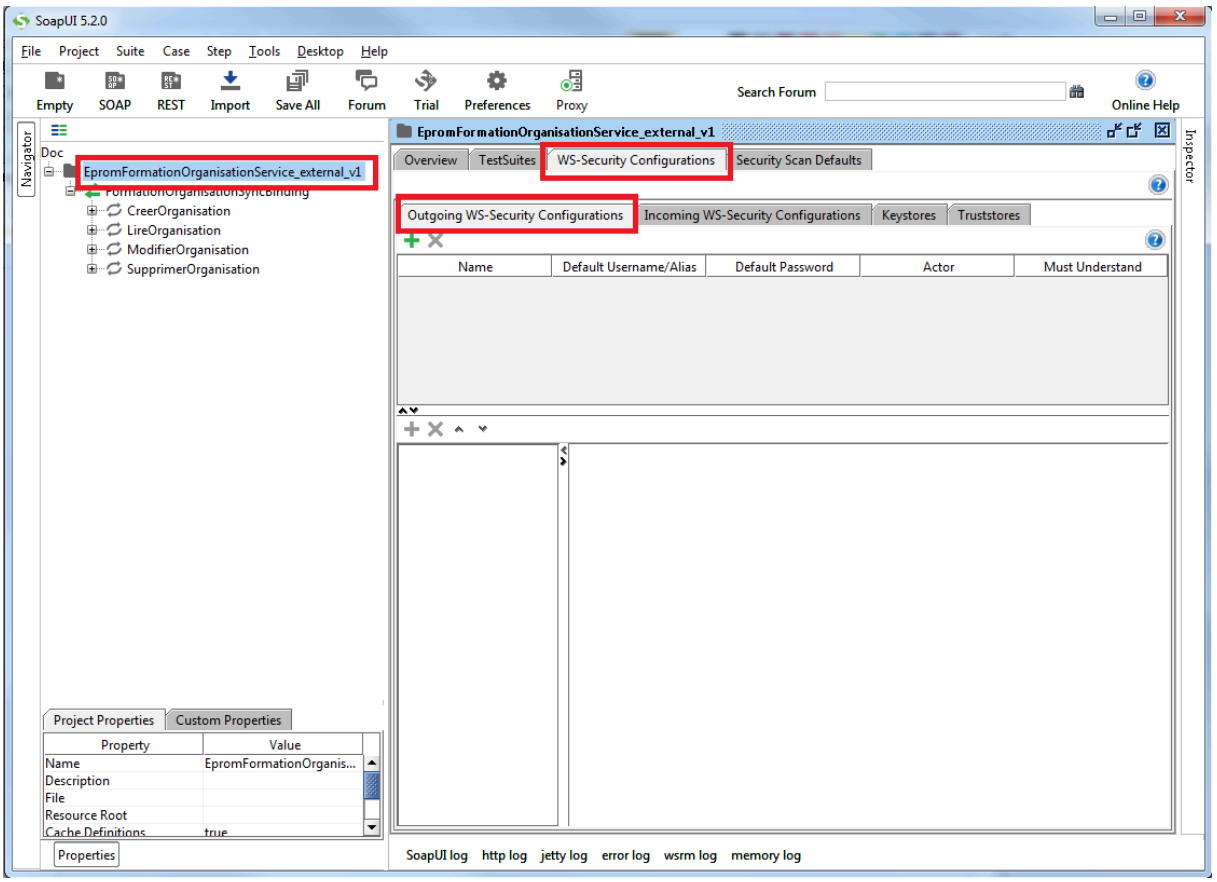
Projet de test SoapUI

Configuration du WS Security

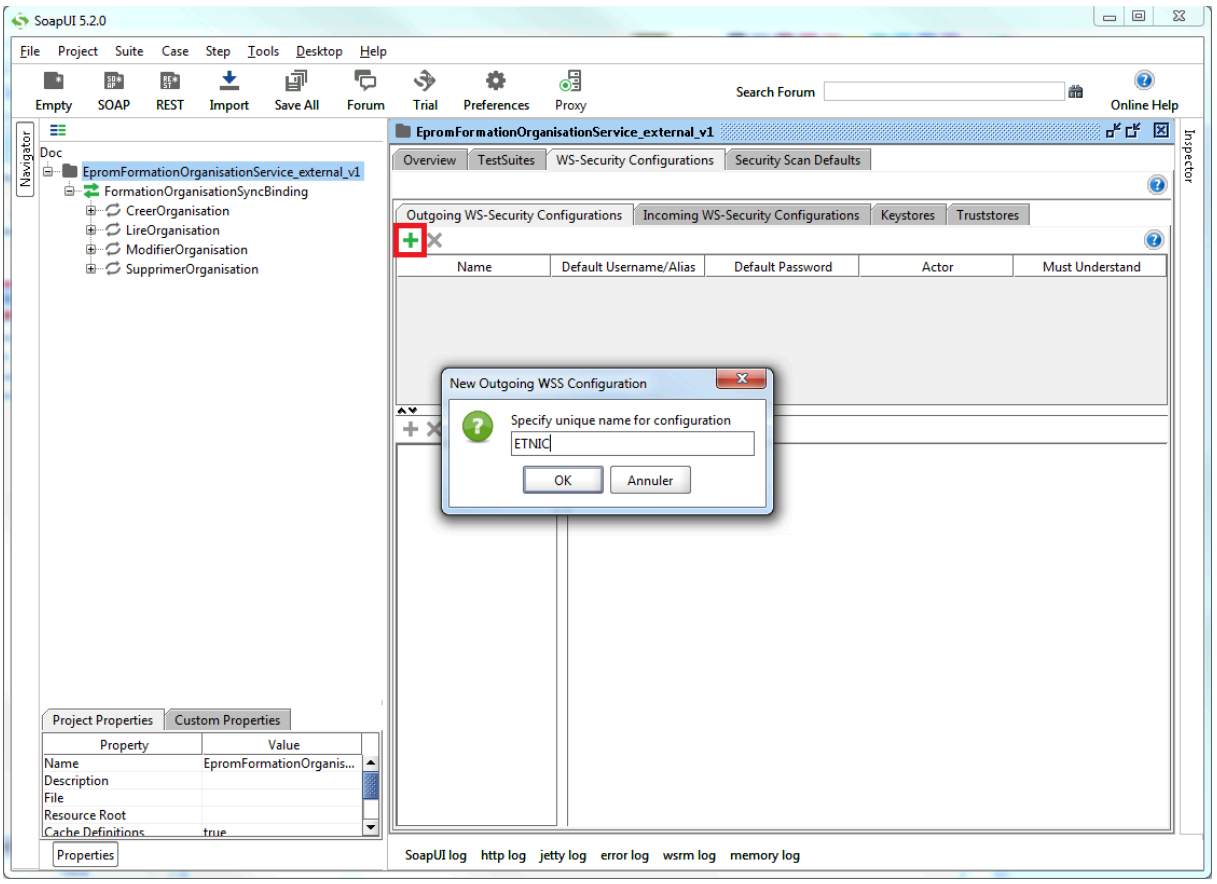
1. Configuration WS-Security

Pour configurer SOAP-UI afin d'utiliser WS-Security avec *x509Token Profile,* vous devez suivre les étapes suivantes:

Tout d'abord, double-cliquez sur le nom de votre projet dans la conne de gauche. Cela ouvrira une fenêtre dans la partie droite de l'écran. Dans cette fenêtre cliquez sur l'onglet WS-Security Configurations et le sous-onglet "Outgoing WS-Security Configurations".



