Trident User Manual Documentation

Release 1.0.3

Dave Dittrich

Jan 22, 2018

Contents

This document serves as a guide to using a Trident portal trust group management system[1] as a trust group administrator or a trust group member.

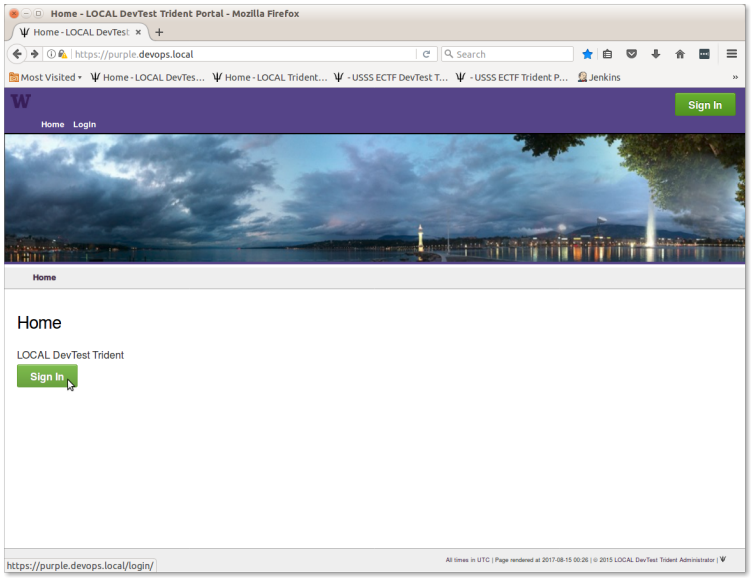

Fig. 1: Trident Login Page

Note: This is not an official document of the Trident project or its sponsors. In some places it cites and/or refers to content on the Trident web site. It was written based on the author's own experience as a trust group member who has used the ops-trust (and now Trident) portal system[1] as well as membership in multiple other closed security groups since the late 1990s. Its purpose is to support a pilot deployment of a Trident portal as part of the Distributed Incident Management System (DIMS) project. DIMS uses a Trident portal at the core of a larger open source distributed system for incident response event management. You can find more information on DIMS, including links to source code and other related documentation, at https://staff.washington.edu/dittrich/home/dims.html.

[1] Thanks to Paul Vixie who designed, implemented, and operated the original Ops Trust software infrastructure for its first few years. In response to an early request from Nick Ianelli, Vixie virtualized the original Ops Trust membership and trust set into a single silo inside of a new multiple-memberships multiple-trust-sets system. Such silos needed a category name, and in that moment, Vixie coined the term "*trust group*". This may have been Vixie's most important contribution, and in the spirit of innovation, it was accidental.

CHAPTER 1

Chapter Index

1.1 Introduction

This document is called the "Trident User Manual" because it is focused on the daily operational aspects of using a Trident portal in the context of trust group activities. It is thus focused on "user" activities, not "system administration" activities. There are some terms that will be used in this document and that form the basis for how it is structured:

- A **trust group** (also known as a "TG" for short), is an operational concept of the Trident portal that includes users who are **trust group administrators** and/or **trust group members**. These are all portal users, so the term "users" is too vague to be useful. Details on TG formation and operation are covered in *Trust Groups and Trident*.
- A **trust group administrator** is someone who has leadership responsibility for handling the membership details and overall organization of information in a Trident portal system. Things that TG admins need to know are found in *Trust Group Administration*.
- A **trust group member** is someone who is a member of a given trust group. (There may be more than one trust group, but you can only be active in one trust group at a time, so the focus will always be on "the active trust group.") Information about using the portal for TG members is covered in *Trust Group Member Activities*.
- Finally, there are also **portal administrators** who have access to the `trident` account, which is the primary account for controlling the entire portal. They are also sometimes called **site administrators**. (They may or may not be the same as the **system administrators**, who have full access to the operating system underlying the Trident portal. The system administrators are the ones who manage the Ansible variables and run the Ansible playbooks described in the DIMS Ansible playbooks v 2.14.0 document.)

1.2 Trust Groups and Trident

The concept of **trust groups** has its history in the efforts of computer security researchers, network operators, and expert system administrators at large sites, working together to help guide law enforcement and federal government entities and organizations like Carnegie Mellon CERT/CC, in combatting computer system and computer network compromises affecting the integrity, availability, and/or confidentiality of information and information systems.

These compromises, while sometimes innocent exploration, are none the less potentially criminal acts. At the extreme, things like massive-scale distributed denial of service (DDoS) attacks cost businesses who are disrupted tens of thousands to potentially millions of dollars in lost revenue and expenses. High profile data losses like those suffered by the likes of TJ Maxx, Sony Pictures, Target, and Saudi Aramco arguably cost in multi-million dollar range.

Those who perpetrate these crimes operate in the shadows, using pseudonyms. They cover their tracks using proxies, stepping stones on compromised hosts at innocent third-party sites, or sophisticated multi-layer distributed attack networks commonly known as *botnets*, often operated at *bullet-proof hosting* sites who are non-responsive to requests from the private sector or law enforcement to stop the abuse.

Those who try to defend against these compromises, working with law enforcement to try to bring the perpetrators into the criminal justice system. This may mean disrupting the flow of millions of dollars in ill-gotten gains from criminal acts. When someone impacts the flow of that much money, sometimes the people who are profiting get unhappy and fight back. For those reasons, *trust groups* are formed to try to keep the efforts to counter the criminals secret from those criminals.

1.2.1 Limitations to Trust

As pointed out by Raaum [Raaum(2011)] in his Master's thesis on barriers to trust, trust does not scale well (either within a single trusted information sharing group, or across multiple trusted information sharing groups). At the Coordinating Attack Response at Internet Scale (CARIS) workshop [Internet Architecture Board(2015)] at least two interviewees used the number 100 as the approximate limit at which trust within a single group begins to noticeably decrease within the group. (The original ops-trust group from which the Trident portal grew, has many times this number of members.)

Besides Raaum, there are other studies, reports, and resources related to information sharing and trust (see [Jøsang et al.(2006a) Jøsang et al.(2006b) Demolombe(2011), Evans and Mahoney(2011)])

To establish a strong trust fabric, the Trident portal supports a rigorous vetting process workflow. This workflow depends on the members of the trust group taking the process seriously and adhering to the spirit of the process in their attestations of the trustworthiness of prospective new members. This process is covered in more depth in Section *Vouching in the Vetting Process*.

