StreamServe™ Persuasion™

StreamServe Persuasion SP5 Encryption and Authentication

User Guide

Rev A

StreamServe Persuasion SP5 Encryption and Authentication User Guide
Rev A

StreamServe Web Site

Contents

About encryption and authentication

A StreamServer application can be configured as an SSL server or SSL client that communicates over an encrypted HTTPS channel.

Authentication

An SSL server must always authenticate itself to all SSL clients, and the SSL client must authenticate itself to the SSL server if the SSL server requires client authentication.

S/MIME

Encryption and authentication can also be applied to data sent via email, where the StreamServer application uses S/MIME to sign and encrypt/decrypt emails.

Digital certificates

SSL servers and clients use digital certificates for encryption and authentication. A digital certificate is used to verify that a user sending a message is who he claims to be, and to provide the receiver with the means to encode a reply.

Certificate Authority

A Certificate Authority (CA) is a trusted third-party organization or company that issues digital certificates.

Certificate chain

A certificate chain is a tree structure of certificates. The validity of a certificate in a certificate chain is verified by the certificate one level up in the tree. The root node in the tree is the self signed root CA certificate.

Before the StreamServer can trust a certificate provided by an SSL server or client, it must verify the complete certificate chain – up to the root CA certificate. To be able to do this, it must have access to all certificates in the certificate chain.

Certificate chain example

In this example, a three level deep certificate chain consists of the following certificates:

- Root CA certificate (level 1).
    - Intermediate CA certificate (level 2).
    - Subject certificate (level 3).

The level 1 and 2 certificates are available to the SSL client in this example, and the level 3 certificate is sent by the SSL server to the SSL client.

1. The SSL client sends a request to an SSL server that returns the level 3 certificate.
2. The SSL client uses the public key embedded i the level 2 certificate to verify the signature of the level 3 certificate, and to verify that the level 3 certificate has not been revoked.
3. If the level 3 certificate is OK, the SSL client uses the public key embedded i the level 1 certificate to verify the signature of the level 2 certificate, and to verify that the level 2 certificate has not been revoked.
4. If the level 2 certificate is OK, the SSL client verifies the self signed level 1 certificate. It uses the public key embedded i the level 1 certificate to verify the signature of the level 1 certificate, and to verify that the level 1 certificate has not been revoked.
5. If all tests are OK, the complete certificate chain can be trusted, and the identity and integrity of the level 3 certificate is verified.

Security configurations

In Design Center, digital certificates are managed using a specific resource type called security configuration. There are two types of security configurations:

- **Trust Server** – all certificate information is retrieved from an XKMS (XML Key Management Specification) compliant Trust Server. Only the certificate chain that verifies the identity of the Trust Server is stored locally. See *Trust Server security configurations* on page 12.
- **Legacy** – all certificate and private key data is stored locally. See *Legacy security configurations* on page 22.

Entropy

When running on a Windows platform, the StreamServer uses a default entropy source to generate randomness for SSL. When running on a UNIX platform, the StreamServer searches for the entropy using the following sources:

- `/dev/random`
- `/var/run/egd-pool`
- `/dev/egd-pool`
- `/etc/egd-pool`
- `/etc/entropy`
- `/dev/urandom`

The StreamServer only uses the first source found in the list, starting at the top. You must make sure that the appropriate entropy source is available.

Note: If no source is found in the list above, the StreamServer will use an entropy source of low quality.

Trust Server administration

The Trust Server is installed separately. For information on how to administer the Trust Server, see the documentation included in the Trust Server installation.

Creating security configurations

You can create security configurations for different purposes. For example, if the StreamServer is both an SSL server (specified using an HTTPS input connector) and an SSL client (specified using an HTTPS Submit output connector or HTTPS Poll input connector), you can create one security configuration for the server and another for the client. Then you connect the server security configuration to the HTTPS input connector, and the client security configuration to the HTTPS Submit output connector.

Note: You should be experienced in the area of SSL and S/MIME to be able to create security configurations.

Trust Server security configurations

If the StreamServer and all involved parties (SSL server/client and email sender/receiver) are registered in a Trust Server, you can use Trust Server security configurations. In this case all certificate information is retrieved from the Trust Server, and only the certificates that verify the identity of the Trust Server are stored locally.

Prerequisites

- The certificates that verify the identity of the Trust Server are added to the same resource set as the security configuration.
- The certificates for all involved parties (SSL server/client and email sender/receiver) are registered in the Trust Server.

