



Trident Training Manual Documentation

Release 1.0.3

Dave Dittrich

Dec 13, 2017

Contents:

1	Chapter Index	3
1.1	Introduction	3
1.1.1	Document Overview	3
1.1.2	Logging in to Trident	3
1.2	Trust Group Member Activities	5
1.2.1	User Management	5
1.2.2	Group Management	20
1.2.3	Vouching for Trust Group Members	37
1.3	Trust Group Administration Activities	46
1.3.1	Admin Password Reset	46
1.3.2	Group Admin Activities	47
1.3.3	CLI Activities	55
1.4	System Administration Activities	66
1.5	License	67

This document serves as a training guide for people using a Trident user portal system. This includes management of the Trident server by systems administrators, creating and administering trust groups by trust group leader(s), and trust group member activities (such as management of the member's profile, mailing list memberships, using the Wiki, etc.)

1.1 Introduction

1.1.1 Document Overview

The remainder of this document is divided into chapters that are focused on specifics needed by as follows:

- Section *Trust Group Member Activities* guides members through activities and attributes they can manage.
- Section *Trust Group Administration Activities* guides trust group admins through activities and attributes they can manage.
- Section *System Administration Activities* guides system admins through activities and attributes they can manage.

Each of these groups of activities requires logging in to Trident, so the remainder of this section covers this initial basic task.

1.1.2 Logging in to Trident

In order to do anything in Trident, authentication is required. This can be done at the command line, or through the web application using a web browser.

Note: This section only covers authentication and actions using the web application user interface. For details of command line use, see examples in Section *System Administration Activities*.

In a web browser, navigate to the URL of the Trident system. A page similar to the one shown in Figure *Trident home page* should open.

Click one of the **Sign In** buttons to go to the login page (Figure *Trident login page*).

Enter your credentials, and click the **Sign In** button. This will bring you to your user's home page, which will look similarly to Figure *User logged in*.

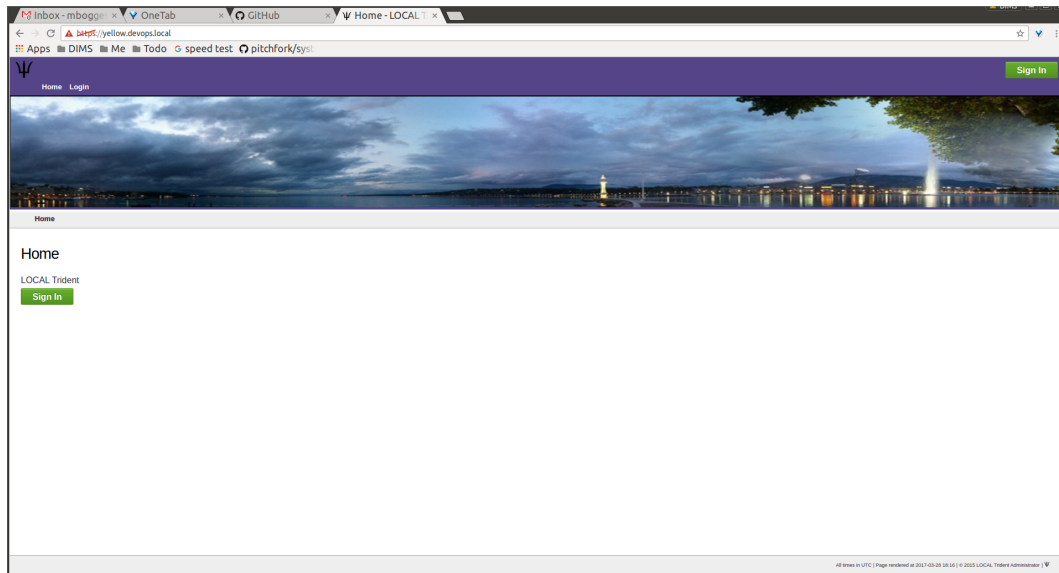


Fig. 1.1: Trident home page

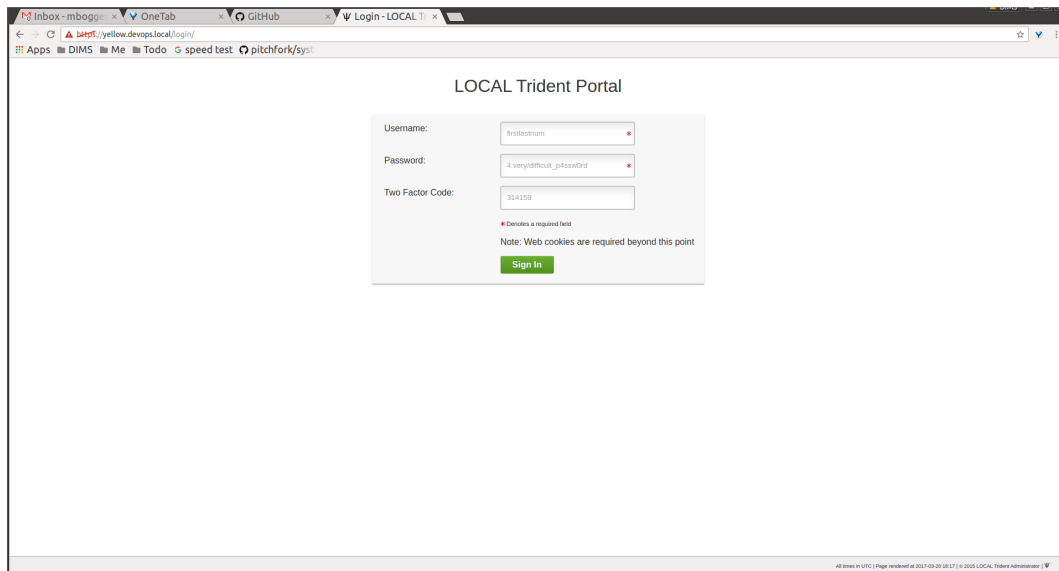


Fig. 1.2: Trident login page

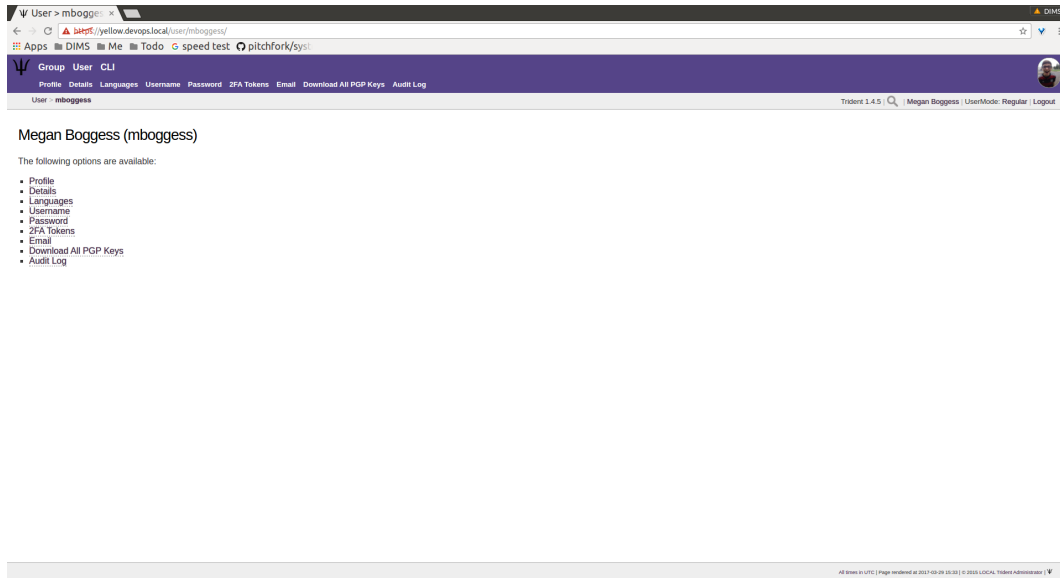


Fig. 1.3: User logged in

In the top right corner, below the user's image, are some smaller links. These show the current Trident version, the current user, the logout link, and the UserMode. It initially indicates the UserMode is Regular or not an admin user. To “swap” to being an admin user, click the UserMode link (*User swapadmin, regular*).

This will swap the user into SysAdmin mode (*User swapadmin, admin*). This does not necessarily mean the user is a system administrator, though it may. It does mean the user is now, at the least, a trust group administrator.

1.2 Trust Group Member Activities

This chapter serves as a training guide for members of a trust group using a Trident portal system. It clearly shows what activities a member may pursue and attributes she may manage. These activities include updating a member's profile and other personal details, managing mailing list memberships, using the wiki, etc.

1.2.1 User Management

This section will cover management of a user's attributes. While most (if not all) of the time, a user of the Trident portal system will be a member of a trust group, a user can exist without being a member. This section covers actions any user or member can take. Thus, the words “user” and “member” are used interchangeably. It should be noted, there are actions which only a user who is also a trust group member can take. These actions are covered in Section *Group Management*.

Profile Management

Most of the details a regular member of a trust group can modify about himself are found in the Profile page. This page is accessible by clicking the Profile tab in the second row of links at the top of the page from most user-related pages, or the Profile link in the list of links on the user's home page. Click either of those to get to the Profile page that has editable attributes. The profile can be seen in Figures *User profile, top*, *User profile, middle*, and *User profile, bottom*.

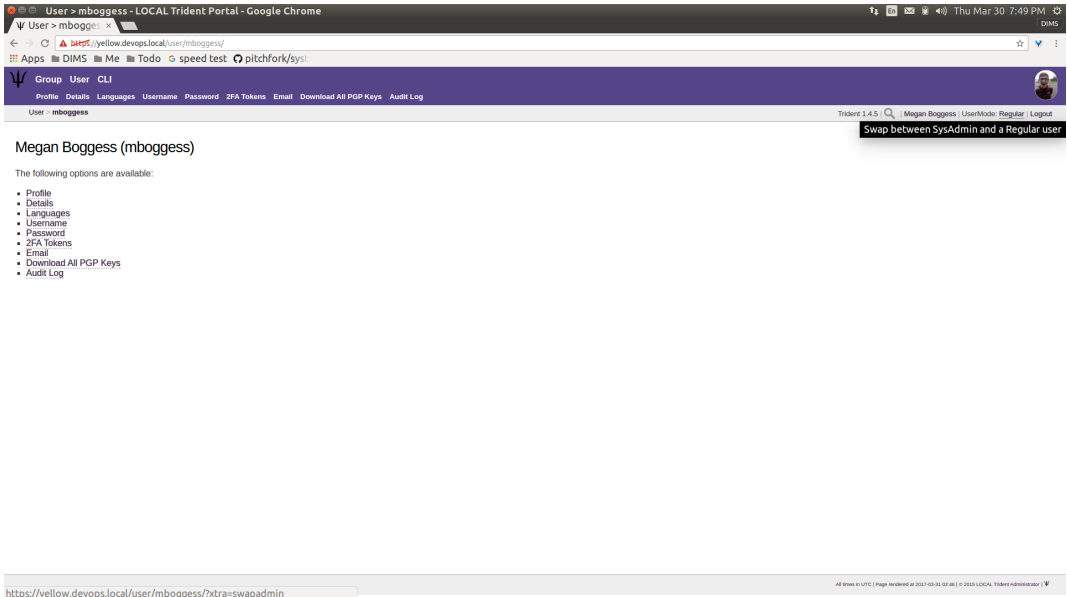


Fig. 1.4: User swapadmin, regular

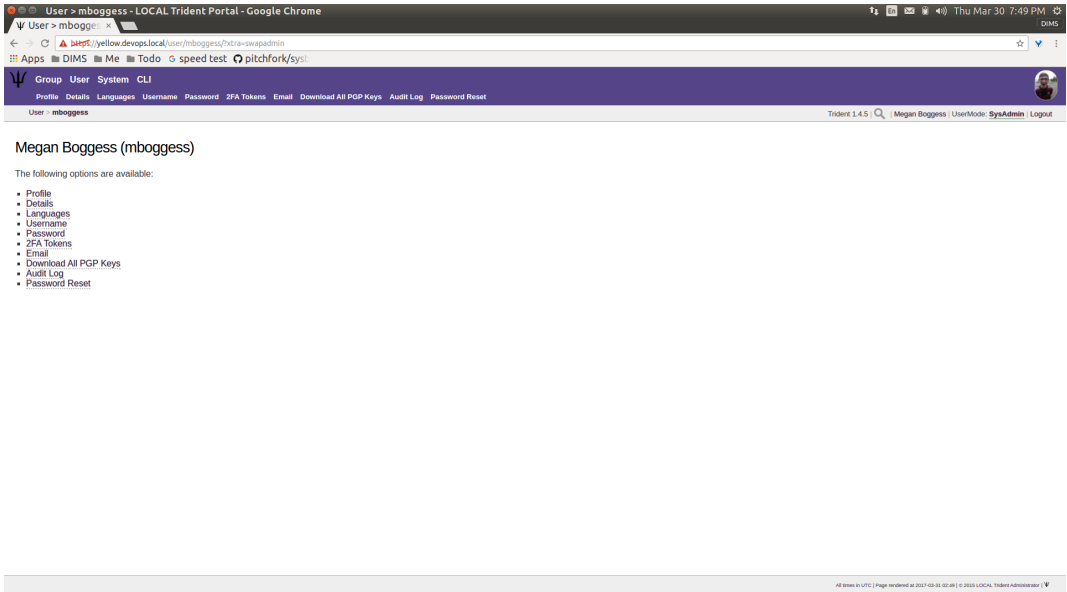


Fig. 1.5: User swapadmin, admin

User > mboggess > Profile

Megan Boggess (mboggess)

Image:
 No file chosen

User Name:
 mboggess

Full Name:
 Megan Boggess

First Name:
 Megan

Last Name:
 Boggess

Affiliation:
 DIMS

Postal Details:
 Philadelphia, PA

Fig. 1.6: User profile, top

SMS:

IM:
 n/a

Timezone:
 Eastern

Telephone:
 3042796931

Airport:
 PHL

Biography:

Number of failed Login Attempts:
 0

Email Disabled:
☐

Hide email address:
☐

Email Recovery address:
 mboggess@devops.local

Furlough:
☐

Entered:
 03/27/2017, 05:48 PM

Fig. 1.7: User profile, middle

Airport:
 Biography:
 Number of failed Login Attempts:
 Email Disabled: ☐
 Hide email address: ☐
 Email Recovery address:
 Furlough: ☐
 Entered: 03/27/2017, 05:48 PM
 Last Activity: 03/29/2017, 08:17 AM

Fig. 1.8: User profile, bottom

On the profile page, details such as name, affiliation, address, phone number, and airport can be added or modified. A profile image can be uploaded. Longer-form attributes can be edited, such as postal details and biography. Failed logins and some activity statistics are also tracked on a member's profile.

Click the `Update Profile` button to save the changes after modifications have been made. The page will refresh with the newly saved information, as well as indicate how many fields were updated and how many fields were not updated.

Other Personal Details

Other personal details can be modified through the `Details`, `Languages`, and `Username` tabs found in the second row at the top of any user-related page or in the list of links found on a user's home page. This section covers these actions.

The `Details` page (Figure *User details*) is a place to add any other details that don't conform to the profile. Currently, the only detail type is a callsign.

The `Languages` page (Figure *User languages, choose language*) is the place to add languages a member knows and her skill level (Figure *User languages, choose skill level*) at that language. Click the `Add Language` button to add a new language (Figure *User languages, updated language*).

The `Username` page (Figure *User username change*) allows a member to change her username. This can affect external systems, so this change should be used with care and caution. Enter the new username in the field and use the toggle to confirm the change before clicking the `Change username` button.

Password Change

The `Password` page (Figure *Define new password*) allows a member to change her password, provided she knows her current password (which she should, since she is logged in already). When the member clicks the `Change Password` button, she is immediately logged out and must login again with the new password (Figure *Login with new password*).

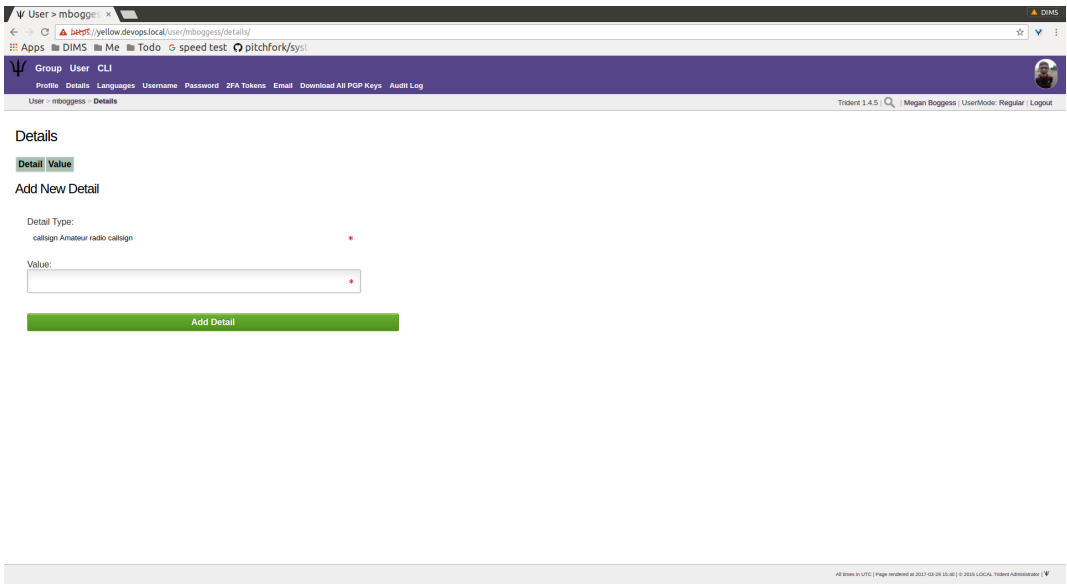


Fig. 1.9: User details

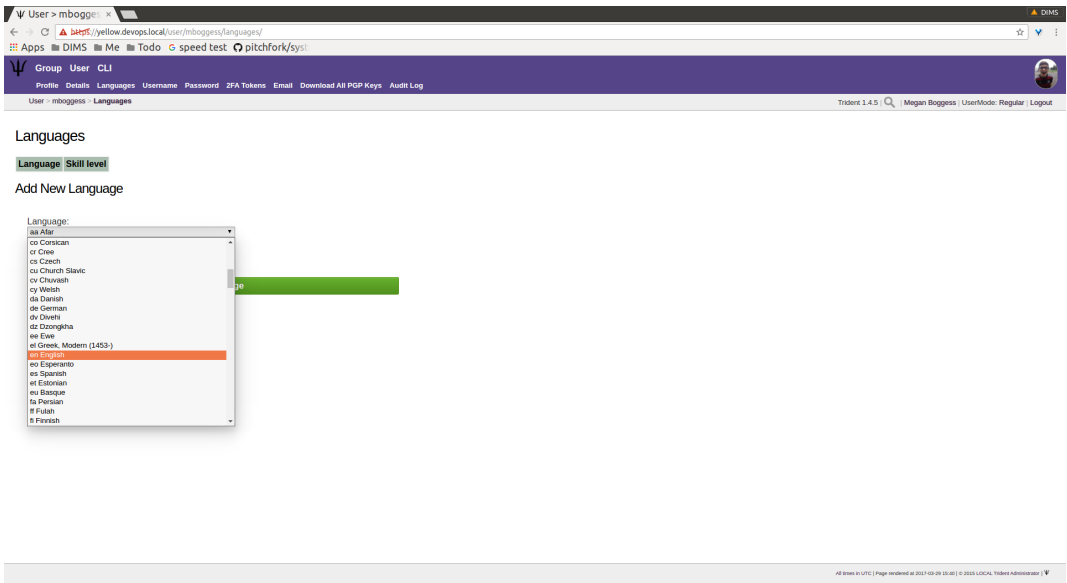


Fig. 1.10: User languages, choose language

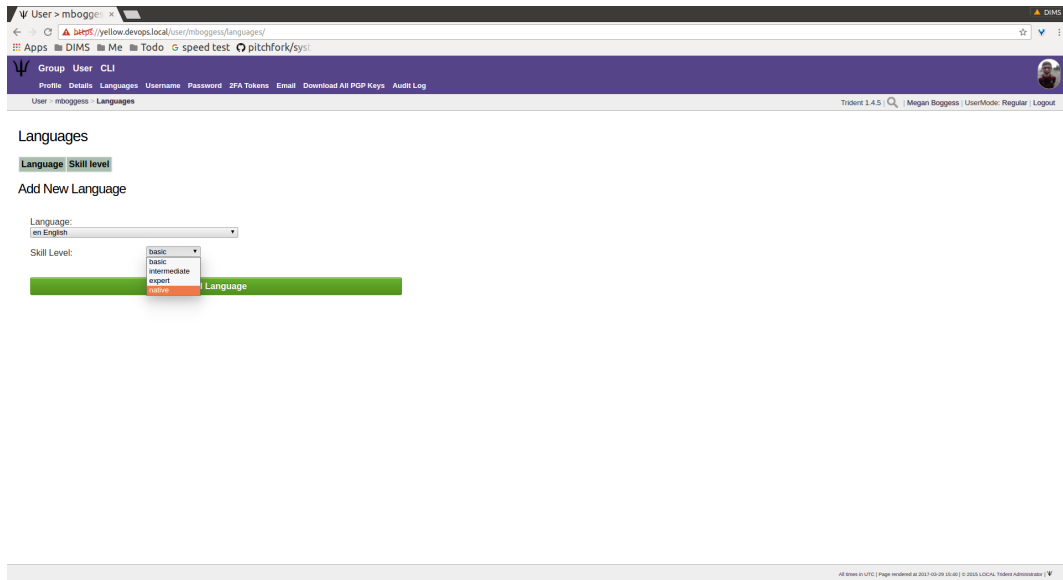


Fig. 1.11: User languages, choose skill level

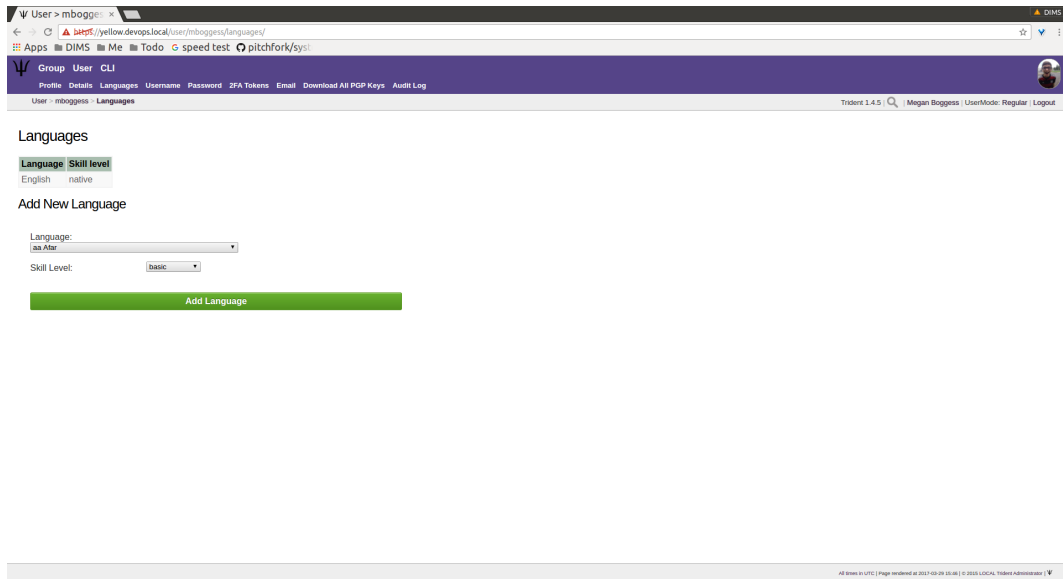


Fig. 1.12: User languages, updated language

Username

This page allows you to change your username.

Please note that username changes might affect external systems where you are also using this username.

On successful username change **you will be logged out** and redirected to the Login page. This to flush the old authentication tokens/cookies which are then invalid.

New username:

Confirm username change:

[Change username](#)

Fig. 1.13: User username change

Password

This page allows you to change your password.

Username:

Current password:

New password:

Repeat new password:

[Change Password](#)

Fig. 1.14: Define new password

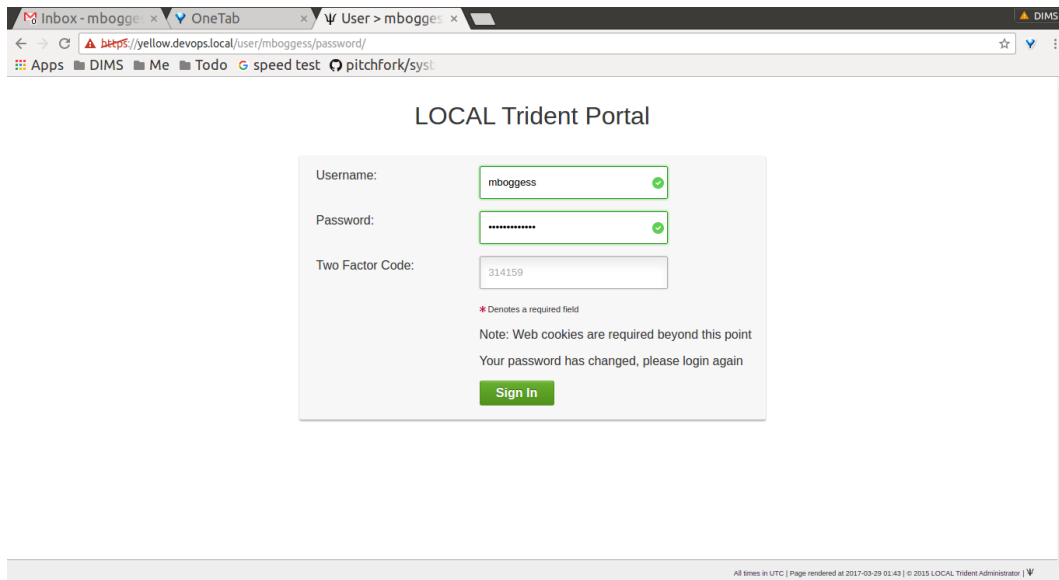


Fig. 1.15: Login with new password

Two Factor Authentication

The 2FA Tokens page (Figure *Two-factor authentication*) allows a member to add two-factor authentication tokens. Types of two-factor authentications include a variety of one-time passwords: time-based, HMAC-based, and single-use. The user must give his current password and a description for the token, as well as choose which OTP type. Once those fields have been filled out, click the **Create** button, and the new token will show in the list of two-factor authentication tokens.

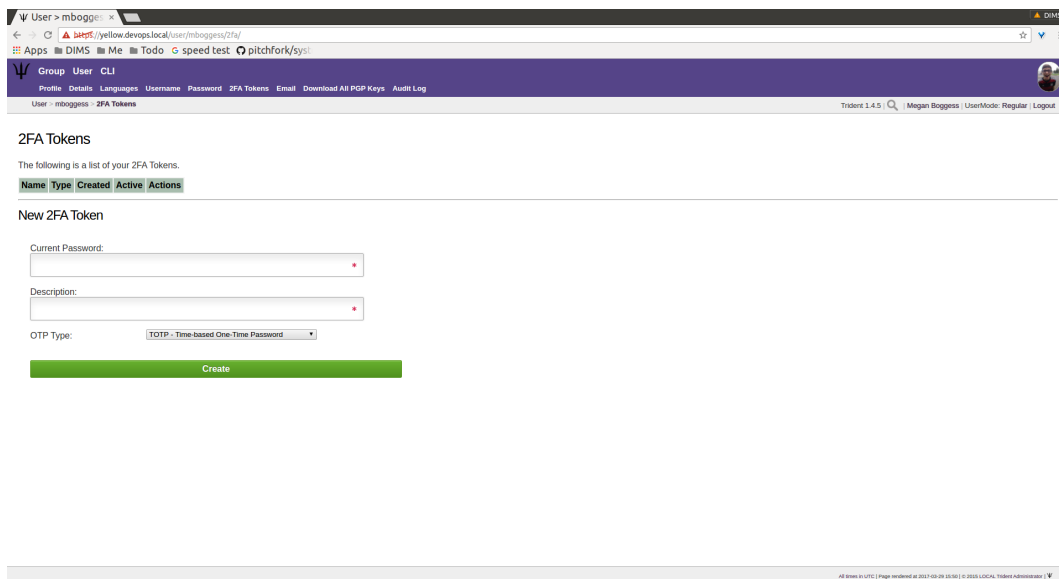


Fig. 1.16: Two-factor authentication

Email Management

The `Email` page (Figure [Main email page](#)) covers a variety of things. It lists email addresses tied to a user's account, showing if each email address has a PGP key tied to it, whether it is verified, whether it is the recovery email address associated with the user's account, and with which trust group it will be used. This page also provides a way to add a new email address, and lists each group and associated email addresses for that group.

Note: Encryption keys are discussed in Section [PGP Keys](#).

