

# **Entire Connection**

## **Installation**

Version 9.1.4

Oktober 2021

Dieses Dokument gilt für Entire Connection ab Version 9.1.4.

Hierin enthaltene Beschreibungen unterliegen Änderungen und Ergänzungen, die in nachfolgenden Release Notes oder Neuausgaben bekanntgegeben werden.

Copyright © 1984-2021 Software AG, Darmstadt, Deutschland und/oder Software AG USA, Inc., Reston, VA, USA, und/oder ihre Tochtergesellschaften und/oder ihre Lizenzgeber.

Der Name Software AG und die Namen der Software AG Produkte sind Marken der Software AG und/oder Software AG USA Inc., einer ihrer Tochtergesellschaften oder ihrer Lizenzgeber. Namen anderer Gesellschaften oder Produkte können Marken ihrer jeweiligen Schutzrechtsinhaber sein.

Nähere Informationen zu den Patenten und Marken der Software AG und ihrer Tochtergesellschaften befinden sich unter <http://documentation.softwareag.com/legal/>.

Diese Software kann Teile von Software-Produkten Dritter enthalten. Urheberrechtshinweise, Lizenzbestimmungen sowie zusätzliche Rechte und Einschränkungen dieser Drittprodukte können dem Abschnitt "License Texts, Copyright Notices and Disclaimers of Third Party Products" entnommen werden. Diese Dokumente enthalten den von den betreffenden Lizenzgebern oder den Lizenzen wörtlich vorgegebenen Wortlaut und werden daher in der jeweiligen Ursprungssprache wiedergegeben. Für einzelne, spezifische Lizenzbeschränkungen von Drittprodukten siehe PART E der Legal Notices, abrufbar unter dem Abschnitt "License Terms and Conditions for Use of Software AG Products / Copyrights and Trademark Notices of Software AG Products". Diese Dokumente sind Teil der Produktdokumentation, die unter <http://softwareag.com/licenses> oder im Verzeichnis der lizenzierten Produkte zu finden ist.

Die Nutzung dieser Software unterliegt den Lizenzbedingungen der Software AG. Diese Bedingungen sind Bestandteil der Produktdokumentation und befinden sich unter <http://softwareag.com/licenses> und/oder im Wurzelverzeichnis des lizenzierten Produkts.

**Dokument-ID: PCC-INSTALL-914-20210929DE**

# Inhaltsverzeichnis

Vorwort .....	v
1 Über diese Dokumentation .....	1
Dokumentationskonventionen .....	2
Online-Informationen und Support .....	2
Datenschutz .....	4
2 Unterstützte Kommunikationsmethoden .....	5
TN3270(E) .....	6
Telnet VTxxx .....	6
BS2000 TCP/IP .....	6
3 Mögliche Installationsszenarios .....	9
Kommunikation über TCP/IP-Netze .....	11
Terminal-Emulation für UNIX-Systeme .....	12
4 Entire Connection installieren .....	13
Systemvoraussetzungen .....	14
Entire Connection für den Administrator installieren .....	15
Stille Installation und Deinstallation .....	17
Programmordner .....	19
Umgebungsvariablen .....	21
Entire Connection aktualisieren (Upgrade) .....	21
Entire Connection auf einer Client-Workstation installieren .....	21
Entire Connection deinstallieren .....	22
Versionsportabilität und Parallelität .....	22
5 SSL/TLS-Unterstützung für TN3270 .....	27
In Entire Connection unterstützte SSL/TLS-Funktionalität .....	28
Eine TN3270-Session mit SSL/TLS aufbauen .....	29
SSL/TLS für Entire Connection konfigurieren .....	29
Server-Zertifikate mit Entire Connection überprüfen .....	30
Client-Authentifizierung .....	31
Mehr zu Zertifikaten .....	33
6 SSL/TLS-Unterstützung für BS2000 .....	37
7 SSH-Unterstützung für Telnet .....	39
8 Sichern und Wiederherstellen .....	41
Was kann gesichert werden? .....	42
Standardinstallation sichern .....	42
Standardinstallation wiederherstellen .....	43



---

# Vorwort

---

Die folgenden Themen bieten alle erforderlichen Informationen zur Installation von Entire Connection.

**Unterstützte Kommunikationsmethoden**

**Mögliche Installationsszenarios**

**Entire Connection installieren**

**SSL/TLS-Unterstützung für TN3270**

**SSL/TLS-Unterstützung für BS2000**

**SSH-Unterstützung für Telnet**

**Sichern und Wiederherstellen**

---

# 1 Über diese Dokumentation

---

■ Dokumentationskonventionen .....	2
■ Online-Informationen und Support .....	2
■ Datenschutz .....	4

## Dokumentationskonventionen

---

Konvention	Beschreibung
<b>Fettschrift</b>	>Kennzeichnet Elemente auf einem Bildschirm.
Nichtproportionale Schrift	Kennzeichnet Namen und Orte von Diensten im Format <i>Ordner.Unterordner.Dienst</i> , Programmierschnittstellen (APIs), Namen von Klassen, Methoden und Properties in Java.
<i>Kursivschrift</i>	Kennzeichnet:  Variablen, für die Sie situations- oder umgebungsspezifische Werte angeben müssen. Neue Begriffe, wenn sie erstmals im Text auftreten. Verweise auf andere Dokumentationsquellen.
Nichtproportionale Schrift	Kennzeichnet:  Text, den Sie eingeben müssen. Meldungen, die vom System angezeigt werden. Programmcode.
{ }	Zeigt eine Reihe von Auswahlmöglichkeiten an, von denen Sie eine auswählen müssen. Geben Sie nur die innerhalb der geschweiften Klammern vorhandenen Informationen ein. Geben Sie nicht die Klammersymbole { } ein.
	Trennt zwei sich gegenseitig ausschließende Auswahlmöglichkeiten in einer Syntaxzeile voneinander ab. Geben Sie eine der Auswahlmöglichkeiten ein. Geben Sie nicht das Symbol   ein.
[ ]	Zeigt eine oder mehrere Optionen an. Geben Sie nur die innerhalb der eckigen Klammern vorhandenen Informationen ein. Geben Sie nicht die Klammersymbole [ ] ein.
...	Zeigt an, dass Sie mehrere Auswahlmöglichkeiten desselben Typs eingeben können. Geben Sie nur die Informationen ein. Geben Sie nicht die drei Auslassungspunkte (...) ein.

## Online-Informationen und Support

---

### Dokumentationswebsite der Software AG

Sie finden die Dokumentation zu den Produkten der Software AG auf der Dokumentationswebsite der Software AG unter <https://documentation.softwareag.com>.



## Empower, die Produktsupportwebsite der Software AG

Falls Sie noch kein Benutzerkonto für Empower haben, können Sie eine E-Mail an [empower@softwareag.com](mailto:empower@softwareag.com) senden. Geben Sie darin Ihren Namen, den Namen Ihrer Firma und deren E-Mail-Adresse an und beantragen Sie die Einrichtung eines Benutzerkontos.

Wenn Sie ein Benutzerkonto erhalten haben, können Sie den eService-Bereich von Empower unter <https://empower.softwareag.com/> aufrufen und dort Support-Fälle online öffnen.

Informationen zu Software AG-Produkten finden Sie auf der Empower-Produktsupportwebsite unter <https://empower.softwareag.com>.

Unter **Products & Documentation** können Sie Anträge bezüglich Produktmerkmalen und Produktverbesserungen einreichen, Informationen über die Verfügbarkeit von Produkten abrufen und Produkte herunterladen.

Im **Knowledge Center** finden Sie Informationen zu Programmkorrekturen (Fixes) und frühzeitige Warnungen, technische Abhandlungen (Papers) und Artikel aus der Wissensdatenbank.

Wenn Sie noch Fragen haben und telefonisch mit uns Kontakt aufnehmen möchten, können Sie im Kontaktverzeichnis des Globalen Supports unter [https://empower.softwareag.com/public\\_directory.aspx](https://empower.softwareag.com/public_directory.aspx) eine der dort für Ihr Land angegebenen örtlichen oder gebührenfreien Telefonnummern auswählen.

## Software AG TECHcommunity

Auf der Website der Software AG TECHcommunity unter <http://techcommunity.softwareag.com> finden Sie Dokumentationen und andere technische Informationen.

- Sie können auf Produktdokumentationen zugreifen, wenn Sie die erforderlichen Authentifizierungsdaten für die TECHcommunity haben. Andernfalls müssen Sie sich registrieren und "Documentation" als Interessengebiet angeben.
- Sie erhalten Zugang zu Artikeln, Code-Beispielen, Demos und Lernprogrammen.
- Sie können an von Software AG-Experten moderierten Online-Diskussionsforen teilnehmen, um Fragen zu stellen, über bewährte Methoden und Prozesse (Best Practices) zu diskutieren und zu erfahren, wie andere Kunden die Technologien der Software AG nutzen.
- Sie können Links auf externe Websites benutzen, die sich mit offenen Standards und Web-Technologien befassen.

## Datenschutz

---

Die Produkte der Software AG stellen Funktionen zur Verarbeitung von personenbezogenen Daten gemäß der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union zur Verfügung. Gegebenenfalls sind in der betreffenden Systemverwaltungsdokumentation entsprechende Schritte dokumentiert.

## 2      Unterstützte Kommunikationsmethoden

---

■ TN3270(E) .....	6
■ Telnet VTxxx .....	6
■ BS2000 TCP/IP .....	6

## TN3270(E)

---

Entire Connection unterstützt die TCP/IP-Kommunikation mit TN3270 und TN3270E für Anzeige-Sessions. Unterstützt wird auch die TCP/IP-Kommunikation mit TN3270E für Host-Drucker-Sessions.

Sie können jeden Netzwerkadapter verwenden, der von jeder TCP/IP-Stack-Software unterstützt wird, die die WinSock 2-Schnittstelle zur Verfügung stellt. Erweiterte Attribut-Bytes (EABs) werden unterstützt.

Die TCP/IP-Stack-Software muss installiert und aktiv sein, damit die Terminal-Emulation gestartet werden kann.

Für die IBM-Host-Drucker-Emulation müssen Sie generische, spezifische oder assoziierte Drucker auf dem Telnet-Server definieren. Dies ist in Ihrer Telnet-Server-Dokumentation beschrieben.

