Entire Connection

Installation

Version 4.5.4

November 2016

ADABAS & NATURAL

This document applies to Entire Connection Version 4.5.4.

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

Document ID: PCC-INSTALL-454-20161118

Table of Contents

Preface

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

1 Supported Communication Methods

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 predefined 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.

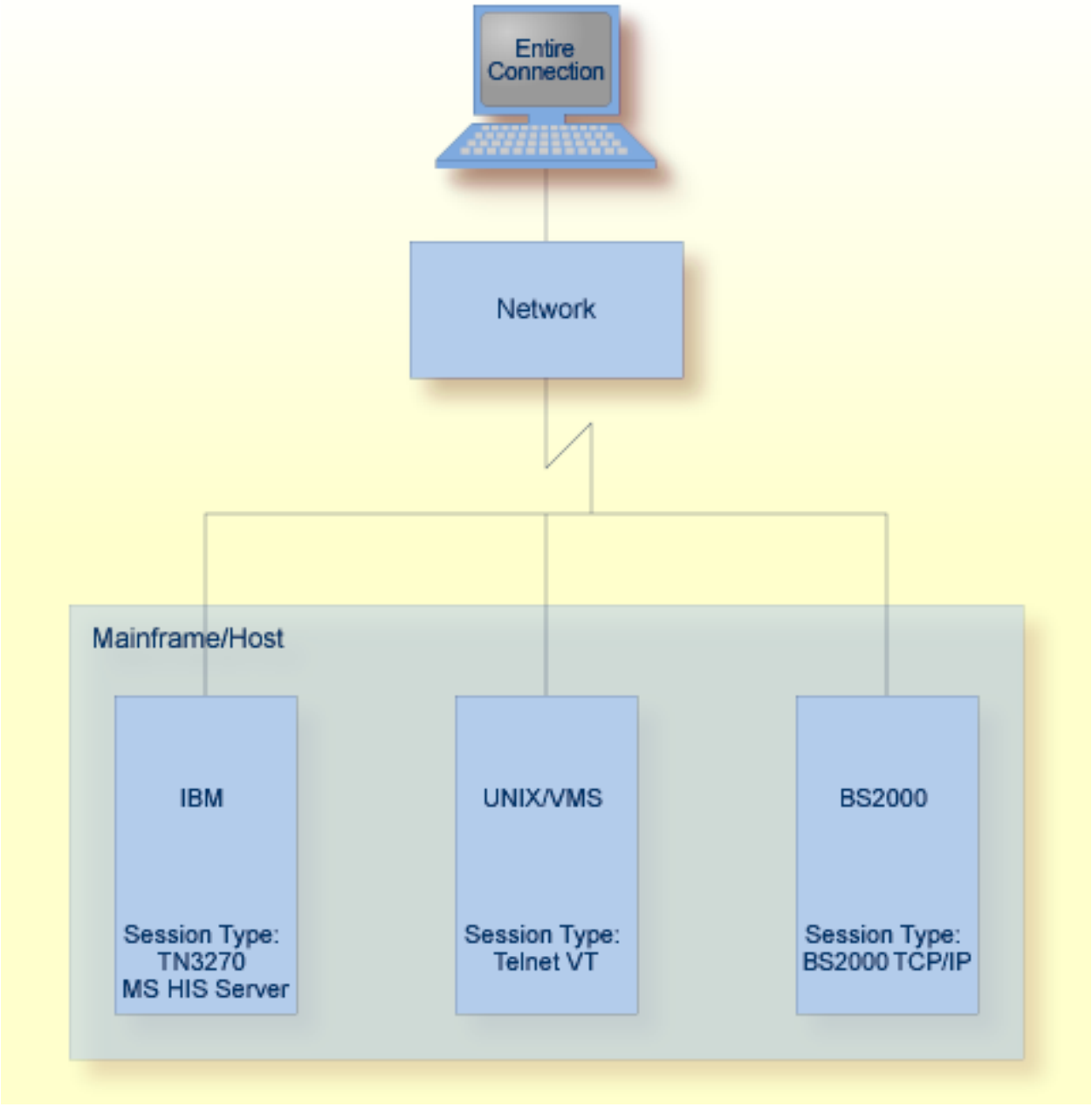
See also: communication parameters for the VTxxx serial port in the *Overview of Object Properties*.