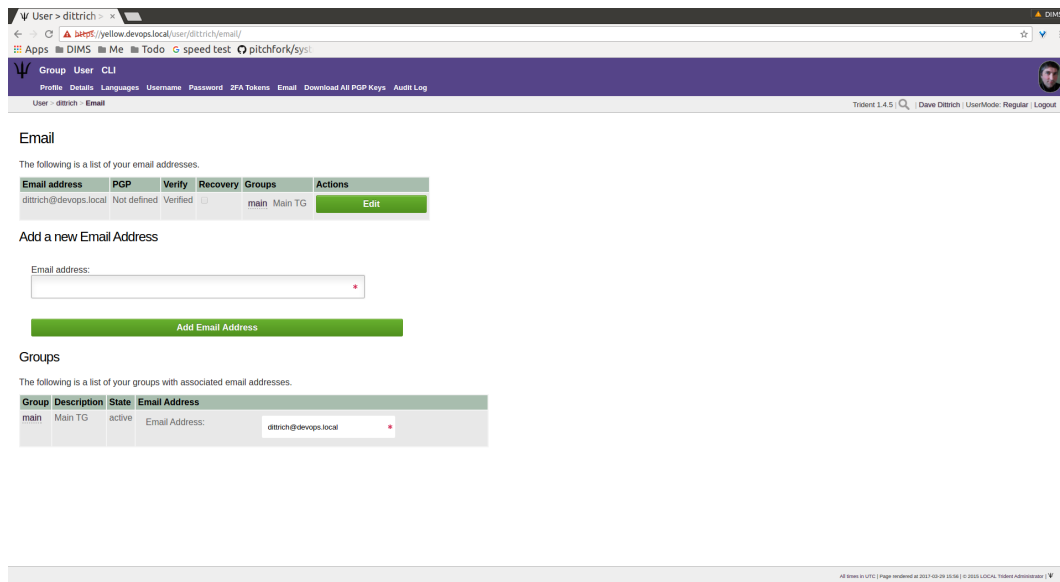


Fig. 1.17: Main email page

A user can edit (Figure [Email edit page](#)) attributes about email addresses associated with his account by clicking the `Edit` button in the row of the email address for which the edits should be made.

Click the `Make Recover Email` button to make the selected email address the recovery email address for the user's account.

Once this is completed, the button disappears and a check box appears in the `Recover` row (Figure [Make recover email](#)).

As can be seen, this is also the page where PGP keys are to be added, and we will cover this in the next section.

Going back to the `Email` page shows another check box in the list of email address (Figure [Recover email confirmed](#)).

To add an email address (Figure [Add new email](#)), type it in the requested field:

After clicking the `Add Email Address` button, the page will refresh with the new address in the list at the top of the page. Click the `Edit` button to make additional changes (Figure [New email attributes](#)).

A member must verify any new email addresses he manually adds. Click the `Verify` button. This will send an email to the provided address. The email will contain a verification code. Copy and paste the code in the `Verification Code` field, and click the `Confirm` button (Figure [Verify email](#)).

Until the email address is verified, the list of email addresses will retain an `In Process` status in the `Verify` column (Figure [New email status](#)).

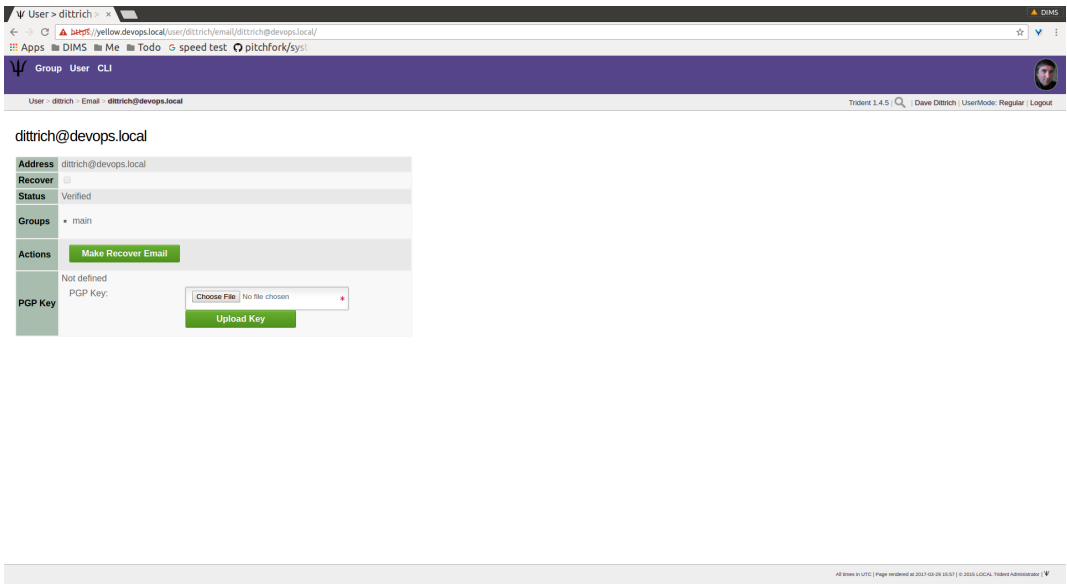


Fig. 1.18: Email edit page

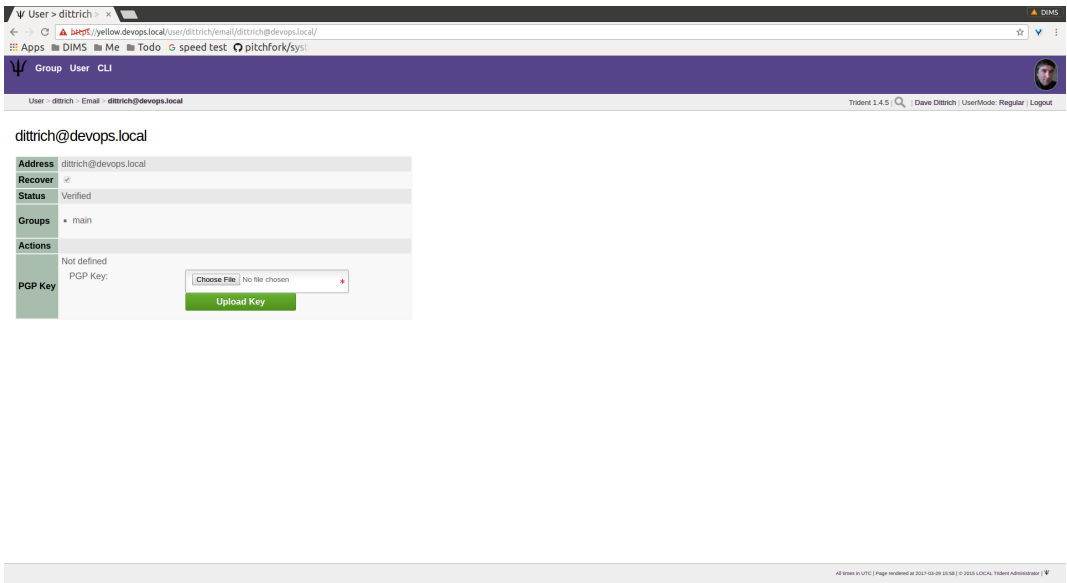


Fig. 1.19: Make recover email

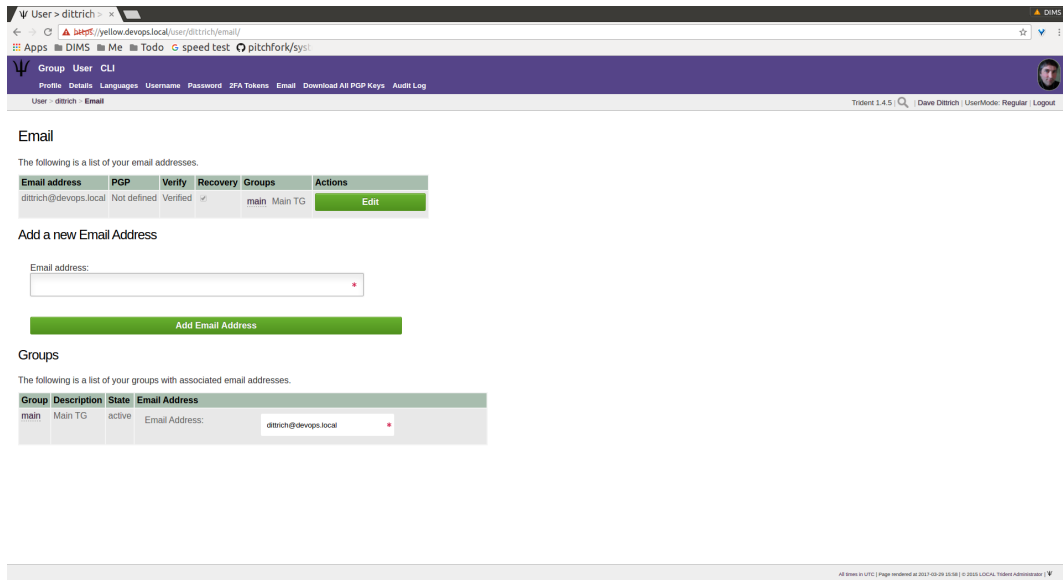


Fig. 1.20: Recover email confirmed

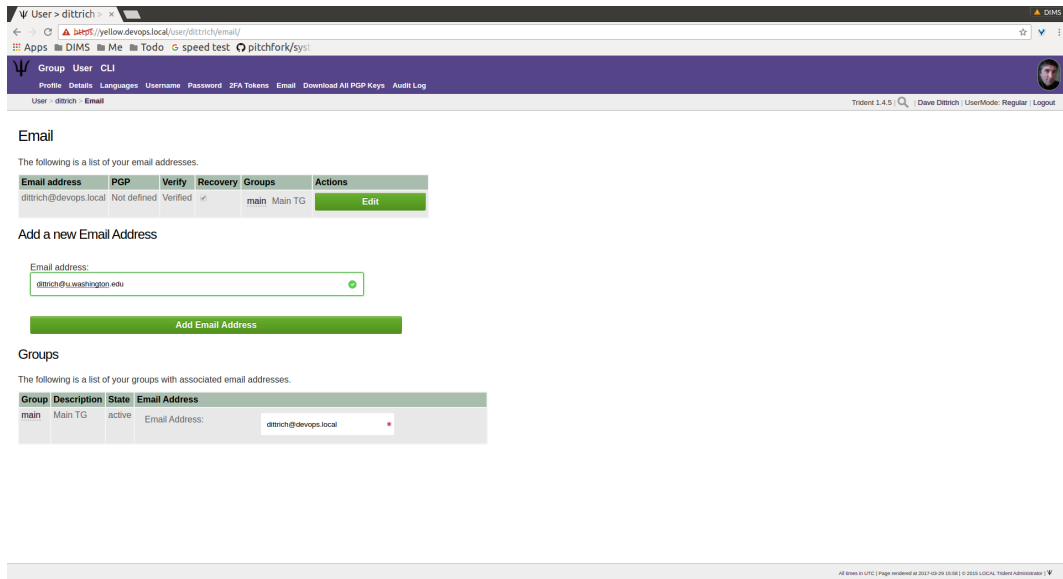


Fig. 1.21: Add new email

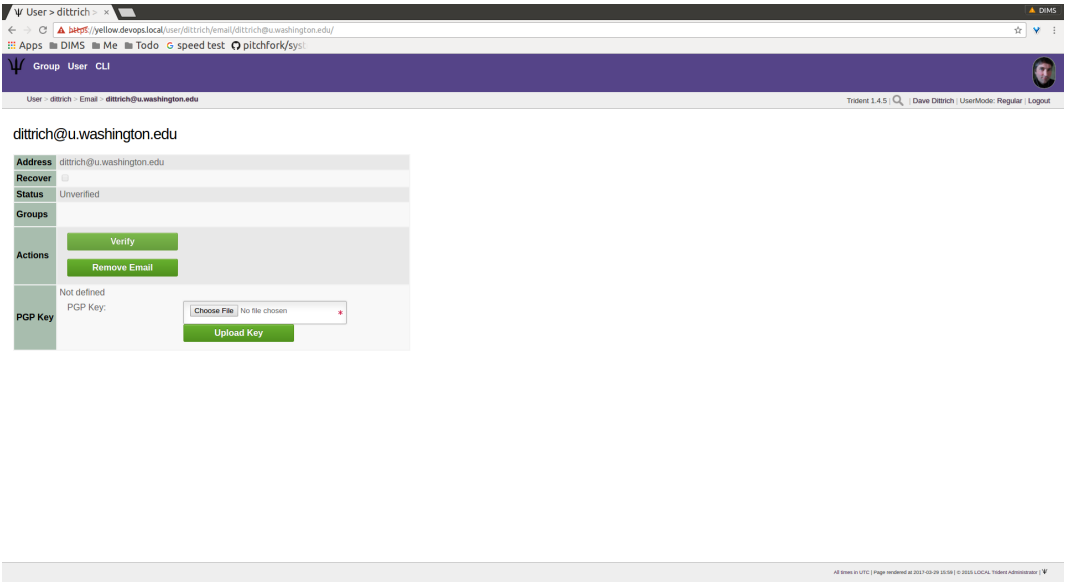


Fig. 1.22: New email attributes

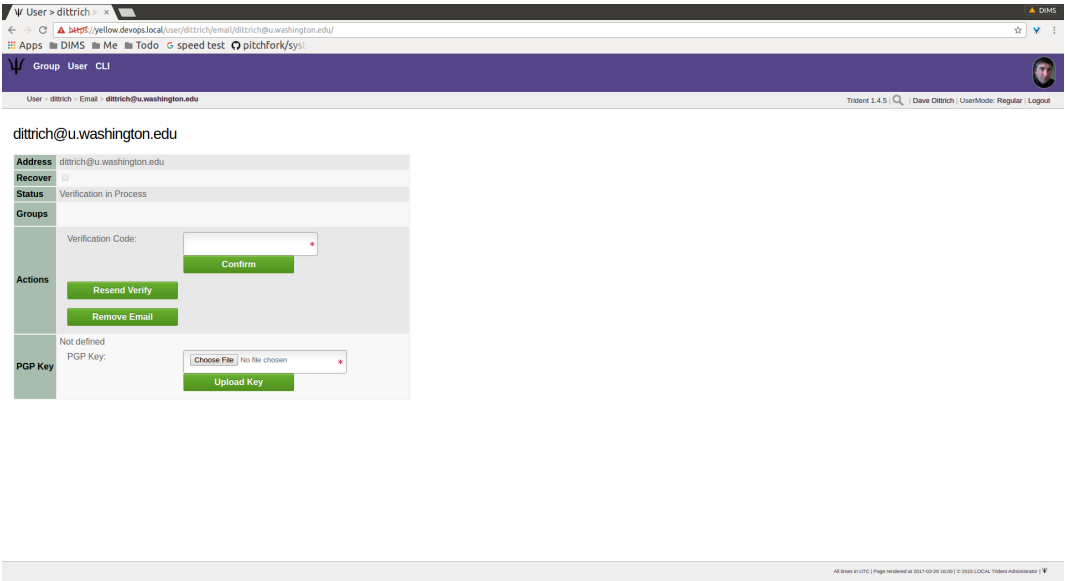


Fig. 1.23: Verify email

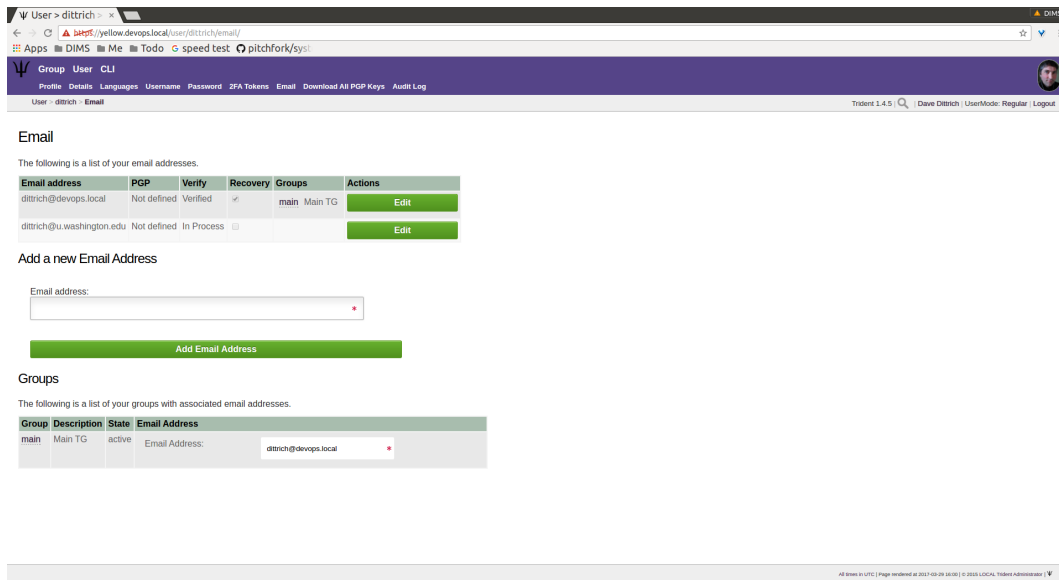


Fig. 1.24: New email status

Remember, a recovery email address for an account can be set using the “Edit” screen. Only one address may be the recovery email.

Since the `dittrich` user has not confirmed his new email address yet, let’s take a look at what happens when a user does have multiple verified email addresses.

A user can choose which email address will be associated with each trust group of which she is a member. In the case of the user `mbogges`, she has two email addresses. Only one address can be associated with a trust group at a time. Since she has two email addresses, she must chose one to be associated with the `main` trust group of which she is a member (Figure *Multiple emails*).

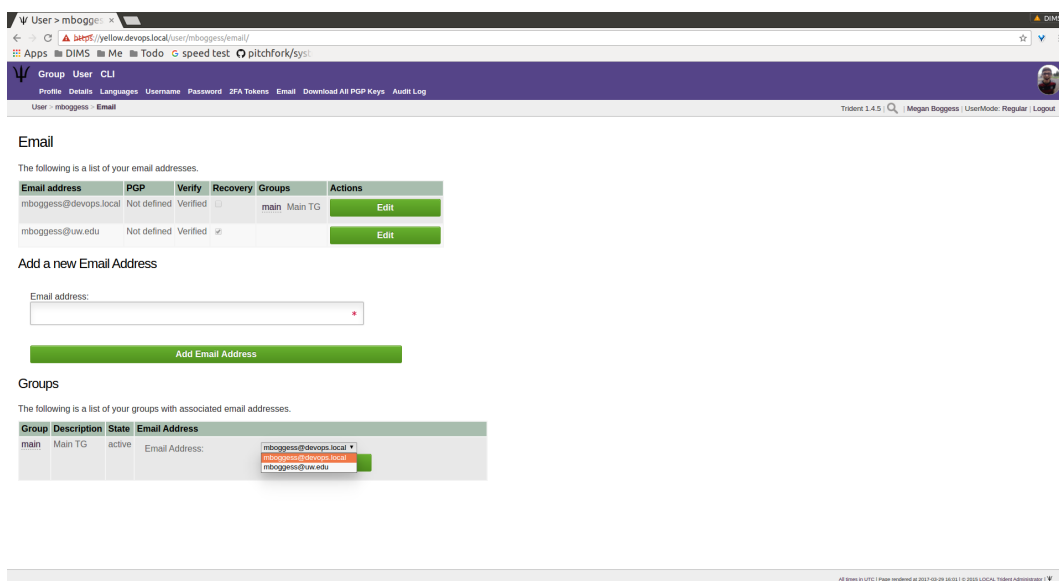


Fig. 1.25: Multiple emails

By choosing the second email address (the @uw email address) to be the email address associated with the main trust group, the list at the top of the page changes. It now shows the @uw email address is associated with the main trust group, as indicated by the Groups column in the list (Figure *Email-group association swap*).

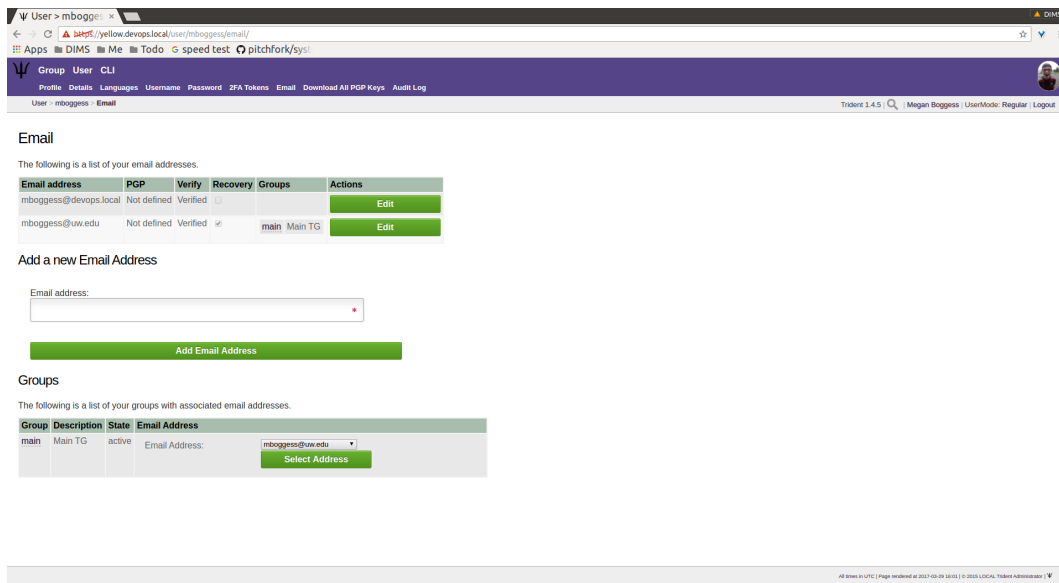


Fig. 1.26: Email-group association swap

PGP Keys

PGP keys can be downloaded and uploaded. They must stay current for a user to be able to read any encrypted email sent via the trust groups of which the user is a member.

Note: For information on using PGP (or GNU Privacy Guard) keys for secure email communication, see the Free Software Foundation's [Email Self-Defense](#) guide and Section [Using GPG or PGP Encrypted Email](#) of the [Trident User Manual v 1.0.2](#).

To download all PGP keys tied to any emails associated with a user's account, just click the Download All PGP Keys tab in the second row at the top of any User page, or click the Download All PGP Keys link in the list of links on the user's home page (Figure *Download PGP keys*).

To add PGP keys, return to the Email page. Click the Edit button in the row of the email address with which a new PGP key should be associated. In the PGP Key row, choose the PGP key file. Then click the Upload Key button (Figure *Upload PGP key*).

Audit Log

The Audit Log page (Figure *Audit log*) has no editable attributes. It shows all activities accomplished by the user. Searches are possible. Additionally, only 10 activities are shown at a time, so click the Forward button to see older activities.

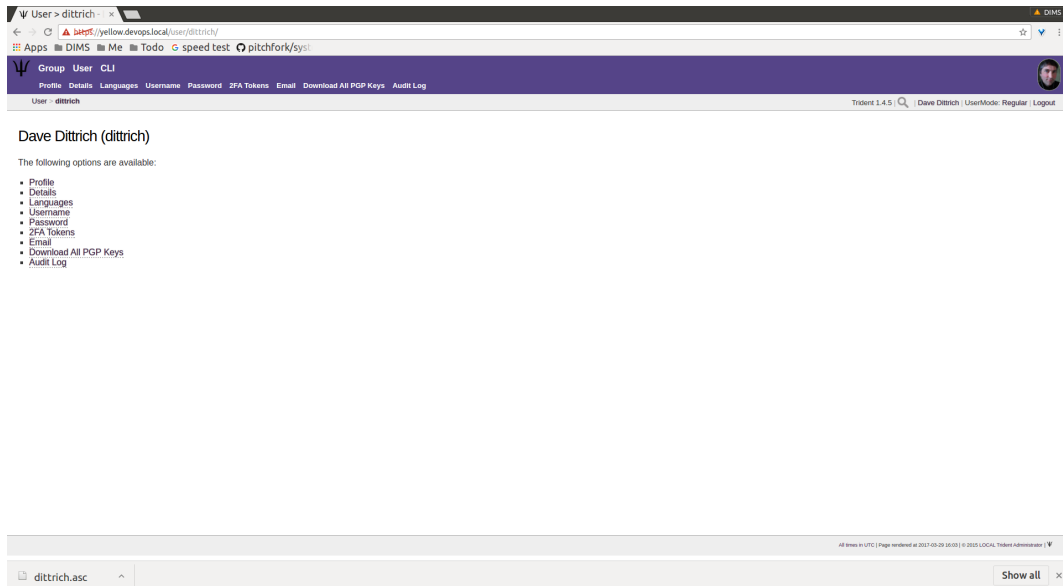


Fig. 1.27: Download PGP keys

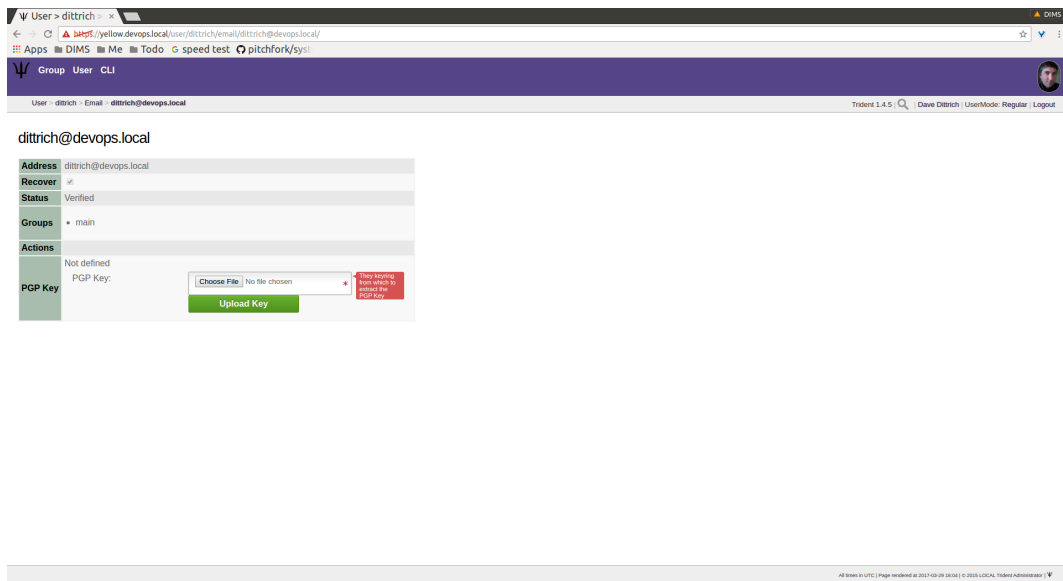


Fig. 1.28: Upload PGP key

What	User	Group	Who	Entered	Remote
Send Verification Code to dittrich@u.washington.edu	dittrich		dittrich	2017-03-29 09:00	192.168.56.1, 127.0.0.1
Added email address dittrich@u.washington.edu for member dittrich	dittrich		dittrich	2017-03-29 08:59	192.168.56.1, 127.0.0.1
Update member: id = dittrich property recover_email from "" to 'dittrich@devops.local'	dittrich		dittrich	2017-03-29 08:58	192.168.56.1, 127.0.0.1
Update member: id = dittrich property password	dittrich		trident	2017-03-29 08:56	192.168.56.1, 127.0.0.1
Update member: id = dittrich property airport from "" to 'SEA'	dittrich		trident	2017-03-27 17:56	192.168.56.1, 127.0.0.1
Update member: id = dittrich property tel_info from "" to '2063213551'	dittrich		trident	2017-03-27 17:56	192.168.56.1, 127.0.0.1
Update member: id = dittrich property im_info from "" to 'hla'	dittrich		trident	2017-03-27 17:56	192.168.56.1, 127.0.0.1
Update member: id = dittrich property affiliation from "" to 'DIMS'	dittrich		trident	2017-03-27 17:56	192.168.56.1, 127.0.0.1
Update member: id = dittrich property name_last from "" to 'Dittrich'	dittrich		trident	2017-03-27 17:56	192.168.56.1, 127.0.0.1
Update member: id = dittrich property name_first from "" to 'Dave'	dittrich		trident	2017-03-27 17:56	192.168.56.1, 127.0.0.1

Fig. 1.29: Audit log

1.2.2 Group Management

This section will cover group activities and attributes a member of a trust group may view or manage. The user must be a member of a trust group to be able to access any of the following pages.

Viewable Group Attributes

This subsection will cover attributes viewable from the Member, Airports, Contacts, and Vouches tabs.

First of all, to view a list of groups of which a user is a member, click the Group tab in the top row of any page (Figure *Trust group list*).

To see more information about a certain group, click one of the links in the list (Figure *Trust group attributes list*).

This presents a page with a list of links to all attributes viewable or manageable by the member. There are some activities the member may take part in, such as nominating and vouching for new group members, but, for the most part, a regular member may only view group attributes. Regular members are not allowed to change attributes about the group or its members. One notable exception is that regular members are allowed to nominate new users to a trust group and vouch for current members of a trust group. Nominating and vouching will be covered in Section Figure *Vouching for Trust Group Members*. For now, let's go over the attributes viewable by members.

The first link on the group home page, or the first tab in the second row of all group-related pages, is titled Members. Click either the link or the tab to go to a page listing all members in the current trust group (Figure *Trust group members list*).

Click on any member's username link to view their profile (Figures *Member profile, top*, *Member profile, middle*, *Member profile, vouches for*).

Within a trust group, any member's profile is viewable. At the bottom of the profile, there are lists of vouching activities of which the current member has been a part: vouches he has made or vouches other members have made for him. In the above example, another user vouched for the user dittrich, but he has not yet vouched for anyone.

In this next example, the user trident has vouched for another member, but has not yet been vouched for by any other member (Figure *Member profile, no vouches for*).

