Configuring Service Provider Metadata

The identity provider should have all the information to communicate with the service provider using SAML 2.0 authentication.

Base configuration of service provider metadata

A complex service provider metadata configuration is not needed. Only two options must be configured in an identity provider management system: the Assertion Consumer Service URL and the Service Provider Entity ID:

1. **Assertion Consumer Service URL:** The URL where SAML assertions are sent after a user has been authenticated. The URL is composed of the OAuth server URL, authentication type, and /Acs postfix, e.g., https://server.com/instance/OAuthServer/Saml2-AzureAD/Acs. Suppose internal and external clients connect to the OAuth server using different URLs. The Assertion Consumer Service URL should be configured in a used identity provider management system according to each OAuth server URL.
2. **Service Provider Entity ID:** The unique identifier most often used as an audience of SAML assertion.

Important

Case sensitivity is important while configuring the Assertion Consumer Service URL. Make sure that it is in the same registry as the path where the OAuth server authentication cookie is stored (it is the OAuth server path, e.g., Innovator/OAuthServer from the Assertion Consumer Service URL example above).

Some identity providers make configuring SAML 2.0 authentication possible using service provider metadata. This metadata is accessible via the Metadata Endpoint URL, which is composed of the OAuth server URL and the authentication type, such as https://server.com/instance/OAuthServer/Saml2-AzureAD. The next section provides information about configuring service provider metadata.

Configuring Metadata Options

The following is an example of configuring service provider metadata:

```
{
"Name": "Aras.OAuth.Server.Plugins.Saml2Authentication",
"Enabled": true,
   "Options": [{
      "AuthenticationType": "<AuthenticationType>",
      "DisplayName": "<DisplayName>",
      "ServiceProviderOptions": {
         "EntityId": "<ServiceProviderEntityId>",
"Metadata": {
   "CacheDuration": "01:00:00",
   "WantAssertionsSigned": true,
   "Organization": {
      "Names": [
         "Aras Corp"
      ],
      "DisplayNames": [
         "Aras"
      ],
               "Urls": [
                  "https://www.aras.com"
               ],
               "Language": "en"
            },
            "Contacts": [
               {
                  "Type": "Support",
                  "Company": "Aras Corp",
                  "GivenName": "John",
                  "Surname": "Smith",
                  "PhoneNumbers": [
                     "978-806-9400"
                  ],
                  "Emails": [
                     "info@aras.com"
                  ]
               }
            ]
}
         },
      "IdentityProviderOptions": {
         "EntityId": "http://idp.example.com"
      }
   }]
}
```

This configuration example specifies the following parameters:

- **ServiceProviderOptions:** The options for configuring the service provider.
- **Metadata:** The configuration of service provider metadata.

1. **Important**

All Metadata configuration properties are optional.

- **CacheDuration:** The time interval during which anyone should cache the metadata presented by the service provider before trying to fetch a new copy (the default is one hour, 01:00:00).
- **WantAssertionsSigned:** The value (true or false) indicating whether the service provider wants assertions provided by the identity provider signed (the default is true).
- **Organization:** The basic information about an organization responsible for a SAML entity.
- **Names:** One or more language-qualified names that may or may not be suitable for human consumption (required if the Organization is configured; at least one item is required).
- **DisplayNames:** One or more language-qualified names suitable for human consumption (required if the Organization is configured; at least one item is required).
- **URLs:** One or more language-qualified URLs that specify a location to direct a user to additional information. The language qualifier refers to the material's content at the specified location (required if the Organization is configured; at least one item is required).
- **Language**: The language **Tag** in the xml:lang XML attribute for all Names, DisplayNames, and URLs (the default language is English, en language **Tag**).

1. **Important**

   Examples of language **Tags** are ja (Japanese), de (German), and fr (French). The **Tags** for Identifying Languages specification has more information at https://tools.ietf.org/html/rfc5646.

- **Contacts:** The basic contact information for a person responsible for a SAML entity.
- **Type:** The type of contact (the default is Unspecified). Other possible values are Technical, Support, Administrative, Billing, and Other.
- **Company:** The name of the company for the contact person.
- **GivenName:** The first name of the contact person.
- **Surname:** The surname of the contact person.
- **PhoneNumbers:** Zero or more string elements specifying a telephone number for the contact person.
- **Emails:** Zero or more string elements specifying the e-mail address of the contact person.

1. **Important**

All Contacts configuration properties are optional.

Loading Metadata to the Identity Provider

The service provider's metadata endpoint is inaccessible to the identity provider because it is located on localhost. In this case, service provider metadata (configured in the Configuring metadata options section) can be downloaded from the Metadata Endpoint URL, saved as an XML file, and imported to the identity provider's side.

If the service provider's metadata endpoint URL is accessible from the identity provider's side, the URL can be configured in an identity provider management system.

The base plugin configuration is completed after the service provider metadata is loaded in the identity provider.