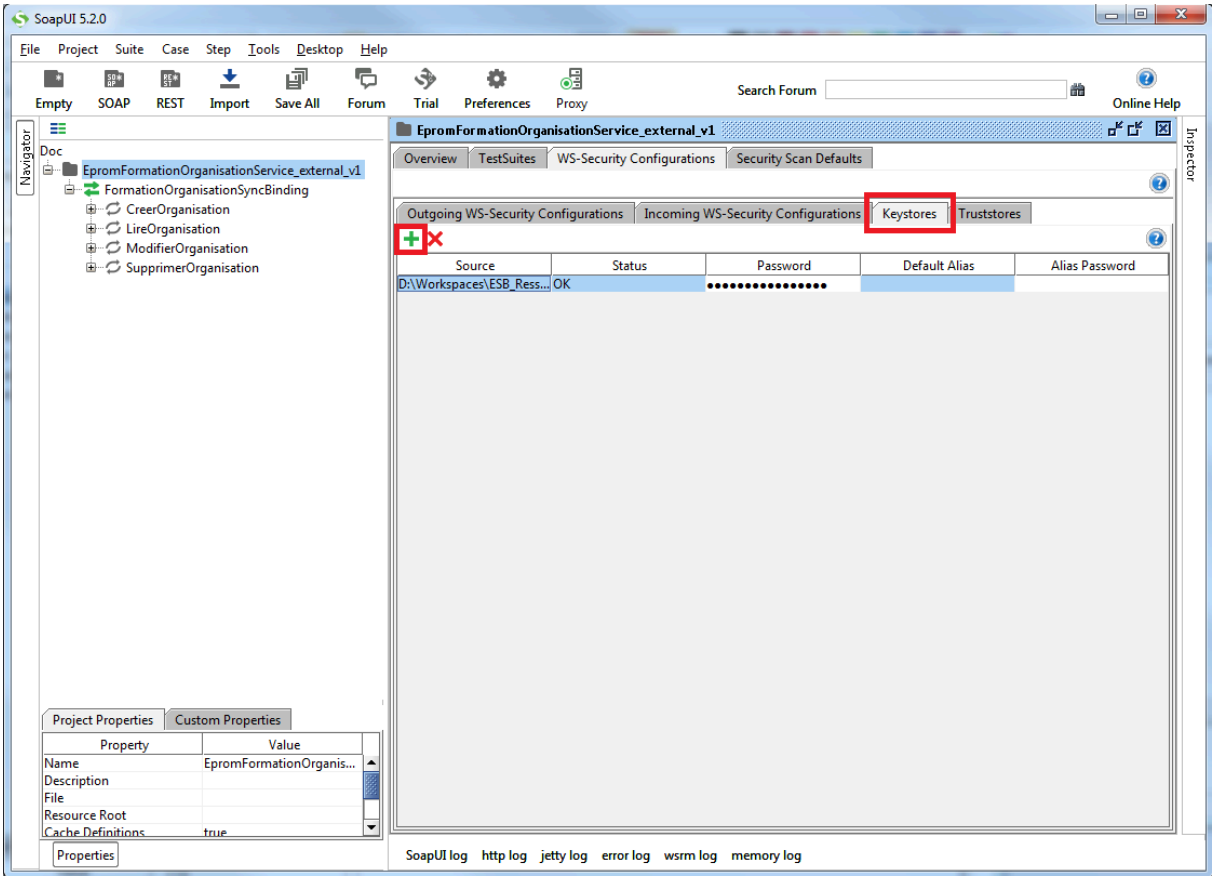
Cliquez sur l'icone "+" pour créer un alias pour une nouvelle configuration. Entrez le nom que vous désirez. Pour l'exemple, nous l'appellerons "ETNIC".



