Alan Turing Institute Research Computing Service Documentation

Release 1.0

EPCC

Jan 08, 2020

Helpdesk

The Alan Turing Institute Research Computing Service are data science platforms hosted by EPCC for the Alan Turing Institute.

The Alan Turing Institute Research Computing Service consists of:

- a Helpdesk, run by EPCC.
- the Alan Turing Institute Remote Access Service (Atiras), a Secure Safe Haven with an Intel cluster.

Note: the Cray Urika-GX service was closed on 31st December 2019.

This documentation contains:

- *Helpdesk*: general information on how to contact the Helpdesk.
- *SAFE Documentation*: general information on how to use the Turing's SAFE for helpdesk and support, managing user accounts and project research computing resources, and obtaining resource usage reports.
- *Atiras, Secure Safe Haven and Intel cluster User Guide*: general information on how to access, connect to and use Atiras.

How we collect, use and share information about your use of the service are explained in the *Alan Turing Institute Research Computing Service Personal Data and Privacy Policy*.

How the information you provide is used to administer your use of the services through SAFE is explained in the SAFE Privacy Policy.

CHAPTER 1

Contents

1.1 Alan Turing Institute Research Computing Service Helpdesk

This chapter contains information about the Helpdesk for the Turing's Research Computing Service. This Helpdesk is run by EPCC.

1.1.1 EPCC Helpdesk

The Helpdesk is the first point of contact for all questions relating to the Turing's Research Computing Service hosted by EPCC.

Support is available Monday to Friday from 08:30 until 18:00, excluding UK public holidays.

The Helpdesk can be reached by e-mail research-computing-support@turing.ac.uk.

Please try and provide as much background information as possible as this will speed up the processing time considerably. Existing Research Computing Service users will be asked for their user ID, project code, and, where applicable, the commands they are using and the error message they get.

1.1.2 How the helpdesk ticket system works

When a query is submitted by email it is placed in the Turing's SAFE query system (see *Alan Turing Institute SAFE Overview*).

When you email your query, you will normally get an automatic acknowledgment by email, including a tracking ID, within a few minutes. If you submit your query through SAFE, it will give you a tracking ID at once. A few minutes later, your query will be assigned to the appropriate expert within the Turing to handle.

The expert may contact you to discuss your problem or to get extra information.

Finally, the expert will send you an answer, and the query will be closed. At this point the helpdesk will send you another message, telling you that this has happened.

Closed queries are kept in the Turing's SAFE database, so that we can refer back to them when solving future problems, and when writing documentation, etc.

The Turing's SAFE database is protected by the *Alan Turing Institute Research Computing Service Personal Data and Privacy Policy*.

1.2 Alan Turing Institute Research Computing Service Personal Data and Privacy Policy

Information about you: how we use it and with whom we share it

In the Terms and Conditions of Access, the service undertakes to observe this Policy.

This policy applies to personal data about users of the Turing's Research Computing service. It relates to data gathered on the service itself.

The details that you provide on registration are stored in the Turing's SAFE and will be processed according to the Turing's SAFE privacy policy.

We will store in the service's database the personal data you supply to us through the website, when you register as a user of the service and later.

We will also store in the database details of your use of all aspects of the service, including, for example, the amount of processor time and storage space you use, the courses you attend and the queries you send to the helpdesk. This may include some personally identifiable data such as the network addresses you use to connect to the system.

We will use this information to help us manage and administer the service, to review, analyse and audit its performance, security, its patterns of use, and to plan for the future.

This information will be available to appropriate members of the staff who are working on the Turing's Research Computing Service. They will also be available to the Principal Investigator of your research project and to anyone whom the PI designates as a manager of the project.

Resource usage information will be uploaded to the SAFE where it will be processed according to the SAFE data privacy policy.

Periodically, the service will be examined by auditors acting on behalf of your funders, and they may see your personal data. They will be acting under conditions of professional confidentiality.

We reserve the right to monitor your use of the service, including anything you transmit over the Internet, and any data or software you store on our systems, in order to ensure that you and all the other users are complying with the Terms and Conditions of Access and not breaking the law. We must allow any court or other competent authority to inspect our records of your use of the system, or your data, and to take copies of it, if this is legally required; and we must report your activities to the competent authorities if we know or suspect that you are breaking the law. These are legal obligations for us.

