



Manual SOAP UI

Configurar peticiones con certificado

Índice General

1	SOAP UI. Configuración	3
1.1	Configurar almacenes de claves posibles.....	3
1.2	Añadimos un nuevo keystore.....	3
1.3	Añadimos una nueva configuración “Outgoing WS Security Configuration”.	4
1.4	Añadir dentro de la recién creada “Outgoing WS Securty” un almacen.	4
1.5	Configurar ese almacén creado.....	5
1.6	Utilizar el certificado en la petición SOAP.....	6
Ilustración 1. Ws- Securty Configurations		3
Ilustración 2. Keystores		3
Ilustración 3. Outgoing WS-Security		4
Ilustración 4. Almacén del Outgoing WS-Securty		4
Ilustración 5. Configuración del almacén.....		5
Ilustración 6. Configuración de la Request		6

1 SOAP UI. Configuración

1.1 Configurar almacenes de claves posibles.

Dentro de nuestro proyecto SOAP debemos acceder a la Ws-Security -> Keystores para dejar disponibles keystores para utilizarlos en nuestras llamadas.

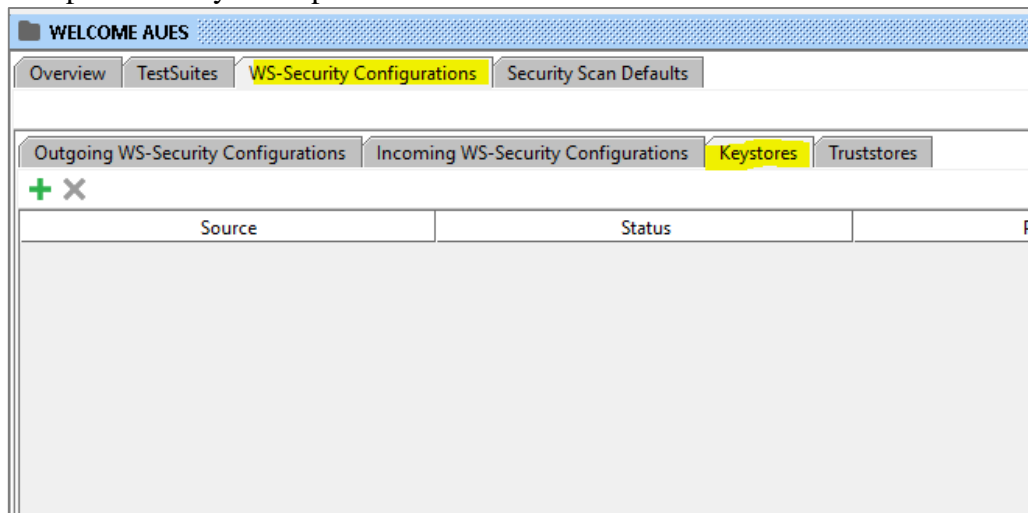


Ilustración 1. Ws- Security Configurations

1.2 Añadimos un nuevo keystore.

Seleccionamos el archivo con nuestro certificado. Nos solicitará el password de dicho certificado.

