Installing Encryption for Entire Net-Work

Before you install Encryption for Entire Net-Work, be sure you have met the requirements described in *Prerequisites*.

This chapter covers the following topics:

- Mainframe Installation
- Open Systems Installation

Mainframe Installation

On mainframe systems, the installation of Encryption for Entire Net-Work involves installing the software for the SSL line driver that is included with the Entire Net-Work TCP/IP Option. This section describes the steps required for this installation on z/OS and z/VSE platforms.

- Contents of the Release Tape
- Step 1. Unload the Entire Net-Work Libraries
- Step 2. Alter the Entire Net-Work Startup Job
- Step 3. Add the SSL DRIVER and LINK Statements
- Step 4. Configure Client Information
- Step 5. Start Entire Net-Work and Verify the Installation

Contents of the Release Tape

The following table describes most of the libraries included on the release tape. Once you have unloaded the libraries from the tape, you can change these names as required by your site, but the following lists the names that are delivered when you purchaseEncryption for Entire Net-Work.

Note:
Some of the libraries listed below may not appear on your release tape. If this is the case, it is likely that an update to that library was not necessary for the release.

Library Name	Description
APS*vrs*.LD*nn*	One or more Software AG internal libraries. The *vrs* in the library name represents the *version* of the internal library code, which is not necessarily the same as the version of Entire Net-Work
BTE*vrs*.LD*nn*	A Software AG internal library. The *vrs* in the library name represents the *version* of the internal library code, which is not necessarily the same as the version of Entire Net-Work
WSL*vrs*.LIBR	The z/VSE library for Encryption for Entire Net-Work. The *vrs* in the library name represents the *version* of Encryption for Entire Net-Work, which is not necessarily the same as the version of Entire Net-Work.
WSL*vrs*.LOAD	The z/OS load library for Encryption for Entire Net-Work. The *vrs* in the library name represents the *version* of Encryption for Entire Net-Work, which is not necessarily the same as the version of Entire Net-Work.

Step 1. Unload the Entire Net-Work Libraries

If not already performed, install the Entire Net-Work mainframe and Entire Net-Work TCP/IP Option libraries, using the procedure for your operating system environment. Then unload the SSL line driver components from the installation tape as follows:

Platform	Installation Procedure
z/OS	IEBCOPY to restore the required data sets. Refer to the *Report of Tape Creation* for the correct data set sequence numbers and names.
z/VSE	LIBR RESTORE to restore the required data sets. Refer to the *Report of Tape Creation* for the correct data set sequence numbers and names.

Step 2. Alter the Entire Net-Work Startup Job

Make the following changes to the Entire Net-Work startup JCL.

Platform	Startup Job Change
z/OS	A sample startup JCL member called JCLNET is provided in the source libraries. Add the SSL line driver load library to the STEPLIB concatenation.
z/VSE	Alter the Entire Net-Work startup job to add the SSL line driver library/sublibrary to the LIBDEF search chain. (See the sample source member JCLNET in the source library for an example of Entire Net-Work startup JCL.)

Step 3. Add the SSL DRIVER and LINK Statements

Use the existing Entire Net-Work configuration to create the necessary SSL DRIVER and LINK statements for your environment in the Entire Net-Work DDKARTE input file.

Note:
If you are installing the SSL line driver on z/VSE systems, the value of the SSL DRIVER's API parameter must be "CNS".

Step 4. Configure Client Information

For a client to correctly send the database request to the Entire Net-Work node where the database is located, Adabas Directory Server entries must be added for each database. These entries tell the client application where the server (Entire Net-Work) is located and which databases it serves. A Directory Server access entry must be added for each database that the client will call via the security option of the SSL line driver.

For more information, read *Access and Connection Definition Setup*.

Step 5. Start Entire Net-Work and Verify the Installation

Because of the many possible variations of the Entire Net-Work, Adabas, and applications topology, Software AG does not provide standard installation verification procedures. However, the following procedure is suggested for verifying the SSL line driver installation:

1. Start the Entire Net-Work system and make connections to each link defined to the system.
2. Test the connections and verify that the links can be established from either side by connecting and disconnecting the links several times from each node. While the links are connected, issue the Entire Net-Work operator command DISPLAY TARGET to display the targets and the nodes on which they are located.
3. Test your applications running across Entire Net-Work. At first, run one application at a time, and then verify the results.
4. For the final verification test, run a load test through the network (that is, multiple users on each node accessing data on the partner node).

Open Systems Installation

On open systems, the installation of Encryption for Entire Net-Work involves installing the open source SSL Toolkit that you can use to create certificates. This section describes general information you should understand prior to completing the installation as well as providing installation and uninstallation steps for Windows environments.

Note:
The Entire Net-Work OpenSSL support code is no longer included in Encryption for Entire Net-Work. Instead, it is installed automatically when you install Entire Net-Work or Entire Net-Work Client.

- License Key Requirements, File Location, and Use
- Windows Installation Steps
- Uninstalling Encryption for Entire Net-Work

License Key Requirements, File Location, and Use

To use SSL and Encryption for Entire Net-Work on open systems, you must have an Entire Net-Work license that supports it. Contact your Software AG support representative to obtain one.

The Entire Net-Work license key file is generally distributed on diskette, although, in special cases, it can be shipped via e-mail. The file name is in the following format, where *vr* is the version and release number of the product: *wcpvrm.xml* (Entire Net-Work Server) or *wclvrm.xml* (Entire Net-Work Client).

Be sure that the file containing the license key is in a location that will be accessible during the Entire Net-Work installation, such as on the file system or in a disk drive. During the installation of Entire Net-Work with the InstallShield, you are asked to locate the license file. Once it is located, the license file will be copied into a Software AG common area.

If you are installing Entire Net-Work on a laptop and you have received your license file on a diskette, note that some laptop configurations do not allow you access to the CD-ROM drive and the diskette drive simultaneously. In such cases you must copy the license file to a location that is accessible while the CD-ROM drive is in use, such as your laptop’s hard disk, before you start the installation procedure. In general, Software AG recommends that you place the license file on the file system before starting the installation procedure.

Note:
The license file is sometimes transmitted via e-mail. If you received the file via e-mail, copy it to a directory on your hard drive. If you received the file on a floppy disk, you may leave it there.

The license key file is provided as an XML document. This document can be viewed, using a browsing tool or text editor. It contains text, which represents the licensing information and a digital signature. It displays Software AG legal notices, copyright information, etc., as well as the product license information.

⚠ **Warning:**
Any modification of the license key file will invalidate the digital signature and the license key check will fail. If the check fails, you will not be able to install or run the product. In the event of a check failure, please contact your Software AG Support representative.

Windows Installation Steps

If you decide to use the SSL Toolkit to create certificates, transfer the SSL toolkit zip file to a directory to which you have write authorization outside of the Entire Net-Work or Entire Net-Work Client installation directory.

The SSL Toolkit zip file is called *wsl120_win32.zip*. To obtain this file, contact your Software AG support representative.

Note:
The SSL Toolkit is a 32-bit application that runs in both 32-bit and 64-bit environments.

Once the file is transferred to an appropriate Windows directory, unzip it. For information on using the SSL Toolkit to create certificates, read *Using the SSL Toolkit*.

Uninstalling Encryption for Entire Net-Work

The SSL Toolkit is uninstalled simply by deleting its unzipped files.