We would not be able to administer the service properly, nor adequately account to our funding bodies for our conduct of this project, without processing your personal data in our database in this way. For this reason, we have to ask you to consent to this policy. This consent is included in the Terms and Conditions of Access.

We may retain the data that we gather on the system for the duration of the Turing's Research Computing Service. Data that could be used to identify you directly will not be retained longer than two years after the end of the service.

If you have any questions about the treatment of your personal data, please email the Helpdesk at research-computing-support@turing.ac.uk.

1.3 Alan Turing Institute SAFE Overview

The Turing's SAFE is a web-based application that is used for:

- Administering Alan Turing Institute Research Computing Service user accounts.
- Managing account a project resources (kAU, disk quotas, etc.)
- Reporting on usage of the system.
- Helpdesk and support.

1.3.1 SAFE for individual users

All users have accounts on the Turing's SAFE through which they can view the resources they have access to, administer their account, query their usage of the service, and submit support requests.

More information on performing these tasks can be found in *SAFE for Individual Users*.

1.3.2 SAFE for project leaders

Project leaders (PI's and any designated project managers) can also use the Turing's SAFE to approve requests to join the project, manage their project resources on the Turing's Research Computing Service, and generate reports on the project usage on the Turing's Research Computing Service.

More information on performing these tasks can be found in *SAFE for Project Leaders*.

1.4 SAFE for Individual Users

The Turing's SAFE is an online user service management system. Through SAFE, individual users can request machine accounts, reset passwords, see available resources and track their usage. All users must be registered on SAFE before they can apply for accounts on the machines in the Turing's Research Computing Service.

1.4.1 Registering, logging in, passwords

Register on SAFE

1. Go to SAFE New User Signup Form
2. Fill in your personal details. You can come back later and change them if you wish
3. Click "Register"
4. You are now registered. Your SAFE password will be emailed to the email address you provided. You can then login with that email address and password

At this point your account is registered on SAFE but you do not have a machine account on the Turing's Research Computing Service.

To obtain a machine account on the Turing's Research Computing Service you require a *Project Code*. Your project's PI or Project Manager should be able to supply you with these details. Once you have them you should:

1. *Login to SAFE*.
2. *Request an account for a Research Computing Service machine*.

Login to SAFE

1. Go to SAFE
2. Type in the email address you have registered with.
3. Type in your SAFE password.
4. Click "Login".
5. You are now on the Main Page and here you can see menus along the top which give access to SAFE functionality.

Change your personal details on SAFE

1. *Login to SAFE*.
2. Go to the menu *Your details* and select *Update personal details*
3. Make the changes you wish
4. Click *Commit Update* to save the changes
5. Go back to *Your details* and you will see the revised information

Do not forget the last step, or nothing will happen.

Note: your postal address does not automatically include the name of your department and institution; if you want these in your postal address, you must type them again.

Change your email address on SAFE

1. *Login to SAFE*.
2. Go to the menu *Your details* and select *Update email*
3. Enter the new email address and click *Request*

A verification email will then be sent to the new email address. This email contains a link which you must use to verify your new address. On acknowledging your new address the change will be committed and you must use the new email address when logging into SAFE.

Change your SAFE password

1. *Login to SAFE*.
2. Go to the menu *Your details* and select *Change SAFE password*
3. Fill in the boxes and click *Change*

Reset your SAFE password

1. *Login to SAFE*.
2. Enter your email address
3. Click *Email*
4. The SAFE will mail your password to your email address.

SAFE will only mail to email addresses it already knows. But email is not a secure medium, so if you change your password this way, you should immediately change it again from inside SAFE.

Note: anyone could go to SAFE, type your email address and request a new password by clicking "Email". If that happens you will receive an email message out of the blue saying that your password has been changed. In this case you should change your password again as soon as possible.

Request an account for a Research Computing Service machine

1. *Login to SAFE*.
2. Go to the menu *Login accounts* and select *Request login account*
3. Choose the project code for the machine you want from the *Project* pull-down list.
4. Then press *Select Project*. A new screen will appear.
5. Press the radio button next to the machine you want the account for then press *Select Machine*.
6. In the field next to *Request username*, enter the username you would prefer to use on this machine.