2 Possible Setup Scenarios

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

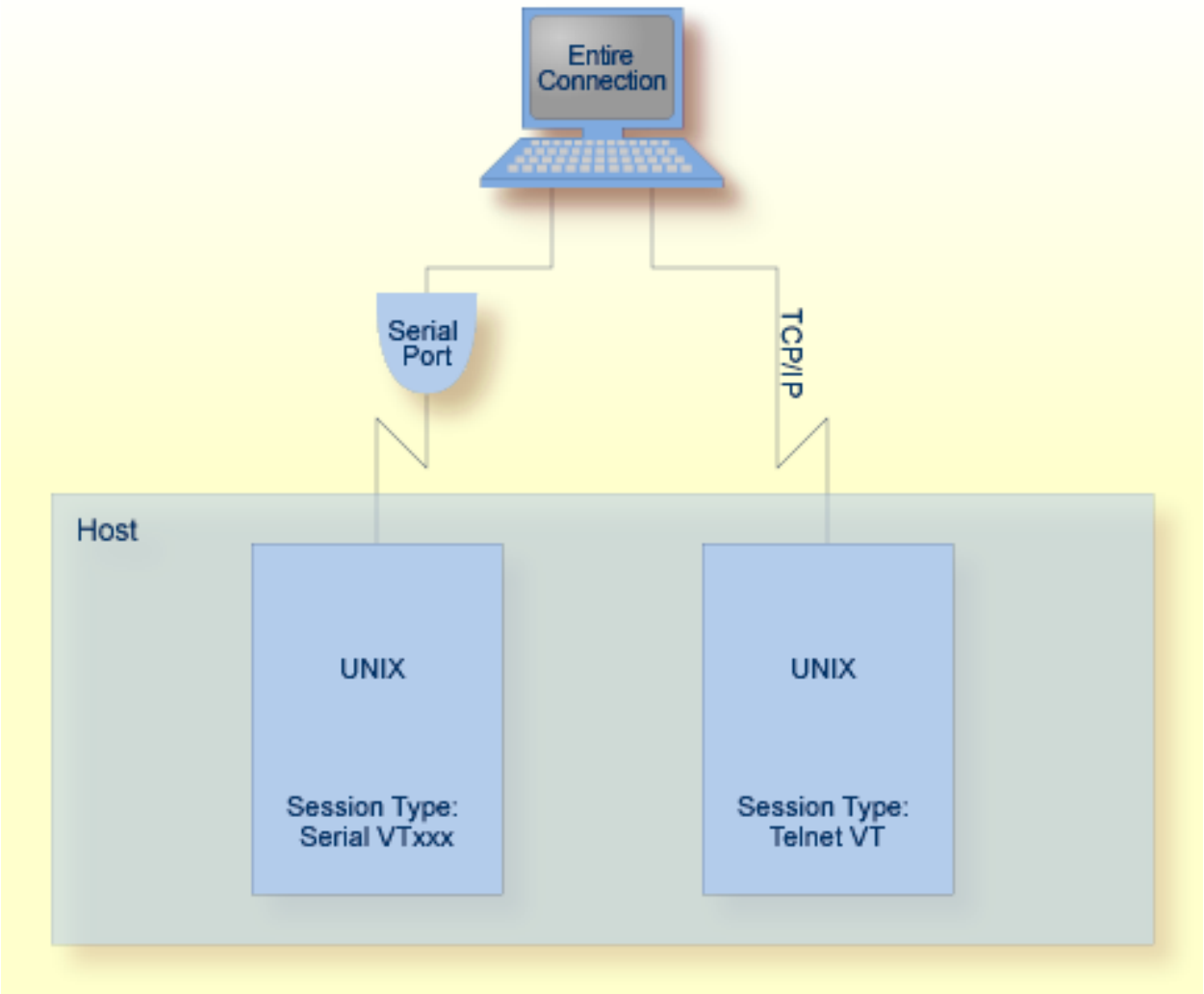
For each scenario, the diagram indicates the prerequisites and the session type you must define once Entire Connection is installed.

