



SWITCH

The Swiss Education & Research Network

Group Management Tool

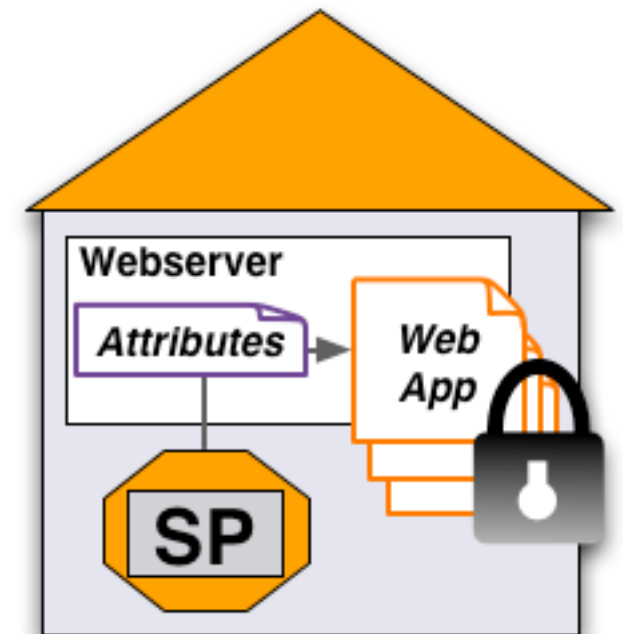
Lukas Haemmerle

haemmerle@switch.ch

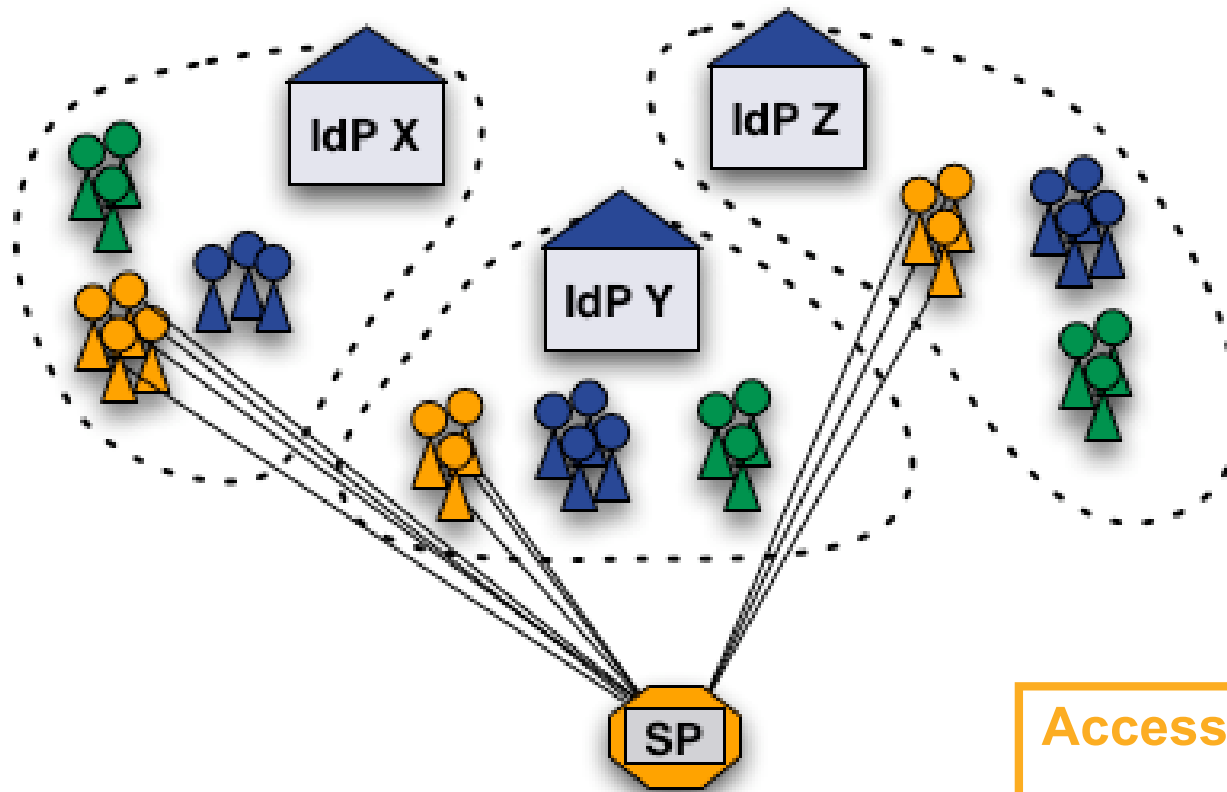
Situation

- Web application with more than 10 users
- Web application must be protected
- Access restricted to certain users
- Shibboleth SP is available on the same host

