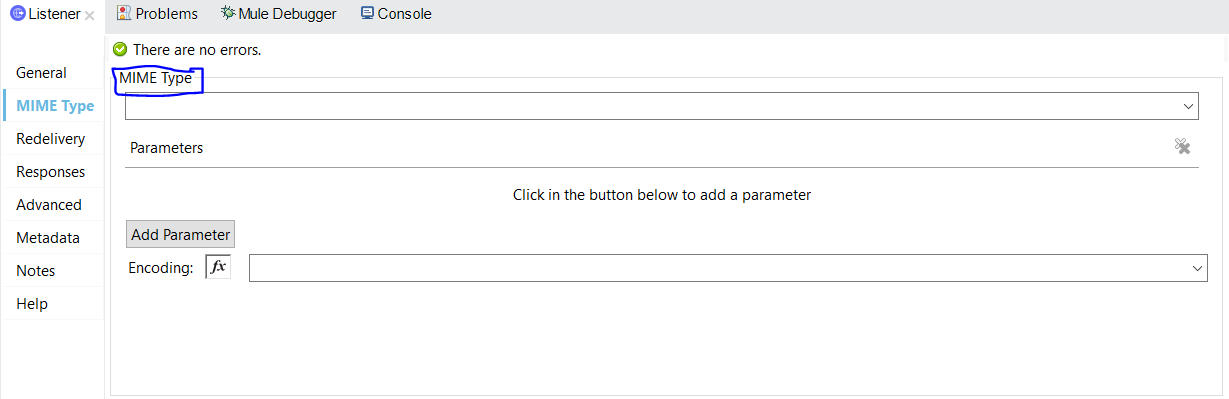
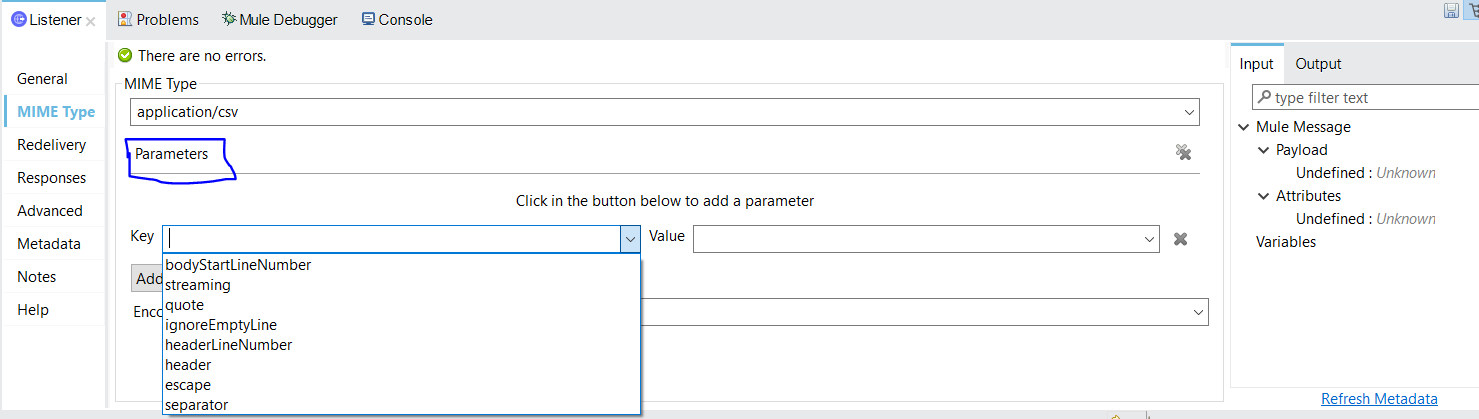
Http-Configuration

