use the following Natural terminal command (either in a screen or in a program):

```
%T=9763
```

When activating the terminal type 9763, it is recommended that you also load the Siemens function keys F1 through F20 using the following Natural terminal command:

```
%KN
```

Entire Connection supports TCP/IP communication with BS2000 hosts with any network adapter that is supported by any TCP/IP stack software which provides the WinSock 2 interface.

The prerequisite on the host side is the communication subsystem BCAM version V.11, which establishes the connection with the host (available within the Siemens product DCAM).

No third-party software is needed for Entire Connection to activate terminal emulation.

To make the terminal emulation key settings similar to those on a BS2000 keyboard, use the pre-defined key scheme BS2000KEYS.

See also: communication parameters for BS2000 TCP/IP in the *Overview of Object Properties*.

## HLLAPI

---

Entire Connection supports any communication environment for which HLLAPI software for Windows (32 bit) is available. Support for extended attribute bytes (EABs) depends on the third-party HLLAPI software.



### Notes:

1. Many programs will support extended attribute bytes in DFT mode, but not in CUT mode.
2. Some vendors' APIs must be started before Entire Connection.

To activate terminal emulation, Entire Connection requires the vendor-supplied emulator package and HLLAPI. Install and test the vendor's emulator in your specific communication environment before you start Entire Connection.

Once your vendor-supplied programs are successfully communicating with the host, invoke Entire Connection. If any of the vendor-supplied software required by Entire Connection is removed from memory when Entire Connection is terminated, the vendor-supplied software must be reinvoked each time you wish to invoke Entire Connection.

When using HLLAPI mode to communicate with the mainframe, the `SESSION` command allows you to switch to different logical unit (LU) sessions.

Windows Terminal Services are not supported.

See also: communication parameters for HLLAPI in the *Overview of Object Properties*.

## Serial, VTxxx

---

Entire Connection supports any serial port (COM1 through COM4). If you are not using a direct connection, an internal or external asynchronous modem is required.

VT100/VT220/VT320 escape sequences are supported (private DEC codes as well as ANSI standard codes for VT100/VT220/VT320). ANSI colors (VT340+) are also supported.

When using Entire Connection to communicate with a VMS or UNIX machine, the line from the PC must be connected to a port on the VMS host or on a terminal server that is either identified as VT100/VT220/VT320 or set to request terminal identification.

To set up Entire Connection for serial communication with a VTxxx host, enable `XON/XOFF` flow control if it is supported by the host machine to which you are connected. If the host machine supports bidirectional flow control (i.e. an `XOFF` can be sent from the host to an application and an `XOFF` can be sent from the application or user to the host), enable both directions.

Windows Terminal Services are not supported.

See also: communication parameters for the VTxxx serial port in the *Overview of Object Properties*.

## VT100 Protocol Converter

---

A protocol converter converts the 3270 data stream into another communication protocol. There are a number of different communication protocols. Entire Connection, however, supports only the ANSI VT100 protocol. Non-standard extensions to the ANSI VT100 protocol are not supported.

Extended attribute bytes (EABs) are not supported.

Most protocol converters convert normal 3270 field types and then assign VT100 attributes to each field type. You can define the colors you want to use for displaying the attributes.

See also: communication parameters for VT100 Protocol Converter in the *Overview of Object Properties*.

---

▶ **To set up your protocol converter for use with Entire Connection**

- 1 Configure the protocol converter for VT100 mode.
- 2 Set the protocol converter to enable XON/XOFF flow control, if available. If the protocol converter supports bidirectional flow control (i.e. an XOFF can be sent from the protocol converter to the application and an XOFF can be sent from the application or user to the protocol converter), both directions should be enabled.
- 3 Disable any status line display generated by the protocol converter.
- 4 Import the terminal function code table for your protocol converter.
- 5 Use one of the supplied *.key files* or create a *.key* file that contains all valid escape code sequences required by your protocol converter.

If none of the supplied *.key* files is compatible with your protocol converter, you must either create a new *.key* file or modify one of the supplied *.key* files.

- 6 Check each escape sequence in the *.key* file to ensure that it corresponds to the escape sequence required by your particular protocol converter.

Because most protocol converters may be customized when installed, this applies to both supplied and customized *.key* files. It is important to verify that the escape sequences needed by the protocol converter have not been modified.

If you are using multiple protocol converters and different sets of escape sequences are required among them, you must create a unique *.key* file for each protocol converter.

- 7 Import each *.key* file to internally store this information for terminal emulation purposes.
- 8 Define all required communication parameters.



