Group Management Tool

Light weight group management, access control and authorization

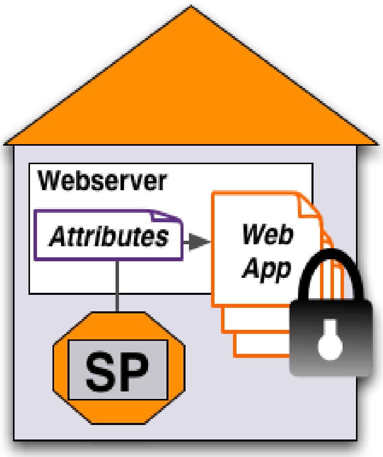
SWITCH

Serving Swiss Universities

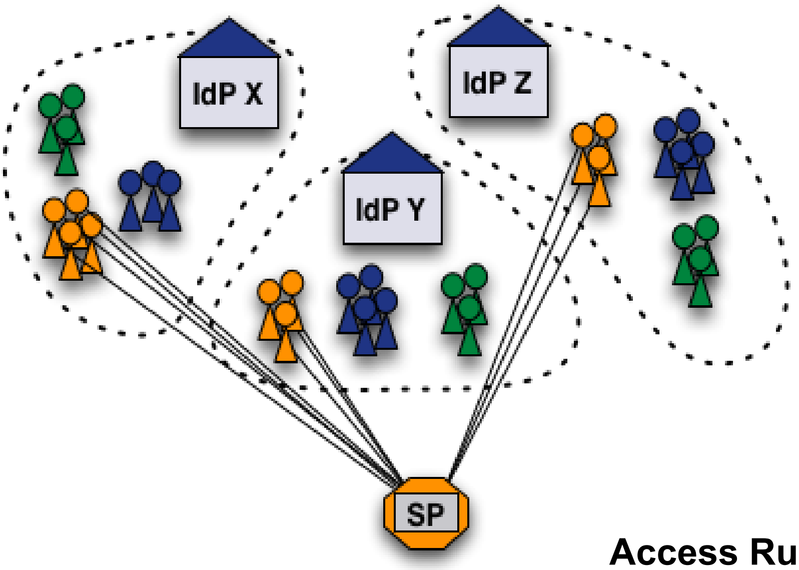
Situation

- Web application/files/functions that must be protected
- Access/authorization shall be based on user groups
- Overhead for group administration shall be small
- Shibboleth/Other solution available
- All users have an AAI account

- **Real life example:**
  The slides/photos of this workshop shall only be accessible by all people who attended this meeting.



Case 1: Users share common attributes

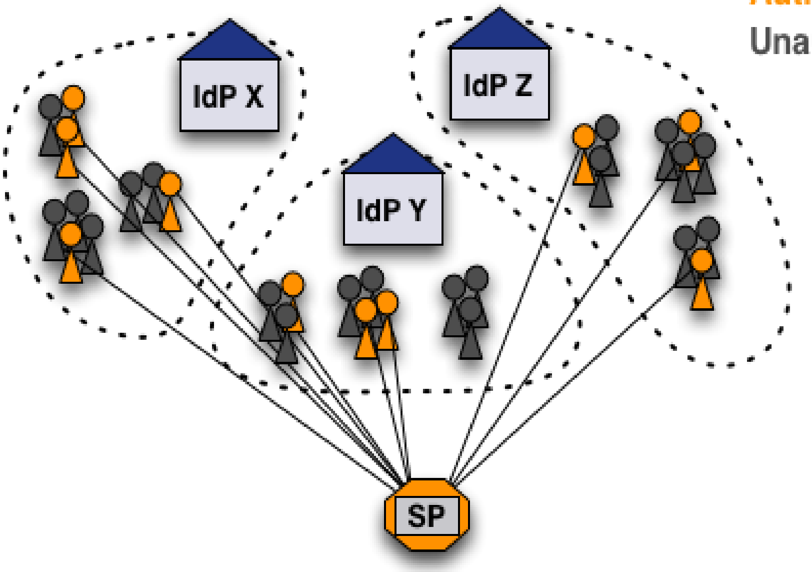


Medicine students (authorized)
Chemistry students
Staff

Access Rule

HomeOrg = IdP X| IdP Y| IdP Z
Affiliation = Student
StudyBranch = Medicine

Case 2: No common user attributes



Authorized
Unauthorized

How can these users be authorized?

