Authentication

- Auth BookStack on Lemonldap::NG

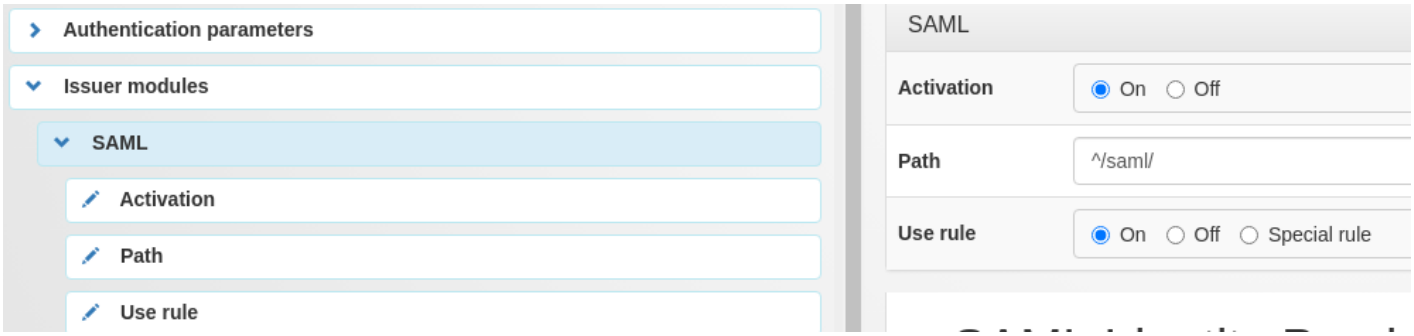
Auth BookStack on Lemonldap::NG

BookStack can use an SAML2 IDP to authenticate users. And Lemonldap::NG can be used as such, but there are a few things to configure to have this working.

In this example, Lemonldap::NG portal is https://auth.example.org and BookStack is https://bookstack.example.org

Enable SAML2 service on Lemonldap::NG

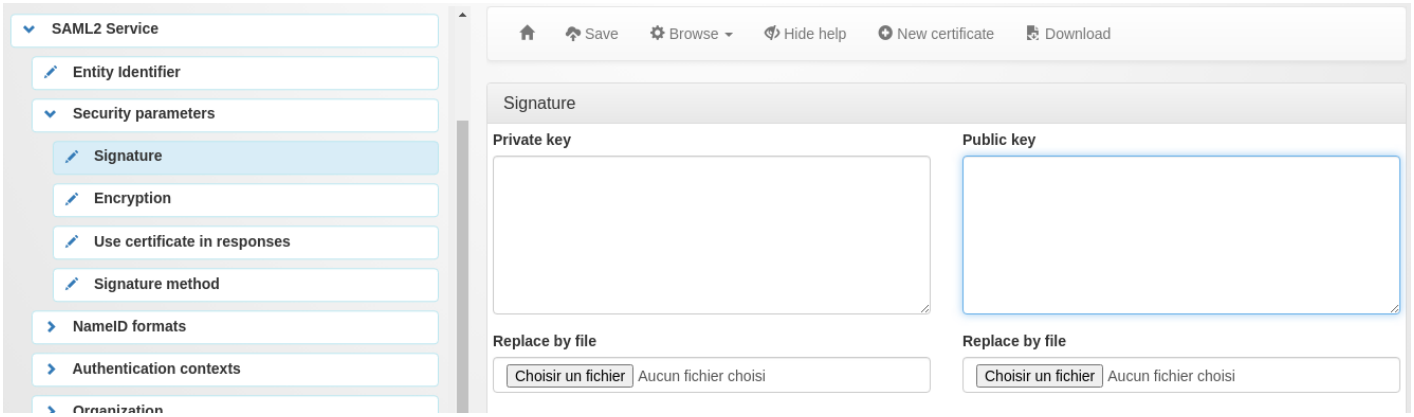
In the manager, the SAML issuer module must be enabled



Configure SAML2 on Lemonldap::NG

Now, you have to configure SAML2 service on Lemonldap::NG

Go in SAML2 Service in the manager, then Security -> Signature and create a new certificate



Do the same for encryption

There are a few other things you can configure here, like your organization display name, name and URL.