   Every username must be unique, and you must create a new machine account with a unique username for each project you work on. Usernames cannot be used on multiple projects, even if the previous project has finished.
7. Accept the Terms and Conditions of Access by clicking the appropriate button.

When you do this, you will be sent an acknowledgment by email, which will include your SAFE password — you should change this as soon as possible.

You will have to wait for your PI or project manager to accept your request to register. When this has happened, the systems team are prompted to create your account on the machine. Once this has been done, you will be sent an email. You can then *Get your password for the service machine* from your SAFE account.

Get your password for the service machine

Wait till you receive the email with your details. Then:

1. *Login to SAFE*.
2. Go to the menu *Login accounts* and you will see your account on the machine listed. Click *username*
3. This will display details of your account. Click *View Login Account Password* You will need to enter in your SAFE password and then click *view*, and you will see your password to the machine

This password is generated randomly by SAFE. It's best to copy-and-paste it across when you login to the machine.

Reset the password on your machine account

If you have forgotten your current password, or it has expired, then you can ask for it to be reset:

1. *Login to SAFE*.
2. Go to the menu *Login accounts* and select the account you need the new password for
3. Click *username* which displays details of this machine account.
4. Click *New Login Account Passwd*

The systems team will change your password. When this has been done, you will be informed by email; this means that you can come back to SAFE and *Get your password for the service machine*.

Change a password on your machine account

This is machine-specific.

Note: When you change your password on machines in this way, the changes are **not** reflected on SAFE, so please remember your new password.

hydra-vpn.epcc.ed.ac.uk gateway:

1. At the command-line, run:

```
passwd
```

2. You will be prompted to enter your old password.
3. You will be prompted to enter your new password twice.

Alan Turing Institute Cray Urika-GX Service:

1. At the command-line, run:

```
change_ldap_passwd
```

2. You will be prompted to enter your new password twice.
3. You will be prompted to enter your old password.

Atiras portal:

1. Go to the Atiras portal home page.
2. Click the menu labelled by your username at the top-right of the page.
3. Select 'Settings'.
4. **Fill in the following fields:**
    - 'Current Password'
    - 'New Password'
    - 'Confirm New Password'
5. Click 'Update Password'.

Atiras Secure Safe Haven and build arena virtual machines:

If running a SSH (secure shell) session, or from terminal window in an RDP (remote desktop) session:

1. Run:

```
passwd
```

2. You will be prompted to enter your old password.
3. You will be prompted to enter your new password twice.

Alternatively, if running an RDP (remote desktop) session:

1. Click the button icon on the top right hand side of the desktop.
2. You will be presented with a dialog box. Click your user name then select 'Account Settings'.
3. Click '<your-virtual-machine-username>' on the row of user names.
4. Click the button (with five blobs) next to the 'Password' field.
5. **Fill in the following fields:**

- 'Current Password'
- 'New Password'
- 'Verify New Password'

6. Click 'Change'.

1.4.2 User Mailing Options

View user mailings

All mailings are archived and can be viewed in SAFE.

1. *Login to SAFE*.
2. Go to the section *View user mailings*.
3. Press the *View* button to access the mailings.

Join, or leave, a mailing list

There are three mailing lists available.

- *Major Announcements* mailings contain information on major service upgrades and future plans. All users are subscribed to this list by default.
- *Service News* mailings contain information on training courses, newsletters, events, and other general announcements. All users are subscribed to this list by default.
- *System Status Notifications* inform users when the service goes up or down, including the reminders of the next planned maintenance shutdowns. Users are not subscribed to this list by default. You will need to explicitly subscribe to this list if you wish to receive these emails.

You can subscribe to any combination of these email lists via SAFE:

1. *Login to SAFE*.
2. Go to the menu *Your details* click *Email list settings*
3. In the panel headed *Mailing list preferences* click on the mailing lists you would like to subscribe to.
4. Click *Update List Preferences*

If you wish to unsubscribe from user mailings completely:

1. Click on the menu *Your details* click *Update personal details* find *Opt out of user emails* field and click it.
2. Click *Commit Update*. Do not forget this step, or nothing will happen.

Note: This overrides any option enabled in *Mailing list preferences* panel.

Note: Regardless of whether you are subscribed to a particular mailing list, you can still view **all** user mailings which have been sent, from within SAFE. See *View user mailings* for details.