# 3 Possible Setup Scenarios

---

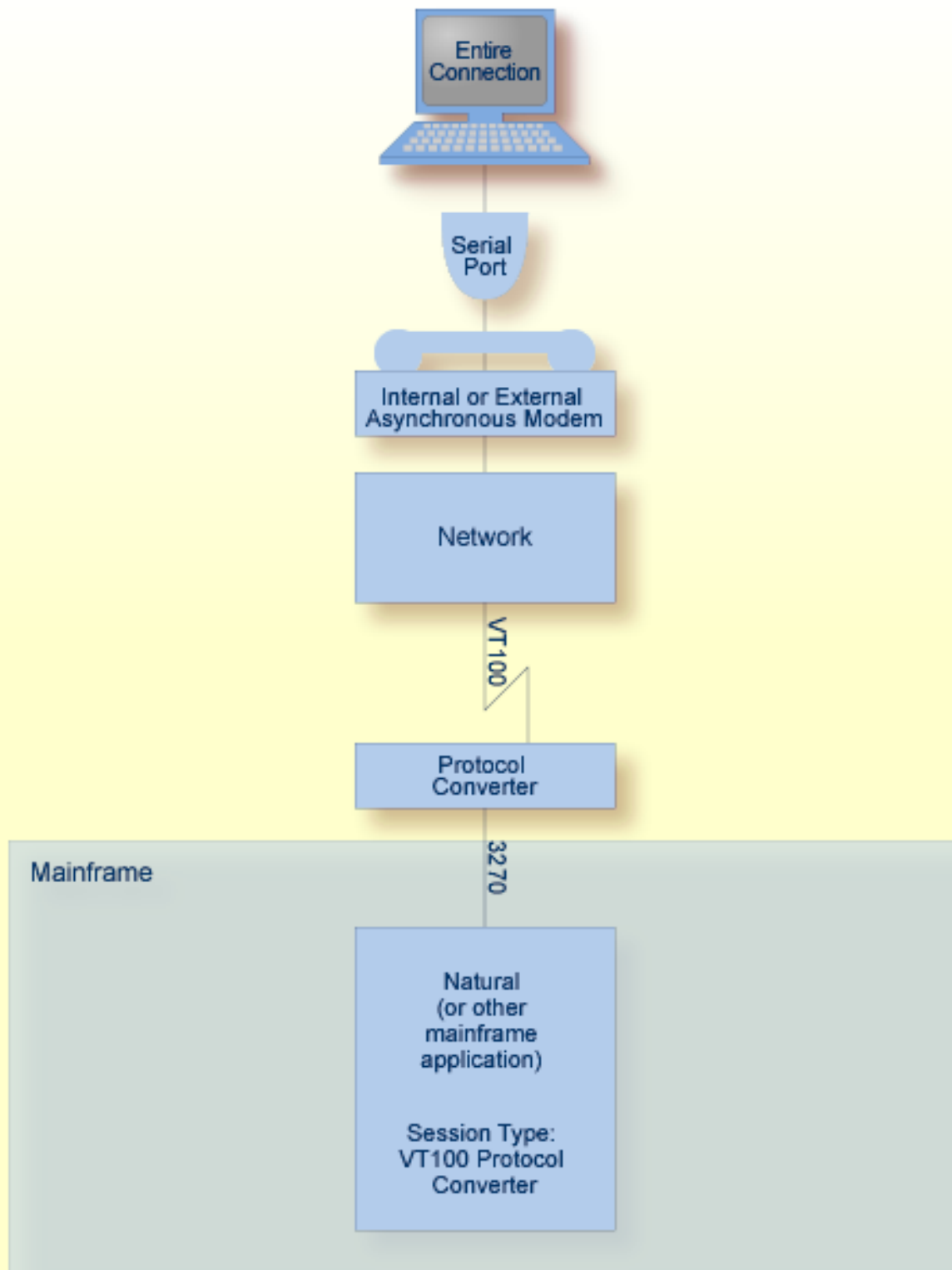
- Asynchronous Communication with IBM Host Systems ..... 11
- Communication via TCP/IP Networks ..... 13
- Terminal Emulation for UNIX Systems ..... 14

Entire Connection can be installed in a wide range of network configurations. The diagrams in this section illustrate the possible scenarios.

For each scenario, the diagram indicates the prerequisites and the session type you must define once Entire Connection is installed.

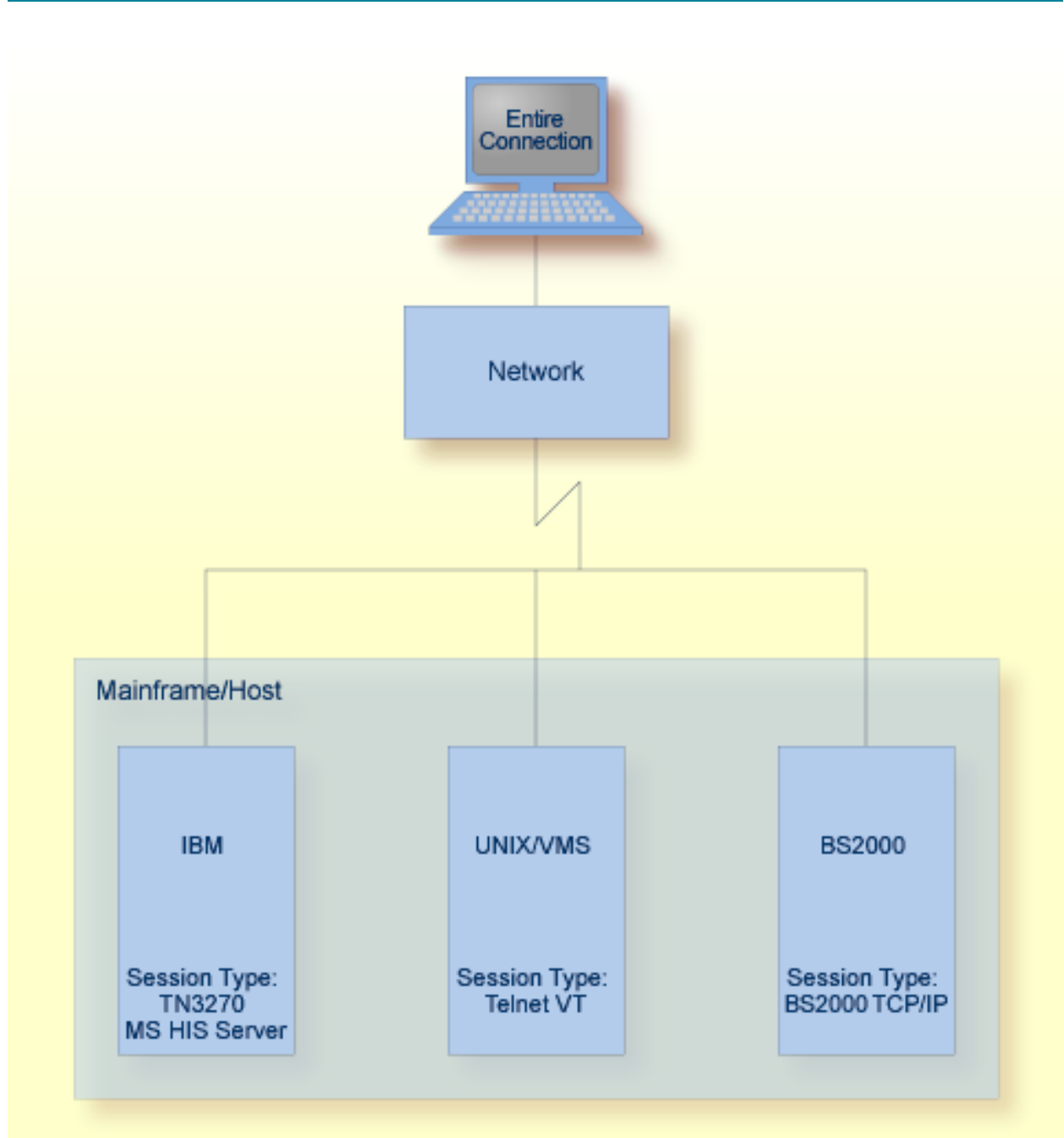
## Asynchronous Communication with IBM Host Systems

