Practice 7-1: Configuring the Security Environment

Overview

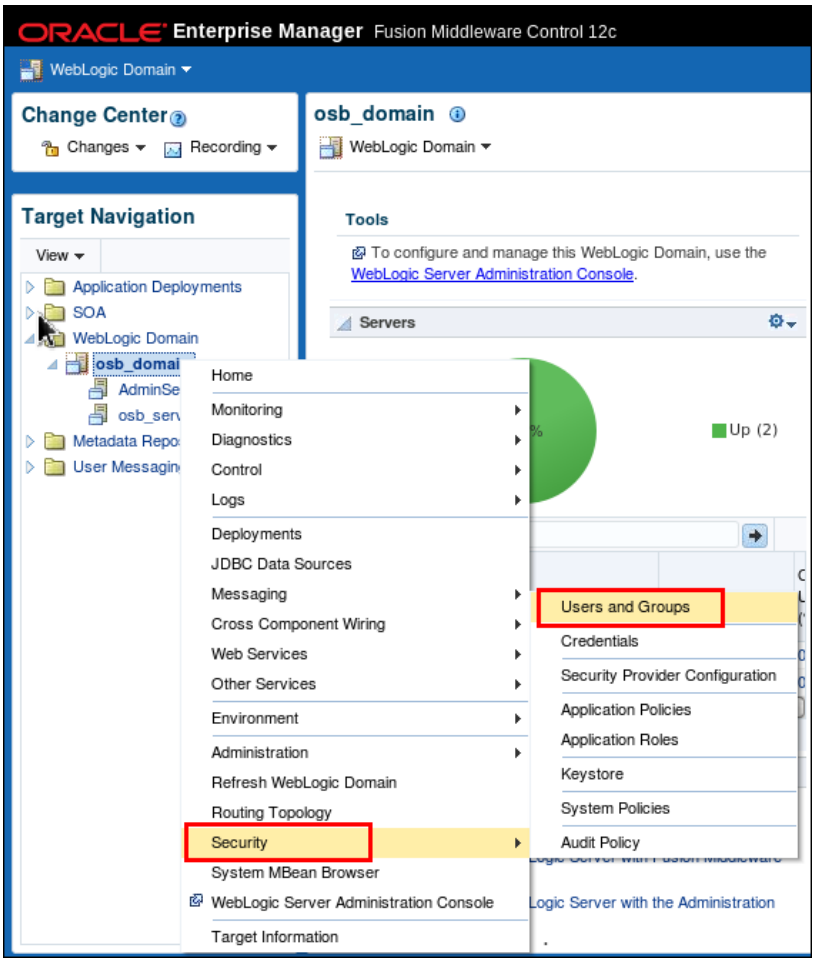
In this practice, you configure Oracle WSM security by configuring the identities.

Assumptions

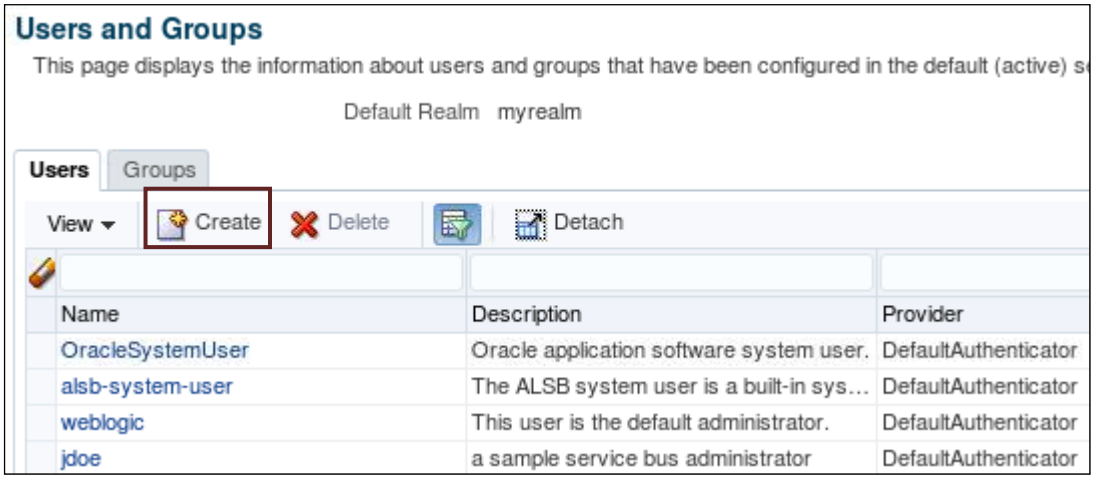
- Oracle Service Bus 12c 12.1.3.0 is installed and is running for the `osb_domain`.
- Oracle Web Services Manager is enabled and configured to work with Service Bus.
- `CreditCardValidationService` web service application is deployed and running on Oracle WebLogic server.

Tasks

1. Create a user in WebLogic Server (WLS) by using Enterprise Manager. The Service Bus proxy service uses the WLS default authenticator to authenticate the username and password in the WS-Security SOAP Headers received from the client. The user created using Enterprise Manager is available to the WLS default authenticator.
   a. In Enterprise Manager, right-click **osb_domain** and select **Security** > **Users and Groups**.



b. In the Users and Groups page, click **Create**.

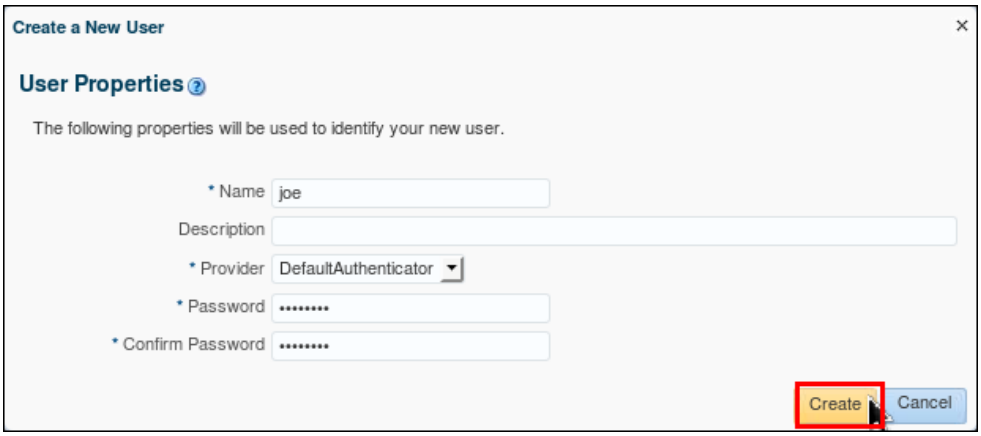


c. Create a user by specifying the following, and then click **Create**:

User Name: **`joe`**

New Password: `See` **`OracleServiceBus12cPassword`** `File`

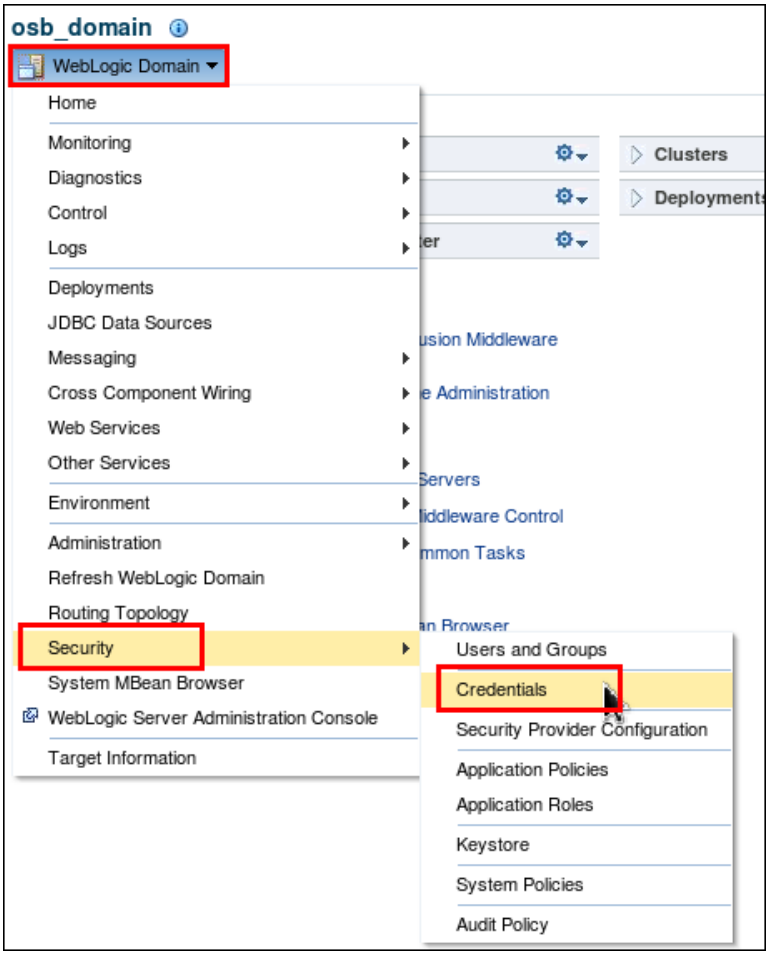
Confirm Password: `See` **`OracleServiceBus12cPassword`** `File`



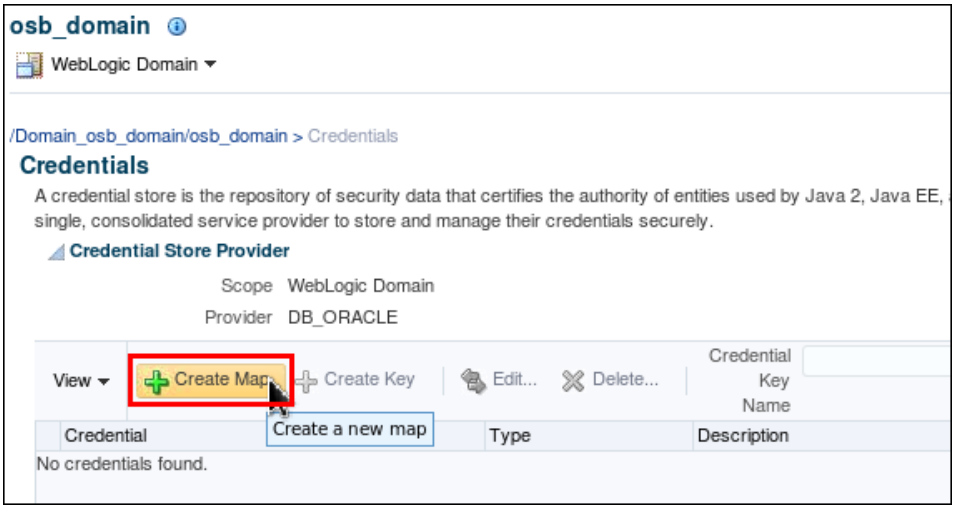
2. Add a csf-key for the user `joe` in Enterprise Manager. This step is required for the Service Bus Test Console to look up the username and password using the csf-key.

a. In Enterprise Manager, expand **WebLogic Domain**, and click **osb_domain**.

