Gentran Integration Suite™

Implement SSL

Version 4.3

Sterling Commerce
An IBM Company

Implement SSL

What is SSL?

Secure Sockets Layer (SSL) is a protocol that provides secure communication over the Internet. It uses both symmetric and asymmetric cryptography.

The SSL protocol provides server authentication and client authentication:

- Server authentication is performed when a client connects to the server. After the initial handshake, the server sends its digital certificate to the client. The client validates the server certificate or certificate chain.
- Client authentication is performed when a server sends a certificate request to a client during the handshake. If the client certificate or chain is verified and the certificate verify message is verified, the handshake proceeds further.
- An optional additional authentication is performed by checking the common name in the certificate against the server's fully qualified domain name from a reverse Domain Name Server (DNS) lookup where the server's fully qualified domain name can be obtained.

Types of Trust

Gentran Integration Suite supports two types of trust for SSL certificates:

- CA Trust - Hierarchical trust based on a root certificate used to issue other certificates. This is the standard SSL certificate trust model.
- Direct Trust - Direct trust of self-signed certificates assumed to be distributed through secure out-of-band mechanisms. Direct trust and self-signed certificates are not part of the SSL standards, but are frequently used in certain trading communities.

SSL Certificates

To communicate using the SSL protocol in Gentran Integration Suite, configure the systems involved to support either server authentication or client/server authentication. To perform authentication against a server, you need a root Certificate Authority (CA) certificate and the set of intermediate certificates in the chain or, if the server uses a self-signed certificate, a copy of the self-signed certificate.

To support client/server authentication you need a CA or self-signed certificate and a system certificate.

You can obtain an SSL certificate from a trusted CA by providing a Certificate Signing Request (CSR) to the CA. The SSL certificate binds the public key and the SSL server or client.

You can check in a CA certificate or a self-signed certificate in a CA certificate store by selecting **Trading Partners** > **Digital Certificates** > **CA** > **Check in New Certificate**.

If you plan to use client/server authentication, configure a system certificate. You can create system certificate in the following ways:

- Checking in an existing key certificate file or pkcs12 file

- Generating a self-signed system certificate
- Using Certificate Wizard to generate a CSR and get a certificate from a CA

Certificates for Testing

For testing, you can use self-signed certificates. They can be generated and managed in Gentran Integration Suite. To create a self-signed certificate:

1. Select **Trading Partners** > **Digital Certificates** > **System Certificates** > **Create Self-Signed Certificate**.
2. After it is created, find it, and check it out to a file.
3. Check the certificate back in to Gentran Integration Suite as a CA certificate by selecting **Trading Partners** > **Digital Certificates** > **CA** > **Check In New Certificate**.

Configure Client Adapters for SSL

The following client adapters in Gentran Integration Suite support SSL:

- FTP Client adapter
- HTTP Client adapter
- Connect:Direct Requester adapter (with Secure+ Option)

Parameters for SSL can be set in the trading partner profile or for the adapter. For the FTP Client adapter, these parameters are set in the FTP Client Begin Session service. For the HTTP Client adapter, these parameters are set in the HTTP Client Begin Session service. Parameters set in the Begin Session service override settings in a trading partner profile.

There are slight variations in the parameter names and values. See the documentation for the specific adapter or service you are configuring. The following parameters control SSL from a client perspective:

Field	Description
SSL	Determines SSL socket negotiation. Optional. Valid values are: ◆ SSL_IMPLICIT – FTP server expects and requires SSL to happen automatically at the time of connection. CACertificateId is required. ◆ SSL_EXPLICIT – FTP client requests SSL and a secure connection is negotiated. CACertificateId is required. ◆ SSL_NONE – Connection will not use SSL. (Default)
CACertificateId (trusted_root)	List of trusted CA public certificates. In process data, this parameter is displayed as an object ID. Required if SSL = SSL_IMPLICT or SSL_EXPLICIT. Obtain an SSL certificate from a CA or from your trading partner. Check it into Gentran Integration Suite from the Admin menu by selecting **Trading Partner** > **Digital Certificates** > **CA** to make it available in the list.

