

Install OpenAthens SP on Apache

Prerequisites

- Application running under Apache on a Linux server in the Red Hat family - e.g. RHEL, CentOS.
- Server time synchronised by NTP or similar
- Familiarity with your chosen platform.
- Access to the [publisher dashboard](#).

Method

1. Add the OpenAthens repo to the `/etc/yum.repos.d/` directory with a `.repo` extension, e.g: `openathens.repo`.

```
[openathens-sp]
name = yum repository for athens rpms
baseurl = https://username:password@repo.openathens.net/yum/pkgs/rhel$releasever/sp/2.2/$basearch
enabled = 1
gpgcheck = 0
failovermethod = priority
```

For details see: [Configuring Yum for OpenAthens SP](#)

2. Install OpenAthens SP

```
sudo yum install openathens-sp
```

For details see: [Installing OpenAthens SP on Apache in detail](#)

3. Generate or install a metadata signing certificate - most federations allow these to be self-signed and last several years. Run the script in the `/usr/share/atacama-platform/keys` folder, or insert an existing `.pem` file in that folder containing both private and public keys.

```
sudo ./gen_self_signed_cert.sh 'yourdomain.com' 'Short Description'
```

For details see: [Install metadata signing certificates on Apache](#)

4. If you have not already done so, [create an application in the publisher dashboard](#). You will have the opportunity to paste in the signing certificate you generated in the previous step when you set it up.
 - a. If this is for an existing application, go to the connection for that application and add it in the SAML connector section.
5. Configure the vhost - the publisher dashboard will have generated some web-server configuration to copy and paste. Add it with a `.conf` extension in the `/etc/httpd/conf.d/` directory. In the file you must also:
 - a. Update the SSL certificate and key references to the relevant locations.
 - b. Update the protected location to cover your application.

Finally restart Apache to download the configuration from the publisher dashboard and start using it.

For details see: [Configuring Apache vhosts for OpenAthens SP](#)

Configure your application

See [OpenAthens SP common](#)

Advanced

You can optionally further restrict access in the vhost before passing the user to your application should you need or wish to. See: [Restricting access via vhost](#).