1.4.3 Tracking and Managing Available Resources

Check how much time and space are available to you

1. *Login to SAFE*.

2. Go to the menu *Login accounts*.
3. Select the *username* which you wish to see details for.

You will then see the information for this account. You will see the quotas for disk space (if your project group is using these) and how much is in use.

You can also see which file systems your project is using. Under the heading *Volume* you will see entries for RDF (if used by your project), *home* and *work* and in brackets after each, the name of the file system they are hosted on, followed by the current usage by your project, and total quota.

The budget values displayed are updated every morning, and the values shown for disk use are updated four times a day. For this reason, all these values may not be completely up-to-date. If there is a lot of activity in your project, the numbers shown could be significantly different from from the current ones.

Request more kAUs/disk space

In the first instance, please contact the principal investigator, or the project manager of your project. The PI will then take the necessary steps to either allocate you more resources out of the project reserve, or to request an increase from the helpdesk/research councils.

The helpdesk does not own project resources and has no authority to allocate them to individual users. This responsibility lies with the project PI/project manager.

Review the use you have made of the service, or the activity of the service as a whole

1. *Login to SAFE*.
2. Go to the menu *Service information* and select *Report Generator*.
3. Select the report you wish to run and the format you want the output in (web, PDF, CSV, XML) by clicking the appropriate icon in the list.
4. Complete the required information in the form: this will usually consist of at least a date range to analyse and may have other options depending on the report you are running.
5. Click *Generate Report*.

If you are a PI or Project Manager, you will have access to additional reports to generate information on whole projects or groups as well as your own usage and the usage of the service as a whole.

1.4.4 Miscellaneous

Check the queries you have submitted to the helpdesk

1. *Login to SAFE*.
2. Go to the menu *Help and Support* and select *Your support requests*.
3. Click the number of a query to check the contents of the query log.

This will show you the queries of yours that haven't yet been resolved.

Note: some of the internal correspondence about a query will not be shown.

You can also use SAFE to submit a query — use *New support request*.

Register your approval — or your annoyance

1. *Login to SAFE*.
2. Go to the menu *Help and Support* and select *Service feedback*.
3. Click on the scale somewhere between 5 penalty points and 5 gold stars indicating your level of anger or delight.
4. Optionally: enter a comment in the comment box.
5. Click *Set Token*.

The tokens may appear in the public service reports, although your name will not be published with them. Although an entry in the comment field is optional, it necessarily gives greater weight to your feelings - without it we cannot tell why you have set a token.

1.5 SAFE for Project Leaders

Project Leaders can manage the resources and users associated with their projects through the Turing's SAFE.

1.5.1 Getting Started

Your allocation has been set up as a project on the service. Your first steps.

Here are some of the things you should consider doing; not all of them will be needed for every project:

1. Change your SAFE password.
2. *Get your own account on a Research Computing Service machine*.
3. *Register project users*.
4. *Designate a user as a project manager*.
5. Decide whether to *Set up project groups within your project*, in order to administer time and other resources.

Get your own account on a Research Computing Service machine

If you are not going to work on the machine yourself, you do not need to do this. You can administer your project through SAFE alone. But if you want a machine account:

1. Login to SAFE.
2. Go to the menu *Login accounts* and select *Request login account* button.
3. Select the desired project from the pull down list and click *Select Project*.
4. Select the desired machine from the pull down list and click *Select Machine*.
5. Enter your Requested username and click on *Request*.

You will get an acknowledgment screen, from which you can return to your main page. Now (as a project leader) you have to accept your own request for an account, see *Register project users*.

Check project alerts

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to check.
3. This will display a page with a variety of options for managing your project.
4. Project alerts and warning are highlighted in Amber and Red.
5. To request emails for alerts, or to change the frequency of the emails.
6. Click *Update*.
7. Beside "Frequency of Alerts" select the required frequency.
8. If the emails should go to someone other than the PI, enter the email address(es) into the 'Recipients for alerts' box.
9. Click *Update* to save the changes. Do not forget this step, or nothing will happen.

1.5.2 Managing your allocated resources

What is "period allocation"?