Solution 1: Create a common attribute

- Add an entitlement attribute for specific users

Access Rule

Require entitlement
urn:mace:rediris.es:entitlement:wiki:jra5

⊕
- Easy solution for a difficult problem

⊖
- Additional work for user directory administrator
- Difficult to efficiently manage many entitlement values
- **Only IdP admin can manage access**

Solution 2.a: Use uniqueIDs or email

1. Get unique IDs or AAI email addresses of users.
2. Create access rules like:

Access Rule

require uniqueID *465@idp-x.ch 234@idp-y.ch* […]
require email *hans.muster@idpx.ch pierre.m@idpz.ch* […]

⊕
- Straight-forward solution

⊖
- SP administrator must know unique ID/Email address
- Difficult to efficiently manage for many users/apps
- **Only SP admin can manage access**

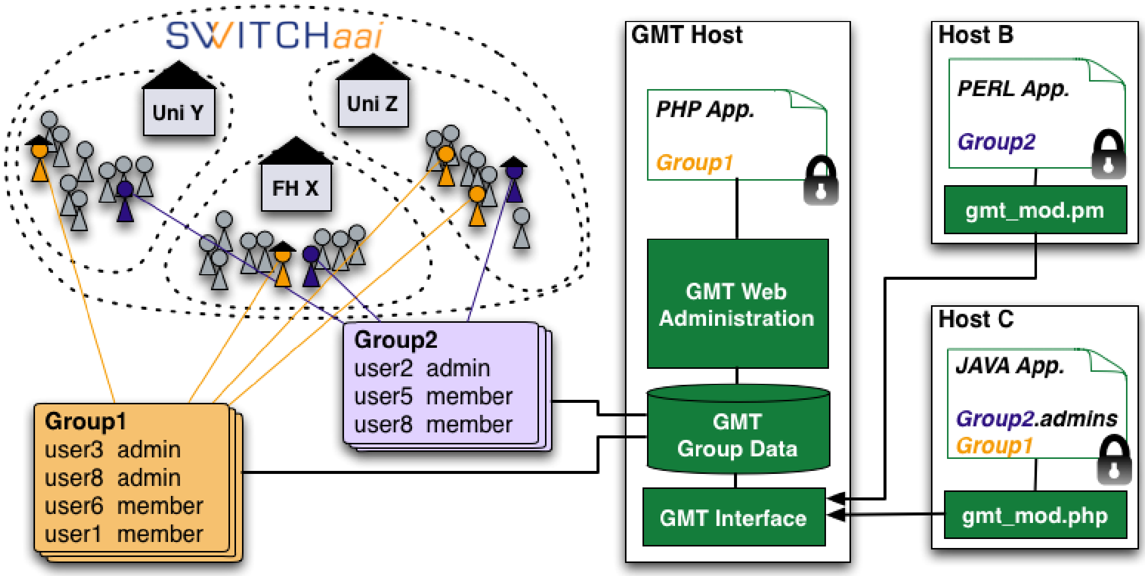
Solution 2.b: Use SWITCH GMT 1.3

- Open Source software (BSD license)
- Easy to install
- Light-weight PHP application
- Human readable text files to store group data

Features

- Manage multiple groups for multiple applications
- Three user/admin roles with different privileges
- Transfer privileges to other users
- Invite new users to join group via email
- User can request to join a group (self-registration)
- Generate authorization files (Apache .htaccess)
- API for use on remote hosts

GMT Overview



SWITCHaai

Uni Y

Uni Z

FH X

Group2
user2 admin
user5 member
user8 member

Group1
user3 admin
user8 admin
user6 member
user1 member

GMT Host

PHP App.

Group1

GMT Web Administration

GMT Group Data

GMT Interface

Host B

PERL App.

