Security Scenarios

This chapter describes various mainframe and open system SSL scenarios using Encryption for Entire Net-Work.

- Mainframe Scenarios
- Open Systems Scenarios

Mainframe Scenarios

The following information is supplied for each mainframe scenario described in this section:

- The client-side alterations you need to make to your database entries in either your Directory Server definitions or the Entire Net-Work Client definitions in the System Management Hub, as well as what parameters you must specify on those entries. For more information about these definitions, read *Access and Connection Definition Setup*.
- The server-side data sets that must be defined in the Entire Net-Work startup JCL as well as the SSL DRIVER statement parameters that are expected.

The scenarios that are described are:

- Simple Encryption
- Client-Only Authentication
- Server-Only Authentication
- Client and Server Authentication
- Simple Encryption Between Entire Net-Work 7 and Entire Net-Work on the Mainframe

Simple Encryption

To perform simple encryption from a client:

- Change the communication protocol type to "SSL". For example, suppose the existing entry specified this:

  ```
  TCPIP://ahost:9734
  ```

  In this example, you would change the entry to look like this:

  ```
  SSL://ahost:9734
  ```

  This update can be made using the System Management Hub in either your Directory Server definitions or the Entire Net-Work Client definition. For more information, read *Access and Connection Definition Setup*.

To perform simple encryption from a server:

1. Make sure the data sets and members defined by the following symbolic names are supplied in the Entire Net-Work startup JCL:

   - NETPC
   - NETPK
   - NETRND

   For more information about each of these data sets, read *Step 6. Alter the Entire Net-Work Startup JCL* in *Mainframe Activation*.

2. Specify the SSL DRIVER statement in the Entire Net-Work startup JCL. For more information, about the SSL DRIVER statement, read *SSL DRIVER Statement*.

Client-Only Authentication

To perform client-only authentication from a client:

- Change the communication protocol type to "SSL" and specify values for the CERT_FILE, CERT_PSSWD, and KEY_FILE parameters. For example, suppose the existing entry specified this:

  ```
  TCPIP://ahost:9734
  ```

  In this example, you might change the entry to look like this:

  ```
  SSL://ahost:9734?CERT_FILE=testcert.pem&KEY_FILE=testkey.pem&CERT_PSSWD=testing
  ```

  This update can be made using the System Management Hub in either your Directory Server definitions or the Entire Net-Work Client definition. For more information, read *Access and Connection Definition Setup*.

To perform client-only authentication from a server:

1. Make sure the data sets and members defined by the following symbolic names are supplied in the Entire Net-Work startup JCL:

   - NETCAF
   - NETPC
   - NETPK
   - NETPSW
   - NETRND

   For more information about each of these data sets, read *Step 6. Alter the Entire Net-Work Startup JCL* in *Mainframe Activation*.

2. Specify the SSLCAF (SSLCAF=YES), SSLVRF (SSLVRF=3), and SSLVRS (SSLVRS=2) parameters on the SSL DRIVER statement in the Entire Net-Work startup JCL. The SSLVRF and SSLVRS parameters are optional. For more information, about the SSL DRIVER statement, read *SSL DRIVER Statement*.

Server-Only Authentication

To perform server-only authentication from a client:

- Change the communication protocol type to "SSL" and specify values for the CAFILE, CAPATH, and VERIFY parameters. For example, suppose the existing entry specified this:

  ```
  TCPIP://ahost:9734
  ```

  In this example, you might change the entry to look like this:

  ```
  SSL://ahost:9734?CAFILE=cacert.pem&CAPATH=path.&VERIFY=1
  ```

  This update can be made using the System Management Hub in either your Directory Server definitions or the Entire Net-Work Client definition. For more information, read *Access and Connection Definition Setup*.