To create a Trust Server security configuration

1. In a resource set, create a new Security Configuration resource.
2. Give the security configuration a unique name.
3. Open the security configuration and select the type **Trust Server**.
4. On the Certificates tab, add all the certificate resources to include in the certificate chain used to verify the identity of the Trust Server.
5. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.

Depending on the purpose of the security configuration, you must also configure a number of additional parameters:

- *Security configuration for an SSL server* on page 12
- *Security configuration for an SSL client* on page 13
- *Security configuration for signing emails* on page 13
- *Security configuration for rejecting emails from non-trusted addresses* on page 14
- *Security configuration for encrypting emails* on page 14
- *Security configuration for receiving encrypted emails* on page 15

Security configuration for an SSL server

You can run the StreamServer as an SSL server that communicates with one or more SSL clients. To achieve this, you must create a security configuration and an HTTPS input connector, and connect the security configuration to the HTTPS input connector.

To create a security configuration

1. Create a new security configuration. See *To create a Trust Server security configuration* on page 12.

2 On the HTTP tab, enter the **Key name** and **Passphrase** to access the StreamServer private key.

To connect the security configuration to the connector

1 Open the HTTPS input Connector Settings dialog box.

2 In the **Security configuration** field, browse to and select the security configuration.

Security configuration for an SSL client

You can run the StreamServer as an SSL client that communicates with an SSL server. To achieve this, you must create a security configuration and an HTTPS Submit output connector (or HTTPS Poll input connector), and connect the security configuration to the connector.

To create a security configuration

1 Create a new security configuration. See *To create a Trust Server security configuration* on page 12.

2 If the SSL server requires client authentication, you must also select the **HTTP** tab and enter the **Key name** and **Passphrase** to access the StreamServer private key.

To connect the security configuration to an HTTPS Submit output connector

1 Open the HTTPS Submit Output Connector Settings dialog box.

2 Select **Use security configuration**.

3 In the **Security configuration** field, browse to and select the security configuration.

To connect the security configuration to an HTTPS Poll input connector

1 Open the HTTPS Poll Input Connector Settings dialog box.

2 In the **Security configuration** field, browse to and select the security configuration.

Security configuration for signing emails

The StreamServer can sign emails. The email recipients use the signature to verify that the email comes from a trusted address. To achieve this you must create a security configuration for each From address, and enable signing of emails on the output connector that delivers the emails (`SMTP (MIME)` or `SMTP (MIME) for MailOUT`).

To create a security configuration

1 Create a new security configuration. See *To create a Trust Server security configuration* on page 12.

2 On the Email tab, enter the **Key name** and **Passphrase** to access the private key for the From address.

To enable signing

Open the email Output Connector Settings dialog box and select **Sign**.

Security configuration for rejecting emails from non-trusted addresses

The StreamServer can reject emails from non-trusted addresses. The StreamServer uses the sender's public key to verify the identity of the sender. To achieve this you must create a security configuration, and enable rejection of emails on the EmailIN input connector.

To create a security configuration

Create a new security configuration. See *To create a Trust Server security configuration* on page 12.

To enable rejection

1 Open the EmailIN input Connector Settings dialog box and select **Retrieve email** > **Advanced**.

2 Select **Request signature**.

Security configuration for encrypting emails

The StreamServer can encrypt emails, and prevent emails from being sent to non-trusted addresses. The StreamServer encrypts an email with the recipient's public key. To achieve this you must create a security configuration, and enable encryption of emails on the output connector that delivers the emails (`SMTP (MIME)` or `SMTP (MIME) for MailOUT`).

To create a security configuration

Create a new security configuration. See *To create a Trust Server security configuration* on page 12.

To enable encryption

Open the email Output Connector Settings dialog box and select **Encrypt**.

Security configuration for receiving encrypted emails

The StreamServer can decrypt received emails, and reject unencrypted emails. The StreamServer decrypts emails with the private key. To achieve this you must create a security configuration, and enable rejection of unencrypted emails on the EmailIN input connector.

To create a security configuration

1. Create a new security configuration. See *To create a Trust Server security configuration* on page 12.
2. On the Email tab, enter the **Key name** and **Passphrase** to access the private key for the recipient address.