Communication via TCP/IP Networks



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+)

3 Installing Entire Connection

Prerequisites

Entire Connection 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:

Hardware	Any PC capable of running Microsoft Windows. Approximately 80 MB of free disk space. During installation, additional 80 MB are required in the Temp directory.
Operating System	Entire Connection can be installed on the following operating systems: ■ Microsoft Windows 7 Professional ■ Microsoft Windows 8 Professional ■ Microsoft Windows Server 2008 ■ Microsoft Windows Server 2012
Communication Method	At least one of the supported PC-to-host **communication methods**.
Data Transfer Software	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: ■ A version of Natural for Mainframes, Natural for UNIX or Natural for OpenVMS which supports the use of Entire Connection. ■ Natural for Mainframes: The version of Natural Connection that is compatible with the version of Natural you are using. **Note:** Natural Connection is automatically installed when Natural for UNIX or Natural for OpenVMS is installed. If you want to download data to Excel format or upload Excel data, Microsoft Excel 97 or higher must be installed on your PC. The Excel version depends on the operating system you are using.
Online Documentation	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 installation medium.

The setup program on the installation medium 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 4.5* folder. By default, this is *\Program Files\Software AG\Entire Connection 4.5\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 installation medium into your CD/DVD 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 installation medium.

3 After the installation, the administrator can define parameters, objects (for example, 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 and Uninstallation

InstallShield enables you to install and uninstall Entire Connection in silent mode. This also includes silent update installations. No user interaction is required in this mode.

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

To make sure that no user interaction is required during silent mode installation or uninstallation, it may be necessary to turn off or disable the user account control (UAC).

To install, update or uninstall in silent mode

1 Insert the Entire Connection installation medium in the CD/DVD drive of the PC on which you want to install or uninstall Entire Connection in silent mode.

2 Invoke the Command Prompt.

3 Change to the *\Windows\PCC* folder on the Entire Connection installation medium.

4 For a first-time installation or update installation, use the following installer command syntax:

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

Or:

To uninstall, use the following installer command syntax:

```
setup /s /w /x /v"/lvoicewarmup! %TEMP%\pccsilentnnnuninstmsi.log /qn"
```

The options have the following meanings:

`/s`	Silent mode (no user interaction).
`/L1033`	Optional. Language. "L1033" installs an English version of Entire Connection. "L1031" installs a German version.
`/w`	Optional. Used in combination with a preceding `start /WAIT` command. Causes *setup.exe* to wait until the first-time installation, update installation or uninstallation is finished.
`/x`	Uninstall mode. Uninstalls a previously installed product.
`/v`	List of parameters for the Windows installer. See below.
`/lvoicewarmup! %TEMP%\name.log`	Log file for the installation or uninstallation. It is not recommended to remove this parameter. For silent mode, it is recommended that you use the following log file names: ■ Installation: *pccsilentnnnmsi.log* ■ Uninstallation: *pccsilentnnnuninstmsi.log* where *nnn* in the log file name stands for the current version number of Entire Connection.
`SERIALNUMBER=serial-number`	Required for the installation. The serial number of Entire Connection. **Important:** For an update installation, you have to specify the serial number of the new version.
`INSTALLDIR=installation-folder`	The installation folder (the default is *\Program Files\Software AG\Entire Connection 4.5*). **Important:** For an update installation, you have to specify the same installation folder as for the original installation.

INSTALLLEVEL=*installlevel*	Optional. Possible values are 1 or 100 (the default is 1). The value 1 stands for the setup type **Typical**; the value 100 stands for the setup type **Complete** (see above).
/qn	Required. Silent mode for the Windows installer.

