Connecting Gitlab to eduTEAMS

This guide describes how Gitlab CE v13.x can be configured as a SAML Service Provider for eduTEAMS. The integration via SAML provides more benefits than the integration via OIDC, as the OIDC implementation in Gitlab has (limited) support for authorizing users using groups. The OIDC implementation in Gitlab supports only authenticating users.

1. In order to set up a basic configuration, which would allow all users from your VO to authenticate via eduTEAMS and access the Gitlab service, you should edit the *omniauth* section **/etc/gitlab/gitlab.rb** config file.

NOTE: The "STEP nnn" comments refer directly to the OmniAuth guide https://docs.gitlab.com/13.0/ee/integration/saml.html.

/etc/gitlab/gitlab.rb

```
# STEP 3
gitlab_rails['omniauth_enabled'] = true
gitlab_rails['omniauth_allow_single_sign_on'] = ['saml']
gitlab_rails['omniauth_block_auto_created_users'] = false

# STEP 4
gitlab_rails['omniauth_auto_link_saml_user'] = true

# STEP 6
gitlab_rails['omniauth_providers'] = [
   {
      name: 'saml',
      label: 'eduTEAMS',
      args: {
         attribute_service_name: "eduTEAMS Test Gitlab",
         assertion_consumer_service_url: 'https://gitlab.example.com/users
/auth/saml/callback',
         idp_cert_fingerprint: '72:8A:6C:6B:63:35:3F:E0:BF:70:8D:41:0E:B7:
02:CF:C5:86:53:24',
         idp_sso_target_url: 'https://proxy.eduteams.org/saml2sp/sso
/redirect',
         issuer: 'https://gitlab.example.com',
         name_identifier_format: 'urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent',
         uid_attribute: 'urn:oid:1.3.6.1.4.1.5923.1.1.1.13',

             request_attributes: [
                 {
                         name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                         name: "urn:oid:0.9.2342.19200300.100.1.3",
                             is_required: "true",
                             friendly_name: "mail"
                  },
                      {
                             name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                         name: "urn:oid:2.5.4.3",
                             is_required: "true",
                             friendly_name: "cn"
                      },
                      {
                             name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                         name: "urn:oid:2.5.4.42",
                             is_required: "true",
                             friendly_name: "givenName"
                      },
                      {
                             name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                         name: "urn:oid:2.5.4.4",
                             is_required: "true",
                             friendly_name: "sn"
                      },
                      {
                             name_format: "urn:oasis:names:tc:SAML:2.0:
```

```
attrname-format:uri",
                            name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.7",
                                is_required: "true",
                                friendly_name: "eduPersonEntitlement"
                        },
                        {
                                name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                            name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.13",
                                is_required: "true",
                                friendly_name: "eduPersonUniqueId"
                        },
                {
                                name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                            name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.6",
                                is_required: "true",
                                friendly_name: "eduPersonPrincipalName"
                        }
            ],
            attribute_statements: {
                name: ["urn:oid:2.5.4.3"],
                uid: ["urn:oid:1.3.6.1.4.1.5923.1.1.1.13"],
                nickname: ["urn:oid:1.3.6.1.4.1.5923.1.1.1.6"],
                email: ["urn:oid:0.9.2342.19200300.100.1.3"],
                first_name: ["urn:oid:2.5.4.42"],
                last_name: ["urn:oid:2.5.4.4"]
            },
            private_key: '-----BEGIN PRIVATE KEY-----
            ...
            -----END PRIVATE KEY-----'
            certificate: '-----BEGIN CERTIFICATE-----
            ...
            -----END CERTIFICATE-----'
            security: {
                authn_requests_signed: true,
                want_assertions_signed: false,
                want_assertions_encrypted: false,
                embed_sign: true,
                metadata_signed: false,
                signature_method: 'http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256',
                digest_method: 'http://www.w3.org/2001/04/xmlenc#sha256',
            }
        },
        groups_attribute: 'urn:oid:1.3.6.1.4.1.5923.1.1.1.7',
        required_groups: [],
        admin_groups: [],
        audit_groups: []
    }
]
```

2. In order to edit this part of the config file correctly, you should have the values for the configuration options defined and known.

