Configuring Identity Provider Metadata

To use SAML 2.0 authentication, the service provider should know all the relevant information for communication with the identity provider.

When the identity provider does not provide its metadata by URL to the EntityId property, the location for the metadata can be specified, or the metadata can be configured manually.

Configuring of Metadata Location

Metadata can be retrieved from the identity provider using a URL or an XML file.

The following example shows the configuration of the SAML 2.0 plugin:

```
{
"Name": "Aras.OAuth.Server.Plugins.Saml2Authentication",
"Enabled": true,
   "Options": [{
      "AuthenticationType": "<AuthenticationType>",
      "DisplayName": "<DisplayName>",
      "ServiceProviderOptions": {
         "EntityId": "<ServiceProviderEntityId>"
            },
      "IdentityProviderOptions": {
         "EntityId": "https://idp.example.com",
"MetadataSource": "MetadataLocation",
         "MetadataLocation": "https://idp.com/metadata"
      }
   }]
}
```

This configuration example specifies the following parameters:

- **IdentityProviderOptions:** The options for configuring the identity provider.
- **EntityId:** The unique identifier of the identity provider (required). It must be the same as the identifier in the metadata.
- **MetadataSource:** The type of source from which metadata will be loaded.
- **MetadataLocation:** The location from which metadata will be loaded (required when MetadataSource has MetadataLocation value). It can be a URL, an absolute path to a local file, or an app-relative path.

Configuring Metadata Manually

The SAML 2.0 authentication plugin enables specifying metadata options for the identity provider, if necessary.

The following is an example of a SAML 2.0 plugin configuration with identity provider metadata options:

```
{
"Name": "Aras.OAuth.Server.Plugins.Saml2Authentication",
"Enabled": true,
   "Options": [{
      "AuthenticationType": "<AuthenticationType>",
      "DisplayName": "<DisplayName>",
      "ServiceProviderOptions": {
         "EntityId": "<ServiceProviderEntityId>"
         },
      "IdentityProviderOptions": {
         "EntityId": "https://idp.example.com",
"MetadataSource": "MetadataOptions",
            "Metadata": {
"SingleSignOnService": {
                  "Location": "https://idp.example.com/sso",
                  "Binding": "HttpRedirect"
               },
               "ArtifactResolutionServices": [
                  {
                     "Index": "0",
                     "Location": "https://idp.example.com/ars"
                  }
               ],
               "WantAuthnRequestsSigned": false,
               "SigningCertificate": {
                  "SourceType": "File",
                  "FilePath": ".\\secure_files\\SigningCertificate.cer"
               }
}
      }
   }]
}
```

This configuration example specifies the following parameters:

- **IdentityProviderOptions:** The options for configuring the identity provider (optional, like all child properties).
- **MetadataSource:** The source type from which metadata is loaded.
- **Metadata:** The configuration of the identity provider metadata (required if the MetadataSource has a MetadataOptions value).

- **SingleSignOnService:** Describes the authentication request protocol endpoint to which the user agent delivers the authentication request message or **Artifact** representing it (required if Metadata is configured).
- **Location:** The URL where the identity provider listens for incoming sign-on requests (required if **SingleSignOnService** is configured). The URL must be written in a way that the client understands since the client's web browser will be redirected to the URL. Specifically, this means that using a host name-only URL or a host name that only resolves on the server's network will not work.
- **Binding:** The SAML binding supported by the endpoint (defaults to HttpRedirect). Other possible values are HttpPost and Artifact.

1. **Important**

   Single sign out (SingleLogoutService in terms of SAML 2.0 specification) is currently not supported.

- **ArtifactResolutionServices**: Zero or more elements that describe indexed endpoints used for dereferencing a SAML **Artifact** into a corresponding protocol message.
- **Index:** The non-negative integer that is used to distinguish the possible endpoints.
- **Location:** The URL to which a requester, having received an **Artifact**, sends a request for **Artifact** resolution (required if ArtifactResolutionServices is configured).
- **WantAuthnRequestsSigned:** A value (true or false) that indicates whether the identity provider wants the authentication request messages to be signed (default is false to support authentication flow without certificates).

1. **Important**

   The WantAuthnRequestsSigned value is used together with the ServiceProviderOptions. The SigningBehavior option is only considered if SigningBehavior has IfIdpWantAuthnRequestsSigned or Always values.

- **SigningCertificate:** The identity provider's certificate to sign its messages. Refer to the identity provider certificate configuration description in the Configuring Identity Provider Metadata section.