

How to add the OpenAthens federation to common SP software

If you are already using or are planning on using other SP software within the OpenAthens federation, you will need to make it aware of the OpenAthens federation metadata. Since terminology can sometimes vary, this page will show the federation specific settings for some common SAML SP software; for up-to-date installation help you should refer to the documentation and provider of that software.

First create the application record in the OpenAthens federation.

- [Shibboleth](#)
- [SimpleSAMLphp](#)

Shibboleth

Update your shibboleth2.xml file with a metadata provider:

```
<MetadataProvider type="XML" uri="http://fed.openathens.net/oafed/metadata"
  backingFilePath="oafed-metadata.xml" reloadInterval="7200">
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
  <MetadataFilter type="Signature" certificate="oafed-certificate.pem"/>
</MetadataProvider>
```

Where oafed-certificate.pem is the x509 certificate from our metadata, saved in the same folder as your shibboleth2.xml file.

OA fed metadata x509 certificate

```
-----BEGIN CERTIFICATE-----
MIIDqDCCApCgAwIBAgIETwsgCzANBgkqhkiG9w0BAQUFADBEMRAwDgYDVQQKEwdFZHVzZXJ2MRMw
EQYDVQQLLEwpPcGVuQXRoZW5zMRswGQYDVQQDEXJmZWQub3BlbmF0aGVucy5uZXQwHhcNMTIwMTA5
MTcxNTM2WhcNMjIwMTA5MTcxNTM2WjBEMRAwDgYDVQQKEwdFZHVzZXJ2MRMwEQYDVQQLLEwpPcGVu
QXRoZW5zMRswGQYDVQQDEXJmZWQub3BlbmF0aGVucy5uZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQQdk0ZtlaKS6dzJWudKiKqFvDuMiIjryNjP2wKd1GvJ2WfA4HeN407rXvp0Bwt3
xzDblJs740UfC9nAQspLN/OpxNgcfIN29ZDbM3/7DThRqfGgMIJ1Z5CoD46jbJNKhmZigg6JD5tZ
RBvQNIJ02kFj6xLgNRlmiCnOc8yMCbVSWHmf16TvwZN5j8F8JZj1Iz6b0BC5NTk480doS/ha0uR
2mVIw7edhhPGZ9MIrnvwXRqgLERZg8C/SPhWy9UF4Ck5Mn4gJi/0BluweVa4xhDBvMeflGwdJi0R
KSCsc3W9HVYCq2A4gqOsthL6GfiZoDBDbIFK+hvhSBk6iTT3rt7fAgMBAAGjgaEwgZ4wHQYDVDR00
BBYEFGoS69KyhWRw9zwgfNmhwpGrKiAFMAwGAlUdEwQFMAMBAf8wbwYDVR0jBGgwZoAUY6zr0rKF
ZHD3PCB82aGnAasqIAWhSKRGMEQxEDA0BgNVBAoTB0VkdXNlcnYxZzARBgNVBAStCk9wZW5BdGhl
bnMxGzAZBgNVBAMTEmZlZC5vcGVuYXRoZW5zLm5ldiIETwsgCzANBgkqhkiG9w0BAQUFAAOCAQEA
4cQSjMp8mre2mX7XRtssesHyr3a3s5J6k/KJDPDCw0mZ+8HUECHshqMt6Mr5goCeV1OdQct9Qd2Y
CT+yEKZGz4Z7Q0mdT4sSiRVMRygA/AISlp+zq6dYwPHGJCoJEji/oJFDLvlWI911Z8hlh0HwKD0Q
UqM8HmkrG2cW4qVtCqQGfBPEW61JoppkG6GvTvbskK8fWldYcwjppZ4ZoxoUuG233sNuZMH2B3kp
IrvoyVPPqfBYMXqAmp206OUTlgULGHc2buJefPhWnazSMq0nE5vhMyAXzmqEACGwdsi9gKc04zQG
oofiTt08kAT9QpJU41DsLUmUKhtoY2djbQxRtQ=
-----END CERTIFICATE-----
```

SimpleSAMLphp

You will need a signing certificate. Create one in the cert directory:

```
cd cert
openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pem
```

Refer to it in your authsources.php file:

```
'default-sp' => array(
  'saml:SP',
  'privatekey' => 'saml.pem',
  'certificate' => 'saml.crt',
),
```

Enable the metadata and cron modules:

```
touch modules/metarefresh/enable
cp modules/metarefresh/config-templates/*.php config/
touch modules/cron/enable
cp modules/cron/config-templates/*.php config/
```

Create a directory to cache the metadata:

```
mkdir metadata/openathens
chmod go+rw metadata/openathens
```

Edit config/metadatarerefresh.php:

```
<?php
$config = array(
    'sets' => array(
        'uk' => array(
            'cron'      => array('hourly'),
            'sources'   => array(
                array(
                    'src' => 'https://fed.openathens.net/oafed/metadata',
                    'validateFingerprint' => '49:EC:EB:FE:CA:2F:F8:A7:74:48:2D:EB:81:9A:5A:0A:B4:02:ED:91',
                ),
            ),
            'expireAfter'      => 60*60*24*1, // Maximum 1 days cache time.
            'outputDir'       => 'metadata/openathens/',
            'outputFormat'    => 'serialize',
        ),
    ),
);
```

Finally set the cache to be a metadata source in config.php:

```
'metadata.sources' => array(
    array('type' => 'flatfile'),
    array('type' => 'serialize', 'directory' => 'metadata/openathens'),
),
```

You will also need to upload your SP metadata in the publisher dashboard when you register your app. Get it from the federation tab on the simpleSAMLphp front page. If you encounter metadata loading issues you may need to increase the `memory_limit` and `max_execution_time` in your php configuration file.