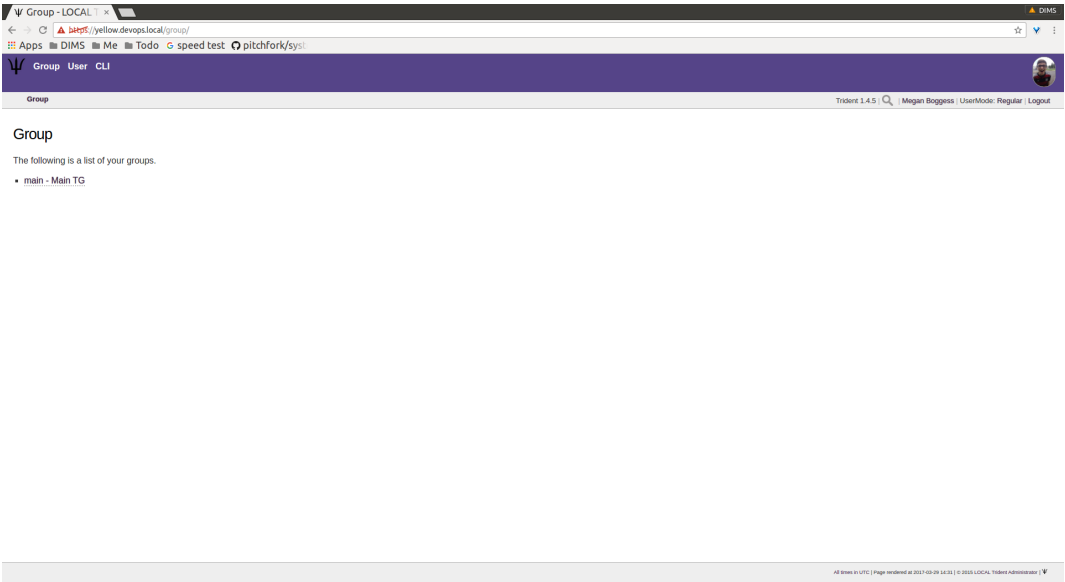


Fig. 1.30: Trust group list

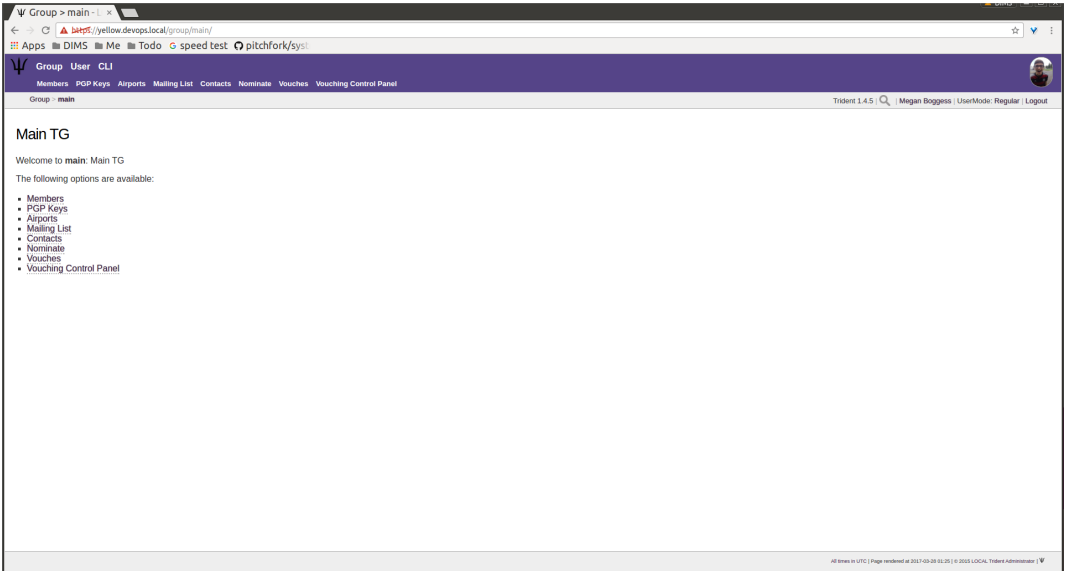


Fig. 1.31: Trust group attributes list

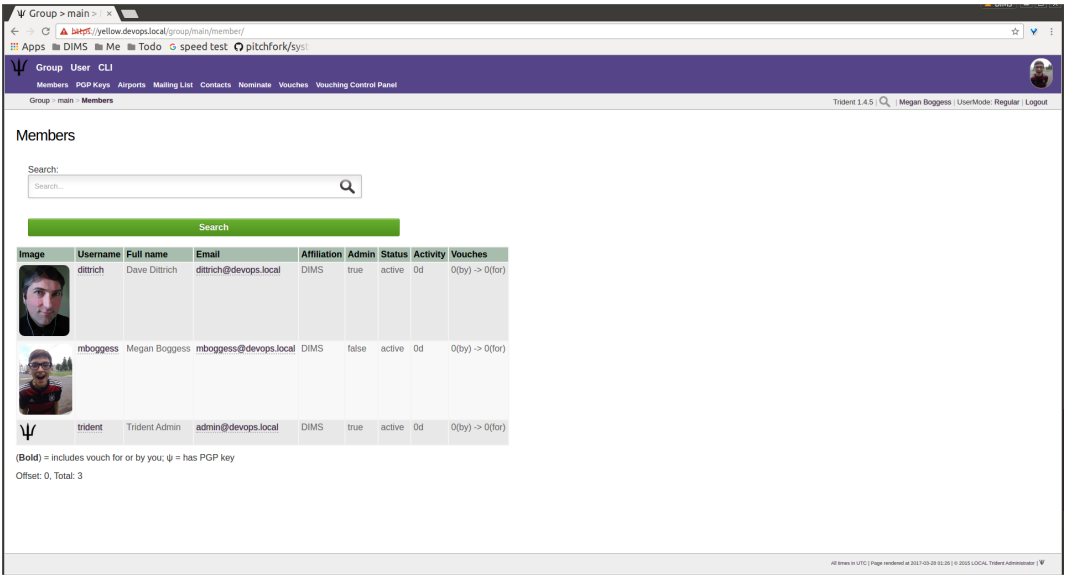


Fig. 1.32: Trust group members list

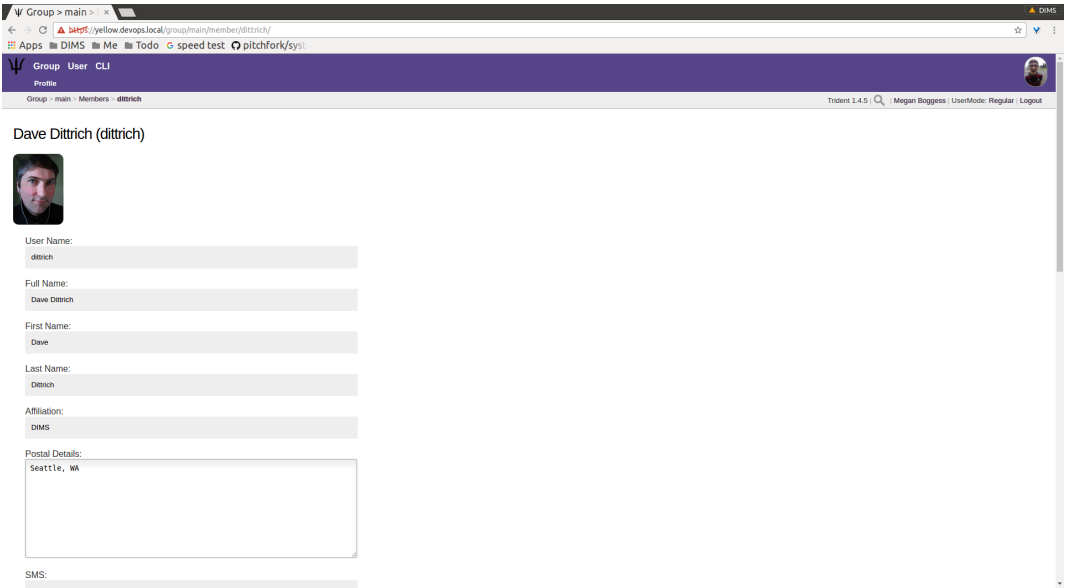


Fig. 1.33: Member profile, top

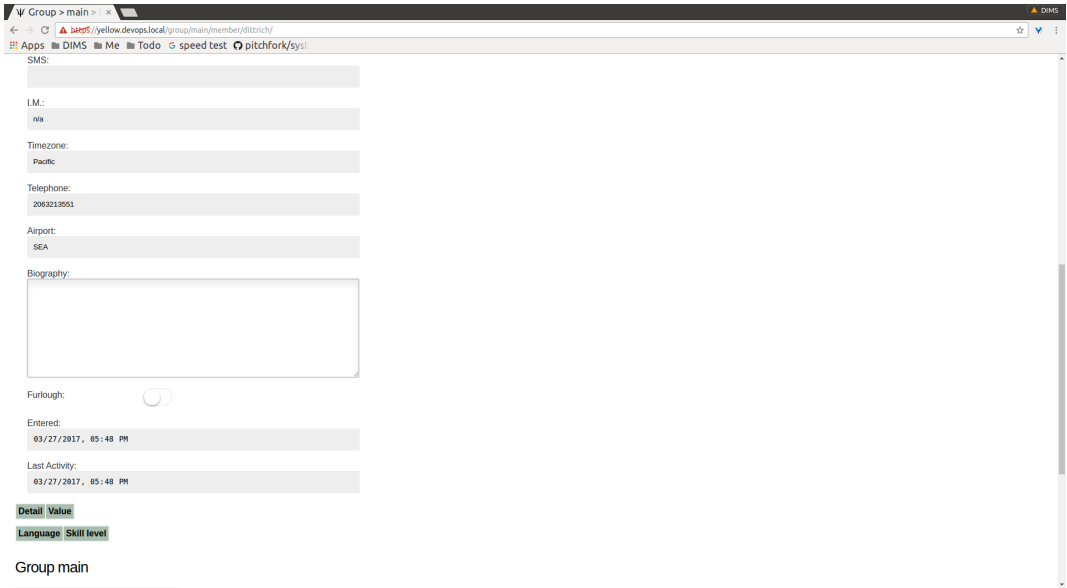


Fig. 1.34: Member profile, middle

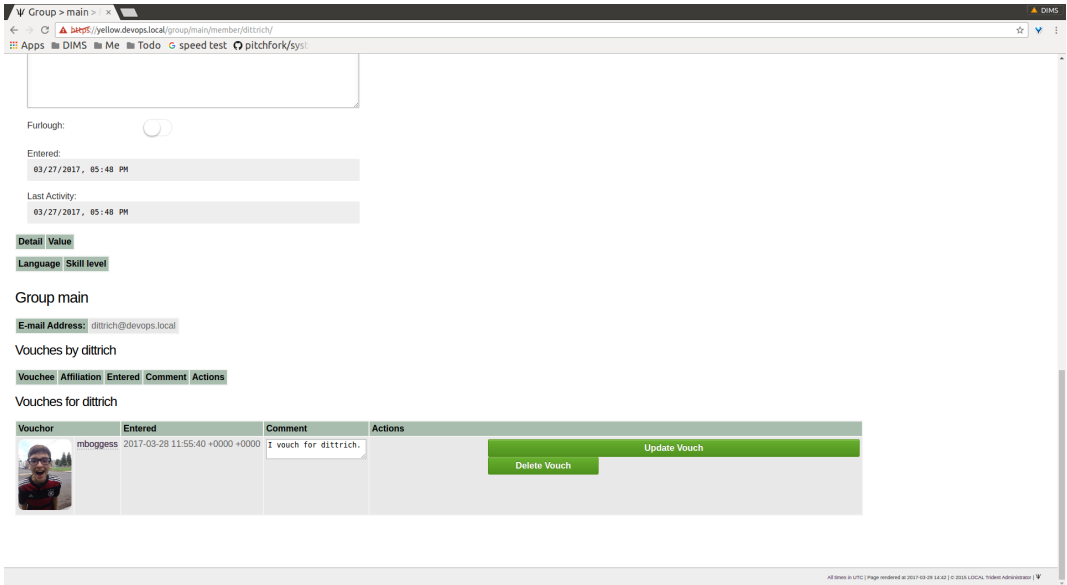


Fig. 1.35: Member profile, vouches for

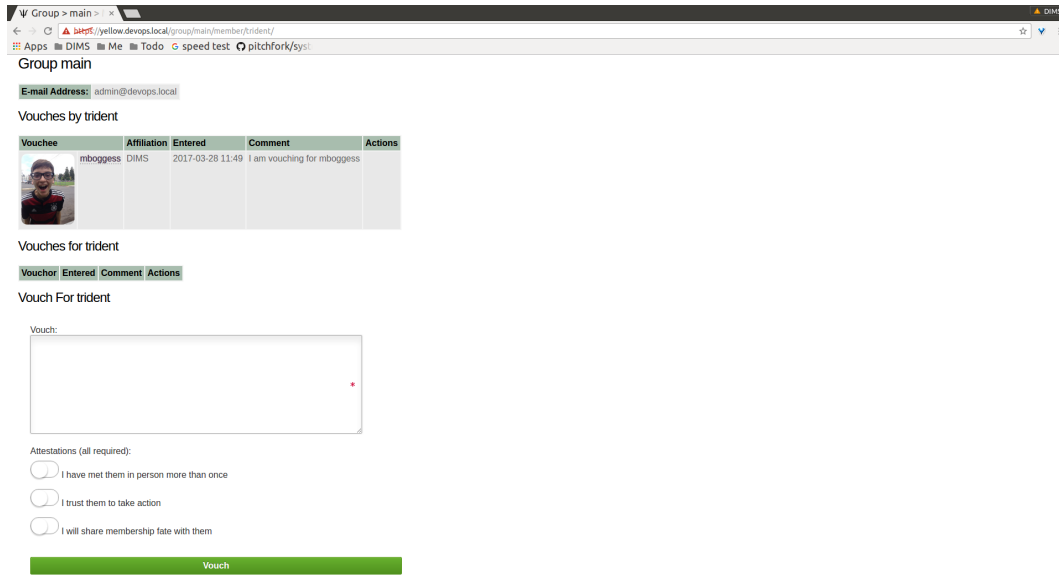


Fig. 1.36: Member profile, no vouches for

The `Airports` page (Figure [Airports list](#)) shows a list of airports members of the current trust group indicate as the airport nearest to them.

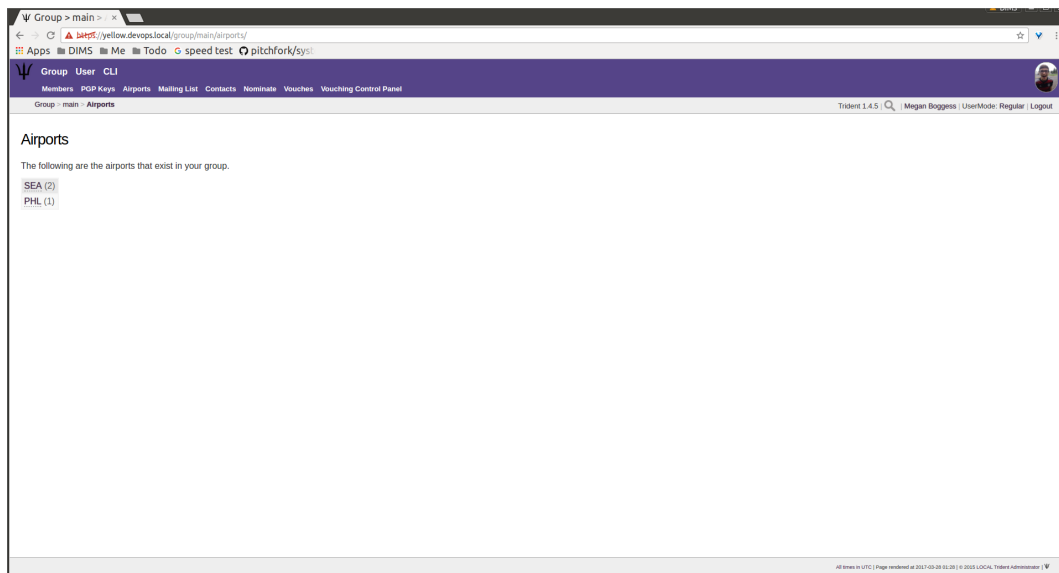


Fig. 1.37: Airports list

Click on any airport abbreviation in the list, and a new page will open with a list of members who have indicated the airport is the airport nearest to them (Figures [Members with PHL airport](#) and [Members with SEA airport](#)).

The `Contacts` page (Figure [Member contact list](#)) shows a list of members of the current trust group with their contact information, including affiliation, email, telephone, and SMS.

The `Vouches` page shows a list of all vouches made for members of the current trust group. This list indicates who was vouched for and by whom and on what date the vouch was made.

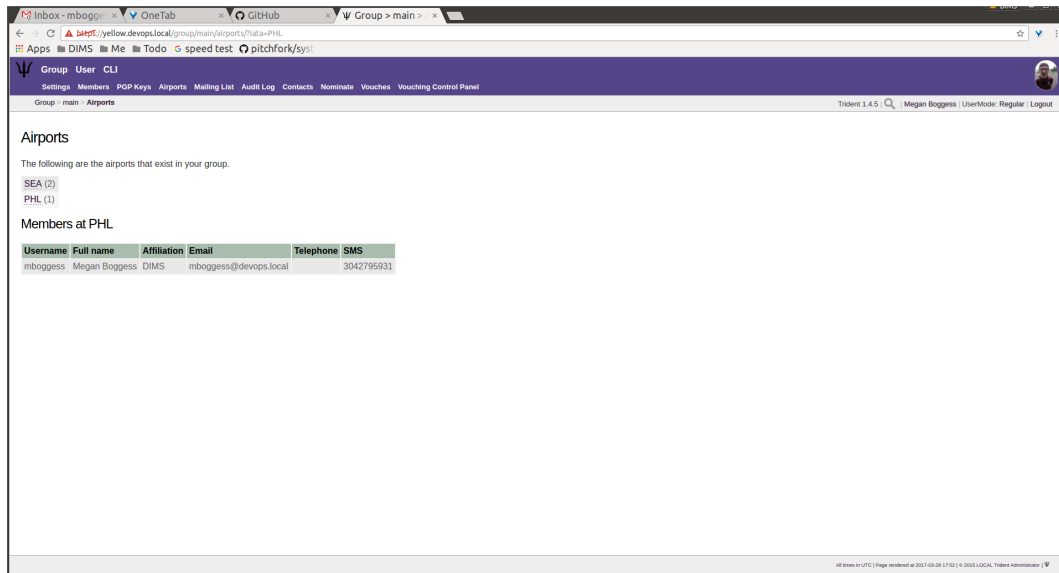


Fig. 1.38: Members with PHL airport

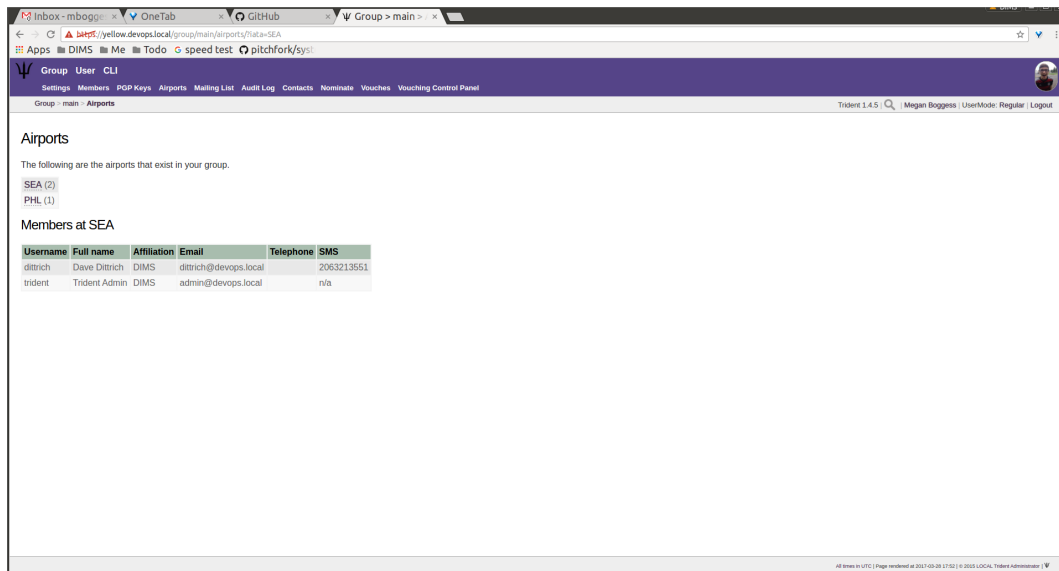
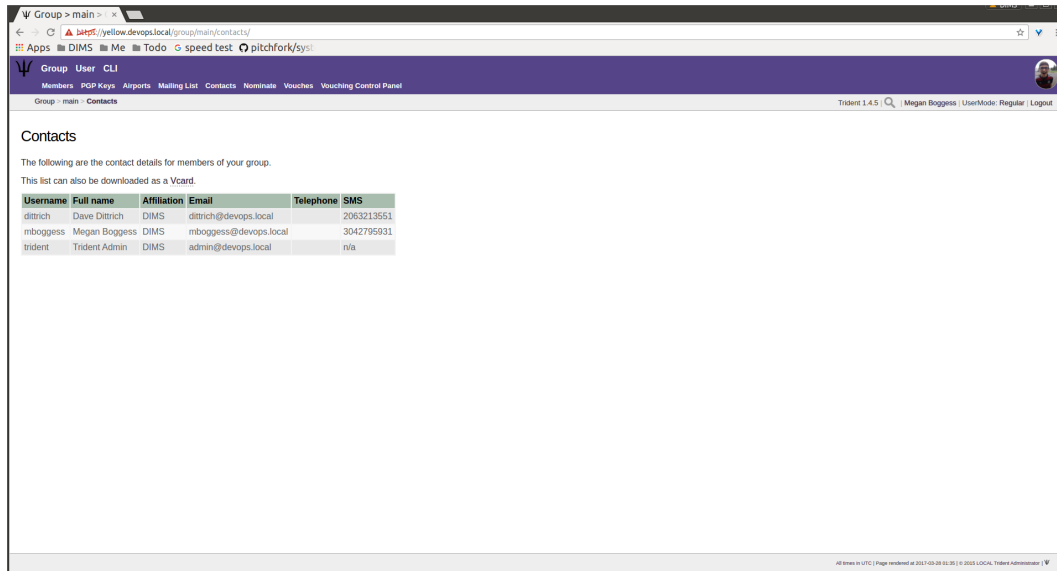


Fig. 1.39: Members with SEA airport



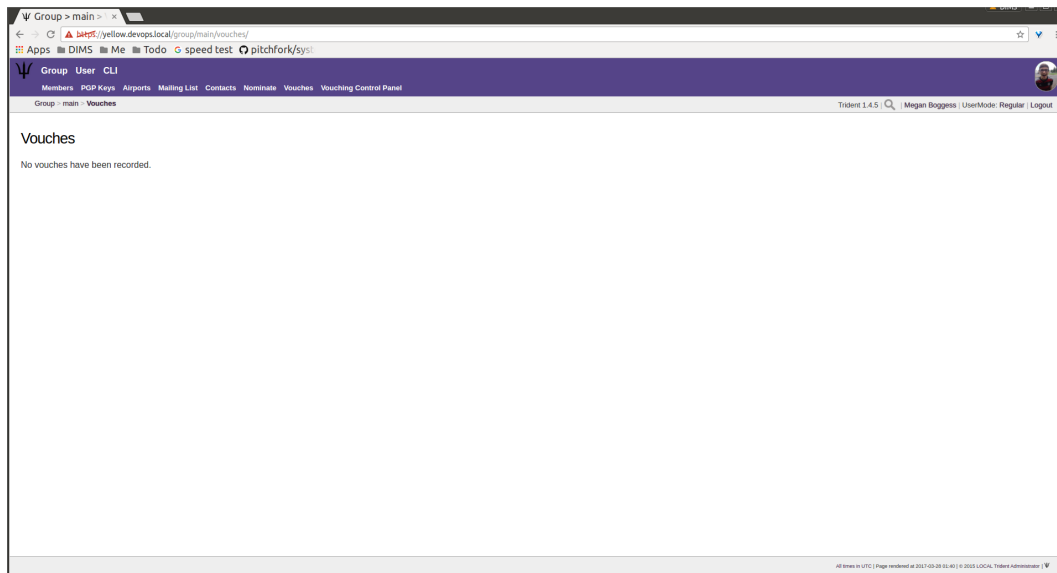
Contacts

The following are the contact details for members of your group.
This list can also be downloaded as a Vcard.

Username	Full name	Affiliation	Email	Telephone	SMS
dittrich	Dave Dittrich	DIMS	dittrich@devops.local	2063213551	
mboguess	Megan Boguess	DIMS	mboguess@devops.local	3042795931	
trident	Trident Admin	DIMS	admin@devops.local	n/a	

Fig. 1.40: Member contact list

If no vouches have been made yet, the page will be mostly blank (Figure *No vouches*):



Vouches

No vouches have been recorded.

Fig. 1.41: No vouches

Once at least one vouch has been made, a list will appear (Figure *Vouches made*):

Manageable Group Activities

This subsection will cover attributes and activities manageable from the PGP Keys, Mailing List, Wiki, Files, Nominate, and Vouching Control Panel tabs or links. Remember, the tabs will be found in the second row at the top of any group-related page and the links can be found listed on the group's main page.

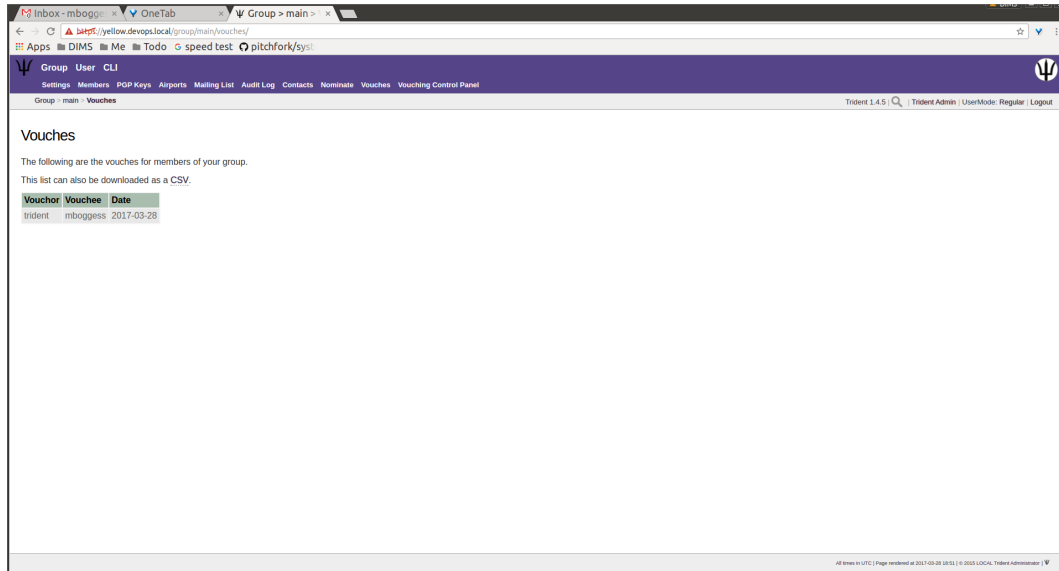


Fig. 1.42: Vouches made

The PGP Keys tab or link doesn't actually open a new page, it just downloads all PGP keys for the current trust group (Figure [Download PGP keys](#)).

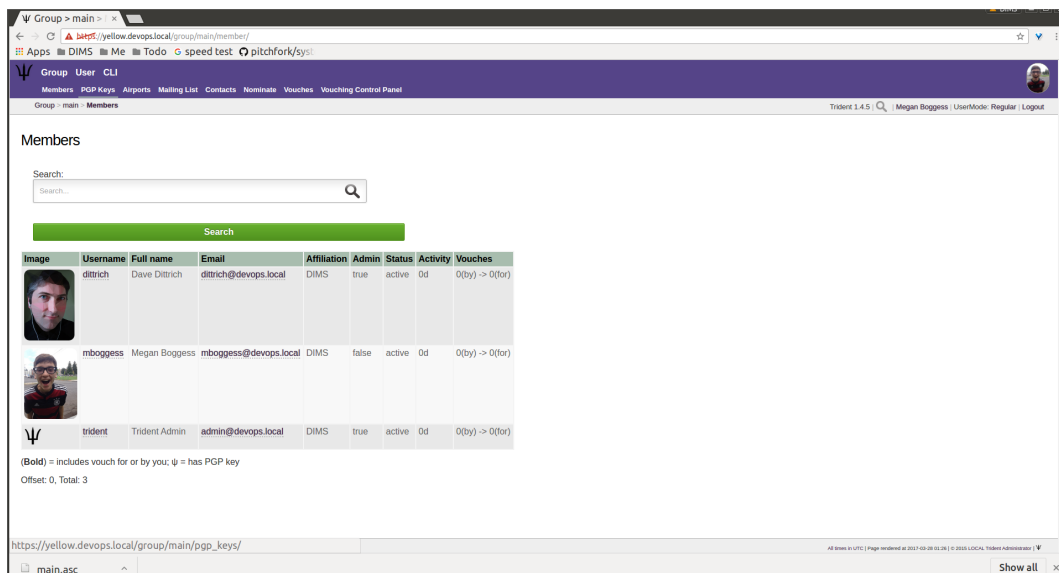


Fig. 1.43: Download PGP keys

The Mailing List tab or links opens a new page listing the current trust group's mailing lists and information about them (Figure [Mailing lists list](#)).

