Hands-On Exercises

Enroll in Registry Using Federated Identity

Upload Your SSH Public Key

SSH Into the VM

Hands-on with SAML
  Hands-on with SAML: Advanced

Hands-on with OpenID Connect
  Hands-on with OpenID Connect: Advanced

Hands-on with Globus Auth
  Pre-baked application registration
  Register your own application
  Using Globus Auth with native application or thick-client
  Learn more about Globus

Hands-on with Federation
  Hands-On with Federation: Advanced

Hands-on with Participant Lifecycle Management
  Create COUs
  Organizational Identity
  CO Identity
  CO Groups
  Advanced: Edit Enrollment Flow
Enroll in Registry Using Federated Identity

Browse to https://registry.vo.idm.training/enroll/.

Choose your university or home organization login provider and authenticate. Google authentication is available if you cannot find your organization.

Complete the form with your name, email, and optionally your organization and then click the SUBMIT button.
Click on the link in the verification email to verify your email address and wait for your petition to be confirmed.
Welcome to COmanage Registry.
Upload Your SSH Public Key

Click LOGIN to login again. From the top right click on your name and select "My VO Training Identity".

In the "Identifiers" section note your assigned UID. This will be the login for the training virtual machine (VM).
Scroll down and next to 'SSH Keys' click the 'Add' button.

Use the "Browse" and "UPLOAD" buttons to upload your public SSH key. Do not cut and paste your key. It is faster, easier, and more reliable to browse, select the file, and then upload it. Ask your instructor if you do not know how to find your SSH public key. If you are using Windows and the Putty SSH client ask your instructor for help.
Add a New SSH Key

Comment
Key Type: DSA

Key

* denotes required field

ADD

Upload a New SSH Key

Key

Browse... No file selected.

UPLOAD
SSH Into the VM

Use the UID or login created for you when you registered and your SSH key to SSH to the VM assigned to you by your instructor. The hostname of the VM will be of the form 'spN.vo.idm.training' where N is a number.

The SSH command to use to login should have the form

```
ssh UID@spN.vo.idm.training
```

For example if the UID is 'jbasney' and you are logging into sp06.vo.idm.training then enter

```
ssh jbasney@sp06.vo.idm.training
```

You may be prompted to enter the passphrase for your private key if you have not already used it this session.

After you have logged in execute the command 'sudo bash' to become the root user.
Hands-on with SAML

Here is an overview of the SAML protocol:

To trace the SAML protocol, install SAML tracer for Firefox (or SAML DevTools for Chrome).
To activate SAML tracer, click its icon in the Firefox toolbar.

From the Firefox menu, select "SAML tracer".

This will open a Tracer window. Switch back to the primary Firefox window and open https://wiki.refeds.org. That will open the REFEDS Wiki home page. Click "Log in" on that page.

Select your identity provider and log in. You can try using your university's identity provider or a social network (like Facebook or Google). You can also sign up for a guest account at the National Center for Supercomputing Applications (https://go.ncsa.illinois.edu/idp-guest) or United ID (https://unitedid.org/).

Then switch back to the "SAML tracer" window. Deselect "Autoscroll". Look for a "SAML" icon on the right to indicate the SAML messages. First, find a SAML Authentication Request (AuthnRequest):
Use the SAML tab to view the SAML message.

What is the Issuer? __________________________

What is the Destination? __________________________

Do you see a second AuthnRequest with a different Issuer/Destination? If yes:

What is the Issuer? __________________________

What is the Destination? __________________________

Next, find a SAML IdP Response (saml2p:Response):
Does the response contain a saml:Assertion or saml2:EncryptedAssertion?

Look for a response containing an EncryptedAssertion:
What is the Issuer of the EncryptedAssertion, if you found one? __________________________

Next, look for a response containing a cleartext Assertion:
What is the Issuer of the cleartext Assertion, if you found one?  