A period allocation contains kAUs which have been allocated for a project to use within the specified time period. Period allocations are valid for a specific resource pool (machine) and have definitive start and end dates. When the end date of the period allocation passes, any leftover kAUs will automatically expire.

View and manage your period allocation

You can view and manage your period allocation via SAFE.

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to work with.
3. This will display a screen with a variety of options for managing the project.
4. Click on *Manage Project Resources*.
5. Click on *Manage Group Time Allocations for Resource Pool (ATI)*.

You will then see the details of your allocation. *Please check them carefully to make sure you are looking at the correct one.*

- **Resource Pool (machine)**. "ATI" refers to the Turing's Research Computing Service.
- **Amount of kAUs**.
- **Dates** It is possible to have multiple successive period allocations, but they can never overlap if they are for the same resource pool. Before carrying out any project management tasks please check the dates and make sure you are managing the correct allocation.

You can skip between the period allocations by clicking on the ">>>" (next period) and "<<<" (previous) buttons at the bottom of the page.

To manage the allocation, see:

- *Set up project groups within your project*
- *Administer time within your project*.

Project management tasks for the period allocation can be carried out at any time, but the allocation will be active, i.e. usable, only between the specified dates. Thus, you can set up project groups in advance.

Set up project groups within your project

Project groups can be used to administer time and other resources within your project.

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to create the group.
3. This will display a screen with a variety of options for managing the project.
4. Click *Project Group Administration*.
5. Click *Add new sub-group*.
6. This will take you to the screen for creating new project groups.

   Fill in a suffix to your project code in the box: for example, if your project code is t01, you might chose t01-a. Project group names cannot be more than eight characters in total.
7. If this group is to be used for guest budget users, tick "Guest Budget".
8. Click *Create*.

Single user accounts can only belong to one project group.

Delete a project group

You can only delete a project group if it has no resources or members. You must remove all its members (see *Remove a user from a project group*) and all its time (See *Move time between budgets*). Also, if it has disk quotas set (see *Administer disk space*), it cannot be deleted; they will have to be removed first. Then:

1. Go to the menu *Projects managed* and select the *project* you wish to delete the sub-group from.
2. Click on *Project Group Administration*.
3. Select the project sub-group you want to delete. You will only be able to select the groups which have no time, space or members.
4. Click *Delete*. This will ask for confirmation that you wish to delete the sub-group.
5. Click *Yes*.

Deleting a group involves removing its various directories. The systems team has to do this, so there will be a short delay.

Administer time within your project

Time is measured in *allocation units* (kAUs), and is held in *budgets*. Every project group has its own budget. There are always at least two project groups in your project:

- *general group*: This has the same code as the project itself. Every member of the project is a member of this group, so the time in its budget is available to them all.
- *reserve* project group. This has a name of form *t01-reserve*. It has no members, so no one can use the time in its budget. This budget can be used to hold time which the PI or project manager wishes to hold in reserve for later use.

Initially, all your time is in the general group's budget. If you are happy with all your users using the same budget, you can leave things as they are.

If you wish to divide the time up between groups, you can *Set up project groups within your project*. In this case you will probably want to move all the time out the general group, since this can be used by everyone.

You may wish to *Allocate time to a single user*. This is a special case of a project group: one with only one member.

The reserve budget is provided so that if you wish you can control the use of time by your project members: you can keep most of the time in your reserve budget, and move it to the other budgets as required. We recommend that you should do this, even if you don't need to create other project groups.

Move time between budgets

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to work with. This displays a panel with information for the project.
3. Click *Manage Project Resources*.
4. Click *Manage Group Time Allocations for ATI*.
5. Click the *Move From* and *Move To* buttons of the project groups you want to change.
6. Enter the number of kAUs you wish to move in the box.
7. Click the *Submit Budget Allocation Changes* button. Do not forget this step, or nothing will happen.

Allocate time to a single user

As all the time in a project group is shared by all its members, the only way to reserve some time for a single user is to create a project group for that user alone.

1. Create a group for the user (see *Set up project groups within your project*). For example, if we are in project *t01* and the user is *fred*, you might call the new project group *t01-fred*.
2. Add the user to the group (see *Add users to an existing project group*).
3. *Move time between budgets* into the new project group so that the user has the time you want them to have.

Remember that time in the general group's budget is accessible to all, so you will probably want to move all of the project's time away from there.