Click the link found in any row of the Shortname column to access a page listing members on that mailing list. Click the link in any row of the PGP column to download the PGP keys for that mailing list (Figure [Download list PGP keys](#)).

When new mailing lists are added, trust group members may have to manually add, or subscribe, themselves to the list.

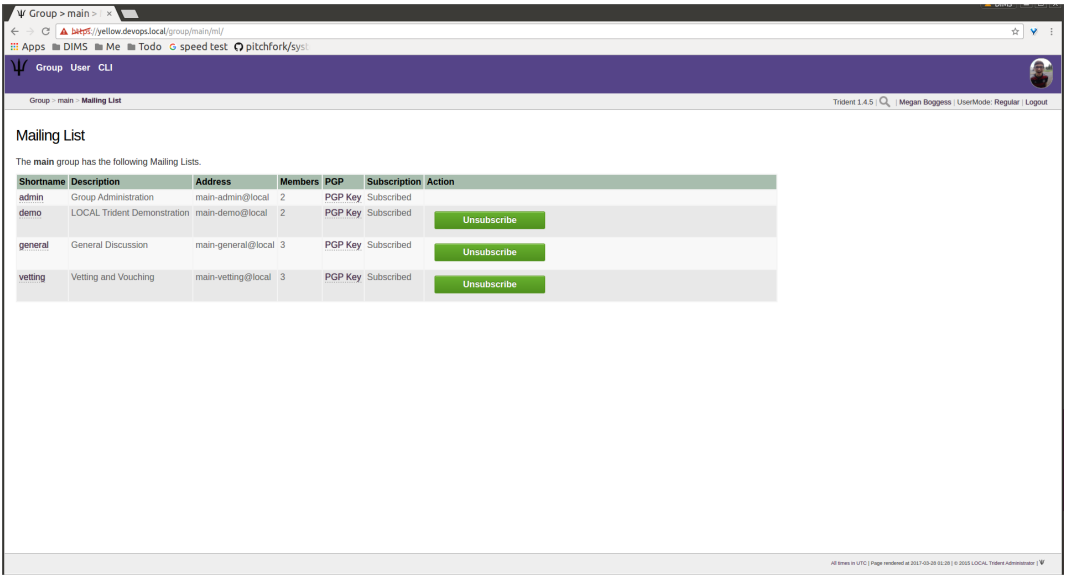


Fig. 1.44: Mailing lists list

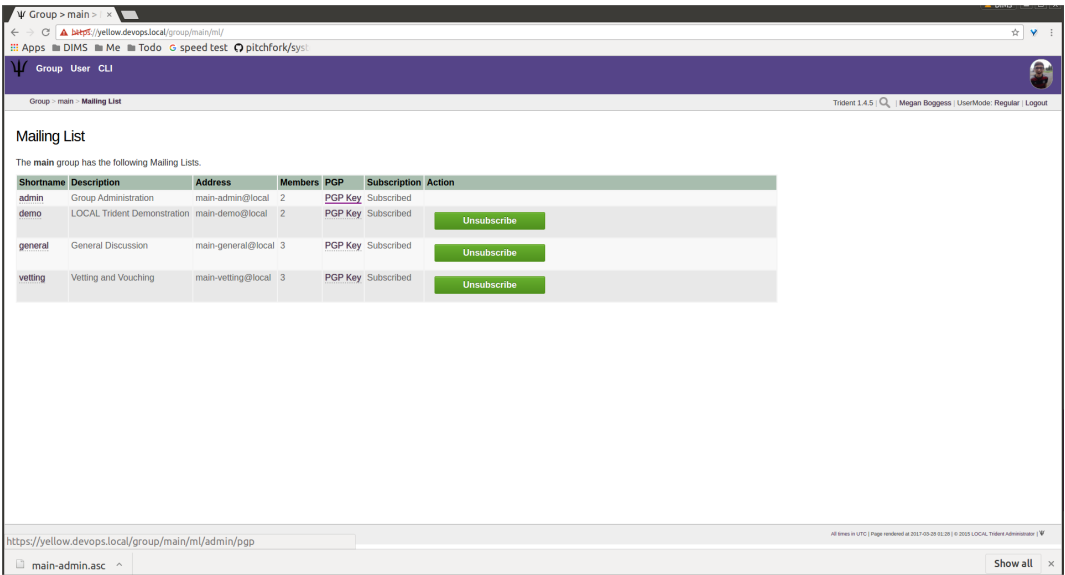


Fig. 1.45: Download list PGP keys

Click the `Subscribe` button found in the `Action` column of the mailing list in order to subscribe (Figure *Subscribe to new mailing list*).

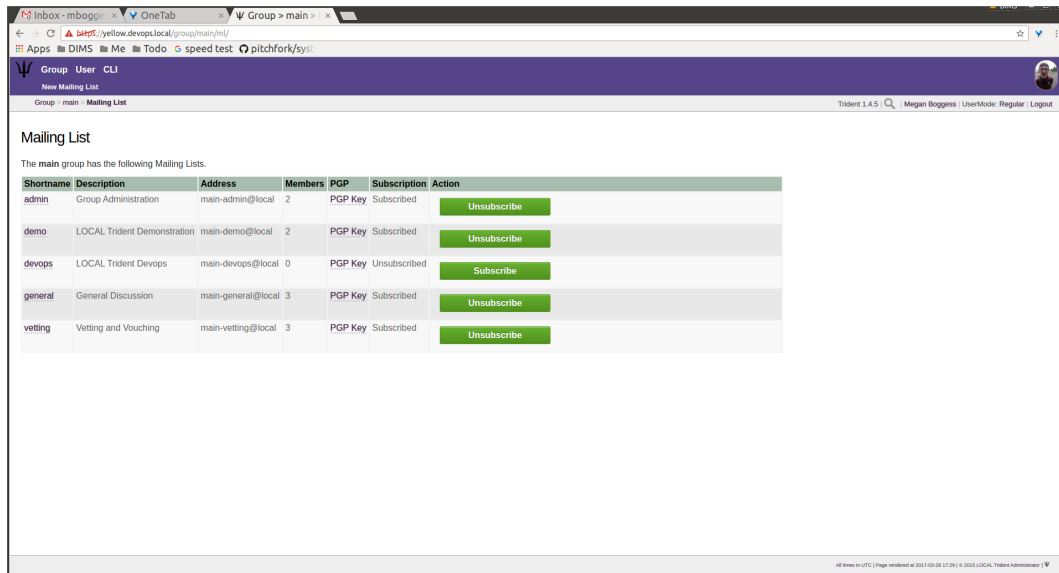


Fig. 1.46: Subscribe to new mailing list

Likewise, to unsubscribe to a mailing list and not receive email from that list any more, click the `Unsubscribe` button in the `Action` column of the mailing list from which to unsubscribe (Figure *Unsubscribe from mailing list*).

To return to either the user or group perspective, click the `User` or `Group` tabs in the top row of the page. If returning to a group, chose the group from the list of available trust groups.

The `Wiki` tab or link opens a new page showing the wiki's home page (Figure *Wiki home page*). The second row at the top of the page changes to be wiki-related tabs, rather than group-related tabs.

If no content has been added to the wiki before, as the image Figure *Wiki home page* shows, click the `edit me` link. This will open an editor (which is also the `Edit` tab).

Any page available to edit will have an editor view similar to what is shown in the image Figure *Wiki editor*. Once all edits have been completed, add a summary in the `Edit Summary` field, then click the `Save Revision` button.

Once the edit has been saved, a new page will be available to view, with the edits made (Figure *Wiki edit made*).

Use the `Source` tab (Figure *Wiki source*) to see the markdown source and its HTML preview for the wiki home page. This page will also contains a link to the raw markdown file.

To see a history of edits made to the wiki, use the `History` tab (Figure *Wiki edit history*).

The next tab, `Options`, pages can be moved, deleted, and/or copied (Figures *Wiki options, top*, *Wiki options, bottom*).

The `Child Pages` tab (Figure *Empty child pages*) lists any child pages of the wiki. Click on the `Path` links to list any child pages of that root page. Click the `View` link in the `Action` column to view any of the child pages. If no child pages have been added, as is the case in image Figure *Empty child pages*, just the root paths will be shown.

To add more child pages, go to the `New Page` tab (Figure *Create a new page*). Name the page, then click the `Create New Page` button.

This will open an editor page where the new wiki page can be written (Figure *Edit a new page*).

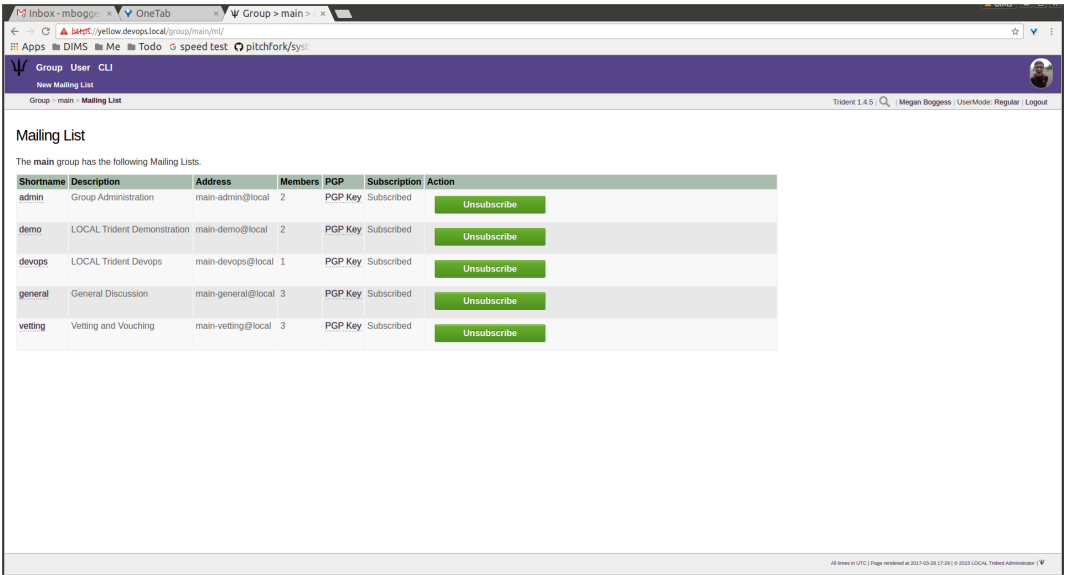


Fig. 1.47: Unsubscribe from mailing list

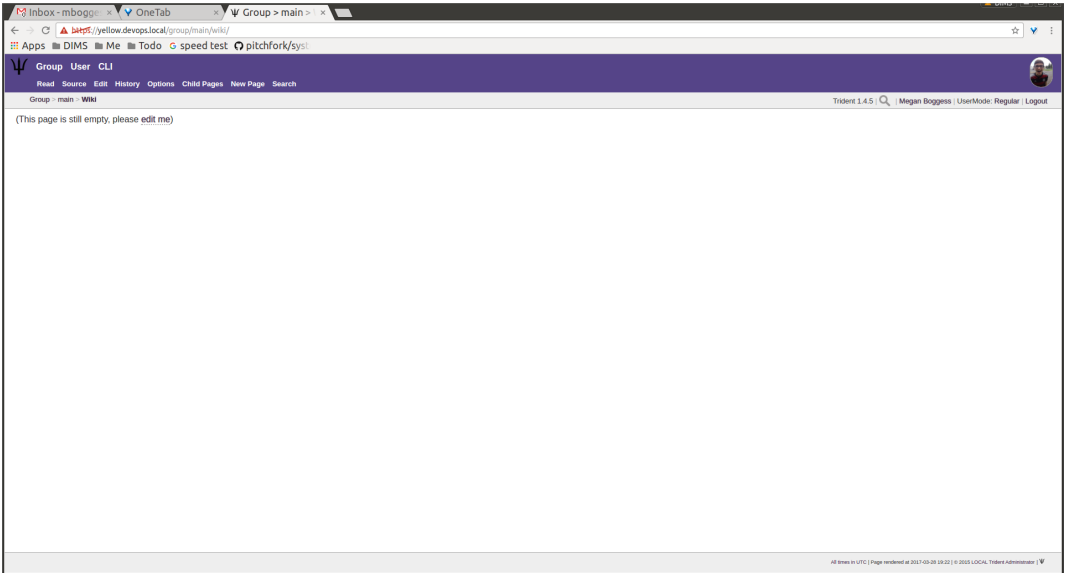


Fig. 1.48: Wiki home page

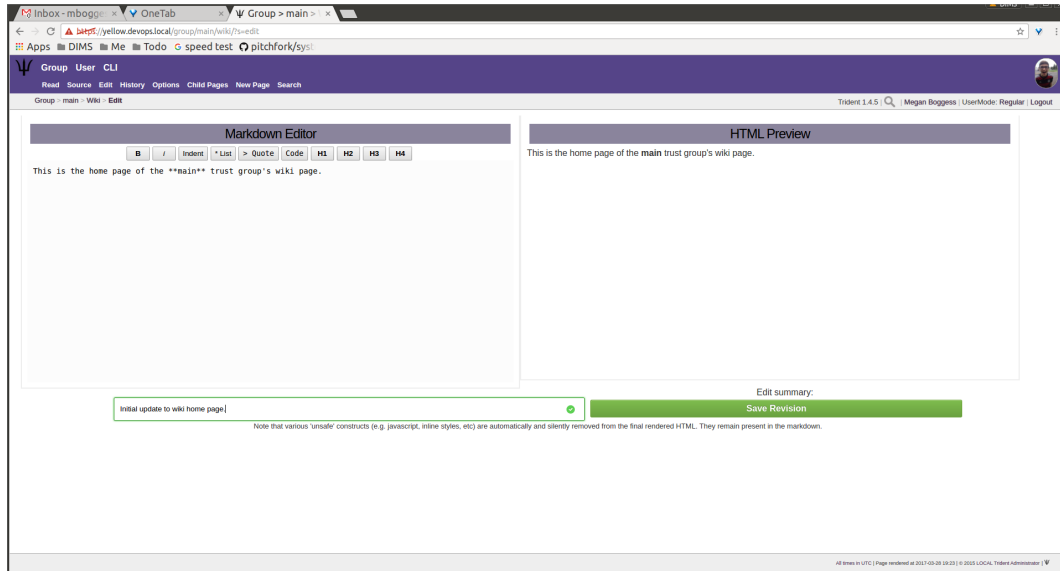


Fig. 1.49: Wiki editor

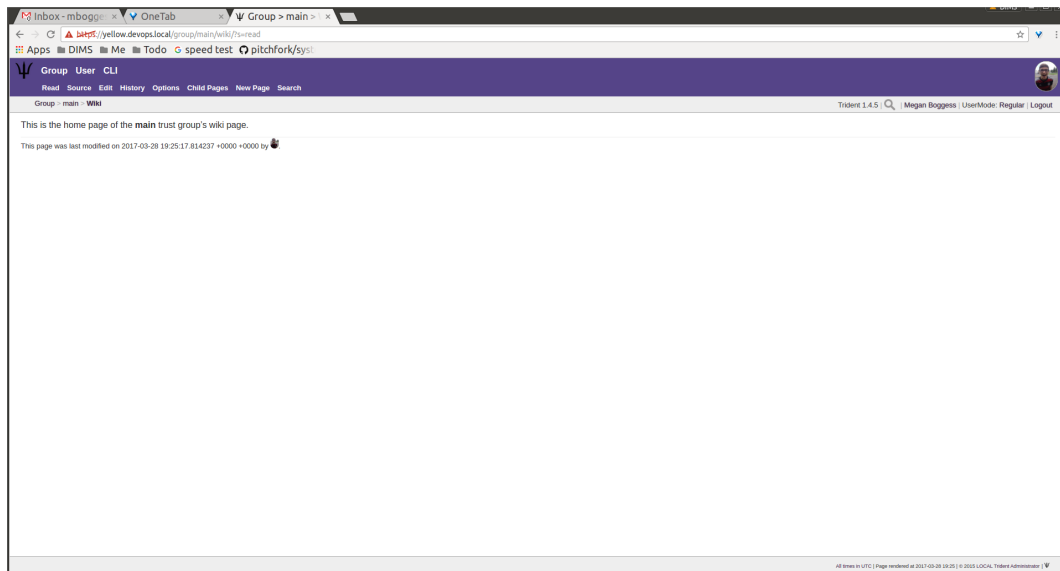


Fig. 1.50: Wiki edit made

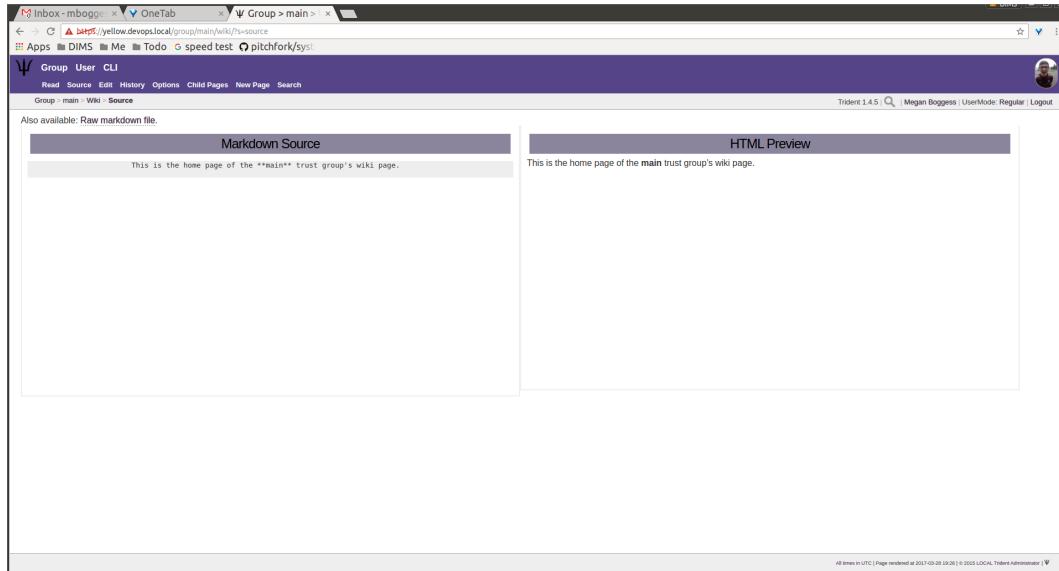


Fig. 1.51: Wiki source

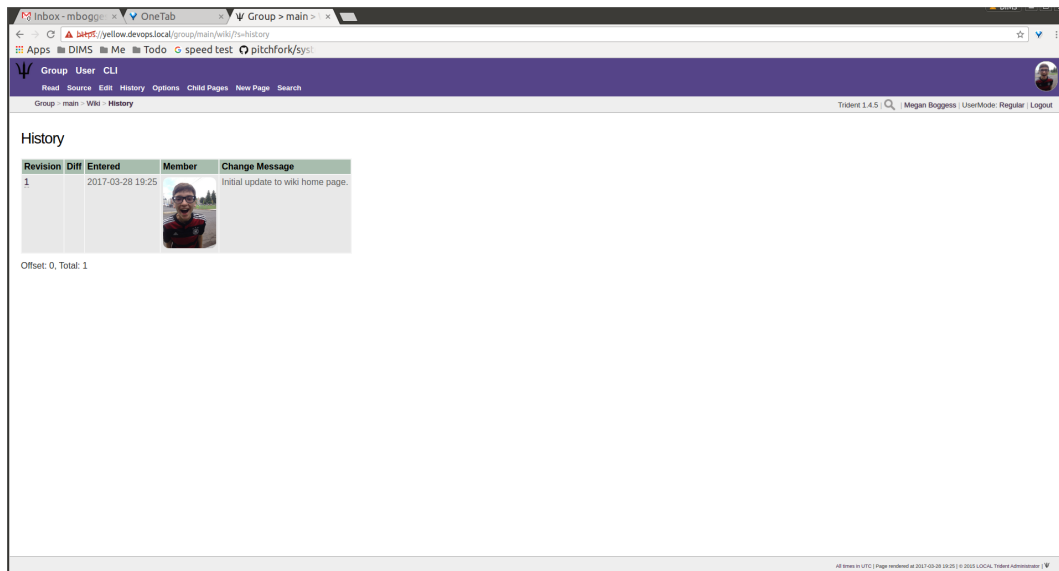


Fig. 1.52: Wiki edit history

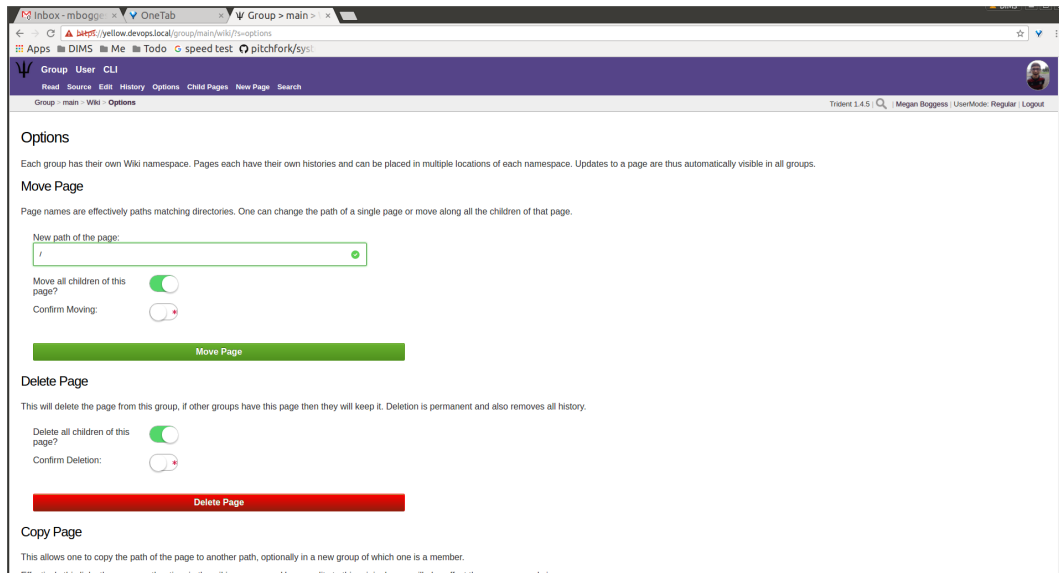


Fig. 1.53: Wiki options, top

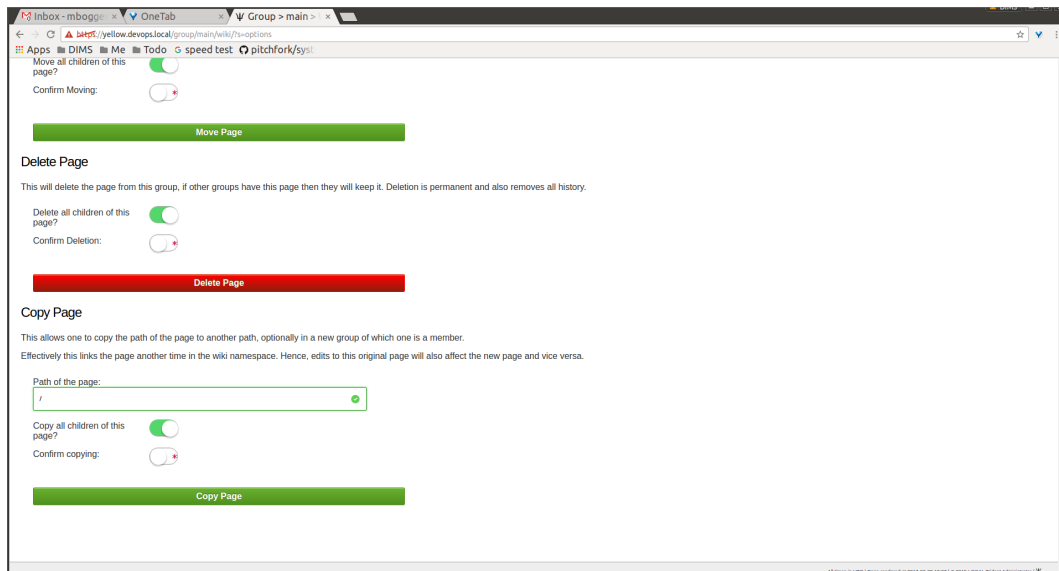


Fig. 1.54: Wiki options, bottom

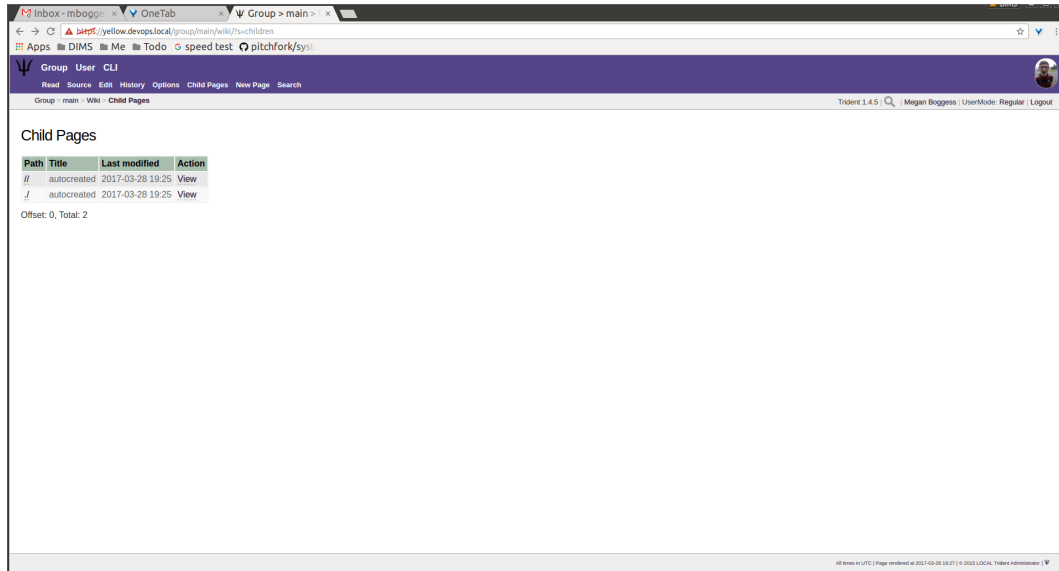


Fig. 1.55: Empty child pages

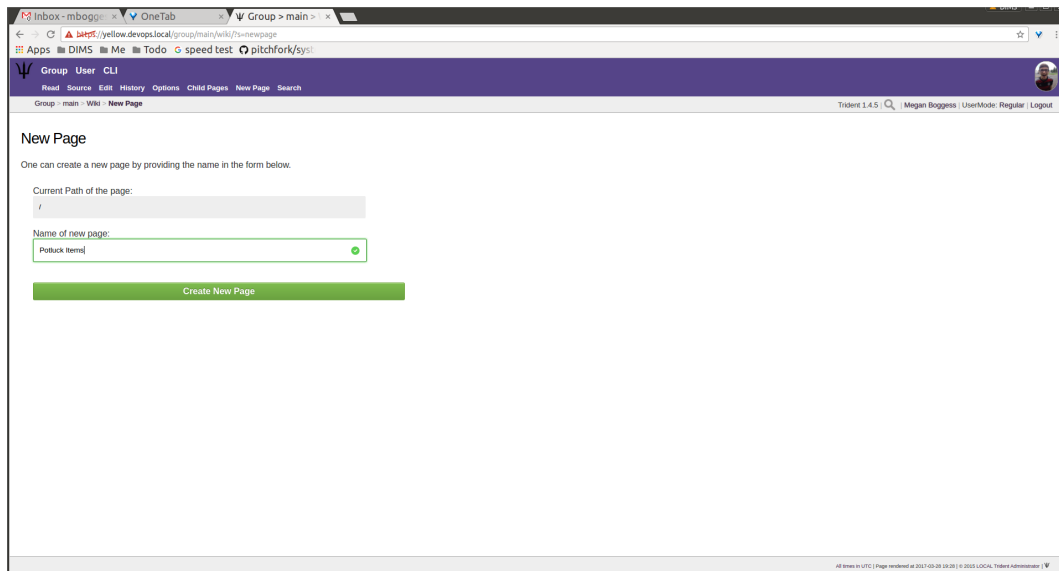


Fig. 1.56: Create a new page

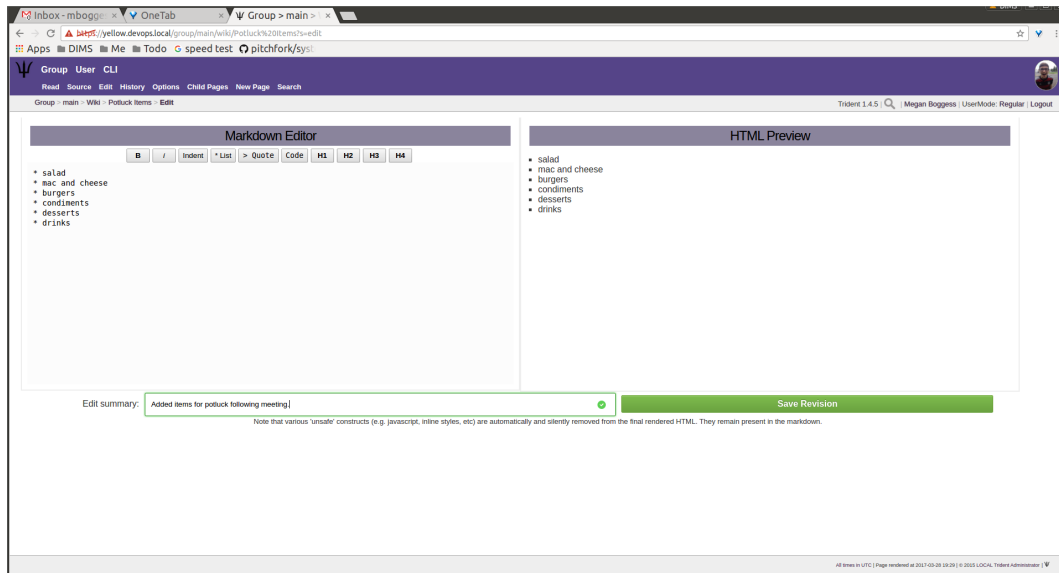


Fig. 1.57: Edit a new page

Once edits are complete, give a summary of the edits in the `Edit Summary` field, and click the `Save Revision` button. This will open a new page, showing the new page (Figure [New wiki page](#)).