1.2.2 Trust and the Need to Know

The **Need to Know** is a primary and strong motivator for the sharing of highly-sensitive information for incident response. At the same time, need to know is a limiting factor on the sharing of information, since the more people who have a piece of information, the greater the chances that it loses its secrecy (in the worst case, becoming widely public).

Even in a tightly coherent trust group, not every member of the group needs to know every piece of information. The person sharing the information must decide whether the person they are sharing it with needs to know it, though some people make the assumption that being a member of the trust group by definition means they need to know it.

There are some mechanisms or tactics that are used to address *need to know*.

- Prior to sharing information, it can be tagged with labels defined by the Traffic Light Protocol (TLP) to indicate how to handle the information to protect it from disclosure. (See FIRST announces Traffic Light Protocol (TLP) version 1.0 and Traffic Light Protocol (TLP) Definitions and Usage.) The responsibility for handling TLP-tagged information properly then falls on the recipient. An effort to define a more rigorous information sharing protocol known as the Information Exchange Policy (IEP) - Version 1.0 is being sponsored through FIRST.
- Rather than sending information in broadcast form to the full trust group membership, limiting the number of recipients by sending to a task-specific trust group list (e.g., a "warroom" list that focuses on operations-related information about emerging threats), or by sharing directly with individuals rather than sending to generic email lists.

- For some sensitive operations, such as active investigations of criminal intrusion activity that is likely to move to criminal process, information must be tightly held. In those cases, creating a new trust group and limiting membership to just those victim sites who are involved is the right choice. For this reason, spinning up new trust groups should be very low cost, and retiring them when the incident is resolved should be just as easy.

1.2.3 Trust Group Formation

Trust groups are commonly formed by a group of individuals with a common goal of protecting their own networks, responding to common threats, and ideally collecting information about compromises to their computer and network assets to provide them to others (up to and including law enforcement, who may eventually bring evidence to grand juries and courts of law in the criminal process.)

Trust group formation typically goes like this:

1. Someone takes the lead and offers to form the group.
2. The leader, or someone who wants to help them, sets up an email list server.
3. The initial members populate the list and start communicating over it.
4. For the next month or two, list members send the leader suggestions for new members, or they send the suggestion to the list. The leader asks existing members if the suggested new members should be trusted, and a handful of members respond to the list (or directly to the leader) with their opinions. The leader then makes a command decision for the new members and manually adds them to the list. This takes a significant amount of the leader's time.
5. Every now and then, someone wants a list of all of the current members, with their contact information. Not wanting to send this out in a clear-text email, the leader figures out how to encrypt an Excel spreadsheet. Then the leader sends the password (in clear text, but in a different message) to get it to the list. (This is slightly better than just sending the list in clear text.)
6. Periodically, during a crisis event in the news, someone asks for indicators or feedback about potentially malicious sites, malware, etc. They ask that the details be sent directly, not to the list (defeating somewhat the purpose of a list for sharing actionable information).
7. On a regular basis, information about upcoming meetings, events, etc., is sent to the list. Sometimes a flurry of emails occurs if the exterior door to the building is locked prior to the meeting. This creates noise on the list for those who could not attend and don't need to know that the door is locked.
8. When a cyber exercise occurs, a flurry of exercise emails are sent to the list (that are marked something like "EXERCISE - NOT REAL!" with headlines about buildings exploding and major DDoS events taking down the power grid. Anyone who is not participating in the exercise has their inbox spammed that day and just deletes everything with the list address (loosing the announcement about the next meeting, which was hidden in the noise.)
9. At some point, members start to gripe about not having a wiki for notes, not having a secure place to upload indicators and securely store the membership list (which is now out of date and the leader needs to spend a couple hours updating it), and for only having one email list that carries all of the communication.

While this is somewhat in jest, all of these things actually do happen. The Trident portal (actually its predecessor, the ops-trust portal) was designed specifically to meet the requirements implicit in the above listed friction points. It handles the vetting and vouching workflow, supports a wiki, secure file upload storage, encrypted mailing lists, idle user detection, multi-factor authentication, and much more.

1.2.4 Trust Group Membership Life-cycle

Note: The Figures in this section come from the Trident Documentation page. There may be inaccuracies due to changes in the code base over time. If you notice any discrepancies, please report them (or issue a pull request) to help get them updated.

Figure *Member states and what they mean* shows a list of the *states* in which a member may exist.

- The process starts by an existing member or trust group administrator *nominating* a new member, giving them a user name, establishing their email address, and registering a *vouch* for their trustworthiness.
- Current members of the trust group are notified of the nomination and are then able to *vouch* for the person themselves. Anyone wishing to register a private concern over the trustworthiness of the person can contact a trust group or system administrator to let them know about the concern.
- When a sufficient number of positive vouches is registered, the person reaches the `approved` state and a system password is prepared for secure transmission to the new user to allow them to log in to the portal and complete their account profile.
- Once the new user's profile is complete, their GPG/PGP key is uploaded, and they have registered some vouches themselves to help grow the bi-directional trust network, their account becomes `active` and they begin to receive emails for lists to which they are subscribed.

Other states are reached when users are idle, are blocked because of some serious breach of trust (for example, they are arrested for suspicion of a crime), or they did not receive enough vouches to become active in the first place. The table in Figure *Member state transitions* describes these state transitions.