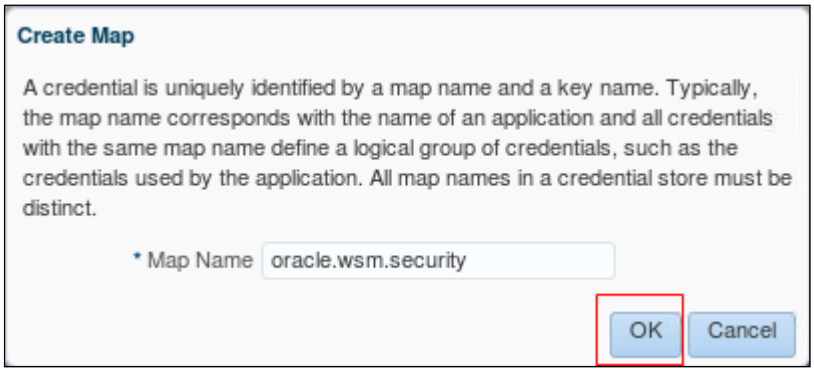
b. In the osb_domain page, from the **WebLogic Domain** drop-down menu, click **Security > Credentials**.



c. Click **Create Map.**



d. Add the following name: **`oracle.wsm.security`** and click **OK**.



e. Select the **`oracle.wsm.security`** map and click **Create Key.**

f. In the Create Key page, specify the following options and then click **OK**.

Map: **oracle.wsm.security**

Key: **`joe-key`**

Type: **Password**

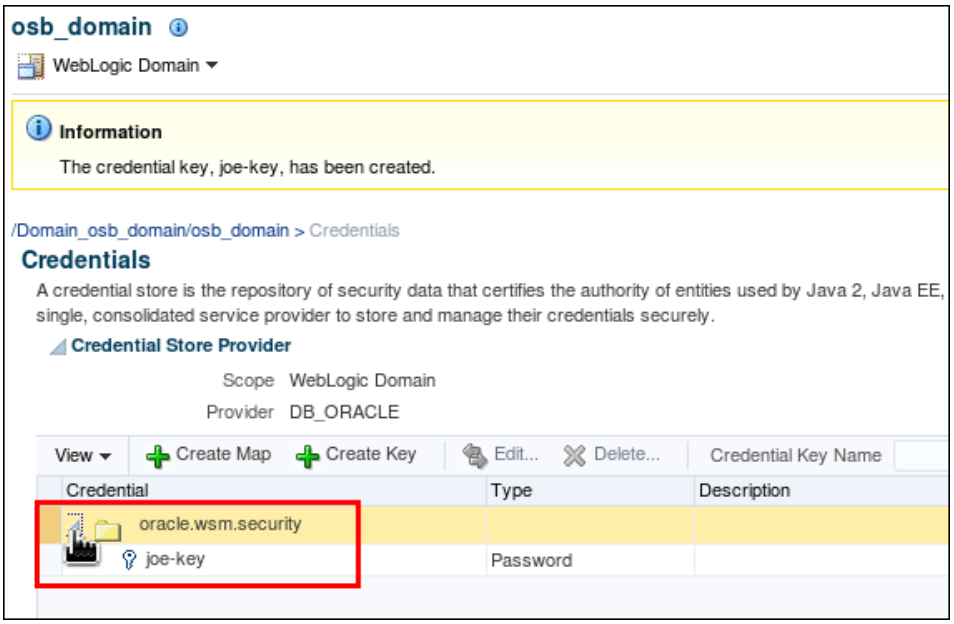
User Name: **`joe`** (same as entered in Service Bus Console)

Password: `See` **`OracleServiceBus12cPassword`** `File` (same as entered in Service Bus Console)

Confirm Password: `See` **`OracleServiceBus12cPassword`** `File`

You should see the message: "**The credential key, joe-key, has been created**."

g. Expand **oracle.wsm.security** and you should see joe-key.



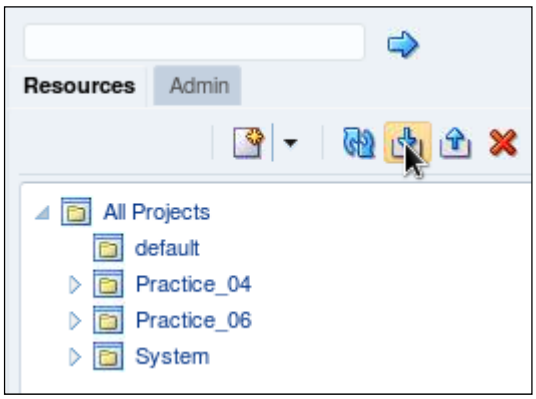
Practice 7-2: Applying a Security Policy to Proxy Services

Overview

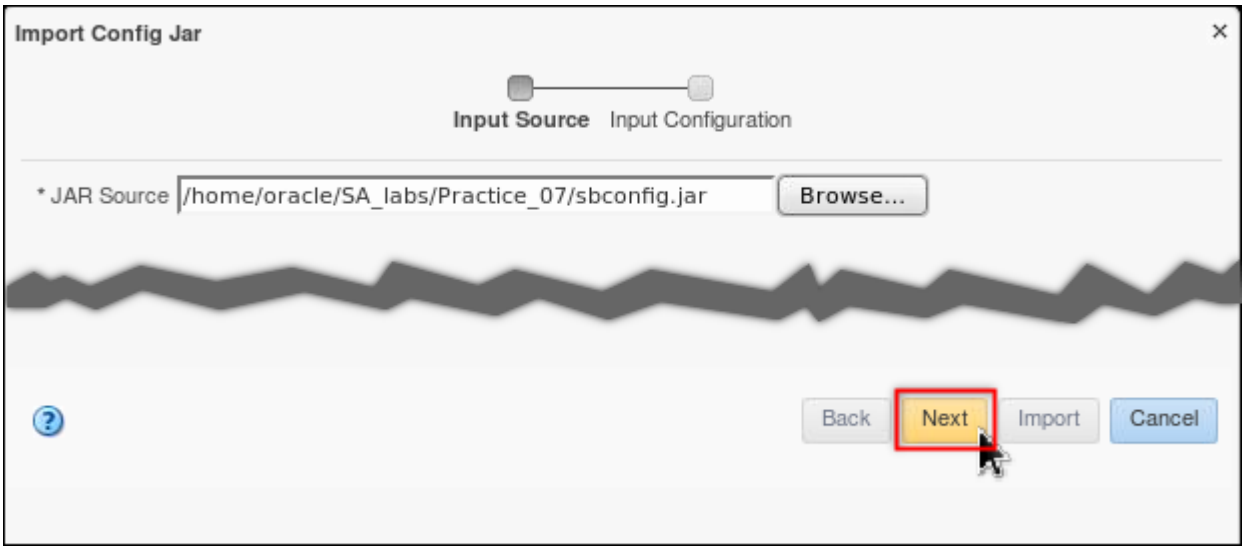
In this practice, you add oracle/wss_username_token_service_policy Oracle WSM policy, at run time to the CreditCardService_Proxy proxy service by using the Service Bus Console.

Tasks

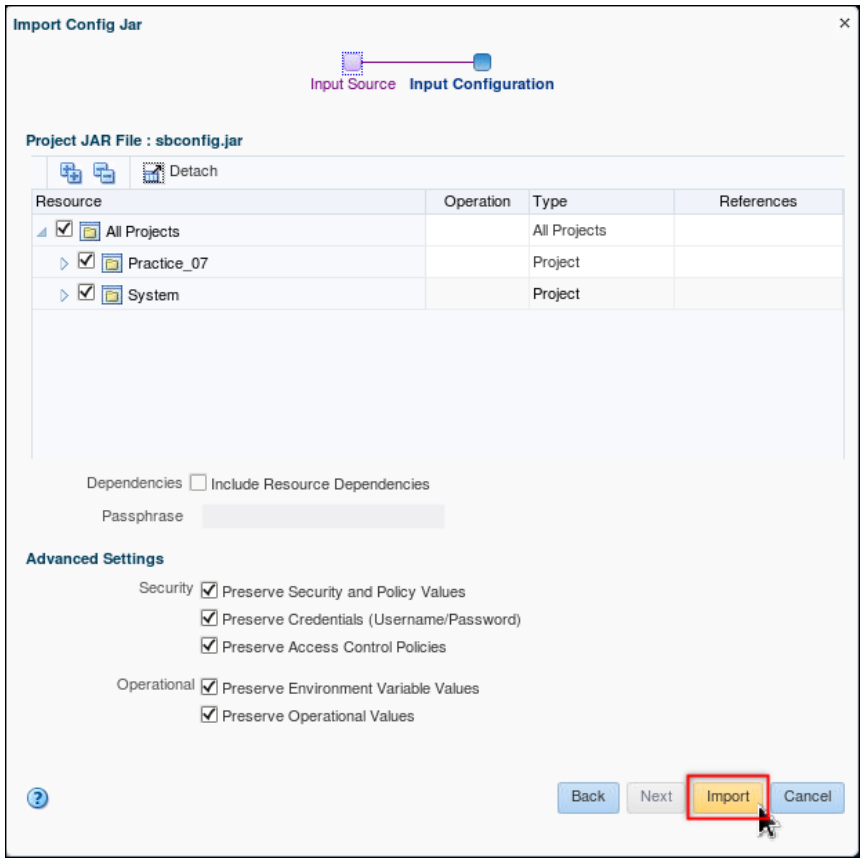
1. Import the sample Service Bus project by using the Service Bus console.
   a. In Service Bus Console, create a new session.
   b. In the Resources tab, click **Import Config Jar.**



   c. On the Import Config Jar page, browse and navigate to `/home/oracle/labs_SA/Practice_07` directory, and open the `sbconfig.jar` file. Click **Next**.



d. On the Import Config Jar > Input Configuration page, click **Import**.



e. You should see the message indicating the import was successful, and then click **Close**.