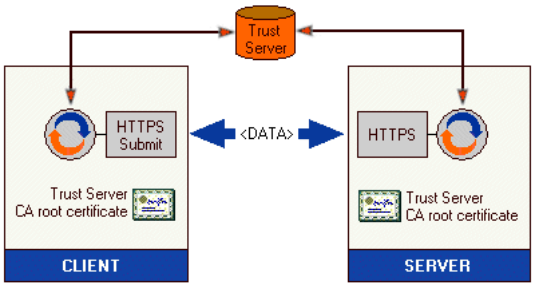
To enable rejection of unencrypted emails

1. Open the EmailIN input Connector Settings dialog box and select **Retrieve email** > **Advanced**.
2. Select **Request encryption**.

Trust Server scenarios

SSL server and SSL client

This scenario involves the two StreamServers SERVER and CLIENT. The SERVER communicates via an HTTPS input connector, and the CLIENT communicates via an HTTPS Submit output connector.



Prerequisites

- Both SERVER and CLIENT use SSL version SSLv3.
- Both SERVER and CLIENT have the following resource in the default resource set:
  - **TS root.cer** – the Trust Server CA root certificate. This is the only certificate in the certificate chain.

Configuring the SERVER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SSL SERVER.
2. Open SSL SERVER and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.
5. On the HTTP tab, enter the **Key name** and **Passphrase** to access the SERVER private key.

Configure the HTTPS input connector

1. Select **security configuration** > **SSL SERVER**.
2. Select **SSL Version** > **SSLv3**.

Configuring the CLIENT

Create the Security configuration

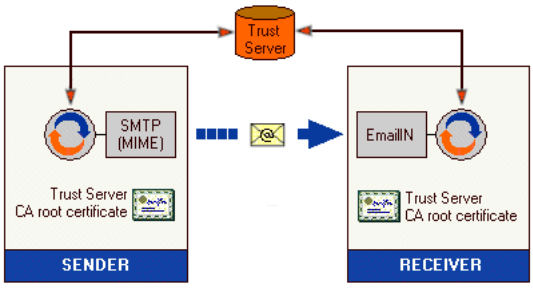
1. Add a security configuration to the default resource set and rename it to `SSL CLIENT`.
2. Open `SSL CLIENT` and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.
5. On the HTTP tab, enter the **Key name** and **Passphrase** to access the `CLIENT` private key.

Configure the HTTPS Submit output connector

1. Select **Use security configuration**.
2. Select **Security configuration** > **SSL CLIENT**.
3. Select **SSL Version** > **SSLv3**.

Encrypted emails

This scenario involves the two StreamServers `SENDER` and `RECEIVER`. The `SENDER` sends encrypted emails to the `RECEIVER` via an SMTP (MIME) output connector, and the `RECEIVER` receives the emails via an EmailIN input connector.



Prerequisites

Both `SENDER` and `RECEIVER` have the following resource in the default resource set:

- **TS root.cer** – the Trust Server CA root certificate. This is the only certificate in the certificate chain.

Configuring the SENDER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to ENCRYPT.
2. Open ENCRYPT and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.

Configure the SMTP (MIME) output connector

Select **Encrypt**.

Configuring the RECEIVER

Create the Security configuration

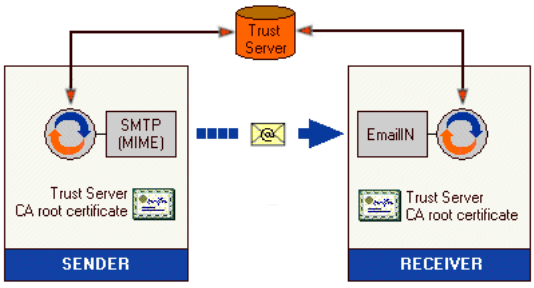
1. Add a security configuration to the default resource set and rename it to DECRYPT.
2. Open DECRYPT and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.
5. On the Email tab, enter the **Key name** and **Passphrase** to access the private key for the recipient address.

Configure the EmailIN input connector

1. Select **Retrieve email** > **Advanced**.
2. Select **Request encryption**.

Signed emails

This scenario involves the two StreamServers SENDER and RECEIVER. The SENDER sends signed emails to the RECEIVER via an SMTP (MIME) output connector, and the RECEIVER receives the emails via an EmailIN input connector.



Prerequisites

Both SENDER and RECEIVER have the following resource in the default resource set:

- **TS root.cer** – the Trust Server CA root certificate. This is the only certificate in the certificate chain.

Configuring the SENDER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SIGN.
2. Open SIGN and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.
5. On the Email tab, enter the **Key name** and **Passphrase** to access the private key for the sender address.

Configure the SMTP (MIME) output connector

Select **Sign**.