Group2

gmt_mod.pm

Host C

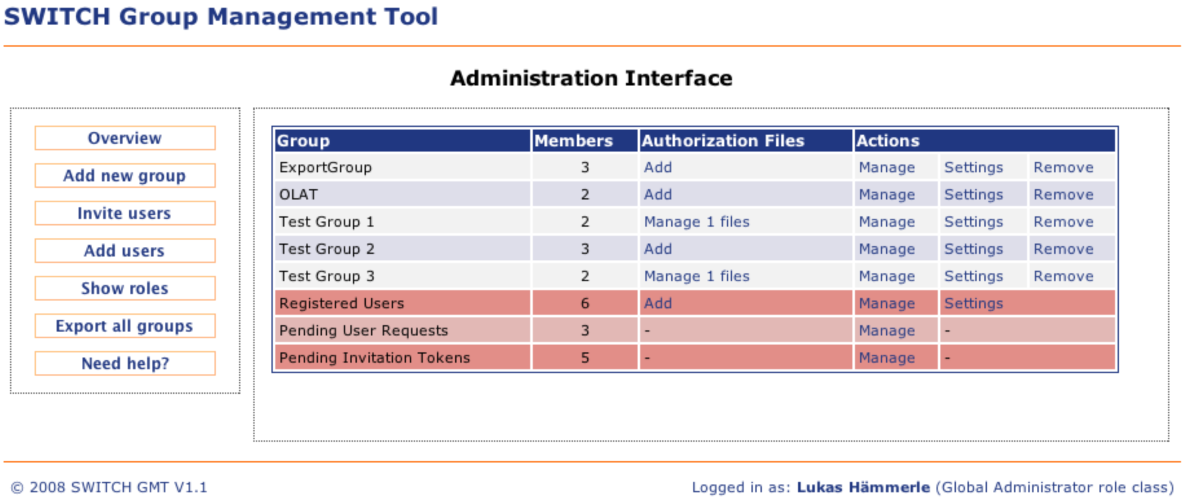
JAVA App.