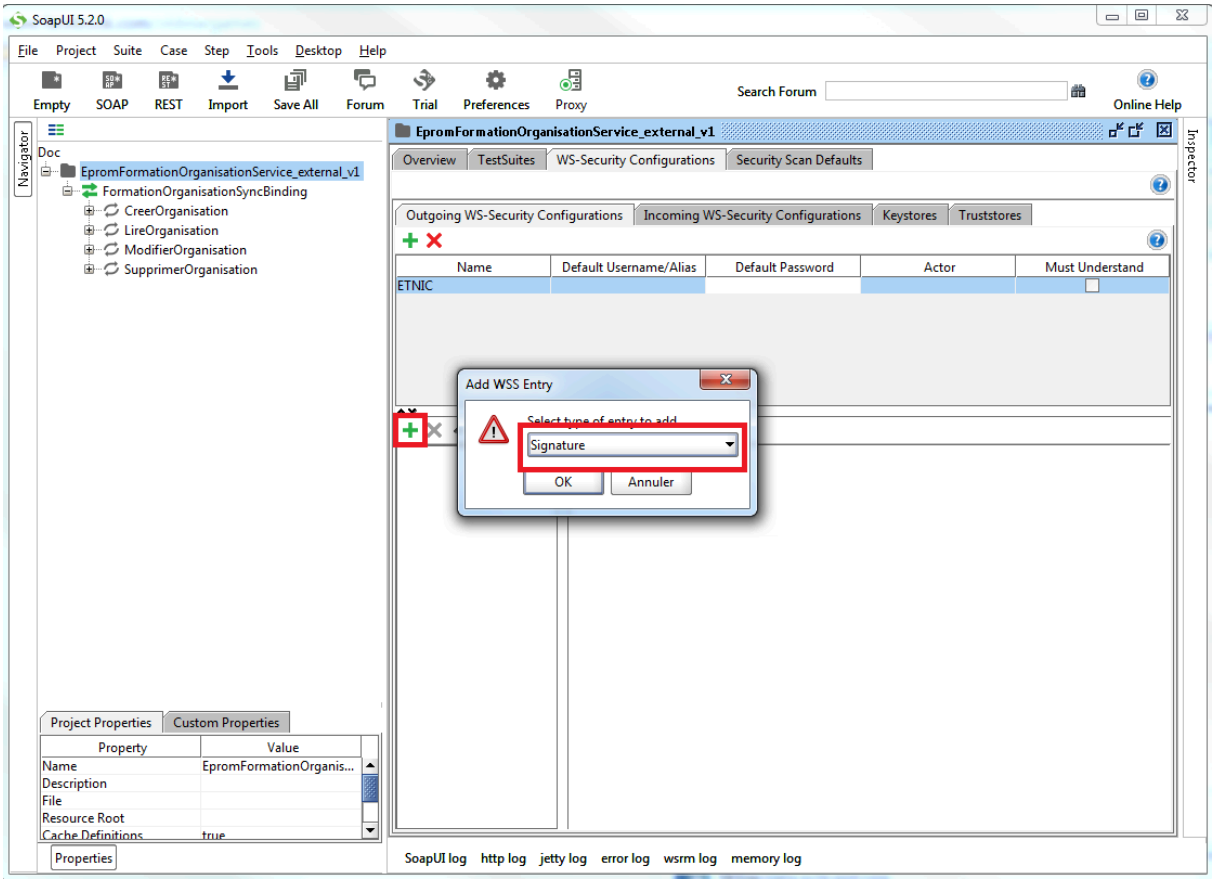
1.1 Configuration x509Token Profile

Pour configurer SOAP-UI afin de signer vos requêtes à l'aide du certificat que vous détenez, veuillez suivre les étapes suivantes:

Cliquez sur le sous-onglet "Keystore" et ajoutez un nouveau keystore via l'icone "+". Le fichier à ajouter est soit un fichier suffixé par .jks ou .p12. Tapez son mot de passe s'il est protégé.