Configuring the RECEIVER

Create the Security configuration

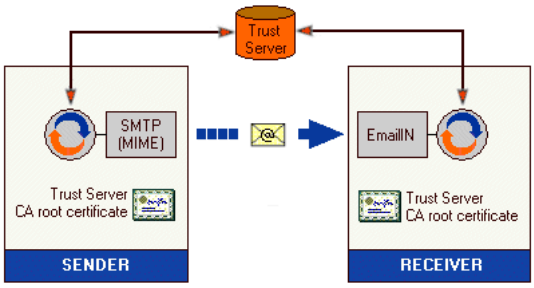
1. Add a security configuration to the default resource set and rename it to SIGNED.
2. Open SIGNED and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.

Configure the EmailIN input connector

1. Select **Retrieve email** > **Advanced**.
2. Select **Request signature**.

Encrypted and signed emails

This scenario involves the two StreamServers SENDER and RECEIVER. The SENDER sends signed and encrypted emails to the RECEIVER via an SMTP (MIME) output connector, and the RECEIVER receives the emails via an EmailIN input connector.



Prerequisites

Both SENDER and RECEIVER have the following resource in the default resource set:

- **TS root.cer** – the Trust Server CA root certificate. This is the only certificate in the certificate chain.

Configuring the SENDER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SIGN_ENCRYPT.
2. Open SIGN_ENCRYPT and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.
5. On the Email tab, enter the **Key name** and **Passphrase** to access the private key for the sender address.

Configure the SMTP (MIME) output connector

Select **Sign** and **Encrypt**.

Configuring the RECEIVER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SIGNED_ENCRYPTED.
2. Open SIGNED_ENCRYPTED and select the type **Trust Server**.
3. On the Certificates tab, add the certificate resource **TS root.cer**.
4. On the Trust Server tab, enter the Trust Server **URL**, and the **User** name and **Password** to access the Trust Server.

5 On the Email tab, enter the **Key name** and **Passphrase** to access the private key for the recipient address.

Configure the EmailIN input connector

1 Select **Retrieve email** > **Advanced**.

2 Select **Request signature** and **Request encryption**.

Legacy security configurations

If the StreamServer, or any of the involved parties (SSL server/client and email sender/receiver), are not registered in a Trust Server, you can create security configurations using locally stored certificates.

To create a Legacy security configuration

1 In a resource set, create a new Security Configuration resource.

2 Give the security configuration a unique name.

3 Open the security configuration and select the type **Legacy**.

Depending on the purpose of the security configuration, you must also configure a number of additional parameters:

- *Security configuration for an SSL server (with client authentication)* on page 22.
- *Security configuration for an SSL server (without client authentication)* on page 23.
- *Security configuration for an SSL client (with client authentication)* on page 24.
- *Security configuration for an SSL client (without client authentication)* on page 25.
- *Security configuration for signing emails* on page 25.
- *Security configuration for rejecting emails from non-trusted addresses* on page 26.
- *Security configuration for encrypting emails* on page 26.
- *Security configuration for receiving encrypted emails* on page 27.

Security configuration for an SSL server (with client authentication)

You can run the StreamServer as an SSL server that requires client authentication. To achieve this, you must create a security configuration and an HTTPS input connector, and connect the security configuration to the HTTPS input connector.

Multiple clients

If the StreamServer communicates with multiple clients, you must:

- Create one security configuration per client.
- Create one HTTPS input connector per client. These connectors cannot share the same port.

Prerequisites

- The StreamServer private key file is added to the same resource set as the security configuration.

- The StreamServer CA root certificate is distributed to the clients.
- The certificates that verify the identity of the client are added to the same resource set as the security configuration.
- The client certificate is added to the same resource set as the security configuration.

To create a security configuration

1. Create a new security configuration. See *To create a Legacy security configuration* on page 22.
2. On the Certificates tab, add all the certificate resources to include in the certificate chain used to verify the identity of the client.
3. Click the **HTTP Server** tab.
4. Select the StreamServer **Private key file** and enter the **Password** to access the private key.
5. Select **Client authentication** and select the **Client certificate**.

To connect the security configuration to the connector

1. Open the HTTPS input Connector Settings dialog box.
2. In the **Security configuration** field, browse to and select the security configuration.

Security configuration for an SSL server (without client authentication)

You can run the StreamServer as an SSL server that does not require client authentication. To achieve this, you must create a security configuration and an HTTPS input connector, and connect the security configuration to the HTTPS input connector.