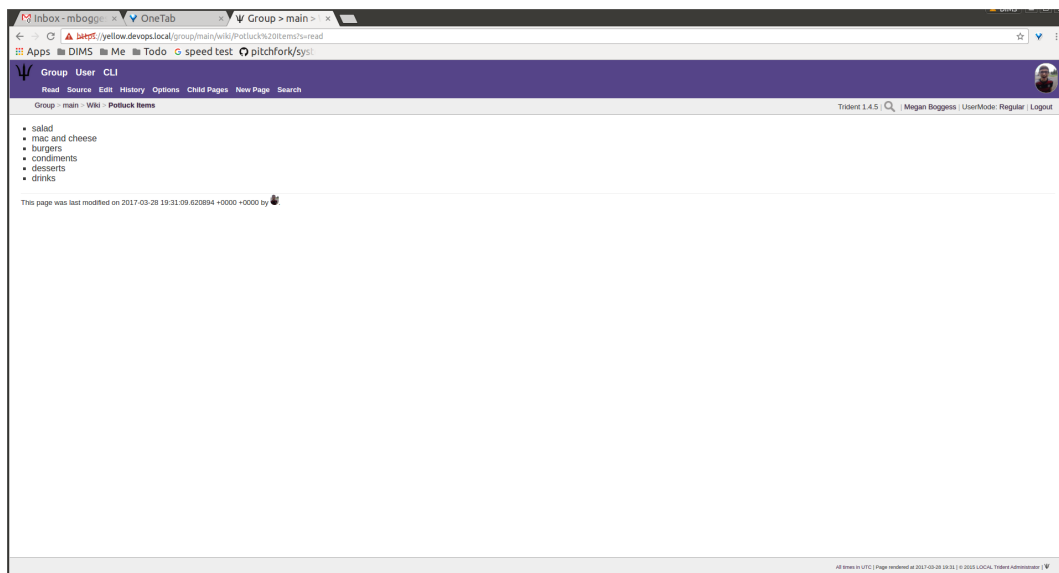


Fig. 1.58: New wiki page

This automatically updates the list of child pages found on the `Child Pages` page (Figure [Child pages list updated](#)).

Searches through all the wiki pages available to the current trust group is possible (Figure [Wiki search](#)).

When done editing the wiki, to return to either the user or group perspective, click the `User` or `Group` tabs in the top row of the page. If returning to a group, chose the group from the list of available trust groups.

The `Files` link or tab (Figure [Files home page](#)) organizes files for the current trust group. Members can add both

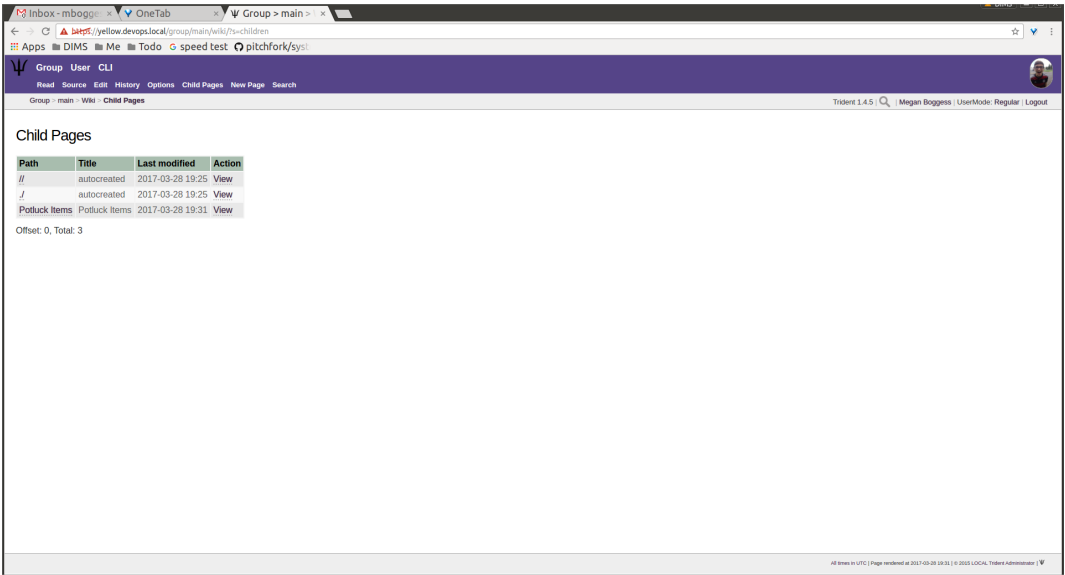


Fig. 1.59: Child pages list updated

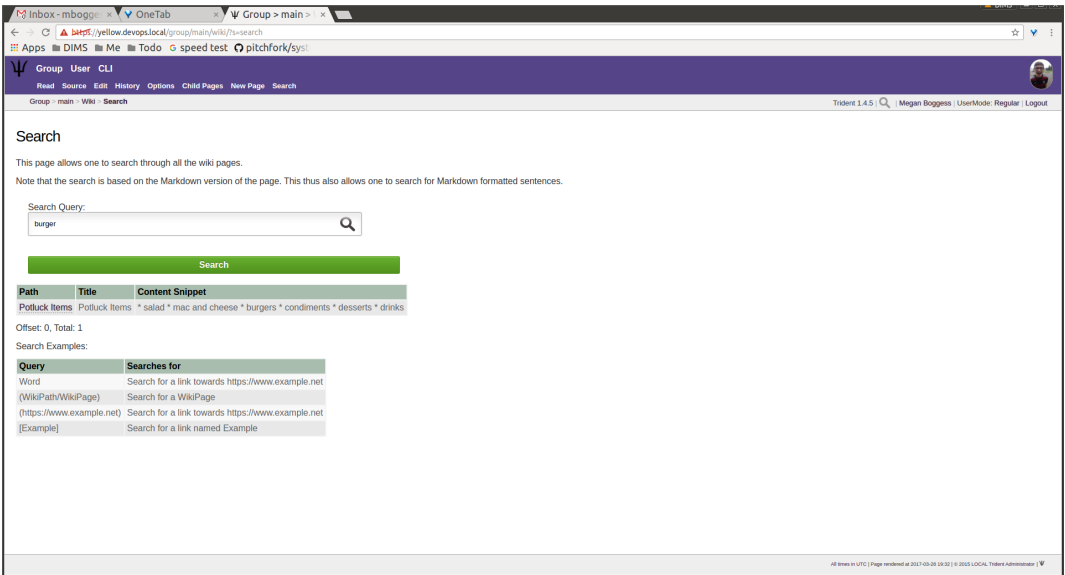


Fig. 1.60: Wiki search

directories and files, view a list of available artifacts, and view the available artifacts. If no files or directories have been added, the Files home page will only show two buttons, an Add a new file button and an Add a new directory button. Otherwise, it will show a list of available directories, as well as the Add buttons.

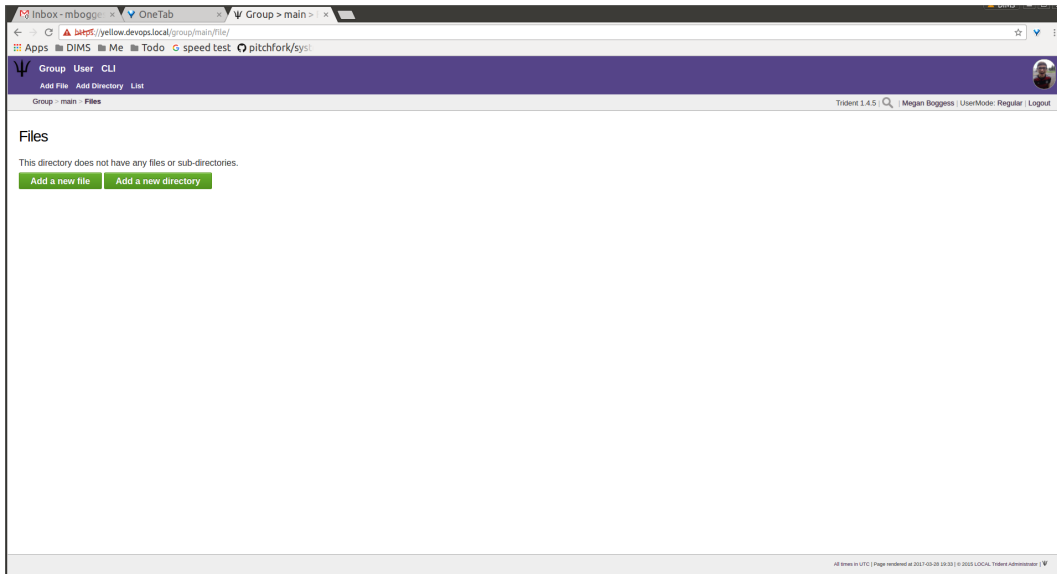


Fig. 1.61: Files home page

To add a directory, use the Add Directory tab (Figure [Add directory](#)) in the second row at the top of the page, or the Add a new directory button from the Files home page.

To add a new directory, the filepath of the new directory is required and a brief description of the directory is optional. Then click the Create new directory button.

The home page list of directories will be updated accordingly (Figure [Available directories updated](#)).

To add a file, click either the Add File tab or the Add a new file button from the Files home page. This takes opens a new page. Name the file, give a description, and choose the file from the local filesystem. Then, click the Create new file button (Figure [Add a new file](#)).

Once submitted, a new page will show that the file has been uploaded and to which path. It also gives some statistics about the current directory and files (Figure [Confirmation of a new file](#)).

The Files home page is also updated, but it is a little subtle when only a file has been added (Figure [Home page file add confirmation](#)).

The only difference is that the 'Total' count has gone up by one. If a new file is added to the root path, the file itself would show up, and the count would increase. Since the added file is stored in the logs directory, it is hidden on this page. Click the Path link for any subdirectories to get a list of files or more subdirectories in that directory.

The List tab opens the Files home page, listing available directories and files.

Again, to return to group or user settings, click the Group or User tabs in the top row of the page.

1.2.3 Vouching for Trust Group Members

For a new user to become a member of a trust group, she must be vetted by existing members of the trust group. This is accomplished by other *vouching* for the prospective new user.

The screenshot shows the 'Add Directory' form in the Trident web interface. The browser address bar shows the URL `http://yellow.devops.local/group/main/file?ps=add_dir`. The page title is 'Group > main > Add Directory'. The form includes a 'Current path:' field with the value `/`. Below it is a 'Filepath of new directory:' field with the value `/logs` and a green checkmark. The 'Description of new directory:' field has the value `Share log files here` and a green checkmark. A green 'Create new directory' button is at the bottom. The page footer shows 'Trident 1.4.5' and 'Megan Boggess | UserMode: Regular | Logout'.

Fig. 1.62: Add directory

The screenshot shows the 'Files' page in the Trident web interface. The browser address bar shows the URL `http://yellow.devops.local/group/main/file`. The page title is 'Group > main > Files'. The table below shows the updated directory list:

Path	Details	Size	Revision	Last modified
/logs/	Details		1	2017-03-28 19:35

Offset: 0, Total: 1

Buttons: Add a new file, Add a new directory

The page footer shows 'Trident 1.4.5' and 'Megan Boggess | UserMode: Regular | Logout'.

Fig. 1.63: Available directories updated

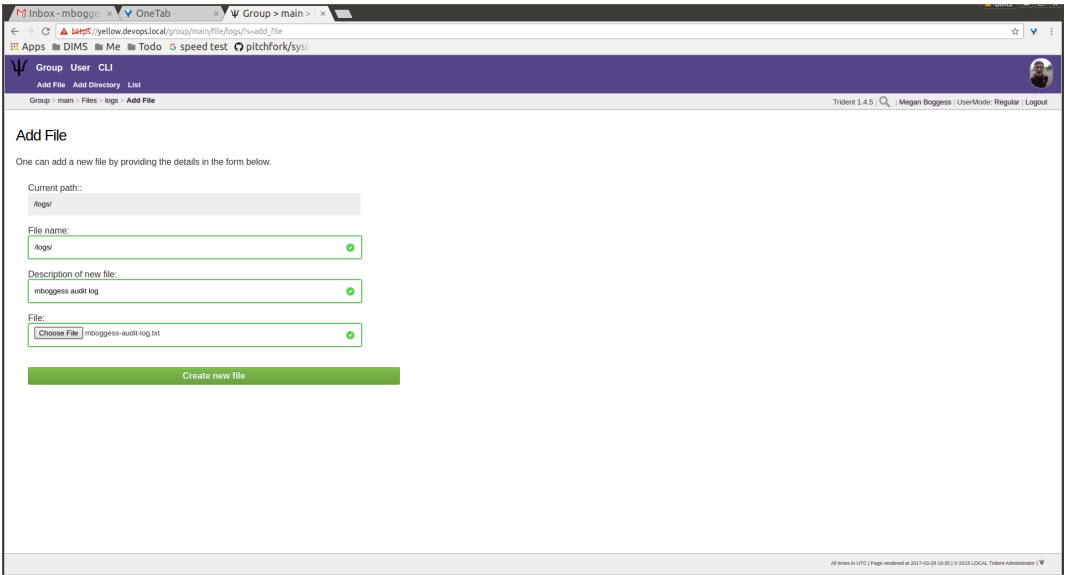


Fig. 1.64: Add a new file

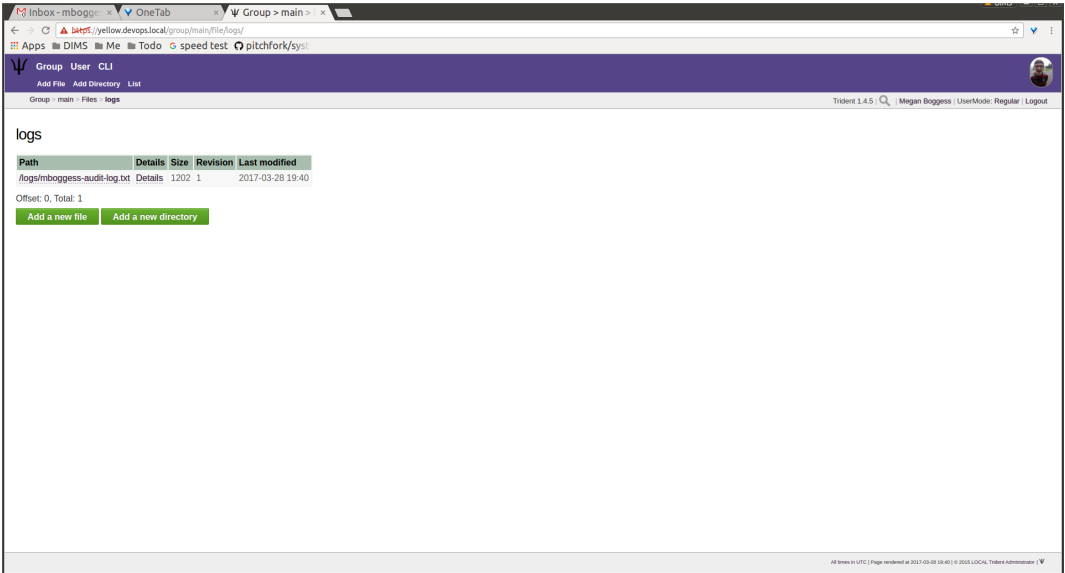


Fig. 1.65: Confirmation of a new file

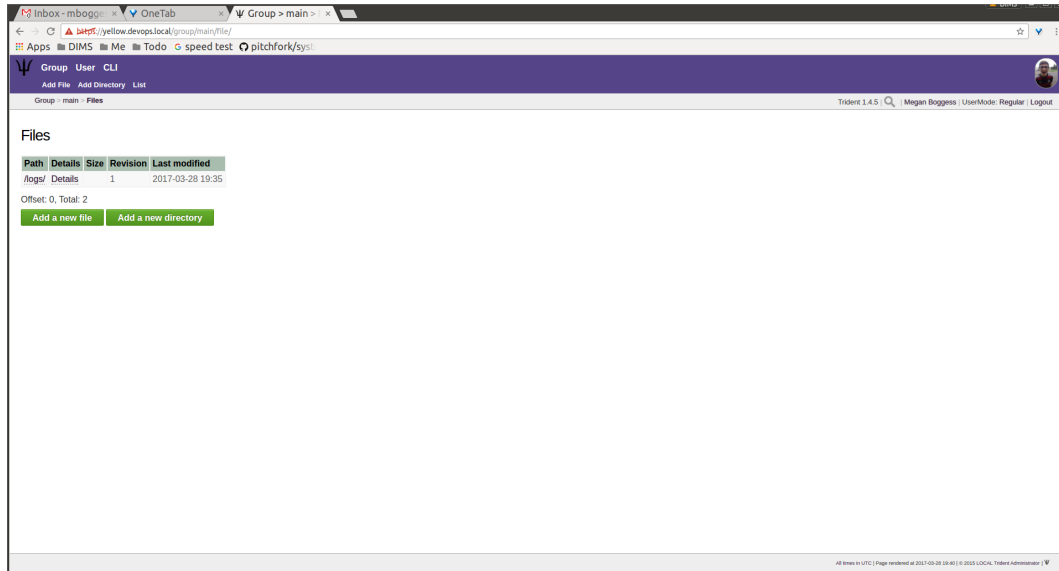


Fig. 1.66: Home page file add confirmation

Caution: In a trust group where very sensitive information is shared, the vouching process is a serious matter that is not to be taken lightly. When you vouch for someone, that should mean that you personally *know* the person, have *met* them in person, have worked with them on a project demanding *trust* so you have first-hand experience with them and you believe trust is warranted in that person. If this person should violate the trust of the group by improperly sharing or exposing extremely sensitive information, not only could they be kicked out of the trust group, but anyone who *vouched for them* could also be removed (if the violation was severe enough.) A breakdown in trust in a group that shares highly sensitive information can potentially damage the trust fabric of the group such that the effectiveness of the group is lost.

Each trust group may have unique requirements about the number of vouches a user must obtain before she will be permitted to become a member of the trust group. For our training guide, only one vouch is required for membership. Most groups will have more significant requirements.

Vouching is not required only for member admittance, but vouches are recorded and available for visualization or for network analysis to identify cliques, strength of the trust network, etc.

There are three ways for a trust group member to vouch for another member: vouch for a member through the member's profile, nominate a user through the group's profile, and use the `Vouching Control Panel`.

The first way to vouch for a member is through the member's profile. This means the user must already be a member of the trust group, and has already been vouched for enough times to meet the current trust group's requirements for membership.

To see what vouches have already been made, go to a trust group's main page and click the `Vouches` tab. To start vouching for a member, click the `Members` tab or link, then choose the user. This opens his profile page. Scroll all the way to the bottom of the profile, and there is a form section where a comment can be written regarding the vouch to be made and attestations about relationship with the member (Figure [Member profile, blank vouch section](#)).

Fill in the form, then click the `Vouch` button (Figure [Member profile, filled-in vouch section](#)).

Once a vouch is recorded, it will be visible on that member's profile forever (though vouches can be updated, or deleted it, if necessary). Outbound vouches *from* the member are listed right above inbound vouches *to* the member (Figure [Member profile, vouch made](#)).

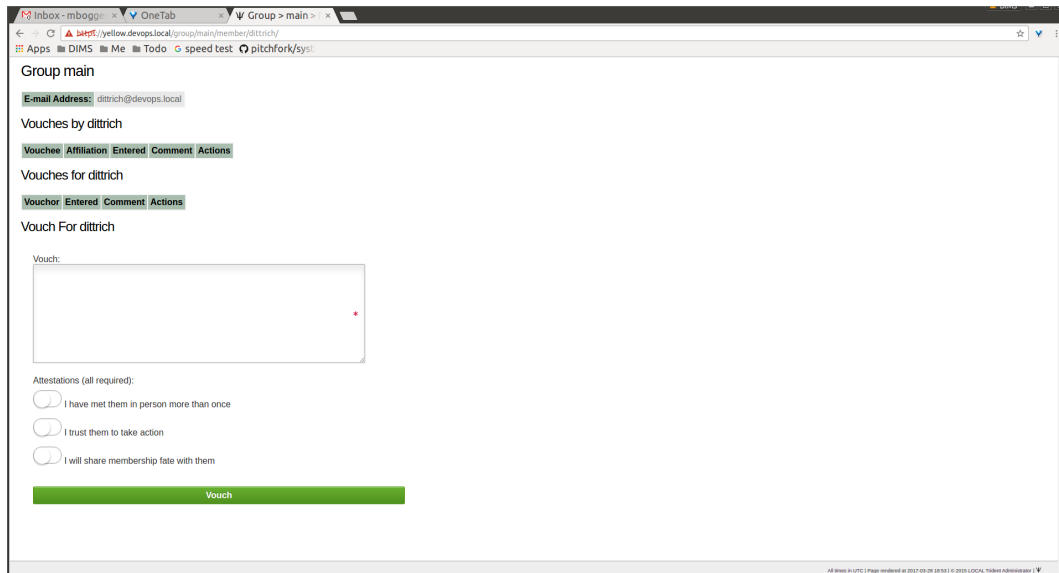


Fig. 1.67: Member profile, blank vouch section

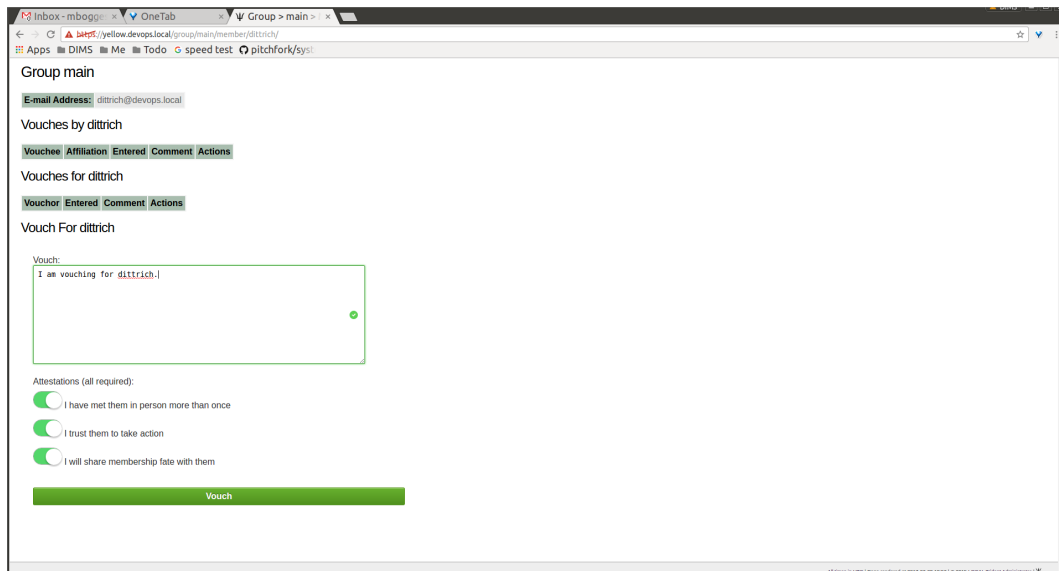


Fig. 1.68: Member profile, filled-in vouch section

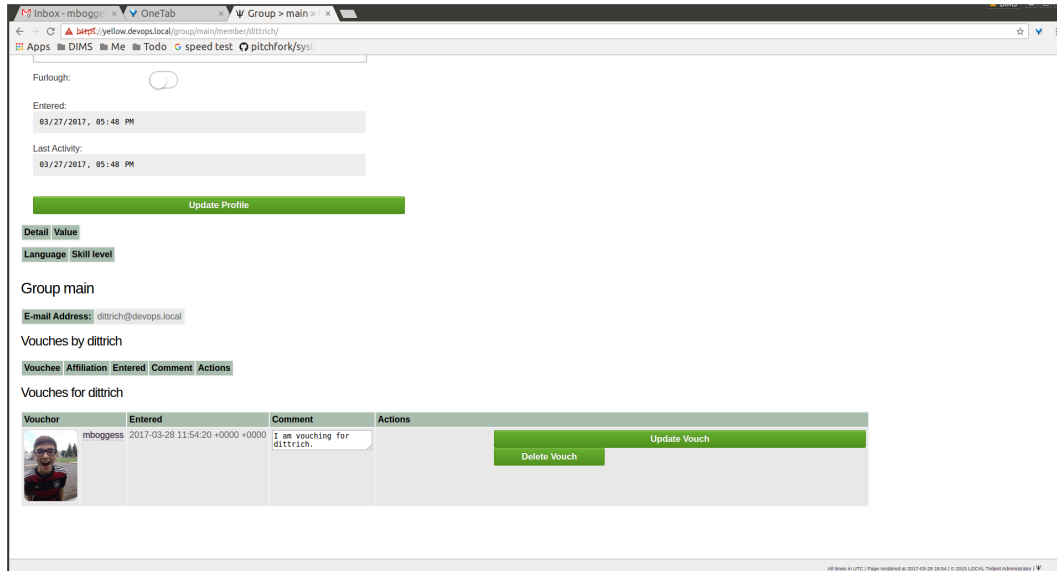


Fig. 1.69: Member profile, vouch made

The typical way to start the process of onboarding a new trust group member is to *nominate* them. Go to the home page of the group to which the user should be nominated. The `Nominate` tab opens a page which to start the process of nominating a user to the trust group. First, the user must exist in the system. Then, search for the user by the email address associated with their account.

Attention: Standard practice is to *not mention* the existence of the trust group to the prospective member before you nominate them. Should they not receive sufficient vouches to be added to the trust group, it will be an uncomfortable conversation trying to explain why you were not able to get them into the group. Some in the trust group may feel like a degree of breach of trust may have occurred from disclosing the existence of the trust group to the public. If someone in the group negatively vouches (i.e., raises a red flag about the trustworthiness of the nominee), it may necessitate an internal policy discussion to adjudicate the situation, which can make the nominee feel slighted and cause a great deal of consternation or bad feelings.

Fill in the email in the `Search email` field, and click the `Search` button (Figure [Search for a user to nominate](#)).

If there is a user tied to the given email address, the user will show up in a list on the next page. Click the `Select` button to continue (Figure [User search results](#)).

Part of the nomination process is vouching for the user. A trust group will have its own requirements, but, in general, any given trust group will require a user to obtain a certain number of vouches in order for them to be vetted into the trust group.

A vouch form opens in the page that follows the selection of a user to nominate. Write a comment about the reason for vouching for the user, then toggle the three attestations to confirm relationship with the user. Then, click the `Nominate` button (Figure [Vouch for a user](#)).

If the submission goes correctly, it is indicated at the bottom of the page (Figure [Successful nomination](#)).

Return to the `Members` page for the current trust group. The list of members is updated. The user `bob` had previously not been on the list of members, but now that member is there. The user's `Vouches` column is also automatically updated (Figure [Updated trust group members](#)).

The final way to vouch for members is to use the `Vouching Control Panel` found in a tab or link of the same name within the group perspective. This panel allows vouches to be submitted in batches (Figure [Vouching control](#)).