===============================================================================

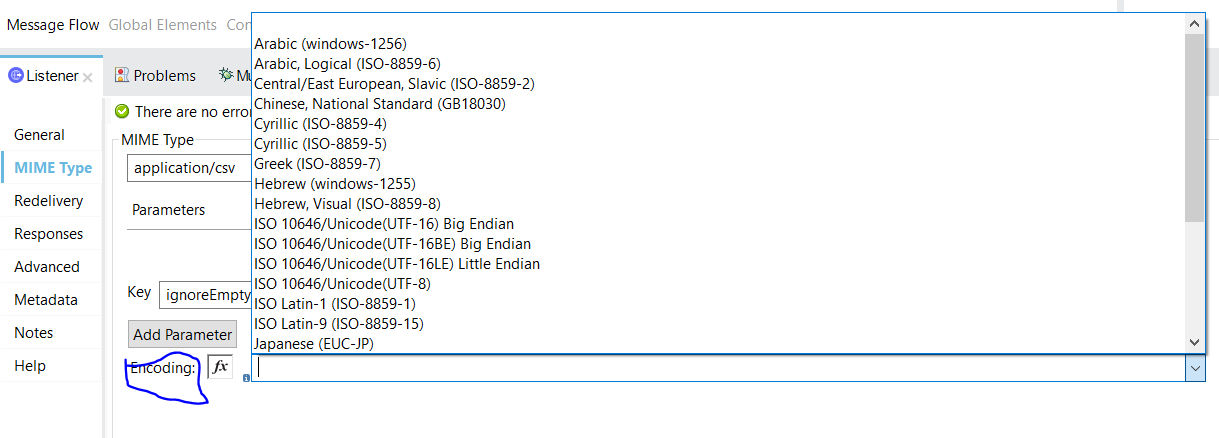
**MIMETYPE**:- 

MIMETYPE :- if we need to validate the input request here we can set the MIMTYPE



Parameters:- here we can set the payload Attributes is true are false

Ex:-( header, streaming,quote,escape….etc)

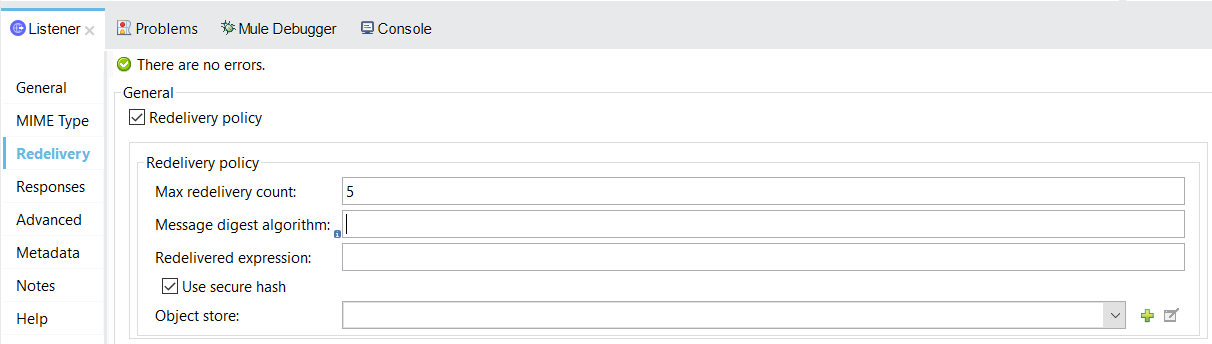


Encoding:-some time we can’t able to read the payload because of encryption format

So here we can set the format

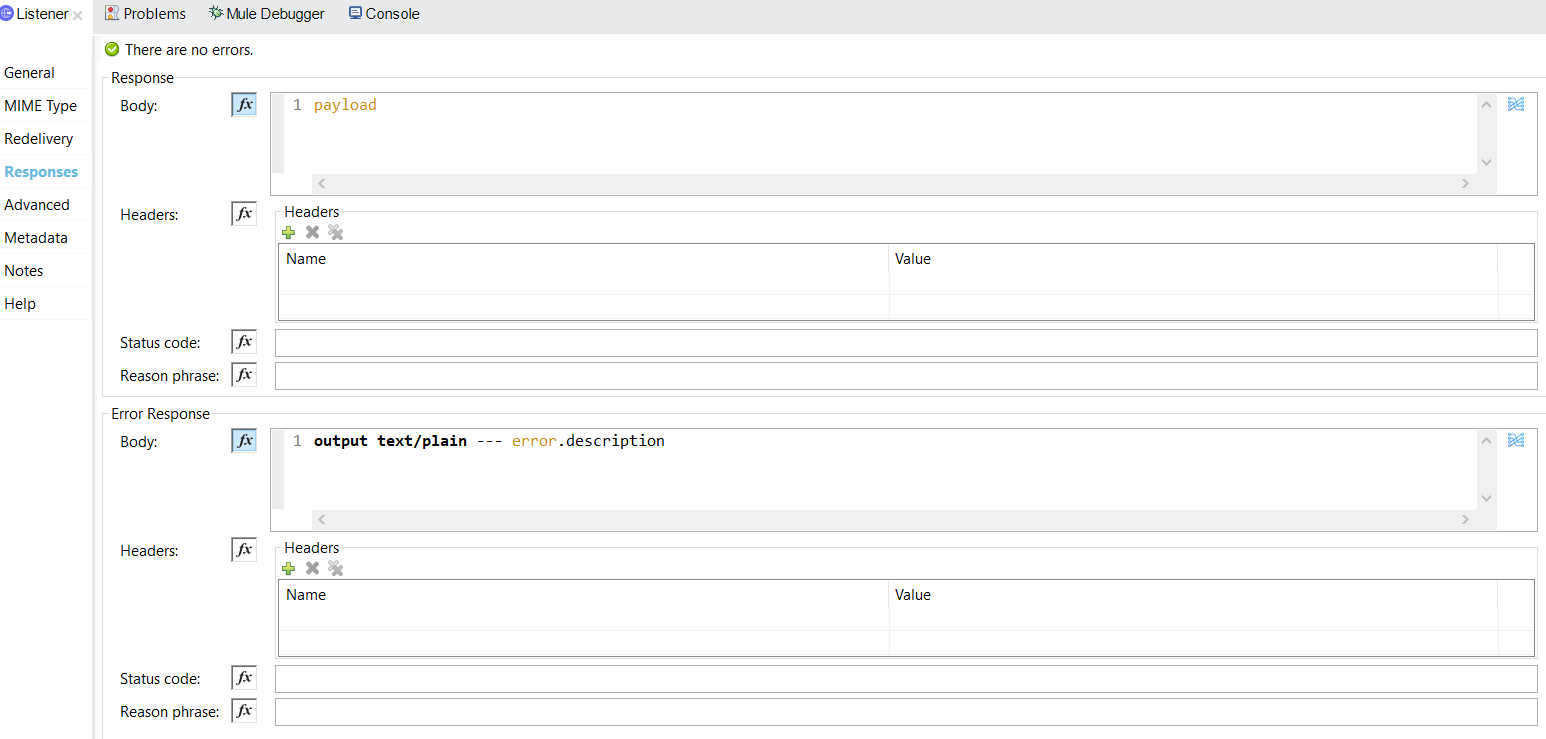
==================================================================================