____________________________

What Attribute Names and Values do you see?
Finally, Log Out from [https://wiki.refeds.org/](https://wiki.refeds.org/):

If you have extra time, you can try using different identity providers to Log In to [https://wiki.refeds.org/](https://wiki.refeds.org/). How do the SAML messages differ?

**Hands-on with SAML: Advanced**

Now let's configure the Shibboleth Service Provider in your training VM. If you're not already logged in to your assigned VM, see the [SSH Into the VM](#) section above.

You may edit the Shibboleth configuration file directly as detailed below or if you don't want to make the edits yourself, you can just do

```
cd /etc/shibboleth/
cp shibboleth2.xml.template shibboleth2.xml
```

If you want to make the edits yourself, begin by editing the file `/etc/shibboleth/shibboleth2.xml` and replace

```xml
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
   REMOTE_USER="eppn persistent-id targeted-id">
```

with

```xml
<ApplicationDefaults entityID="https://spN.vo.idm.training/shibboleth"
   REMOTE_USER="eppn persistent-id targeted-id">
```
where 'spN' is the hostname for your assigned host, eg. 'sp01'

Then, replace

```xml
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
    checkAddress="false" handlerSSL="false" cookieProps="http">
</Sessions>
```

with

```xml
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
    checkAddress="false" handlerSSL="true" cookieProps="https">
</Sessions>
```

Then, replace

```xml
(SSO entityID="https://idp.example.org/idp/shibboleth"
    discoveryProtocol="SAMLDS" discoveryURL="https://ds.example.org/DS/WAYF">
    SAML2 SAML1
</SSO>
```

with

```xml
(SSO entityID="https://registry.vo.idm.training/idp/shibboleth">
    SAML2
</SSO>
```

Then, below

<!-- Example of locally maintained metadata. -->

insert

```xml
<MetadataProvider type="XML" validate="true"
    file="vo-idm-training-idp-metadata.xml"/>
```

Now test your Shibboleth config and restart the Shibboleth service:

```
[root@sp0N ~]# LD_LIBRARY_PATH=/opt/shibboleth/lib64 /usr/sbin/shibd -t -u shibd -g shibd
overall configuration is loadable, check console for non-fatal problems
[root@sp0N ~]# /bin/systemctl restart shibd.service
[root@sp0N ~]# tail /var/log/shibboleth/shibd.log
2017-12-06 19:28:19 INFO Shibboleth.Application : building AttributeFilter of type XML...
2017-12-06 19:28:19 INFO Shibboleth.AttributeFilter : loaded XML resource (/etc/shibboleth/attribute-policy.xml)
2017-12-06 19:28:19 INFO Shibboleth.Application : building CredentialResolver of type File...
```

```
Now, browse to https://sp0N.vo.idm.training/secure to test your Shibboleth SP. Log in with your testuser account.

After you log in, you'll see the HTTP headers set by the Shibboleth SP:
Next, visit https://sp0N.vo.idm.training/Shibboleth.sso/Session for Shibboleth session info:

```
Next, try Shibboleth access control. Edit /etc/httpd/conf.d/shib.conf and replace

require shib-session

with

require shib-attr eppn testuser0N@vo.idm.training

to only allow a single user. You can reload httpd since only editing access control:

/bin/systemctl reload httpd.service
```
Make sure you try a negative test to prove you can deny access.

Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn’t understand how to supply the credentials required.

To log out of your Shibboleth session, browse to https://sp0N.vo.idm.training/Shibboleth.sso/Logout.

Local Logout

Status of Local Logout: Logout completed successfully.

You MUST close your browser to complete the logout process.
Hands-on with OpenID Connect

This OpenID Connect section uses the Google OAuth Playground, which requires a Google Account. If you don't already have a Google Account, you'll need to create one at https://accounts.google.com/SignUp before continuing with this section.

Next, visit the Google OAuth Playground at https://developers.google.com/oauthplayground/. In the text box that says "Input your own scopes", enter "openid email profile" to request 3 standard OpenID Connect scopes:

Then click "Authorize APIs". You will be prompted to log in to your Google account. After logging in, you will receive the OAuth Authorization Code. Next, click "Exchange authorization code for tokens" to obtain a Refresh Token and Access Token. If the "Request / Response" does not appear on the right side, increase the width of your window until it appears.
Optional Command-Line Step (ok to skip): Next, open a command-line window and save the access_token value to a shell variable. We'll use it later. Be sure to copy your long, unique access token. It will be different than the value in the following example.