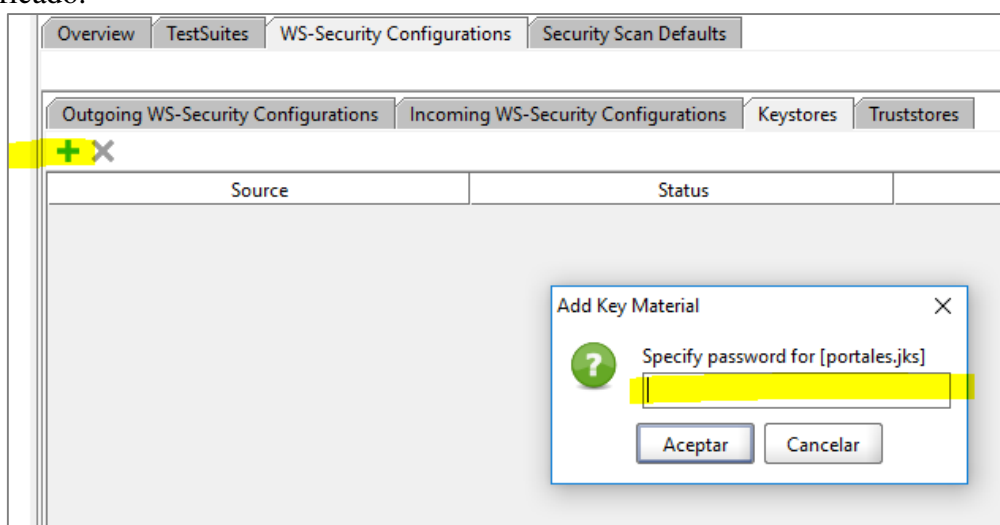


Ilustración 2. Keystores

1.3 Añadimos una nueva configuración “Outgoing WS Security Configuration”.

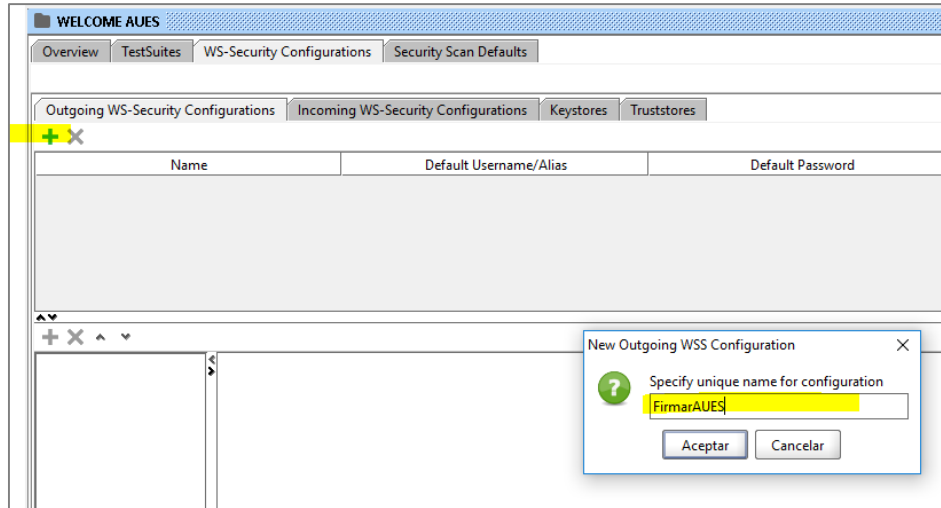


Ilustración 3. Outgoing WS-Security

1.4 Añadir dentro de la recién creada “Outgoing WS Securty” un almacén.

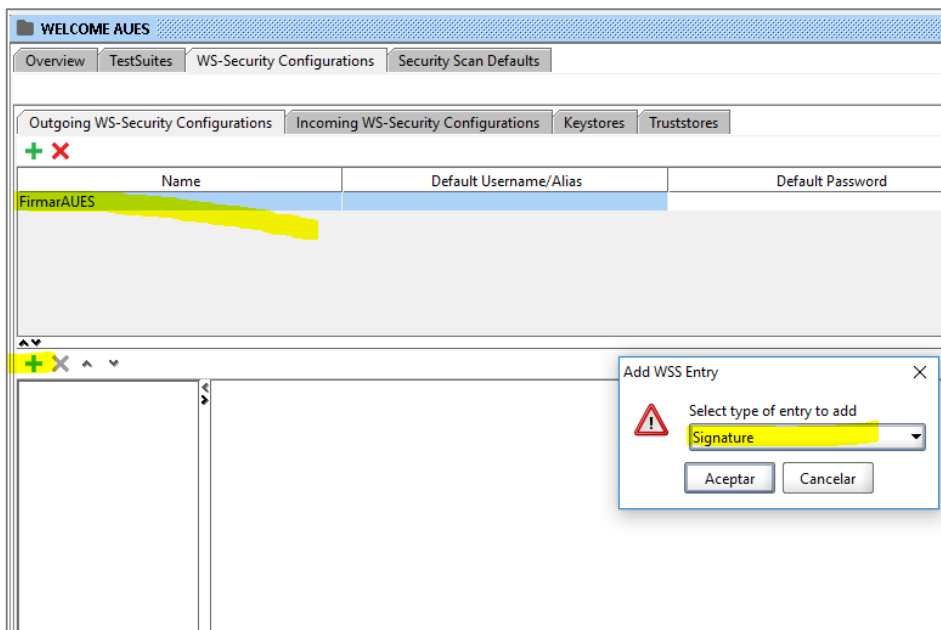


Ilustración 4. Almacén del Outgoing WS-Security

Seleccionar “Signature”.

1.5 Configurar ese almacén creado.

The screenshot shows the 'WELCOME AUES' application interface. The top navigation bar includes 'Overview', 'TestSuites', 'WS-Security Configurations', and 'Security Scan Defaults'. The 'WS-Security Configurations' tab is active, showing sub-tabs for 'Outgoing WS-Security Configurations', 'Incoming WS-Security Configurations', 'Keystores', and 'Truststores'. The 'Keystores' sub-tab is selected, displaying a table with one entry: 'FirmarAUES'. Below this, the 'Signature' configuration for 'FirmarAUES' is shown. The configuration includes fields for 'Keystore' (set to 'portales.jks'), 'Alias' (set to 'portales'), 'Password' (masked with dots), 'Key Identifier Type' (set to 'X509 Certificate'), 'Signature Algorithm' (set to '<default>'), 'Signature Canonicalization' (set to '<default>'), 'Digest Algorithm' (set to '<default>'), and a checked checkbox for 'Use Single Certificate' (labeled 'Use single certificate for signing'). There are also fields for 'Custom Key Identifier' and 'Custom Key Identifier ValueType'. At the bottom, there is a 'Parts' section with a table header: 'ID', 'Name', 'Namespace', and 'Encode'.