Siehe auch: Kommunikationsparameter für TN3270(E) im Abschnitt *Übersicht der Objekteigenschaften*.

## Telnet VTxxx

---

Entire Connection unterstützt die VT100-, VT220-, VT320-Kommunikation mit jedem Netzwerkadapter, der von jeder TCP/IP-Stack-Software unterstützt wird, die die WinSock 2-Schnittstelle zur Verfügung stellt.

Die TCP/IP-Stack-Software muss installiert und aktiv sein, damit die Terminal-Emulation gestartet werden kann.

Siehe auch: Kommunikationsparameter für Telnet VTxxx im Abschnitt *Übersicht der Objekteigenschaften*.

## BS2000 TCP/IP

---

Diese Kommunikationsmethode emuliert ein Standard-9750-Terminal mit einer Bildschirmgröße von 24 x 80 Zeichen ohne Farben. Lokales Drucken wird nicht unterstützt. Zusätzlich zu den Standard-9750-Terminal-Funktionen, werden die folgenden Funktionen der 975x-Familie unterstützt:

- 80 FTZ pro Zeile
- 20 P-Tasten
- 24 F-Tasten

- Inversdarstellung
- Speicherplatz für die P-Register entsprechend dem 9756-Terminal

In Natural-Umgebungen wird außerdem der Farbterminaltyp 9763 (7 Bit) unterstützt. Hierfür muss Natural Version 3 oder höher installiert sein. Standardmäßig benutzt Natural den Terminaltyp 9750 (monochrom). Den Terminaltyp 9763 können Sie mit dem folgenden Natural-Terminalkommando aktivieren (entweder in einem Schirm oder einem Programm):

```
%T=9763
```

Wenn Sie den Terminaltyp 9763 aktivieren, sollten Sie zusätzlich die Funktionstasten F1 bis F20 mit dem folgenden Natural-Terminalkommando aktivieren:

```
%KN
```

Entire Connection unterstützt die TCP/IP-Kommunikation zu BS2000-Hosts mit jedem Netzwerkdapter, der von jeder TCP/IP-Stack-Software unterstützt wird, die die WinSock 2-Schnittstelle zur Verfügung stellt.

Voraussetzung auf der Host-Seite ist das Kommunikationssystem BCAM Version V.11, das die Verbindung mit dem Host herstellt (erhältlich mit dem Produkt DCAM).

Für das Aktivieren der Terminal-Emulation ist keine weitere Software erforderlich.

Wählen Sie das vordefinierte Tastenschema BS2000KEYS, um die Terminal-Emulationstasten an die einer BS2000-Tastatur anzupassen.

Siehe auch: Kommunikationsparameter für BS2000 TCP/IP im Abschnitt *Übersicht der Objekteigenschaften*.



# 3

## Mögliche Installationsszenarios

---

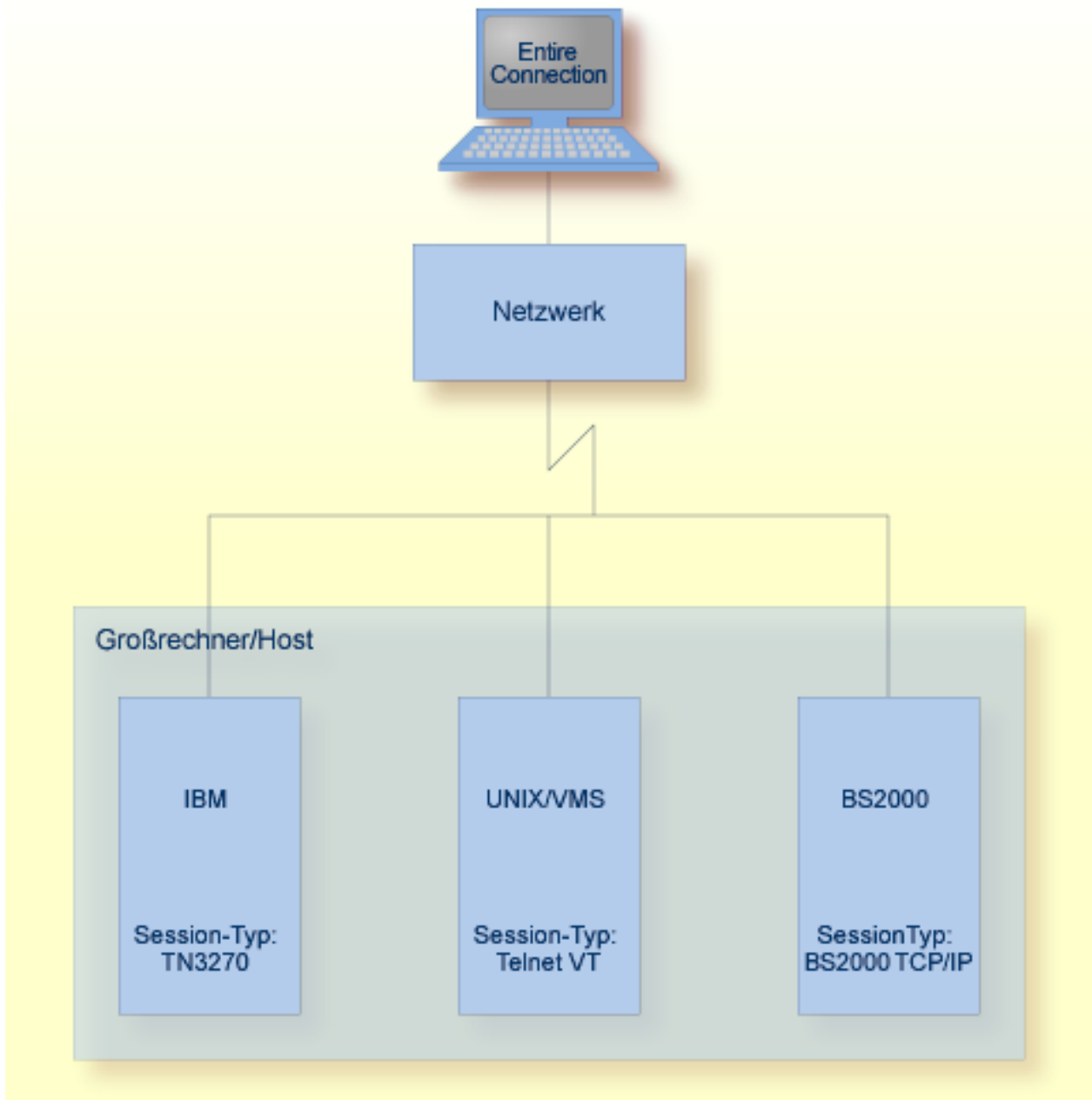
■ Kommunikation über TCP/IP-Netze .....	11
■ Terminal-Emulation für UNIX-Systeme .....	12

Entire Connection kann in verschiedenen Netzwerkkonfigurationen installiert werden. Die Diagramme in diesem Abschnitt veranschaulichen die verschiedenen Möglichkeiten.

Jedes Diagramm enthält Angaben zu den Systemvoraussetzungen und den Session-Typ, den Sie nach der Installation von Entire Connection definieren müssen.



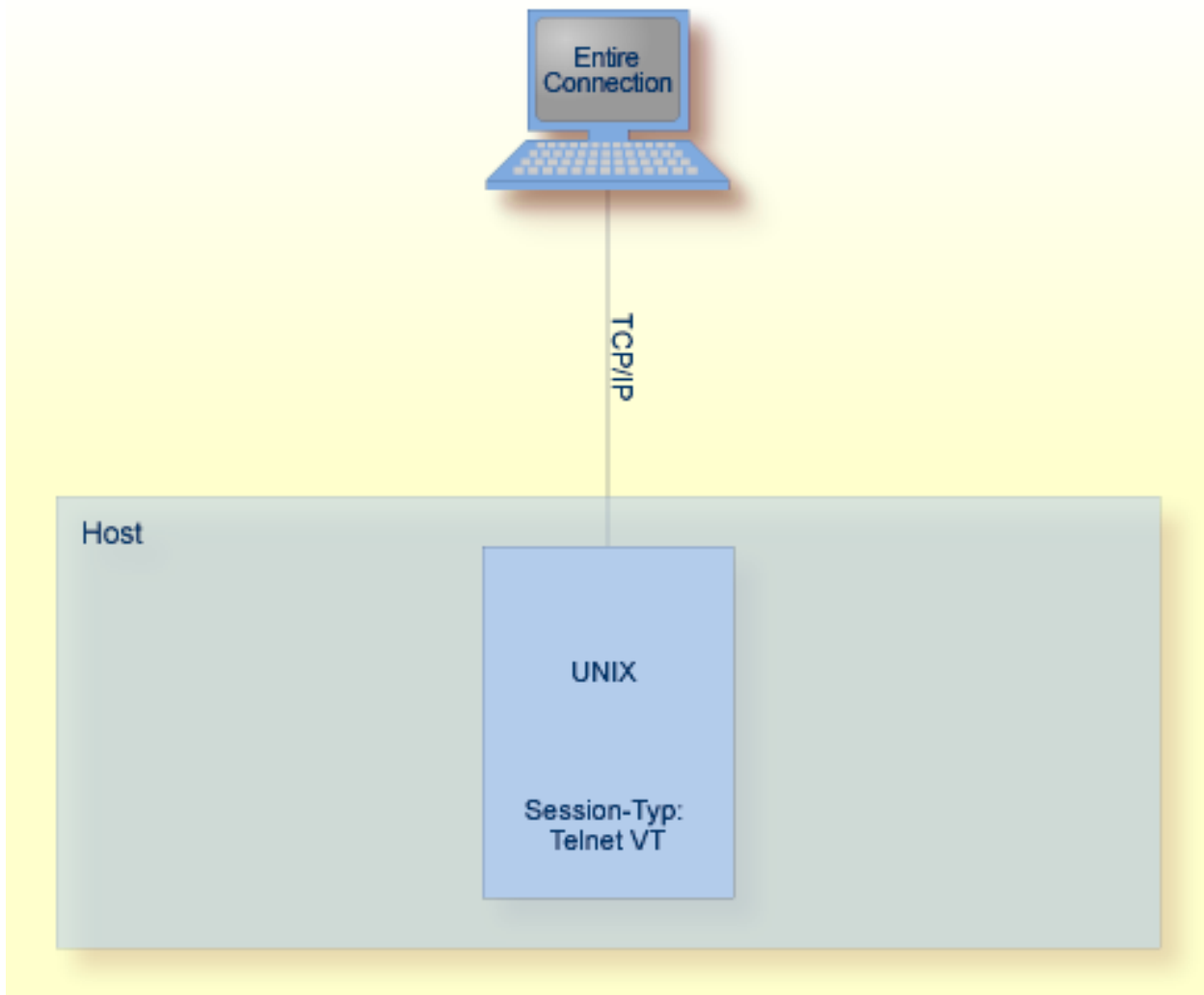
## Kommunikation über TCP/IP-Netze



**Anmerkung:** Session-Typ BS2000 TCP/IP bietet nicht die komplette 975x-Funktionalität.

## Terminal-Emulation für UNIX-Systeme

---



UNIX-Terminal-Emulation:

- VT100
- VT220
- ANSI-Farbunterstützung (VT340+)

## 4 Entire Connection installieren

---

■ Systemvoraussetzungen .....	14
■ Entire Connection für den Administrator installieren .....	15
■ Stille Installation und Deinstallation .....	17
■ Programmordner .....	19
■ Umgebungsvariablen .....	21
■ Entire Connection aktualisieren (Upgrade) .....	21
■ Entire Connection auf einer Client-Workstation installieren .....	21
■ Entire Connection deinstallieren .....	22
■ Versionsportabilität und Parallelität .....	22

## Systemvoraussetzungen

Entire Connection ist eine 32-Bit-Anwendung. Bei einer 64-Bit-Version von Windows läuft Entire Connection unter WOW64. WOW64 ist ein x86-Emulator, der es ermöglicht, 32-Bit-Anwendungen mit einer 64-Bit-Version von Windows auszuführen.

Die folgende Hardware und Software ist für die Installation und den Einsatz von Entire Connection erforderlich:

<b>Hardware</b>	Ein PC auf dem Microsoft Windows lauffähig ist und der ca. 80 MB freien Speicherplatz hat. Während der Installation sind weitere 80 MB im Temp-Verzeichnis erforderlich.
<b>Betriebssystem</b>	<p>Entire Connection unterstützt die folgenden 64-Bit-Betriebssystemplattformen:</p> <ul style="list-style-type: none"> <li>■ Microsoft Windows 10</li> <li>■ Microsoft Windows Server 2016</li> <li>■ Microsoft Windows Server 2019</li> </ul> <p>Bevor Sie mit der Installation beginnen, achten Sie darauf, dass alle aktuellen Windows-Updates auf der Maschine installiert sind, auf der Sie Entire Connection installieren wollen.</p> <p>Die Laufzeitkomponenten von Entire Connection sind immer 32-Bit-Anwendungen, auch auf 64-Bit-Plattformen.</p> <p>Home-Editionen von Microsoft Windows werden nicht unterstützt.</p>
<b>Kommunikationsmethode</b>	Mindestens eine der unterstützten <a href="#">Methoden für die Kommunikation</a> zwischen PC und Host.
<b>Datentransfer-Software</b>	<p>Wenn Sie Daten zwischen dem Host und Ihrem PC übertragen wollen, müssen die folgenden Produkte der Software AG auf dem Host installiert sein, mit dem der PC verbunden ist:</p> <ul style="list-style-type: none"> <li>■ Eine Version von Natural für Großrechner, Natural für UNIX oder Natural für OpenVMS, mit der die Benutzung von Entire Connection unterstützt wird.</li> <li>■ Natural für Großrechner: die Version von Natural Connection, die mit Ihrer Natural-Version kompatibel ist.</li> </ul> <p><b>Anmerkung:</b> Natural Connection wird automatisch installiert, wenn Natural für UNIX oder Natural für OpenVMS installiert wird.</p> <p>Wenn Sie Daten nach Excel herunterladen oder Daten im Excel-Format hochladen wollen, muss Excel 97 oder eine höhere Version auf Ihrem PC installiert sein. Die Excel-Version ist abhängig von Ihrem Betriebssystem.</p>
<b>Online-Dokumentation</b>	Ein Browser zum Lesen der Dokumentation von Entire Connection im HTML-Hilfe-Format.

## Entire Connection für den Administrator installieren

Lesen Sie vor der Installation zuerst die Datei *Install\_gr.txt* auf dem Installationsmedium von Entire Connection.

Das Setup-Programm auf dem Installationsmedium installiert Entire Connection für einen Benutzer, den Administrator. Im einfachsten Fall ist dies eine einzelne Installation auf einem lokalen PC, wobei der Benutzer auch gleich Administrator ist und alle erforderlichen Objekttypen selbst definiert.

Wenn mehrere Benutzer mit der selben Installation arbeiten sollen, kann der Administrator Entire Connection auf einem Netzwerk-File-Server oder einem freigegebenen Laufwerk installieren und das System für alle Benutzer vorbereiten, die in der Lage sein sollen, Entire Connection von verschiedenen Client-Workstations aus zu starten. Für diese Art der Installation müssen Sie den Setup-Typ **Komplett** wählen (oder den Setup-Typ **Benutzer** und die Option **Client-Setup** markieren). Die Option **Client-Setup** erstellt den Ordner *netsetup* im Ordner *Entire Connection*. Standardmäßig ist das *\Program Files\Software AG\Entire Connection\netsetup*. Der Ordner *netsetup* enthält das Client-Installationsprogramm *Setup.exe*. Jeder Benutzer kann dieses Programm von der eigenen Client-Workstation aus aufrufen. Es registriert Entire Connection auf der Client-Workstation und erstellt einen Ordner für Entire Connection im Windows-Startmenü. Nach dem Start sucht *Setup.exe* nach der Datei *Readme.doc* im Ordner *netsetup*. Wenn sie gefunden wird, wird ihr Inhalt angezeigt. Der Administrator kann diese Datei dafür verwenden, den Benutzern umgebungsspezifische Informationen (z.B. Benutzernamen, Vorgaben oder Session-Namen) für ihre Arbeit mit Entire Connection mitzuteilen. Weitere Informationen zur Installation auf einer Client-Workstation finden Sie später in diesem Abschnitt unter [Entire Connection auf einer Client-Workstation installieren](#).

Bei der Installation stehen folgende Setup-Typen zur Verfügung:

Setup-Typ	Installiert
Standard (Vorgabe)	Die gängigsten Optionen. Empfohlen für die meisten Benutzer.
Komplett	Alle Optionen. Erforderlich wenn mehrere Benutzer mit der selben Installation arbeiten sollen.
Benutzer	Sie können wählen, welche Optionen Sie installieren möchten. Empfohlen für fortgeschrittene Benutzer.

Die folgende Tabelle zeigt die Optionen, die bei einem bestimmten Setup-Typ installiert werden (bzw. installiert werden können):

Option	Standard	Komplett	Benutzer
Konfigurationsmanager	X	X	X
Terminal	X	X	X
Formatkonverter	X	X	X
Host-Drucker-LU-Unterstützung		X	(X)
Beispielprozedurdateien	X	X	X
Beispiel-Natural-Programme	X	X	X
Client-Setup		X	(X)

Die Standardeinstellung beim Setup-Typ **Benutzer** ist dieselbe wie beim Setup-Typ **Standard**.

Die folgenden Optionen werden immer installiert: Konfigurationsmanager und Terminal. Beim Setup-Typ **Benutzer** ist es nicht möglich, diese Optionen zu deaktivieren.

#### ➤ Entire Connection installieren

- 1 Beenden Sie alle aktiven Windows-Anwendungen.
- 2 Legen Sie das Installationsmedium von Entire Connection in Ihr CD-/DVD-Laufwerk ein.

Das Setup-Programm startet automatisch und führt Sie durch die Installation.

Wenn die automatische Startoption bei Ihnen ausgeschaltet ist, müssen Sie *Setup.exe* selbst ausführen. Diese Datei befindet sich im obersten Verzeichnis des Installationsmediums.

- 3 Nach der Installation kann der Administrator die Parameter, Objekte (z.B. Sessions), Benutzergruppen und Zugriffsrechte für alle Benutzer definieren (siehe *Konfigurationsmanager*). Als Erstes sollte überprüft werden, ob die Einstellungen im Dialogfeld **Systemvoreinstellungen** für alle Benutzer gültig sind. Es ist wichtig, dass alle Benutzer auf die hier definierten Verzeichnisse für die Prozedurdateien und die Log- und Trace-Dateien zugreifen können.
- 4 Wenn Sie die Benutzerprofile der Version 3.1 übernehmen wollen, müssen Sie dies direkt nach der Installation tun. Weitere Informationen hierzu finden Sie im Abschnitt *Konfigurationsmanager* unter *Bestehende Benutzerprofile übernehmen*.
- 5 Bei einem Upgrade von Entire Connection 4.3.1 oder einer früheren Version müssen Sie einen Share-Datei-Upgrade durchführen. Ansonsten stehen Ihnen bestimmte neue Funktionen nicht zur Verfügung. Weitere Informationen hierzu finden Sie im Abschnitt *Konfigurationsmanager* unter *Share-Datei-Upgrade*.

## Stille Installation und Deinstallation

Mit InstallShield können Sie Entire Connection im stillen Modus installieren und deinstallieren. Dies beinhaltet auch stille Update-Installationen. In diesem Modus ist kein Benutzereingriff erforderlich.

Für eine stille Installation oder Deinstallation dürfen Sie nicht *setup.exe* im obersten Verzeichnis des Installationsmediums benutzen. Benutzen Sie statt dessen *setup.exe* im Verzeichnis `\Windows\PCC` des Installationsmediums.

Um sicherzustellen, dass kein Benutzereingriff während des stillen Installationsmodus oder Deinstallationsmodus erforderlich ist, kann es notwendig sein, die Benutzerkontensteuerung (UAC) abzuschalten oder zu deaktivieren.