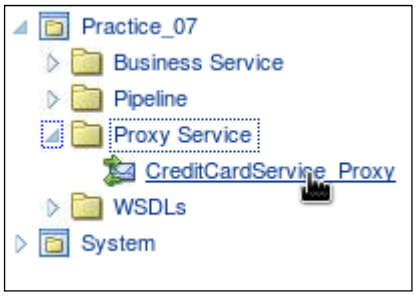
f. Activate the changes with an appropriate description.

2. Add User Name Token Service Oracle WSM policy to the proxy service.

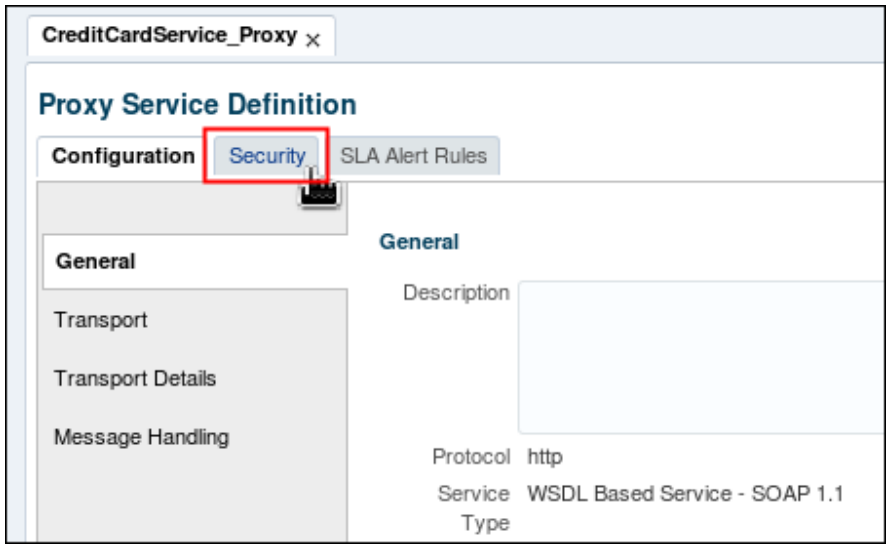
a. Create a new session in Service Bus.

b. Expand **Project Explorer**, and click **Practice_07** > **Proxy Service**.

c. On the Proxy Service page, click **CreditCardService_Proxy**.



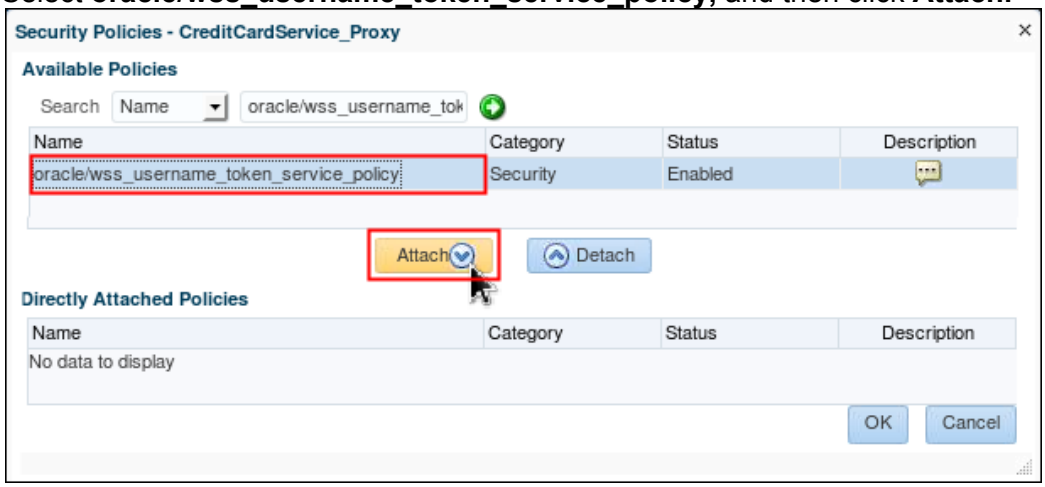
d. On the Proxy Service Definition page, click the **Security** tab.



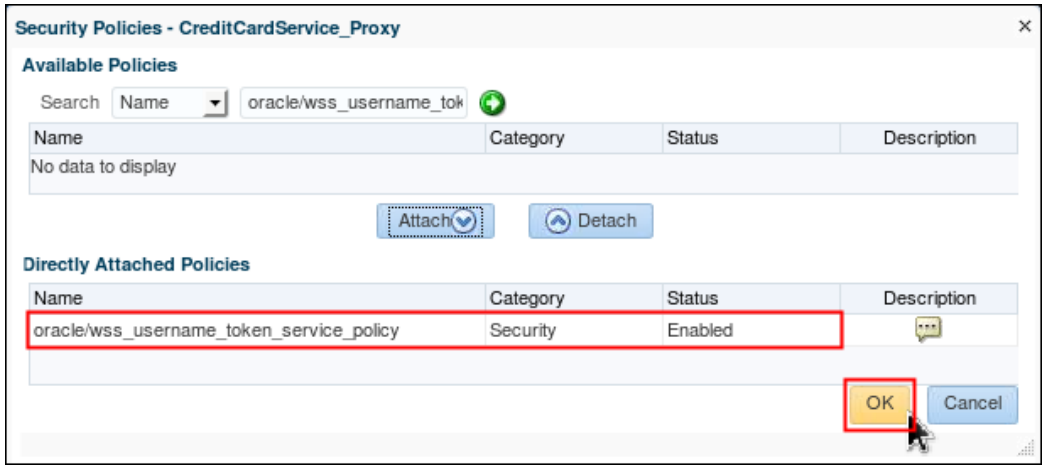
e. Under the Security tab, select **From OWSM Policy Store,** and then click **Attach Policies.**

f. In the **Security Policies – CreditCardService_Proxy** dialog box, enter **`oracle/wss_username_token_service_policy`** in the Name field, and then click **Search.**

g. Select **oracle/wss_username_token_service_policy,** and then click **Attach.**



h. Verify that the policy is attached, and then click **OK.**



i. **Save** the changes and **Activate** the session with an appropriate description.

Practice 7-3: Testing the Proxy Service Security Implementation

Overview

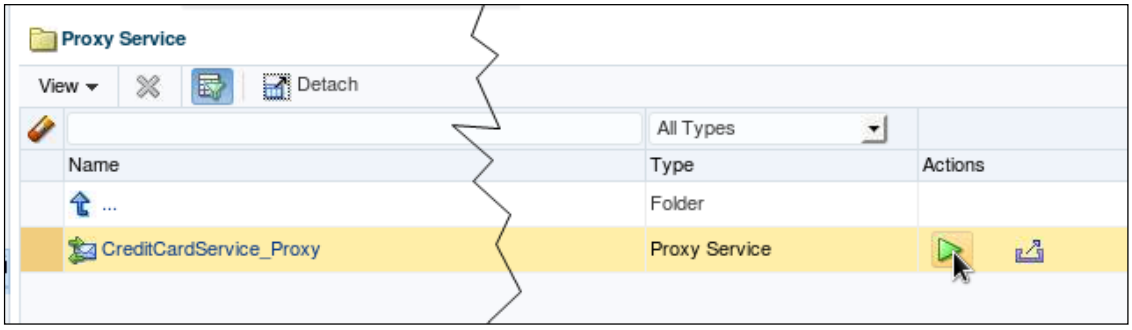
In this practice, you perform a positive test and a negative test to confirm the Oracle WSM security (User Name Token policy) implementation on the proxy service by using the Service Bus Test Console.

Assumptions

- The Oracle WSM security environment is configured to protect Service Bus services.
- Respective Oracle WSM key is defined.
- Respective user identities are created in Oracle WebLogic Server.
- The Service Bus proxy service is secured with the oracle/wss_username_token_service_policy Oracle WSM policy.

Tasks

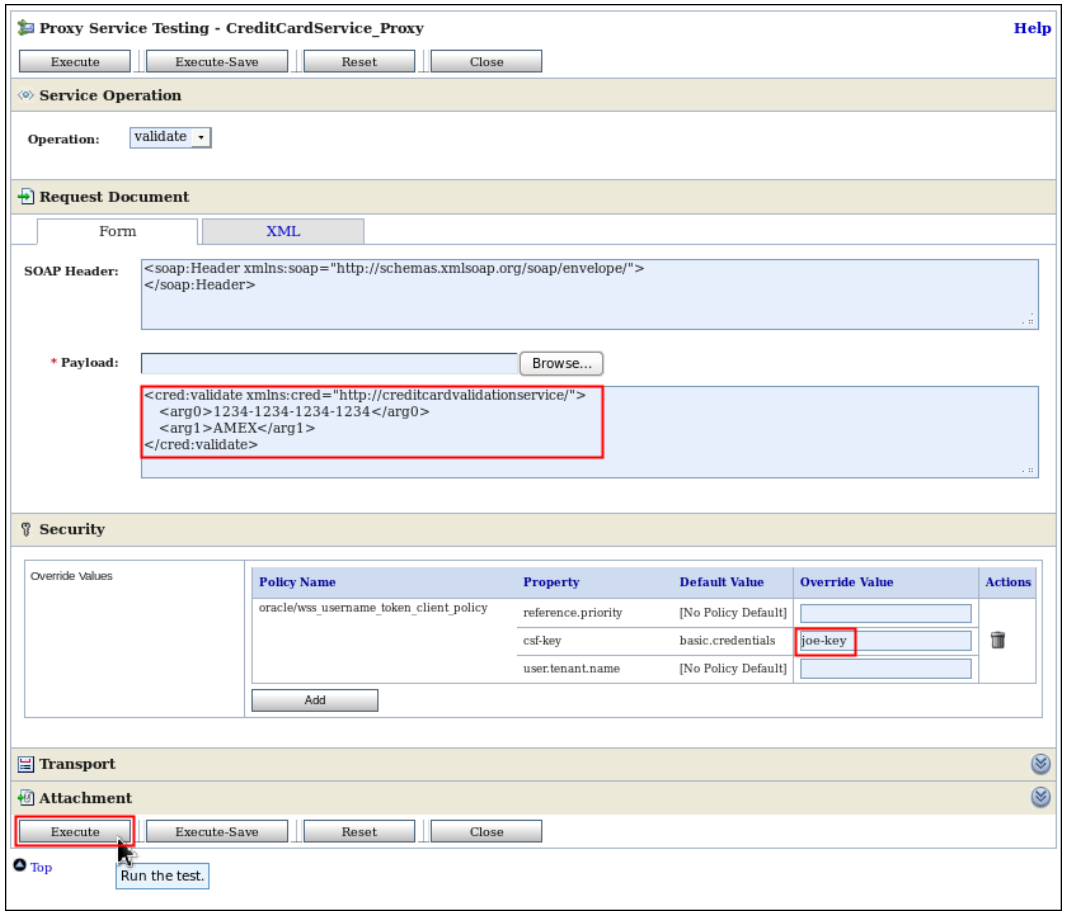
1. Perform a positive test to verify that the proxy service is securely invoked successfully.
   a. In Service Bus Console, navigate to the **Practice_07** > **Proxy Service** folder.
   b. Click the green arrow button in the Actions section to launch the Test Console for the **CreditCardService_Proxy** proxy service.



   c. In the Test Console, enter values in the Payload field. Specify the card number as `1234-1234-1234-1234` and the card type as **`AMEX`** as shown in the screenshot below.