User authorization with Shibboleth



Case 1: Users share common attributes

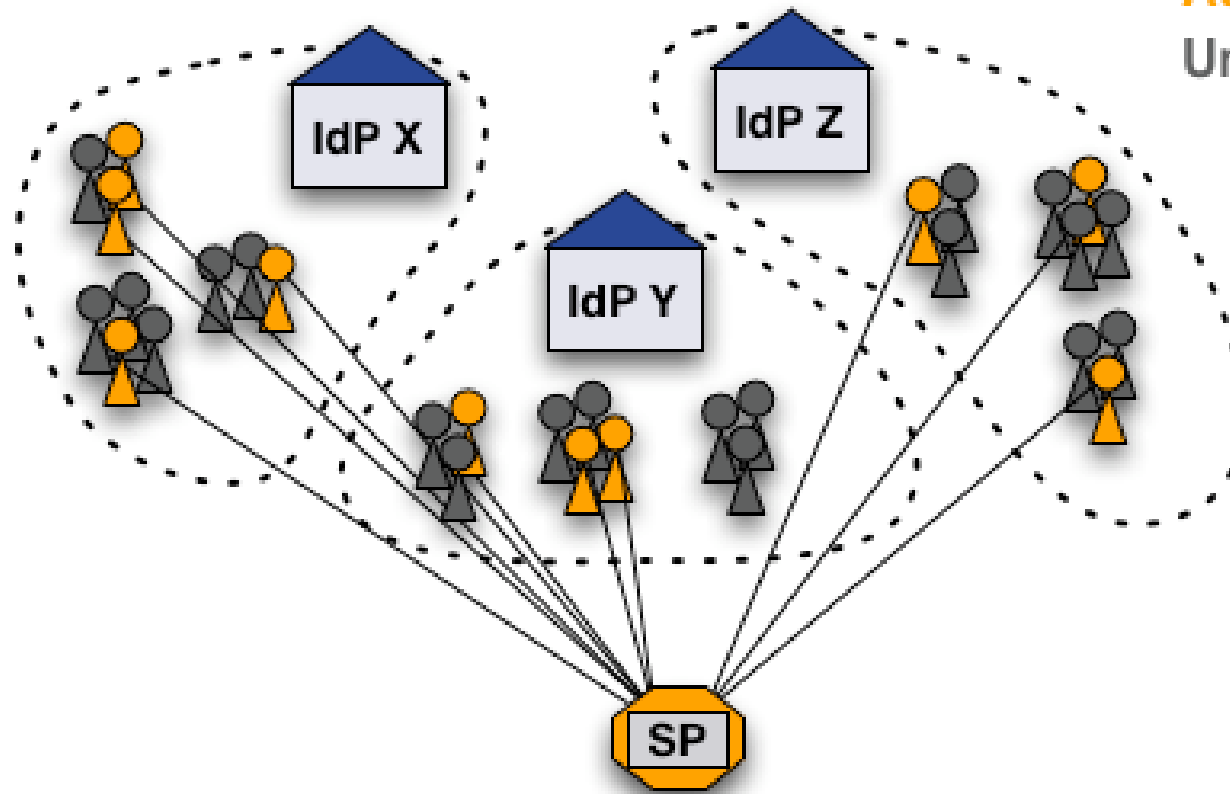


Medicine students
(authorized)
Chemistry students
Staff

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

Entitlement = <https://www.host.ch/protected/app>

- ⊕ **▪ Clean solution to a difficult problem**
- ⊖ **▪ Additional work for user directory administrator**
 - Difficult to efficiently manage many entitlement values**

Solution 2.a: Use uniqueIDs or email

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

Access Rule

uniqueID = 465@idpx.ch | 234@idpy.ch | ...
email = hans.muster@idpx.ch | pierre.m@idpz.ch | ...