### ➤ Im stillen Modus installieren oder deinstallieren

- 1 Legen Sie das Installationsmedium von Entire Connection in das CD-/DVD-Laufwerk des PCs ein, auf dem Sie Entire Connection im stillen Modus installieren oder deinstallieren möchten.
- 2 Rufen Sie die Eingabeaufforderung (DOS-Fenster) auf.
- 3 Wechseln Sie in das Verzeichnis `\Windows\PCC` des Installationsmediums.
- 4 Für eine Erstinstallation oder Update-Installation geben Sie den folgenden Befehl ein:

```
setup.exe /s /L1033 /w /v"/lvoicewarmup! %TEMP%\pccsilentnnmsi.log
SERIALNUMBER=seriennummer INSTALLDIR=installationsverzeichnis
INSTALLLEVEL=installlevel /qn"
```

Oder:

Für eine Deinstallation geben Sie den folgenden Befehl ein:

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

Die Optionen haben die folgende Bedeutung:

/s	Stiller Modus (kein Benutzereingriff).
/L1031	Optional. Language (Sprache). "L1031" installiert eine deutsche Version von Entire Connection. "L1033" installiert eine englische Version.

/w	Optional. Wird in Verbindung mit einem vorhergehenden <code>start /WAIT</code> -Befehl benutzt. <i>setup.exe</i> wird hiermit veranlasst so lange zu warten, bis die Erstinstallation, Update-Installation oder Deinstallation fertig ist.
/x	Deinstallationsmodus. Deinstalliert ein vorher installiertes Produkt.
/v	Parameterliste für den Windows-Installer. Siehe unten.
/lvoicewarmup! %TEMP%\name.log	<p>Logdatei für die Installation oder Deinstallation. Es wird nicht empfohlen, diesen Parameter zu entfernen.</p> <p>Es wird empfohlen, dass Sie beim stillen Modus die folgenden Namen verwenden:</p> <ul style="list-style-type: none"> <li>■ Installation: <i>pccsilentnnnmsi.log</i></li> <li>■ Deinstallation: <i>pccsilentnnnuninstmsi.log</i></li> </ul> <p>wobei <i>nnn</i> im Namen der Logdatei für die aktuelle Versionsnummer von Entire Connection steht.</p>
SERIALNUMBER= <i>seriennummer</i>	<p>Erforderlich für die Installation. Die Seriennummer von Entire Connection.</p> <p><b>Wichtig:</b> Bei einer Update-Installation müssen Sie die Seriennummer der neuen Version angeben.</p>
INSTALLDIR= <i>installationsverzeichnis</i>	<p>Das Installationsverzeichnis (die Vorgabe ist <i>\Program Files\Software AG\Entire Connection</i>).</p> <p><b>Wichtig:</b> Bei einer Update-Installation müssen Sie dasselbe Installationsverzeichnis angeben wie für die ursprüngliche Installation.</p>
INSTALLLEVEL= <i>installlevel</i>	Optional. Mögliche Werte: 1 oder 100 (die Vorgabe ist 1). Der Wert 1 steht für den Setup-Typ <b>Standard</b> ; der Wert 100 steht für den Setup-Typ <b>Komplett</b> (siehe oben).
/qn	Erforderlich. Stiller Modus für den Windows-Installer.





2. Bei einem 64-Bit-Windows-Betriebssystem wird Entire Connection standardmäßig im folgenden Programmordner installiert: "Program Files (x86)". Im Datei-Explorer wird dann der symbolische Name "Programme (x86)" angezeigt.

Programmordner	Inhalt
\Entire Connection	*.exe *.dll API-ActiveX-Control <i>PccAPI.ocx</i> .
\Entire Connection\doc	<i>Readme_gr.txt</i>  Deutsche und englische Online-Dokumentation, und die Hilfedateien <i>Pccnnnxx.chm</i> (wobei <i>nnn</i> die aktuelle Versionsnummer ist und <i>xx</i> der Sprachcode "GR" für Deutsch (German) oder "US" für US-Englisch).
\Entire Connection\netsetup	Client-Installationsprogramm <i>Setup.exe</i> . Steht nur zur Verfügung, wenn bei der Installation die Option <b>Client-Setup</b> angegeben wurde (Setup-Typ <b>Benutzer</b> ).

Standardmäßig werden die Ordner für die Benutzerdaten hier installiert:

\ProgramData\Software AG\Entire Connection

Der Ordner *ProgramData* ist ein versteckter Ordner. Er ist nur dann im Explorer zu sehen, wenn die entsprechende Option in den Orderoptionen des Explorers aktiviert ist.

Wenn Sie nicht in den Standardprogrammordner (d.h. nicht in den Windows-Ordner *Program Files*) installieren, dann werden die Ordner für die Benutzerdaten in den von Ihnen angegebenen Ordner installiert.

Dies sind die Ordner für die Benutzerdaten:

Ordner	Inhalt
<i>certs</i>	Dateien für die SSL/TLS-Unterstützung von TN3270.
<i>data</i>	<i>Share411.sag</i> .
<i>home</i>	Leer nach der Installation. *.log Trace-Dateien (z.B. <i>Monnn.trc</i> ). Temporäre Dateien für die Host-Drucker-LU-Unterstützung.
<i>proc</i>	Systemprozedurdateien. Wenn dies bei der Installation angegeben wurde, enthält dieser Ordner auch Beispielprozedurdateien und Natural-Beispielprogramme.
<i>tables</i>	Übersetzungs-, Tastatur- und physische Funktionscodetabellen.

Bei einer Installation für mehrere Benutzer unter Terminal Services müssen Sie Folgendes beachten: wenn Sie den Benutzern das Ändern ihrer eigenen Profile in der Share-Datei erlauben wollen, dann müssen Sie die Sicherheitseigenschaften für die Datei *Share411.sag* ändern und den Benutzern Schreibrechte erteilen.

## Umgebungsvariablen

---

Entire Connection ändert keine Umgebungsvariablen.

## Entire Connection aktualisieren (Upgrade)

---

Es kann nur eine Version von Entire Connection auf einem PC installiert werden (Installation für den Administrator). Wenn Sie Entire Connection aktualisieren, wird die bisherige Version zuerst entfernt und die neue Version anschließend installiert. Alle Benutzerdaten der vorherigen Version, insbesondere die Share-Datei, werden gesichert und wiederhergestellt.



**Vorsicht:** Wenn sich durch die Aktualisierung Ihrer Installation der Ort für Ihre Benutzerdaten geändert hat, sind die in der Share-Datei gespeicherten Verzeichnisnamen möglicherweise nicht mehr gültig. In diesem Fall müssen Sie diese Verzeichnisnamen im Anschluss an die Aktualisierung anpassen, damit Entire Connection Version 8.4.1 oder höher Ihre Prozedurdateien, Log-Dateien und Trace-Dateien finden kann. Die Verzeichnisnamen für diese Dateien sind in den Systemvoreinstellungen und in den Benutzereigenschaften gespeichert.

## Entire Connection auf einer Client-Workstation installieren

---

Wenn mehrere Benutzer mit der selben Installation arbeiten sollen, muss der Administrator Entire Connection zuerst auf einem Netzwerk-File-Server oder einem freigegebenen Laufwerk installieren und vorbereiten (siehe [Entire Connection für den Administrator installieren](#)). Danach kann jeder Benutzer das Programm *Setup.exe* im Ordner *netsetup* von der eigenen Client-Workstation aus aufrufen. Es registriert Entire Connection auf der Client-Workstation und erstellt einen Ordner für Entire Connection im Windows-Startmenü.



**Wichtig:** Jeder Benutzer, der Entire Connection wie oben beschrieben auf einer Client-Workstation installieren möchte, benötigt Administratorrechte.

## Entire Connection auf einer Client-Workstation aktualisieren (Upgrade)

Für eine Client-Workstation gibt es keine Upgrade-Installation.

Der Administrator muss zuerst die existierende Installation von Entire Connection auf dem Netzwerk-File-Server oder freigegebenen Laufwerk aktualisieren (siehe [Entire Connection aktualisieren \(Upgrade\)](#)). Anschließend müssen Sie auf dem PC, auf dem sich eine existierende Client-Installation befindet, folgendermaßen vorgehen:

1. Deinstallieren Sie Entire Connection auf allen Client-Workstations (siehe unten).
2. Installieren Sie Entire Connection auf allen Client-Workstations (siehe oben).

## Entire Connection auf einer Client-Workstation deinstallieren

Siehe [Entire Connection deinstallieren](#).

## Entire Connection deinstallieren

---

Entire Connection wird in der Windows-Systemsteuerung mit der Windows-Standardfunktionalität deinstalliert. Sie können Entire Connection aber auch im [stillen Modus](#) deinstallieren.

Beim Deinstallieren werden die Benutzerdaten in den Installationsordnern von Entire Connection nicht gelöscht. Dies gilt auch für die Share-Datei im Ordner *data*.

## Versionsportabilität und Parallelität

---



**Vorsicht:** Es wird allgemein empfohlen, Entire Connection mit dem Installationsprogramm zu installieren. In bestimmten Fällen, wie zum Beispiel bei Migrations- oder Rehosting-Projekten, kann es sinnvoll sein, eine portable Version laufen zu lassen, um verschiedene Versionen parallel auszuführen. Es wird jedoch empfohlen, eine portable Version nur zu Testzwecken zu verwenden.

Da Entire Connection keine Einträge in der Registrierung benötigt, kann es durch Kopieren und Einfügen auf andere Rechner übertragen werden.

Solch eine kopierte Version kann als portable Version fungieren. Als Folge davon können viele verschiedene Versionen parallel existieren, und es ist möglich, eine installierte Version und eine portable Version auf demselben Windows-Computer laufen zu lassen.



**Wichtig:** Die Nachteile der Verwendung von Entire Connection als portable Version sind:

- Microsoft Visual Studio Redistributable muss auf dem Zielsystem installiert sein. Normalerweise wird dies vom Installationsprogramm erledigt.
- Kann nicht einfach über "Apps & Features" oder andere Windows-typische Wege entfernt werden.
- Die Konfiguration muss von Ihnen selbst verwaltet werden, da sie vom Installationsprogramm nicht automatisch unter *C:\Program Files\Software AG\Entire Connection* gespeichert wird.
- Kann versehentlich leicht entfernt werden, da der Ordner nicht (wie zum Beispiel *C:\Programme (x86)*) geschützt ist.
- Das API kann nicht verwendet werden, ohne die Registrierung zu ändern. Dies erfordert einen Programmstart mit Administratorrechten.