From	To	Description
NULL	nominated	When somebody nominates you, and mail is sent to vetting@ asking that folks check you out
nominated	vetted	When a cron job detects that you have enough invouches (target_invouches), and notifies admin@ about this)
vetted	approved	When an admin notes that there are no negvouches and manually slots you into "approved" status, and you finally hear for the first time that you are a member, or if that's not implemented yet, it's when a cron job notices that you've been vetted and automatically approves you
approved	active	when a cron job detects that you're approved but that you need to input a pgp (if that's required) and outvouch (if that's required)
active	inactive	When you lose your pgp key or it's suddenly required, or when you used to have enough invouches (min_invouches) but now you don't.)
inactive	active	When a cron job detects that you've outvouched and input a pgp key, and notifies by e-mail you about this
ANY	blocked	When an admin wants the system to camp onto your e-mail address and not allow further state changes or new nominations)
active	soonidle	When a cron job detects that you have not logged in or sent mail for some significant period of time, and sends you mail telling you that you will soon be idle.)
soonidle	active	When you log back into the UI or transmit to a mailinglist.
soonidle	idle	When you go a few more days without activity after being told you will soon be idle
idle	active	Same as soonidle -> active

Fig. 1.1: Member state transitions

State	Description
nominated	means somebody has nominated you but you don't know yet.
vetted	means you've been invouched and you still don't know about it
approved	will someday mean that admin@ has noted your vettedness and noted the absence of controversy about you. Right now you just go from vetted to approved immediately (criteria is identical.)
active	means you've done everything you need to do and the system is not sending you any annoy-o-grams about your checklist
inactive	means you used to be approved but lost your pgp key or lost a vouch or the vouch criteria was raised and now excludes you
blocked	means somebody negvouched you and there's an investigation.
idle	means it's been X days (imagine "60") since you either logged into the UI or sent e-mail to one of the lists.
soonidle	means you will soon be "idle" (we send mail warning of this so that you can log into the portal and prevent going idle.)
failed	means your nomination timed out without reaching "vetted"

Fig. 1.2: Member states and what they mean

The table in Figure *Permissions in each state* shows what permissions apply to a user account in a given state. The table in Figure *Permissions descriptions* details those permissions.

state	can_login	can_see	can_send	can_recv	blocked	hidden
nominated	false	false	false	false	false	false
vetted	false	false	false	false	false	false
approved	true	true	false	false	false	false
active	true	true	true	true	false	false
inactive	true	true	true	false	false	false
blocked	false	false	false	false	true	true
failed	false	false	false	false	false	true
soonidle	true	true	true	true	false	false
idle	true	true	true	false	false	false
deceased	false	false	false	false	true	false

Fig. 1.3: Permissions in each state

Permission	Description
can_login	means your password works at the main web portal UI
can_see	means you can see the membership list and other primary materials, including the wiki
can_send	means you're allowed to send mail to the non-public-access mailing lists
can_recv	means you can receive mail to the subscription-checkbox mailing lists
blocked	means you can't be nominated, nor log in, nor receive or send e-mail, nor be seen

Fig. 1.4: Permissions descriptions

1.3 Trust Group Administration

Attention: The way that the Trident portal is installed and configured using the DIMS Ansible playbooks v 2.14.0, some of the trust group configuration settings are set by the roles `trident-core` and `trident-configure`. As described in Section Backup Directories and Files, any configuration changes made through the `tcli` command line interface, or the Trident portal interface, are independent of the variables in the Ansible inventory used to bootstrap the Trident portal. That means that any changes made interactively will be reverted to what the inventory says they should be the next time the `trident-configure` role is applied.

1.3.1 Trust Group Administrators

There may be more than one administrator in each trust group, depending on the size and the activity level of the trust groups. The larger the group, the more likely you will want more than one administrator to ensure that there are multiple people keeping an eye on the portal and handling trust group policy issues, as well as to make sure there is always someone available in case of emergencies to keep the portal running.

Trust group administrators work with the site administrators to ensure trust policy settings match the desired policy of the organization, including things like branding, icons, domain names, etc.

While there are references in this document to Ansible inventory settings, including excerpts from the inventory file showing the names of variables, this document does not cover the underlying system administration aspects of installing, updating, or patching the underlying operating portal system. It assumes that installation and configuration management of the server(s) providing the Trident web and command line interfaces, Postgres database back end, and Postfix email services were done as described in the DIMS Ansible playbooks v 2.14.0 document. Look to that document for operating system level instructions.

1.3.2 TG Admin Responsibilities

TG admins should familiarize themselves with the history and political issues that may arise when leading trust groups that were mentioned in Chapter *Trust Groups and Trident*. Other things that TG admins should do include:

- Ensuring new TG members are aware of their responsibilities in regards to vetting, vouching, and handling sensitive information. This includes adjudicating issues regarding potential breaches of trust related to publication or public release of information shared in the trust group.
- Working with site administrators to work out and understand disaster recovery procedures in the event of hardware failures, emergency response procedures in the event of system outages during critical events, procedures for account revocation or temporary account disablement in the event of suspected account compromise, or other continuity of operations issues.
- Ensuring accuracy in meeting schedules, availability of dialup or online meeting systems availability for group teleconferences, and other administrivia.
- Handle password recovery and related account maintainence tasks for trust group members.

Most of these tasks can and should be addressed with content placed into the trust group wiki, where trust group members can refer to it whenever they need. This also puts it behind the secure login front end of the portal, so there is no need to share anything in clear text emails beyond an URL referring to the content in the wiki (as long as the path and file name does not expose sensitive information), or just a general reference to "see the TG wiki for more information." Figure *Main TG wiki page* shows what that might look like. (Editing this page is covered in Section *Using the Wiki*).

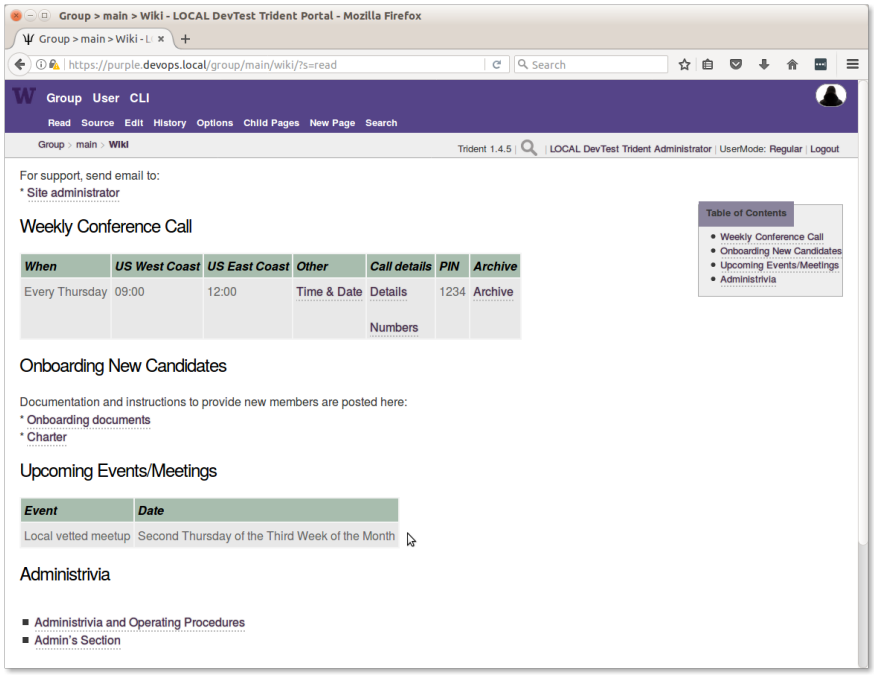

Fig. 1.5: Main TG wiki page

1.3.3 Setting Trust Group Policies

There are a group of policy settings that can be applied to each trust group. They are found in the **Settings** page on the **Group** menu as seen in Figure :ref:

The following subset of variables from the `inventory/trident/nodes.yml` YAML inventory file show those settings that are supported by `ansible-dims-playbooks`. The names of the variables reflect those you would use in `tcli` command lines (`tcli` is the Trident Command Line Interface).

```
trident_site_trust_groups:
  - name: 'main'
    settings:
      descr: 'Main TG'
      pgp_required: 'no'
      has_wiki: 'yes'
      has_file: 'yes'
      has_calendar: 'yes'
      please_vouch: 'yes'
      vouch_adminonly: 'no'
      min_invouch: 0
      min_outvouch: 0
      target_invouch: 0
      max_inactivity: '4320:00:00'
      can_time_out: 'no'
      max_vouchdays: 0
      idle_guard: '168:00:00'
      nom_enabled: 'yes'
```

These are described by pop ups in the **Settings** panel, or can be seen by using the **CLI** option to run `tcli` commands through the portal GUI. To do this, your account must be an admin account, and you must toggle **UserMode** to be **SysAdmin** or use `system swapadmin` before issuing `system set` to see help information about the settings as

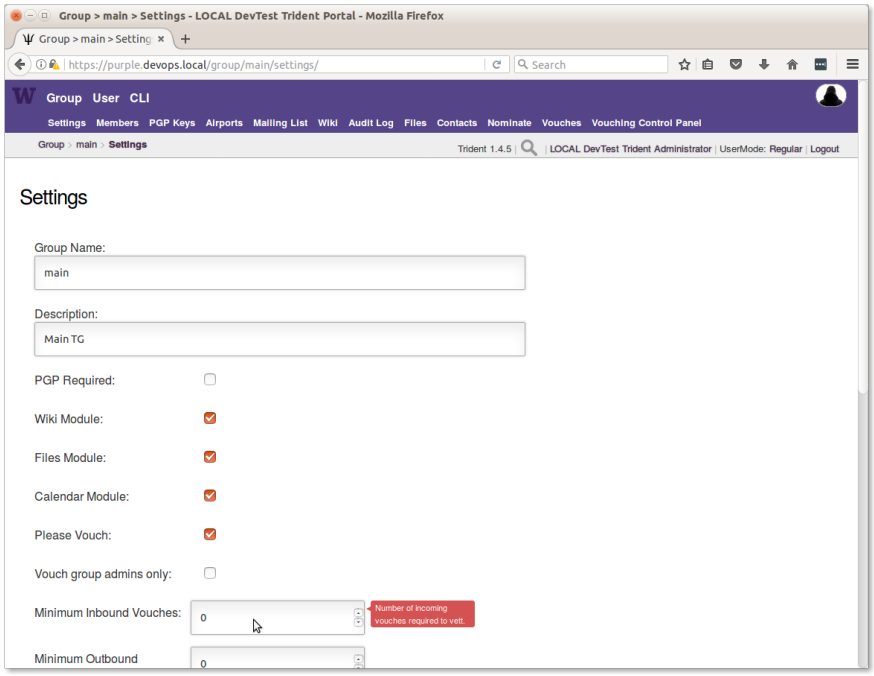

Fig. 1.6: Main TG Settings

shown in Figure *CLI system set (part 1)* and Figure *CLI system set (part 2)*.

You would use `system get` to get the current settings, while `system set` would set them to new values.

1.3.4 Resetting Passwords

Resetting a user's password can be done *directly* by explicitly setting it immediately, or *indirectly* by triggering an email exchange that the user can manage independantly of the system administrator.

You can reset the password or trigger a password recovery operation using the `tcli` command line interface, or the graphical user interface. The use of `tcli` is shown here.

1. Log into `trident`

```
$ tcli system login trident THETRIDENTADMINPASSWORD
Login successful
```

2. Enable system administrator mode.

```
$ tcli system swapadmin
Now a SysAdmin user
```

3. To directly reset the user's password, use the `set` option as illustrated by the following command:

```
$ tcli user password set portal davedittrich NEWPASSWORD NEWPASSWORD
```

Note: The word `portal` in this command specifies the **type** of password being set. In this case, it is the user's portal account.

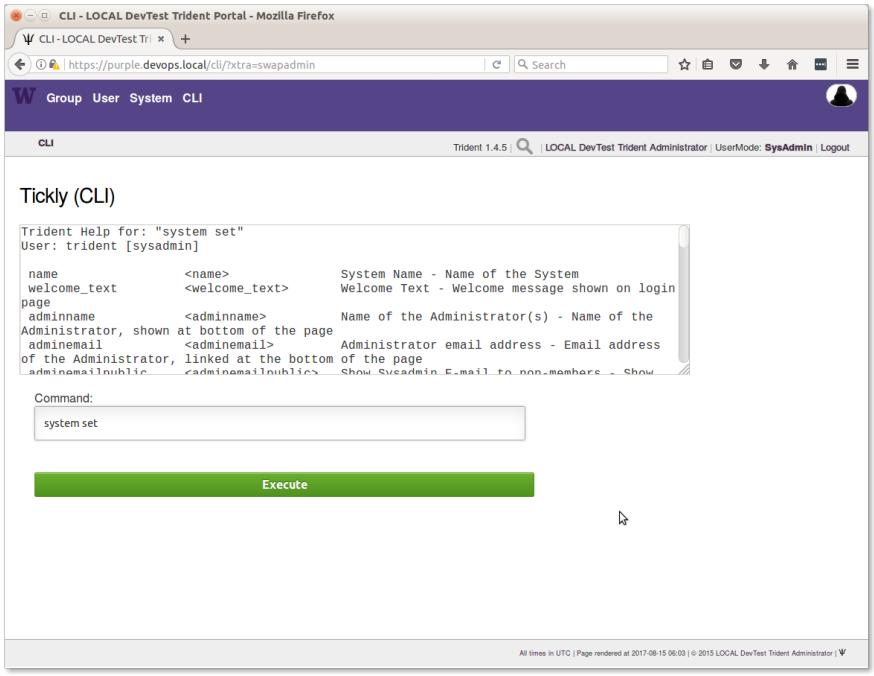

Fig. 1.7: CLI `system set` (part 1)