To perform server-only authentication from a server:

1. Make sure the data sets and members defined by the following symbolic names are supplied in the Entire Net-Work startup JCL:

   - NETPC
   - NETPK
   - NETPSW
   - NETRND

   For more information about each of these data sets, read *Step 6. Alter the Entire Net-Work Startup JCL* in *Mainframe Activation*.

2. Specify the SSLVRF (SSLVRF=3) and SSLVRS (SSLVRS=2) parameters on the SSL DRIVER statement in the Entire Net-Work startup JCL. The SSLVRF and SSLVRS parameters are optional. For more information, about the SSL DRIVER statement, read *SSL DRIVER Statement*.

Client and Server Authentication

To perform client and server authentication from a client:

- Change the communication protocol type to "SSL" and specify values for the CAFILE, CAPATH, CERT_FILE, CERT_PSSWD, KEY_FILE, and VERIFY parameters. For example, suppose the existing entry specified this:

  ```
  TCPIP://ahost:9734
  ```

In this example, you might change the entry to look like this:

```
SSL://ahost:9734?CAFILE=cacert.pem&CAPATH=path&VERIFY=1&CERT_FILE=testcert.pem&KEY_FILE=testkey.pem&CERT_PSSWD=testing
```

This update can be made using the System Management Hub in either your Directory Server definitions or the Entire Net-Work Client definition. For more information, read *Access and Connection Definition Setup*.

To perform client and server authentication from a server:

1. Make sure the data sets and members defined by the following symbolic names are supplied in the Entire Net-Work startup JCL:

   - NETCAF
   - NETPC
   - NETPK
   - NETPSW
   - NETRND

   For more information about each of these data sets, read *Step 6. Alter the Entire Net-Work Startup JCL* in *Mainframe Activation*.

2. Specify the SSLCAF (SSLCAF=YES), SSLVRF (SSLVRF=3), and SSLVRS (SSLVRS=2) parameters on the SSL DRIVER statement in the Entire Net-Work startup JCL. The SSLVRF and SSLVRS parameters are optional. For more information, about the SSL DRIVER statement, read *SSL DRIVER Statement*.

Simple Encryption Between Entire Net-Work 7 and Entire Net-Work on the Mainframe

To perform simple encryption between Entire Net-Work 7 (open systems) and Entire Net-Work on the mainframe:

- Change the communication protocol type to "SSL" and specify values for the CAFILE, CAPATH, CERT_FILE, CERT_PSSWD, KEY_FILE, and VERIFY parameters. For example, suppose the existing entry specified this:

  ```
  TCPIP://USZHOST:9734?retry=32767&retryint=60&reconnect=yes
  ```

  In this example, you might change the entry to look like this:

  ```
  SSL://USZHOST:9734?retry=32767&retryint=60&reconnect=yes
  ```

  This update can be made using the System Management Hub in either your Directory Server definitions or the Entire Net-Work Client definition. For more information, read *Access and Connection Definition Setup*.

Open Systems Scenarios

For each open systems scenario described in this section, the client-side alterations you need to make to your Kernel and Entire Net-Work Client access and connection definitions are given.

The scenarios that are described are:

- Simple Encryption
- Client-Only Authentication
- Server-Only Authentication
- Client and Server Authentication
- Authentication with Certificates Elsewhere
- Authentication with a Hidden Password

Simple Encryption

To perform simple encryption for an Entire Net-Work Client:

1. Access the Entire Net-Work Client access definition to Adabas databases in the System Management Hub. For more information, read *Maintaining Adabas Access Definitions*, in the *Entire Net-Work Client Installation and Administration Guide*.
2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.
3. Save the definition.

To perform simple encryption for a Kernel connection:

1. Access the Kernel connection definition in the System Management Hub. For more information, read *Maintaining Connection Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.
2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.
3. Save the definition.

To perform simple encryption for an Entire Net-Work Server:

1. Access the Entire Net-Work Server Kernel access definitions in the System Management Hub. For more information, read *Adding Kernel Definitions* and *Maintaining Access Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.
2. For each Kernel definition that needs to support SSL, verify that either the **E-business SSL Access** or **E-business SSL Client Access** option is selected and that appropriate port numbers are specified.