### Voraussetzungen

- Ein Windows-Computer (sollte keine Produktionsumgebung sein), auf dem Sie die neueste Version von Entire Connection installieren können.
- Ein Windows-Zielcomputer, auf dem die parallele Version laufen soll. Hier muss Microsoft Visual Studio Redistributable installiert werden.

Die folgenden Schritte zeigen, wie Sie eine portable Version von Entire Connection einrichten und ausführen:















1. Verwenden Sie einen Computer, auf dem Sie die neueste Version von Entire Connection installieren können. Installieren Sie Entire Connection mit den erforderlichen Einstellungen.
2. Öffnen Sie das Installationsverzeichnis. Standardmäßig ist dies *C:\Program Files (x86)\Software AG\*.
3. Kopieren Sie das Installationsverzeichnis an einen nicht schreibgeschützten Speicherort, zum Beispiel nach *C:* oder auf den Desktop.
4. Erstellen Sie eine ZIP-Datei mit dem gesamten Inhalt des neu erstellten *Entire Connection*-Verzeichnisses.
5. Kopieren Sie die neue ZIP-Datei auf den Computer, auf dem Sie die portable Version von Entire Connection ausführen möchten.
6. Entpacken Sie die Dateien an einen geeigneten Speicherort auf dem Zielcomputer.
7. Hier können die ausführbaren Dateien (zum Beispiel *PccTerminal.exe* oder *PCCAdmin.exe*) direkt aus diesem Verzeichnis gestartet werden.

Name	Date modified	Type ^	Size
doc	26/04/2021 14:27	File folder	
netsetup	26/04/2021 14:27	File folder	
PccAPI.ocx	26/04/2021 11:11	ActiveX control	145 KB
OpenSSL.exe	26/04/2021 11:11	Application	478 KB
PCCAdmin.exe	26/04/2021 11:11	Application	762 KB
PccConvert.exe	26/04/2021 11:11	Application	143 KB
PccPLUMn.exe	26/04/2021 11:11	Application	251 KB
PccPLUSv.exe	26/04/2021 11:11	Application	371 KB
PccTerminal.exe	26/04/2021 11:11	Application	1.217 KB
icudt63.dll	26/04/2021 11:10	Application exten...	26.554 KB
icuuc63.dll	26/04/2021 11:10	Application exten...	1.333 KB
libcrypto-1_1.dll	26/04/2021 11:10	Application exten...	2.455 KB
libssh2.dll	26/04/2021 11:10	Application exten...	245 KB
libssl-1_1.dll	26/04/2021 11:10	Application exten...	525 KB
Pcc3270.dll	26/04/2021 11:10	Application exten...	80 KB
PccAdminResGR.dll	26/04/2021 11:10	Application exten...	265 KB
Pccbs2.dll	26/04/2021 11:10	Application exten...	83 KB

8. Um zu überprüfen, ob die beabsichtigte Version wirklich ausgeführt wird, wählen Sie aus dem Menü **Hilfe** den Befehl **Info über Entire Connection Terminal**.
9. Entire Connection benutzt eine Share-Datei, die sich standardmäßig im Verzeichnis *C:\Program Files\Software AG\Entire Connection\data* befindet. Sie können dieses Verzeichnis ersetzen, indem Sie ein Verzeichnis, welches ebenfalls den Namen *data* trägt, parallel zu den ausführbaren Dateien erstellen und die Share-Datei in dieses Verzeichnis hinein kopieren.

data	26/04/2021 21:49	File folder	
doc	26/04/2021 14:27	File folder	
netsetup	26/04/2021 14:27	File folder	
PccAPI.ocx	26/04/2021 11:11	ActiveX control	145 KB
OpenSSL.exe	26/04/2021 11:11	Application	478 KB
PCCAdmin.exe	26/04/2021 11:11	Application	762 KB
PccConvert.exe	26/04/2021 11:11	Application	143 KB
PccPLUMn.exe	26/04/2021 11:11	Application	251 KB
PccPLUSv.exe	26/04/2021 11:11	Application	371 KB
PccTerminal.exe	26/04/2021 11:11	Application	1.217 KB
icudt63.dll	26/04/2021 11:10	Application exten...	26.554 KB

Auch alle anderen Verzeichnisse aus *C:\Program Files\Software AG\Entire Connection\* können Sie hier erstellen (kopieren und einfügen), damit eine komplette parallele Umgebung ausgeführt werden kann.

	certs	26/04/2021 21:52	File folder	
	data	26/04/2021 21:52	File folder	
	doc	26/04/2021 14:27	File folder	
	home	18/11/2020 14:23	File folder	
	netsetup	26/04/2021 14:27	File folder	
	proc	26/04/2021 21:52	File folder	
	tables	26/04/2021 21:52	File folder	
	PccAPI.ocx	26/04/2021 11:11	ActiveX control	145 KB
	OpenSSL.exe	26/04/2021 11:11	Application	478 KB
	PCCAdmin.exe	26/04/2021 11:11	Application	762 KB
	PccConvert.exe	26/04/2021 11:11	Application	143 KB
	PccPLUMn.exe	26/04/2021 11:11	Application	251 KB
	PccPLUSv.exe	26/04/2021 11:11	Application	371 KB
	PccTerminal.exe	26/04/2021 11:11	Application	1.217 KB

Die portable Version ändert keine Registrierungseinträge, die eine bereits installierte Version betreffen, vorausgesetzt, die portable Version wird nicht mit Administratorrechten gestartet. Das Programm ändert nur Einträge in HKEY\_CURRENT\_USER, wie zum Beispiel die Fenstergröße. Wenn die portable Version jedoch mit Administratorrechten gestartet wird und eine andere Version parallel installiert ist, dann ändert sie die Einträge für das API.



**Vorsicht:** Wenn Sie Entire Connection mit Administratorrechten starten, dann verwendet das API die laufende Instanz von Entire Connection.





# 5

## SSL/TLS-Unterstützung für TN3270

---

■ In Entire Connection unterstützte SSL/TLS-Funktionalität .....	28
■ Eine TN3270-Session mit SSL/TLS aufbauen .....	29
■ SSL/TLS für Entire Connection konfigurieren .....	29
■ Server-Zertifikate mit Entire Connection überprüfen .....	30
■ Client-Authentifizierung .....	31
■ Mehr zu Zertifikaten .....	33

Entire Connection unterstützt TN3270-SSL/TLS. Dies ermöglicht eine sichere Verbindung zwischen Entire Connection und einem Telnet-TN3270-Server. In einer SSL/TLS-Session werden alle Daten verschlüsselt, bevor sie an den Telnet-Server gesendet werden. Vor der weiteren Verarbeitung werden die vom Server empfangenen verschlüsselten Daten entschlüsselt.

Als Voraussetzung benötigen Sie einen Telnet-TN3270-Server mit einem Port, der für SSL/TLS aktiviert wurde. Damit SSL/TLS benutzt werden kann, muss der Server einen privaten Schlüssel und ein hiermit verknüpftes Server-Zertifikat haben.



**Anmerkung:** Dieses Produkt enthält Software, die vom OpenSSL Project für die Benutzung im OpenSSL Toolkit entwickelt wurde (<https://www.openssl.org/>).

## In Entire Connection unterstützte SSL/TLS-Funktionalität

---

In Entire Connection steht die SSL/TLS-Unterstützung für TN3270-Anzeige-Sessions und TN3270-Drucker-Sessions zur Verfügung. Die folgenden SSL/TLS-Optionen werden unterstützt:

### ■ Server-Authentifizierung

Die Server-Authentifizierung dient dazu, den Server beim Client zu legitimieren. Die Server-Authentifizierung kann für eine verschlüsselte SSL/TLS-Session ein- und ausgeschaltet werden. Sie kann mit oder ohne Client-Authentifizierung benutzt werden.

Bevor die Session aufgebaut wird, prüft der Client (Entire Connection) das Server-Zertifikat, das mit dem privaten Schlüssel des Servers verknüpft ist.

### ■ Überprüfung des Hostnamens

Der Name des Hosts zu dem der Client (Entire Connection) eine Verbindung aufbaut, wird mit dem Wert für den Common Name (CN) im Server-Zertifikat verglichen. Diese Option verstärkt die Server-Authentifizierung.

### ■ Client-Authentifizierung

Die Client-Authentifizierung dient dazu, den Client beim Server zu legitimieren.

Die SSL/TLS-Client-Authentifizierung bietet eine zusätzliche Authentifizierungs- und Zugriffskontrolle durch das Überprüfen der Client-Zertifikate auf dem Server. Dies verhindert, dass ein nicht berechtigter Client auf dem Server Zugriff erhält.

## Eine TN3270-Session mit SSL/TLS aufbauen

---

Es gibt zwei Möglichkeiten, eine TN3270-Session mit SSL/TLS aufzubauen.

Die eine Möglichkeit ist, eine SSL/TLS-Verbindung mit einem SSL/TLS-Handshake direkt zu öffnen. Das heißt, dass der Client die Verbindung zu einem Port herstellt, der für SSL/TLS aktiviert wurde und dass das SSL/TLS-Protokoll von Anfang an benutzt wird.

Die andere Möglichkeit ist verhandelbare Telnet-Sicherheit. In diesem Fall wird eine normale Telnet-Verbindung zwischen dem Client und dem Telnet-TN3270-Server geöffnet. Der Telnet-Server sendet dann einen speziellen Befehl (`IAC DO START_TLS`) an den Client, um zu prüfen, ob der Client die SSL/TLS-Verhandlung starten möchte. Bei einer positiven Antwort macht der Server mit dem SSL/TLS-Handshake weiter. Wenn keine positive Antwort empfangen wird, wird - in Abhängigkeit von der Server-Konfiguration - eine normale Telnet-Session benutzt oder die Verbindung wird beendet.

## SSL/TLS für Entire Connection konfigurieren

---

Der folgende Ordner enthält mehrere Server-Zertifikate von unterschiedlichen Zertifizierungsstellen (auch „Certification Authority“ oder kurz „CA“ genannt).