Group2.admins
Group1

gmt_mod.php

Main Administration Interface

- View depends on role(s) a user has



SWITCH Group Management Tool

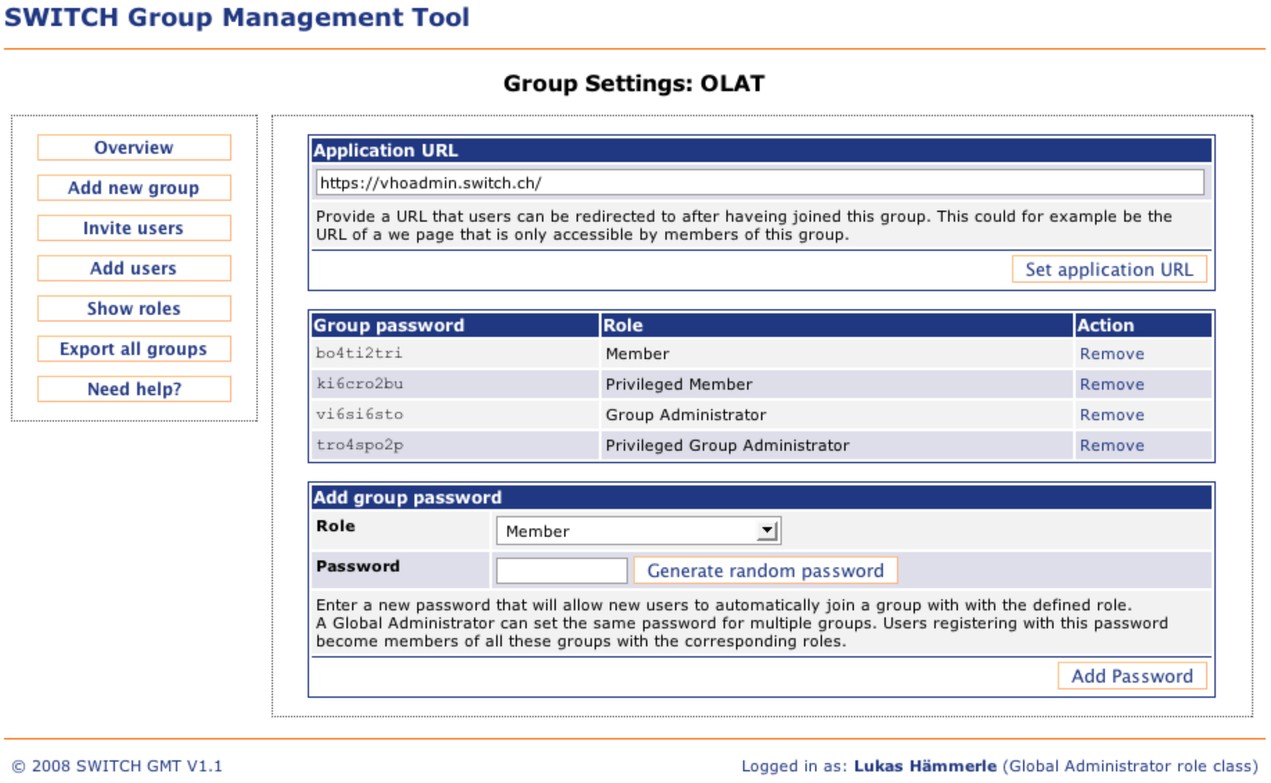
Administration Interface

Group	Members	Authorization Files	Actions		
ExportGroup	3	Add	Manage	Settings	Remove
OLAT	2	Add	Manage	Settings	Remove
Test Group 1	2	Manage 1 files	Manage	Settings	Remove
Test Group 2	3	Add	Manage	Settings	Remove
Test Group 3	2	Manage 1 files	Manage	Settings	Remove
Registered Users	6	Add	Manage	Settings	
Pending User Requests	3	-	Manage	-	
Pending Invitation Tokens	5	-	Manage	-	

© 2008 SWITCH GMT V1.1

Logged in as: **Lukas Hämmerle** (Global Administrator role class)

Group Settings



SWITCH Group Management Tool

Group Settings: OLAT

Application URL

https://vhoadmin.switch.ch/

Provide a URL that users can be redirected to after haveing joined this group. This could for example be the URL of a we page that is only accessible by members of this group.

Group password	Role	Action
bo4ti2tri	Member	Remove
ki6cro2bu	Privileged Member	Remove
vi6si6sto	Group Administrator	Remove
tro4spo2p	Privileged Group Administrator	Remove

Add group password

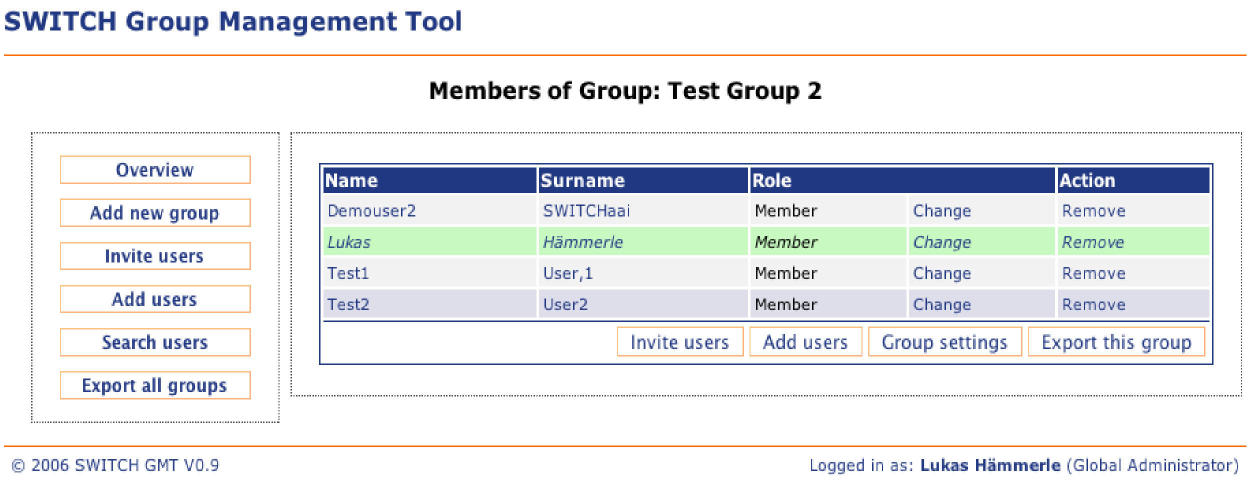
Role	Member
Password	Generate random password

Enter a new password that will allow new users to automatically join a group with with the defined role.
A Global Administrator can set the same password for multiple groups. Users registering with this password become members of all these groups with the corresponding roles.