Also you need to generate a private / public key pair that will be used by the SAML SP to digitally sign and optionally decrypt SAML Assertsions. You can generate a key pair with the following command from your terminal:

Configuration Option	Value	Description
attribute_service_name:	(example) eduTEAMS Test Gitlab	The name of your service. This name will be visible to the end users
assertion_consumer_service_url	(example)https://gitlab.example.com/users/auth/saml/callback	The HTTPS endpoint of your GitLab instance
idp_cert_fingerprint	72:8A:6C:6B:63:35:3F:E0:BF:70:8D:41:0E:B7:02:CF:C5:86:53:24	This is the SHA1 fingerprint of the signing certificate used by the eduTEAMS SAML frontend
idp_sso_target_url	https://proxy.eduteams.org/saml2sp/sso/redirect	This is the eduTEAMS endpoint supporting the HTTP-Redirect SAML 2.0 Binding

```
openssl req -x509 -nodes -
newkey rsa:2048 -keyout
/dev/stdout \
        -days 3650 -subj "
/CN=SAML Certificate"
```

Note: The private and the public key are going to be printed in the standard output.

issuer	(example) https://gitlab.example.com	A unique name identifying the gitlab application to the proxy. This should be changed to the toplevel domain of your Gitlab instance
name_identifier_format	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	The NameID format requested
uid_attribute	urn:oid:1.3.6.1.4.1.5923.1.1.1.13	By default Gitlab uses the NameID attribute as the unique identifier. With this configuration option we configure gitlab to use urn:oid:1.3.6.1.4.1.5923.1.1.1.13 (eduPersonUniqueId)
request_attributes		This option controls the SAML attributes that are going to be include in the SAML of metadata for Gitlab. The attributes required are: • mail • cn (Full name) • givenName (First name) • sn (Surname) • eduPersonEntitlement (the groups the user is assigned to) • eduPersonUniqueID (the unique identifier of the user) • eduPersonPrincipalName (the username of the user) For more information on the attributes that are available to services from eduTEAMS, you can read Attributes available to Relying Parties

```
[
{
  name_format: "urn:oasis:
names:tc:SAML:2.0:
attrname-format:uri",
  name: "urn:oid:
0.9.2342.19200300.100.1.3"
,
  is_required: "true",
  friendly_name: "mail"
},
{
  name_format: "urn:oasis:
names:tc:SAML:2.0:
attrname-format:uri",
  name: "urn:oid:2.5.4.3",
  is_required: "true",
  friendly_name: "cn"
},
{
  name_format: "urn:oasis:
names:tc:SAML:2.0:
attrname-format:uri",
  name: "urn:oid:
2.5.4.42",
  is_required: "true",
  friendly_name:
"givenName"
},
{
  name_format: "urn:oasis:
names:tc:SAML:2.0:
attrname-format:uri",
  name: "urn:oid:2.5.4.4",
  is_required: "true",
  friendly_name: "sn"
},
{
  name_format: "urn:oasis:
names:tc:SAML:2.0:
attrname-format:uri",
  name: "urn:oid:
1.3.6.1.4.1.5923.1.1.1.7",
  is_required: "true",
  friendly_name:
"eduPersonEntitlement"
},
{
  name_format: "urn:oasis:
names:tc:SAML:2.0:
attrname-format:uri",
  name: "urn:oid:
1.3.6.1.4.1.5923.1.1.1.13"
,
  is_required: "true",
  friendly_name:
"eduPersonUniqueId"
},
{
  name_format: "urn:oasis:
names:tc:SAML:2.0:
attrname-format:uri",
  name: "urn:oid:
1.3.6.1.4.1.5923.1.1.1.6",
  is_required: "true",
  friendly_name:
"eduPersonPrincipalName"
}
]
```