Prerequisites

- The StreamServer private key file is added to the same resource set as the security configuration.
- The StreamServer CA root certificate is distributed to the clients.

To create a security configuration

1. Create a new security configuration. See *To create a Legacy security configuration* on page 22.
2. Click the **HTTP Server** tab.
3. Select the StreamServer **Private key file** and enter the **Password** to access the private key.

To connect the security configuration to the connector

1. Open the HTTPS input Connector Settings dialog box.

2 In the **Security configuration** field, browse to and select the security configuration.

Security configuration for an SSL client (with client authentication)

You can run the StreamServer as an SSL client that communicates with an SSL server that requires client authentication. To achieve this, you must create a security configuration and an HTTPS Submit output connector (or HTTPS Poll input connector), and connect the security configuration to the connector.

Prerequisites

- The StreamServer private key file is added to the same resource set as the security configuration.
- The certificates that verify the identity of the SSL server are added to the same resource set as the security configuration.
- The StreamServer CA root certificate and client certificate are distributed to the SSL server.

To create a security configuration

1 Create a new security configuration. See *To create a Legacy security configuration* on page 22.

2 On the Certificates tab, add all the certificate resources to include in the certificate chain used to verify the identity of the SSL server.

3 Click the **Email and HTTP client** tab.

4 Select the StreamServer **Private key file** and enter the **Password** to access the private key.

To connect the security configuration to an HTTPS Submit output connector

1 Open the HTTPS Submit Output Connector Settings dialog box.

2 Select **Use security configuration**.

3 In the **Security configuration** field, browse to and select the security configuration.

To connect the security configuration to an HTTPS Poll input connector

1 Open the HTTPS Poll Input Connector Settings dialog box.

2 In the **Security configuration** field, browse to and select the security configuration.

Security configuration for an SSL client (without client authentication)

You can run the StreamServer as an SSL client that communicates with an SSL server that does not require client authentication. To achieve this, you must create a security configuration and an HTTPS Submit output connector (or HTTPS Poll input connector), and connect the security configuration to the connector.

Prerequisites

The certificates that verify the identity of the SSL server are added to the same resource set as the security configuration.

To create a security configuration

1. Create a new security configuration. See *To create a Legacy security configuration* on page 22.
2. On the Certificates tab, add all the certificate resources to include in the certificate chain used to verify the identity of the SSL server.

To connect the security configuration to an HTTPS Submit output connector

1. Open the HTTPS Submit Output Connector Settings dialog box.
2. Select **Use security configuration**.
3. In the **Security configuration** field, browse to and select the security configuration.

To connect the security configuration to an HTTPS Poll input connector

1. Open the HTTPS Poll Input Connector Settings dialog box.
2. In the **Security configuration** field, browse to and select the security configuration.

Security configuration for signing emails

The StreamServer can sign emails. Email recipients use the signature to verify that the email comes from a trusted address. To achieve this you must create a security configuration for each From address, and enable signing of emails on the output connector that delivers the emails (`SMTP (MIME)` or `SMTP (MIME) for MailOUT`).

Prerequisites

- The StreamServer private key file is added to the same resource set as the security configuration.
- The StreamServer CA root certificate is distributed to the recipients.

To create a security configuration

1 Create a new security configuration. See *To create a Legacy security configuration* on page 22.

2 Click the **Email and HTTP client** tab.

3 Select the StreamServer **Private key file** and enter the **Password** to access the private key.

To enable signing

Open the email Output Connector Settings dialog box and select **Sign**.

Security configuration for rejecting emails from non-trusted addresses

The StreamServer can reject emails from non-trusted addresses. The StreamServer uses the sender's public key to verify the identity of the sender. To achieve this you must create a security configuration, and enable rejection of emails on the EmailIN input connector.

Prerequisites

- The certificates that verify the identity of the email sender are added to the same resource set as the security configuration.
- If the email senders have different CA root certificates, you must create one security configuration for each CA root certificate.

To create a security configuration

1 Create a new security configuration. See *To create a Legacy security configuration* on page 22.

2 On the Certificates tab, add all the certificate resources to include in the certificate chain used to verify the identity of the email sender.

To enable rejection

1 Open the EmailIN input Connector Settings dialog box and select **Retrieve email** > **Advanced**.

2 Select **Request signature**.

Security configuration for encrypting emails

The StreamServer can encrypt emails, and prevent emails from being sent to non-trusted addresses. The StreamServer encrypts an email with the recipient's public key. To achieve this you must create a security configuration, and enable encryption of emails on the output connector that delivers the emails (`SMTP (MIME)` or `SMTP (MIME) for MailOUT`).