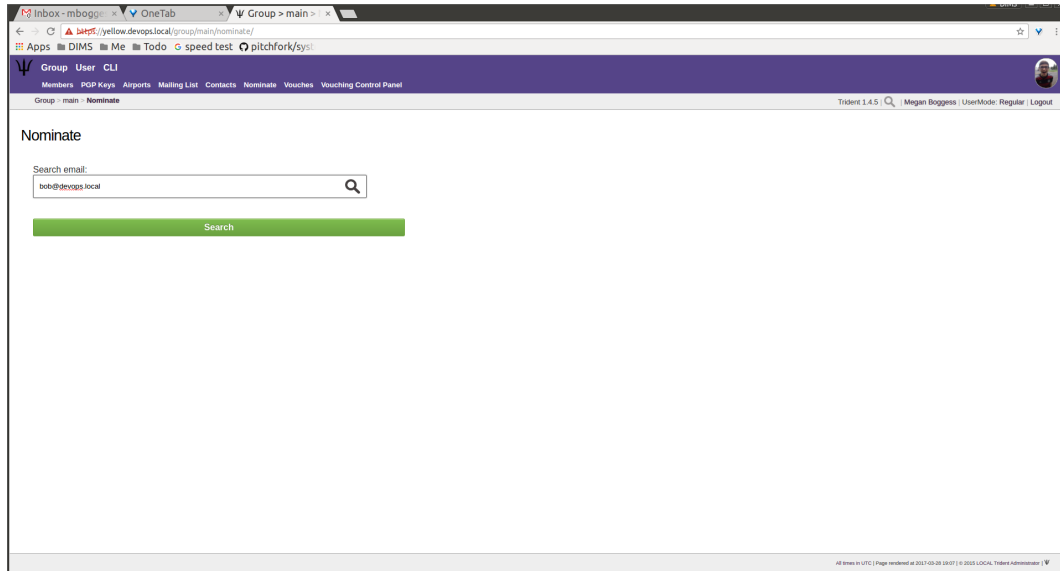


Fig. 1.70: Search for a user to nominate

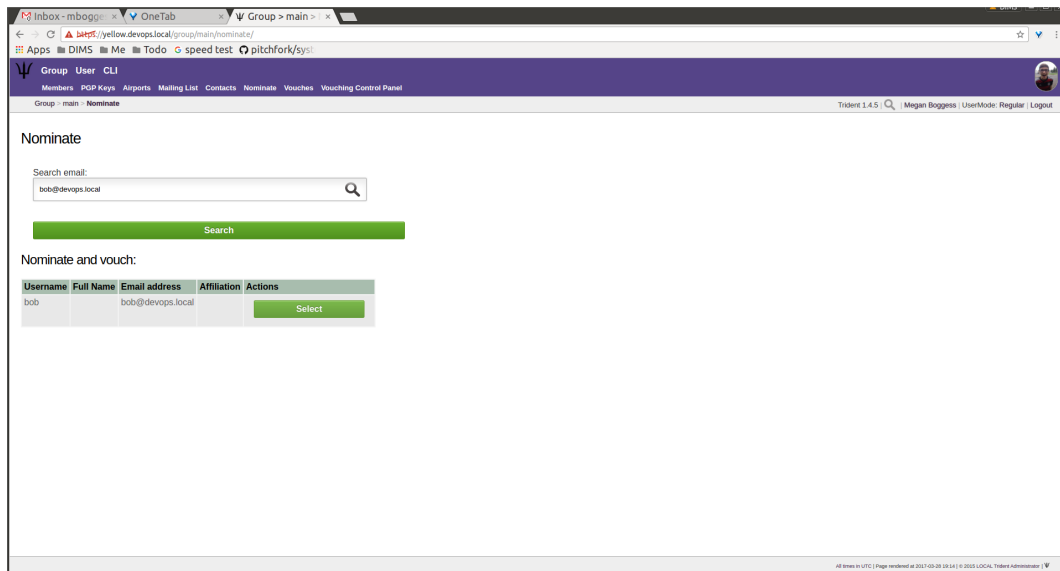


Fig. 1.71: User search results

The screenshot shows a web browser window with the URL `http://yellow.devops.local/group/main/nominate_existing/`. The page title is "Nominate existing user". Below the title, it says "Nominate an existing user". There are two bullet points: "Nominate: bob" and "For group: main". The "Username:" field contains "bob". The "Vouch comment:" field contains "I am vouching for bob." and has a green checkmark icon. Below the comment field, there are three radio buttons for "Attestations (all required)": "I have met them in person more than once", "I trust them to take action", and "I will share membership fate with them". All three are selected. At the bottom is a green "Nominate" button.

Fig. 1.72: Vouch for a user

The screenshot shows the same web browser window as Fig. 1.72, but the "Vouch comment:" field is now empty and has a red asterisk icon. Below the "Attestations" section, there is a green "Nominate" button and a green checkmark icon with the text "Nomination added".

Fig. 1.73: Successful nomination

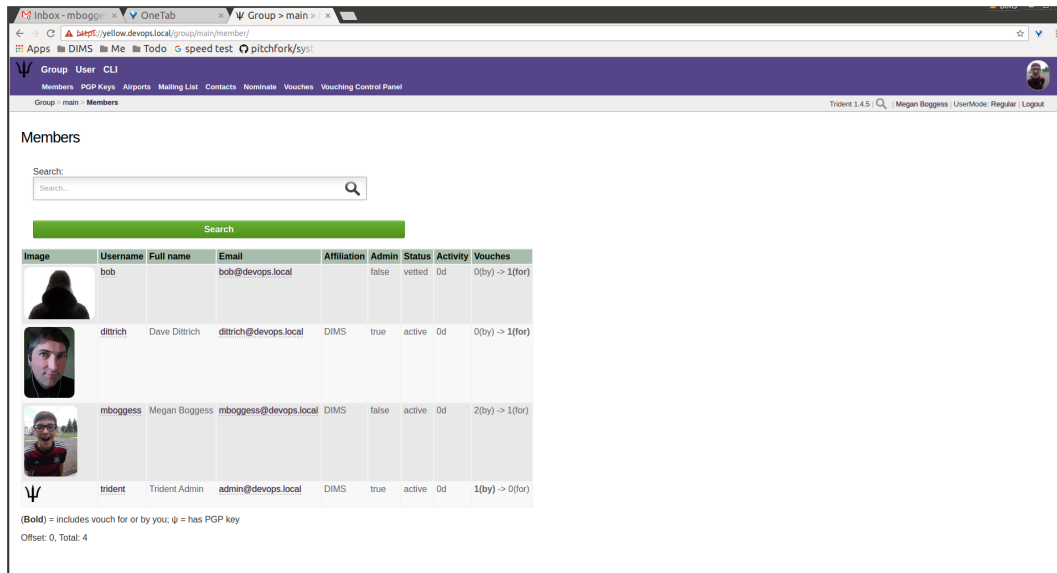


Fig. 1.74: Updated trust group members

panel).

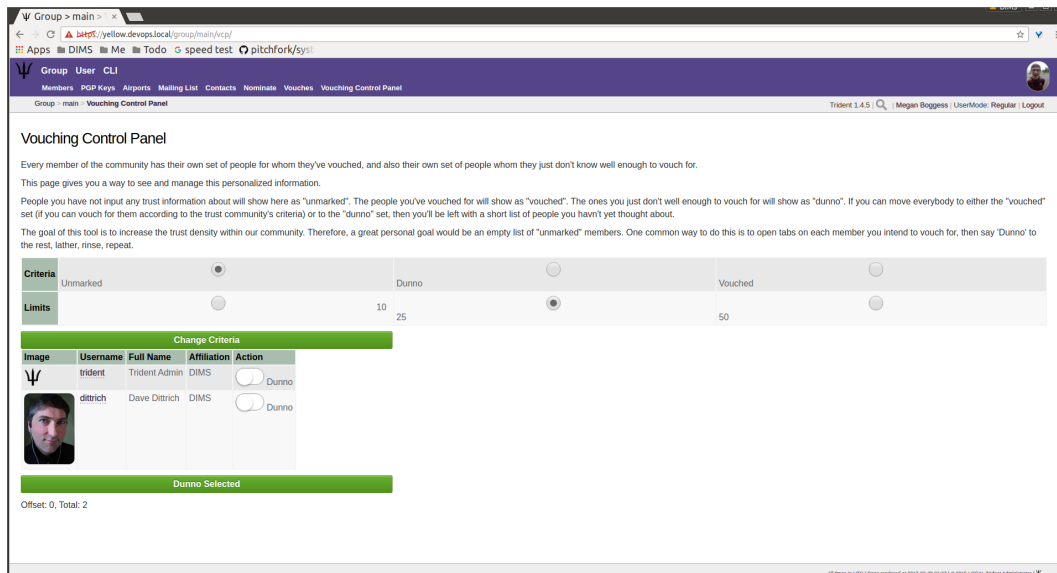


Fig. 1.75: Vouching control panel

There are two selections to make to form groups of members which can then be acted against all at one time. Choose a criteria (Unmarked, Dunno, or Vouched).

- Unmarked means there is no vouch established to date for those users.
- Dunno means there is no existing relationship or experience with the user.
- Vouched means the user already has a recorded vouch.

Then choose a limit to create the actual batch. To see the criteria, click the `Change Criteria` button.

Walk through the batch, and apply an action against each member by toggling the button in the `Action` column. Once all actions have been applied, click the button at the bottom of the list. Its name changes, depending on which action is being applied.

Those are all the tasks a member of a trust group can perform. To see tasks for admins of trust groups or for system administrators, please see the other chapters in this document (Section *Trust Group Administration Activities* and Section *System Administration Activities*, respectively).

1.3 Trust Group Administration Activities

This chapter serves as a training guide for people who will be administering and managing trust groups using a Trident portal system. It includes activities such as setting trust group policies for vetting, vouching, and idle timeouts, resetting user passwords, adding users manually, and more. Only trust group administrator members are allowed to view or manage these tasks.

1.3.1 Admin Password Reset

There is one user-related activity that only a trust group administrator can manage: initiating the reset of a password for another user (Figure *Admin password reset for user*). Make sure to confirm via the toggle before clicking the `Request Password reset` button.

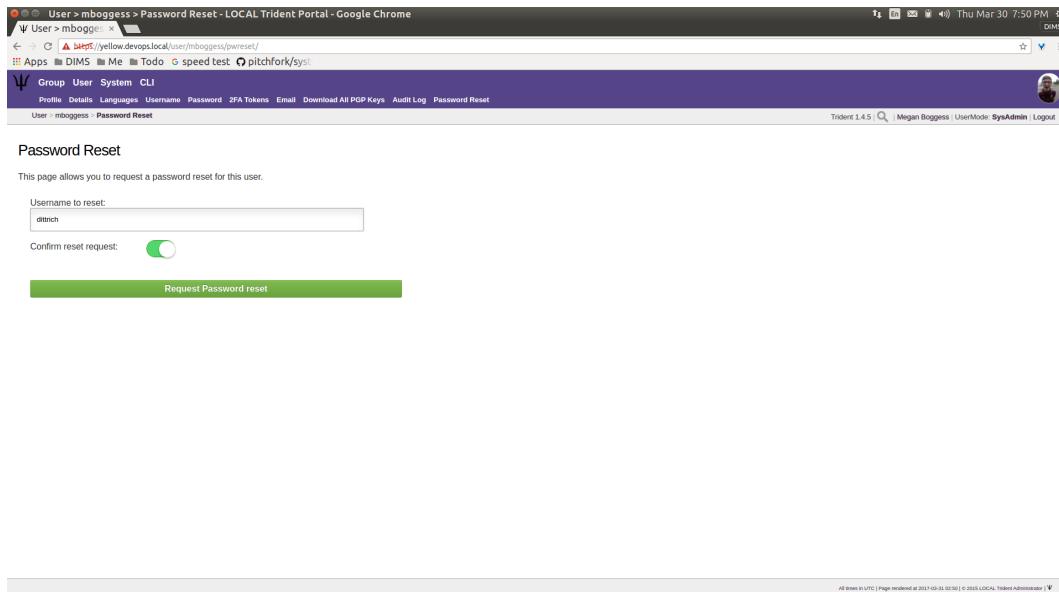


Fig. 1.76: Admin password reset for user

An admin can only begin the process for resetting a user's password, she cannot do it directly. Each user was initially nominated to the trust group before being allowed membership in the trust group. The nominator of a user is part of the process to reset a user's password. As such, because none of the users in our example group were nominated (nor have any of the users uploaded PGP keys), this activities fails (Figure *Admin password reset fail*). Once all members have uploaded keys and there are members who have been nominated, this activity can continue.

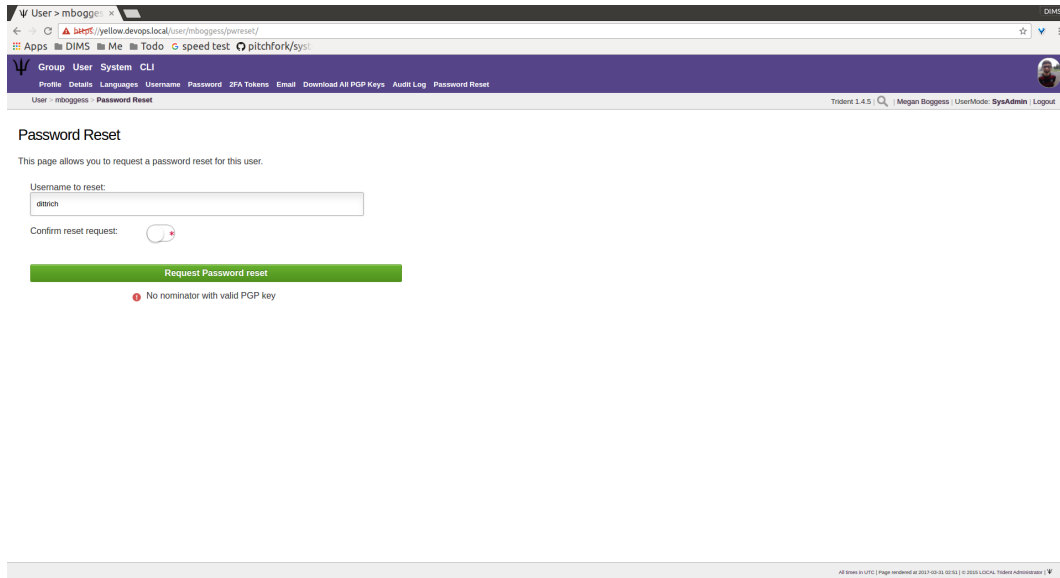


Fig. 1.77: Admin password reset fail

1.3.2 Group Admin Activities

This section describes the group-related activities manageable only by trust group administrators. These activities include adding new mailing lists to a trust group, adding a new trust group, updating the group's settings and adding modules to the group, and a couple member-related actions.

When logged in as a trust group administrator, the `Group` home page looks like what is shown in Figure *Group home, sysadmin*).

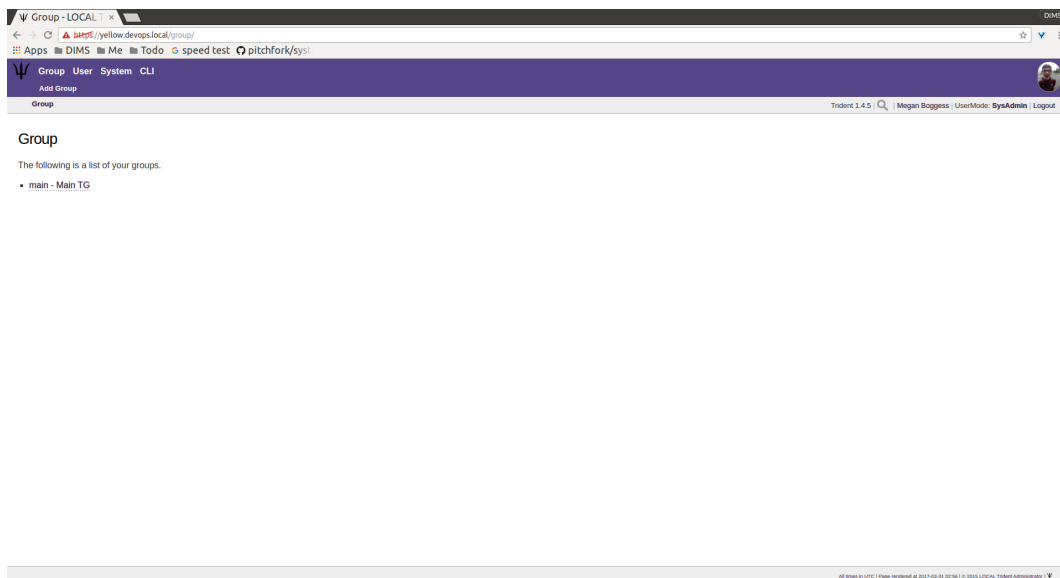


Fig. 1.78: Group home, sysadmin

To add a new trust group, click the `Add Group` link in the second row at the top of the page (Figure *Add group*). This opens a new page with a field for the new trust group's name. Fill in the field, then click the `Create` button.

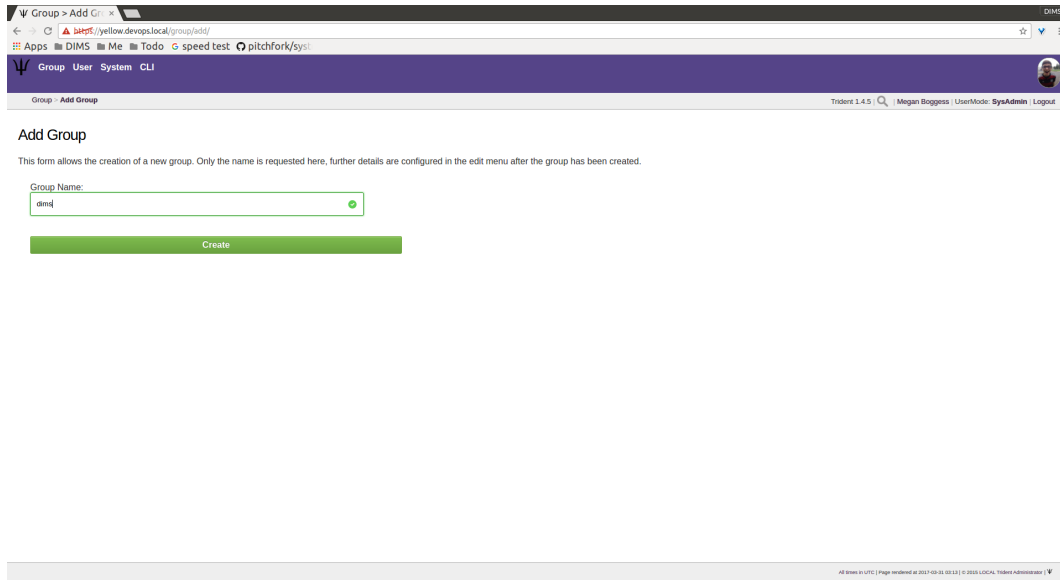


Fig. 1.79: Add group

This opens a new page with settings for the new group (Figure *New group settings, top*). Configure these settings as needed and, if any modifications are made, click the `Update Group` button at the bottom of the page (Figure *New group settings, bottom*).

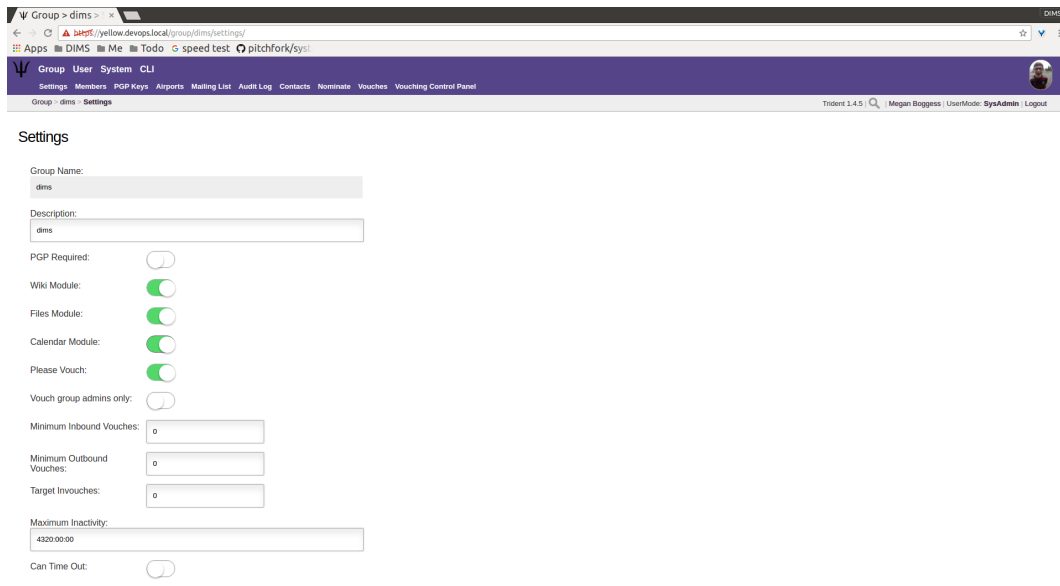


Fig. 1.80: New group settings, top

Returning to the `Group` home page, the new group will be added in the list of links to current trust groups of which the current user is a member (Figure *Group home page, updated*).

Once a trust group exists, changes can be made to it or to its members. A specific group's home page might look like the page shown in Figure *"Main" group's home page*.

This page contains almost exactly the same set of links on the page itself or tabs in the second row at the top of the

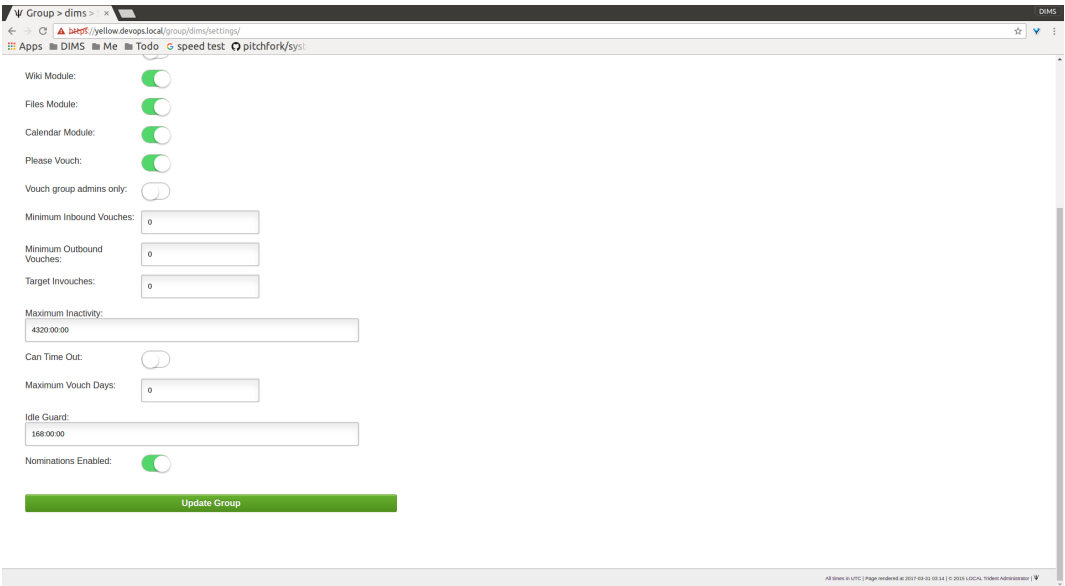


Fig. 1.81: New group settings, bottom

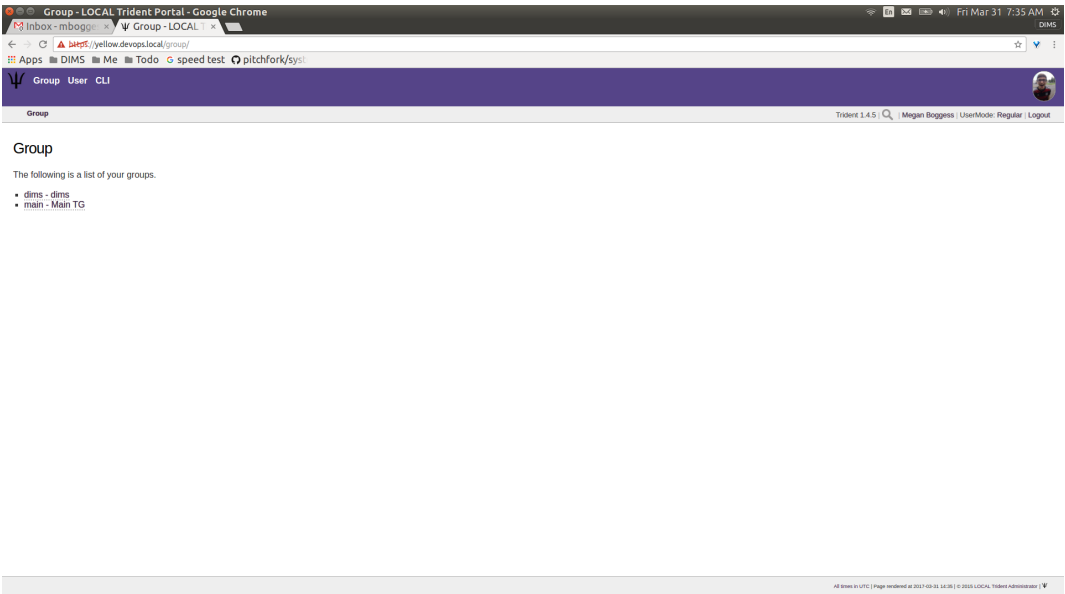


Fig. 1.82: Group home page, updated

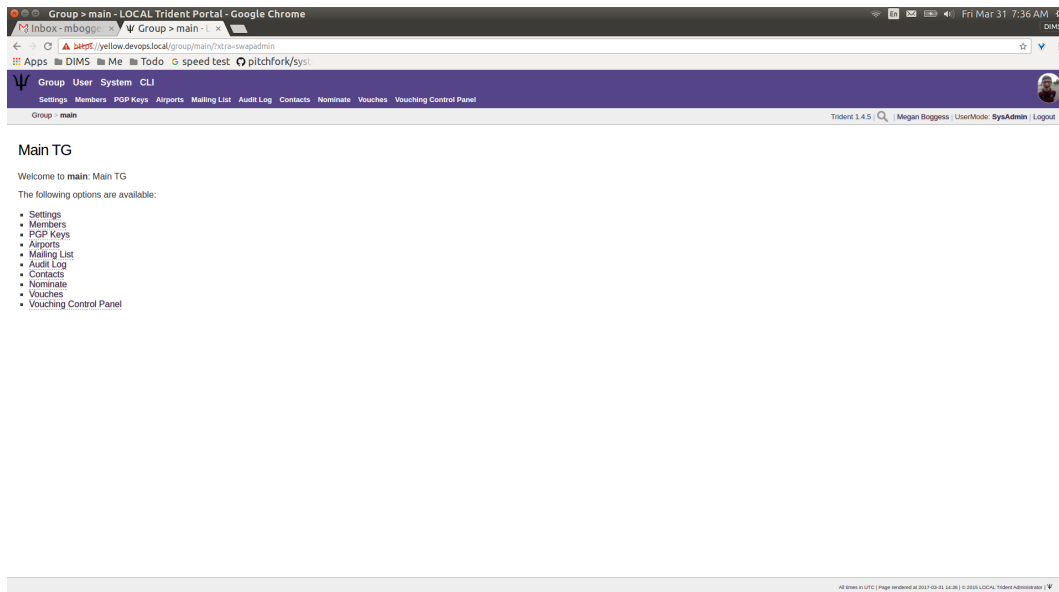


Fig. 1.83: “Main” group’s home page

page. The `Settings` link and tab can now be seen. Group settings include vouching policies, timeout policies, idle policies, PGP requirement policy, and including additional modules (not yet added in Figure [Group settings, top](#)).

There are three additional modules that are option to the use of a Trident portal system and may be added at any time: the Wiki module, the Files module, and the Calendar module.

Note: At this time, the Calendar module seems to still be under development. Toggling “on” the Calendar module in group settings does not add a Calendar link or tab. We are reporting this to the Trident developers.

To view potential modules to add, go to the current trust group’s `Settings` page. If a module has not been added, its toggle will not be in the “on” position (highlighted and the toggle moved to the right), as can be seen in the page shown in Figure [Group modules off](#).

To add modules, toggle each desired module to the “on” position as shown in Figure [Group modules on](#).

Make sure to click the `Update Group` button at the bottom of the `Settings` page. From the `Settings` page, links for the newly-added modules will appear in the second row of links at the top of the page, as can be seen in the page shown in Figure [Group modules added](#). Returning to the group’s home page would show links for the modules in the list of links.

The `Member` page changes slightly when a user has trust group administration privileges (Figure [Group member admin actions](#)). A new column is added, `Actions`, to the list of trust group members and information. These actions allow the administrator to block or unblock a member and demote or promote a group administrator. These are accomplished through the buttons found in the `Actions` column.

Thes actions (blocking/unblocking and demoting/promoting) are also available on each trust group member’s profile. Click the member’s link from the list on the `Members` page to go to the member’s profile (Figure [Group member profile, top](#)).

Scroll down towards the bottom of the profile until just before the vouching section of the profile. There is a section titled `Admin functions` for a given user. This section contains the same buttons to block or unblock and demote or promote as can be found in the `Actions` column on the member page (Figure [Group member profile, bottom](#)).