Field	Description
CipherStrength	The level of encryption to apply to the data that flows through the socket connection. Optional. Valid values are: ◆ ALL – WEAK or STRONG is accepted ◆ WEAK – 40-bit encryption is required ◆ STRONG – 128-bit or higher encryption is required (Default)
SystemCertificateId	Select from the list of available system certificates. This certificate confirms the identity of the client to the server. Required if SSL = SSL_IMPLICIT or SSL_EXPLICIT and the server requires client authentication. Select the client's system certificate.

Configure Server Adapters for SSL

The following server adapters in Gentran Integration Suite support SSL:

- FTP Server adapter
- HTTP Server adapter
- Connect:Direct Server adapter (with Secure+ Option)
- SMTP Send adapter

There are slight variations in the parameter names and values. See the documentation for the specific adapter or service you are configuring. The following parameters control SSL from a server perspective:

Field	Description
SSL	Whether SSL is active. Required. Valid values are: ◆ None – If SSL is requested by a client it will be rejected. (Default) ◆ Optional – SSL is used if requested by a client. ◆ Must – Clients who do not request SSL are not allowed to connect. **Note:** If Optional or Must is specified, the asset protection key must enable SSL for the appropriate protocol.
Key Certificate Passphrase	Password that protects the server key certificate. Required if SSL option is Must or Optional. This passphrase is used internally by the system to initialize the SSL libraries. It should be a strong password, but it does not need to correspond to any password used to check in certificates.
CipherStrength	Strength of the algorithms used to encrypt data. Required if SSL option is Must or Optional. Valid values are: ◆ ALL ◆ WEAK – Often required for international e-commerce, because government regulations prohibit STRONG encryption from being exported. ◆ STRONG (Default)
Key Certificate (System Store)	Private key and certificate for server authentication. Required if SSL option is Must or Optional.

Field	Description
CA Certificate	Certificate used to validate the certificate of a client. This is the public key. If no CA certificate is chosen, no client certification is performed. Optional.

Cipher Strength Settings

To implement a cipher strength setting, contact Customer Support.

Enable Earlier Versions of SSL

To enable an earlier version of SSL, contact Customer Support.

Troubleshoot SSL

Corrupt or Unusable Certificate Error Messages

If you receive the following error message:

```
FATAL Alert:BAD_CERTIFICATE - A corrupt or unusable certificate was
received.
```

The information from the Perimeter log is as follows:

```
ERROR <HTTPClientAdapter_HTTPClientAdapter_node1-Thread-19>
HTTPClientAdapter_HTTPClientAdapter_node1-Thread-172105824724com.sterlingcom
merce.perimeter.api.conduit.SSLByteDataConduit@4c2b95c6:Doing reset3
com.certicom.net.ssl.SSLKeyException: FATAL Alert:BAD_CERTIFICATE - A
corrupt or unusable certificate was received.
 at com.certicom.tls.d.b.a(Unknown Source)
 at com.certicom.tls.d.b.do(Unknown Source)
```

When checking in the certificate, Gentran Integration Suite shows a Status value of "Invalid Signature" on the naming screen. If a business process that performs an outbound HTTP POST with SSL fails on HTTP Method service with error, the following message is displayed::

```
HTTP Status Code: -1
HTTP Reason Phrase: Internal Error: Connection was closed from the perimeter
side with error: CloseCode.CONNECTION_RESET
```

Obtain the appropriate CA certificate for the trading partner. If the trading partner is using a self-signed certificate, the certificate itself can be used as the CA certificate.

CA and Direct Trust

When Gentran Integration Suite is the client, if the server has a certificate issued by a CA and that certificate has the DNS name of the server in the subject Relative Distinguished Names (RDN), you can put the root

CA certificate in the CA store and trust that. If SSL still does not work, try direct trust. Put the server certificate in the CA store and trust that.

If the server is using a self-signed certificate, put that in the CA store and trust it. You are doing direct trust in this case as well.

Use SSL without a Certificate

You cannot use SSL-enabled adapters without having the required certificate or system certificate.

Disable SSL Empty Records for CBC-Mode Cipher Suite

If you selected the CBC-mode cipher suite, and SSL does not work, disable SSL Empty Records:

1. Edit the tmp.sh file.
2. Find the server flag for the OS you are configuring and add:

```
-DDisableSSLEmptyRecords=true
```