Prerequisites

The encryption certificates for all email addresses are added to the same resource set as the security configuration. Each certificate resource must be renamed to <*email address*>.*crt*, for example `arnold_abc.com.crt`.

Note: You must not use "@" – use "_" instead.

To create a security configuration

Create a new security configuration. See *To create a Legacy security configuration* on page 22.

To enable encryption

Open the email Output Connector Settings dialog box and select **Encrypt**.

Security configuration for receiving encrypted emails

The StreamServer can decrypt received emails, and reject unencrypted emails. The StreamServer decrypts emails with the private key.

To achieve this you must create a security configuration, and enable rejection of unencrypted emails on the EmailIN input connector.

Prerequisites

- The StreamServer private key file is added to the same resource set as the security configuration.
- The StreamServer email certificate is distributed to the senders.

To create a security configuration

1. Create a new security configuration. See *To create a Legacy security configuration* on page 22.
2. Click the **Email and HTTP client** tab.
3. Select the StreamServer **Private key file** and enter the **Password** to access the private key.

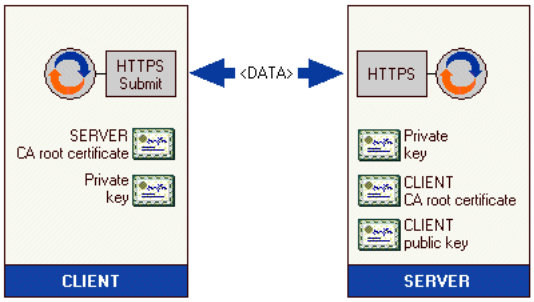
To enable rejection of unencrypted emails

1. Open the EmailIN input Connector Settings dialog box and select **Retrieve email** > **Advanced**.
2. Select **Request encryption**.

Legacy scenarios

SSL server and SSL client with client authentication

This scenario involves the two StreamServers SERVER and CLIENT. The SERVER communicates via an HTTPS input connector, and the CLIENT communicates via an HTTPS Submit output connector. The CLIENT must authenticate itself to SERVER.



Prerequisites

- Both SERVER and CLIENT use SSL version SSLv3.
- SERVER has the following resources in the default resource set:
  - **Private key.pfx** – the private key file for SERVER.
  - **CLIENT CA root certificate.crt** – the CA root certificate for CLIENT. This is the only certificate in the certificate chain.
  - **CLIENT public key.crt** – the certificate for CLIENT.
- CLIENT has the following resources in the default resource set:
  - **SERVER CA root certificate.crt** – the CA root certificate for SERVER. This is the only certificate in the certificate chain.
  - **Private key.pfx** – the private key file for CLIENT.

Configuring the SERVER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SSL SERVER.
2. Open SSL SERVER and select the type **Legacy**.
3. On the Certificates tab, add the certificate resource **CLIENT CA root certificate.crt**.
4. On the HTTP Server tab, select **Private key file** > **Private key.pfx** and enter the **Password** to access the private key.
5. Select **Client authentication** and select **Client certificate** > **CLIENT public key.crt**.

Configure the HTTPS input connector

1 Select **security configuration** > **SSL SERVER**.

2 Select **SSL Version** > **SSLv3**.

Configuring the CLIENT

Create the Security configuration

1 Add a security configuration to the default resource set and rename it to `SSL CLIENT`.

2 Open `SSL CLIENT` and select the type **Legacy**.

3 On the Certificates tab, add the certificate resource **SERVER CA root certificate.crt**.

4 On the Email and HTTP client tab, select **Private key file** > **Private key.pfx** and enter the **Password** to access the private key.

Configure the HTTPS Submit output connector

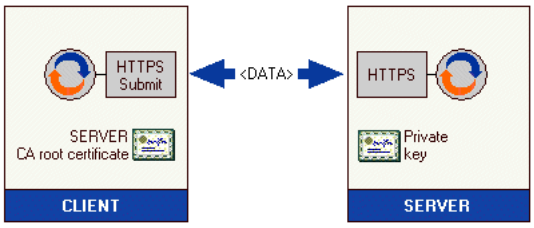
1 Select **Use security configuration**.

2 Select **Security configuration** > **SSL CLIENT**.

3 Select **SSL Version** > **SSLv3**.

SSL server and SSL client without client authentication

This scenario involves the two StreamServers `SERVER` and `CLIENT`. The `SERVER` communicates via an HTTPS input connector, and the `CLIENT` communicates via an HTTPS Submit output connector. The `CLIENT` does not authenticate itself to `SERVER`.