- ⊕ Straight-forward and efficient solution
- ⊖
 - Unique ID is unknown to administrator
 - Email address must be AAI email address!
 - Difficult to efficiently manage for many users

Solution 2.b: Use SWITCH GMT

- **Open Source, software (BSD license)**
- **Easy to install**
- **Light-weight PHP application**
- **Text files to store group data**

Features

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

Administration Interface

https://ebulobo.switch.ch/gmt/administration/index.php

SWITCH Group Management Tool

Administration Interface

- Admin Home
- Add user to group
- Invite new user
- View user's group
- Add new group
- Export groups

Group	Members	Actions	Authorization Files
Test_Group_1	1	Edit Remove	Add
Test_Group_2	2	Edit Remove	Add
ApprovedUsers	3	Edit	Add
PendingInvitations	0	Edit	Add
WaitingApproval	0	Edit	Add

Logged in as: **Lukas Hämmerle**

Manage a group

The screenshot shows a web browser window titled "Administration Interface" with the URL `https://ebulobo.switch.ch/gmt/administration/viewUsers.php?gName=Test_Group_2`. The page title is "SWITCH Group Management Tool". The main heading is "Members of Group: Test_Group_2".

On the left side, there is a vertical menu with the following buttons: "Admin Home", "Add user to group", "Invite new user", "View user's group", "Add new group", and "Export groups".

The main content area contains a table with the following data:

User ID	Name	Surname	Rights	Action
000001@aitest.switch.ch	Test	User_1	globalAdmin	-
000002@aitest.switch.ch	Test	User_2	groupAdmin	Change Remove

Below the table, there are two buttons: "Invite a new user" and "Add user to group".

At the bottom right of the interface, it says "Logged in as: **Lukas Hämmerle**".

Adding users to a group

The screenshot shows a web browser window titled 'Administration' with the URL https://ebulobo.switch.ch/gmt/administration/add_new.php?type=user&gName=Test_Group_2. The page title is 'SWITCH Group Management Tool' and the main heading is 'Add users to group'. On the left, there is a sidebar with buttons: 'Admin Home', 'Add user to group', 'Invite new user', 'View user's group', 'Add new group', and 'Export groups'. The main content area features a table with three columns: 'Users', 'Role', and 'Group'. The 'Users' column lists 'Test User_1 (000001@aatetest.switch.ch)', 'Test User_2 (000002@aatetest.switch.ch)', and 'Test User_3 (000003@aatetest.switch.ch)'. The 'Role' column has a checkbox for 'Group admin'. The 'Group' column lists 'Test_Group_1' and 'Test_Group_2'. An 'Add to group' button is located at the bottom right of the table area. At the bottom right of the page, it says 'Logged in as: Lukas Hämmerle'.

Users	Role	Group
Test User_1 (000001@aatetest.switch.ch)	<input type="checkbox"/> Group admin	Test_Group_1
Test User_2 (000002@aatetest.switch.ch)		Test_Group_2
Test User_3 (000003@aatetest.switch.ch)		

Inviting new users

The screenshot shows a web browser window titled "Administration" with the URL `https://ebulobo.switch.ch/gmt/administration/add_new.php?type=invite&gName=Test_Group_2`. The page title is "SWITCH Group Management Tool". The main heading is "Invite new user".

On the left side, there is a navigation menu with the following buttons: "Admin Home", "Add user to group", "Invite new user", "View user's group", "Add new group", and "Export groups".