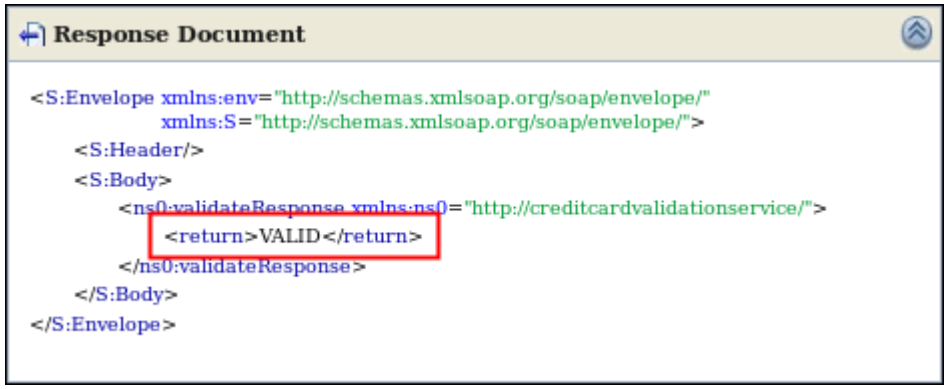
      Because the CreditCardService_Proxy proxy service is attached with the User Name Token Oracle WSM policy, you notice a Security section in the Test Console with an oracle/wss_username_token_client_policy policy name and with a csf-key property.

d. In the Test section, specify `joe-key` as the override value. The username and password have already been created, and a mapping joe-key csf-key with the same credentials has already been created by using the OEM Console.



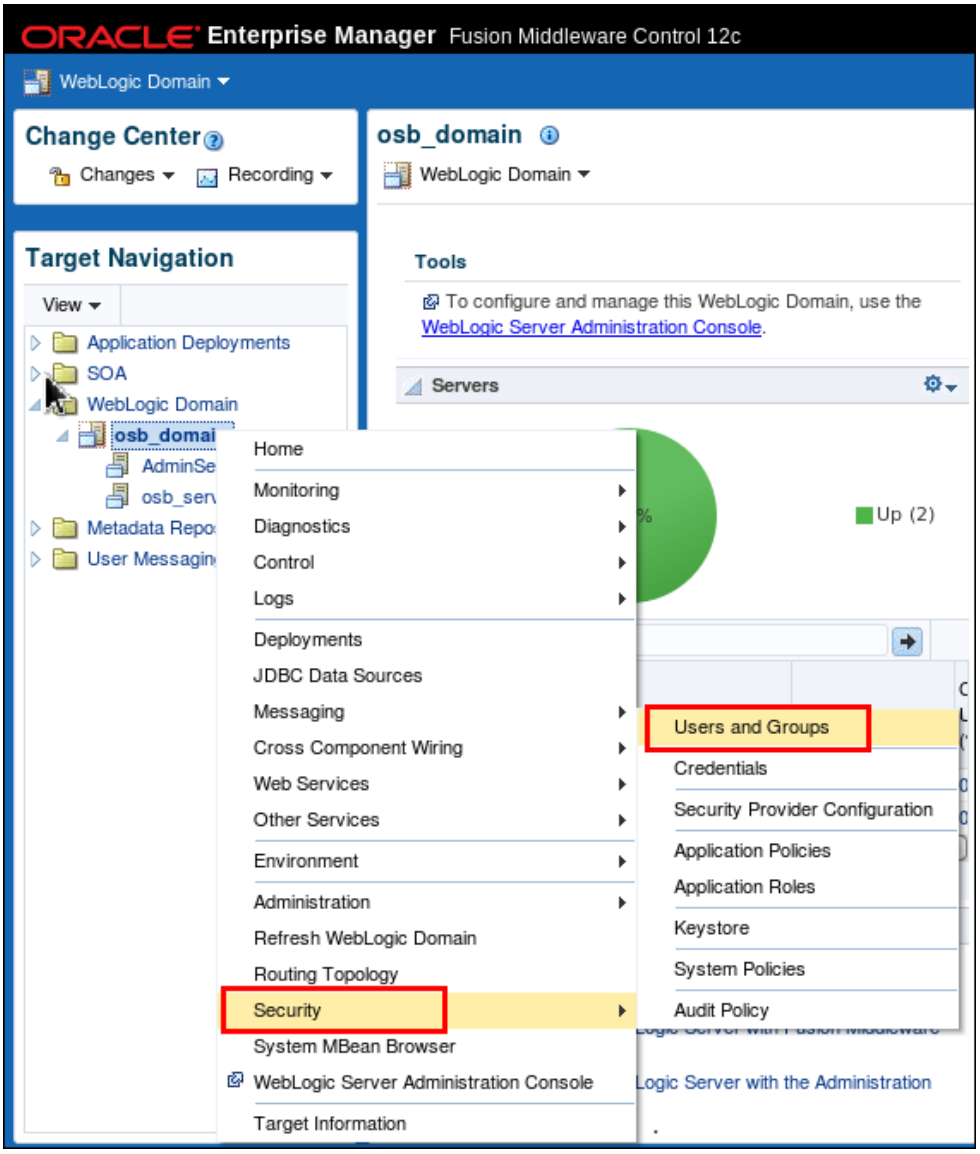
e. Click **Execute** to test the proxy service.

f. You should see the following response (in addition to SOAP headers).

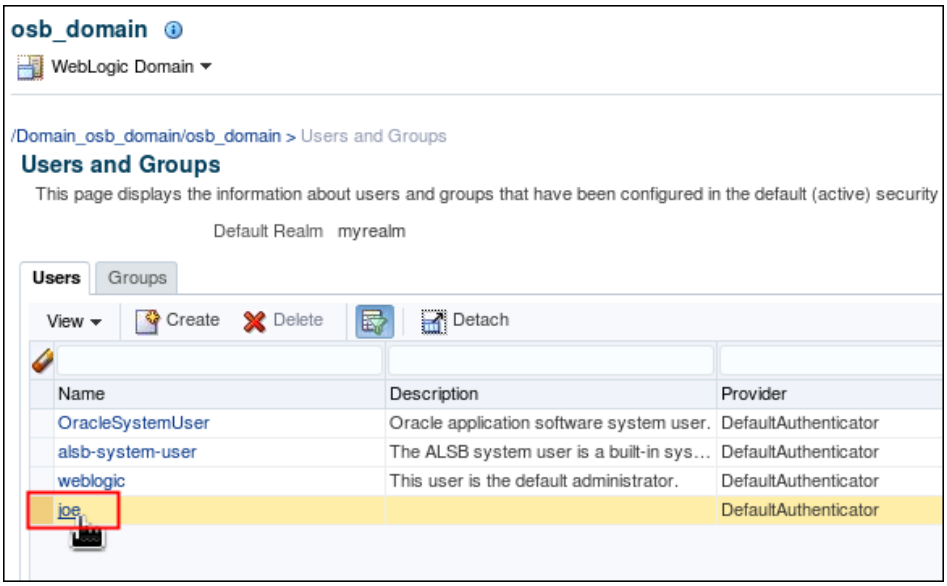


g. Close the Test Console.

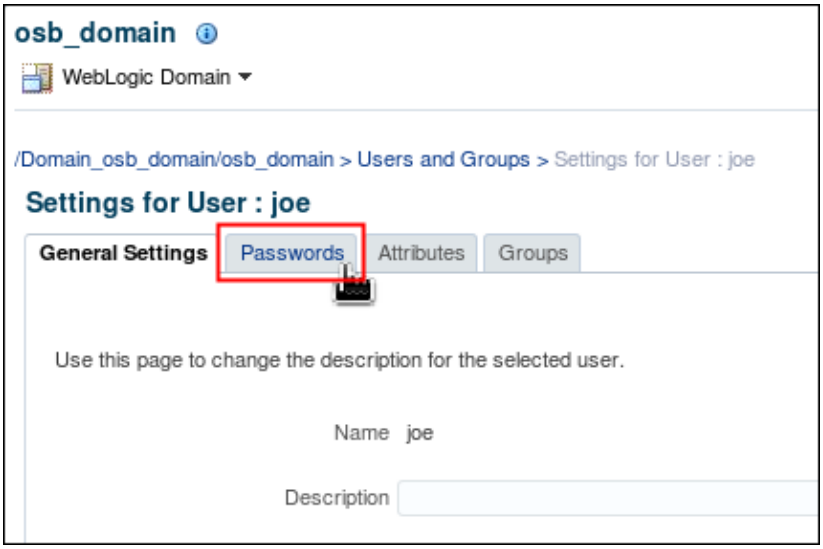
2. Perform a negative test by modifying the password of user `joe` to a different value, and then invoking the proxy service.
   a. In Enterprise Manager, right-click **osb_domain** and select **Security** > **Users and Groups**.