Examples

First-time installation

To start the first-time installation for the setup type **Complete** where *setup.exe* waits until the first-time installation is finished, enter the following command:

```
start /WAIT setup.exe /s /L1033 /w /v"/lvoicewarmup! %TEMP%\pccsilent4530msi.log
SERIALNUMBER=PCC4539999999999 INSTALLDIR=\"C:\Software AG\Entire Connection 4.5\"
INSTALLLEVEL=100 /qn"
```

Update installation

To start an update installation for the setup type **Typical** where *setup.exe* does not wait until the update installation is finished, enter the following command:

```
setup.exe /s /L1033 /w /v"/lvoicewarmup! %TEMP%\pccsilent4530msi.log
SERIALNUMBER=PCC4539999999999 INSTALLDIR=\"C:\Software AG\Entire Connection 4.5\"
/qn"
```

Uninstallation

To start an uninstallation where *setup.exe* waits until the uninstallation is finished, enter the following command:

```
start /WAIT setup /s /w /x /v"/lvoicewarmup! %TEMP%\pccsilent4530uninstmsi.log /qn"
```

Installation Log Files

By default, Entire Connection uses the following log files for additional information, especially in case of errors:

- The installation and uninstallation log files in `%TEMP%`, with the names as described above.
- The Windows event log.

Program Folders

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

\Program Files\Software AG\Entire Connection 4.5

Notes:

1. The Windows Explorer always shows a language-specific symbolic name for the program files folder. When the language of your operating system is English, the symbolic name is also "Program Files". This is different with other languages. For example, when the language of your operating system is German, the name "Programme" is shown in the Windows Explorer.
2. On a 64-bit Windows operating system, Entire Connection is installed in the following program files folder by default: "Program Files (x86)". The symbolic name, for example, for a German operating system is then "Programme (x86)".

Program Folder	Contents
\Entire Connection 4.5	**.exe* **.dll* API ActiveX control *PccAPI.ocx*.
\Entire Connection 4.5\doc	*Readme.txt* English and German online documentation, and the help files *Pccnnnxx.chm* (where *nnn* is the current version number and *xx* is the language code "US" for US English or "GR" for German).
\Entire Connection 4.5\netsetup	Client installation program *Setup.exe*. Only available when the option **Client Setup** has been specified during installation (setup type **Custom**).

The folders for the user data are by default installed at the following location:

\ProgramData\Software AG\Entire Connection

The *ProgramData* folder 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
certs	Files for TN3270 SSL/TLS support.
data	*Share411.sag*.
home	Empty after installation. **.log* Trace files (e.g. *Monnn.trc* and *Hllapi.trc*). Temporary files for host printer LU support.
proc	System procedure files. If specified during installation, this folder may also contain sample procedure files and sample Natural programs.
tables	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 restored.

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 or later, 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, or uninstall Entire Connection in **silent mode**.

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.

4 TN3270 SSL/TLS Support

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 contains several server certificate files from different Certification Authorities (CAs):

\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 negociated 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 *clientprivkey.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 4.5\OpenSSL.exe" genrsa -des3 -out
testkey.pem 2048
```

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 4.5\OpenSSL.exe" req -new -x509
-key clientprivkey.pem -out clientcert.crt -days 1095 -config openssl.cnf
```

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.

To export certificates

This description applies to Internet Explorer 9.

1 From the **Tools** menu, choose **Internet options**.
2 Go to the **Content** tab.
3 Choose the **Certificates** button.
4 Go to the **Trusted Root Certification Authorities** tab.
5 Select the certificate that you want to export.
6 Choose the **Export** button.

The Certificate Export Wizard appears.

7 Choose the **Next** button.
8 Select the **Base-64 Encoded X.509 (.CER)** option.
9 Choose the **Next** button.
10 Specify the name of the file into which the certificate is to be exported.
11 Choose the **Next** button.