3. For both **E-business SSL Access** and **E-business SSL Client Access**, specify valid values for the SSL CERT_FILE, KEY_FILE, and CERT_PSSWD parameters in the **Additional Parameters** field. In the following example, *xxcert.pem* is the certificate file, *xxkey.pem* is the certificate key file, and "pempswd" is the Public Encryption Method (PEM) password:

   ```
   &CERT_FILE=xxcert.pem&CERT_PSSWD=pempswd&KEY_FILE=xxkey.pem
   ```

4. Save the definition.

Client-Only Authentication

To perform client-only authentication for an Entire Net-Work Client:

1. Access the Entire Net-Work Client access definition to Adabas databases in the System Management Hub. For more information, read *Maintaining Adabas Access Definitions*, in the *Entire Net-Work Client Installation and Administration Guide*.

2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.

3. Specify values for the CERT_FILE, KEY_FILE, and CERT_PSSWD parameters in the **Additional Parameters** field. For example:

   ```
   &CERT_FILE=testcert.pem&KEY_FILE=testkey.pem&CERT_PSSWD=pempswd
   ```

4. Save the definition.

To perform client-only authentication for a Kernel connection:

1. Access the Kernel connection definition in the System Management Hub. For more information, read *Maintaining Connection Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.

2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.

3. Specify values for the CERT_FILE, KEY_FILE, and CERT_PSSWD parameters in the **Additional Parameters** field. For example:

   ```
   &CERT_FILE=testcert.pem&KEY_FILE=testkey.pem&CERT_PSSWD=pempswd
   ```

4. Save the definition.

To perform client-only authentication for an Entire Net-Work Server:

1. Access the Entire Net-Work Server Kernel access definitions in the System Management Hub. For more information, read *Adding Kernel Definitions* and *Maintaining Access Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.

2. For each Kernel definition that needs to support SSL client-only authentication, verify that the **E-business SSL Client Access** option is selected and that an appropriate port number is specified.

3. For **E-business SSL Client Access**, specify valid values for the CAFILE, CAPATH, CERT_FILE, KEY_FILE, CERT_PSSWD, and VERIFY parameters in the **Additional Parameters** field. The VERIFY parameter must be set to "3" for client authentication.

4. Save the definition.

Server-Only Authentication

To perform server-only authentication for an Entire Net-Work Client:

1. Access the Entire Net-Work Client access definition to Adabas databases in the System Management Hub. For more information, read *Maintaining Adabas Access Definitions*, in the *Entire Net-Work Client Installation and Administration Guide*.

2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.

3. Specify values for the CAFILE, CAPATH, and VERIFY parameters in the **Additional Parameters** field. For example:

   ```
   &CAFILE=cacert.pem&CAPATH=path&VERIFY=1
   ```

4. Save the definition.

To perform server-only authentication for a Kernel connection:

1. Access the Kernel connection definition in the System Management Hub. For more information, read *Maintaining Connection Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.

2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.

3. Specify values for the CAFILE, CAPATH, and VERIFY parameters in the **Additional Parameters** field. For example:

   ```
   &CAFILE=cacert.pem&CAPATH=path&VERIFY=1
   ```

4. Save the definition.

To perform server-only authentication for an Entire Net-Work Server:

1. Access the Entire Net-Work Server Kernel access definitions in the System Management Hub. For more information, read *Adding Kernel Definitions* and *Maintaining Access Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.

2. For each Kernel definition that needs to support SSL server-only authentication, verify that the **E-business SSL Access** option is selected and that an appropriate port number is specified.

