Single-sign-on (SSO) authentication is now required more than ever. Nowadays, almost every website requires some form of authentication to access its features and content. With the number of websites and services rising, a centralized login system has become a necessity. This guideline explaining how SSO authentication is implemented for the web and provide a working example using Apache server with mod_mellon(for apache).

Main goal to provide access to application on port 80 to customer with authorization through idP.

Requirements:

I) CentOS 7 64-bit
  Docker container with application on localhost port 80
  SSL certificate generated.
II) Console configuration:

Commands for apache:

```
sudo systemctl restart httpd
sudo systemctl stop httpd
sudo systemctl start httpd
```

logs - /var/log/httpd

1) Versions of installed packages:

```
rpm -qa | grep httpd
httpd-tools-2.4.6-40.el7.centos.4.x86_64
httpd-2.4.6-40.el7.centos.4.x86_64
rpm -qa | grep mellon
mod_auth_mellon-0.11.0-1.el7.x86_64
yum install httpd mod_ssl
yum install mod_auth_mellon.x86_64
vim sudo /etc/httpd/httpd.conf
```

2) Apache config files:

2.1) Conf.d:

```
<VirtualHost *:443>
    ServerName projects.com
    SSLEngine on
    ProxyRequests Off
    ProxyPreserveHost On
```

```
        <Proxy *>
          AddDefaultCharset off
          Order deny,allow
          Allow from all
        </Proxy>
            SSLCertificateFile /etc/pki/tls/certs/tkmi-repl.projects.com.cer
        SSLCertificateKeyFile /etc/pki/tls/private/tkmi-repl.projects.com.key
            RequestHeader set X-Forwarded-Proto "https"
            RequestHeader set X-Forwarded-Port "443"
            #Proxy for mellon is disabled!!!
            ProxyPass /mellon/ !
            #Reverse proxy to application
        ProxyPass / http://localhost:80/
        ProxyPassReverse / http://localhost:80/

</VirtualHost>

<Location />
        Require all granted
        AuthType "Mellon"
        MellonEnable "auth"
        MellonSPMetadataFile /etc/httpd/mellon/https_questions.tkmi_repl.projects.com.xml
        MellonSPPrivateKeyFile
/etc/httpd/mellon/https_questions.tkmi_repl.projects.com.key
        MellonSPCertFile /etc/httpd/mellon/https_questions.tkmi_repl.projects.com.cert
        MellonIdPMetadataFile /etc/httpd/mellon/MetadataFile.xml
        MellonIdPCAFile /etc/httpd/mellon/ADFS_Cert_base64.cer
        MellonPostReplay On
        MellonCookiePath /
        MellonSecureCookie Off
        MellonEndpointPath /mellon
        MellonVariable "sso-cookie"
        MellonUser "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"
        MellonSetEnv "upn" "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"
        #set available field in request
        RequestHeader unset LOGON_USER
        RequestHeader set LOGON_USER "%{MELLON_upn}e" env=MELLON_upn
</Location>

Listen 443
```

2.2) Conf.ssl

```
sudo vim /etc/httpd/conf.d/ssl.conf
```

#For disabling SSLv3 proto

```
SSLProtocol All -SSLv2 -SSLv3
```

#Listen 443 https

```
SSLCertificateFile /etc/pki/tls/certs/tkmi-repl.projects.com.cer
SSLCertificateKeyFile /etc/pki/tls/private/tkmi-repl.projects.com.key
```

3) Creating certificates for mellon:
/usr/libexec/mod_auth_mellon/mellon_create_metadata.sh https://projects.com https://projects.com/mellon

4) Ensure that NameID policy in Metadata.xml (mellon metadata file generated on step 4) set to unspecified:

```
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
```

5) Comment out SAML Redirect Binding metadata in Metadata.xml as follows:
Metadata.xml comment block

```
<!--SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="idP URL"/-->
```

II)

```
https://idpSite.com:44301/entries/view?id=https%3A%2F%2Fprojects.com&kind=Relying Party
```

Tab General:
Identifiers https://projects.com

Tab SAML-SECURITY (add mellon cert):

```
Signed SAML requests requiredNo
Signature algorithmSHA-1
Signing certificates
Subj: CN=projects.com, Valid: mm/dd/yyyy-mm/dd/yyyy
```

Tab SAML:
Assertion Consumer POST Yes 0 https://projects.com/mellon/postResponse