```bash
export ACCESS_TOKEN="ya29.GlvfBB7urUfLM8nhBULt99ATPe3"
```

Next, open https://jwt.io/ and paste the id_token value into the box under the "ENCODED - PASTE TOKEN HERE" message, and you should see the token decoded on the right side:
Optional Command-Line Step (ok to skip): Lastly, use the Access Token to obtain user information on the command line. In the command-line window you opened previously, use the `ACCESS_TOKEN` environment variable with the `curl` command:

```
curl -H "Authorization: Bearer $ACCESS_TOKEN"
https://www.googleapis.com/oauth2/v3/userinfo
```

Hands-on with OpenID Connect: Advanced

Now let's configure OpenID Connect in your training VM. If you're not already logged in to your assigned VM, see the [SSH Into the VM](#) section above.
To update Apache to use Google OIDC instead of Shibboleth:

```
cd /etc/httpd/conf.d
mv shib.conf shib.conf.template
ln -sf openidc-google.conf.template openidc.conf
/bin/systemctl restart httpd.service
```

Now, browse to https://sp0N.vo.idm.training/secure again. You should be prompted to log in to your Google account:

Then you'll see the HTTP headers set by `mod_auth_openidc`:
Next, configure mod_auth_openidc to require specific claims for access to a subdirectory:

```bash
mkdir -p /var/www/html/secure/mygroup
echo "hello, world" > /var/www/html/secure/mygroup/hello.txt
echo -e "require claim email:jbasney@illinois.edu" \ 
  > /var/www/html/secure/mygroup/.htaccess
```

Now, browse to https://sp0N.vo.idm.training/secure/mygroup/.

If authorization is successful, you should see a directory listing:

```
Index of /secure/mygroup

  Name    Last modified  Size   Description
---  --------------  -------  ----------------
  ..       2017-12-07 21:22  13     Parent Directory
 hello     2017-12-07 21:22  13     hello.txt

```

Otherwise, you should see an authorization error:
Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn’t understand how to supply the credentials required.

See https://github.com/zmartzone/mod_auth_openidc/wiki/Authorization for details on the authorization options supported by mod_auth_openidc. Try using different OIDC claims for authorization.

Next, update the mod_auth_openidc configuration to use CILogon for authentication rather than Google:

```bash
cd /etc/httpd/conf.d
rm -f openidc.conf
ln -s openidc-cilogon.conf.template openidc.conf
/bin/systemctl restart httpd.service
```

Now, browse to https://sp0N.vo.idm.training/secure again. This time you'll be prompted to log on at cilogon.org:

After you log on, you'll see the claims provided by cilogon.org:
You can now update `/var/www/html/secure/mygroup/.htaccess` to experiment with access control using these new claims. Visit [http://www.cilogon.org/oidc](http://www.cilogon.org/oidc) for more information about CILogon's OIDC service.

Optional: To reset the configuration back to use the Shibboleth SP:

```
cd /etc/httpd/conf.d
mv shib.conf.template shib.conf
rm -f openidc.conf
/bin/systemctl restart httpd.service
```
Hands-on with Globus Auth

Pre-baked application registration

We have registered the application that is being secured with Globus and necessary configuration is in a file on the machine. Here you will update the server to use the Globus Auth configuration.

- Log into your training machine
- cd /etc/httpd/conf.d
- mv shib.conf shib.conf.template # make sure Shibboleth is not enabled
- rm openidc.conf
- ln -s openidc-globus.conf.template openidc.conf
- /bin/systemctl restart httpd
- Browse to https://sp0N.vo.idm.training/secure/

You’ll note that this will use Globus Auth, and you’ll be asked to choose a federated identity to log into the server.

- Move things back to shib:
  o mv shib.conf.template shib.conf
  o /bin/systemctl restart httpd

Register your own application

To secure applications and services using OIDC (and this Globus) you’ll need to register them with the authorization service. This section walks you through the registration steps for the training application we have.

With these steps, you can register the application yourself with Globus, and will get new client id and secret to use for your application.

- Log into https://developers.globus.org/ and choose “register your app”.

You'll be prompted to login, and you can use your institutional credentials.

Log in to Globus Auth

Use your existing organizational login
e.g., university, national lab, facility, project

Argonne National Laboratory

Didn't find your organization? Then use Globus ID to sign in. (What's this?)

Continue

You’ll be prompted to create a new project. This is a way to keep your application associated with a single project grouped together and give other administrators access to manage registration for applications on a project.
Create New Project

Project name
AGU Training

Contact email
rachana@globus.org

Please enter an email address where Globus can contact the people responsible for this project. Depending on your situation, this may be a distribution list, a standard support contact, or a personal address. We will only use this if we need to contact you about a technical issue with your services.

Send announcements of new features, changes and updates to the Globus platform

Create Project  Cancel

- Add a new application, using the “Add” menu
You will need to configure the new app - give it a name, and choose the following scopes so your application can get the following information about a user who logs in:

- OpenID
- Email
- Profile
• Set the redirect URL to your training machine to be https://spN.vo.idm.training/secure/redirect. For example for sp01 machine, it would be https://sp01.vo.idm.training/secure/redirect.

App Registration

<table>
<thead>
<tr>
<th>App Name</th>
<th>Rachana AQU Training App</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scopes</td>
<td>opened [Know who you are in Globus.] email [Know your email address.] profile [Know some details about you.]</td>
</tr>
<tr>
<td>Redirects</td>
<td><a href="https://sp01.vo.idm.training/secure/redirect">https://sp01.vo.idm.training/secure/redirect</a></td>
</tr>
<tr>
<td></td>
<td>one per line, must be HTTPS</td>
</tr>
<tr>
<td>ed Identity Provider</td>
<td>□ Require a specific Identity Provider</td>
</tr>
<tr>
<td>act Identity Provider</td>
<td>□ Pre-select a specific Identity Provider on login page</td>
</tr>
<tr>
<td>Privacy Policy</td>
<td><a href="https://example.com/privacy">https://example.com/privacy</a></td>
</tr>
<tr>
<td>Terms &amp; Conditions</td>
<td><a href="https://example.com/terms-and-conditions">https://example.com/terms-and-conditions</a></td>
</tr>
<tr>
<td>Native App</td>
<td>□ Will be used by a native application</td>
</tr>
</tbody>
</table>

• Choose “Create App” and you should see a screen that shows you the configuration.
• We’ll need to generate client secret to use with this application. You might need to scroll down to find the “Generate New Client Secret” option
You’ll be prompted to give a label to identify where the secret will be used and a secret will be printed. You’ll need this for configure the file on the training machine.

On the training machine, to edit the OpenID configuration file.

- Log into your training machine
  - $ sudo bash
  - $ cd /etc/httpd/conf.d
  - $ cp openidc-globus.conf.template openidc-globus.conf

Edit openidc-globus.conf to update the following:

- OIDCClientID to client id for your app
- OIDCClientSecret to secret for your app
- OIDCRedirectURI to ensure that has your training machine in the URL

Update the Apache configuration to use this new file

- $ rm openidc.conf
  - $ ln -s openidc-globus.conf openidc.conf
  - $ service httpd restart

Browse to https://sp0N.vo.idm.training/secure/. It should prompt you to log in using your federated identity, and to consent for this app to get the information set up via scopes (openid, profile and email). Note that the application name is the one you setup when you registered, rather than the default one we had in the training template.
Using Globus Auth with native application or thick-client

The previous sections showed using a browser to access an application secured using Globus Auth. One can also use with thick-clients or native applications to access services secured using Globus Auth.

You can find examples of such code which has a client to other Globus services (transfer and sharing) that can be run from a command line. You can download and run on your local machine by following instructions here:

https://github.com/globus/native-app-examples

Read me file on that repository shows how to set it up and use it:
https://github.com/globus/native-app-examples/blob/master/README.md

- example_copy_paste.py
  - Access Globus Transfer and do an ls on an endpoint.
- example_copy_paste_refresh_token.py -
  - Long term/recurring access to Globus Transfer to do an ls on an endpoint and automatically retrieve a new access token when necessary.
- example_local_server.py
  - Same as above but with the app using a local web server to automatically receive the "auth code."

Learn more about Globus

- Documentation: https://docs.globus.org/
- Python SDK: https://github.com/globus/globus-sdk-python/
  - Example web application, Jupyter Notebook and technical article
Hands-on with Federation

Browse to https://incommon.org/federation/info/all-entities.html to view the InCommon Federation Info: Entities web page. Click and scroll to find your university or home organization URL.

Click to display information about the IdP.
Then click on "more technical info" to see technical information about the SAML entity.
What is the Entity ID for your home organization identity provider?

__________________________________________________________________

Does the IdP have a privacy statement URL?  _____________________________

Does the IdP have a technical contact ? __________________________________

Next register for a free account with the unaffiliated UnitedID IdP. Begin by installing an app on your smart phone that can provide 2-Step Verification codes. Some popular choices are (you only need one but can use more than one if you like)

- [Google Authenticator](https://en.wikipedia.org/wiki/Google_Authenticator)
- [Last Pass Authenticator](https://en.wikipedia.org/wiki/Last_Pass_Authenticator)
- [Duo](https://en.wikipedia.org/wiki/Duo_Mobile)

Then browse to [https://unitedid.org/](https://unitedid.org/) and click "Sign up".

Use a private browsing window and log into https://wiki.refeds.org again but this time use the United ID IdP.
Hands-On with Federation: Advanced

**SSH into your assigned VM.** Use the `wget` command to download the InCommon metadata signing certificate and the `openssl` command to compute the SHA fingerprints of the certificate:

```
wget https://ds.incommon.org/certs/inc-md-cert.pem
cat inc-md-cert.pem | openssl x509 -sha1 -noout -fingerprint
cat inc-md-cert.pem | openssl x509 -sha256 -noout -fingerprint
```

How do the fingerprints of the certificate you downloaded compare to the official fingerprints InCommon lists at [https://ops.incommon.org/inc_md_cert.html](https://ops.incommon.org/inc_md_cert.html)?

Now let's configure the Shibboleth SP to download the InCommon metadata and verify that it is properly signed and valid. You may edit the Shibboleth configuration file directly as detailed below or if you don't want to make the edits yourself, you can just do

```
cd /etc/shibboleth/
cp shibboleth2-incommon.xml.template shibboleth2.xml
```

If you want to make the edits yourself, edit the file `/etc/shibboleth/shibboleth2.xml` and after this line

```xml
<MetadataProvider type="XML" validate="true" file="vo-idm-training-idp-metadata.xml"/>
```

add this configuration:

```xml
<MetadataProvider type="XML" url="http://md.incommon.org/InCommon/InCommon-metadata-idp-only.xml"
    backingFilePath="InCommon-metadata.xml"
    maxRefreshDelay="3600"
    legacyOrgNames="true">
    <MetadataFilter type="Signature" certificate="inc-md-cert.pem"
        verifyBackup="false"/>
    <MetadataFilter type="RequireValidUntil"
        maxValidityInterval="1209600"/>
    <MetadataFilter type="EntityRoleWhiteList">
        <RetainedRole>md:IDPSSODescriptor</RetainedRole>
        <RetainedRole>md:AttributeAuthorityDescriptor</RetainedRole>
    </MetadataFilter>
</MetadataProvider>
```
Now test that the configuration is valid and restart the Shibboleth daemon and Apache. Note that it may take some time for the test to complete since the SP will download the metadata and check the signature (normally the daemon does this in a background thread):