Prerequisites

- Both `SERVER` and `CLIENT` use SSL version SSLv3.
- `SERVER` has the following resource in the default resource set:
  - **Private key.pfx** – the private key file for `SERVER`.
- `CLIENT` has the following resource in the default resource set:
  - **SERVER CA root certificate.crt** – the CA root certificate for `SERVER`. This is the only certificate in the certificate chain.

Configuring the SERVER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SSL SERVER.
2. Open SSL SERVER and select the type **Legacy**.
3. On the HTTP Server tab, select **Private key file** > **Private key.pfx** and enter the **Password** to access the private key.

Configure the HTTPS input connector

1. Select **security configuration** > **SSL SERVER**.
2. Select **SSL Version** > **SSLv3**.

Configuring the CLIENT

Create the Security configuration

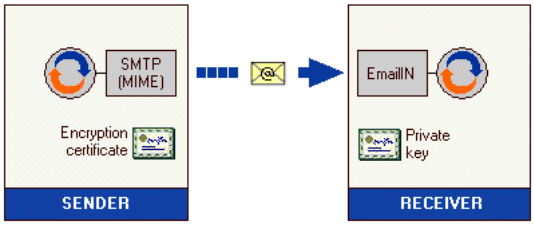
1. Add a security configuration to the default resource set and rename it to SSL CLIENT.
2. Open SSL CLIENT and select the type **Legacy**.
3. On the Certificates tab, add the certificate resource **SERVER CA root certificate.crt**.

Configure the HTTPS Submit output connector

1. Select **Use security configuration**.
2. Select **Security configuration** > **SSL CLIENT**.
3. Select **SSL Version** > **SSLv3**.

Encrypted emails

This scenario involves the two StreamServers SENDER and RECEIVER. The SENDER sends encrypted emails to the RECEIVER via an SMTP (MIME) output connector, and the RECEIVER receives the emails via an EmailIN input connector.



Prerequisites

- SENDER has the following resource in the default resource set:
  - **info_abc.com.crt** – the encryption certificate for RECEIVER.

- RECEIVER has the following resource in the default resource set:
  - **Private key.p12** – the private key file for RECEIVER.

Configuring the SENDER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to ENCRYPT.
2. Open ENCRYPT and select the type **Legacy**.

Configure the SMTP (MIME) output connector

Select **Encrypt**.

Configuring the RECEIVER

Create the Security configuration

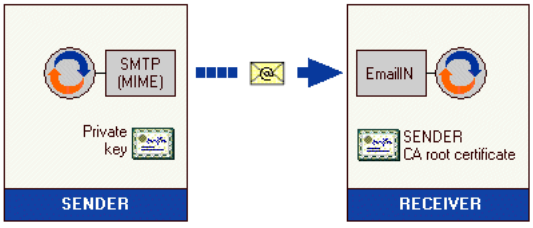
1. Add a security configuration to the default resource set and rename it to ENCRYPTED.
2. Open ENCRYPTED and select the type **Legacy**.
3. On the Email and HTTP client tab, select **Private key file** > **Private key.p12** and enter the **Password** to access the private key.

Configure the EmailIN input connector

1. Select **Retrieve email** > **Advanced**.
2. Select **Request encryption**.

Signed emails

This scenario involves the two StreamServers SENDER and RECEIVER. The SENDER sends signed emails to the RECEIVER via an SMTP (MIME) output connector, and the RECEIVER receives the emails via an EmailIN input connector.



Prerequisites

- SENDER has the following resource in the default resource set:
  - **Private key.p12** – the private key file for SENDER.
- RECEIVER has the following resource in the default resource set:

– **SENDER CA root certificate.crt** – the CA root certificate for SENDER. This is the only certificate in the certificate chain.

Configuring the SENDER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SIGN.
2. Open SIGN and select the type **Legacy**.
3. On the Email and HTTP client tab, select **Private key file** > **Private key.p12** and enter the **Password** to access the private key.

Configure the SMTP (MIME) output connector

Select **Sign**.