attribute_statements	<pre>{
	  name: ["urn:oid:
	2.5.4.3"],
	  uid: ["urn:oid:
	1.3.6.1.4.1.5923.1.1.1.13"
	],
	  nickname: ["urn:oid:
	1.3.6.1.4.1.5923.1.1.1.6"]
	,
	  email: ["urn:oid:
	0.9.2342.19200300.100.1.3"
	],
	  first_name: ["urn:oid:
	2.5.4.42"],
	  last_name: ["urn:oid:
	2.5.4.4"]
	},</pre>
		This configure options controls the mapping from the SAML attributes to the Gitlab internal attributes

private_key	<pre>-----BEGIN PRIVATE
	KEY-----
	
	...
	
	-----END PRIVATE KEY-----</pre>
		This is the private key that is going to be used to sign the and optionally decrypt encrypted SAML assertions.
		
		Copy the private key that you generated in your terminal

certificate	<pre>-----BEGIN
	CERTIFICATE-----
	
	...
	
	-----END CERTIFICATE-----</pre>
		This is the certificate that is going to be used to sign the and optionally decrypt encrypted SAML assertions.
		
		Copy the certificate that you generated in your terminal

security	<pre>{
	  authn_requests_signed:
	true,
	  want_assertions_signed:
	false,
	
	want_assertions_encrypted:
	false,
	  embed_sign: true,
	  metadata_signed: false,
	  signature_method:
	'http://www.w3.org/2001/04
	/xmldsig-more#rsa-sha256',
	  digest_method:
	'http://www.w3.org/2001/04
	/xmlenc#sha256',
	}</pre>
		This configuration option controls several aspects of the security configuration for the SP

Full group definition: urn:geant:eduteams.org:service:eduteams:group:<VO_Name>:<Top_level group>[:<Sub_group_name>]#eduteams.org	(examples) urn:geant:eduteams.org:service:eduteams:group:Test_VO:Developers#eduteams.org urn:geant:eduteams.org:service:eduteams:group:Test_VO:Admins:Gitlab#eduteams.org urn:geant:eduteams.org:service:eduteams:group:Test_VO:Admin:Gitlab:Auditors#eduteams.org	You should replace the <VO_Name> with your VO name to which you would like to connect the Gitlab service; You should replace the <Top_level group>:[<Sub_group_name>] with your group (and subgroup) name which should have access to the Gitlab service;

CONFIGURE GROUPS

The SAML login in Gitlab includes support for limiting access to specific groups from your VO and authorizing users using these groups. There are four groups types that can be configured: *required*, *admin*, *audit* and *external*.

1. In order to add to a basic configuration, which would allow all users from your VO to authenticate via eduTEAMS and access the Gitlab service, you should edit the *omniauth* section **/etc/gitlab/gitlab.rb** config file, after the `groups_attribute` section.

- You can control which groups can access the Gitlab instance using the `required_groups` configuration option. When `required_groups` is not set or it is empty, anyone with proper authentication will be able to use the service.
- You can control if a user should be assigned the *admin* role, using the `admin_groups` configuration option.
- You can control if a user should be assigned the *auditor* role, using the `audit_groups` configuration option.
- You can control if a user should be marked as *external*, using the `external_groups` configuration option.