---





## Communication via TCP/IP Networks



Third-party software requirements:

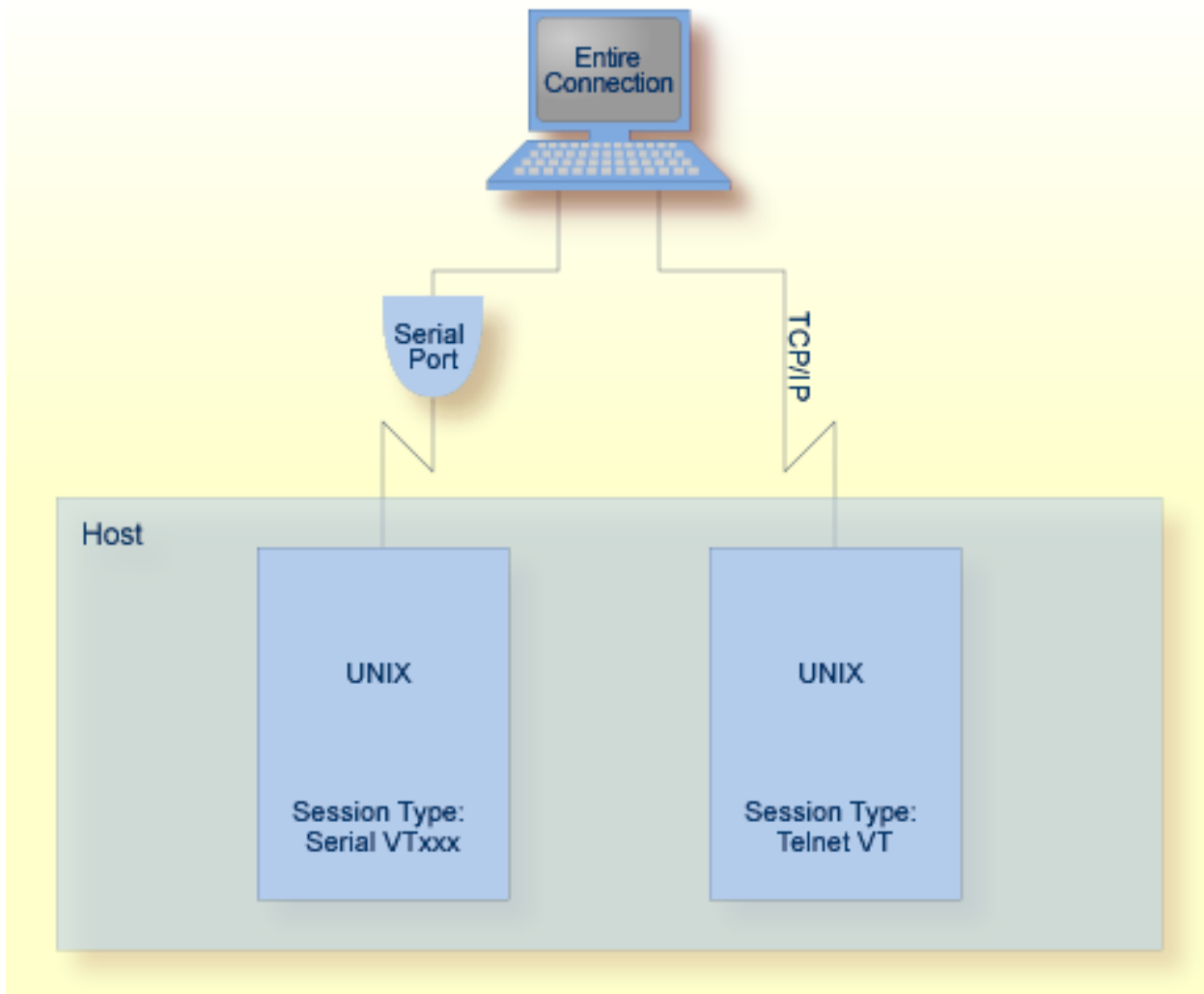
- WinSock 2



**Note:** Session type BS2000 TCP/IP does not provide the complete 975x functionality.

## Terminal Emulation for UNIX Systems

---



UNIX terminal emulation:

- VT100
- VT220
- ANSI color support (VT340+)

Third-party software requirements:

- WinSock 2

# 4 Installing Entire Connection

---

- Prerequisites ..... 16
- Installing Entire Connection for the Administrator ..... 17
- Silent Installation ..... 18
- Program Folders ..... 19
- Environment Variables ..... 21
- Upgrading Entire Connection ..... 21
- Installing Entire Connection on a Client Workstation ..... 21
- Uninstalling Entire Connection ..... 22

## Prerequisites

Entire Connection Version 4.5.2 is a 32-bit application. When installed on a 64-bit Windows operating system, Entire Connection will run under WOW64. WOW64 is an x86 emulator that allows 32-bit Windows-based applications to run seamlessly on 64-bit Windows.

The following hardware and software is required in order to install and run Entire Connection:

<b>Hardware</b>	Any PC capable of running Microsoft Windows. Approximately 60 MB of free disk space. During installation, additional 80 MB are required in the Temp directory.
<b>Operating System</b>	Entire Connection can be installed on the following operating systems: <ul style="list-style-type: none"> <li>■ Microsoft Windows XP Home Edition or Professional.</li> <li>■ Microsoft Windows Server 2003 Standard Edition or Enterprise Edition.</li> <li>■ Microsoft Windows Vista.</li> <li>■ Microsoft Windows Server 2008.</li> </ul>
<b>Communication Method</b>	At least one of the supported PC-to-host <a href="#">communication methods</a> .
<b>Data Transfer Software</b>	<p>If you want to transfer data between the host and your PC, the following Software AG products must be installed on the host to which the PC is being linked:</p> <ul style="list-style-type: none"> <li>■ A version of Natural for Mainframes, Natural for UNIX or Natural for OpenVMS which supports the use of Entire Connection.</li> <li>■ Natural for Mainframes: The version of Natural Connection that is compatible with the version of Natural you are using.</li> </ul> <p><b>Note:</b> Natural Connection is automatically installed when Natural for UNIX or Natural for OpenVMS is installed.</p> <p>If you want to download data to Excel format or upload Excel data, one of the following Excel versions must be installed on your PC:</p> <ul style="list-style-type: none"> <li>■ Excel 97, or</li> <li>■ Excel 2000, or</li> <li>■ Excel 2002, or</li> <li>■ Excel 2003, or</li> <li>■ Excel 2007.</li> </ul>
<b>Online Documentation</b>	Microsoft Internet Explorer 4.0 or higher for viewing the Entire Connection documentation in HTML help format.