3. For **E-business SSL Access**, specify valid values for the CERT_FILE, KEY_FILE, and CERT_PSSWD parameters in the **Additional Parameters** field. In the following example, *xxcert.pem* is the certificate file, *xxkey.pem* is the certificate key file, and "pempswd" is the Public Encryption Method (PEM) password:

```
&CERT_FILE=xxcert.pem&CERT_PSSWD=pempswd&KEY_FILE=xxkey.pem
```

4. Save the definition.

Client and Server Authentication

▶ **To perform client and server authentication for an Entire Net-Work Client:**

1. Access the Entire Net-Work Client access definition to Adabas databases in the System Management Hub. For more information, read *Maintaining Adabas Access Definitions*, in the *Entire Net-Work Client Installation and Administration Guide*.

2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.

3. Specify values for the CAFILE, CAPATH, CERT_FILE, KEY_FILE, CERT_PSSWD, and VERIFY parameters in the **Additional Parameters** field. For example:

   ```
   &CAFILE=cacert.pem&CAPATH=path&CERT_FILE=xxcert.pem&KEY_FILE=xxkey.pem&CERT_PSSWD=pempswd&VERIFY=1
   ```

4.

   ```
   &CERT_FILE=testcert.pem&KEY_FILE=testkey.pem&CERT_PSSWD=pempswd
   ```

5. Save the definition.

▶ **To perform client and server authentication for a Kernel connection:**

1. Access the Kernel connection definition in the System Management Hub. For more information, read *Maintaining Connection Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.

2. Change the communication protocol type to "SSL" by selecting the **SSL** or **SSL Protocol** radio button in the definition.

3. Specify values for the CAFILE, CAPATH, CERT_FILE, KEY_FILE, CERT_PSSWD, and VERIFY parameters in the **Additional Parameters** field. For example:

   ```
   &CAFILE=cacert.pem&CAPATH=path&CERT_FILE=xxcert.pem&KEY_FILE=xxkey.pem&CERT_PSSWD=pempswd&VERIFY=1
   ```

4. Save the definition.

▶ **To perform client and server authentication for an Entire Net-Work Server:**

1. Access the Entire Net-Work Server Kernel access definitions in the System Management Hub. For more information, read *Adding Kernel Definitions* and *Maintaining Access Definitions*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.

2. For each Kernel definition that needs to support SSL client and server authentication, verify that either the **E-business SSL Access** or **E-business SSL Client Access** option is selected and that appropriate port numbers are specified.

3. For **E-business SSL Access**, specify valid values for the CERT_FILE, KEY_FILE, and CERT_PSSWD parameters in the **Additional Parameters** field. In the following example, *xxcert.pem* is the certificate file, *xxkey.pem* is the certificate key file, and "pempswd" is the Public

Encryption Method (PEM) password:

```
&CERT_FILE=xxcert.pem&CERT_PSSWD=pempswd&KEY_FILE=xxkey.pem
```

4. For **E-business SSL Client Access**, specify valid values for the CAFILE, CAPATH, CERT_FILE, KEY_FILE, CERT_PSSWD, and VERIFY parameters in the **Additional Parameters** field. The VERIFY parameter must be set to "3" for client authentication.

5. Save the definition.

Authentication with Certificates Elsewhere

To perform client or server authentication from a client or a server when the certificates and certificate authorities are not in the current directory:

- Complete the authentication steps described in other scenarios in this section, but specify the path to the certificate authority and certificate files in the CAFILE, CERT_FILE, and KEY_FILE parameters.

  Note:
  If parameter CAFILE includes path information, the value of CAPATH should be ".".

Authentication with a Hidden Password

To perform client or server authentication from a client or a server without specifying the Public Encryption Method password directly in the target entries:

- Complete the authentication steps described in other scenarios in this section, but specify the fully-qualified file name of a file that contains the password in the CERT_PSSWD parameter. For example:

```
&CAFILE=cacert.pem&CAPATH=path&CERT_FILE=xxcert.pem&KEY_FILE=xxkey.pem&CERT_PSSWD=FILE://C:/certs/certpswd.txt&VERIFY=3
```