Cryptographic exception error when accessing Cora SeQuence sites

Description

In environments with more than one server per Cora SeQuence component, the following error occurs:

The error occurs when the user refreshes any of the Cora SeQuence pages, restarts working in the a site after a pause, or navigates between pages.

Cause

The load balancer redirects a user with an open session on one server to another server that uses a different encryption key.

Solution

Cora SeQuence components on different servers need to use the same encryption key.
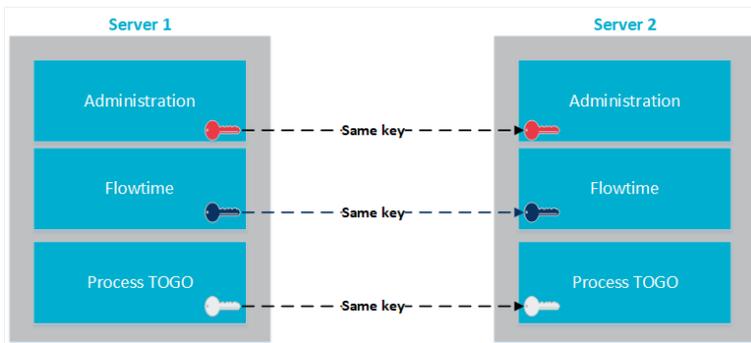
Perform the following steps on each server that includes these Cora SeQuence components:

- Flowtime
- Administration
- Process TOGO

Edit the `web.config` file.

1. On all the servers with Cora SeQuence components, add the following code to the `web.config` file under `system.identitymodel` within `identityconfiguration` section.

Generate keys for all the Cora SeQuence sites

1. Open **Internet Information Services**, select the relevant Cora SeQuence site, and select the **Machine Key** feature.
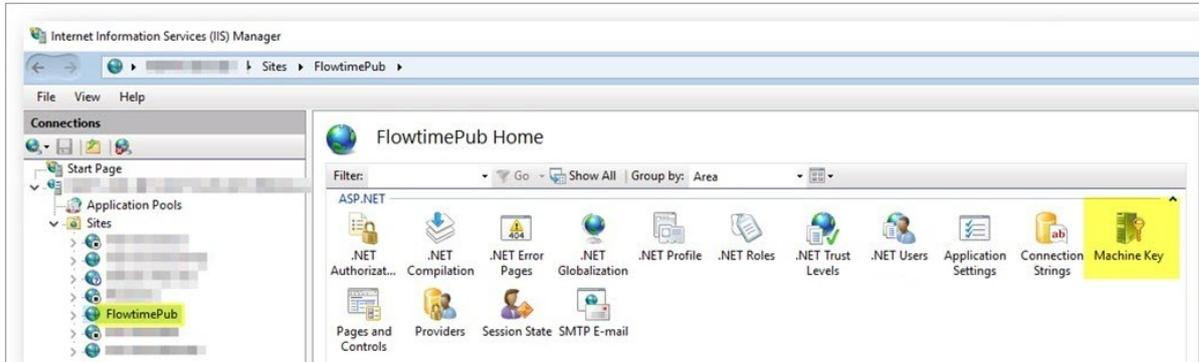
2. Under Machine Key, configure the following:
   a. **Validation method**: Set SHA1.
   b. **Encryption method**: Set AES.
   c. Clear the **Automatically generate at runtime** option.
   d. Click **Generate Keys** to fill in the Validation key and Decryption key fields.
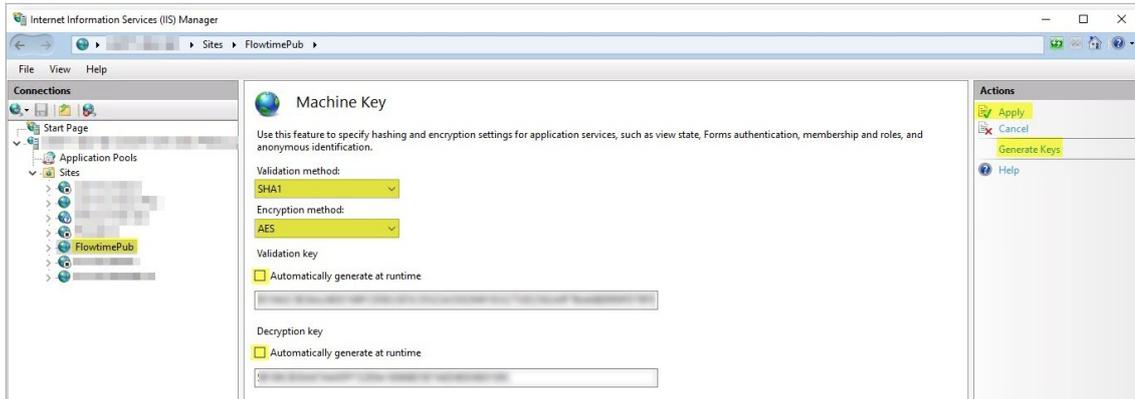
   e. Copy the generated keys.
   You will use these keys to set up this component on the other server.
3. Repeat step 2 for all the Cora SeQuence *sites* on this server.
4. Repeat steps 1-2 on the *remaining servers*.

Because you have already generated the keys, you do not need to generate new keys.
Fill in the Validation key and Decryption key fields with the previously generated keys for the site.