Configuring Local and Outbound Authentication for a Service Provider

The responsibility of the local authenticators is to authenticate the user with locally available credentials. This can be either username/password or even IWA (Integrated Windows Authentication) or FIDO (Fast Identity Online). Local authenticators are decoupled from the Inbound Authenticators. Once the initial request is handed over to the authentication framework from an inbound authenticator, the authentication framework talks to the service provider configuration component to find the set of local authenticators registered with the service provider corresponding to the current authentication request.

Once the local authentication is successfully completed, the local authenticator will notify the framework. The framework will now decide no more authentication is needed and hand over the control to the corresponding response builder of the inbound authenticator. See Architecture for more information on this.

You can configure the following for local and outbound authentication.

1. Expand Local & Outbound Authentication Configuration.

Select the Authentication Type you require from the available options. This is a required field.

- If you choose Local Authentication, you need to select the local authentication option from the dropdown list.
- If you choose Federated Authentication, you need to select the identity provider from the dropdown list.
- If you choose Advanced Configurations, you can configure additional authentication steps and additional authentication options.

   - Assert identity using mapped local subject identifier: This option will use the local subject identifier when asserting the identity.
   - Always send back the authenticated list of identity providers: This option will send back the list of identity providers that the current user is authenticated by.
   - Use tenant domain in local subject identifier: This option will append the tenant domain to the local subject identifier.
   - Use user store domain in local subject identifier: This option will append the user store domain that the user resides in the local subject identifier.
   - Enable Authorization: This option enables you to engage authorization policies for the service provider. For more information, see Configuring Access Control Policy for a Service Provider.
1. Select the Multi-Option and Multi-Step authentication.

   a. There are two types of multi-factor authentication that can be configured here.
      
      i. **Multi-step authentication**: Click **Add Authentication Step**. Clicking this again will enable you to create another authentication step. Once this is done you can configure a Local or Federated authenticator for the step by selecting one from the dropdown and clicking **Add Authenticator**.
      
      ii. **Multi-option authentication**: Click **Add Authenticator** to add either a Local or Federated authenticator after selecting it from the dropdown. Adding more than one of these within a single step enables multi-option authentication.

   b. Select whether to **Use subject identifier from this step**, **Use attributes from this step** or both. In the case of multiple steps, you can have only one step to use subject identifier from

---

**Note**

If you apply the WUM update for WSO2 IS 5.5.0, released on the 1st of August 2018, you will see **Use user store domain in roles** in the **Local & Outbound Authentication Configuration** section.

This check box is selected by default, and appends the userstore domain name to user roles. If you do not want to append the userstore domain name to user roles, clear the check box.

**Tip**

If a user role is not mapped to a service provider role, and you clear the **Use user store domain in roles** check box, the userstore domain name will be removed from the role claim value unless the userstore domain name is APPLICATION, INTERNAL, or WORKFLOW.
this step and one to use attributes from this step.
For example let's say, we configure 1st step as Facebook and enable Use subject identifier from this step. Then configure Google for 2nd step and enable Use attributes from this step. Once authentication is complete subject id will be taken from the Facebook claims and Google claims will be used as user attributes.

c. Click Add Authenticator to add a Local Authenticator. You can choose the type of authenticator using the dropdown. Clicking Add Authenticator again will enable you to add a second local authenticator. Basic authentication allows you to authenticate users from the enterprise user store.

d. Click Add Authenticator to add a Federated Authenticator. You can choose the type of authenticator using the dropdown. Clicking Add Authenticator again will enable you to add a second federated authenticator.

e. Click the Update button. This will return you to the previous screen with your newly configured authentication steps.

3. Add a local authenticator under Request Path Authentication Configuration by clicking the Add button. Clicking the Add button again enables you to add another local authenticator. The two types of local authenticators available are as follows.
   - OAuthRequestPathAuthenticator
   - BasicAuthRequestPathAuthenticator

Look through the following for more details on the various authentication types.

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>This is the default authenticator sequence for a configured service provider in the Identity Server. This sequence can be modified by updating the following section in the <code>&lt;IS_HOME&gt;/repository/conf/identity/application-authentication.xml</code> file.</td>
</tr>
</tbody>
</table>

```
<Sequences>
    <!-- Default Sequence. This is mandatory -->
    <Sequence appId="default">
        <Step order="1">  
            <Authenticator name="BasicAuthenticator"/>
        </Step>
    </Sequence>
</Sequences>
```

<table>
<thead>
<tr>
<th>Local Authentication</th>
<th>In this case, Identity Server itself authenticate the user. There are three types of local authenticators OOTB in a fresh Identity Server pack.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The <strong>basic</strong> authenticator is used to authenticate the user using the credentials available in the Identity Server.</td>
</tr>
<tr>
<td></td>
<td><strong>IWA</strong> stands for Integrated Windows Authentication and involves automatically authenticating users using their Windows credentials.</td>
</tr>
<tr>
<td></td>
<td><strong>FIDO</strong> authenticator is a local authenticator that comes with the WSO2 Identity Server. This will handle FIDO authentication requests related key validation against stored keys, the public key, key handler, and the counter, attestation certificate of FIDO registered users.</td>
</tr>
</tbody>
</table>
Federated Authentication

In this case, Identity Server trust third-party Identity provider to perform the user authentication. These Identity providers use various protocols to transfer authentication/authorization related messages. Currently, the Identity Server only supports the following federated authenticators OOTB.

- SAML2 Web SSO
- OAuth2/OpenID Connect
- WS-Federation (Passive)
- Facebook
- Microsoft (Hotmail, MSN, Live)
- Google
- SMS OTP
- Email OTP
- Twitter
- Yahoo
- IWA Kerberos
- Office365

Advanced Configuration

Advanced configurations enable you to add multiple options or steps in authentication. When multiple authentication steps exists, the user is authenticated based on each and every one of these steps. If only one step is added then the user is only authenticated based on the local and/or federated authenticators added in a single step. However, in the case of local and/or federated authenticators, the authentication happens based on any one of the available authenticators.

Request path authenticators

A request path authenticator will get executed only if the initial authentication request brings the applicable set of credentials with it. See Request Path Authentication for more details.

Related Topics

- See Multi-factor Authentication using FIDO for more information on configuring multi-step and multi-option authentication using FIDO.
- See Request Path Authentication for information on a local authenticator that is executed if the initial authentication request brings a set of credentials with it.
- See Try Request Path Authentication for more information on how the request path authenticator works using the WSO2 playground sample.