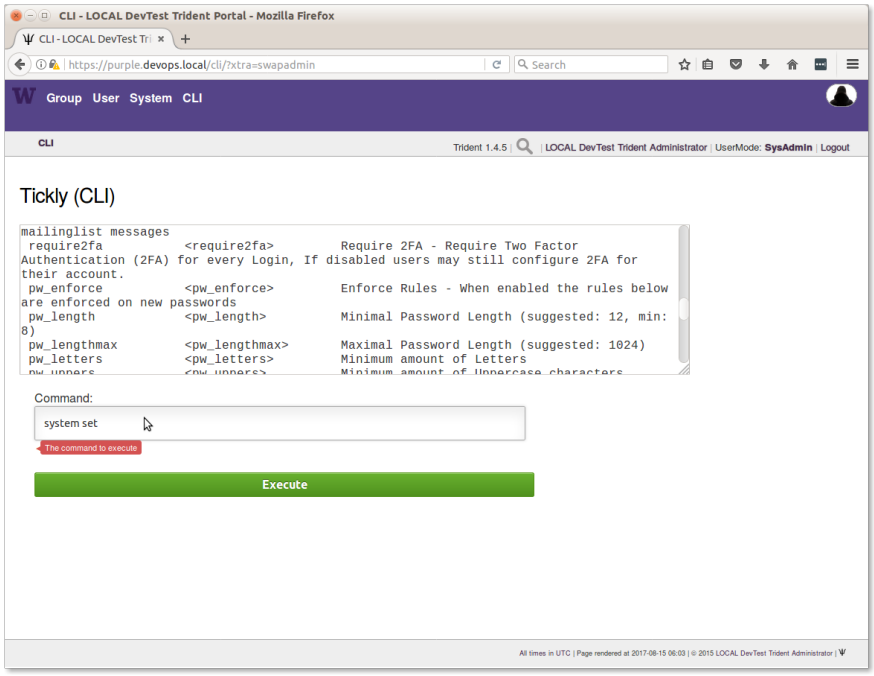

Fig. 1.8: CLI `system set` (part 2)

> **Attention:** If password rules are being enforced by the portal, the string you provide when directly setting the new password **must** conform with the minimum standards as set in **System / Settings**.

4. To indirectly reset the password, use the `reset` optin. Using the account name of the user whose password needs to be reset (in this example, `davedittrich`), and the account name of the person who originally nominated that user (in this example, `trident`), enter the following command:

```
$ tcli user password reset davedittrich trident
Recovery passwords sent to the user and trident
```

5. The user (`davedittrich`) will receive an email that looks like this:

```
From: Trident Portal <bounce@trident.example.com>
Subject: [Trident Portal] Password Reset (User Portion)
To: Dave Dittrich <dave.dittrich@gmail.com>

Dear Dave Dittrich,

A password reset request was made.

We are therefor sending you two token portions.
The user portion is in this email, the other portion
has been sent to your nominator who will forward it in
a secure method towards you.

Your nominator is:
 Trident Administrator <dittrich@u.washington.edu>

When both parts have been received by you, please proceed to:
  https://trident.example.com/recover/
and enter the following password in the User Portion:
  3zXhvsJ1LRkH-27d

If you do not perform this reset the request will be canceled.

Regards,
  Trident Administrator for Trident Portal

--
Trident Portal -- https://trident.example.com
```

6. The nominator (`trident`) will receive an email that looks like this:

```
From: Trident Portal <bounce@trident.example.com>
Subject: [Trident Portal] Password Reset (Nominator Portion)
To: Trident Administrator <dittrich@u.washington.edu>

Dear Trident Administrator,

A password reset request was made for:
 Dave Dittrich <dave.dittrich@gmail.com>

As you are a nominator of this person, you are receiving
the second portion of this email.

Please securely inform Dave Dittrich
of the following Nominator Portion of the password reset:
```

```
  p5Am9Agk8H09M6s0

Regards,
  Trident Administrator for Trident Portal

--
Trident Portal -- https://trident.example.com
```

The nominator should now follow the instructions and securely communicate the nominator portion of the recovery key to the user, such as over a telephone call, through encrypted email, etc.

Note: Since the recovery key is split into two parts, it will be difficult (though not entirely impossible, depending on the situation) for an adversary to obtain both parts of the recovery key without the user being aware.

7. Once the user has both portions of the recovery key, they follow the link in their copy of the email and enter their username, both portions of the recovery key, a new password, and again to confirm the password, then press the button to reset the password. After this, they will receive a confirmation email that the password has been reset.

```
From: Trident Portal <bounce@trident.example.com>
Subject: [Trident Portal] Password changed
To: Dave Dittrich <dave.dittrich@gmail.com>

Dear Dave Dittrich,

Somebody (probably you) has changed the password associated to your account:
  dave.dittrich@gmail.com

If you did not change your password, please reply to the administrator at:
   Trident Administrator <dittrich@u.washington.edu>
and we will try to figure out what went wrong.

Regards,
  Trident Administrator for Trident Portal

--
Trident Portal -- https://trident.example.com
```

Attention: Users should be told that if they *ever* receive an email notification that their password has been changed and they did not participate, they should immediately use another email account or communication mechanism (such as a phone call) to inform the system administrators about the suspicious activity!

1.4 Trust Group Member Activities

1.4.1 Using GPG or PGP Encrypted Email

Encrypting email messages using public/private key cryptography is one of the core means of protecting electronic communications, both in transit as well as in storage. One of the first programs to gain wide-spread use for encrypting email communications was Phil Zimmerman's Pretty Good Privacy (PGP). PGP eventually become a commercial product, prompting development of a compatible free alternative as part of the GNU project known as GNU Privacy

Guard (GPG).*[0]

While GPG/PGP may be disliked by many because of the complexity of managing time-limited keys, signatures that are used to create trust chains, and contents of key rings, these programs do work well and there aren't any viable alternatives that are available freely and in widespread use. They also support things beyond just encrypted email.