© 2008 SWITCH GMT V1.1

Logged in as: **Lukas Hämmerle** (Global Administrator role class)

Managing a Group



SWITCH Group Management Tool

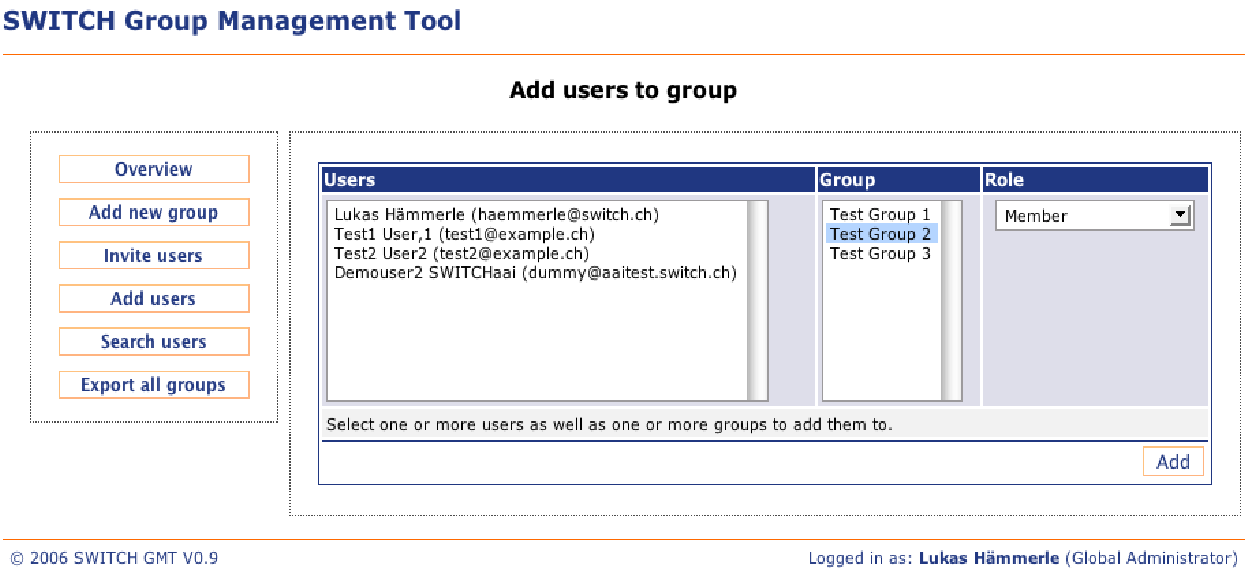
Members of Group: Test Group 2

Name	Surname	Role		Action
Demouser2	SWITCHaai	Member	Change	Remove
Lukas	*Hämmerle*	*Member*	*Change*	*Remove*
Test1	User,1	Member	Change	Remove
Test2	User2	Member	Change	Remove

© 2006 SWITCH GMT V0.9

Logged in as: **Lukas Hämmerle** (Global Administrator)

Adding Users to a Group



SWITCH Group Management Tool

Add users to group

Users:
Lukas Hämmerle (haemmerle@switch.ch)
Test1 User,1 (test1@example.ch)
Test2 User2 (test2@example.ch)
Demouser2 SWITCHaai (dummy@aaitest.switch.ch)