`\ProgramData\Software AG\Entire Connection\certs`

1. Wenn die Server-Authentifizierung eingeschaltet ist, überprüfen Sie, ob das Server-Zertifikat, das Sie für Ihren Telnet-SSL/TLS-Server erhalten haben, bereits im Ordner *certs* enthalten ist. Wenn Ihr Server-Zertifikat von einer anderen Zertifizierungsstelle ist, oder wenn Sie ein selbstsigniertes Zertifikat benutzen, müssen Sie es ebenfalls im Ordner *certs* ablegen und in die Datei *CAList.pem*, die sich auch in diesem Ordner befindet, eintragen. Ausführliche Informationen hierzu finden Sie im Abschnitt [Server-Zertifikate mit Entire Connection überprüfen](#).
2. Erstellen Sie mit dem Konfigurationsmanager von Entire Connection eine Host-Session (Anzeige-Session) vom Typ TN3270. Geben Sie im Dialogfeld **Session-Eigenschaften** einen Session-Namen ein und wählen Sie die Befehlsschaltfläche **Kommunikation**. Geben Sie auf der Eigenschaftenseite **Allgemein** des daraufhin erscheinenden Dialogfelds **Kommunikation** alle erforderlichen Informationen ein. Geben Sie die Nummer eines Ports an, der SSL/TLS unterstützt. Zeigen Sie die Eigenschaftenseite **Sicherheit** an und aktivieren Sie SSL/TLS. Sie werden zunächst überprüfen, ob eine einfache SSL/TLS-Verbindung hergestellt werden kann. Aktivieren Sie hierzu entweder das Kontrollkästchen **SSL/TLS Handshake-Verbindung**, um eine Handshake-Verbindung einzurichten oder Sie deaktivieren dieses Kontrollkästchen, um eine Session mit verhandelbarer Telnet-Sicherheit einzurichten. Aktivieren Sie noch nicht die anderen Optionen auf dieser Eigenschaftenseite. Ausführliche Informationen zu den Kommunikationsparametern finden Sie in der *Übersicht der Objekteigenschaften* im Abschnitt *TN3270(E) für Anzeige-Sessions*.

3. Rufen Sie die Terminal-Anwendung von Entire Connection auf, um die Session zu testen, die Sie im vorherigen Schritt erstellt haben.
4. Wenn diese einfache SSL/TLS-Verbindung korrekt funktioniert, können Sie die restlichen Optionen auf der Eigenschaftenseite **Sicherheit** aktivieren und testen:

- **Überprüfung des Hostnamens**

Sie können diese SSL/TLS-Option nur dann benutzen, wenn der Wert für den Common Name (CN) im Server-Zertifikat derselbe ist wie der Hostname auf der Eigenschaftenseite **Allgemein** des Dialogfelds **Kommunikation**.

Um diese SSL/TLS-Option zu nutzen, müssen Sie auf der Eigenschaftenseite **Sicherheit** des Dialogfelds **Kommunikation** die Option **Common Name im Zertifikat mit Hostnamen vergleichen** aktivieren.

- **Client-Authentifizierung**

Ihr Server muss für die Benutzung der Client-Authentifizierung konfiguriert sein. Sie benötigen einen privaten Schlüssel für den Client und ein Zertifikat für diesen Schlüssel. Dieser Schlüssel und das Zertifikat müssen bei Entire Connection zur Verfügung stehen. Ausführliche Informationen hierzu finden Sie im Abschnitt *Client-Authentifizierung*.

Um diese SSL/TLS-Option zu nutzen, müssen Sie auf der Eigenschaftenseite **Sicherheit** des Dialogfelds **Kommunikation** die Option **Zertifikat an den Server senden, wenn dieser eines verlangt** aktivieren.

5. Wiederholen Sie die oben aufgeführten Schritte, um eine Host-Drucker-Session vom Typ TN3270E zu erstellen. Ausführliche Informationen zu den Kommunikationsparametern finden Sie in der *Übersicht der Objekteigenschaften* im Abschnitt *TN3270E für Drucker-Sessions*.

## Server-Zertifikate mit Entire Connection überprüfen

---

Die Informationen in diesem Abschnitt gelten wenn die Server-Authentifizierung eingeschaltet ist. Es wird beschrieben, wie Sie eine einfache SSL/TLS-Verbindung mit Server-Authentifizierung einrichten. Das heißt: Entire Connection stellt eine SSL/TLS-Verbindung her und überprüft das Zertifikat des TN3270-Servers. Wenn das Server-Zertifikat nicht gültig ist, wird die Verbindung beendet.

Beim Starten einer TN3270-SSL/TLS-Verbindung vergleicht Entire Connection das Server-Zertifikat mit den Zertifikaten in der Datei *CAList.pem*. Diese Datei enthält die (Stamm-) Zertifikate der Zertifizierungsstellen, denen Sie vertrauen. Eine Zertifizierungsstelle ist eine Firma, die Zertifikatsanfragen signiert. Ein Beispiel für eine solche Firma ist Verisign (siehe <http://www.verisign.com/>).

Die mit Entire Connection ausgelieferte Datei *CAList.pem* enthält verschiedene Zertifikate von bekannten Zertifizierungsstellen. Wenn Sie für Ihren Server ein selbstsigniertes Zertifikat haben, oder wenn Sie noch ein weiteres Zertifikat zur Liste der vertrauenswürdigen Zertifikate hinzufügen möchten, müssen Sie wie nachfolgend beschrieben vorgehen.

## ➤ Ein Zertifikat in die Datei *CAList.pem* eintragen

- 1 Gehen Sie zum *certs*-Ordner von Entire Connection.

Dieser Ordner enthält mehrere Zertifikatdateien (.*crt*) und die Datei *CAList.pem*, die eine Zusammenfassung der *crt*-Dateien darstellt. Mit der Stapelverarbeitungsdatei *create-calist.bat* wird die Datei *CAList.pem* erstellt. Die Datei *create-calist.bat* enthält eine Befehlszeile für jedes Zertifikat, das in die Datei *CAList.pem* geschrieben werden soll.

- 2 Kopieren Sie Ihre *crt*-Datei (zum Beispiel ein selbstsigniertes Zertifikat oder ein neues Zertifikat von einer Zertifizierungsstelle) in den Ordner *certs*.
- 3 Editieren Sie die Stapelverarbeitungsdatei *create-calist.bat* und erstellen Sie eine neue Befehlszeile für Ihr Zertifikat.

Wenn Sie zum Beispiel das Zertifikat in der Datei *meincert.crt* hinzufügen möchten, müssen Sie die folgende Befehlszeile hinzufügen:

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

- 4 Überprüfen Sie, ob die Variable *OPENSSL* in der ersten Zeile der Stapelverarbeitungsdatei bei Ihnen korrekt gesetzt ist. Sie muss auf *OpenSSL.exe* zeigen. Dieses Programm befindet sich im Stammverzeichnis von Entire Connection.
- 5 Führen Sie die Datei *create-calist.bat* aus. Die Datei *CAList.pem* wird jetzt mit der neuen Zertifikatsdatei neu erstellt.

## Client-Authentifizierung

Mit der Client-Authentifizierung kann der Telnet-Server die Identität des Client überprüfen. Der Server kann nicht nur überprüfen, ob das Zertifikat von einer vertrauenswürdigen CA (unterste Sicherheitsstufe) ausgegeben wurde, es ist auch möglich, das Client-Zertifikat gegen eine interne Datenbank (zum Beispiel RACF) zu registrieren und zu gewährleisten, dass der Client die Verbindung von einer definierten TCP/IP-Adresse und einem definierten Port aus herstellt. Client-Authentifizierung ist optional.

### Generieren Sie einen privaten Schlüssel für jeden Benutzer

Für die Client-Authentifizierung muss für jeden Benutzer ein privater Schlüssel generiert werden. Der private Schlüssel wird mit dem Programm *OpenSSL.exe* generiert. Dieses Programm befindet sich im Stammverzeichnis von Entire Connection.

Informationen darüber, wie der private Schlüssel erstellt wird (in englischer Sprache), finden Sie im Dokument *keys.txt*, das sich im Ordner *certs* befindet.

Ihr privater Schlüssel sollte den Namen *clientprivkey.pem* haben.

➤ **Einen 2048-Bit-RSA-Schlüssel erstellen (Beispiel)**

- 1 Öffnen Sie ein Fenster für die Eingabeaufforderung.
- 2 Wechseln Sie in den *certs*-Ordner von Entire Connection.
- 3 Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

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

Wenn Sie "-des3" angeben, werden Sie beim Generieren des privaten Schlüssels aufgefordert, ein Passwort anzugeben.



**Wichtig:** Aus Sicherheitsgründen empfehlen wir, den privaten Schlüssel mit einem Passwort zu generieren. Dadurch wird verhindert, dass der private Schlüssel - falls er in falsche Hände gelangt - ohne Passwort benutzt werden kann.

**Erstellen Sie ein auf dem Client-Schlüssel basiertes Zertifikat**

Sie müssen auch ein Zertifikat erstellen, das auf dem Client-Schlüssel basiert. Hier zu wird auch das Programm *OpenSSL.exe* benutzt, das sich im Stammverzeichnis von Entire Connection befindet.

Weitere Informationen (in englischer Sprache) finden Sie im Dokument *certificates.txt*, das sich im Ordner *certs* befindet.

Ihr Zertifikat sollte den Namen *clientcert.crt* haben.

➤ **Ein selbstsigniertes Zertifikat mit der Konfigurationsdatei *openssl.cnf* erstellen (Beispiel)**

- 1 Öffnen Sie ein Fenster für die Eingabeaufforderung.
- 2 Wechseln Sie in den *certs*-Ordner von Entire Connection.
- 3 Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

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

Denken Sie daran, dass Sie Ihren TN3270-Server für die Client-Authentifizierung konfigurieren müssen und dass Sie auch den Client-Schlüssel und das Zertifikat auf dem Server „installieren“ müssen.

## Mehr zu Zertifikaten

---

### Zertifikate mit Microsoft Internet Explorer exportieren

Es ist möglich, vertrauenswürdige Zertifikate aus dem Microsoft Internet Explorer heraus zu exportieren.

#### ➤ Zertifikate exportieren

Diese Beschreibung gilt für Internet Explorer 9.

