Gentran Integration Suite™

Implementing SSL

Version 4.2

Sterling Commerce
An IBM Company

Implementing SSL

What is SSL?

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

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 checks that the certificate has not expired and that certificate path validation is acceptable. The client must have a trusted certificate that identifies the Certificate Authority.
- Client authentication is performed when a server sends a certificate request to a client during the handshake. If the client certificate is signed by a trusted source, the handshake will proceed. In order to perform this security check, the client must have a key certificate file configured and the server must have a trusted certificate that validates client's certificate path.
- An optional additional authentication is performed by checking the common name in the certificate against the server’s fully qualified domain name lookup in a reverse DNS where the server's fully qualified domain name can be obtained.

SSL Certificates

To communicate using the SSL protocol, you must configure the systems involved to support either server authentication or client-server authentication. To perform authentication against a server, you need a root CA certificate, an intermediate CA, or a self-signed certificate that can be used to verify the server’s certificate or chain. If you are dealing with a trusted partner, such as an internal department, you can use a server’s certificate received by independent means (such as email) on the client side to verify the server’s certificate received during the handshake.

To support client-server authentication you need both an SSL certificate and a private key.

You obtain an SSL certificate from a trusted Certificate Authority (CA) by providing a CSR to the CA. The SSL certificate proves the binding between the public key and the SSL server or client.

After you receive the SSL certificate, check it into Gentran Integration Suite at **Trading Partners** > **Digital Certificates** > **CA** > **Check in New Certificate**

If you plan to use client-server authentication:

1. You must append the SSL certificate to a private key to create a key certificate file.
2. You can use the Certificate Wizard at **Trading Partners** > **Digital Certificates** > **System** > **Certificate Signing Request** to create a Certificate Signing Request.
3. Send the request to a CA to get an SSL certificate.
4. Create a key certificate file and check it in at **Trading Partners** > **Digital Certificates** > **System**.

Certificates for Testing

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

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

Configuring 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 Certificate Authority 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 Certificate Authority or from your trading partner. Check it into Gentran Integration Suite from the Admin menu selecting **Trading Partner** > **Digital Certificates** > **CA** to make it available in this list.
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)

Field	Description
SystemCertificateId	Select from the list of Private Keys/Public Certificates that are signed by the trading partner Trusted Certificate Authority. 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. Obtain the certificate from your trading partner. Check it into Gentran Integration Suite from the Admin menu selecting **Trading Partner** > **Digital Certificates** > **System** to make it available in this list.

Configuring 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 Secure Sockets Layer (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 that 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.
Cipher Strength	Strength of the algorithms used to encrypt data. Valid values are: ◆ ALL ◆ WEAK – Often required for international e-commerce, because government regulations prohibit STRONG encryption from being exported. ◆ STRONG Default is STRONG. Required if SSL option is Must or Optional.
Key Certificate (System Store)	Private key and certificate for server authentication. Required if SSL option is Must or Optional.
CA Certificate	Certificate used to validate the certificate of an client. This is the public key. If no CA certificate is chosen, no client certification is performed. Optional.

SSL Customizable Settings

The security.properties file contains lines that define the Weak, Strong, or All Cipher Suites and the valid values for each cipher strength. These are commented out by default and contain the values that Gentran Integration Suite uses based on the settings in the adapter configurations. To modify these, remove the # preceding the lines. You can change the order, add, or delete values to control which cipher is accepted.

Note: The order of the ciphers listed in each setting is significant. If you redefine or reorder them, you must test to ensure your intended cipher is supported and applied.

The following are the lines for customizing cipher strength for SSL in the security.properties file:

```
#SSL Customizable Settings
#WeakCipherSuite=TLS_RSA_EXPORT_WITH_RC4_40_MD5,TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
#StrongCipherSuite=TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WIT
H_AES_256_CBC_SHA,\
TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_MD5,TLS_RSA_WITH_RC4_128_MD
,TLS_RSA_WITH_DES_CBC_SHA
#AllCipherSuite=TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_A
ES_256_CBC_SHA,\
TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_MD5,TLS_RSA_WITH_RC4_128_MD5
,TLS_RSA_WITH_DES_CBC_SHA\
TLS_RSA_EXPORT_WITH_RC4_40_MD5,TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
```

Caution: If using TLS_RSA_WITH_3DES_EDE_CBC_MD5, you must have SSLHelloProtocol=TLS1/2HI in the security.properties.in file.

Enabling Previous Versions of SSL

By default, Gentran Integration Suite only accepts SSLv3 or TLSv1.0.

To circumvent this security feature, edit the SSLHelloProtocol value in the security.properties file. The possible values are as follows:

SSLHelloProtocol Value	Description
TLS1	TLS hello is sent; the client accepts SSL3 or TLS.
SSL3	SSL3 hello is sent; the client accepts SSL3 or SSL2.
TLS1/2HI	SSL2 hello is sent; the client accepts SSL2, SSL3, or TLS.
SSL3/2HI	SSL2 hello is sent; the client accepts SSL3 or SSL2.
TLS1-ONLY	TLS hello is sent; the client accepts TLS.
SSL3-ONLY	SSL3 hello is sent; the client accepts SSL3.
ANY	Synonymous with TLS1/2HI