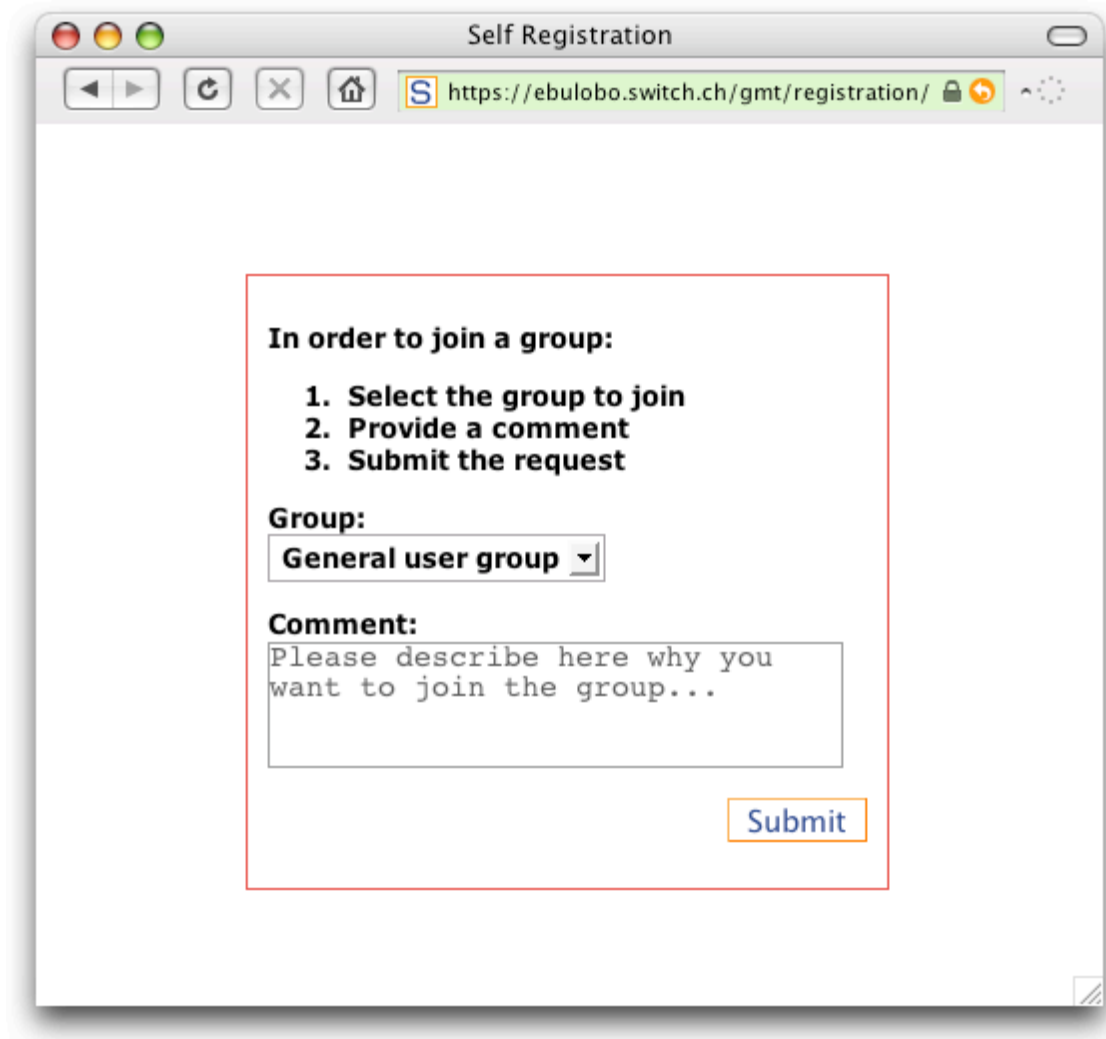
The main content area contains a table with the following structure:

Email addresses	Role	Groups
<code>hans.m@example.ch</code> <code>pierre.m@somedomain.ch</code> <code>mario.m@otherdomain.ch</code>	<input type="checkbox"/> Group admin	Test_Group_2

Below the table, there is an "Invite to group" button.

At the bottom right of the page, it says "Logged in as: **Lukas Hämmerle**".

Request to join a group



The screenshot shows a web browser window with the title "Self Registration". The address bar contains the URL "https://ebulobo.switch.ch/gmt/registration/". The main content area is enclosed in a red border and contains the following text:

In order to join a group:

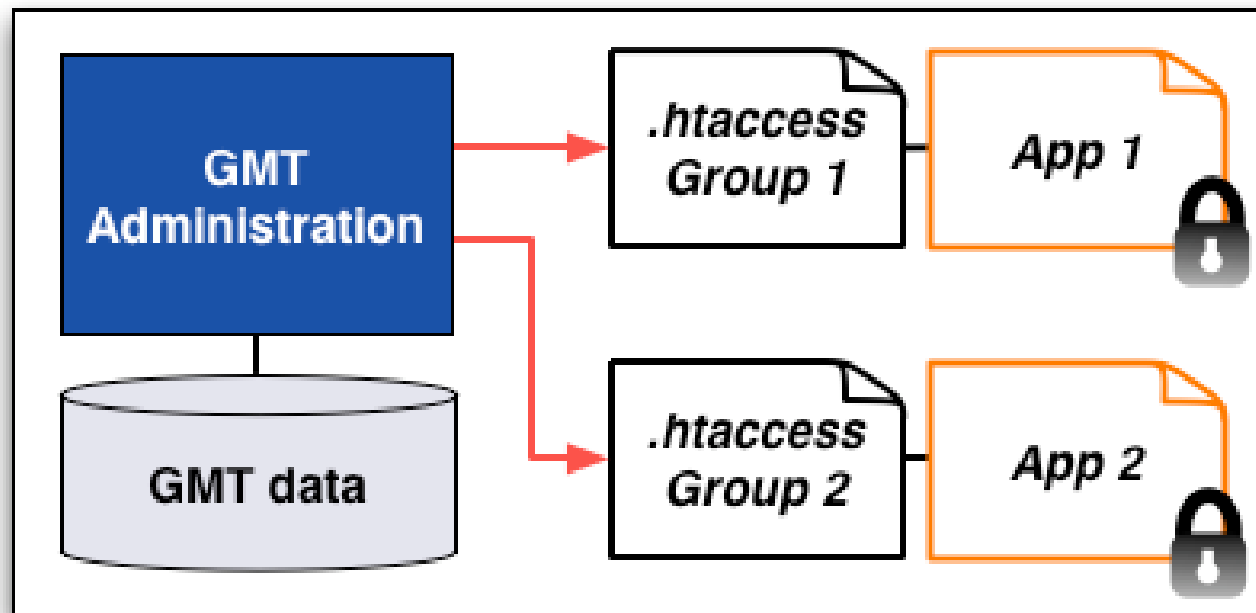
1. Select the group to join
2. Provide a comment
3. Submit the request

Group:

Comment:

Generate authorization files

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



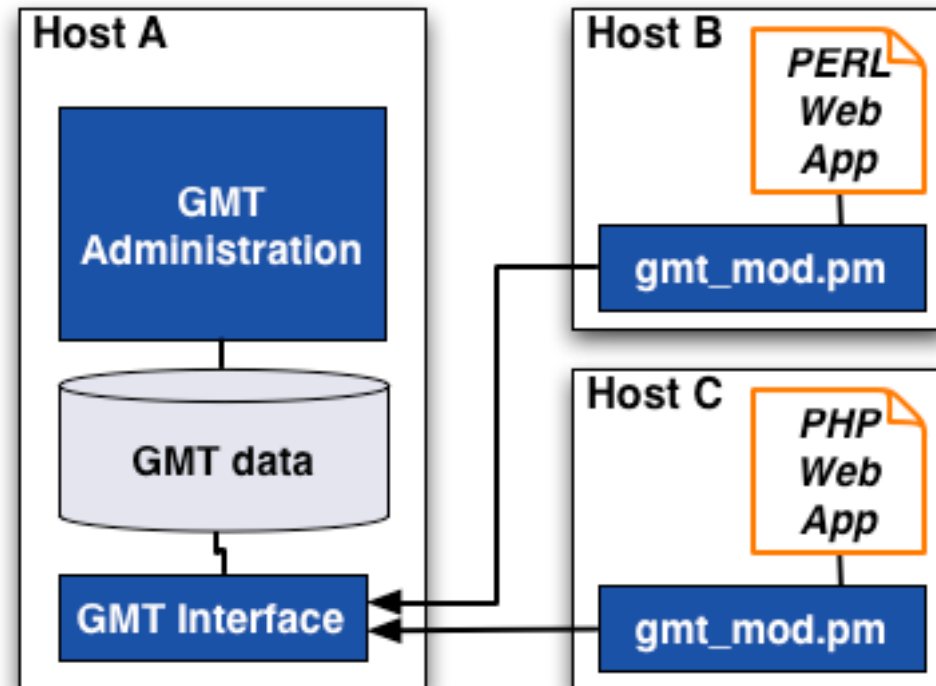
Interface for remote hosts

PHP/PERL functions:

- *isInGroup(\$uniqueID, \$groupName)*
- *getGroupModifyURL(\$groupName)*
- *getUserGroups(\$uniqueID)*
- *getStatus()*
- *getError()*

Secure queries:

- Over SSL
- Encrypted with shared key



Summary

- Convenient management of “virtual” groups
- Privileges can be transferred
- Users can request to join a group with self-registration
- Authorize users on remote servers
- Libraries available for PHP and Perl
- GMT will be available in the next few days on

<http://www.switch.ch/aai/gmt>

Outlook

- Generation of Shibboleth XML authorization files
- Your requested features (feedback appreciated!)

Q & A

 <http://www.switch.ch/aai>

aai@switch.ch