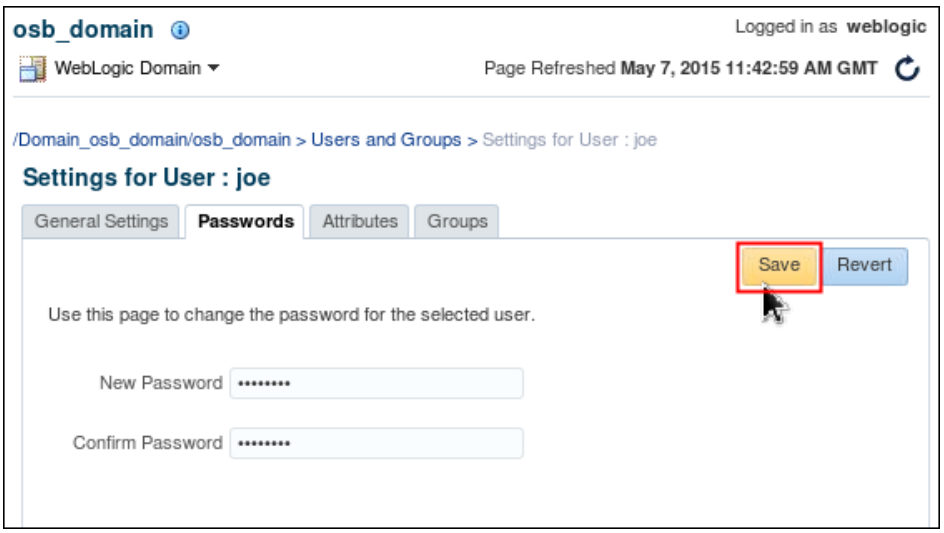
b. On the Users and Groups page, click **joe**.



c. On the "Settings for User: joe" page, click the **Passwords** tab.



d. Modify the password to (`See` **`OracleServiceBus12cPassword`** `File`), and then click **Save**.



e. Execute the same test case (the one you performed for the positive test) using the Service Bus Test Console. You see the request fail with the following response, because **`joe`**'s password does not match the value used in the Credential Map.

3. Reset the password of user **`joe`** back to (`See` **`OraScleServiceBus12cPassword`** `File`).

Practice 7-4: Propagating Identity from Service Bus to Secured Web Service

Overview

In this practice, you propagate the identity of the user authenticated in Oracle Service Bus to the web service application. As a part of this practice, you perform the following steps:

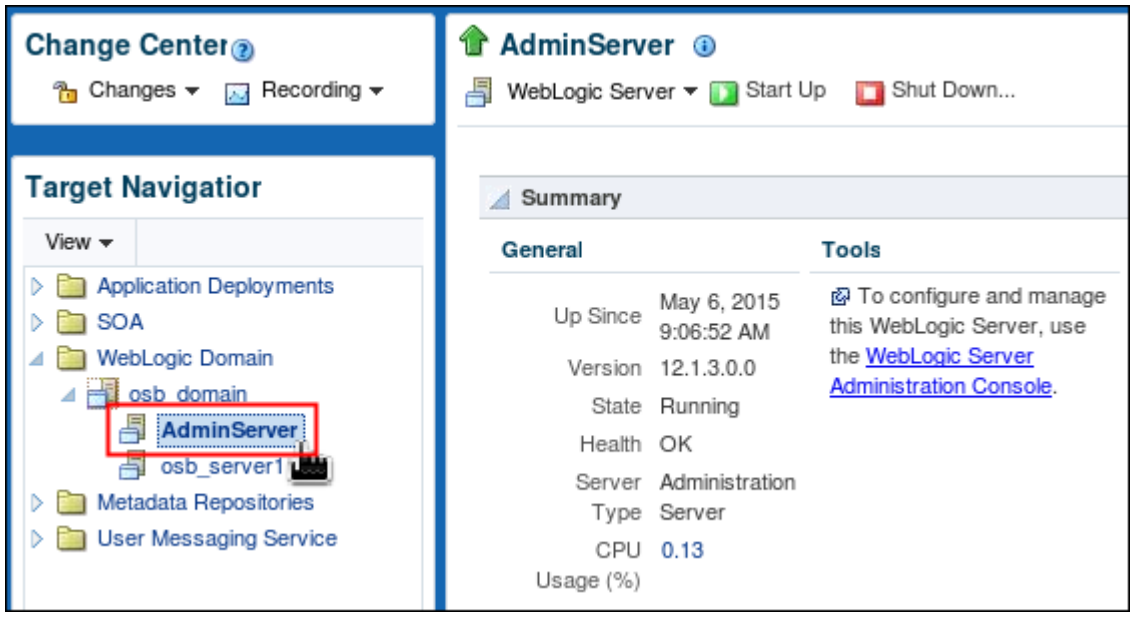
- Protect the CreditCardValidationService Java EE web service application deployed to the WebLogic Server by using the oracle/wss10_saml_token_service_policy service Oracle WSM policy.
- Update and attach the CreditCardService business service in Oracle Service Bus with the oracle/wss10_saml_token_client_policy client Oracle WSM policy.
- Test the security implementation.

Assumptions

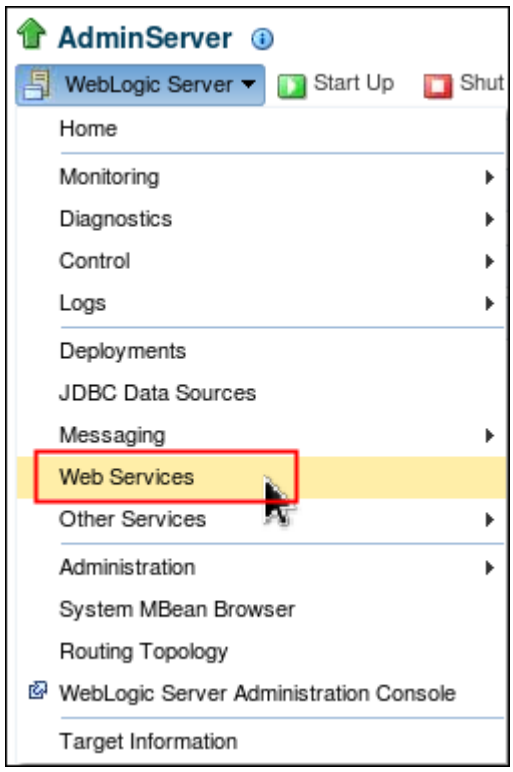
- The **`CreditCardService_Proxy`** proxy service is secured with the User Name Token Oracle WSM policy.
- The password of user **`joe`** is reinstated to `See` **`OracleServiceBus12cPassword`** `File`.

Tasks

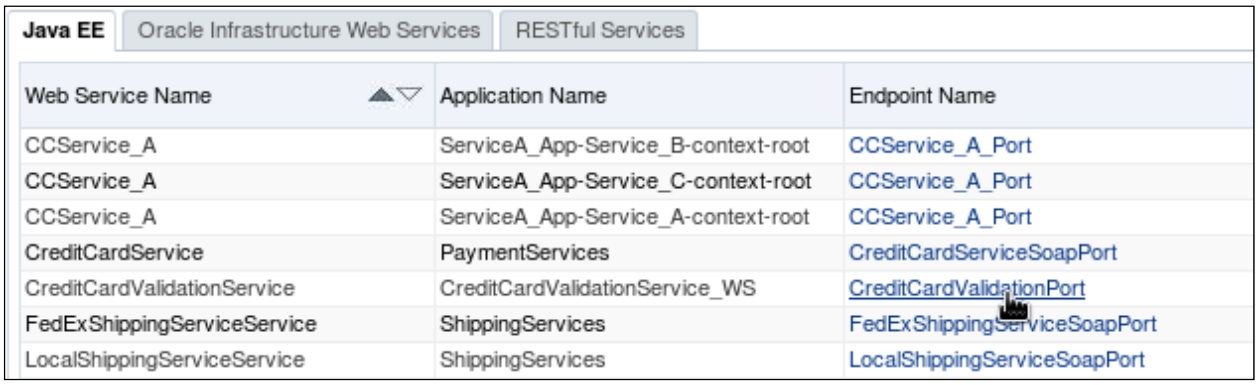
1. Add a SAML service Oracle WSM policy to the **`CreditCardValidationService`** web service application.
   a. In the Target Navigation panel of Enterprise Manager, expand **WebLogic Domain** > **osb_domain** and click **AdminServer**.



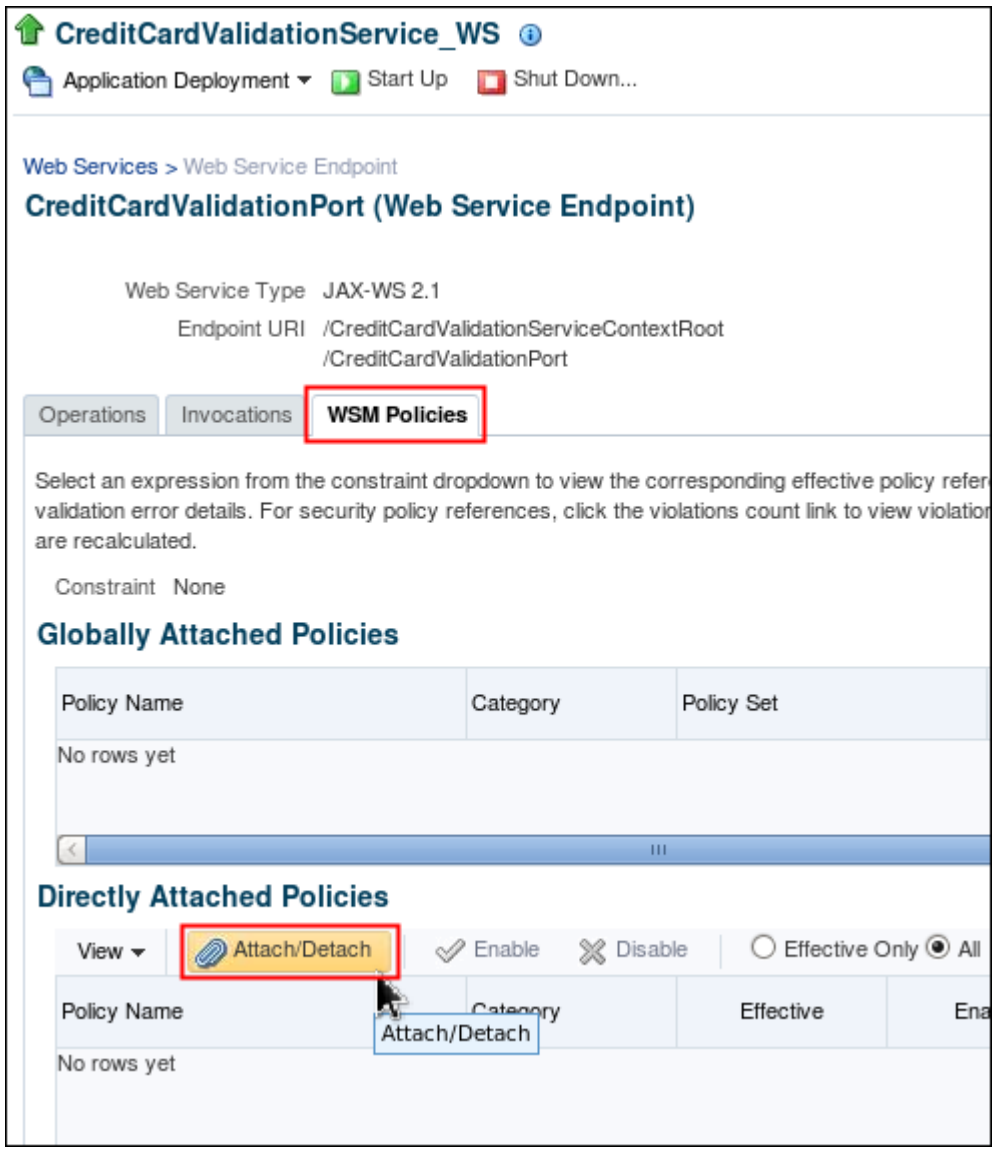
b. On the AdminServer page, from the **WebLogic Server** drop-down menu, click **Web Services**.



c. On the Web Services page, click **CreditCardValidationPort**.