- 1 Wählen Sie aus dem Menü **Extras** den Befehl **Internetoptionen**.
- 2 Gehen Sie zur Registerkarte **Inhalte**.
- 3 Wählen Sie die Befehlsschaltfläche **Zertifikate**.
- 4 Gehen Sie zur Registerkarte **Vertrauenswürdige Stammzertifizierungsstellen**.
- 5 Markieren Sie das Zertifikat, das Sie exportieren möchten.
- 6 Wählen Sie die Befehlsschaltfläche **Exportieren**.

Der Zertifikatexport-Assistent erscheint.

- 7 Wählen Sie die Befehlsschaltfläche **Weiter**.
- 8 Markieren Sie die Option **Base-64-codiert X.509 (.CER)**.
- 9 Wählen Sie die Befehlsschaltfläche **Weiter**.
- 10 Geben Sie den Namen der Datei an, in die das Zertifikat exportiert werden soll.
- 11 Wählen Sie die Befehlsschaltfläche **Weiter**.
- 12 Wählen Sie auf der letzten Seite des Assistenten die Befehlsschaltfläche **Fertig stellen**.

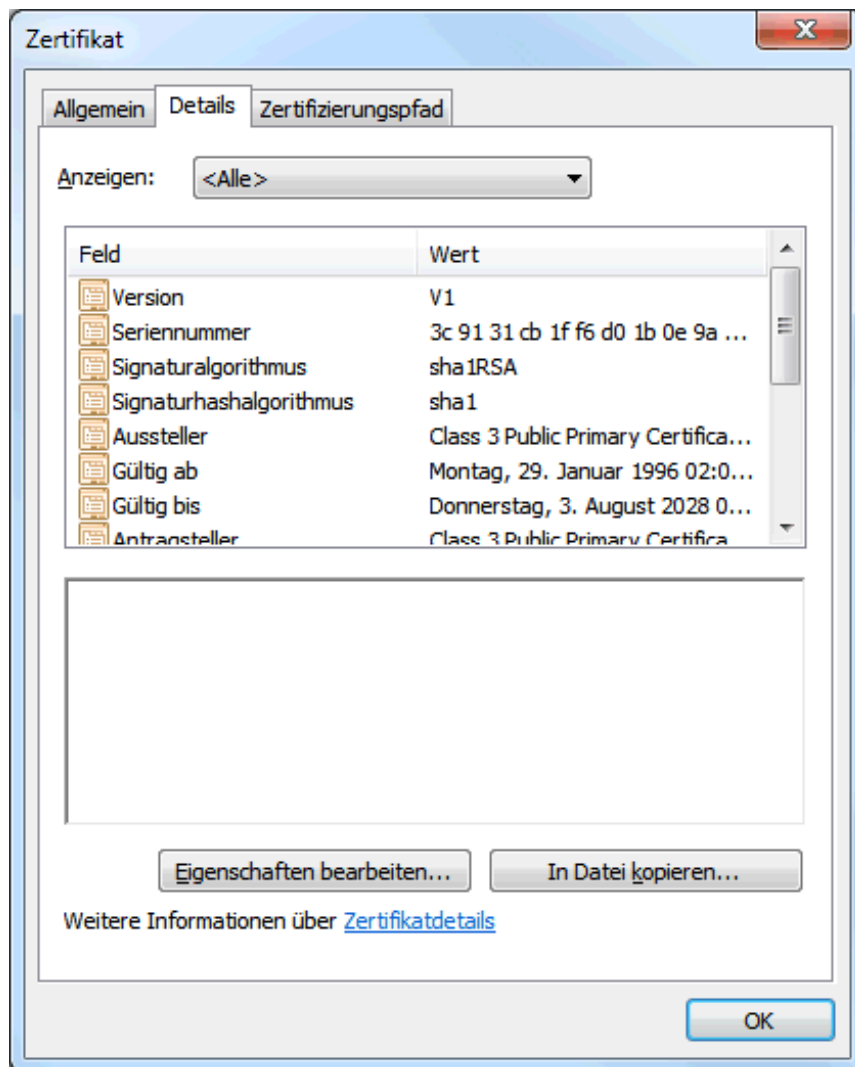
### Stammzertifikate von Zertifizierungsstellen herunterladen

Es ist auch möglich, ein Stammzertifikat direkt von der Web-Seite einer Zertifizierungsstelle herunterzuladen. Dieses Zertifikat ist eventuell nicht im richtigen Format (Entire Connection benötigt Base-64). Um zu überprüfen, ob das Zertifikat im Base-64-Format ist, öffnen Sie es mit einem ASCII-Editor (z.B. dem Windows-Editor). Wenn in der ersten Zeile "BEGIN CERTIFICATE" steht und "END CERTIFICATE" in der letzten Zeile, dann ist das Format bereits Base-64 und Sie können das Zertifikat so benutzen wie es ist.

Wenn das Zertifikat nicht im Base-64-Format ist, müssen Sie es wie unten beschrieben ändern.

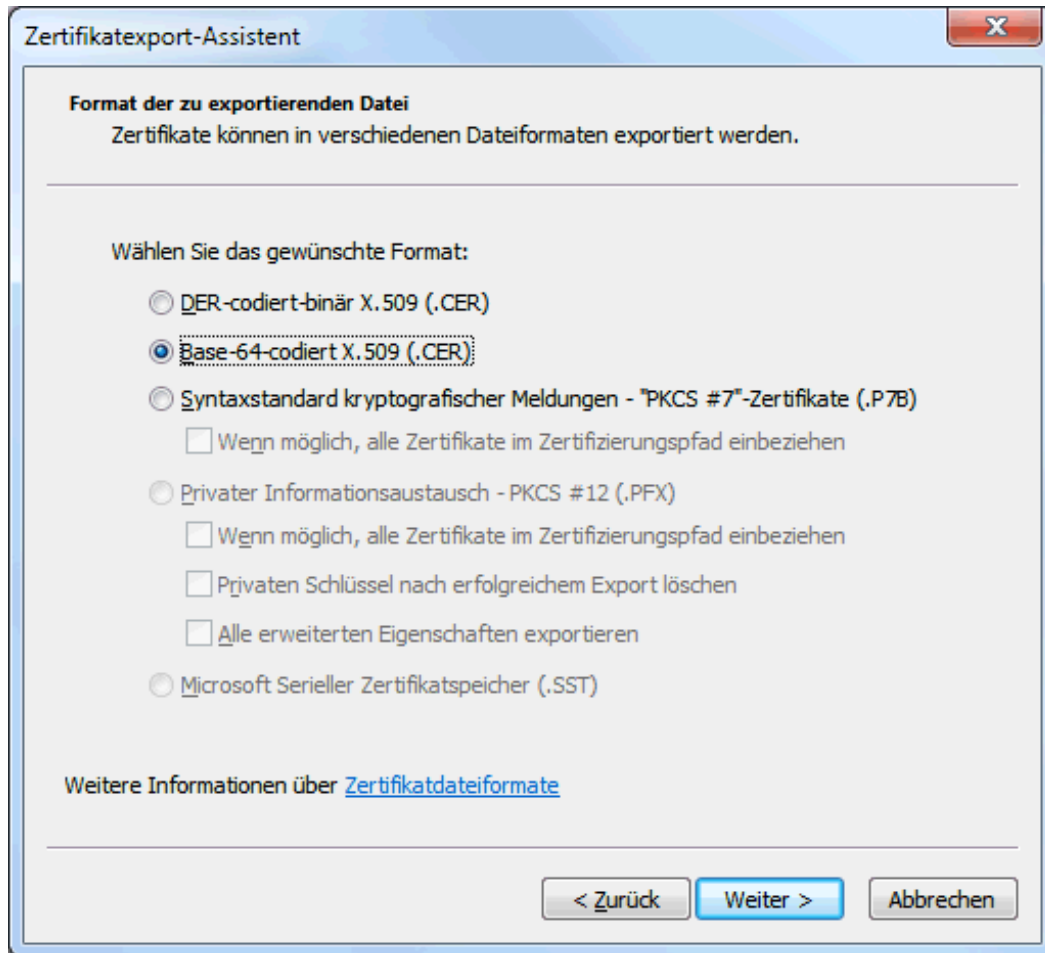
➤ **Das Format des Zertifikats in Base-64 ändern**

- 1 Öffnen Sie das Zertifikat und zeigen Sie die Seite **Details** an. Beispiel:



- 2 Wählen Sie die Befehlsschaltfläche **In Datei kopieren**, um den **Zertifikatsexport-Assistent** aufzurufen.
- 3 Wählen Sie die Befehlsschaltfläche **Weiter**, um die nächste Seite anzuzeigen.
- 4 Markieren Sie die Option **Base-64 codiert X.509 (.CER)**.





- 5 Wählen Sie die Befehlsschaltfläche **Weiter**, um die nächste Seite anzuzeigen.
- 6 Geben Sie den Namen der Datei an, in die Sie das geänderte Zertifikat exportieren möchten.
- 7 Wählen Sie die Befehlsschaltfläche **Weiter**, um die nächste Seite anzuzeigen.
- 8 Wählen Sie die Befehlsschaltfläche **Fertig stellen**.



## 6 SSL/TLS-Unterstützung für BS2000

---

Entire Connection unterstützt BS2000 SSL/TLS.

Der Aufbau einer BS2000-Session mit SSL/TSL erfolgt nach dem gleichen Verfahren wie im vorherigen Abschnitt *SSL/TLS-Unterstützung für TN3270* beschrieben



**Anmerkung:** Die BS2000-Verbindungen erlauben nicht das Erstellen von Host-Drucker-Sessions.



# 7

## SSH-Unterstützung für Telnet

---

Entire Connection unterstützt Telnet SSH für Sessions vom Typ Telnet VTxxx. Dies ermöglicht eine sichere Verbindung zwischen Entire Connection und einem Server. In einer SSH-Session werden alle Daten verschlüsselt, bevor sie an den Telnet-Server gesendet werden. Vor der weiteren Verarbeitung werden die vom Server empfangenen verschlüsselten Daten entschlüsselt.

Sie aktivieren SSH, indem Sie die Verbindungsart SSH für Ihre Telnet-VTxxx-Session wählen (siehe die Beschreibung der Seite **Allgemein** für Telnet VTxxx in *Kommunikationsparameter* in der *Übersicht der Objekteigenschaften*).