12 On the last page of the wizard, choose the **Finish** button.

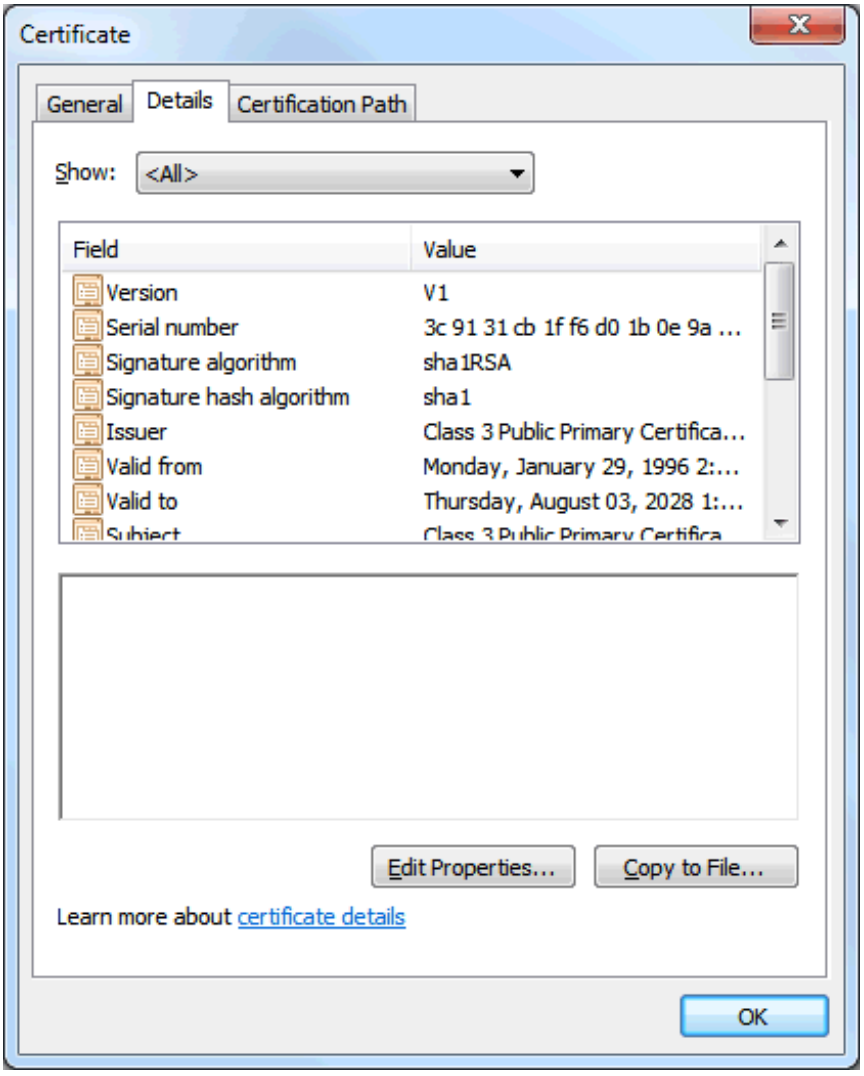
Getting Root Certificates from Certification Authorities