Group:
Test Group 1
Test Group 2
Test Group 3

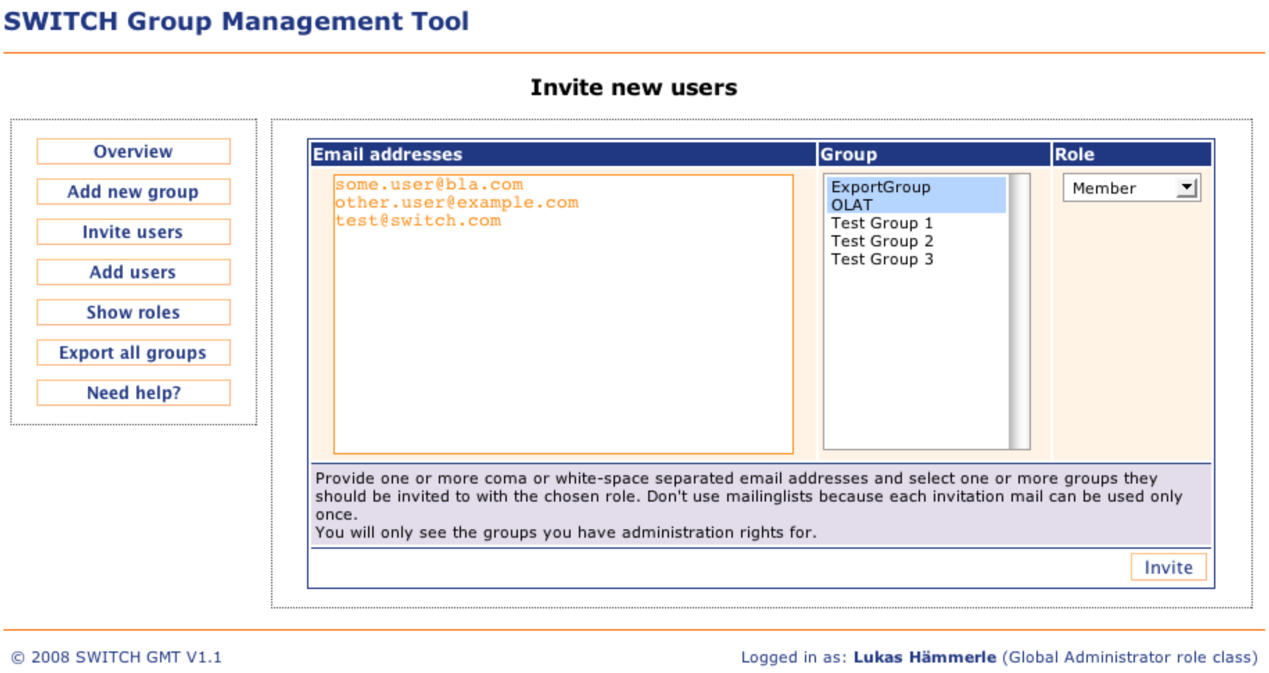
Role: Member

Select one or more users as well as one or more groups to add them to.

© 2006 SWITCH GMT V0.9

Logged in as: **Lukas Hämmerle** (Global Administrator)

Invite New Users



SWITCH Group Management Tool

Invite new users

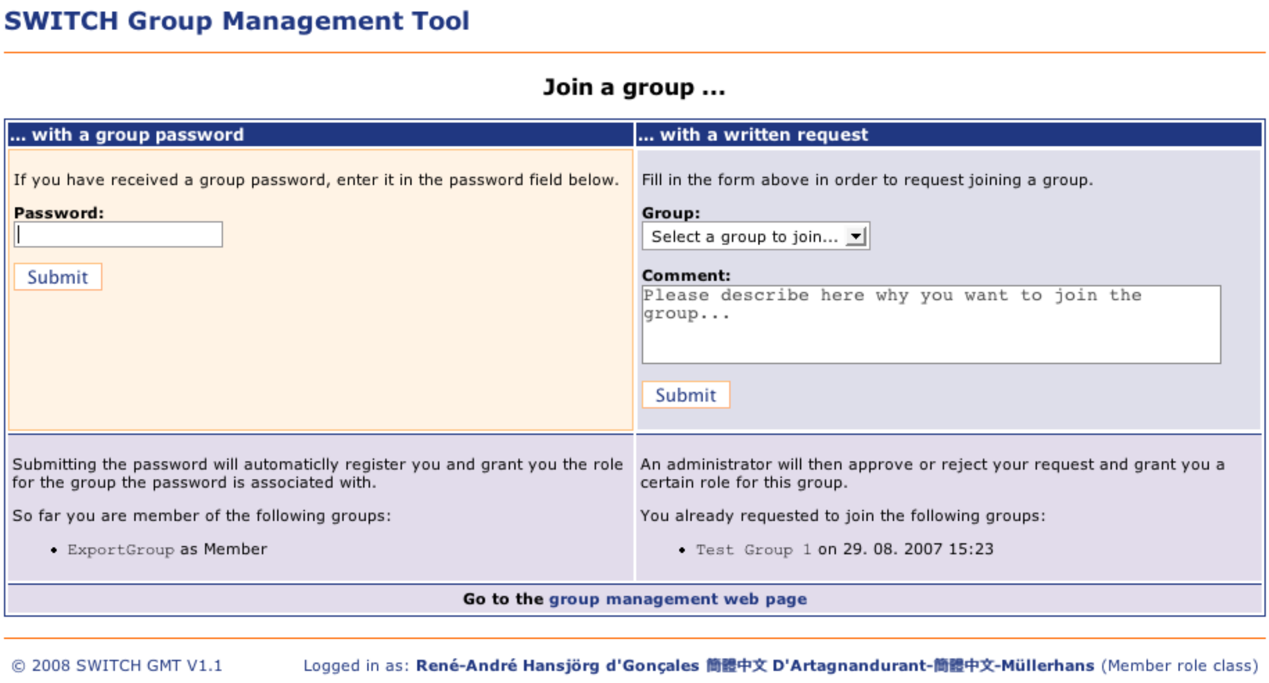
Email addresses	Group	Role
some.user@bla.com other.user@example.com test@switch.com	ExportGroup OLAT Test Group 1 Test Group 2 Test Group 3	Member