/etc/gitlab/gitlab.rb

```
 # STEP 3
gitlab_rails['omniauth_enabled'] = true
gitlab_rails['omniauth_allow_single_sign_on'] = ['saml']
gitlab_rails['omniauth_block_auto_created_users'] = false

# STEP 4
gitlab_rails['omniauth_auto_link_saml_user'] = true

# STEP 6
gitlab_rails['omniauth_providers'] = [
   {
      name: 'saml',
      label: 'eduTEAMS',
      args: {
         attribute_service_name: "eduTEAMS Test Gitlab",
         assertion_consumer_service_url: 'https://gitlab.example.com/users
/auth/saml/callback',
         idp_cert_fingerprint: '72:8A:6C:6B:63:35:3F:E0:BF:70:8D:41:0E:B7:
02:CF:C5:86:53:24',
         idp_sso_target_url: 'https://proxy.eduteams.org/saml2sp/sso
/redirect',
         issuer: 'https://gitlab.example.com',
         name_identifier_format: 'urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent',
         uid_attribute: 'urn:oid:1.3.6.1.4.1.5923.1.1.1.13',

             request_attributes: [
                 {
                         name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                         name: "urn:oid:0.9.2342.19200300.100.1.3",
                             is_required: "true",
                             friendly_name: "mail"
                  },
                      {
                             name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                         name: "urn:oid:2.5.4.3",
                             is_required: "true",
                             friendly_name: "cn"
                      },
                      {
                             name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                         name: "urn:oid:2.5.4.42",
                             is_required: "true",
                             friendly_name: "givenName"
                      },
                      {
                             name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
```

```
                        name: "urn:oid:2.5.4.4",
                            is_required: "true",
                            friendly_name: "sn"
                    },
                    {
                            name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                        name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.7",
                            is_required: "true",
                            friendly_name: "eduPersonEntitlement"
                    },
                    {
                            name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                        name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.13",
                            is_required: "true",
                            friendly_name: "eduPersonUniqueId"
                    },
            {
                            name_format: "urn:oasis:names:tc:SAML:2.0:
attrname-format:uri",
                        name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.6",
                            is_required: "true",
                            friendly_name: "eduPersonPrincipalName"
                    }
          ],
          attribute_statements: {
              name: ["urn:oid:2.5.4.3"],
              uid: ["urn:oid:1.3.6.1.4.1.5923.1.1.1.13"],
              nickname: ["urn:oid:1.3.6.1.4.1.5923.1.1.1.6"],
              email: ["urn:oid:0.9.2342.19200300.100.1.3"],
              first_name: ["urn:oid:2.5.4.42"],
              last_name: ["urn:oid:2.5.4.4"]
          },
          private_key: '-----BEGIN PRIVATE KEY-----
          ...
          -----END PRIVATE KEY-----'
          certificate: '-----BEGIN CERTIFICATE-----
          ...
          -----END CERTIFICATE-----'
          security: {
              authn_requests_signed: true,
              want_assertions_signed: false,
              want_assertions_encrypted: false,
              embed_sign: true,
              metadata_signed: false,
              signature_method: 'http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256',
              digest_method: 'http://www.w3.org/2001/04/xmlenc#sha256',
          }
      },

      # STEP(s) "Required Groups", "Admin Groups", "Auditor Groups"
      groups_attribute: 'urn:oid:1.3.6.1.4.1.5923.1.1.1.7',
      # Only the following groups in the Test_VO will be able to access
this Gitlab instance:
      #
      # - Developers
      # - Admins:Gitlab
      # - Admins:Gitlab:Auditors
      required_groups: [
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:
Developers#eduteams.org',
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:
Developers#eduteams.org',
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:Admins:
Gitlab#eduteams.org',
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:Admin:
Gitlab:Auditors#eduteams.org',
      ],
      # Users from the following groups in the Test_VO will access this
```

```
Gitlab instance as admins
      #
      # - Admins:Gitlab:
      admin_groups: [
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:Admins:
Gitlab#eduteams.org',
      ],
      # Users from the following groups in the Test_VO will access this
Gitlab instance as auditors:
      #
      # - Admins:Gitlab:Auditors
      audit_groups: [
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:Admins:
Gitlab:Auditors#eduteams.org',
      ],
      # Users from the following gorup in the Test_VO will access the
Gitlab instance external users
      #
      # - Guests
      # - Contractors
      external_groups: [
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:
Guests#eduteams.org',
          'urn:geant:eduteams.org:service:eduteams:group:Test_VO:
Conractors#eduteams.org',
      ],
      }
   }
]
```

2. Once you edited the *omniauth* section of the /etc/gitlab/gitlab.rb file as above indicated, you need to reconfigure gitlab with the command:

```
sudo gitlab-ctl reconfigure
```

3. You should be able to check the SAML metadata URL of the Gitlab instance at https://<gitlab.example.com>/users/auth/saml/metadata .