## Installing Entire Connection for the Administrator

Before installing Entire Connection, read the file *Install.txt* on the Entire Connection CD.

The setup program on the CD installs Entire Connection for one user, the administrator. In the simplest case, this is a single installation on a local PC, where the user can act as an administrator and define all required object types.

When several users are to work with the same installation (multi-user installation), the administrator can install Entire Connection on a network file server or shared drive and prepare the system for all users who are to access Entire Connection from different client workstations. For this type of installation, you have to choose the setup type **Complete** (or the setup type **Custom** and select the option **Client Setup**). The **Client Setup** option creates the *netsetup* folder in the *Entire Connection 4.n.n* folder. By default, this is `\Program Files\Software AG\Entire Connection 4.n.n\netsetup`. The *netsetup* folder contains the client installation program *Setup.exe*. Each user can run this program from his or her client workstation. It registers Entire Connection on the client workstation and creates an Entire Connection folder in the Start menu of the client workstation. When started, *Setup.exe* searches for the *Readme.doc* file in the *netsetup* folder. When found, its content is displayed. The administrator can use this file to provide the users with site-specific information for their work with Entire Connection (such as user names, defaults or session names). See [Installing Entire Connection on a Client Workstation](#) later in this section for information about the installation on the client workstation.

The following setup types are available:

Setup Type	Installs
Typical (default)	The most common options. Recommended for most users.
Complete	All options. Required for a multi-user installation.
Custom	You may select the options you want to install. Recommended for advanced users.

The following table indicates the options that are (or can be) installed with a specific setup type:

Option	Typical	Complete	Custom
Configuration Manager	X	X	X
Terminal	X	X	X
Format Converter	X	X	X
Host Printer LU Support		X	(X)
Sample Procedures	X	X	X
Sample Natural Programs	X	X	X
Client Setup		X	(X)

The default setting for a custom installation is the same as for the setup type **Typical**.

The following options are always installed: Configuration Manager and Terminal. With a custom installation, it is not possible to deselect these options.

### ▶ To install Entire Connection

- 1 Close any active Windows applications.
- 2 Insert the Entire Connection CD into your CD drive.

The setup program is automatically started and guides you through the installation.

If the automatic startup option is disabled on your system, you must run *Setup.exe* which is located in the root directory of the CD.

- 3 After the installation, the administrator can define the parameters, objects (e.g. sessions), user groups and access rights for all users (see the section *Configuration Manager*). As the first step, make sure that the settings in the **System Preferences** dialog box are valid for all users. It is important that the directories for the procedure files and for the log and trace files can be accessed by all users.
- 4 If you want to merge version 3.1 user profiles, you must do this directly after installation. See *Merging Existing User Profiles* in the *Configuration Manager* section for further information.
- 5 If you upgrade from a previous 4.n.n version of Entire Connection, you have to upgrade your share file. Otherwise, specific new features will not be available. See *Upgrading the Share File* in the *Configuration Manager* section for further information.

## Silent Installation

---

InstallShield enables you to install Entire Connection in silent mode. No user interaction is required in this silent mode installation.

For installing in silent mode, you cannot run *setup.exe* from the CD root. In this case, you have to run the *setup.exe* from the folder `\Windows\PCC` of the CD.

### ▶ To install in silent mode

- 1 Insert the Entire Connection CD in the CD drive of the PC on which you want to install Entire Connection in silent mode.
- 2 Invoke the Command Prompt.
- 3 Change to the `\Windows\PCC` folder on the Entire Connection CD.
- 4 Enter the following command:

```
setup.exe /s /L1033 /w /v"/lvoicewarmup! %TEMP%\pccnnmsi.log
SERIALNUMBER=serial-number INSTALLDIR=installation-folder
INSTALLLEVEL=installlevel /qn"
```

where the options are:

/s	Silent mode (no user interaction).
/L1033	Language. "L1033" installs an English version of Entire Connection. "L1031" installs a German version.
/w	Wait. <i>setup.exe</i> waits until the installation is finished.
/v	List of parameters for the Windows installer.
/lvoicewarmup! %TEMP%\pccnnmsi.log	Log file for the installation. It is not recommended to remove this parameter. <i>nnn</i> in the log file name stands for the current version number of Entire Connection.
SERIALNUMBER= <i>serial-number</i>	Required. The serial number of Entire Connection.
INSTALLDIR= <i>installation-folder</i>	The installation folder (the default is <i>\Program Files\Software AG\Entire Connection 4.n.n</i> ).
INSTALLLEVEL= <i>installlevel</i>	Possible values are 1 or 100 (the default is 1). The value 1 stands for the setup type <b>Typical</b> ; the value 100 stands for the setup type <b>Complete</b> (see above).
/qn	Required. Silent mode for the Windows installer.



**Note:** Update installations cannot be done in silent mode. If you try to do this, an error message is written to the log file.

## Program Folders

By default, Entire Connection is installed in the following program folder:

*\Program Files\Software AG\Entire Connection 4.n.n*

Program Folder	Contents
<i>\Entire Connection 4.n.n</i>	*.exe *.dll API ActiveX control <i>PccAPI.ocx</i> .
<i>\Entire Connection 4.n.n\doc</i>	<i>Readme.txt</i>  English and German online documentation, and the help files <i>Pccnnnxx.chm</i> (where <i>nnn</i> is the current version number and <i>xx</i> is the language code "US" for US English or "GR" for German).

Program Folder	Contents
<code>\Entire Connection 4.n.n\netsetup</code>	Client installation program <i>Setup.exe</i> . Only available when the option <b>Client Setup</b> has been specified during installation (setup type <b>Custom</b> ).

Depending on the operating system, the folders for the user data are by default installed at the following location:

- Windows 2000, XP and Server 2003:

`\Documents and Settings\All Users\Application Data\Software AG\Entire Connection`

- Windows Vista:

`\ProgramData\Software AG\Entire Connection`

The *ProgramData* folder, which is used with Windows Vista, is a hidden folder. It is only shown in the Explorer when you have activated the corresponding setting in the folder options of the Explorer.