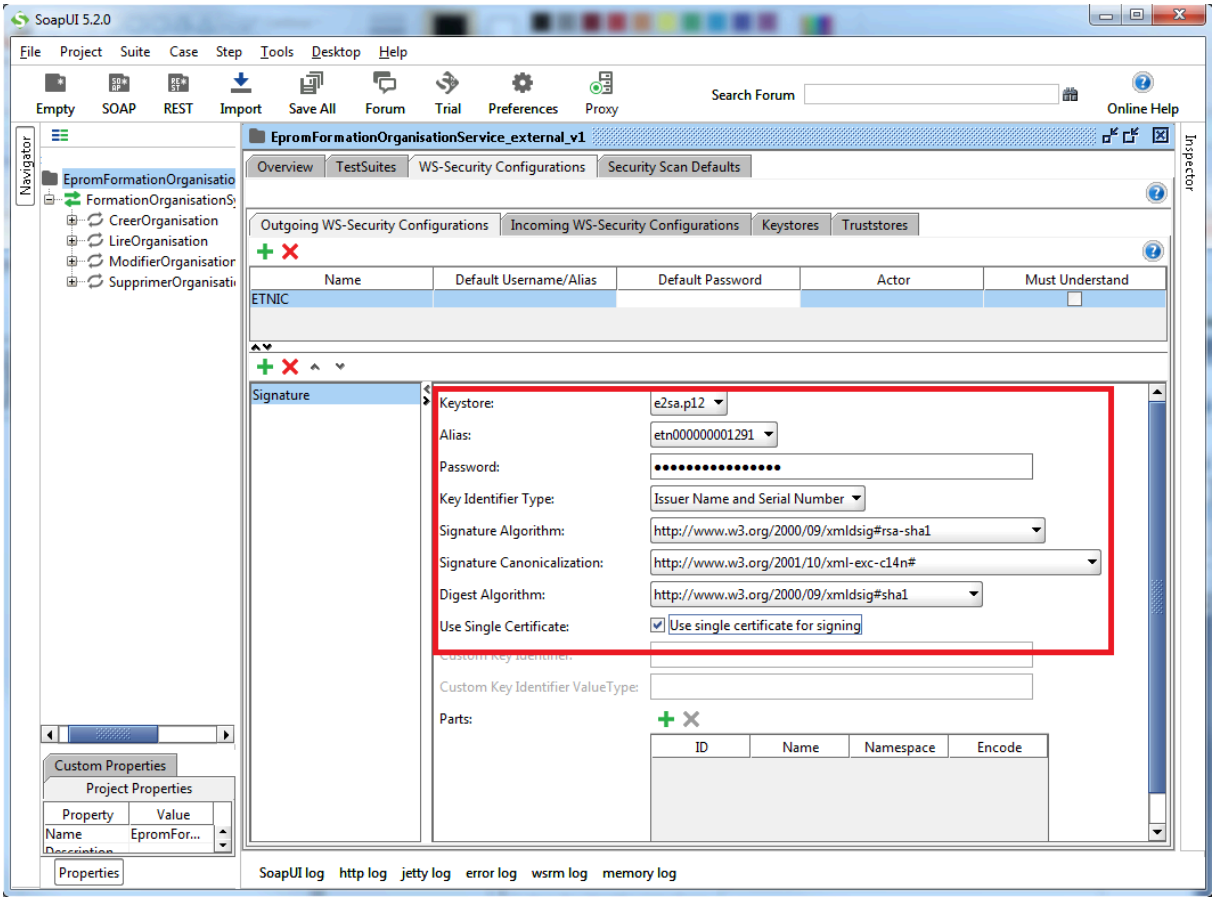


Sélectionnez la configuration "ETNIC" que vous venez d'ajouter et cliquer sur l'icone "+" qui apparait dans une colonne plus bas. Une pop-up apparait vous invitant à choisir le type de configuration que vous désirez introduire. Choisissez "Signature".



Dans la partie droite de la fenêtre de configuration, remplissez les paramètres comme suit:

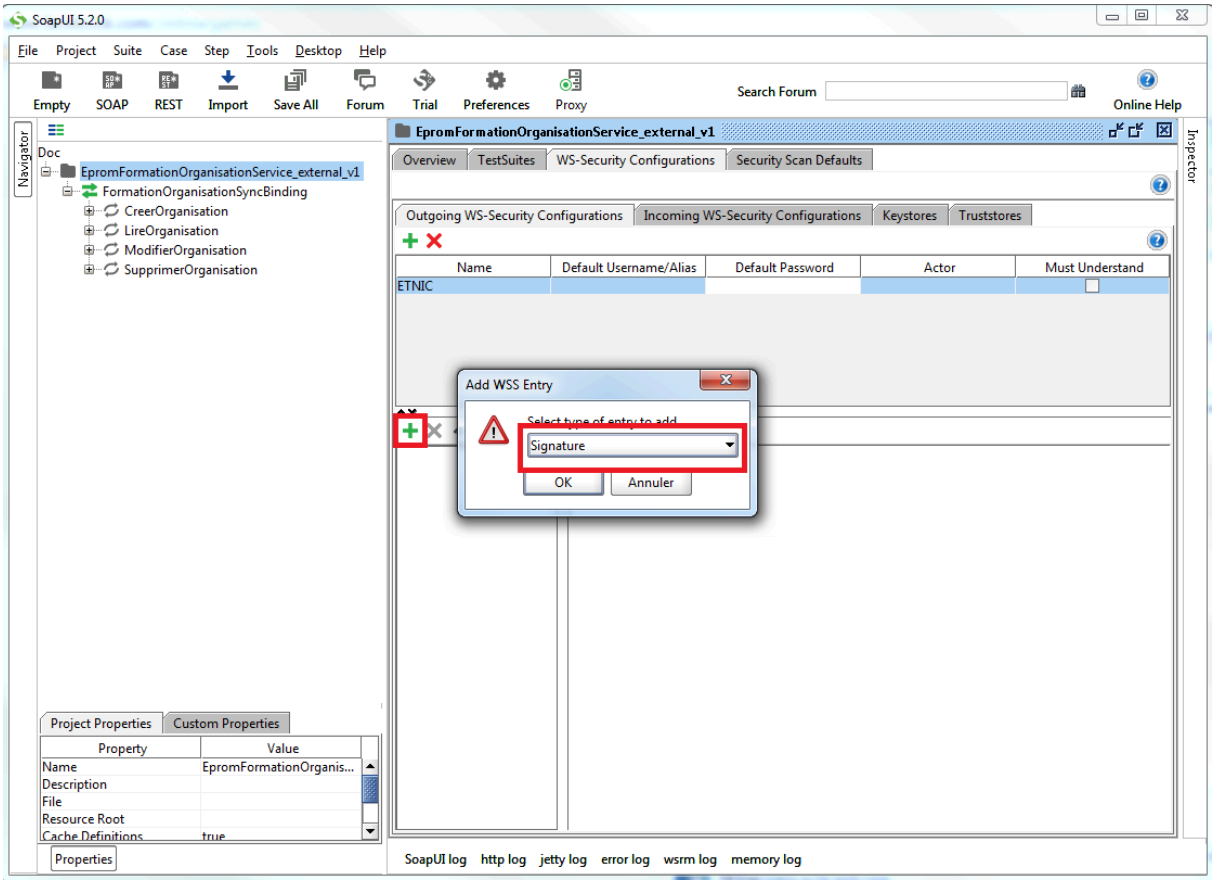
- Keystore: Sélectionnez votre keystore
- Alias: Sélectionnez l'alias de l'entité à authentifier (généralement, il n'y a qu'un choix)
- Password: Entrez le mot de passe du keystore s'il est protégé
- Key Identifier Type: Issuer Name and Serial Number
- Signature algorithm: http://www.w3.org/2000/09/xmldsig#rsa-sha1
- Signature Canonicalization: http://www.w3.org/2001/10/xml-exc-c14n#
- Digest Algorithm: http://www.w3.org/2000/09/xmldsig#sha1
- Use Single Certificate: Coché