Provide one or more coma or white-space separated email addresses and select one or more groups they should be invited to with the chosen role. Don't use mailinglists because each invitation mail can be used only once.
You will only see the groups you have administration rights for.

© 2008 SWITCH GMT V1.1

Logged in as: **Lukas Hämmerle** (Global Administrator role class)

Join a Group Yourself



SWITCH Group Management Tool

Join a group ...

... with a group password

If you have received a group password, enter it in the password field below.

Password:

Submitting the password will automaticlly register you and grant you the role for the group the password is associated with.

So far you are member of the following groups:

- ExportGroup as Member

... with a written request

Fill in the form above in order to request joining a group.

Group: Select a group to join...

Comment: Please describe here why you want to join the group...

An administrator will then approve or reject your request and grant you a certain role for this group.

You already requested to join the following groups:

- Test Group 1 on 29. 08. 2007 15:23

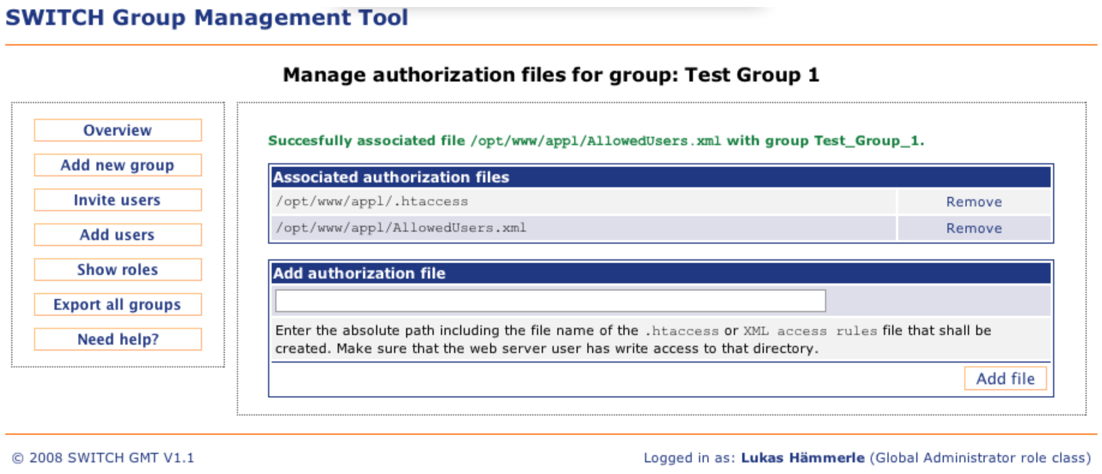
Go to the group management web page

© 2008 SWITCH GMT V1.1

Logged in as: **René-André Hansjörg d'Gonçales 簡體中文 D'Artagnandurant-簡體中文-Müllerhans** (Member role class)

Use Group Information for Authorization

- GMT writes .htaccess or XMLAccess Control files
- Files are automatically updated in case of changes



SWITCH Group Management Tool

Manage authorization files for group: Test Group 1

Succesfully associated file /opt/www/appl/AllowedUsers.xml with group Test_Group_1.