Administer disk space

Start by reading about how to *Administer time within your project* as the administration of disk space is related to this, and is also done using project groups. The two project groups which exist in each project can also be used for administering space.

- *general group*. This has the same code as the project itself, includes every member of the project. The disk quotas of this project group can therefore be used by them all.
- *reserve* project group. This has a name of form *t01-reserve*, has no members, so no one can use the disk space which is in its quotas. You can use these quotas to hold space which you want to hold in reserve for later.

Homespace and workspace are administered separately. A project has an overall limit for each of these. Within that limit, every portion of space must belong to one or other of the project group quotas. Thus, to start with, all the homespace (for example) allocated to a project is either in the general homespace quota or the reserve homespace quota. Space never belongs to more than one group quota.

Note: The reserve quota is not a real quota, in fact. It has no existence on the service machine - just in the database.

Beyond the general and reserve quotas, you can also have quotas for the project groups which you create. But this is not compulsory. If you're thinking about using project group quotas, you need to be aware that they are implemented using Unix groups, which are only just adequate for the task.

Let's use homespace as an example—workspace is similar. Suppose you are project *t01*. To start with, one Unix group will be assigned to this project. The homespace directories for all users will be in directory `/home/t01/t01/` - this is where the general group is held. User *john*, for example, will have directory `/home/t01/t01/john/` as his homespace directory. (In fact, if this is the first project he joined, that's where he will log in.) Any file created in any of the directories under `/home/t01/t01/` will belong to the Unix group for project *t01*.

If you create a project group *t01-a* with no homespace quota, this will not change. But the moment you give a homespace quota to this project group, a Unix group will be assigned to it and a directory will be created for it: `/home/t01/t01-a/` . If user *john* is a member of this project group, he will have a directory `/home/t01/t01-a/john/` . Any files he creates under that directory will belong to *t01-a* and will be counted against its quota.

john is still a member of the general project group, so he can still create files there. If he belongs to other project groups which have quotas, he'll have directories for these as well. He can only create files in the project groups he is a member of, since he can't access the directories of the other groups. It's up to him to make sure that he creates his files in the right places, so that they get charged to the right project groups.

You should also note that once you have instituted project group quotas, there's no easy way back. Removing them and reassigning all the files to other groups is a complex job and will require special arrangement with the systems team - send a request to the Turing's Research Computing Service helpdesk if you need to do this.

Most projects in fact use their project groups only for administering time, and allow their users to have access to all their space. You could if you wish make use of user quotas (see *Create a quota for a project group, or move space between quotas*) to stop individual users from taking too much space.

Note: the above points do not apply to the reserve quotas, since they don't exist on the service machine. They're just a book-keeping fiction, and using them is cost free. We recommend this to any project which is concerned about running out of space.

Create a quota for a project group, or move space between quotas

Start by reading about how to *Administer disk space*. If you are still determined to use project group quotas, this is how.

1. Login to SAFE.
2. Go to the menu *Projects manaaged* and select the *project* you wish to work on. This will display a panel with the project information.
3. Click *Manage Project Resources*.
4. In the *Group Quotas* section, click on *Archive*, *Home* or *Work* depending on which kind of quota you wish to create.
5. You will now see a list of your project groups, including the general and reserve groups. Project groups which have no quota will show the note *No quota set*.
6. Click the *Move From* and *Move To* buttons of the groups you want to change.
7. Fill in the number of Gb to move in the box.
8. Click *Submit Group Allocation Changes*.

Do not forget the final step, or nothing will happen. The act of moving quota space to a project group which has no quota set converts that project group to one with a group quota, administered by a Unix group, as discussed in *Administer disk space* above.

Quota changes are carried out by the systems team. Once this has been done, you will receive an email informing you. If you ask for the quota to be reduced below the current size of the files in the project group, the systems team will reject your request, and you will get an email saying this.

Set a quota for an individual user

User disk quotas are completely separate from project group quotas. A user quota simply places a limit on the amount of space which a particular user can occupy in workspace or homespace. There's nothing to stop you setting user quotas which add up to more (or less) than the total space. To set a quota for a user or users:

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to work on. This will display a panel with the project information.
3. Click *Manage Project Resources*.
4. In the *User Quotas* section, click *Home* or *Work*.
5. You will see a list of users. Enter a value for each of the users whose quota you wish to change.
6. Click *Submit Changes*.

