Access and Connection Definition Setup

To use Encryption for Entire Net-Work, the existing target definitions for your Adabas databases (on mainframe and open systems) must be updated to support secured communications. Each definition must be altered so that the protocol type "SSL" is specified in the access or connection definition and appropriate security parameters are specified.

These definitions are altered via their Adabas Directory Server entries or the Entire Net-Work Client, Kernel, and server access or connection definitions in the System Management Hub.

This chapter covers the following topics:

- Maintaining Target Definitions
- Security Parameters

Maintaining Target Definitions

The target definitions for each database that will be accessed through a secure connection must be altered to specify "SSL" as the protocol type. The format of a secured target entry is:

```
SSL://host:port[?parm=value][&parm=value]...
```

In addition to specifying appropriate host and port numbers, you must change the communication protocol type to "SSL" (as shown) and specify any security parameters that may be required. To determine which specific qualifiers and parameters should be supplied for different security situations, read *Security Scenarios*. The possible parameters are documented in *Security Parameters*.

The port number must match the setting on the SSL line driver SERVERID parameter. If one line driver will serve multiple databases, an entry for each database is required, but these entries would all specify the same port number.

Security Parameters

The following table describes the security parameters that can be used to support secured transmissions with Entire Net-Work.

Parameter	Description	Server Requirements	Client Requirements
CAFILE	The name of the file containing the trusted certificate authority’s (CA) certificates. The certificate of the CA that signed an inbound certificate must reside in this file or in the CAPATH directory. It is a good idea to store this file on a protected network drive. If a specified certificate is corrupt, secured transmissions will fail. If a certificate is received that is signed by a CA other than the CA specified by CAFILE, then the CAPATH is searched. **Note:** The file name specified may include the path information, unless a value for parameter CAPATH is specified.	Required only for client authentication.	Required only for server authentication.
CAPATH	The location (path) where the CAFILE resides or where additional certificates of certificate authorities (CA) reside. **Note:** The hash values of the names of the CA certificate files should be used in this location. Hash names are generated by the OpenSSL tool. If parameter CAFILE includes location information, the value of CAPATH should be ".", which is also the CAPATH default.	Required only for client authentication.	Required only for server authentication.

Parameter	**Description**	**Server Requirements**	**Client Requirements**
CERT_FILE	The file containing the participant's digital certificate. The certificate file may contain the participant's private key. It is a good idea to store this file on a protected network drive. **Note:** The file name specified may include the path information. This is useful if the certificate is not in the current directory.	Always required.	Required only for client authentication.
CERT_PSSWD	The password for extracting information from the certificate file specified in the CERT_FILE parameter. It is a good idea to store this file on a protected network drive. **Note:** You can specify a fully qualified file name for this parameter. In this case, the file name you provide must contain the password.	Always required.	Required only for client authentication.
KEY_FILE	The name of the file containing the server's private key. This parameter must be specified if the private key is kept separate from the certificate file. It is a good idea to store this file on a protected network drive. **Note:** The file name specified may include the path information. This is useful if the certificate is not in the current directory.	Always required.	Required only for client authentication.

Parameter	Description	Server Requirements	Client Requirements
RANDOM_FILE	Identifies a text file that contains at least 14 random characters. The random characters in this file are used by the encryption routines to ensure that encryption itself occurs in a random manner. Some platforms (such as Solaris) require the use of a random file.	Optional	Optional
VERIFY	The level of certificate verification to perform. Valid values are: ● 0 (No peer verification occurs.) ● 1 (The application requests that the peer certificate be verified.) ● 2 (The application requests that the peer certificate be verified. A fatal condition occurs if there is no certificate.) ● 4 (The application requests that the peer certificate be verified only once.) ● 8 (The application requests that the issuer name is checked against the host name.) Values 1, 2, and 4 can be specified in combination. For example, if you want to specify both 1 and 2, you would add them and set the VERIFY parameter to "3". **Note:** This parameter must be set to "3" if you are performing client authentication.	Use VERIFY=1 to request a client certificate and verify that it is sent. Use VERIFY=2 to force the sending of a client certificate. Use VERIFY=4 to limit the client certificate request to a single occurrence. VERIFY=8 is not valid for server processing.	Use VERIFY=0 (the C client default) to request a certificate but proceed even if certificate errors are found. Use VERIFY=1 to validate the server certificate. VERIFY=2 is not valid for client processing. VERIFY=4 is not valid for client processing. Use VERIFY=8 to validate that the common name of the received certificate matches the host name specified in the target entry.

Parameter	Description	Server Requirements	Client Requirements
VERSION	The version of SSL to use for processing. Valid values range from 1 through 4: ● 1: (TLSv1) ● 2: (SSLv2) ● 3: (SSLv23). For C applications only, this indicates that Version 2 or 3 should be used. ● 4: (SSLv3)	Optional	Optional