Associated authorization files	
/opt/www/appl/.htaccess	Remove
/opt/www/appl/AllowedUsers.xml	Remove

Add authorization file

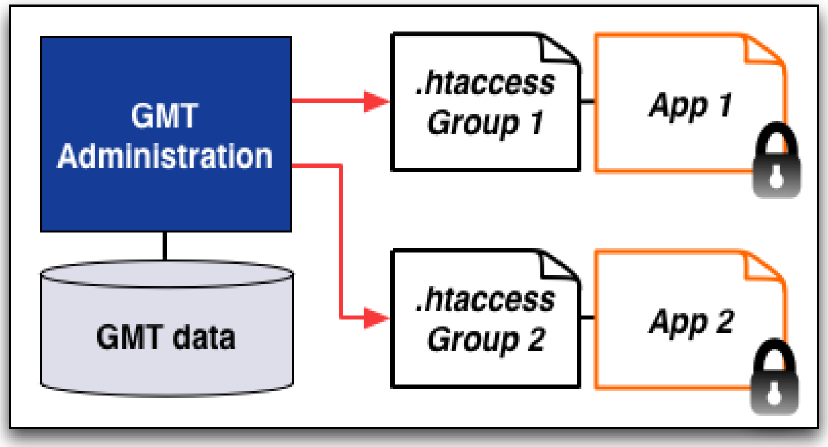
Enter the absolute path including the file name of the .htaccess or XML access rules file that shall be created. Make sure that the web server user has write access to that directory.

© 2008 SWITCH GMT V1.1

Logged in as: **Lukas Hämmerle** (Global Administrator role class)

Generate Authorization Files

- Multiple authorization files can be generated per group
- Files are updated automatically on changes



Authorization File Example

- Multiple groups can write to same authorization file
- Example of an .htaccess file

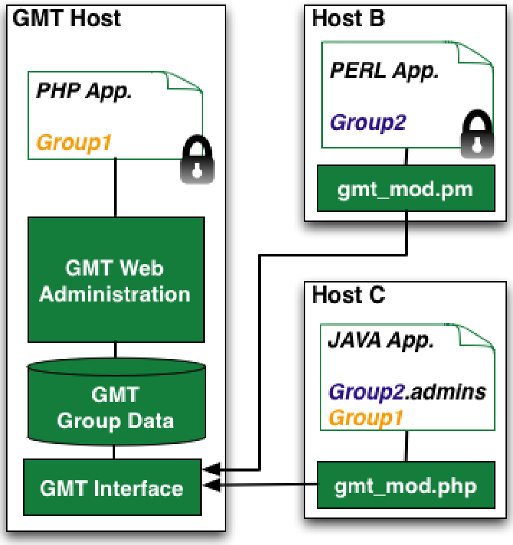
```
# Group Management Tool: Apache Authorization File
# DON'T EDIT LINES THAT CONTAIN ###
# AND ALSO DON'T REMOVE THE FOLLOWING TWO DIRECTIVES
AuthType shibboleth
ShibRequireSession On

require placeholder never.match

###START:Test_Group_1###
require uniqueID 023sdf-345fdg-23401@unizh.ch
require uniqueID 3141324sdd592@ethz.ch
###END:Test_Group_1###
```

Use of API on a Remote Host

Example code for Perl API:



```
# Group Management Tool
use gmt_mod;

$uniqueID = $ENV{’Shib-UniqueiD'};
$host = 'www.switch.ch';
$port = '80';
$path = '/gmt/interface/index.php';
$sharedKey='41a9d9[...]49de351';

# Create new GMT object
$ob = GMT->new($host,
               $port,
               $path,
               $sharedKey);

@res = $ob->getUserGroups($uniqueID);
$res_1 = $ob->isInGroup($user, $group);
@groups = $ob->getUserGroups($user);
@user_roles = $ob->getUserRoles($user);
@all_groups = $ob->getAllRoles();
# … plus 14 other functions, including 7 write functions
```

GMT Summary

- Convenient management of “virtual” groups
- Aimed at single or a few web applications with few users
- Privileges can be easily transferred
- Users can be invited or added to a group
- Users can join a group with a password or request
- GMT allows authorizing users (securely) on remote servers
- API available for PHP, Java and Perl
- Generation of Shibboleth XMLAccessControl files
- See `http://www.switch.ch/aai/gmt/`