```
# LD_LIBRARY_PATH=/opt/shibboleth/lib64 /usr/sbin/shibd -t -u shibd -g shibd
overall configuration is loadable, check console for non-fatal problems
# /bin/systemctl restart shibd.service
# /bin/systemctl restart httpd.service
```

Browse to

https://sp0N.vo.idm.training/Shibboleth.sso/DiscoFeed

and examine the JSON data returned. You should see one entry for each IdP from the InCommon metadata feed.

Next let's configure the Shibboleth SP to use the Shibboleth embedded discovery service (EDS).

You may edit the Shibboleth configuration file directly as detailed below or if you don't want to make the edits yourself, you can just do

```
cd /etc/shibboleth/
cp shibboleth2-incommon.xml.template shibboleth2.xml
```

If you want to make the edits yourself, edit the file /etc/shibboleth/shibboleth2.xml and change the `<SSO>` element so that it looks like this (be sure to substituted your VM hostname):

```
<SSO discoveryProtocol="SAMLDS"
    discoveryURL="https://sp0N.vo.idm.training/shibboleth-ds/index.html">
  SAML2
</SSO>
```

Now test that the configuration is valid and restart the Shibboleth daemon and Apache:
# LD_LIBRARY_PATH=/opt/shibboleth/lib64 /usr/sbin/shibd -t -u shibd -g shibd
overall configuration is loadable, check console for non-fatal problems
# /bin/systemctl restart shibd.service
# /bin/systemctl restart httpd.service

Browse to https://sp0N.vo.idm.training/secure/ and you should be redirected to the EDS running on the VM:

Choose your home organization IdP and click "Continue".

What happens? ________________________________________________________________

Does the IdP trust your SP? __________________________________________________

Why or why not? _____________________________________________________________
Hands-on with Participant Lifecycle Management

Earlier you enrolled in the 'VO Training' collaborative organization or CO as a regular CO member or user and uploaded your SSH key. Next you will enroll in one of the 'sandbox' COs and be promoted to the CO administrator in order to exercise CO configurations.

Browse to https://registry.vo.idm.training/TestCO/N/enroll/ where 'N' is your assigned number for the training. For example if you are assigned VM 9 then you would replace 'N' above with '9'.

Choose your university or home organization login provider and authenticate. Google authentication is available if you cannot find your organization. You may use the same login you used earlier in the training or a different federated identity if you like.

Complete the form with your name, email, and optionally your organization and then click the SUBMIT button.
Click on the link in the verification email to verify your email address and wait for your petition to be confirmed.
Unlike the earlier enrollment, this enrollment flow requires petitions be manually approved.

Please ask your training leader to approve your petition and promote you to CO administrator at this time.

After the training leader approves your petition and promotes you to the CO administrator for the Test CO log back into COmanage Registry and click on the Test CO collaboration.
Create COUs

Click on the 'Configuration' menu item with the wrench icon to display the CO configuration options.
Click on 'COUs' to manage the COU structure for the Test CO.
Click 'Add a new COU' to add a new COU.
Enter a name and description for the COU and then click 'ADD'.
Try adding more COUs and making some COUs children of other COUs to reflect a more complex organizational structure.

**Organizational Identity**

Click on 'People' in the menu and then 'Organizational Identities' to list the organizational identities for the CO.
Click on the 'Name' field for a listed organization identity to display the record.
### Organizational Identities

Organizational Identities represent a person's identity as asserted by a "home" institution, such as their University or a social identity provider. Reading the documentation before editing them is advised.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Department</th>