Configuring the RECEIVER

Create the Security configuration

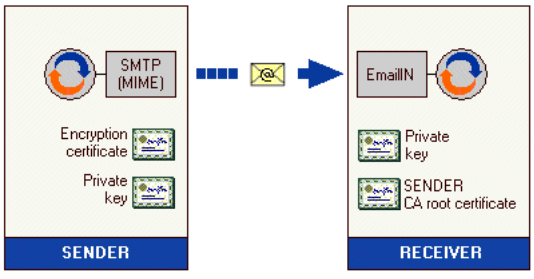
1. Add a security configuration to the default resource set and rename it to SIGNED.
2. Open SIGNED and select the type **Legacy**.
3. On the Certificates tab, add the certificate resource **SENDER CA root certificate.crt**.

Configure the EmailIN input connector

1. Select **Retrieve email** > **Advanced**.
2. Select **Request signature**.

Signed and encrypted emails

This scenario involves the two StreamServers SENDER and RECEIVER. The SENDER sends signed and encrypted emails to the RECEIVER via an SMTP (MIME) output connector, and the RECEIVER receives the emails via an EmailIN input connector.



Prerequisites

- SENDER has the following resources in the default resource set:

  - **info_abc.com.crt** – the encryption certificate for RECEIVER.
  - **Private key.p12** – the private key file for SENDER.
- RECEIVER has the following resources in the default resource set:
  - **Private key.p12** – the private key file for RECEIVER.
  - **SENDER CA root certificate.crt** – the CA root certificate for SENDER. This is the only certificate in the certificate chain.

Configuring the SENDER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SIGN ENCRYPT.
2. Open SIGN ENCRYPT and select the type **Legacy**.
3. On the Email and HTTP client tab, select **Private key file** > **Private key.p12** and enter the **Password** to access the private key.

Configure the SMTP (MIME) output connector

Select **Sign** and **Encrypt**.

Configuring the RECEIVER

Create the Security configuration

1. Add a security configuration to the default resource set and rename it to SIGNED ENCRYPTED.
2. Open SIGNED ENCRYPTED and select the type **Legacy**.
3. On the Certificates tab, add the certificate resource **SENDER CA root certificate.crt**.
4. On the Email and HTTP client tab, select **Private key file** > **Private key.p12** and enter the **Password** to access the private key.

Configure the EmailIN input connector

1. Select **Retrieve email** > **Advanced**.
2. Select **Request signature** and **Request encryption**.

Security configuration GUI reference

Security configuration type	
Trust Server	All certificate information is retrieved from an XKMS (XML Key Management Specification) compliant Trust Server. Only the root CA that verifies the identity of the Trust Server is stored in a file. See *Trust Server settings* on page 34.
Legacy	All digital certificates are stored locally. See *Legacy settings* on page 35.

Trust Server settings

Certificates tab

On this tab, you add all certificate resources to include in the certificate chain used to verify the identity of the Trust Server.

Trust Server tab

On this tab you specify the connection to the Trust Server.

Settings	
URL	The Trust Server URL.
User	The user name to access the Trust Server.
Password	The password to access the Trust Server.

HTTP tab

Use this tab when the StreamServer must authenticate itself to SSL clients or SSL servers. On this tab you enable access to the StreamServer private key.

Settings	
Key name	The key name assigned to the StreamServer when it was registered in the Trust Server. The key name corresponds to a private key.
Passphrase	The passphrase the StreamServer must use to access the private key.

Email tab

Use this tab when the StreamServer must sign or decrypt emails. On this tab you enable access to the StreamServer private key.

Settings	
Key name	The key name assigned to the StreamServer when it was registered in the Trust Server. The key name corresponds to a private key.
Passphrase	The passphrase the StreamServer must use to access the private key.

Legacy settings

Certificates tab

On this tab, you add all certificate resources to include in the certificate chain used to verify the identity of the SSL server or SSL client.

HTTP Server tab

Use this tab when the StreamServer runs as an SSL server. On this tab you enable access to the StreamServer private key and, if required, the client certificate.

Settings	
Private key file	The private key file the StreamServer must use to authenticate itself. The private key file must be included in the same resource set as the security configuration.
Password	The password the StreamServer must use to access the private key file.
Client Authentication	Select if this StreamServer requires client authentication.
Client certificate	The client certificate. The StreamServer must use this certificate to verify the identity of the client. The client certificate must be included in the same resource set as the security configuration.

Email and HTTP Client tab

Use this tab when the StreamServer runs as an SSL client that must authenticate itself to the SSL server, or when it should sign or decrypt emails.

Settings	
Private key file	The private key file the StreamServer must use to authenticate itself or to decrypt emails. The private key file must be included in the same resource set as the security configuration.
Password	The password the StreamServer must use to access the private key file.