Public/private key cryptography also supports creation of digital signatures of messages and files that prove they were created by the person in control of the private key used to sign the message or file.†[0] Cryptographic hashes like SHA256 can be used to verify the integrity of a file by comparing the hash, so they are often provided along side software packages to help validate the integrity of that software. But if someone can gain access to the distribution server and alter both the software package file *and* the hash of that file (which are usually both stored on the same server), they can slip a trojan horse through the gate! For this reason, the files containing hashes for integrity validation are often signed with PGP to verify both their integrity as well as who produced them. The same technique can be used with PGP to sign files containing Indicators of Compromise, intrusion reports, or log files extracted from compromised hosts to help prove *chain of custody* of potential digital evidence. For this reason, incident responders should know how to produce timestamped signed files using PGP.

PGP keys and the GPG library are used internally to Trident to support encrypted email lists. Every list has its own key generated internally, allowing any list member to encrypt a message *to the list address*. The internal email processing scripts decrypt the message, then re-encrypt it to each list member using the list's private key and the list member's public key, ensuring that all list traffic is encrypted in both directions. This is a very powerful capability that helps trust groups maintain secure communications about very sensitive topics. Every trust group members' PGP key is available, along with every key for every list that someone is subscribed to, when you select **PGP Keys** in the sub-menu for the selected trust group. Keys should be updated regularly to deal with trust group membership and list subscription changes.

Because PGP keys are so fundamental to encrypted email in Trident, one of the very first tasks that a new user must perform is to upload a PGP key. This is covered in Section PGP Keys of Trident Training Manual v 1.0.3.

If you have not used PGP before, take some time to review the following guides to get a complete picture of how public/private key cryptography works in general, and how PGP works in particular with email clients like Thunderbird with Enigmail.

- EMAIL SELF-DEFENSE guide, Free Software Foundation
- An Introduction to Public Key Cryptography and PGP, Electronic Frontier Foundation

For step-by-step instructions, EFF has the following guides that are very helpful:

- Surveillance Self-Defense tutorials, Electronic Frontier Foundation + How to: Use PGP for Linux + How to: Use PGP for Mac OS X + How to: Use PGP for Linux

1.4.2 Vouching in the Vetting Process

Vouching for someone is a serious matter. It is a public attestation of trust in someone else. The Trident portal vouching panel has three toggles that are required to be enabled as part of the attestation before a nomination will proceed:

- **I have met them in person more than once**
- **I trust them to take action**
- **I will share membership fate with them**

By answering these questions in the affirmative, it means that you have had sufficient personal experience with someone to warrant trust in them to use information provided to them to minimize harm to those being victimized on the

[0] The phrase "in control of the private key" is important to understand here. The digital signature validates which private key produced the signature, but that may not be the same person who has a copy of the private key. If someone's account is compromised, so is their private key. For this reason, a strong passphrase on the private key helps (but it, too, can be captured by keystroke logging, shoulder surfing, etc. Pay attention to the referenced guides' advice on securing your private key.

[0] For the purpose of this document, and because the Trident portal uses the acronym internally, **PGP** will be used to refer to both GPG and PGP.

Internet and to keep that information secure to minimize any negative consequences to those countering the activity of the criminals who are harming these victims. Should they breach the trust placed in them resulting in a decision by the group to expel them, you may also be expelled.

There is a *vouching control panel* intended to facilitate this process when the group gets large. You can read the reasons for its existence, and how to use it, on the page (see Figure *Vouching Control Panel*).

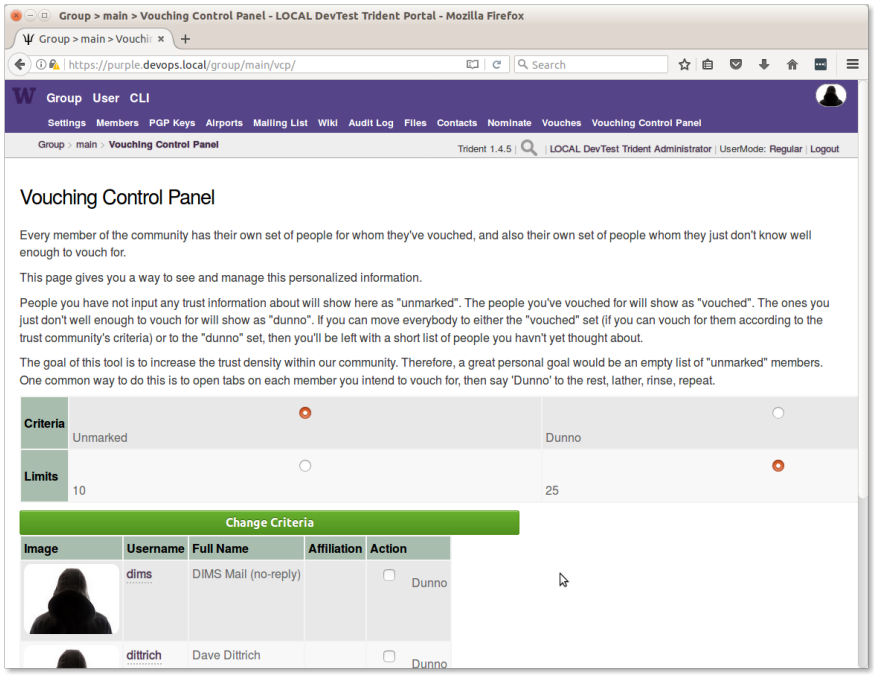

Fig. 1.9: Vouching Control Panel

All members should spend the time to vouch for everyone they can, to help grow and strengthen the trust fabric. This is important to have in place prior to an urgent active threat situation, when those responding come across information related to intermediary systems (e.g., "stepping stones" or command and control resources). When someone has no experience with any staff at an involved intermediary site, there is no way to know if the person you reach out to will be helpful, or whether they are protecting the criminals and will lie to you and inform the criminals that someone is on to them.) Being able to identify someone, and identifying someone you trust who in turn trusts them, allows this contextual transitivity of trust to guide decisions about who to inform and what to say.