If you do not install into the default program folder (that is: the *Program Files* folder of Windows), the folders for the user data are installed into the specified installation folder.

The folders for the user data are:

Folder	Contents
<i>certs</i>	Files for TN3270 SSL/TLS support.
<i>data</i>	<i>Share411.sag</i> .
<i>home</i>	Empty after installation. *.log Trace files (e.g. <i>Monnn.trc</i> and <i>Hllapi.trc</i> ). Temporary files for host printer LU support.
<i>proc</i>	System procedure files. If specified during installation, this folder may also contain sample procedure files and sample Natural programs.
<i>tables</i>	Translation tables, keyboard tables, physical terminal function code tables.

If you install for multiple users on Terminal Services, and if you want to allow the users to change their profiles in the share file, you have to change the security properties for the file *Share411.sag* to allow write access for the users.



## Environment Variables

---

Entire Connection does not change any environment variables.

## Upgrading Entire Connection

---

Only one version of Entire Connection 4 can be installed on a PC (installation for an administrator). When you upgrade Entire Connection, the previous version is removed and the new version is installed. Any user data from the previous version, especially the share file, will be saved and re-stored.

Since the default location for the user data has changed as of Entire Connection Version 4.5.1, the user data can also be found at the new location after the upgrade.



**Caution:** The folder names that are stored in your share file may no longer be valid if the upgrade has changed the folder that contains your user data. In this case, after upgrading to Entire Connection Version 4.5.2, you have to adjust these folder names to ensure that Entire Connection can find your procedure files, log files and trace files. The folder names that Entire Connection uses to locate these files are stored in the system preferences and in the user properties.

## Installing Entire Connection on a Client Workstation

---

For a multi-user installation, the administrator must first install and prepare Entire Connection on a network file server or shared drive (see [Installing Entire Connection for the Administrator](#)). When this has been done, each user can run *Setup.exe* in the *netsetup* folder from his or her client workstation. It registers Entire Connection on the client workstation and creates an Entire Connection folder in the Start menu of the client workstation.



**Important:** Each user who wants to install Entire Connection on a client workstation as described above needs administrator rights.

## Upgrading Entire Connection on a Client Workstation

There is no upgrade installation for the client workstation.

The administrator must first upgrade the existing Entire Connection installation on the network file server or shared drive (see [Upgrading Entire Connection](#)). Then, for the PC on which you have an existing client installation, proceed as follows:

1. Uninstall Entire Connection on all client workstations (see below).
2. Install Entire Connection on all client workstations (see above).

## Uninstalling Entire Connection on a Client Workstation

See [Uninstalling Entire Connection](#).

## Uninstalling Entire Connection

---

Use the standard Windows functionality in the Control Panel to uninstall Entire Connection.

The uninstall does not remove any user-supplied files in the Entire Connection installation folders. This also includes the share file in the *data* folder.

# 5 TN3270 SSL/TLS Support

---

- SSL Functionality Supported in Entire Connection ..... 24
- Establishing an SSL TN3270 Session ..... 24
- Configuring SSL for Entire Connection ..... 25
- Checking Server Certificates in Entire Connection ..... 26
- Client Authentication ..... 27
- More About Certificates ..... 28

Entire Connection supports TN3270 SSL. This allows a secure connection between Entire Connection and a Telnet TN3270 server. In an SSL session, all data is encrypted before it is sent to the Telnet server. Encrypted data received from the server is decrypted before it is processed.

A prerequisite is that you have a Telnet TN3270 server with an SSL-enabled port. To use SSL, the server must have a private key and an associated server certificate.



**Note:** This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

## SSL Functionality Supported in Entire Connection

---

In Entire Connection, SSL support is available for TN3270 display sessions and for TN3270 printer sessions. The following SSL options are supported:

### ■ Server authentication

Server authentication is used to identify the server to the client. Server authentication can be enabled or disabled for an encrypted SSL session. It can be used with or without client authentication.

Before the session is established, the client (Entire Connection) checks the server certificate which is associated with the server's private key.

### ■ Host name check

The name of the host to which the client (Entire Connection) connects is compared with the common name (CN) value of the server certificate. This option strengthens the server authentication.

### ■ Client authentication

Client authentication is used to identify the client to the server.

SSL client authentication provides additional authentication and access control by checking client certificates on the server. This support prevents a client from obtaining a connection without an installation-approved certificate.

## Establishing an SSL TN3270 Session

---

There are two ways to establish an SSL TN3270 session.

One way is to directly open an SSL connection with an SSL handshake. This means that the client connects to an SSL-enabled port of the Telnet TN3270 server and that the SSL protocol is used from the beginning.

Another way is negotiated Telnet security. In this case, a normal Telnet connection is opened between the client and the Telnet TN3270 server. Then the Telnet server sends a special command (IAC DO START\_TLS) to the client to check whether it wants to start SSL negotiation. If a positive response is received, the server continues with the SSL handshake. If no positive response is received, then, depending on the server configuration, a normal Telnet session is used or the connection is dropped.

## Configuring SSL for Entire Connection

The following folder (depending on the operating system) contains several server certificate files from different Certification Authorities (CAs):

- Windows 2000, XP and Server 2003:

*\Documents and Settings\All Users\Application Data\Software AG\Entire Connection\certs*

- Windows Vista:

*\ProgramData\Software AG\Entire Connection\certs*

1. When server authentication has been enabled, check whether the server certificate you have for your Telnet SSL server is already contained in the folder *certs*. If your server certificate is from a different Certificate Authority, or if you use a self-signed certificate, then you have to add it to the *certs* folder and to the *CAList.pem* file in this folder. See [Checking Server Certificates in Entire Connection](#) for detailed information.
2. Use Entire Connections's Configuration Manager to create a host session (display session) of type TN3270. In the resulting **Session Properties** dialog box, specify a session name and choose the **Communication** button. Specify all required information on the **General** property page of the resulting **Communication** dialog box. Specify the number of a port which is able to support SSL. Display the **Security** property page and make sure that SSL is enabled. You will now check whether the basic SSL connection works correctly. Either enable the **SSL/TLS handshake connection** check box if you want to establish a handshake connection or disable this check box if you want to establish a session with Telnet negotiated security. Do not yet activate any other option on this property page. For detailed information on the communication parameters, see *TN3270(E) for Display Sessions* in the *Overview of Object Properties*.
3. Use Entire Connection's terminal application to test the session you have created in the previous step.
4. When the basic SSL connection works correctly, you can activate and test the remaining options on the **Security** property page:

**■ Host name check**

You can only use this SSL option if the common name (CN) value in the server certificate is the same as the host name that is used on the **General** property page of the **Communication** dialog box.