Finally, trust group administrators can add and delete mailing lists. To see a list of current mailing lists, from a trust

Group > main > Settings

Group: main Settings

Trident 1.4.5 | Megan Baggess | UserMode: SysAdmin | Logout

Settings

Group Name:

Description:

PGP Required: ☐

Wiki Module: ☐

Files Module: ☐

Calendar Module: ☐

Please Vouch: ☒

Vouch group admins only: ☐

Minimum Inbound Vouches:

Minimum Outbound Vouches:

Target Invouches:

Maximum Inactivity:

Can Time Out: ☐

Fig. 1.84: Group settings, top

Wiki Module: ☐

Files Module: ☐

Calendar Module: ☐

Please Vouch: ☒

Vouch group admins only: ☐

Minimum Inbound Vouches:

Minimum Outbound Vouches:

Target Invouches:

Maximum Inactivity:

Can Time Out: ☐

Maximum Vouch Days:

Idle Guard:

Nominations Enabled: ☒

All done in UTC | Page rendered at 2017-03-28 01:42 | © 2015 LOCAL Trident Administration |

Fig. 1.85: Group settings, bottom

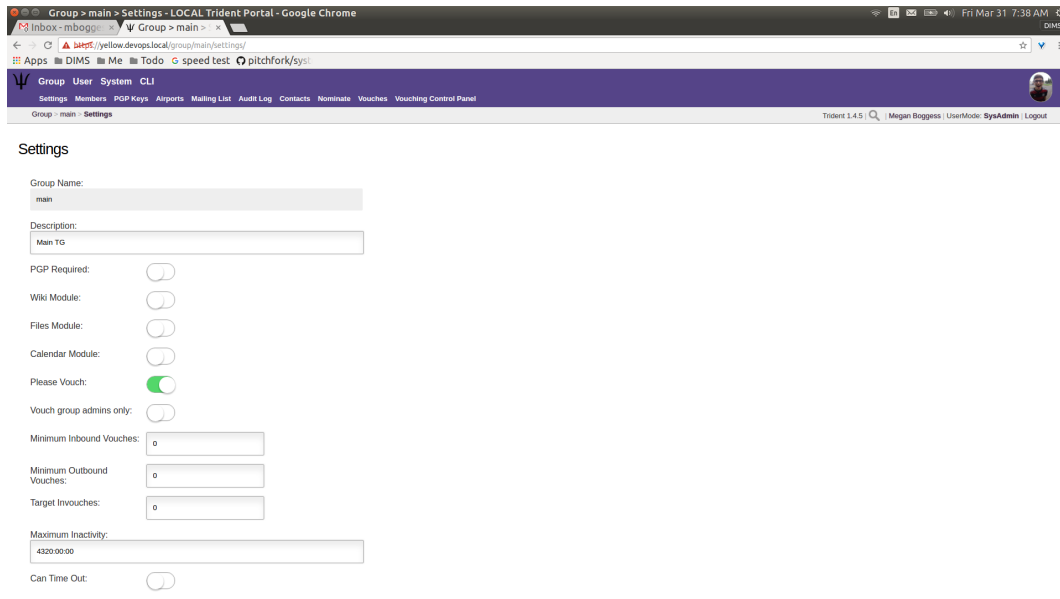


Fig. 1.86: Group modules off

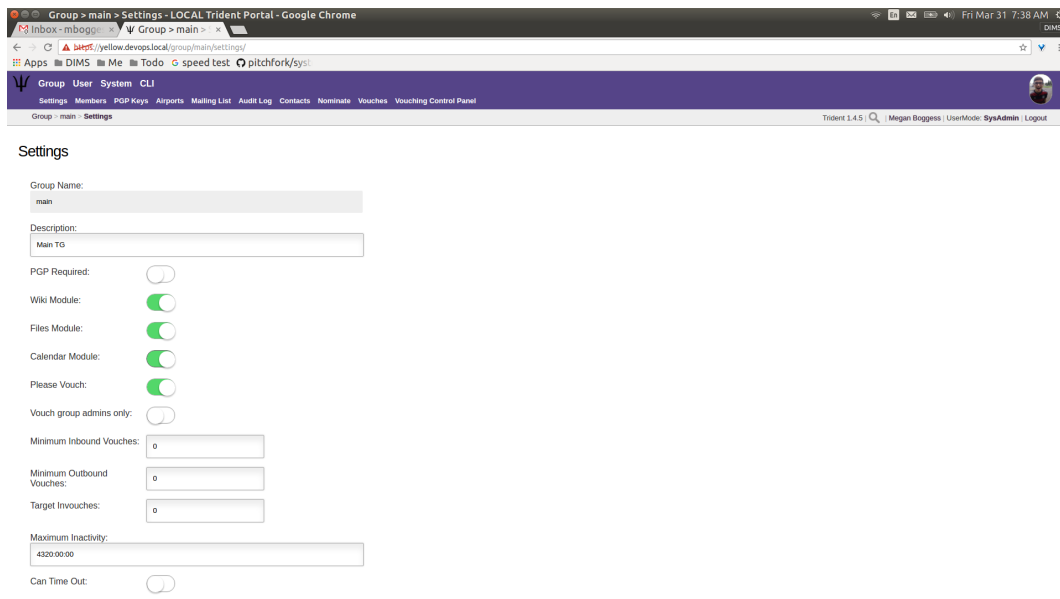


Fig. 1.87: Group modules on

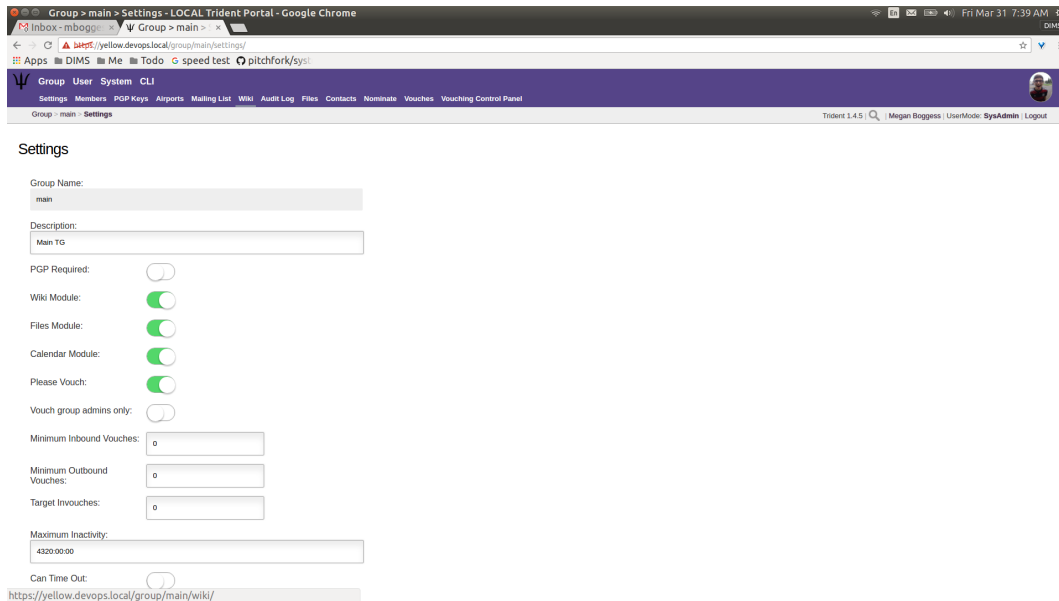


Fig. 1.88: Group modules added

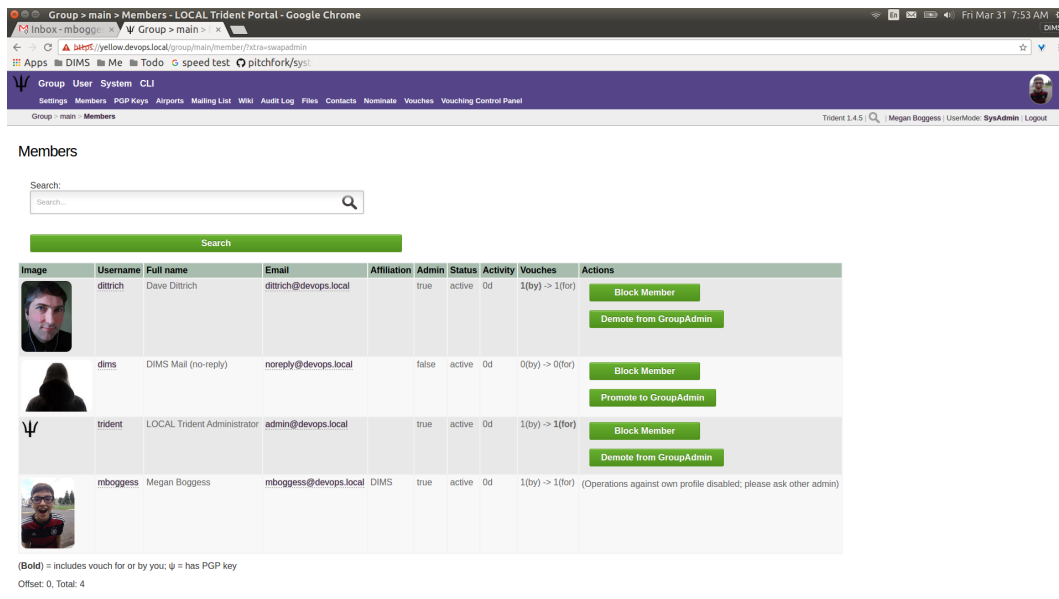


Fig. 1.89: Group member admin actions

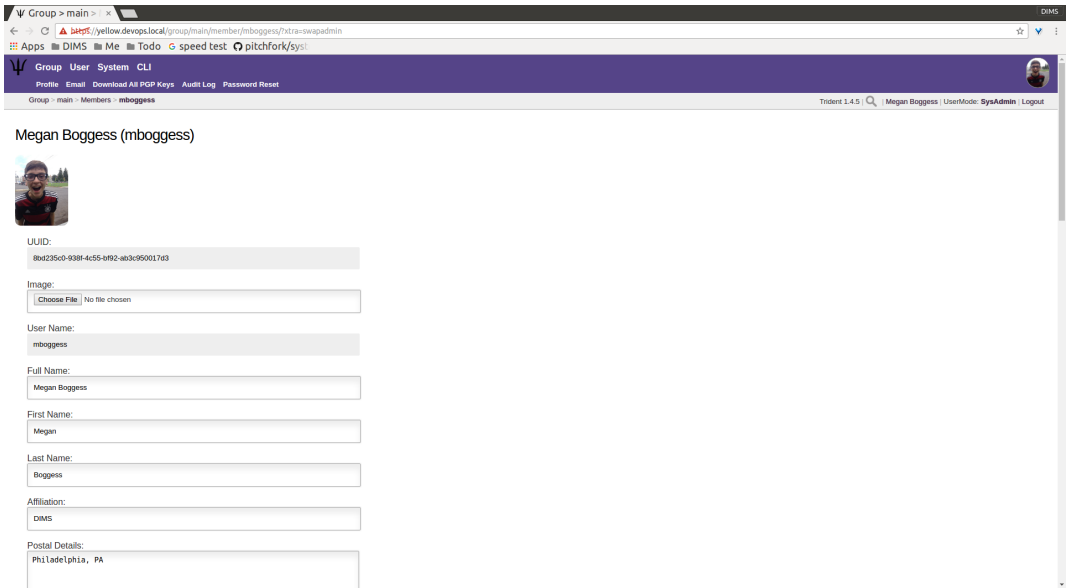


Fig. 1.90: Group member profile, top

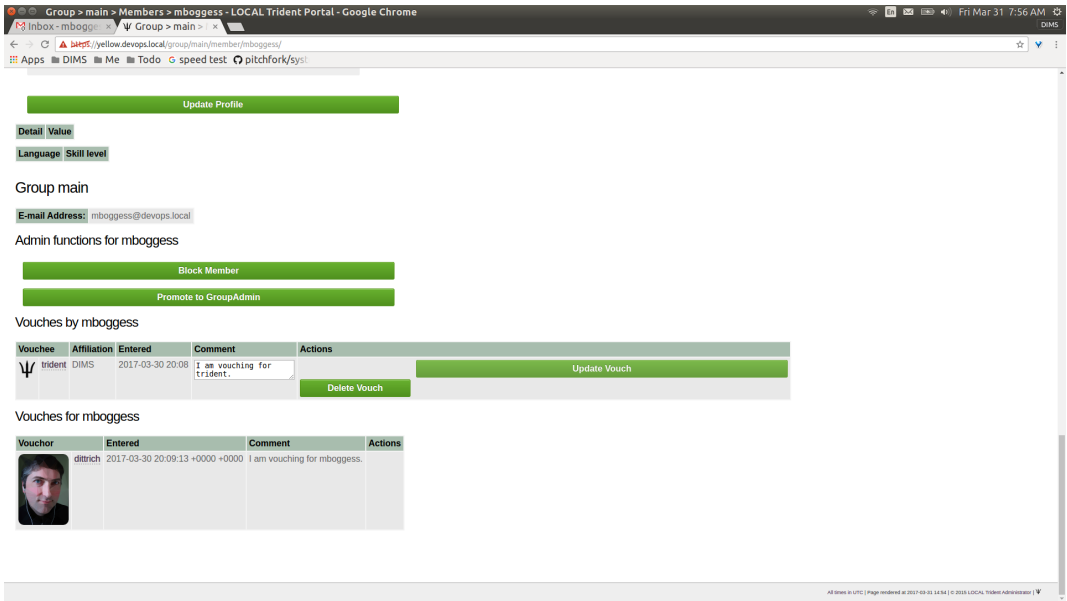


Fig. 1.91: Group member profile, bottom

group's main page, navigate to the `Mailing List` page using either the link on the page or the tab in the second row at the top of the page. The list can be seen on the page shown by Figure *Mailing lists list*.

Shortname	Description	Address	Members	PGP	Subscription	Action
admin	Group Administration	main-admin@local	2	PGP Key	Subscribed	Unsubscribe
demo	LOCAL Trident Demonstration	main-demo@local	3	PGP Key	Subscribed	Unsubscribe
general	General Discussion	main-general@local	4	PGP Key	Subscribed	Unsubscribe
vetting	Vetting and Vouching	main-vetting@local	4	PGP Key	Subscribed	Unsubscribe

Fig. 1.92: Mailing lists list

Now, the second row of tabs at the top of the page has changed to just one, `New Mailing List`. Click this tab to go to a new page to add a new mailing list. Fill in a name for the mailing list in the required field as shown in Figure *Add new mailing list*. Then click the `Create` button.

Clicking the `Create` button immediately opens the `Settings` page (Figure *Mailing list settings*) for the new mailing list. Modify the settings as needed, and click the `Update Configuration` button.

Returning to the `Mailing List` home page, the new mailing list has been added to the list, as can be seen in the page shown by Figure *Updated list of mailing lists*.

A `Settings` page is available for all mailing lists. In the list on the `Mailing List` page (see Figure *Updated list of mailing lists*), there are links in the `Shortname` column. Clicking this link opens a new page with a list of current mailing list members and tabs in the second row at the top of the page (Figure *Mailing list members*) for the `Settings` page (Figure *Mailing list settings*), to `Subscribe` or `Unsubscribe` the current user to or from the mailing list, and to download `PGP` keys for the current mailing list.

Click the `Subscribe` or `Unsubscribe` tabs to subscribe or unsubscribe the current member from the current mailing list. Click the `PGP Key` tab to download the `PGP` key for the current mailing list.

These actions can also be completed from the `Mailing List` home page (Figure *Mailing list activities*).

For the desired mailing list, click the link `PGP Key` in the `PGP` column to download the `PGP` key for that mailing list. To unsubscribe or subscribe to a mailing list, click the available button in the `Action` column.

1.3.3 CLI Activities

The sections covers activities that can only be accomplished via the `CLI` page. This page utilizes a command line interface through which the databases holding information of the Trident system may be manipulated. These activities include adding a new user to the Trident system, removing a member from a trust group, and removing a mailing list from a trust group.

The screenshot shows a web browser window with the URL `http://yellow.devops.local/group/main/new/`. The page title is "Group > main > Mailing List > New - LOCAL Trident Portal - Google Chrome". The breadcrumb trail is "Group > main > Mailing List > New". The page content includes a form with the following fields:

- Group Name:** A text input field containing the value "main".
- List Name:** A text input field containing the value "devops". A green checkmark is visible to the right of the field.
- Create:** A green button at the bottom of the form.

Below the form, there is a footer area with the text "All done in UTC | Page rendered at 2017-03-31 14:41 | © 2018 LOCAL Trident Administration |".

Fig. 1.93: Add new mailing list

The screenshot shows a web browser window with the URL `http://yellow.devops.local/group/main/new/devops/settings/`. The page title is "Group > main > Mailing List > devops > Settings - LOCAL Trident Portal - Google Chrome". The breadcrumb trail is "Group > main > Mailing List > devops > Settings". The page content includes a form with the following fields:

- List Name:** A text input field containing the value "devops".
- Group Name:** A text input field containing the value "main".
- Description:** A text input field containing the value "devops".
- Members Only:** A toggle switch that is currently turned on.
- Can Add Self:** A toggle switch that is currently turned on.
- Automatic:** A toggle switch that is currently turned off.
- Always Encrypt:** A toggle switch that is currently turned off.
- Public PGP Key:** A text area containing a long string of characters, which is a PGP public key block.
- Update Configuration:** A green button at the bottom of the form.

Below the form, there is a footer area with the text "All done in UTC | Page rendered at 2017-03-31 14:41 | © 2018 LOCAL Trident Administration |".

Fig. 1.94: Mailing list settings

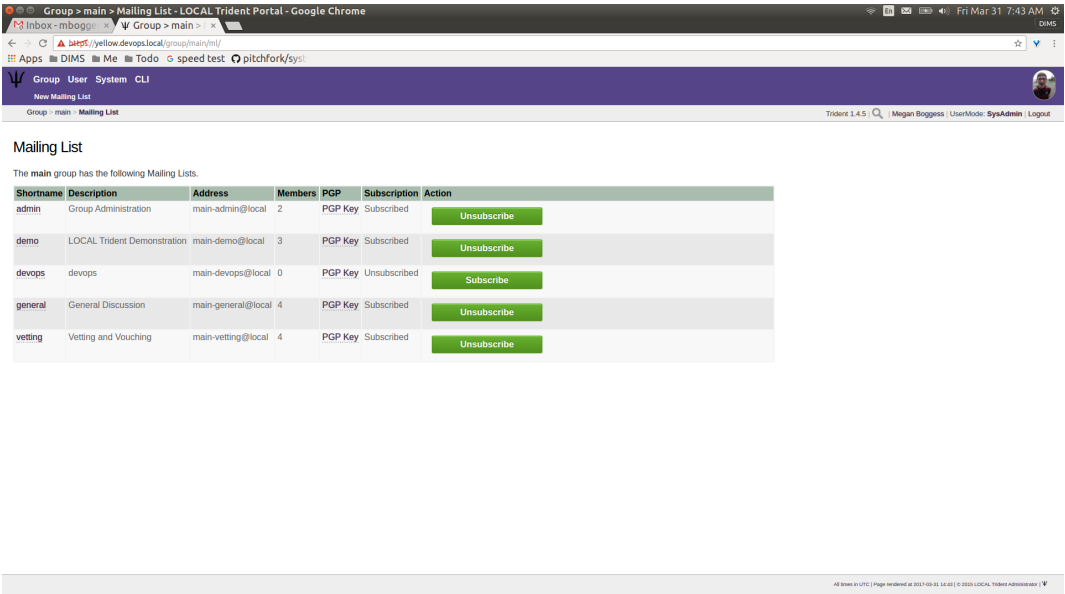


Fig. 1.95: Updated list of mailing lists

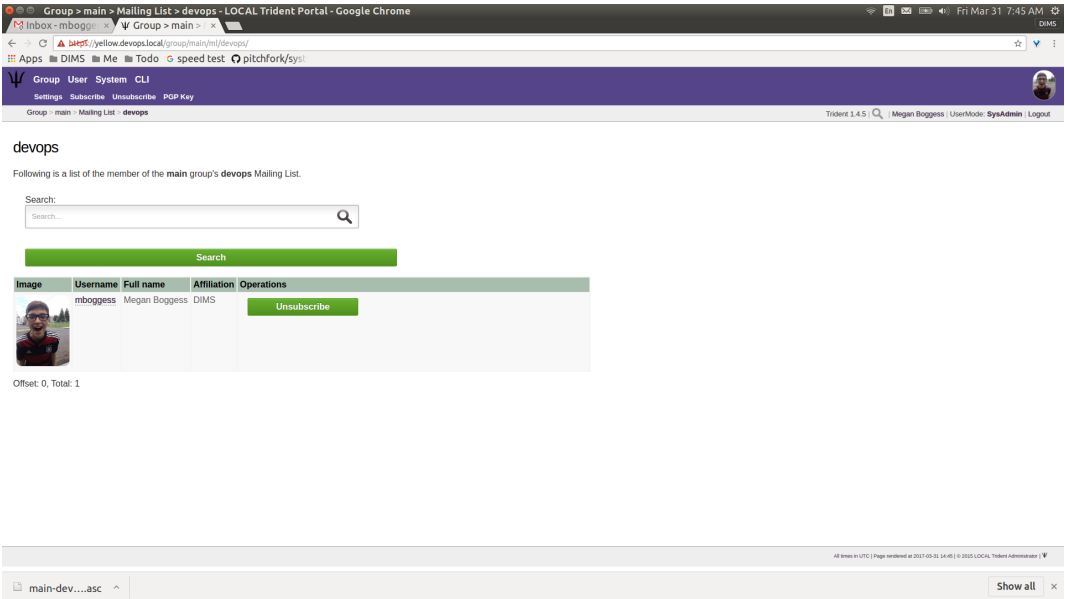


Fig. 1.96: Mailing list members

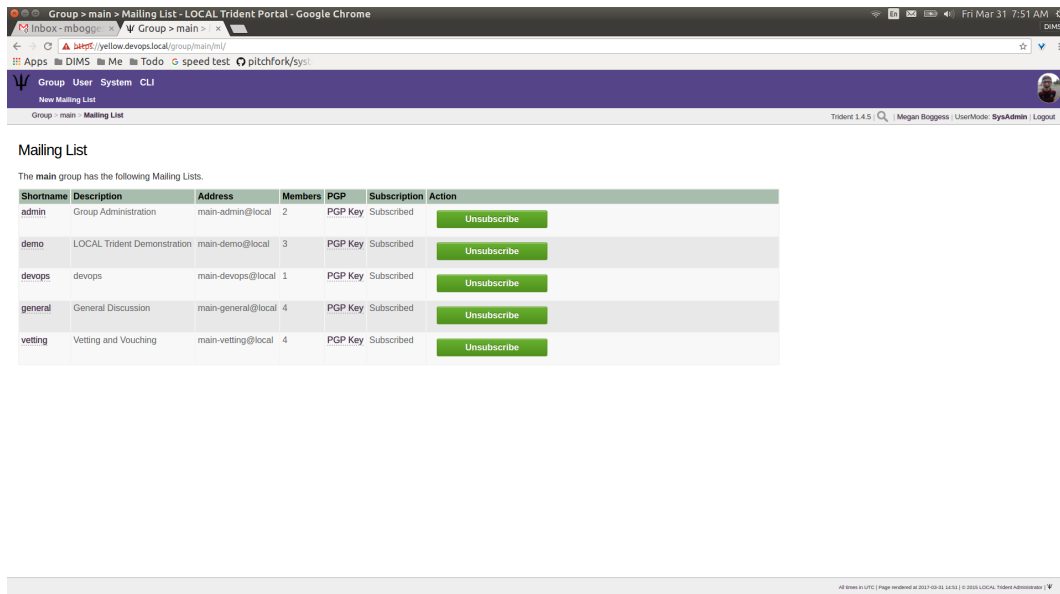


Fig. 1.97: Mailing list activities

Click the link on the user’s home page or the tab in the second row at the top of the page to go to the CLI page. A new page will open with a field to enter the command, simulating a command, and the larger, top box returns the results of the command executed (see Figure cliHomePage which shows the results of running “help” via the command line interface).

Figure *CLI home page* shows help for using the Trident CLI when a user is not logged in as a sysadmin. Each top level command indicates the domains of attributes which can be manipulated via the CLI: `user`, to manipulate user information; `group`, to manipulate trust group information, `ml` to manipulate mailing list information, and `system`, to manipulate system information.

Figure *CLI group help* shows the results from running the command `group help`.

A user must become a sysadmin via the CLI to gain access to sysadmin CLI commands; being logged in as a sysadmin in the webapp does not allow sysadmin access via the CLI. To obtain sysadmin rights, use the command `system swapadmin`, as shown in Figure *CLI sysadmin*.

Once logged in as a sysadmin, more commands are available. See Figure *CLI group help* and compare with Figure *CLI group help* for the additional commands available in the `group` domain.

Trust group admins should use the web app interface for as many tasks as possible. However, there are some tasks which are not able to be accomplished with the web app, and these must be handled using the CLI page. One of those tasks is adding a new user to the system.

All users must be added to the Trident system before they can become members of any trust groups. Help for the `user` domain can be seen in Figure *CLI user help*.

To add a user, use the command `user add new <username> <email>` where `<username>` is a username for the user and `<email>` is a valid email address the user owns. See Figure *CLI user add*.

The user can always change their username using the Username page in the User perspective of the portal. See Figure *User username change* in Section *User Management*. The email must be the correct, valid email address to which the user wishes to receive communications regarding initial Trident use. Email addresses can be changed, added, or deleted once the user has Trident access. See the Section *Email Management*.

Additionally, a trust group admin must set the user’s initial password. The user can change their password via the Password page in the User perspective (see Section *userPwdChange*). The initial password must be set by the