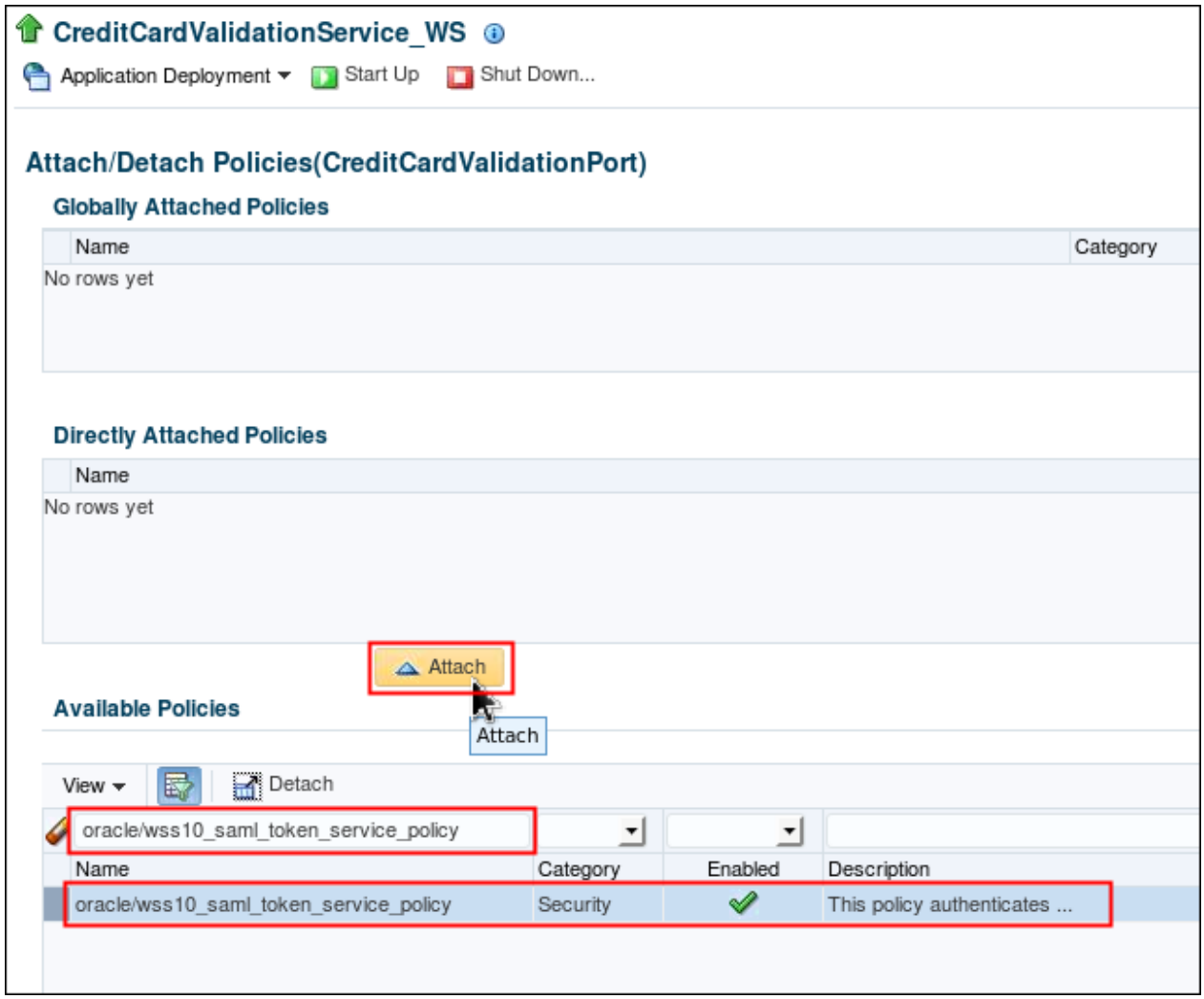


d. On the Web Service Endpoint page, select **WSM Policies** tab, and click **Attach/Detach.**

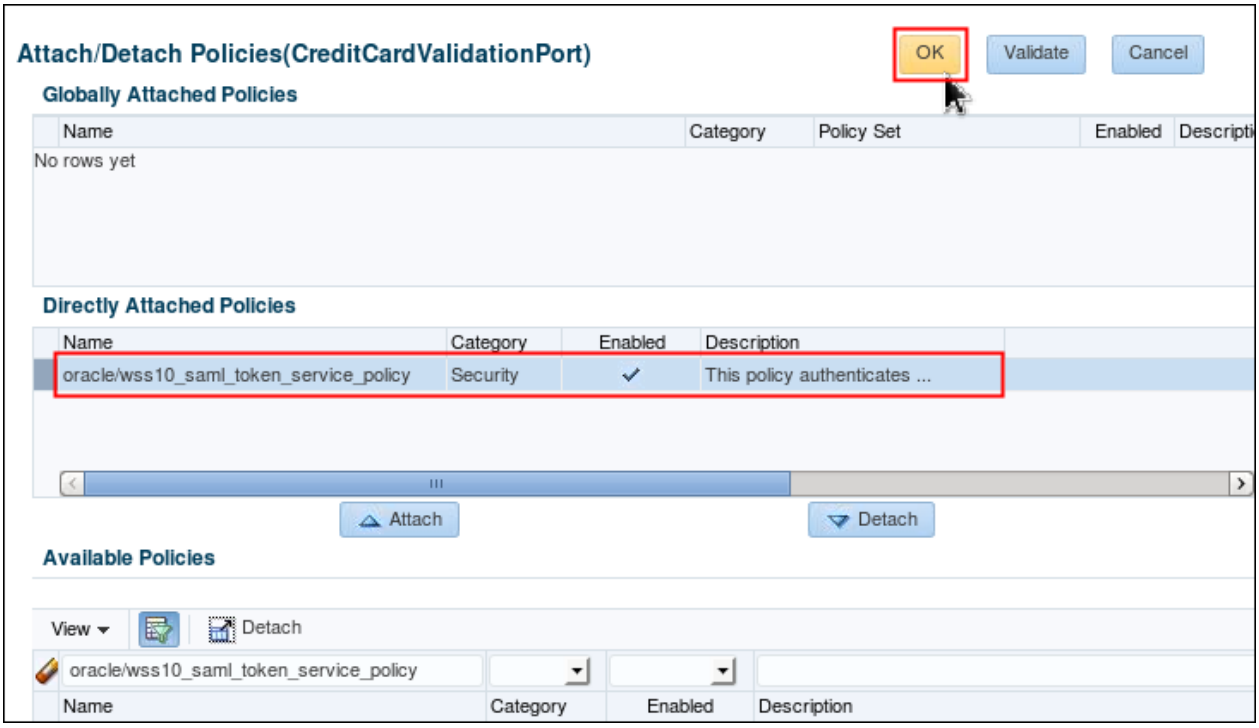


e. On the Attach/Detach Policies page, select `oracle/wss10_saml_token_service_policy` and click **Attach**.

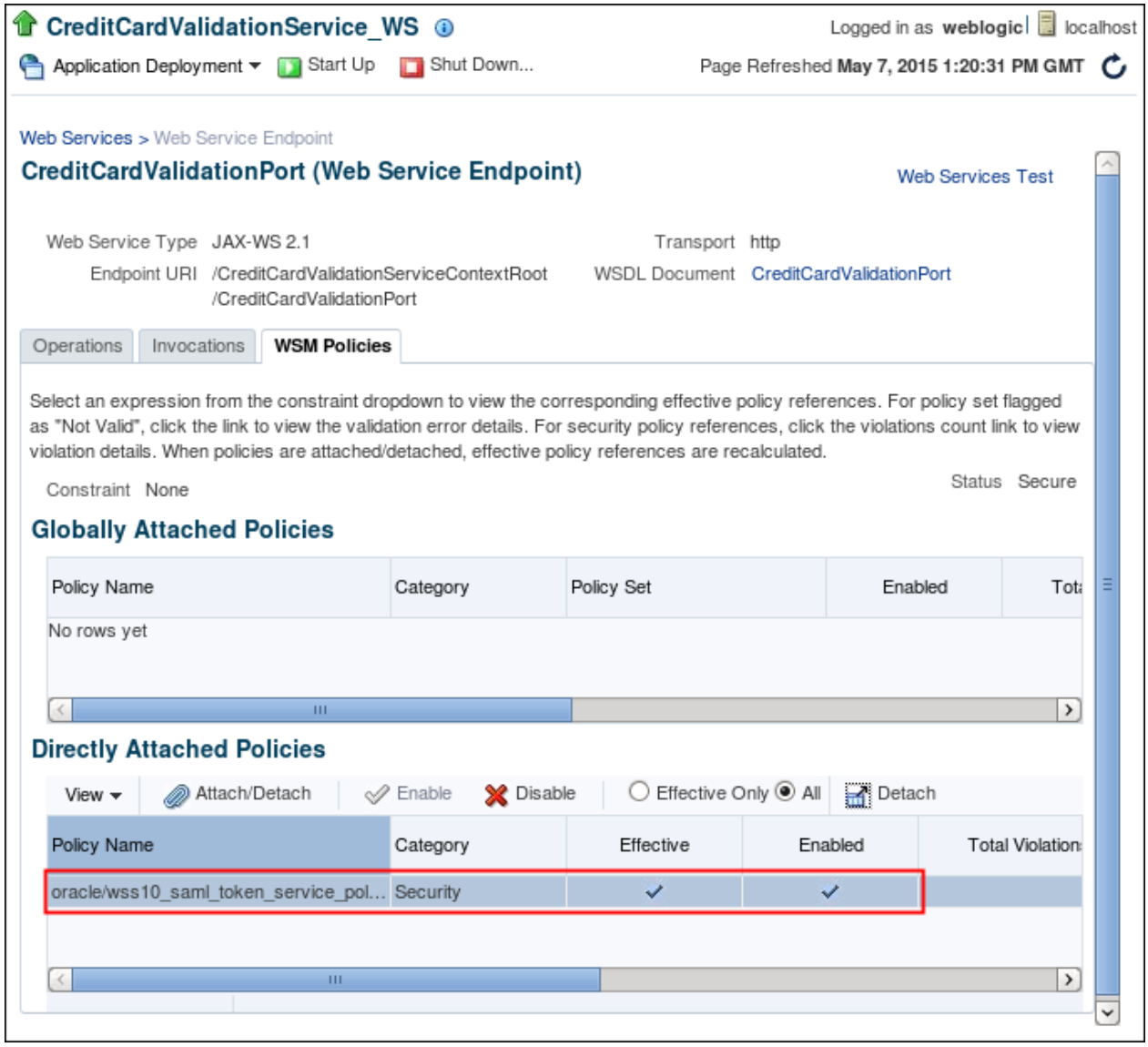
Note: You need to filter by entering the policy name or scroll down to select this policy.