Telnet-VTxxx-Sessions mit der Verbindungsart SSH benötigen die Einstellung CR für die Option **Sende-Option der Eingabetaste** (siehe die Beschreibung der Seite **Terminal** für VT-Typen in *Session-Eigenschaften* in der *Übersicht der Objekteigenschaften*), andernfalls kann es zu Fehlfunktionen kommen. CR ist die Standardeinstellung wenn Sie neue Sessions vom Typ Telnet VTxxx erstellen. Die Option kann jedoch eine andere Einstellung haben, wenn Sie die Verbindungsart einer existierenden Telnet-VTxxx-Session von Telnet nach SSH verändern oder wenn Sie eine Telnet-VTxxx-Session duplizieren; in diesen Fällen müssen Sie darauf achten, dass die Einstellung CR benutzt wird.

Als Voraussetzung für SSH benötigen Sie einen Server mit einem Port, der für SSH aktiviert wurde. Entire Connection unterstützt das SSH-Protokoll Version 2.0.

Die folgenden SSH-Authentifizierungsmethoden werden unterstützt:

- Authentifizierungsmethode "password"
- Authentifizierungsmethode "keyboard-interactive"
- Authentifizierungsmethode "publickey"

In Abhängigkeit von Ihrer SSH-Host-Konfiguration werden eine oder mehrere Authentifizierungsmethoden vom Host angeboten. Die Authentifizierungsmethode "publickey" ist die bevorzugte Methode. Sie wird benutzt, wenn eine private Schlüsseldatei angegeben wurde (siehe die

Beschreibung der Seite **Sicherheit** für Telnet VTxxx in *Kommunikationsparameter* in der *Übersicht der Objekteigenschaften*).

Damit Sie die Authentifizierungsmethode "publickey" benutzen können, benötigen Sie ein Schlüsselpaar bestehend aus einem öffentlichen Schlüssel und einem privaten Schlüssel. Sie können ein solches Schlüsselpaar zum Beispiel mit OpenSSH-Werkzeugen oder mit PuTTY erzeugen. Es wird dringend empfohlen, dass Sie die private Schlüsseldatei mit einer Passphrase schützen. Es ist wichtig, dass die Schlüsseldateien das OpenSSH-Format haben.

Die private Schlüsseldatei muss sich im Ordner *appdata* des lokalen Benutzers befinden, und dort im Ordner *\Software AG\Entire Connection\certs*. Außerdem muss der Name der privaten Schlüsseldatei bei den Kommunikationsparametern für Telnet VTxxx auf der Seite **Sicherheit** angegeben werden.

Der Inhalt der öffentlichen Schlüsseldatei des Benutzers muss auf dem Server der Datei *\$HOME/.ssh/authorized\_keys* hinzugefügt werden. Stellen Sie sicher, dass der öffentliche Schlüssel eine Zeile in der Datei *authorized\_keys* ist. Es ist wichtig, dass die Ordner *\$HOME* und *\$HOME/.ssh* sowie die Datei *authorized\_keys* entsprechende Berechtigungsattribute haben. Die Berechtigungsattribute 700 für die Ordner und 400 für die Datei funktionieren bei den meisten Servern.

Die Authentifizierungsmethoden "password" und "keyboard-interactive" werden in dieser Reihenfolge benutzt, wenn sie vom Server angeboten werden und wenn die Authentifizierungsmethode "publickey" nicht den Vorrang hat, weil Sie den Namen einer privaten Schlüsseldatei auf der Seite **Sicherheit** bei den Kommunikationsparametern für Telnet VTxxx angegeben haben. Mit den Optionen auf der Seite **Sicherheit** können Sie Authentifizierungsmethoden deaktivieren.

# 8      Sichern und Wiederherstellen

---

■ Was kann gesichert werden? .....	42
■ Standardinstallation sichern .....	42
■ Standardinstallation wiederherstellen .....	43

Die Informationen in diesem Abschnitt sind hilfreich wenn Sie Ihre Einstellungen und Daten regelmäßig sichern möchten.

Sie sind auch hilfreich, wenn Sie Entire Connection auf einem neuen PC installieren. In diesem Fall werden zunächst die Standardeinstellungen von Entire Connection herangezogen. Wenn Sie Ihre bestehenden Einstellungen und Daten von Ihrem alten PC weiterverwenden möchten, dann müssen Sie alle erforderlichen Elemente auf dem alten PC sichern und auf dem neuen PC wiederherstellen.

## Was kann gesichert werden?

---

Sie können Folgendes sichern und wiederherstellen:

### ■ Share-Datei

Die mit Entire Connection ausgelieferte Standard-Share-Datei wird zum Beispiel dann geändert, wenn Sie eine neue Host-Session definieren, wenn Sie das aktuelle Farb- oder Tastenschema ändern, oder wenn Sie ein anderes Verzeichnis für Ihre Prozedurdateien definieren. Die Share-Datei wird auch geändert, wenn der Administrator zum Beispiel die Benutzereigenschaften oder Host-Drucker-Sessions ändert. Siehe auch *Über die Objekttypen*.

### ■ Prozedurdateien

Sie können Ihre eigenen Prozedurdateien erstellen oder die existierenden, mit Entire Connection ausgelieferten, Prozedurdateien ändern. Siehe auch *Prozedurdateien*.

### ■ Sicherheitszertifikate

Zertifikate werden für eine sichere Verbindung zwischen Entire Connection und einem Telnet-Server benutzt (SSL/TLS und SSH). Siehe auch *SSL/TLS-Unterstützung für TN3270* und *SSH-Unterstützung für Telnet*.

### ■ Parameter für den Aufruf der Terminal-Anwendung

Eine Verknüpfung für die Terminal-Anwendung auf Ihrem Desktop ist hilfreich, wenn Sie die Terminal-Anwendung mit bestimmten Parametern starten möchten. Siehe auch *Parameter für den Programmaufruf*.

## Standardinstallation sichern

---

1. Kopieren Sie den Ordner `\ProgramData\Software AG\Entire Connection` mit allen Unterordnern an einen Sicherungsort Ihrer Wahl. Die Share-Datei ist standardmäßig in diesem Ordner enthalten. Wenn Zertifikate für eine sichere Verbindung mit SSL/TLS erstellt wurden, dann sind sie auch in diesem Ordner enthalten.
2. Wenn Zertifikate für eine sichere Verbindung mit SSH erstellt wurden, dann müssen Sie auch den Ordner `Software AG\Entire Connection\certs` an einen Sicherungsort Ihrer Wahl kopieren.



Dieser Ordner befindet sich im lokalen *AppData*-Ordner des Benutzers (zum Beispiel in *C:\Users\benutzername\AppData\Local*).



**Anmerkung:** Die Ordner *ProgramData* und *AppData* sind versteckte Ordner. Sie sind nur dann im Explorer zu sehen, wenn die entsprechende Option in den Orderoptionen des Explorers aktiviert ist.

Zusätzliche Kopierschritte können in den folgenden Fällen erforderlich sein:

1. Sie haben Ihre Share-Datei umbenannt oder sie befindet sich an einem anderen Ort.

Standardmäßig befindet sich die Share-Datei im Ordner *\ProgramData\Software AG\Entire Connection\data* und sie hat den Namen *share411.sag*. Sowohl Speicherort als auch Name der Share-Datei können geändert werden. Wenn Sie Ihre Share-Datei nicht gleich finden können, dann starten Sie den Konfigurationsmanager (entweder direkt aus dem **Start**-Menü von Windows oder über das **Dienste**-Menü der Terminal-Anwendung). Speicherort und Name der Share-Datei werden dann im linken Fensterbereich des Anwendungsfensters, im obersten Knoten der Baumstruktur, angezeigt.

2. Sie haben Prozedurdateien erstellt, aber sie befinden sich nicht in *\ProgramData\Software AG\Entire Connection\data*.

Wenn Sie nicht wissen, wo sich Ihre Prozedurdateien befinden, dann starten Sie den Konfigurationsmanager und zeigen Sie Ihre Benutzereigenschaften an. Der Pfad zu Ihren Prozedurdateien wird dann auf der Seite **Prozedur** angezeigt.

Weitere Prozedurdateien (Dateien mit der Erweiterung *.NCP*) können sich auch im Installationsverzeichnis von Entire Connection befinden (das heißt, in *\Program Files\Software AG\Entire Connection*).

3. Sie haben auf Ihrem Desktop eine Verknüpfung für die Terminal-Anwendung erstellt und bestimmte Parameter für den Programmaufruf definiert.

Öffnen Sie die Eigenschaften der Verknüpfung und notieren Sie die Parameter. Oder kopieren Sie die Verknüpfung an einen Sicherungsort Ihrer Wahl.

## Standardinstallation wiederherstellen

1. Kopieren Sie die Ordner, die Sie gesichert haben, an die entsprechenden Orte auf dem neuen PC. Kopieren Sie sie zum Beispiel nach:

- *C:\ProgramData\Software AG\Entire Connection*
- *C:\Users\benutzername\AppData\Local\Software AG\Entire Connection\certs* (nur erforderlich, wenn SSH benutzt wird)

2. Starten Sie den Konfigurationsmanager, zeigen Sie Ihre Benutzereigenschaften an, gehen Sie zur Seite **Prozedur**, und überprüfen Sie die Einstellungen für das Prozedurverzeichnis und das Log- & Traceverzeichnis. Gegebenenfalls müssen Sie diese Einstellungen auf dem neuen PC ändern. Es wird empfohlen, dass Sie die folgenden Standardeinstellungen beibehalten: **Verwende gemeinsames Windows-Anwendungsdatenverzeichnis** für die Prozedurdateien und **Verwende lokales Windows-Benutzeranwendungsdatenverzeichnis** für die Log- & Trace-Dateien.
3. Falls erforderlich, erstellen Sie eine neue Verknüpfung für die Terminal-Anwendung auf Ihrem Desktop, mit den selben Parametern wie auf dem alten PC.

Oder wenn Sie die Verknüpfung gesichert haben: kopieren Sie sie auf Ihren Desktop. Öffnen Sie die Eigenschaften der Verknüpfung und vergewissern Sie sich, dass der Pfad zur Datei *Pccterminal.exe* korrekt ist.