1.1.1 *Service BCED*

Si le web service appelé est un service BCED, veuillez suivre les étapes suivantes:

Sélectionnez la configuration "ETNIC" que vous venez d'ajouter et cliquer sur l'icone "+" qui apparait dans une colonne plus bas. Une pop-up apparait vous invitant à choisir le type de configuration que vous désirez introduire. Choisissez "Signature".

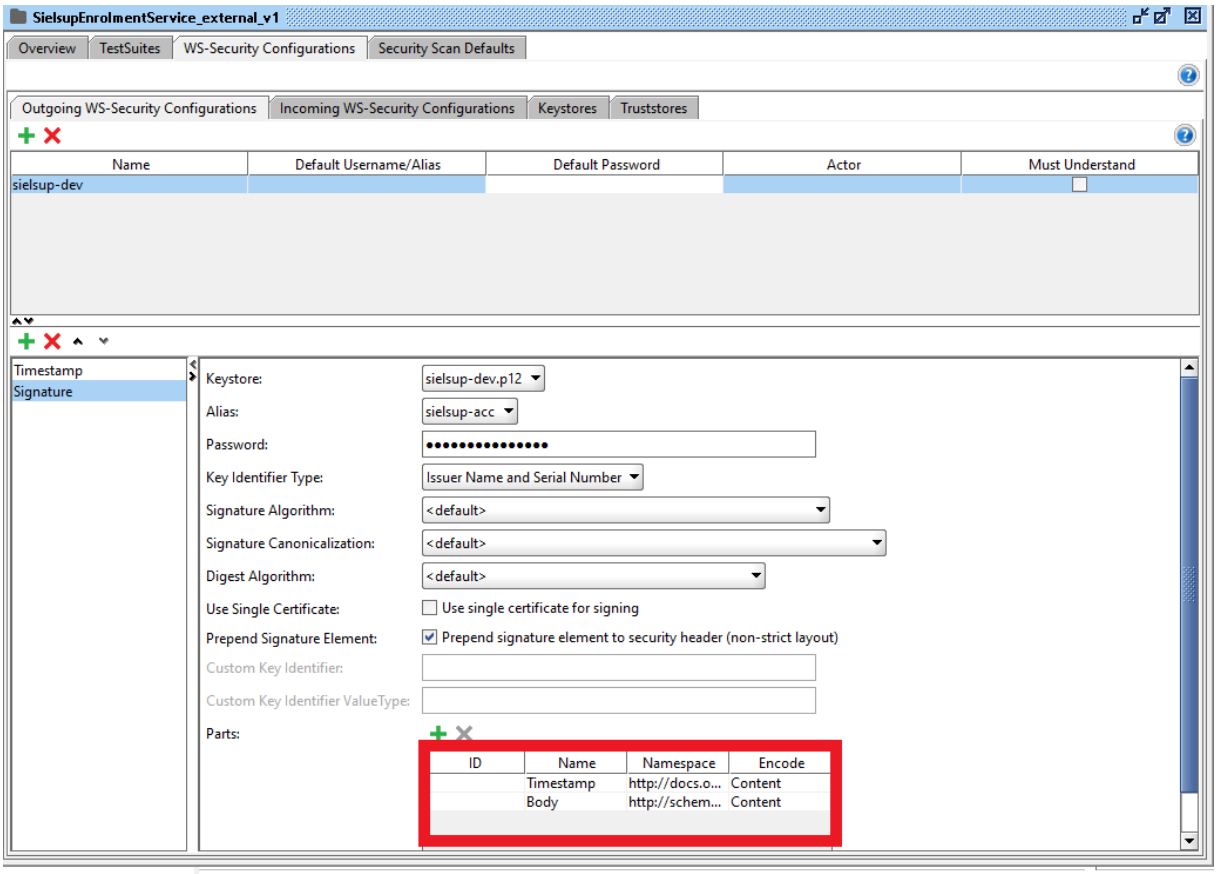


Dans la partie droite de la fenêtre de configuration, remplissez les paramètres comme suit:

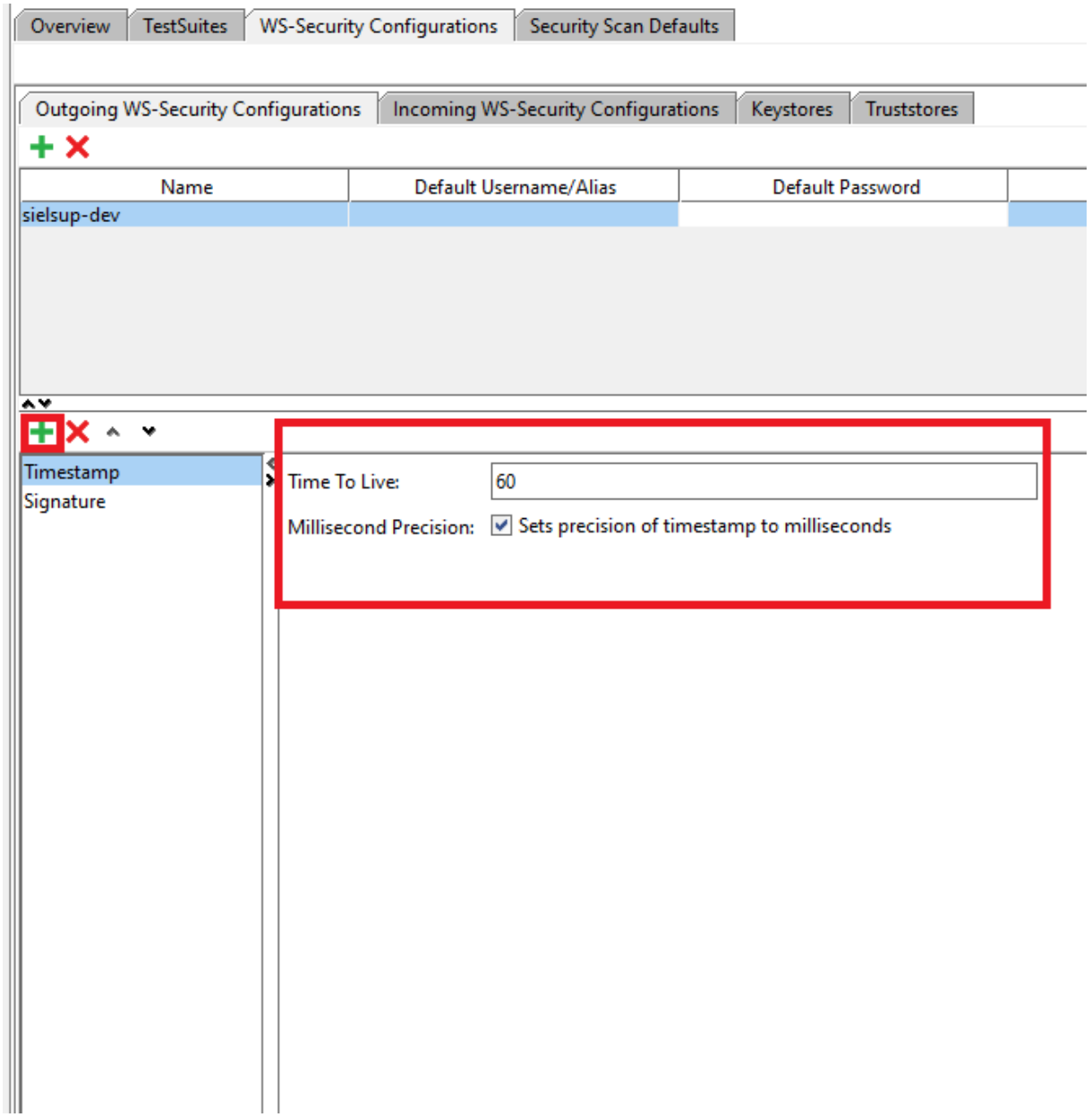
- Keystore: Sélectionnez votre keystore
- Alias: Sélectionnez l'alias de l'entité à authentifier (généralement, il n'y a qu'un choix)
- Password: Entrez le mot de passe du keystore s'il est protégé
- Key Identifier Type: Issuer Name and Serial Number
- Signature algorithm: default
- Signature Canonicalization: default
- Digest Algorithm: default
- Use Single Certificate: Décoché
- Prepend Signature Element: Coché

Dans la table Parts :

- Name: Timestamp
- Namespace : http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
- Encode : Content
- Name : Body
- Namespace : http://schemas.xmlsoap.org/soap/envelope/
- Encode : Content