f. On the Attach/Detach Policies page, verify that the policy is attached and click **OK.**

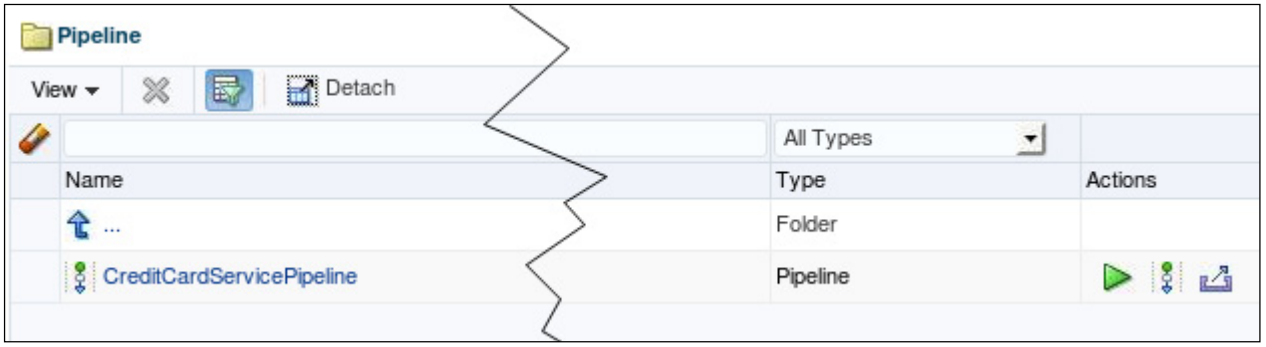


g. You should see the policy information attached to the service.

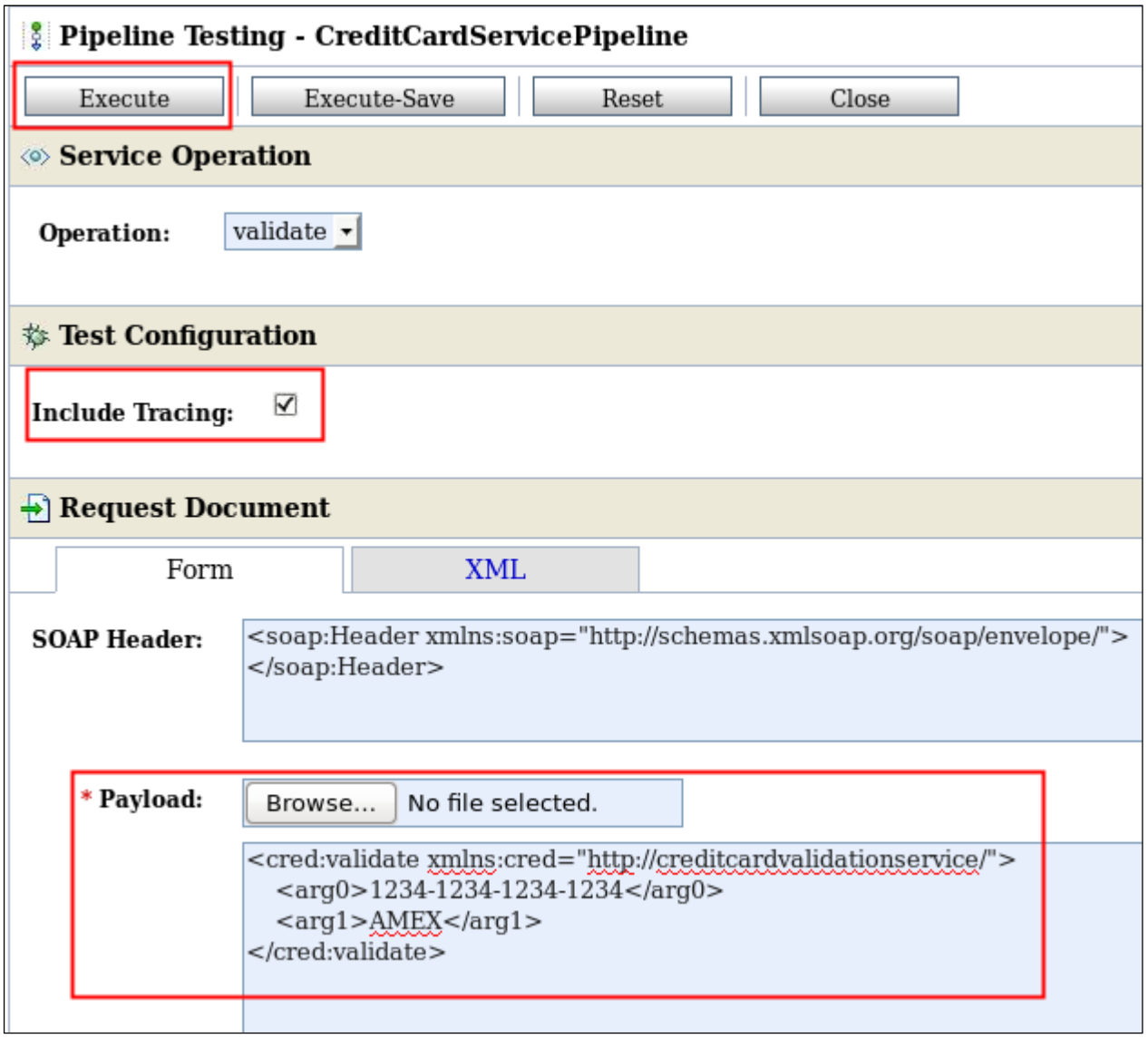


2. Test the security implementation by invoking the `CreditCardValidationService` web service from the Service Bus service without implementing the appropriate OWSM client-side policy.
   a. In Service Bus Console, navigate to the **Projects** > **Practice_07** > **Pipeline** page.

b. Click the green arrow button in the Actions section to launch the Test Console for the **CreditCardServicePipeline**.

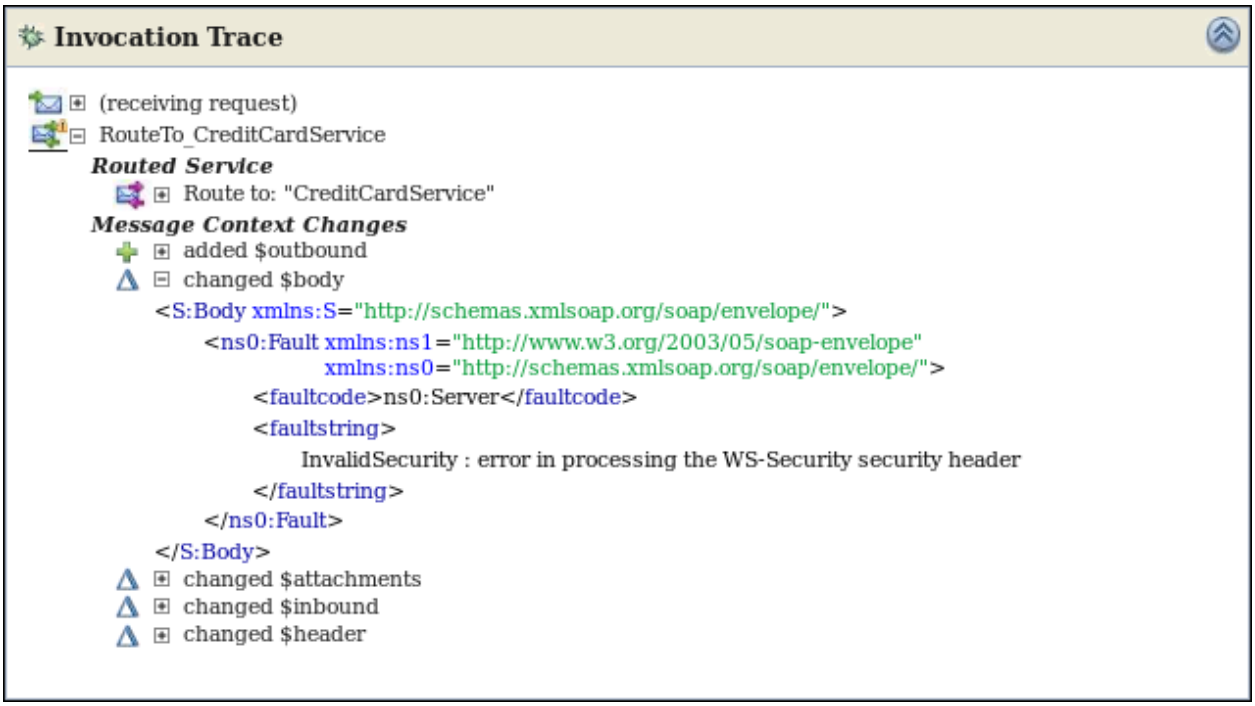


c. In the Test Console, enter values in the Payload field. Specify the card number as `1234-1234-1234-1234` and the card type as **`AMEX`** as shown in the screenshot below. Make sure the "**Include Tracing**" option is selected.