Gitlab SAML Metadata

```
<?xml version='1.0' encoding='UTF-8'?>
<md:EntityDescriptor ID="_44a6dfeb-7bc8-463c-8c4a-363bcdaebd8e" entityID="
https://gitlab.example.com" xmlns:md="urn:oasis:names:tc:SAML:2.0:
metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="
false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:
X509Certificate>MIICsjCCAZoCCQC+5DOdpjdhhDANBgkqhkiG9w0BAQsFADAbMRkwFwYDVQQ
DDBBTQU1MIENlcnRpZmljYXRlMB4XDTIwMTAwMzEyMzM1OVoXDTMwMTAwMTEyMzM1OVowGzEZMB
cGA1UEAwwQU0FNTCBDZXJ0aWZpY2F0ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA
Pn1WdKVdIxOAHNJWJgAxNldX3Vlrb0T18yXCRTiSZX2EDPFkVQDXFIi5NPVIgW3kxMyi28eR7kg
1KnpYcPT4cZbHBaTIliJOrpkvUlXKUFuIHZuRsaFoHv0kDY
/T3BUZul6jx6rnb8AgpHkBAeZludySwYzf5/DcqXaUVLekpZfUUEyrIe6dqFL
/ehGzSXtGl6hWn8ms5lEcmlZeG01l2F
/1FmpXaCwCSNo0QTIwAnlpZ6CvDsnZIzrOvvPOvKrgvmWKqU/vY5rB8eJSNodp6
/gi1+r5TUV95UHGmg3bIe0Flo/SrYYsp9vp
/f1IWlcaM7XjuvsGFMaj4CgVzCCRGsCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAASjSsy9Tltbf
bRvxp21mkxhj6LOx33yuYOmVODs170V+GeDId8bQTi+ddO+YmKHg18zzpz+EA69HVQozshtf7
/5gB8dS1zknvs78xbLevrBZ7Fw8h8Q68je+3MOV
/UYhHd1ViQ+S3Qdeph1RMwv7s9XsJGqCsxF5skrKef2VLqQAsKitNk0ao69H87aDrnSAb88v6kF
eT08MZWTnw64jYj8jH2gaT33WkiAtzVUNJygIrVuqWX9GCZsQK6AehFnSr
/jUUirSMms78rJM8JmPTygWrHveM8BC2QSsSyS9X4YEe/ah2YIfazioDUh8JRPgdbHMUdHwN
/4+heqP1JyirA==</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:
persistent</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:
bindings:HTTP-POST" Location="https://gitlab.example.com/users/auth/saml
/callback" index="0" isDefault="true" />
        <md:AttributeConsumingService index="1" isDefault="true">
            <md:ServiceName xml:lang="en">eduTEAMS Test Gitlab Instance<
/md:ServiceName>
            <md:RequestedAttribute FriendlyName="mail" Name="urn:oid:
0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" isRequired="true" />
            <md:RequestedAttribute FriendlyName="cn" Name="urn:oid:
2.5.4.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true" />
            <md:RequestedAttribute FriendlyName="givenName" Name="urn:oid:
2.5.4.42" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true" />
            <md:RequestedAttribute FriendlyName="sn" Name="urn:oid:
2.5.4.4" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true" />
            <md:RequestedAttribute FriendlyName="eduPersonEntitlement"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" NameFormat="urn:oasis:names:tc:
SAML:2.0:attrname-format:uri" isRequired="true" />
            <md:RequestedAttribute FriendlyName="eduPersonUniqueId" Name="
urn:oid:1.3.6.1.4.1.5923.1.1.1.13" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" isRequired="true" />
            <md:RequestedAttribute FriendlyName="eduPersonPrincipalName"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:
SAML:2.0:attrname-format:uri" isRequired="true" />
        </md:AttributeConsumingService>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

4. Congratulations, you have successfully configured your Gitlab instance for eduTEAMS. Now you can proceed to register your service following the steps described in Registering services on the eduTEAMS Service.