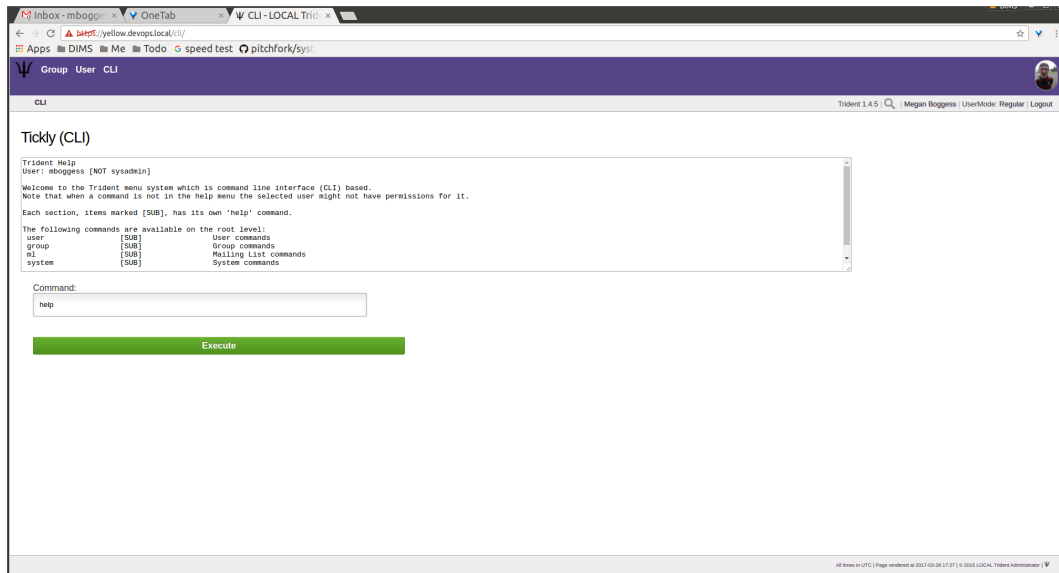


Fig. 1.98: CLI home page

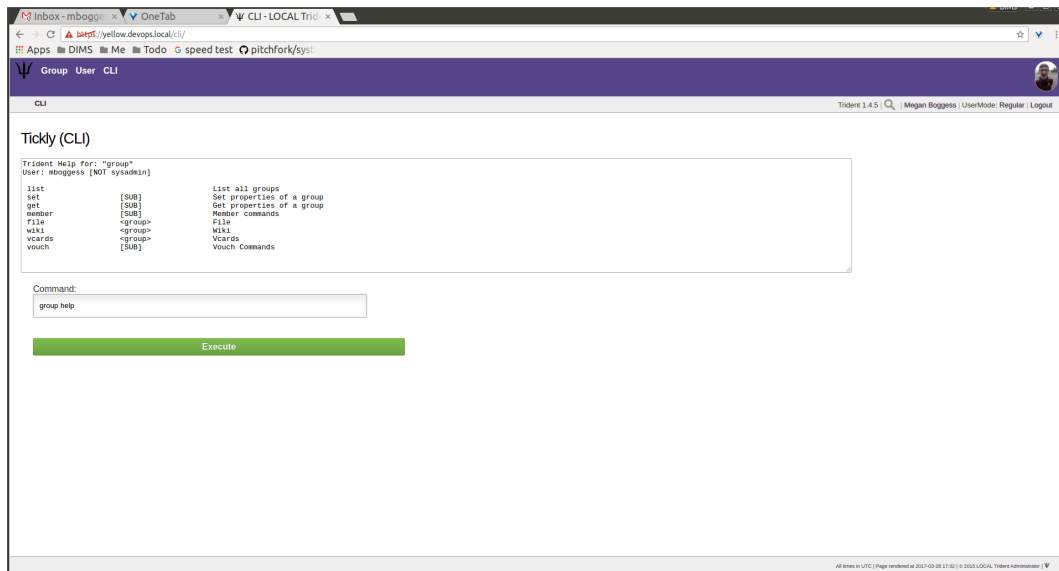


Fig. 1.99: CLI group help

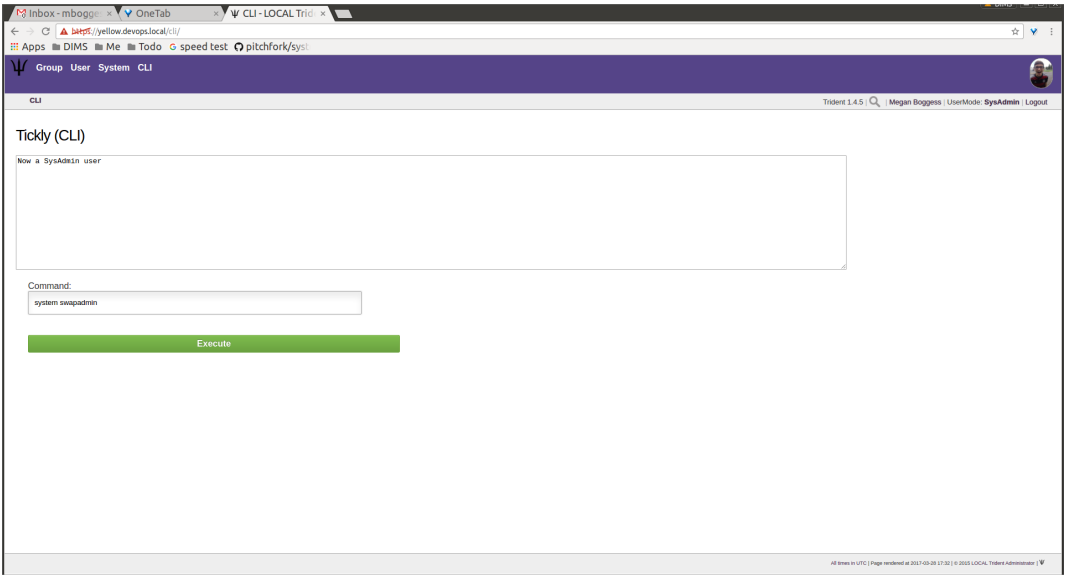


Fig. 1.100: CLI sysadmin

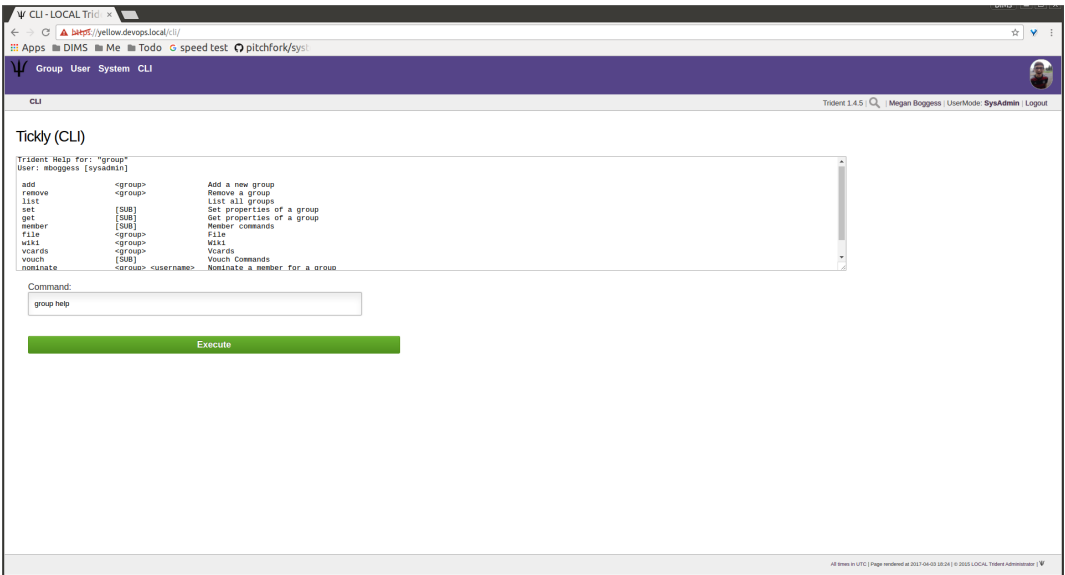


Fig. 1.101: CLI group help

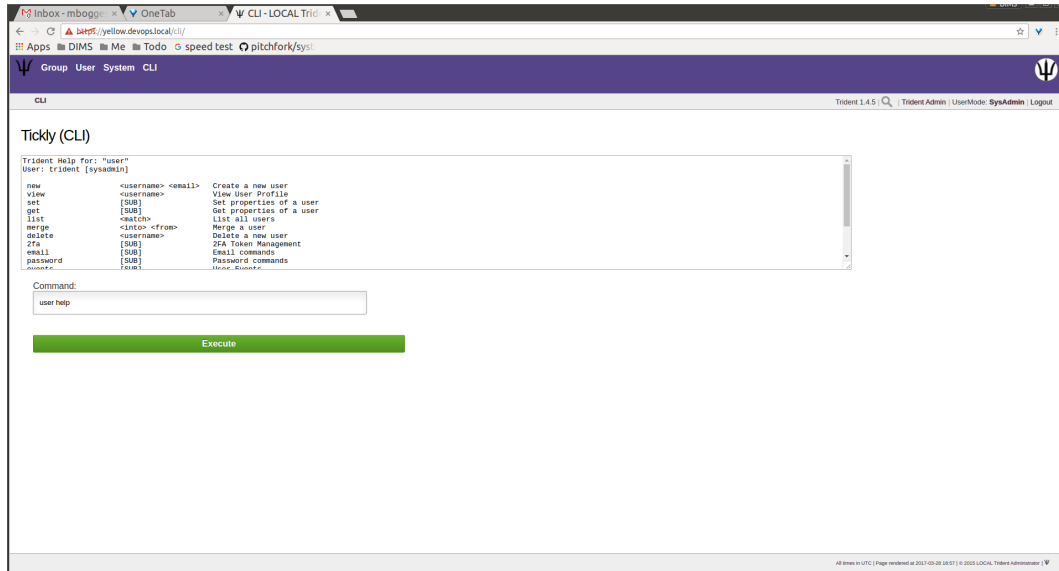


Fig. 1.102: CLI user help

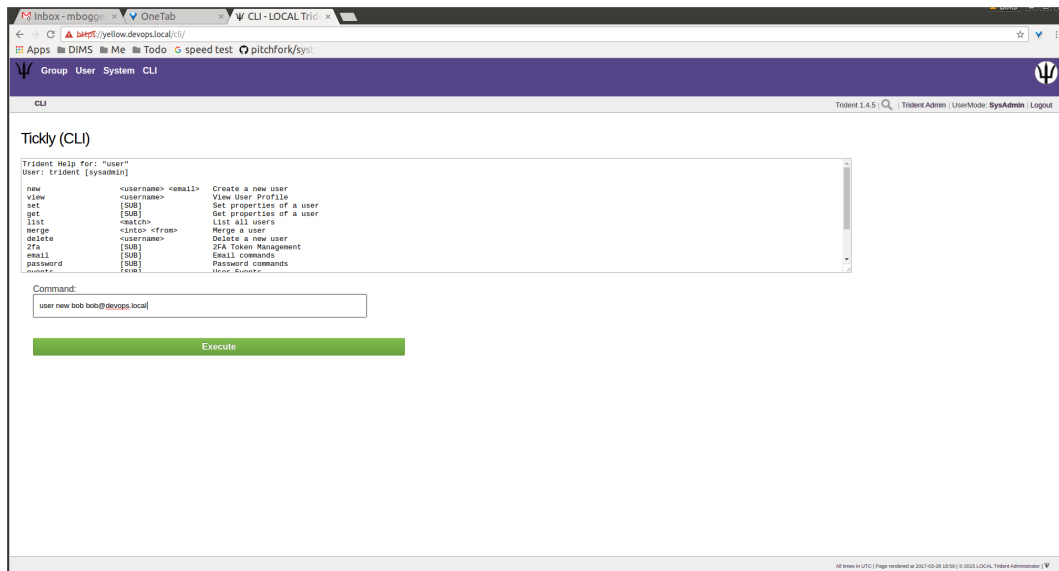


Fig. 1.103: CLI user add

administrator and then passed along to the user either through out-of-band means or via an encrypted message.

To set a user's password via the CLI, use the command `user password set portal <username> <password>` in the field simulating the command line on the CLI page (Figure [CLI set password](#)).

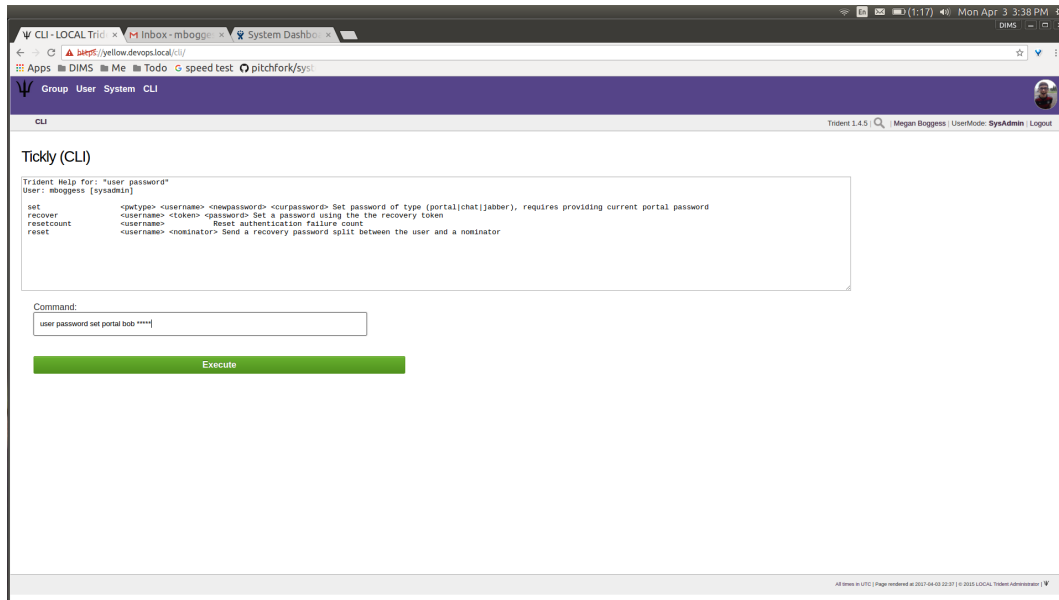


Fig. 1.104: CLI set password

The user will now show up in a trust group administrator's list of users found on the [User](#) home page (see Figure [New user list](#)). The user does not yet exist in the trust group. For the user to become a member of the trust group, follow the trust group's policies for becoming a member (nomination, vouches, etc.).

There are instances where a user must be removed from a trust group. Members can be blocked via the web application's [Group](#) perspective (see Figure [Group member admin actions](#) in Section [Group Admin Activities](#)). This does not remove a member completely from the trust group, nor does it remove a member as a user from the Trident system itself. These actions must be taken via the CLI.

To remove a member from a trust group, use the command `group member remove <group> <username>` in the field simulating the command line, where `<group>` is the trust group from which the user should be removed and `<username>` is the username for the user (Figure [CLI remove member](#)).

To remove a user from the Trident system, use the command `user delete <username>` (Figure [CLI remove user](#)).

Finally, trust group administrators are responsible for the group's mailing lists. Sometimes, lists must be deleted. There is no way to remove a list via the web application [Mailing List](#) home page (see Figure [Mailing lists list](#) in Section [Group Admin Activities](#)). Thus, the removal must be accomplished via the CLI.

To see what subcommands are available in the `ml` domain, use the command `ml help` (Figure [cliAdminMailingListHelp](#)).

To see a current list of available mailing lists, use the command `ml list <group>` where `<group>` is the name of the trust group from which to list available mailing lists (Figure [CLI ml group list](#)).

To remove a mailing list, use the command `ml remove <group> <ml>` where `<group>` is the trust group from which the mailing list is to be removed and `<ml>` is the name of the mailing list to be removed (Figure [CLI ml remove list](#)).

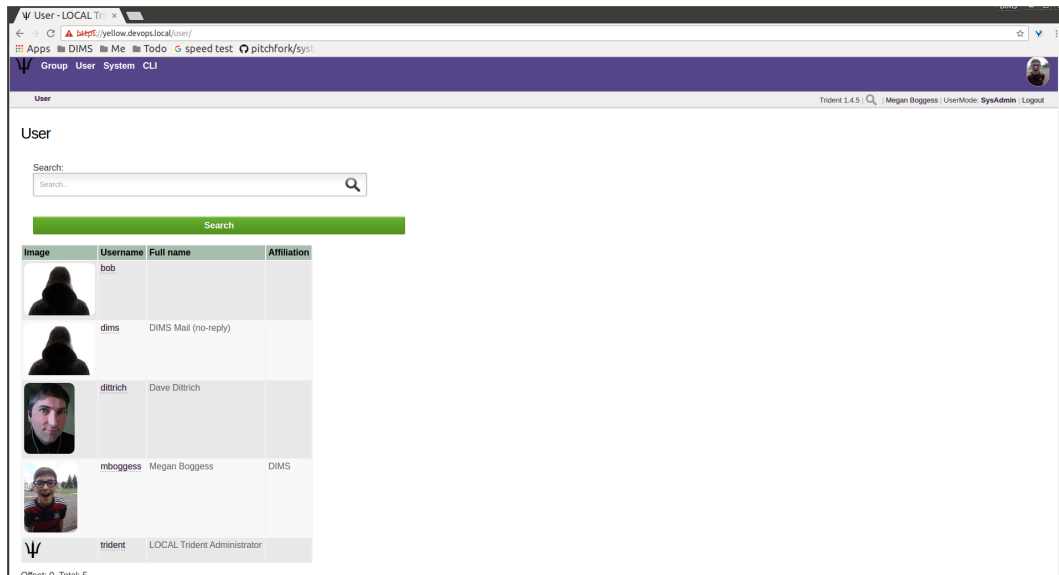


Fig. 1.105: New user list

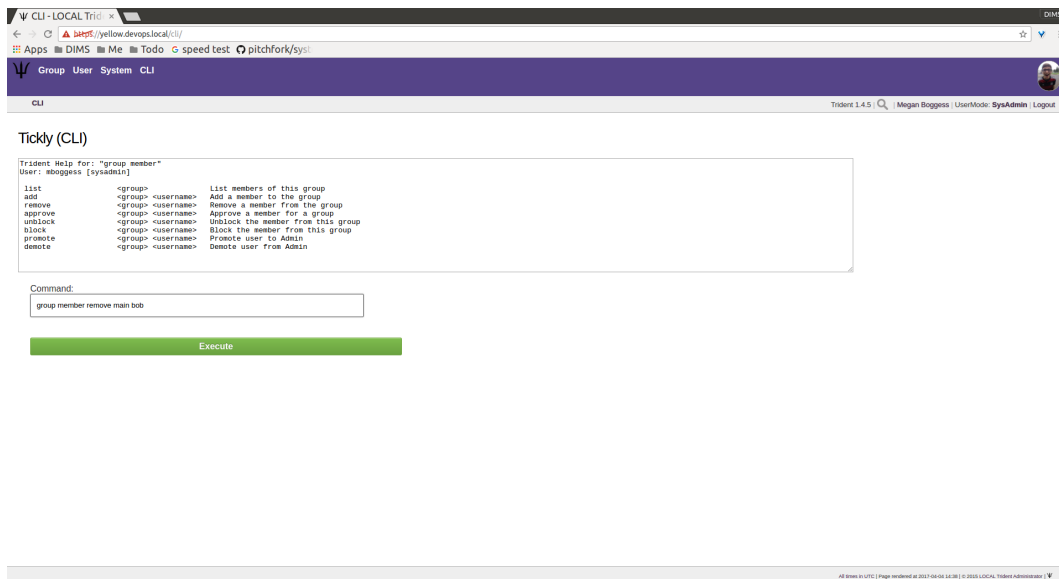


Fig. 1.106: CLI remove member

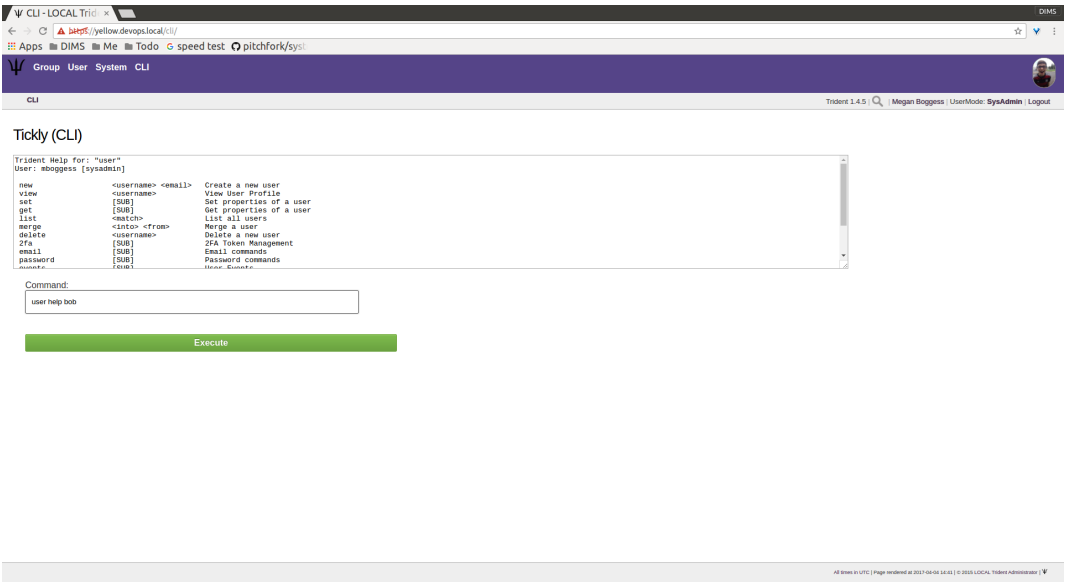


Fig. 1.107: CLI remove user

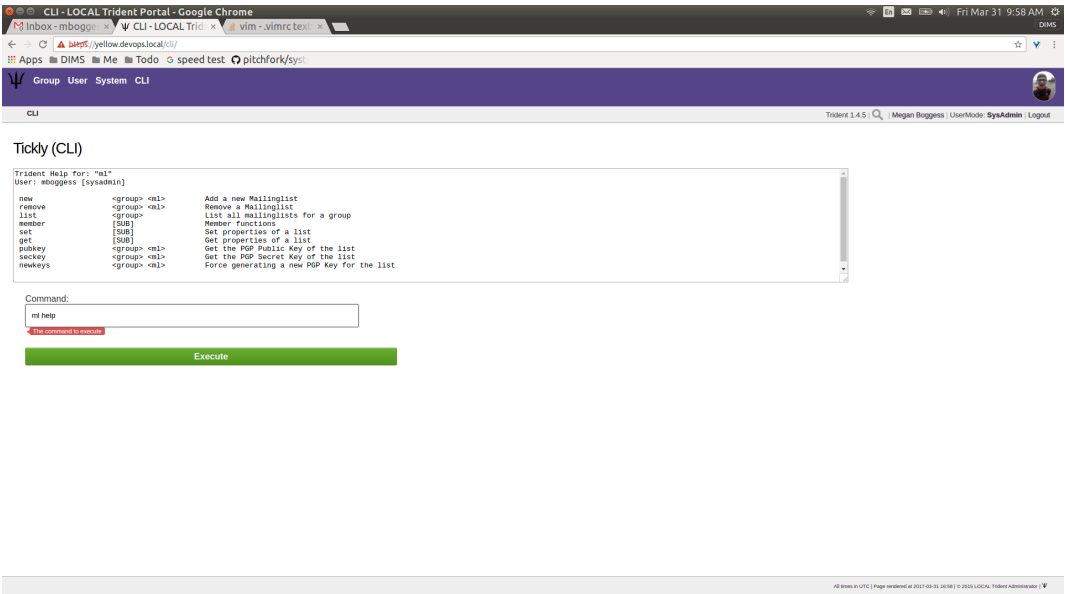


Fig. 1.108: CLI ml help

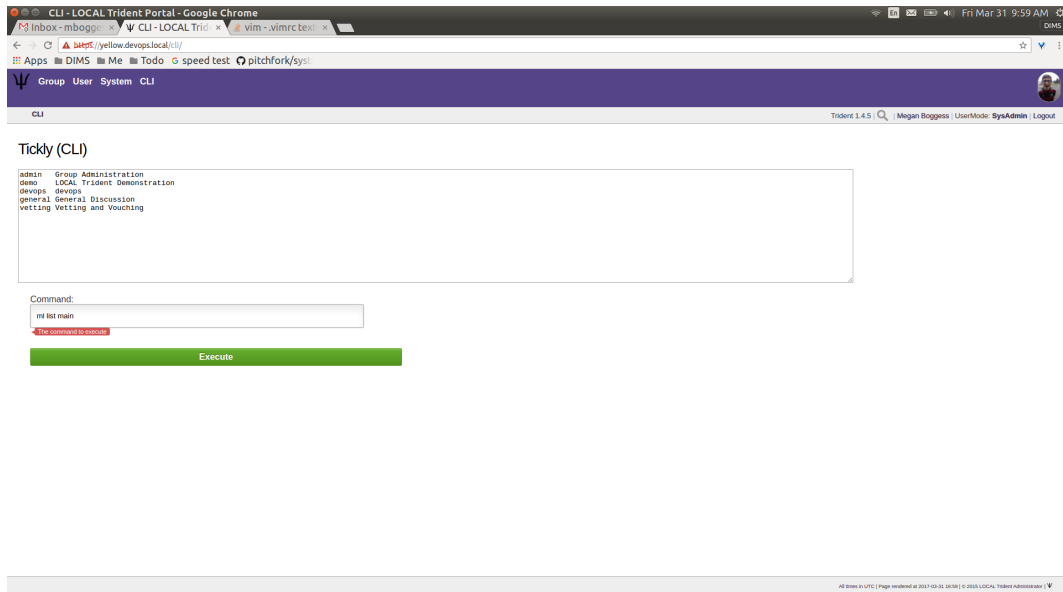


Fig. 1.109: CLI ml group list

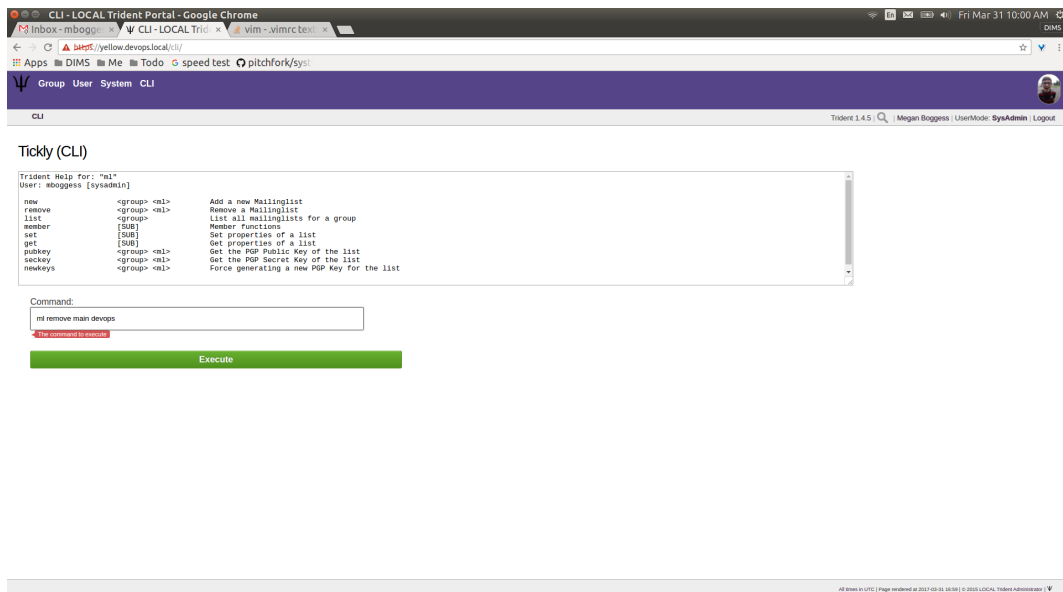


Fig. 1.110: CLI ml remove list

The list of mailing lists on the web app’s Mailing List home page will then be updated (Figure *Mailing list list updated*).

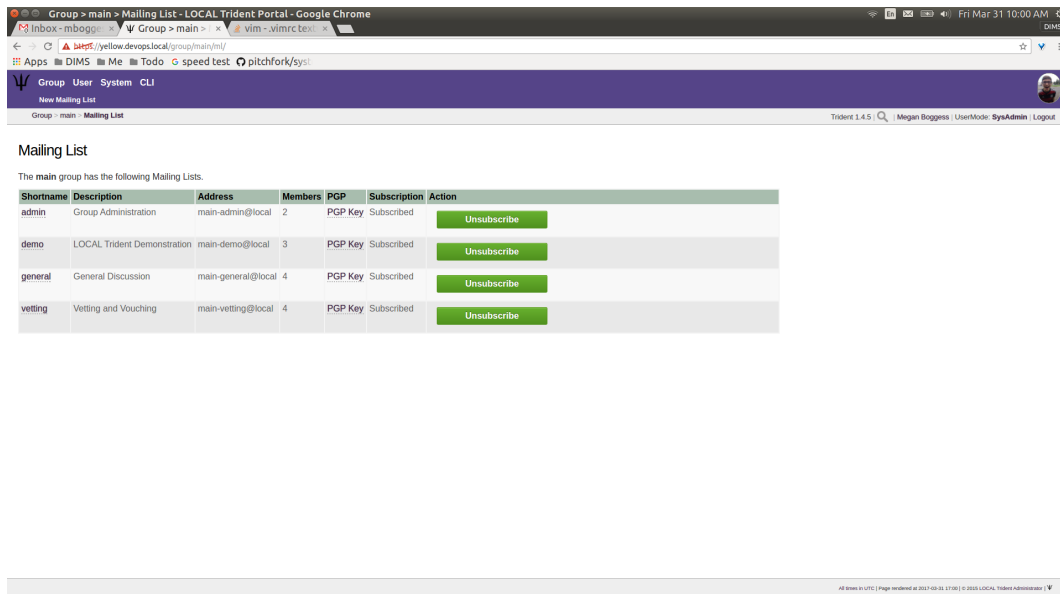


Fig. 1.111: Mailing list list updated

PGP keys are also manageable via the CLI’s `ml` domain. If PGP keys for a mailing list are compromised for some reason, they need to be regenerated. Trust group administrators can retrieve both public and secret PGP keys, as well as regenerate new ones. See Figure *CLI ml help* to see the `ml` subcommands and the necessary parameters. Trust group admins should then notify all members of the change of keys so the members can go retrieve the new keys (see Section *PGP Keys*).

To log out of the CLI as a trust group admin, run the command `system swapadmin` again (Figure *CLI log out*).

This concludes the activities manageable by a trust group administrator. To see tasks for regular members of trust groups or for system administrators, please see the other chapters in this document (Section *Trust Group Member Activities* and Section *System Administration Activities*, respectively).

1.4 System Administration Activities

This chapter introduces the fundamentals of administering the underlying Debian Linux operating system and packages using Ansible and playbooks produced and published by the DIMS project team. For the purposes of training, this chapter will use the published `local` deployment variables and playbook templates that will install Trident and related tools in Virtualbox Vagrant virtual machines on a base Ubuntu 14.04 development system. (This is the platform used by DIMS developers to do development and development testing on laptops or development servers.)

The basic steps covered in the sections below are:

- Cloning the necessary repositories.
- Creating SSH key pairs.
- Running Ansible playbooks to establish a control host.
- Creating required Virtualbox box files using Packer.
- Building Vagrants from Virtualbox box files.

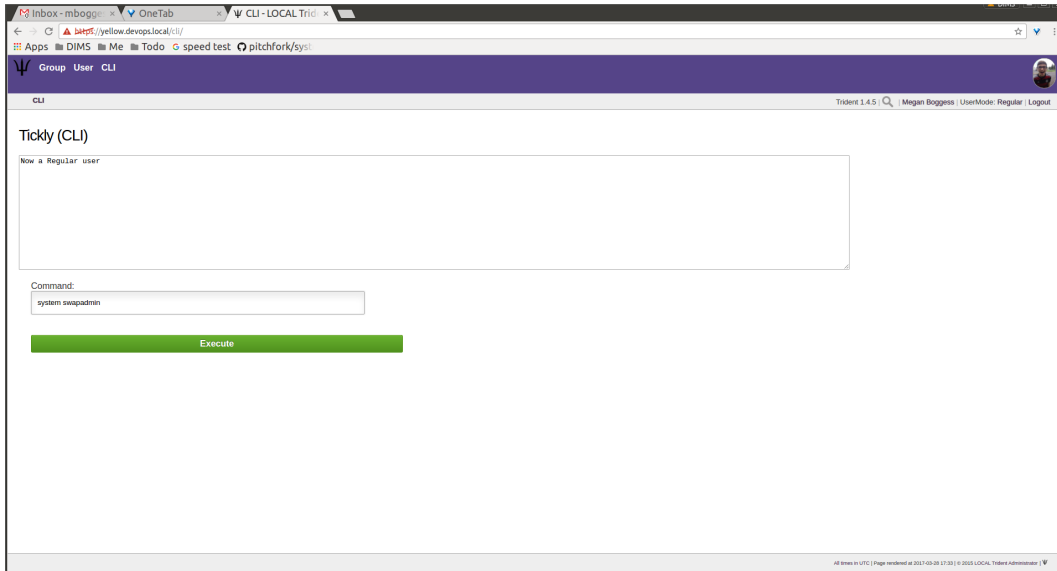


Fig. 1.112: CLI log out

- Running Ansible playbooks to change configuration or update packages.

At the end of these steps, you will have a running Trident instance in local virtual machines with which you can practice customizing Trident or upgrade/update component packages in an isolated deployment that will not impact your production deployment. Once you are comfortable with these tasks, you will be able to administer a production system with greater confidence and reliability.

1.5 License

```

Berkeley Three Clause License
=====

Copyright (c) 2014, 2015 University of Washington. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors
may be used to endorse or promote products derived from this software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE

```

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Section author: Dave Dittrich <dittrich@u.washington.edu>, Megan Boggess <mboggess@uw.edu>

Copyright © 2017 University of Washington. All rights reserved.