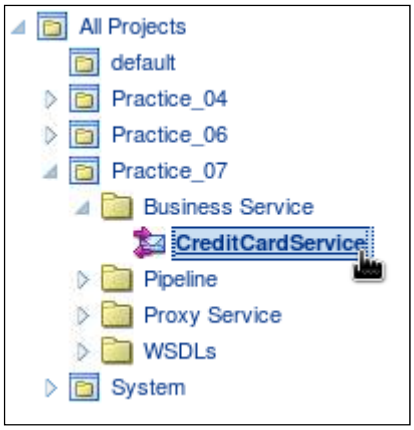
d. Click **Execute** to test the pipeline.

e. You should see the following invalid security message in the **Invocation Trace** section. This indicates that the Service Bus service didn't have the required security infrastructure to invoke the secured web service application.



f. Close the Test Console.

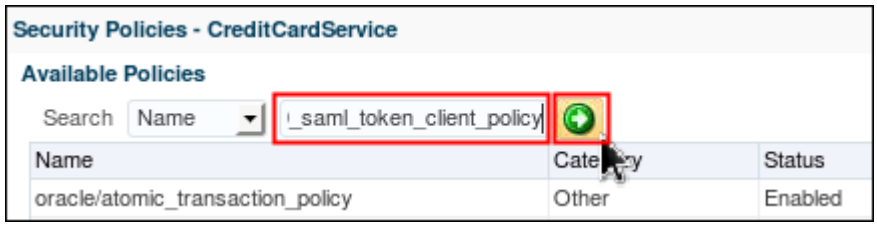
3. Add a SAML client Oracle WSM policy to the `CreditCardService` business service.
   a. In Service Bus Console, create a new session.
   b. Navigate to **Practice_07** > **Business Service** and click **CreditCardService**.



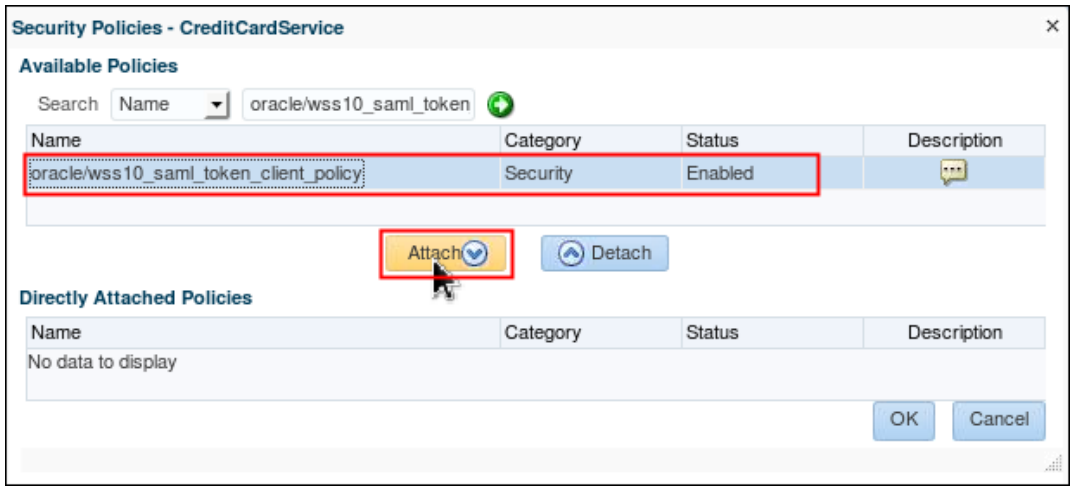
   c. On the Business Service Definition page, click the **Security** tab.

d. Select **From OWSM Policy Store,** and click **Attach Policies.**

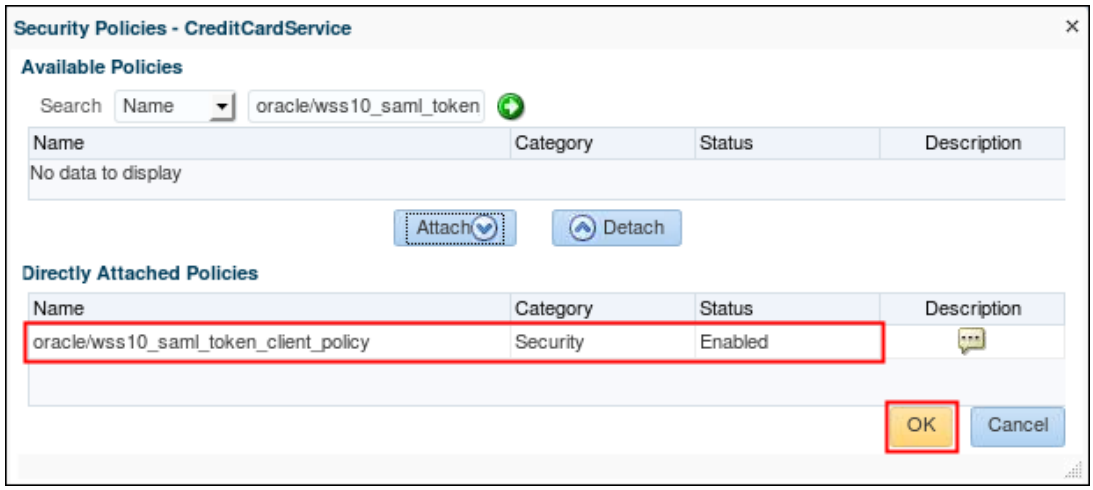
e. Under **Available Policies**, enter `oracle/wss10_saml_token_client_policy` in the Name field, and click the search icon.



f. In the results table, select `oracle/wss10_saml_token_client_policy` and click **Attach.**



g. In the Directly Attached Policies panel, verify that the policy is attached and click **OK.**

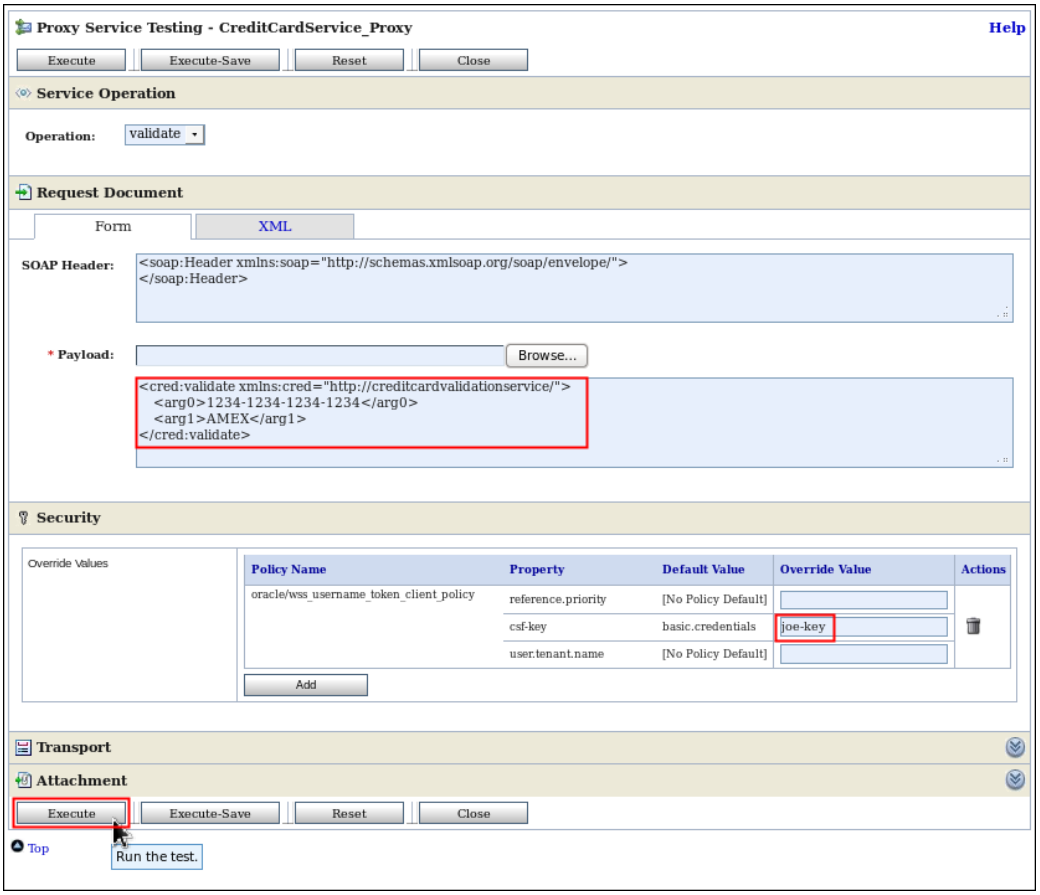


h. **Save** and **activate** the changes with an appropriate description.

4. Test the security implementation.
   a. In SB Console, navigate to the **Practice_07** > **Proxy Service** page.

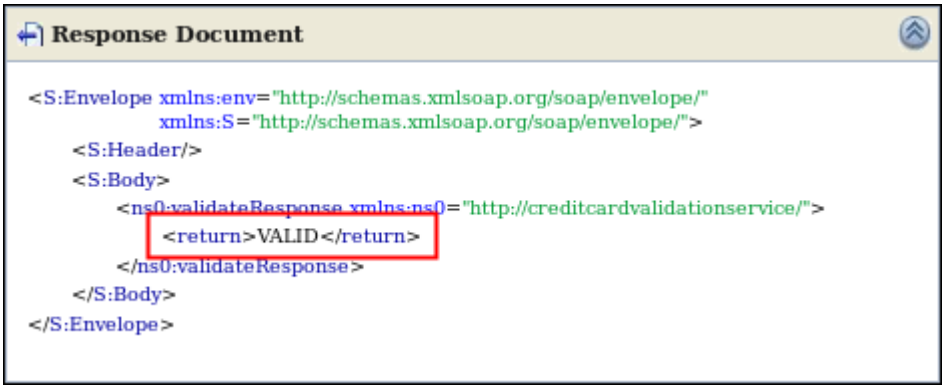
b. Click the green arrow button to launch the Test Console for the **CreditCardService_Proxy** proxy service.

c. In the Test Console, enter values in the Payload field. Specify the card number as `1234-1234-1234-1234` and the card type as `AMEX` as shown in the screenshot below. In the Security section, specify `joe-key` as the override value for the `oracle/wss_username_token_client_policy` policy with the csf-key property.



d. Click **Execute** to test the proxy service.

e. You should see the following response (in addition to SOAP headers). This indicates that the service was successfully invoked by using SAML identity propagation.



f. Close the Test Console.