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

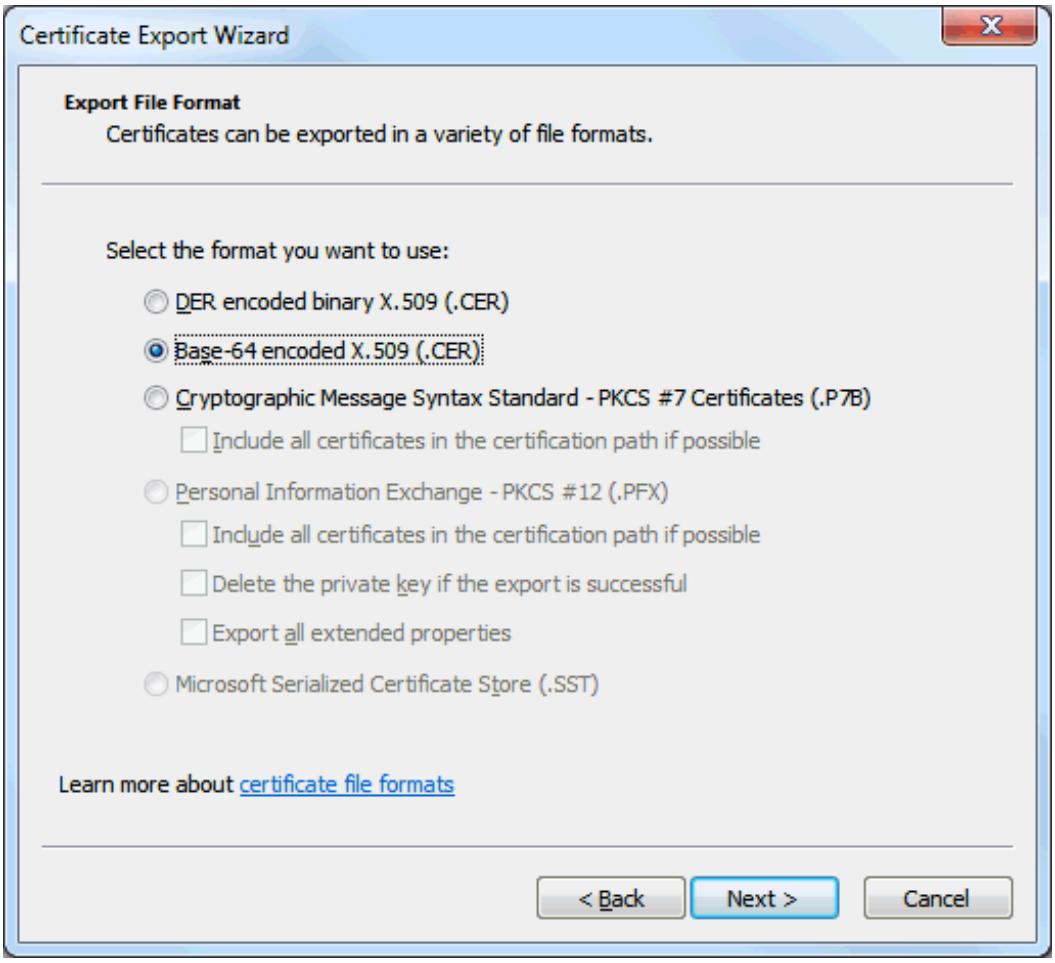
1 Open the certificate and display the **Details** property sheet. Example:



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.

5 Telnet SSH Support

Entire Connection supports Telnet SSH for sessions of type Telnet VTxxx. This allows a secure connection between Entire Connection and a server. In an SSH 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.

You enable SSH by selecting the connection type SSH for your Telnet VTxxx session (see the description of the **General** page for Telnet VTxxx in *Communication Parameters* in the *Overview of Object Properties*).

Telnet VTxxx sessions with the connection type SSH require that the option **Return key send option** is set to `CR` (see the description of the **Terminal** page for VT types in *Session Properties* in the *Overview of Object Properties*), otherwise the sessions may not work properly. `CR` is the default setting when you create new sessions of type Telnet VTxxx. A different setting might be in effect, however, if you change the connection type of an existing Telnet VTxxx session from Telnet to SSH, or if you duplicate a Telnet VTxxx session; in these cases, you have to make sure that `CR` is used.

A prerequisite for using SSH is that you have a server with an SSH-enabled port. Entire Connection supports the SSH protocol version 2.0.

The following SSH authentication methods are supported:

- "password" authentication
- "keyboard-interactive" authentication
- "publickey" authentication

Depending on your SSH host configuration, one or more authentication methods are offered from the host. The "publickey" authentication method is the preferred method. It will be used when a private key file has been specified (see the description of the **Security** page for Telnet VTxxx in *Communication Parameters* in the *Overview of Object Properties*).

To use the SSH "publickey" authentication method, you must have a public/private key pair. You can generate such a key pair using, for example, OpenSSH tools or PuTTY. We strongly recommend that you protect the private key file with a pass phrase. It is important that the key files have the OpenSSH format.

The private key file has to be deployed to the *\Software AG\Entire Connection\certs* folder of your user's local *appdata* folder, and the name of the private key file has to be specified on the **Security** page of the Telnet VTxxx communication parameters.

The content of the user's public key file has to be added to the *$HOME/.ssh/authorized_keys* file on the server. Make sure that the public key is one line in the *authorized_keys* file. It is important that the folders *$HOME* and *$HOME/.ssh* and the *authorized_keys* file have appropriate permission attributes. The permission attributes 700 for the folders and 400 for the file seem to work on most servers.

