Multi-factor Authentication using FIDO

Before you begin

There are a few changes made to the chrome u2f extension which causes the FIDO device to not register properly as an authentication factor. Additionally, Firefox no longer supports the u2f extension anymore. Therefore, WSO2 Identity Server solves this by using the WebAuthn API to enable FIDO-based authentication. The WebAuthn API is already supported by the following browser versions:

- Chrome (CHROME 67)
- Firefox (FIREFOX 60)
- Edge (EDGE 17723)

This fix is available for WSO2 IS 5.3.0 through the 5780 WUM update. You can apply the WUM update using the WSO2 Update Manager (WUM).

1. Shutdown the WSO2 Identity Server if it is already running.
2. Take a backup copy of the authenticationendpoint.war and the extracted authenticationendpoint folder found in the <CARBON_SERVER>/repository/deployment/server/webapps/ folder and then delete them.
3. Apply the 5780 WUM update using WSO2 Update Manager.

To deploy a WUM update into production, you need to have a paid subscription. If you do not have a paid subscription, you can use this feature with the next version of WSO2 Identity Server when it is released. For more information on updating WSO2 Identity Server using WUM, see Getting Started with WUM in the WSO2 Administration Guide.

4. Create the FIDO2_DEVICE_STORE table using the relevant updated DB query located in the <IS_HOME>/dbscripts/identity folder.
5. Add the following properties to the `identity.xml` file found in the `<IS_HOME>/repository/conf/identity` folder.

```xml
<FIDO>
  <WebAuthn>
    <Enable>true</Enable>
  </WebAuthn>
  <FIDO2TrustedOrigins>
    <Origin>${carbon.protocol}://${carbon.host}:${carbon.management.port}</Origin>
  </FIDO2TrustedOrigins>
</FIDO>
```

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebAuthn. Enable</td>
<td>Set this property to true to enable using the WebAuthn API. This feature is only available for the following browser versions:</td>
</tr>
<tr>
<td></td>
<td>• Chrome 67 and later</td>
</tr>
<tr>
<td></td>
<td>• Firefox 60 and later</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Edge 17723 and later</td>
</tr>
<tr>
<td></td>
<td>WSO2 recommends using WebAuthn feature if you are using any of the browsers listed above.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you have used FIDO previously, your devices must be re-enrolled once this property is set to true.</td>
</tr>
</tbody>
</table>

6. Add the following property to the `identity.xml` file under the `<ResourceAccessControl>` tag to secure the WebAuthn endpoints.

```xml
<Resource context="(.*)/api/users/v2/me/webauthn(.*\") secured="true" http-method="all">  
  <Permissions>/permission/admin/manage/identity</Permissions>
</Resource>
```

7. Add the following property to the `identity.xml` file under the `<WebApp>` tag of `<TenantContextsToRewrite>`.

```xml
<Context>/api/users/v2/me/webauthn</Context>
```

8. Add the following property to the `application-authentication.xml` file found in the `<IS_HOME>/repository/conf/identity` folder within the `<AuthenticatorConfig name="FIDOAuthenticator">` tag.

```xml
<Parameter name="Fido2Auth">/authenticationendpoint/fido2-auth.jsp</Parameter>
```
The following topics provide details and instructions on how to configure multi-factor authentication (MFA) using the WSO2 Identity Server. This topic expands on what MFA is and how it can be used in certain scenarios. It also provides information on FIDO and how MFA can be configured using FIDO U2F.

For more information on Multi-factor Authentication concepts with Identity Server, refer Configuring Multi-factor Authentication for WSO2 IS.

- About FIDO
- Configuring multi-factor authentication using FIDO
- Checking browser support for FIDO devices

About FIDO

The Fast IDentity Online (FIDO) attempts to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. In short, FIDO U2F (Universal 2nd Factor) can make it easy for you to authenticate users while ensuring that security is enhanced.

FIDO provides two user experiences to address a wide range of use cases and deployment scenarios. FIDO protocols are based on public key cryptography and are strongly resistant to phishing.

**PASSWORDLESS EXPERIENCE**
(UAF standards)

**SECOND FACTOR EXPERIENCE**
(U2F standards)

![Figure 1: UAF and U2F.](image)

**Universal Authentication Framework (UAF)**

UAF involves a password-less experience with the following key processes:

- The user carries the client device with the UAF stack installed.
- The user presents a local biometric or PIN.
- The website can choose whether to retain the password.