1.4.3 Nominating a New Member

To nominate a new member, you are first asked to search for an email address. This will identify whether the person you wish to nominate is already in the nomination process (or a member). If they are not found, you are prompted to fill in some of the information to start their profile, which includes:

- Full name
- Affiliation (e.g., `@their-company.com`)
- A short biography (they can update it later if they don't like it)
- A vouch comment (e.g., "I have known John Smith and worked with him on several incident responses over the past five years.")

You must then toggle on each of the three attestations described in Section *Vouching in the Vetting Process*.

An email will be sent confirming the nomination has started, asking that the nominator let others know about the nominee to seek vouches from people who are willing and able to vouch.

When a sufficient number of vouches has been received, and a trust group administrator has approved the successful nomination in the portal, an encrypted email message is sent to the nominator with the new member's password and instructions on how to securely provide the password to the new member. The member must change their password on initial login, so they will be the only one to know their portal password.

Note: Trident supports the use of multiple forms of second-factor authentication, or **2FA**, which site administrators are encouraged to require by policy, or at least enable for members to use. This is a simple mechanism, with only a little added friction and cost, to defeat password guessing or password theft due to phishing or keystroke logging. The **2FA Tokens** page is shown in Figure *2FA Tokens Registration Page*.

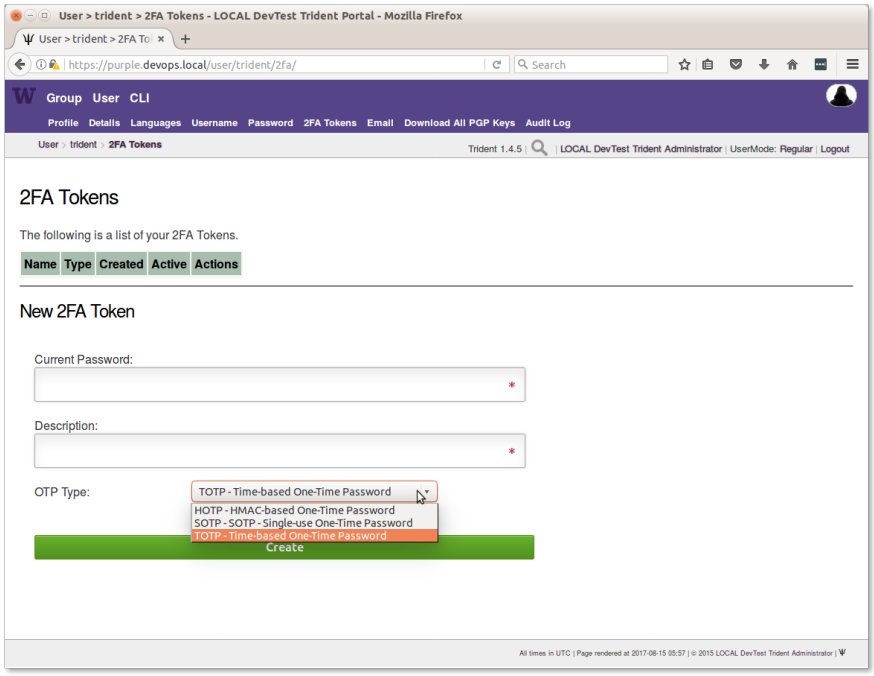

Fig. 1.10: 2FA Tokens Registration Page

1.4.4 Requesting a Password Reset

When requesting a password reset,

```
Dear John Smith,

A password reset request was made for:
 Bobby Tables <littlebobby@drop.table.example.com>

As you are a nominator of this person, you are receiving
the second portion of this email.

Please inform Bobby Tables
of the following Nominator Portion of the password reset:
   XhXblRH_6c5BWul
```

```
Regards,
  LOCAL DevTest Trident
```

Note: Password resets are a very frequent occurrence, which means they have a high system administration overhead cost. Upcoming changes to the Trident portal should result in the password reset behavior changing to be a little more flexible and easier to perform.

- If the user has a PGP key configured in the portal, send them an email with their new password with the message encrypted to their public key.
- If no PGP key is available, send 1/2 of the recovery token to the nominator and the other half to the user in cleartext email like the portal does now. (The nominator should still communicate their portion to the user using an out-of-band mechanism (e.g., a phone call or SMS message.)
- A possible 3rd option would allow a system administrator or trust group administrator to see 1/2 of the token in the portal, with the other 1/2 of the token being sent directly to the trust group member.

1.4.5 Using the Wiki

Trident supports a built-in wiki that uses a version of the Markdown language for simple formatting. When the wiki is enabled in the system settings, the word **Wiki** appears on the submenu for the selected Trust Group (e.g., **Main TG**). Each trust group has its own wiki.

Use of the wiki is described on the Trident Wiki page. Figure *Editing the Main TG wiki page* shows what it looks like when editing the Main TG wiki page from Figure *Main TG wiki page*.

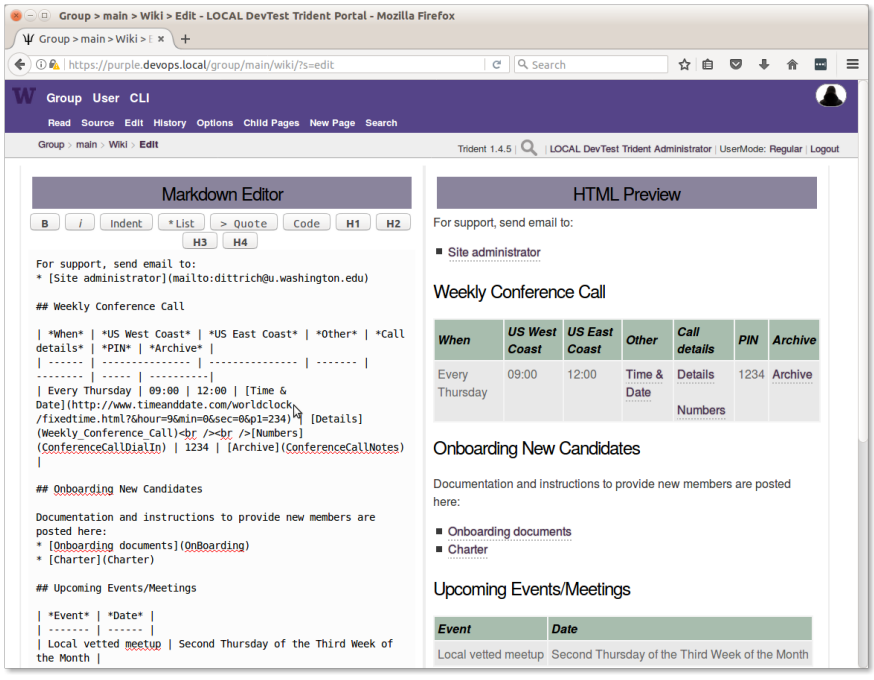

Fig. 1.11: Editing the Main TG wiki page

1.4.6 Adding Files

When file upload is enabled in the system settings, the word **Files** appears on the submenu for the selected Trust Group (e.g., **Main TG**). Each trust group has its own file storage.