<th>Title</th>
<th>Affiliation</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scott Koranda</td>
<td>University of Wisconsin-Milwaukee</td>
<td></td>
<td></td>
<td>Member</td>
<td></td>
</tr>
<tr>
<td>Scott Koranda</td>
<td>Google</td>
<td></td>
<td></td>
<td>Member</td>
<td></td>
</tr>
</tbody>
</table>

Page 1 of 1, Viewing 1-2 of 2
Scroll to explore the organizational identity record.

What identifiers are listed for the organizational identity? _______________________________

Is the identifier one you would expect a user to know and manage? ______________________

CO Identity

Click on 'People' and 'My Population' to list the people in the CO.
Click on the 'Edit' button to edit or view a record.
### Test CO 01 People

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scott Koranda</td>
<td>Active</td>
</tr>
</tbody>
</table>

(address: skoranda@gmail.com)
What identifier was automatically generated for the CO person record? ______________

Try adding another email address to the record.

Try adding another name to the record.

Try promoting the name you added to be the primary name for the record.

**CO Groups**

Click on 'Groups' and then 'All Groups' to list the groups for the CO.
Click on 'Add Group' to add a new group.
Enter a name and description for the group. Choose if the group will be open (anyone in the CO can add or remove himself or herself) or closed (only the group owner or a CO admin may add or remove a member).
Click 'ADD' to add the group. Then click on the name of the group you just added to view it.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Open</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO:admins</td>
<td>Test CO 01 Administrators</td>
<td>Closed</td>
<td>Active</td>
<td>Edit</td>
</tr>
<tr>
<td>CO:members:active</td>
<td>Test CO 01 Active Members</td>
<td>Closed</td>
<td>Active</td>
<td>View</td>
</tr>
<tr>
<td>CO:members:all</td>
<td>Test CO 01 Members</td>
<td>Closed</td>
<td>Active</td>
<td>View</td>
</tr>
<tr>
<td>Team 1</td>
<td>Team 1 members and managers</td>
<td>Closed</td>
<td>Active</td>
<td>Edit, Delete</td>
</tr>
</tbody>
</table>
Click on 'Manage Group Memberships' to edit the membership of the group.
Advanced: Edit Enrollment Flow

Click on 'Configuration' and then 'Enrollment Flows'.
Click 'Edit' to edit the existing enrollment flow.
Click 'Edit Enrollment Attributes' to list the attributes that are collected during enrollment.
Click 'Add Enrollment Attribute' to add a new enrollment attribute.
## Enrollment Attributes (Self Signup With Approval)

<table>
<thead>
<tr>
<th>Label</th>
<th>Attribute</th>
<th>Order</th>
<th>Required</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name (Official, CO Person)</td>
<td>2</td>
<td>Required</td>
<td>Edit, Delete</td>
</tr>
<tr>
<td>Email</td>
<td>Email (Official, CO Person)</td>
<td>3</td>
<td>Required</td>
<td>Edit, Delete</td>
</tr>
<tr>
<td>Affiliation</td>
<td>Affiliation (CO Person Role)</td>
<td>4</td>
<td>Required</td>
<td>Edit, Delete</td>
</tr>
<tr>
<td>Organization</td>
<td>Organization (CO Person Role)</td>
<td>5</td>
<td>Optional</td>
<td>Edit, Delete</td>
</tr>
</tbody>
</table>

Add Enrollment Attribute, Reorder Attributes
For 'Label' enter 'Preferred Name'.

For 'Description' enter 'Your preferred name in the collaboration'.

For 'Attribute' select 'Name (Preferred, CO Person)'.

For 'Required' select 'Optional'.

Click 'ADD' to add the new enrollment attribute.

In the menu click 'People' and then 'Enroll' to list the available enrollment flows.
Welcome to Test CO 01. Please select an action from the menus.
RIGHT-CLICK on the BEGIN button and open the URL with a private browsing window. Authenticate and then verify that the 'Preferred Name' field appears in the enrollment form.