To use this SSL option, activate the option **Compare certificate's common name with host name** on the **Security** property page of the **Communication** dialog box.

**■ Client authentication**

Your server must be set up to use client authentication. You need a client private key and a certificate for this key. This key and certificate must be added to your server installation. The private key and the certificate must also be added to the Entire Connection installation. See [Client Authentication](#) for detailed information.

To use this SSL option, activate the option **Send certificate if requested by server** on the **Security** property page of the **Communication** dialog box.

5. Repeat the above steps to create a host printer session of type TN3270E. For detailed information on the communication parameters, see *TN3270E for Printer Sessions* in the *Overview of Object Properties*.

## Checking Server Certificates in Entire Connection

---

This section applies when server authentication has been enabled. It describes how to set up a basic SSL connection with server authentication. This means Entire Connection connects to an SSL connection and checks the certificate of the TN3270 server. If the server certificate is not valid, the connection will be stopped.

When starting a TN3270 SSL connection, Entire Connection checks the server certificate against the certificates in the file *CAList.pem*. This file contains the (root) certificates of the Certification Authorities (CAs) that you trust. A Certification Authority is a company that signs certificate requests. One example of such a company is VeriSign (see <http://www.verisign.com/>).

The *CAList.pem* file that is provided with Entire Connection contains several certificates from well known Certification Authorities. If you have a self-signed certificate for your server, or if you want to add a certificate to the list of trusted certificates, proceed as described below.

▶ **To add a certificate to the *CAList.pem* file**

- 1 Go to Entire Connection's *certs* folder.

This folder contains several certificate files (*.crt*) and the file *CAList.pem* which is a summary of the *crt* files. The batch file *create-calist.bat* is used to create the file *CAList.pem*. It contains a command line for each of the certificate files to be added to *CAList.pem*.

- 2 Copy your *crt* file (for example, a self-signed certificate or a new certificate from a Certification Authority) to the *certs* folder.
- 3 Edit the batch file *create-calist.bat* and add a command line for the certificate you want to add.

For example, if you want to add the certificate in *mycert.crt*, you have to add the following command line:

```
%OPENSSL% x509 -text -in mycert.crt >> %OUTFILE%
```

- 4 Make sure that the variable `OPENSSL` in the first line of the batch file is set correctly for your installation. It must point to *OpenSSL.exe* which is provided in Entire Connection's root directory.
- 5 Execute the file *create-calist.bat*. The file *CAList.pem* is now regenerated with the new certificate file.

## Client Authentication

---

With client authentication, the Telnet server can check the identity of the client. The server cannot only check whether the certificate is issued by a trusted Certification Authority (lowest level security), it is also possible to register the client's certificate against an internal database (for example, RACF) and make sure that the client is connected from a defined TCP/IP address and port. Client authentication is optional.

### Generate a Private Key for Each User

For client authentication, it is necessary to generate a private key for each user. To generate a private key, use the program *OpenSSL.exe* which is provided in Entire Connection's root directory.

For information on how to generate a private key, see the document *keys.txt* in the *certs* folder.

Your private key should have the name *clientpriokey.pem*.

#### ▶ To create a 2048 bit RSA key (example)

- 1 Open a Command Prompt window.
- 2 Change to Entire Connection's *certs* folder.
- 3 Enter the following command at the command prompt:

```
"\Program Files\Software AG\Entire Connection n.n.n\OpenSSL.exe" genrsa -des3  
-out testkey.pem 2048
```

where *n.n.n* is the version number.

When you specify "-des3", you are prompted for a password while the private key is being generated.



**Important:** For reasons of security, it is recommended that you generate a private key with a password. Then the private key cannot be used without a password which is important if an unauthorized person gets hold of the private key.

### Create a Certificate Based on the Client Key

You also have to create a certificate based on the client key. For this purpose, you also use the program *OpenSSL.exe* which is provided in Entire Connection's root directory.

See the document *certificates.txt* in the *certs* folder for further information.

Your certificate should be named *clientcert.crt*.

#### ▶ To create a self-signed certificate using the configuration file *openssl.cnf* (example)

- 1 Open a Command Prompt window.
- 2 Change to Entire Connection's *certs* folder.
- 3 Enter the following command at the command prompt:

```
"\Program Files\Software AG\Entire Connection n.n.n\openssl.exe" req -new -x509  
-key clientprivkey.pem -out clientcert.crt -days 1095 -config openssl.cnf
```

where *n.n.n* is the version number.

Note that you have to configure your TN3270 server to use client authentication and also "install" the client key and the certificate in the server.

## More About Certificates

---

### Exporting Certificates from within Microsoft Internet Explorer

It is possible to export trusted certificates from Microsoft Internet Explorer. For further information, see <http://www.microsoft.com/windows/ie/using/howto/security/digitalcert/using.msp>.

Export the **Trusted Root Certification Authorities** you need. It is important that you export in **Base-64 Encoded X.509** format.