- Users can **Add a new directory** to create a folder in which to store files.
- Users can **Add a new file** to the selected directory folder.

Figure *Creating a directory path* shows how to create a nested directory using a multi-component directory path.

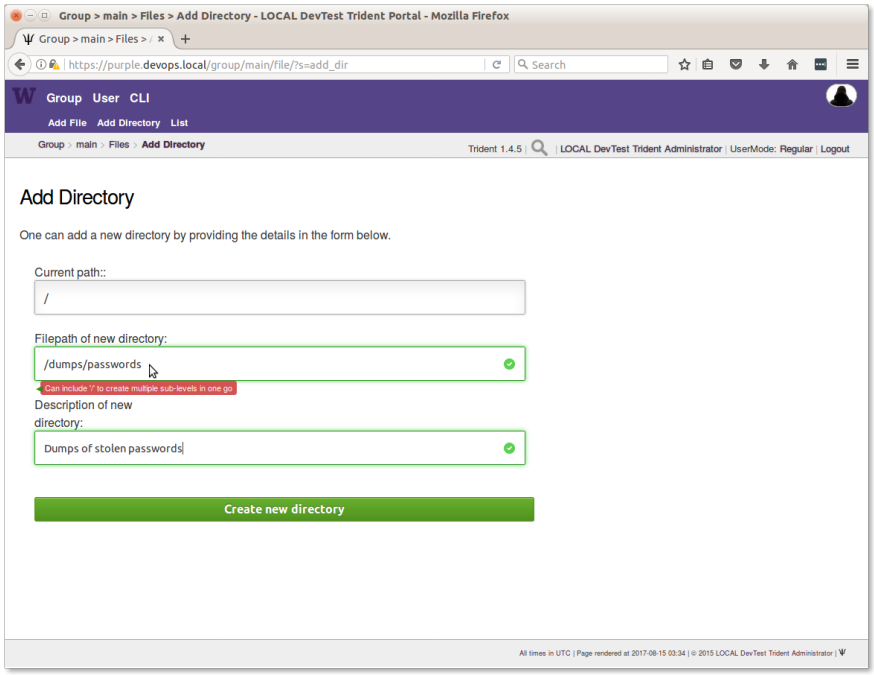

Fig. 1.12: Creating a directory path

Note: It is a good idea to organize files into directories, rather than just have all files in one place. Start with a set of top level directories to categorize things at a high level, then use subdirectories within those categories to further organize content. The structure to use will vary, depending on requirements, but some organization is warranted to make it easier to find files as the number of files grows.

Caution: Pay **very close attention** to the directory for dumps, which was purposefully named `/dumps/unclassified_programs`. While it has become common for dumps of stolen **SECRET** and **TOP SECRET** documents and programs to be made public on leak web sites, or found in underground web sites, this does not mean they can or should be freely accessed and shared within trust groups. Their presence should be reported to federal law enforcement agents immediately to allow them to deal with uncontrolled classified materials.

Trust group administrators should make it **very clear** to all TG members that they should **NEVER COPY LEAKED PROGRAMS OR FILES MARKED "CLASSIFIED SECRET" OR "CLASSIFIED TOP SECRET" OF ANY KIND** into the portal. **Ever**! To do so puts trust group members who hold national security clearances in a problematic position in which they must legally report the files, which must be scrubbed from the system by cleared personnel. This is a very disruptive and time consuming process that could get you expelled from the trust group and/or interviewed by federal law enforcement agents.

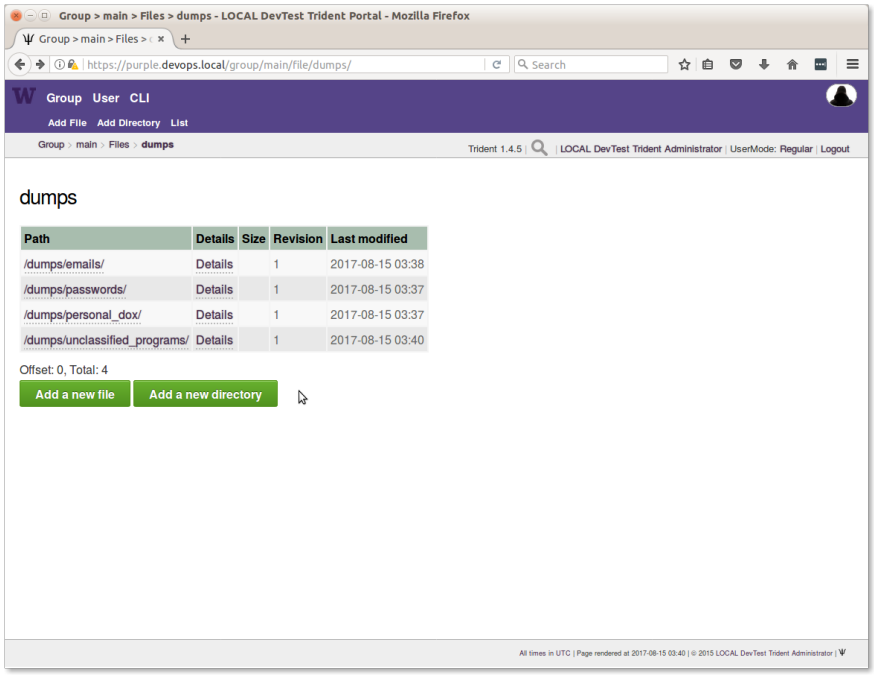

Fig. 1.13: Main TG files/dumps/ directory

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>