

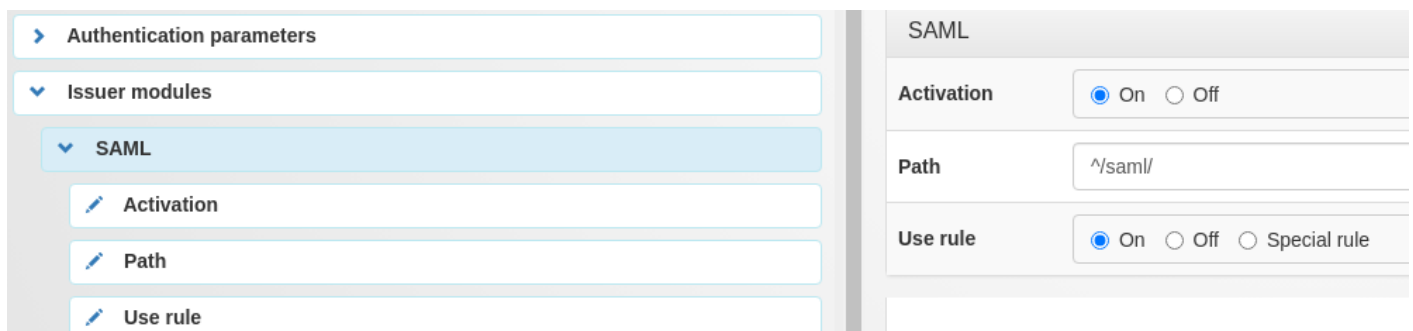
BookStack auth on Lemonldap::NG (using SAML)

[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



The screenshot shows the Lemonldap::NG manager interface. On the left, a sidebar menu has 'Authentication parameters' expanded, showing 'Issuer modules' and 'SAML'. The 'SAML' module is selected. On the right, the 'SAML' configuration panel is visible. It has three sections: 'Activation' with a radio button set to 'On'; 'Path' with a text input field containing '^/saml/'; and 'Use rule' with radio buttons set to 'On'.

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
  A1UEAwKc3NvLmZ3cy5mcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
  ALM8ujG19hs9KBLb1Ct6IkpivmyjrnHsd17kZCXhJwUEYzMDqT/3FiNE0gl9B/o6
  MHCgxvHZBJ7MhKz1qrTD1xdhyCklGTg1vhNYfh7HmubJ5llQkUwm0ykP+dM2Y3Y
  vFMpCKfsA38IT7u7EikGrDtu12xzc7BJAu6feCbu54h610HTZhgPtgnfZ0GXMaAw
  urdh2dRhXd0Ha+6HqIopUwDfwK4iRMIBkaPPpN32cpYNoLbw8n7lmHazobF6Ycbc
  psS2nx/a9jA051DLhmbDzQx8nLK3BwNz8P0tkre4jHlVA0Geeuc4kHqdahJWkGqp
  /eZcfxkH9mZ0IZI8lhnx1tECAwEAATANBgkqhkiG9w0BAQsFAA0CAQEAJ12/WQmw
  3SBdEuPgYQoe90219hiCMRf12Y+SLCTy7atou9yLF+A6LcMH1Xe2sZPl0hNXATI3
  usUhCBaV3eRTz7Wo2lTxaovq11Q0HJVuZCzMiueafPG5mTUBjJ0o/Ntq94Z28k
  bTrNPR0pC8NDNq0bvl5t2ujCHRxxKoCG5VYg9cDNv3X9frt1QmCqxahVZcrIv8zc
  M7qA2E6qrKCG4p7jpv24Qxyy+VLDEY34/vce5ztzwrk3vEXCQCM0W08RE3ouz1c
  TtxJwd1oSmD+IpdAFcGh4eENsf4AJd9gU9EbsEsZFYY9s6vkb3Plv/2FGFaM1ArL
  sIdSKR5JcHXQHw==
</ds:X509Certificate>
```

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="Lapiole"

# 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 carriage returns
SAML2_IDP_x509="MIICPjCCAY6gAwIBAgIECcR3fjANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQDDApzc28uZndzLmZyMB
4XDTIxMDMxNzE2NDcwMVVoXDTQxMDMxMjE2NDcwMVowFTETMBEGA1UEAwKc3NvLmZ3cy5mcjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALM8ujG19hs9KBLb1Ct6IkpivmyjrnHsd17kZCXhJwUEYzMDqT/3FiNE0gl9B/o6MHCgxvHZBJ
7MhKEz1qrTD1xdhyCklGTg1vhNYfh7HmubJ5llQkUwm0ykP+dM2Y3YvFmPCKfsA38IT7u7EikGrDtul2xzc7BJAu6feCbu
54h610HTZhgPtgnfZ0GXMaAwurdh2dRhXd0Ha+6HqIopUwDfwK4iRMIBkaPPpN32cpYNoLbw8n7lmHazobF6YcbcpsS2nx
/a9jA051DLhmBDzQx8nlK3BwNz8P0tkre4jHlVA0Geeuc4kHqdahJWkGqp/eZcfxkH9mZ0IZI8lhnX1tECAwEAATANBgkq
hkiG9w0BAQsFAA0CAQEAAJ12/WQmw3SBdEuPgYQoe90219hiCMRf12Y+SLCTy7atou9yLF+A6LcMH1Xe2sZPl0hNXATI3us
UhCBaV3eRTz7Wo2lTxaoiavq1lQ0HJVuZcMiuheafPG5mTUBjJ0o/Ntq94Z28kbTrNPR0pC8NDNq0bv15t2ujChRxxKoCG
5VYg9cDNv3X9frtlQmCqxahVZcrIv8zcM7qA2E6qrKCG4p7jpv24Qxyy+VLDEY34/vce5ztzwfrk3vEXCQCM0W08RE3ouz
1cTtxJwd1oSmD+IpdAFcGh4eENsf4AJd9gU9EbsEsZFY9s6vkb3Plv/2FGFaM1ArLsIdSKR5JcHXQHw=="

# 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 Lemonldap::NG

Now, you have to create a new SP on Lemonldap::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://example.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://example.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://example.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 :

| Exported attributes | | | |
|--|--|----------------------|---|
| Variable name | Attribute name | Friendly name | Mandatory |
| <input type="text" value="cn"/> | <input type="text" value="cn"/> | <input type="text"/> | <input type="radio"/> On <input checked="" type="radio"/> Off |
| <input type="text" value="groups"/> | <input type="text" value="groups"/> | <input type="text"/> | <input type="radio"/> On <input checked="" type="radio"/> Off |
| <input type="text" value="principal"/> | <input type="text" value="principal"/> | <input type="text"/> | <input type="radio"/> On <input checked="" type="radio"/> Off |

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

Révision #3

Créé 6 novembre 2024 09:40:45 par Daniel Berteaud

Mis à jour 1 juin 2025 21:52:01 par Daniel Berteaud