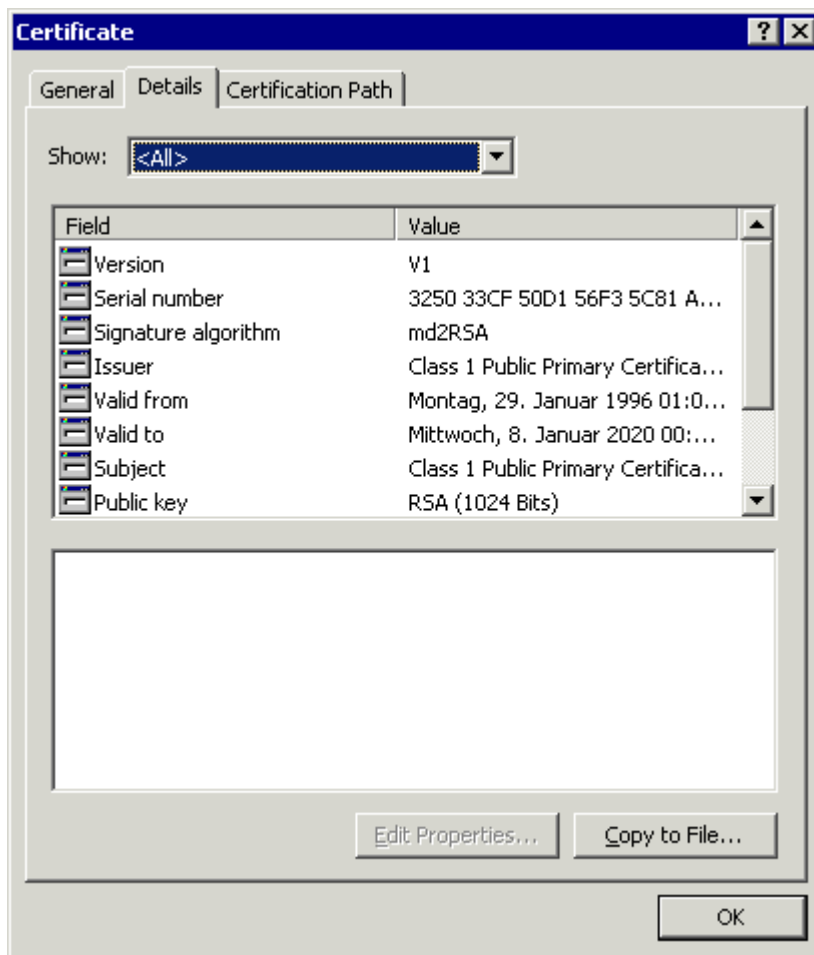
## Getting Root Certificates from Certification Authorities

It is also possible to download the root certificate directly from the web site of the Certification Authority (CA). The certificate may not be in the correct format (Entire Connection requires Base-64). To check whether the certificate is in Base-64 format, open it in an ASCII editor (for example, Notepad). If you see a "BEGIN CERTIFICATE" line in the beginning and a "END CERTIFICATE" line at the bottom, the format is already in Base-64 and you can just use it as it is.

If the certificate is not in base-64 format, you have to proceed as described below.

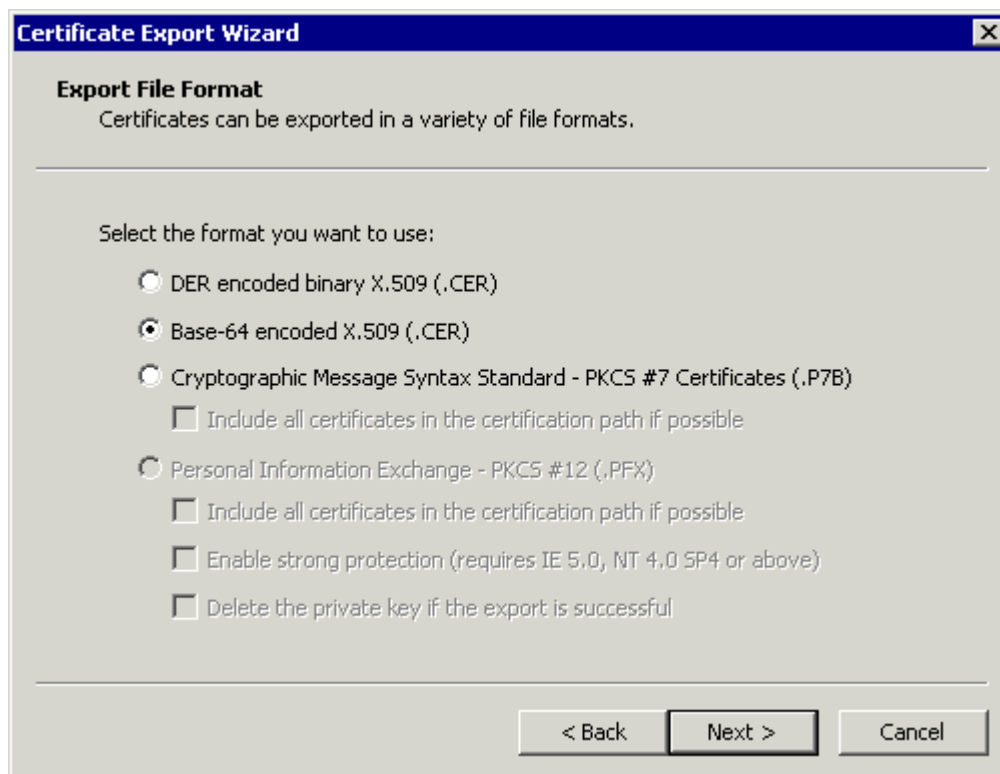
### ▶ To change the certificate to base-64 format

- 1 Open the certificate and display the **Details** property sheet. Example:



- 2 Choose the **Copy to File** button to invoke the Certificate Export Wizard.
- 3 Choose the **Next** button to proceed to the next page.

- 4 Select the option button **Base-64 encoded X.509 (.CER)**.



- 5 Choose the **Next** button to proceed to the next page.
- 6 Specify the name of the file to which you want to export the modified certificate.
- 7 Choose the **Next** button to proceed to the next page.
- 8 Choose the **Finish** button.

# 6 .key Files for Protocol Converters

---

- .key Files Provided with Entire Connection ..... 32
- Sample .key File ..... 32
- Entries with Special Meanings ..... 34
- Mnemonic Names ..... 35

This chapter explains which information can be modified in a *.key* file.

## .key Files Provided with Entire Connection

---

The *tables* directory of Entire Connection contains several *.key* files for protocol converters. Select the *.key* file that is most compatible with your protocol converter. Check whether the entries in this file correspond to the escape sequences required by your protocol converter (see the documentation for your protocol converter). Use only the VT100 escape sequences.

Among others, the following *.key* files are copied to your hard disk during installation:

File	Description
<i>Bb.key</i>	Brown's Box
<i>I3708.key</i>	IBM 3708
<i>I71.key</i>	IBM 7171
<i>Ldi.key</i>	Local Data InterLynx
<i>M80.key</i>	MaComm MDS 8070
<i>Mic.key</i>	MiCom
<i>Pci.key</i>	PCI 1071
<i>Prot.key</i>	Default used in share file
<i>Renex.key</i>	Renex
<i>Sitin.key</i>	SitIntel
<i>Tnt.key</i>	Telenet Network Version of Local Data

## Sample .key File

---

During installation, the file *Ldi.key* (see below) is copied to your hard disk. This sample *.key* file consists of several columns:

- First column: identifies the terminal function key to be defined.
- Second column: XLOCK indicates that the key will wait for a response from the host or protocol converter before allowing additional input from the keyboard.
- Third column: KEYRESET indicates that the keyboard is reset when insert mode is switched on.
- Fourth column: contains the escape sequence assigned to the terminal function key.