Name	Default Username/Alias	Default Password
FirmarAUES		

Signature	Keystore:	portales.jks
	Alias:	portales
	Password:
	Key Identifier Type:	X509 Certificate
	Signature Algorithm:	<default>
	Signature Canonicalization:	<default>
	Digest Algorithm:	<default>
	Use Single Certificate:	<input checked="" type="checkbox"/> Use single certificate for signing
	Custom Key Identifier:	
	Custom Key Identifier ValueType:	
	Parts:	

ID	Name	Namespace	Encode
----	------	-----------	--------

Ilustración 5. Configuración del almacén

Seleccionar el Keystore, Alias, password, X509 y single certificate.

1.6 Utilizar el certificado en la petición SOAP.

En cualquier request, accedemos al apartado “AUTH”.

Insertar una “Basic” y completar el Outgoing WSS, seleccionando el Outgoing WS Security anterior. (En ocasiones no se actualiza ese combo y hay que cerrar y abrir la Request para que aparezca).

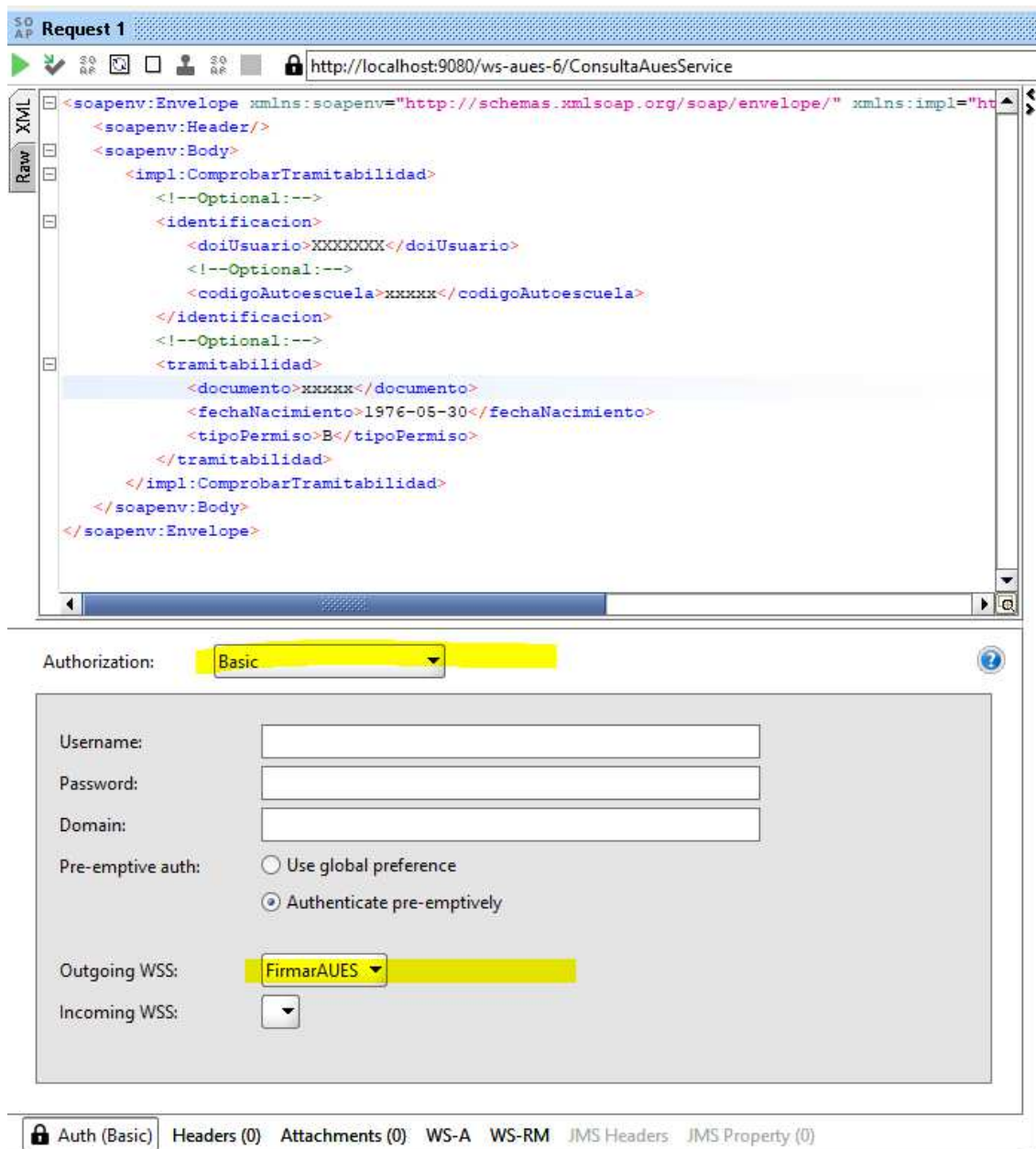


Ilustración 6. Configuración de la Request