The authentication methods "password" and "keyboard-interactive" are used in this order if offered by the server and if the "publickey" authentication method does not get preference because you have entered the name of a private key file on the **Security** page of the Telnet VTxxx communication parameters. If you want to disable authentication methods, see the other options on the **Security** page.

6 Backup and Restore

The information in this chapter is helpful, if you want to back up your settings and data on a regular basis. It is also helpful, if want to install Entire Connection on a new PC and you want to reuse your existing settings and data from your old PC. In this case, you have to back up all required items on the old PC and restore them on the new PC.

What Can be Backed Up?

You can back up and restore the following:

- **Share File**
  The default share file that is delivered with Entire Connection is modified, for example, when you define a new host session, when you modify the current color scheme or key scheme, or when you define a different directory for your procedure files. The share is also modified when the administrator changes, for example, the user properties or host printer sessions. See also *About the Object Types*.
- **Procedure Files**
  You can create your own procedure files, or you can modify the existing procedure files which are delivered with Entire Connection. See also *Procedure Files*.
- **Security Certificates**
  Certificates are used for a secure connection between Entire Connection and a Telnet server (SSL and SSH). See also *TN3270 SSL/TLS Support* and *Telnet SSH Support*.
- **Startup Parameters for the Terminal Application**
  A shortcut on your desktop for the terminal application is helpful if you want to start the terminal application with special parameters. See also *Startup Parameters*.

Backing Up a Standard Installation

1. Copy the folder *\ProgramData\Software AG\Entire Connection* with all of its subfolders to a backup location of your choice. By default, this folder also contains your share file. If certificates have been created for secure connections with SSL, this folder also contains the certificates for SSL.
2. If certificates have been created for secure connections with SSH, you also have to copy the folder *Software AG\Entire Connection\certs* which can be found in the user's local *AppData* folder (for example, *C:\Users\username\AppData\Local*) to a backup location of your choice.

Note: The folders *ProgramData* and *AppData* are hidden folders. They are only shown in the Explorer when you have activated the corresponding setting in the folder options of the Explorer.

Additional copy steps may be required in the following cases:

1. You have renamed your share file or stored it in a different location.

   By default, the share file is located in the folder *\ProgramData\Software AG\Entire Connection\data* and has the name *share411.sag*. It it possible to change both, the location and the name of the share file. If you cannot find your share file at once, start the Configuration Manager (either directly via the Windows **Start** menu, or via the **Utilities** menu of the terminal application). The location and name of your share file is then shown in the left pane, at the top of the tree.
2. You have created procedure files, but they are not stored in *\ProgramData\Software AG\Entire Connection\data*.

   If you do not know where to find your procedure files, start the Configuration Manager and display your user properties. The path to your procedure file is then shown on the **Procedure** page.

   Additional procedure files (that is, files with the extension *.NCP*) may also be located in the installation directory of Entire Connection (that is, in *\Program Files\Software AG\Entire Connection 4.5*).
3. You have created a shortcut for the terminal application on your desktop and have defined specific startup parameters.

   Open the properties of the shortcut and note down the startup parameters. Or copy the shortcut to a backup location of your choice.

Restoring a Standard Installation

1. Copy the folders you have backed up to the approriate locations on the new PC. For example, copy them to:
   - *C:\ProgramData\Software AG\Entire Connection*
   - *C:\Users\username\AppData\Local\Software AG\Entire Connection\certs* (only required if SSH is used)
2. Start the Configuration Manager, display your user properties, go to the **Procedure** page, and check the settings for the procedure directory and the log & trace directory. It may be required to change these settings for the new PC. It is recommended that you use the following default settings: **Use Windows common application data folder** for the procedure files and **Use Windows local user application data folder** for the log and trace files.
3. If required, create a new shortcut for the terminal application on your desktop, with the same startup parameters as on the old PC.

   Or if you have backed up the shortcut, copy it to your desktop. Open the properties of the shortcut and make sure that the path to *Pcctterminal.exe* is correct.