**Universal Second Factor (U2F)**

1. Restart the server using one of the following commands.
   a. Linux/Unix: sh wso2server.sh
   b. Windows: wso2server.bat
2. Once you have restarted the server, navigate to the extracted authenticationendpoint folder found in the `<CARBON_SERVER>/repository/deployment/server/webapps/` folder and merge any customizations to the new artifact using the backup copy of the file you took in step 2 as a reference.
U2F focuses on the 2nd factor experience and has the following key processes:

- The user carries the U2F device with built-in support in web browsers.
- The user presents the U2F device.
- The website can simplify the password (for example, it can be simplified to a 4-digit PIN).

U2F tokens provide cryptographic assertions that can be verified by relying parties. Typically, the relying party is a web server, and the cryptographic assertions are used as second-factors (in addition to passwords) during user authentication. U2F tokens are typically small special-purpose devices and FIDO Client is a web browser that communicates between the token and the relying party.

**U2F protocol operations**

The following are the two main processes that take place when using FIDO U2F.

1. **Registration**: Upon registration, a device gives the server its attestation certificate. This certificate can be (optionally) used to verify the authenticity of the device.
2. **Authentication**: The authentication operation proves possession of a previously-registered keypair to the relying party.

Both the registration and authentication operation consists of three phases depicted in the following figure.

![Figure 2: Three phases of U2F protocol operations](image)

- **Setup**: In this phase, the FIDO Client contacts the relying party and obtains a challenge. Using the challenge (and possibly other data obtained from the relying party and/or prepared by the FIDO Client itself), the FIDO Client prepares a request message for the U2F token.
- **Processing**: In this phase, the FIDO Client sends the request message to the token, and the token performs some cryptographic operations on the message, creating a response message. This response message is sent to the FIDO Client.
- **Verification**: In this phase, the FIDO Client transmits the token's response message, along with other data necessary for the relying party to verify the token response, to the relying party. The relying party then processes the token response and verifies its accuracy. A correct registration response will cause the relying party to register a new public key for a user, while a correct authentication response will cause the relying party to accept that the client is in possession of the corresponding private key.

**Basic authentication process flow of U2F**

The following figure provides the complete authentication process flow when authenticating using FIDO U2F.
Figure 3: Authentication process flow for U2F

Configuring multi-factor authentication using FIDO

The instructions in this section enable you to successfully set up multi-factor authentication using the WSO2 Identity Server.

⚠️ FIDO authenticator can be configured only after a local authenticator is configured in the previous steps. It cannot be configured as the 1st step or if federated authenticator set the subject identifier.

Setting up an account for MFA

1. Log in to the WSO2 Identity Server end-user dashboard.
2. Navigate to the My Profile section by clicking the associated View Details button.
3. Click Manage U2F Authentication.

✔️ When you click this, the FIDO device that you need to add must already be plugged into the computer.
4. You can add a new U2F device to your account and remove it when needed. The new U2F device can be added by clicking the **Attach FIDO Token** button. Then you need to touch the 'key' icon on the FIDO device in order to complete the adding process. Once you have added the devices, they are listed in the page that appears. By clicking the **Remove** button, you can remove any device you want.

![Manage U2F Authentication](image)

**Tip:** You can have multiple devices associated to your account.

![Manage FIDO U2F Device](image)

**Configuring FIDO U2F as an authenticator**

1. Log in to the **Management Console**.
2. Create a Service Provider.

![Attach FIDO Token](image)

For more information on creating a service provider, see **Adding and Configuring a Service Provider**.

a. Navigate to the **Main** menu to access the **Identity** menu. Click **Add** under **Service Providers**.
b. Fill in the **Service Provider Name** and provide a brief **Description** of the service provider. Only **Service Provider Name** is a required field.

c. Click **Register** to add the new service provider.

3. Access the service provider you just created and expand **Local & Outbound Authentication Configuration**.

   For more information on configuring the local and outbound authentication configuration, see **Configuring Local and Outbound Authentication for a Service Provider**.

4. Select **Advanced Configuration** to configure multi-factor authentication.

5. Click **Add Authentication Step**. Then add a local authenticator from **Local Authenticators** section.

Select "**Use subject identifier from this step**" and "**Use attributes from this step**" options from this step since we identify the user from this step.

6. Click **Add Authentication step** and add **FIDO** authenticator from **Local Authenticators** section. This will enable the FIDO as the 2nd step authenticator for the users who authenticated with the basic authentication.

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

**Checking browser support for FIDO devices**
The https://demo.yubico.com/u2f site can be used to check the browser support for FIDO devices.

As for now, Google Chrome (version 38 or later) has support for FIDO devices. Firefox does not support FIDO natively. An add-on must be added to Firefox to support FIDO devices. You can download and install the add-on from here.