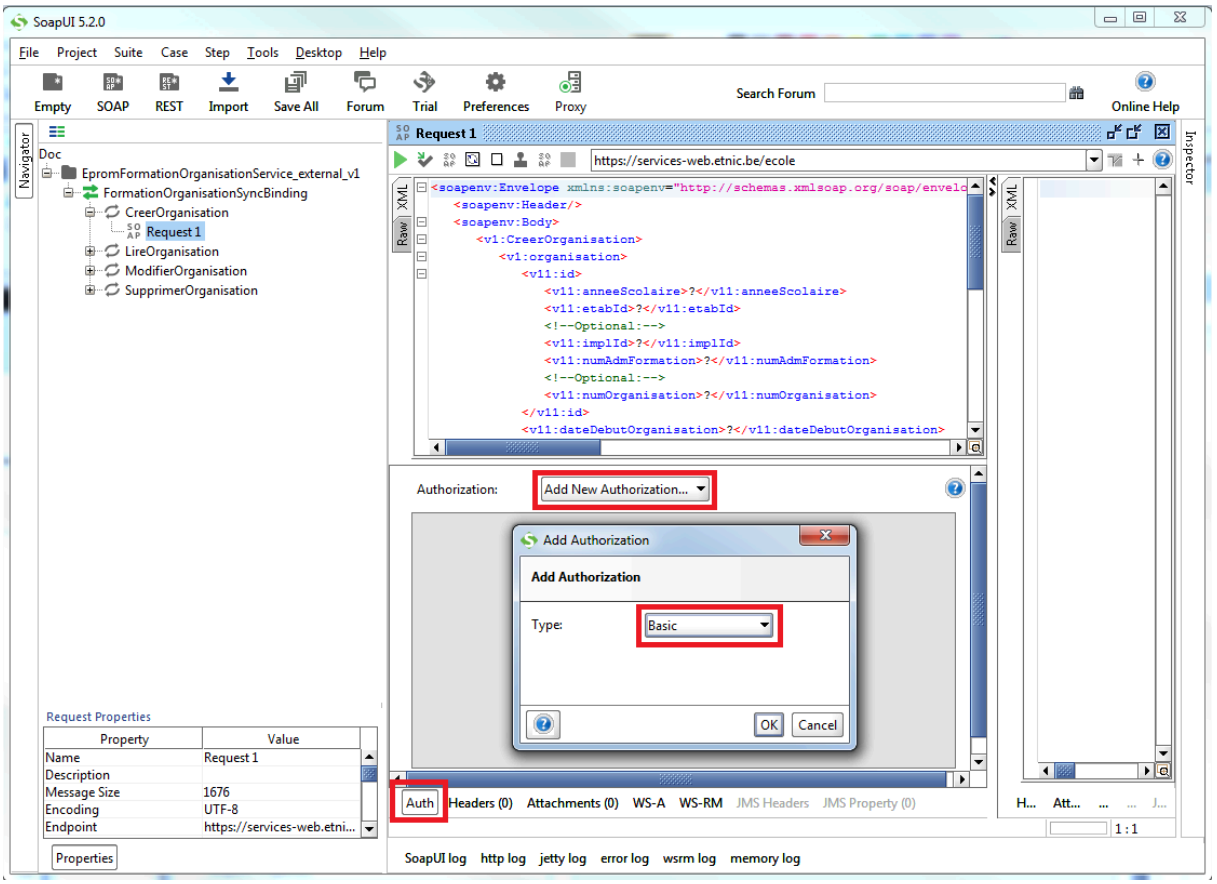


Sélectionnez la configuration "ETNIC" que vous venez d'ajouter et cliquer sur l'icone "+" qui apparait dans une colonne plus bas. Une pop-up apparait vous invitant à choisir le type de configuration que vous désirez introduire. Choisissez "Timestamp".


Overview
TestSuites
WS-Security Configurations
Security Scan Defaults
Outgoing WS-Security Configurations
Incoming WS-Security Configurations
Keystores
Truststores
Name
Default Username/Alias
Default Password
sielsup-dev
Timestamp
Signature
Time To Live:
60
Millisecond Precision:
Sets precision of timestamp to milliseconds

1.2 Application de WS-Security sur la requête

Dans la fenêtre de test d'une requête, cliquez sur l'onglet "Auth" en bas de la fenêtre. Choisissez "Add New Authorization" dans la fenêtre qui vient d'apparaître et "Basic" dans la pop-up suivante.



Sélectionnez l'alias de votre configuration dans le champ "Outgoing WSS". Dans notre exemple, il s'agit d'"ETNIC". Le reste des champs doit rester vide.