OpenID Connect Discovery

The WSO2 Identity Server supports OpenID Connect Discovery as a means of discovering the end user’s OpenID Provider and obtaining information needed to interact with it, including its OAuth 2.0 endpoint locations. For more information, see IssuerDiscovery.

The OpenID Connect Discovery endpoint is as follows:

https://localhost:9443/.well-known/webfinger

The following information is required to make a request.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Identifier for the target end user that is the subject of the discovery request.</td>
<td>acct:admin@localhost (for super tenant) acct:<a href="mailto:admin@wso2.com">admin@wso2.com</a>@localhost (for tenant)</td>
</tr>
<tr>
<td>HostServer</td>
<td>Where the WebFinger service is hosted.</td>
<td>localhost</td>
</tr>
<tr>
<td>rel</td>
<td>URI identifying the type of service whose location is being requested.</td>
<td><a href="http://openid.net/specs/connect/1.0/issuer">http://openid.net/specs/connect/1.0/issuer</a></td>
</tr>
</tbody>
</table>

By default, all endpoints in the WSO2 Identity Server are secured with basic authentication. You will need authentication details to call the endpoints. By default, you can use admin credentials or an access token for the request.

- For more information on how to obtain an access token, see Allowed grant types for OAuth2-OpenID Connect.
- For more information on securing the REST API or customizing authentication/authorization for the REST API, see Authenticating and Authorizing REST APIs.

Sample requests and responses are shown below.

<table>
<thead>
<tr>
<th>Request #1 (for super tenant)</th>
<th>Sample Request</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>curl -v -k --user admin:admin <a href="https://localhost:9443/.well-known/webfinger?resource='acct:admin@localhost&amp;rel=http://openid.net/specs/connect/1.0/issuer">https://localhost:9443/.well-known/webfinger?resource='acct:admin@localhost&amp;rel=http://openid.net/specs/connect/1.0/issuer</a>'</td>
</tr>
</tbody>
</table>
### Response #1 (for super tenant)

```
{
    "subject": "acct:admin@localhost",
    "links": [
        {
            "rel": "http://openid.net/specs/connect/1.0/issuer",
            "href": "https://localhost:9443/oauth2/oidcdiscovery"
        }
    ]
}
```

### Request #1 (for tenant: wso2.com)

**Sample Request**

```
curl -v -k --user admin:admin https://localhost:9443/.well-known/webfinger?resource='acct:admin%40wso2.com@localhost&rel=http://openid.net/specs/connect/1.0/issuer'
```

### Response #1 (for tenant: wso2.com)

```
{
    "subject": "acct:admin@wso2.com@localhost",
    "links": [
        {
            "rel": "http://openid.net/specs/connect/1.0/issuer",
            "href": "https://localhost:9443/t/wso2.com/oauth2/oidcdiscovery"
        }
    ]
}
```

### Request #2

Once you receive the response shown above, use the href received and append `.well-known/openid-configuration` to it.

**Sample Request**

```
curl -v -k --user admin:admin https://localhost:9443/oauth2/oidcdiscovery/.well-known/openid-configuration
```

### Response #2

**Sample Response**

```
{
    "scopes_supported": [
        "address",
        "phone",
        "email",
        "profile",
        "openid"
    ],
```
"check_session_iframe": "https://localhost:9443/oidc/checksession",
"issuer": "https://localhost:9443/oauth2/token",
"authorization_endpoint": "https://localhost:9443/oauth2/authorize",
"claims_supported": [
  "formatted",
  "name",
  "phone_number",
  "given_name",
  "picture",
  "region",
  "street_address",
  "postal_code",
  "zoneinfo",
  "locale",
  "profile",
  "locality",
  "sub",
  "updated_at",
  "email_verified",
  "nickname",
  "middle_name",
  "email",
  "family_name",
  "website",
  "birthdate",
  "address",
  "preferred_username",
  "phone_number_verified",
  "country",
  "gender",
  "iss",
  "acr"
],
"token_endpoint": "https://localhost:9443/oauth2/token",
"response_types_supported": [
  "id_token token",
  "code",
  "id_token",
  "token"
],
"end_session_endpoint": "https://localhost:9443/oidc/logout",
"userinfo_endpoint": "https://localhost:9443/oauth2/userinfo",
"jwks_uri": "https://localhost:9443/oauth2/jwks",
"subject_types_supported": [
  "pairwise"
],
"id_token_signing_alg_values_supported": ["RS256"],
"registration_endpoint": "https://localhost:9443/identity/connect/register"