**Important:** The only data in a *key* file that should be modified are the data contained in the fourth column.

When modifying the data in column four, you can use the **mnemonic names** for the hexadecimal values X'00' through X'1F'. All escape sequences must be enclosed in single quotation marks; they are case-sensitive.

If your protocol converter does not support an entry in the *key* file, insert an asterisk (\*) in the first position of the corresponding line. This entry will then be ignored.

If the *key* file you select contains an asterisk (\*) in front of an entry required by your protocol converter, you must remove the asterisk and replace the question marks in column four with the required escape sequence.

```
* ldi.key
* (C)Copyright Software AG 1993-1999
* terminal emulation function key table for Local Data InterLynx
* and similar Protocol Converters.
*
* DO NOT change the keyword line below ("WiTeKeyTable PROT"):
*
* If you have to change the table in the share file, modify this
* file (or one of the others which is closer to your needs) and
* import the table using the Entire Connection configuration manager.

WiTeKeyTable PROT

* set vtkey attn          type ????????
set vtkey backspace      type esc '[D'
set vtkey backtab        type BS
set vtkey break          type cr
set vtkey clear          xclock keyreset type esc '0m'
set vtkey cr             xclock keyreset type cr
set vtkey delete         type DEL
set vtkey devcnc1        type esc '['
set vtkey down           type esc '[B'
set vtkey dup            type esc '0v'
set vtkey eof            type esc '0t'
set vtkey eraseinp       type esc '0w'
set vtkey fldmark        type esc '0l'
set vtkey home           type esc '0p'
set vtkey icr            keyreset type cr
* set vtkey ident        type ????????
set vtkey insert         type esc '0n'
set vtkey left           type esc '[D'
set vtkey newline        type LF
set vtkey pa1            xclock keyreset type esc '0q'
set vtkey pa2            xclock keyreset type esc '0r'
set vtkey pa3            xclock keyreset type esc '0s'
set vtkey pf1            xclock keyreset type esc '1'
set vtkey pf10           xclock keyreset type esc '0'
set vtkey pf11           xclock keyreset type esc '!'
set vtkey pf12           xclock keyreset type esc '@'
```

```
set vtkey pf13      xclock keyreset type esc '#'
set vtkey pf14      xclock keyreset type esc '$'
set vtkey pf15      xclock keyreset type esc '%'
set vtkey pf16      xclock keyreset type esc '^'
set vtkey pf17      xclock keyreset type esc '&'
set vtkey pf18      xclock keyreset type esc '*'
set vtkey pf19      xclock keyreset type esc '('
set vtkey pf2       xclock keyreset type esc '2'
set vtkey pf20      xclock keyreset type esc ')'
set vtkey pf21      xclock keyreset type esc esc '1'
set vtkey pf22      xclock keyreset type esc esc '2'
set vtkey pf23      xclock keyreset type esc esc '3'
set vtkey pf24      xclock keyreset type esc esc '4'
set vtkey pf3       xclock keyreset type esc '3'
set vtkey pf4       xclock keyreset type esc '4'
set vtkey pf5       xclock keyreset type esc '5'
set vtkey pf6       xclock keyreset type esc '6'
set vtkey pf7       xclock keyreset type esc '7'
set vtkey pf8       xclock keyreset type esc '8'
set vtkey pf9       xclock keyreset type esc '9'
set vtkey por       keyreset type esc '<'
set vtkey print     type esc '0x'
set vtkey refresh   keyreset type ^w
set vtkey reset     keyreset type DC2
set vtkey right     type esc '[C'
* set vtkey sysreq  type ????????
set vtkey tab       type tab
set vtkey test      xclock keyreset type esc '0y'
set vtkey up        type esc '[A'
set vtkey vtdisc    type esc '~'
set vtkey vtnit     type esc '<'
```

## Entries with Special Meanings


The following entries in a *.key* file have special meanings:

Entry	Description
BREAK	Send a break signal only (data are not sent). You can specify a value for the length of the break.
CR	Carriage return - required by Entire Connection when performing file transfers.
HOME	Required by Entire Connection when performing data transfers.
ICR	Immediate Carriage Return - similar to the CR entry except that ICR does not wait for a response from the mainframe or protocol converter. This entry is frequently used when establishing communications.
POR	Simulate a power-on-reset function. It is possible that the required escape sequence is not supported by your protocol converter, or that it can only be invoked from the main menu of the protocol converter.

Entry	Description
REFRESH	Inform the protocol converter that the screen display needs to be refreshed.
VTDISC	VT disconnect - terminate the connection with the protocol converter.
VTINIT	VT initialize - establish a connection with the protocol converter.

## Mnemonic Names

The following table contains all allowed mnemonic names for the hexadecimal values X'00' through X'1F'. The columns labeled "Alternative 1" and "Alternative 2" contain additional mnemonic names that can be used to transmit a particular hexadecimal value.

 **Note:** The caret (^) symbol is the internal representation for the CTRL key.

Hex. Value	Mnemonic Name	Alternative 1	Alternative 2
X'00'	^@	NUL	
X'01'	^A	SOH	
X'02'	^B	STX	
X'03'	^C	ETX	
X'04'	^D	EOT	
X'05'	^E	ENQ	
X'06'	^F	ACK	
X'07'	^G	BEL	
X'08'	^H	BS	
X'09'	^I	HT	
X'0A'	^J	LF	
X'0B'	^K	VT	
X'0C'	^L	FF	
X'0D'	^M	CR	
X'0E'	^N	SO	
X'0F'	^O	SI	
X'10'	^P	DLE	
X'11'	^Q	DC1	XON
X'12'	^R	DC2	
X'13'	^S	DC3	XOFF
X'14'	^T	DC4	
X'15'	^U	NAK	
X'16'	^V	SYN	

Hex. Value	Mnemonic Name	Alternative 1	Alternative 2
X'17'	^W	ETB	
X'18'	^X	CAN	
X'19'	^Y	EM	
X'1A'	^Z	SUB	
X'1B'	^[	ESC	
X'1C'	^\	FS	
X'1D'	^]	GS	
X'1E'	^^	RS	
X'1F'	^_	US	