Check Lemonldap::NG is correctly configured

You can open https://auth.example.org/saml/metadata and you should see an XML document. With lots of informations, among which the public key of your IDP

```
<ds:X509Certificate>
  MIICpjCCAY6gAwIBAgIECcR3fjANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDDApz
  c28uZndzLmZyMB4XDTIxMDMxNzE2NDcwMVoXDTQxMDMxMjE2NDcwMVowFTETMBEG
  A1UEAwwKc3NvLmZ3cy5mcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
  ALM8ujG19hs9KBLb1Ct6IkpivmyjrnHsdl7kZCXhJwUEYzMDqT/3FiNEOgl9B/o6
  MHCgxvHZBJ7MhKEz1qrTD1xdhyCklGTg1vhNYfh7HmubJ5llQkUwmOykP+dM2Y3Y
  vFMpCKfsA38IT7u7EikGrDtul2xzc7BJAu6feCbu54h61OHTZhgPtgnfZ0GXMaAw
  urdh2dRhXdOHa+6HqIopUwDfwK4iRMIBkaPPpN32cpYNoLbw8n7lmHazobF6Ycbc
  psS2nx/a9jA051DLhmBDzQx8nlK3BwNz8P0tkre4jHlVA0Geeuc4kHqdahJWkGqp
  /eZcfxkH9mZOIZI8lhnx1tECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAJ12/WQmw
  3SBdEuPgYQoe9O219hiCMRf12Y+SLCTy7atou9yLF+A6LcMH1Xe2sZPlOhNXATI3
  usUhCBaV3eRTz7Wo2lTxaoiavq11Q0HJVuCzMiuheafPG5mTUBjJOo/Ntq94Z28k
  bTrNPROpC8NDNq0bvl5t2ujCHrXxKoCG5VYg9cDNv3X9frtlQmCqxahVZcrIv8zc
  M7qA2E6qrKCG4p7jpv24Qxyy+VLDEY34/vce5ztzwfrk3vEXCQCMOW08RE3ouz1c
  TtxJwd1oSmD+IpdAFcGh4eENsf4AJd9gU9EbsEsZFYY9s6vkb3Plv/2FGFaM1ArL
  sIdSKR5JcHXQHw==
</ds:X509Certificate>
```

Write it somewhere, you'll need it later

Configure BookStack to use SAML2 auth

In your .env configuration for BookStack, add the following lines :

```
AUTH_METHOD="saml2"
# The name of the auth displayed on the login page
SAML2_NAME="FWS"
# The attribute which will be used for the displayname
SAML2_DISPLAY_NAME_ATTRIBUTES="cn"
# The attribute which will be used as identifier to link your LL::NG user with your BookStack
user
# can be uid, or here, I user principal as LL::NG is using a samba4 directory
SAML2_EXTERNAL_ID_ATTRIBUTE="principal"
SAML2_IDP_ENTITYID="https://auth.example.org/saml/metadata"
# Note : BookStack has a buggy SLO support. So we disable metadata fetching
```

```
# this way we can configure single sign on, but leave single sign out disabled
SAML2_AUTOLOAD_METADATA="false"
# This is the URL for the Single Sign On
SAML2_IDP_SSO="https://auth.example.org/saml/singleSignOn"
# This is the public key you got earlier. Just remove the spaces and cariage return
SAML2_IDP_x509="MIICpjCCAY6gAwIBAgIECcR3fjANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDDApzc28uZndzLmZyMB4
# You can omit the last 3 param if you don't want to MAP your groups from LL::NG to roles on
BookStack
SAML2_USER_TO_GROUPS="true"
SAML2_GROUP_ATTRIBUTE="groups"
SAML2_REMOVE_FROM_GROUPS="true"
```

Create a SP for BookStack on LemonIdap::NG

Now, you have to create a new SP on LemonIdap::NG for BookStack. In your manager, go in SAML Service Providers -> Add SAML SP and name it bookstack (or whatever you want)

Then, in Metadata, put the content your can get when you open https://bookstack.example.org/saml2/metadata

It should looks like

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2021-03-
19T17:03:25Z" cacheDuration="PT604800S" entityID="https://docs.example.org/saml2/metadata">
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://docs.example.org/saml2/sls"/>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://docs.example.org/saml2/acs" index="1"/>
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

In Exported attributes, add the attributes you want to send. In our case, we want to use cn, groups and principal, so lets add them :

There's still some things to configure, in Options -> Signature, disable **Check SSO message signature** and **Check SLO message signature** (this is needed because BookStack doesn't sign outgoing messages)

Last, in **Options -> Security -> Access rule** you can add a rule to limit which users can login to BookStack, eg

```
inGroup('Role_Infra_Admin') or inGroup('Tech') or inGroup('Equipe')
```

Add group mapping to BookStack database

You should be ready to go. Or nearly. The last thing is that you might want to setup mapping between your LDAP groups (well, groups from LL::NG, they will most of the time be coming from an LDAP server) and your BookStack group.

Say you want member of your LDAP group Role_Infra_Admin to be Admin in BookStack. Just set it like this

```
update roles set external_auth_id='Role_Infra_Admin'  where display_name='Admin';
```

For the other mappings, you can configure them from BookStack interface once you've logged in with an admin account