Redelivery:-



Before we redelivery the response if client server was down we don’t want to lose the response like (success or failure). In that time we can use this option

**Responses:-**

****

**Response Body: -**

**Body=here we can we can change the response type like csv,json,xml**

**Headers=**

**Status code= here we can see the default response status code**

**Reason phrase =**

**Error Responses:-**

**Body=here we can we can change the response type like csv,json,xml**

**Headers=**

**Status code= here we can see the default response status code**

**Reason phrase =**

**Advanced:-**

**Allowed methods:- here we can set the what type of methods is the request**

**Response streaming mode:- here we can set the streaming mode**

* **If response is large file of data at that time it give some performance issue so what we can do we can set the streaming Response**
* **It sent the data is step by step process**

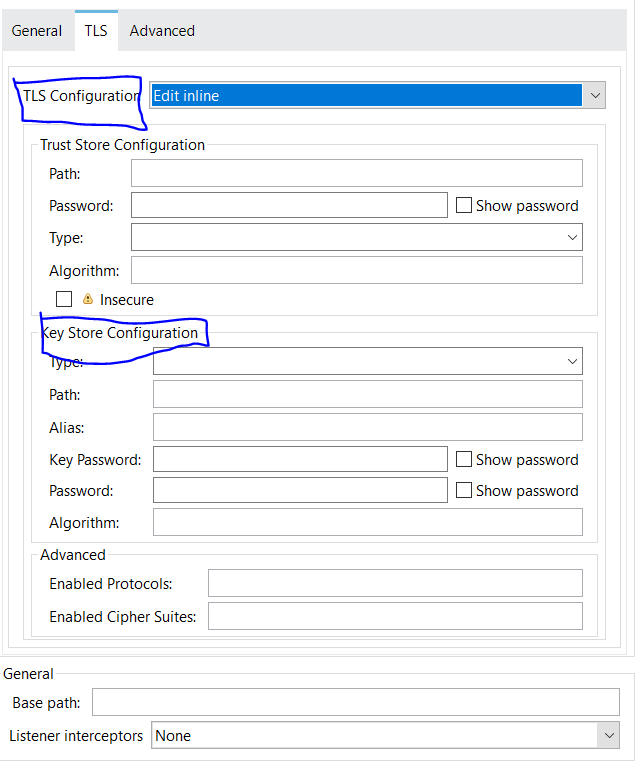
**Reconnection Strategy :-**

**==================================================================================**

**HTTPS**

**==================================================================================**

* **To sending some data through network we need to encrypt the data othere wise some once can easily read our data . for that we need to use key store and trust store**

****

**Client:- client sent some data to server in that case we need to apply Trust store certificate**

**Once we apply the certificate the data will encrypt**

**Server:- now server need to read the client data now server need key store to decrypt**

**Ex:-suppose we have process and system layer**

**🡪 We send data in process layer we need trust store because we are encrypting the data**

**not reading**

**🡪 for system layer we need keystore becaues , what the data was encrypt in processlay**

**we need to decrypt for that we need to key store**