Once again, these quota changes are carried out by the systems team. Once they have finished, you will receive an email.

As with group quotas on the work file-system you can only be absolutely sure of writing data when you are more than 7Gb below your quota limit.

1.5.3 Managing Project Users

Register project users

You must not apply for machine accounts on behalf of other users, or let others use accounts that belong to you. Account sharing is strictly forbidden on the Alan Turing Institute Research Computing Service. Every user must register on SAFE and then request an account for the Research Computing Service machine

In order to get an account, a potential user needs to know your project code. This is included in the email which SAFE sends to you, as PI, when your project is set up.

1. Give the users the project code.
2. Request that every register on SAFE and then request an account for the Research Computing Service machine.
3. If you notice that the menu *Projects managed* is highlighted orange, then this indicates that there is a request for project membership. Now you have to accept (or reject) each user's request.
4. Login to SAFE.
5. Go to the menu *Projects managed* and select *project requests* and you will see the details of the user who has applied.
6. Click the button next to the user.
7. You will see the user's details, and at the bottom of the page buttons to accept or reject them.

If you now accept the user, they will get an account. This is the last chance to stop someone who should not be there! Take a few seconds to check the user's details, especially their email address, to make sure that they are who they say they are. Please check their nationality as well: it's your responsibility to make sure this is right.

When you accept a user, the systems team is automatically requested to create the account on the service machine. When this has been done, the user is emailed; allow a working day for this. The user can then login to SAFE and get their password for the service machine.

Track user sign up requests

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to affect.
3. Click the *Update* button.
4. Enter your email address in the *New Account Signup Notification List* box. By default, the PI is notified.
5. Click *Commit Update*. Do not forget this step, or nothing will happen.

Designate a user as a project manager

A project manager can do everything in a project that a PI can do, except designate another project manager. You can designate as many project managers as you wish.

1. Make sure the user has an account in your project.
2. Login to SAFE.
3. Go to the menu *Projects managed* and select the *project* you wish to appoint a project manager for. This will display a screen with a variety of options for managing the project.
4. Click *Add project manager*.
5. A drop down list will be displayed which contains all the users within the project. Select the user you wish to make a manager.
6. Click *Add*.

If you later wish to remove a project manager, click *Remove project manager*, select the *project manager* and then click *Remove*.

Designate a user as a project sub-group manager

A project sub-group manager can only move time and disk quota between the groups they manage. They can also create new sub-groups underneath these groups. (If you manage a parent group you automatically manage all its children). Sub-group managers can also accept new people into the project and run reports on the project.

1. Make sure the user has an account in your project.
2. Login to SAFE.
3. Go to the menu *Projects managed* and select the *project* you wish to appoint a project sub-group manager for.
4. Scroll down to project groups and click on *Project Group Administration*.
5. Select the project-subgroup that you wish to assign a sub-group manager for. Click on *Add Manager*.
6. You will now have a drop down list of all the users who are sub-group members but not currently managers. Select the new manager from this list and click *Add* and then confirm the change.

To add users to the new project group, see the next question. A user can belong to more than one project group.

Add users to an existing project group

1. Login to SAFE.
2. Go to the menu *Projects Managed* and select the *project* you wish to are work on. This will display a screen with a variety of options for managing the project.
3. Click on *Project Group Administration*.
4. Scroll down and click on the *project sub-group* that you wish to add members to.
5. Scroll down and click on *Add accounts*.
6. This lists all of the active users accounts within project, select the users that you should have access to the project group clicking the boxes next to their names and click *Add*.

To see which members have access to the project group, select *project sub-group* and click *List Members*.

If the project group is using disk quotas (see *Administer disk space*), this operation is carried out by the systems team, so there may be a short delay. Otherwise, it happens at once.

A user can belong to more than one project group.

Remove a user from a project group

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to work on. This will display a screen with a variety of options for managing the project.
3. Click on *Project Group Administration*
4. Scroll down and click on the group you wish to work with.
5. Click on *Set membership* and you will see the list of users with a tick beside those who are members.
6. Tick or Untick the users as required for membership.

To see the membership of a group, select *project group* and then click *List members* which shows the list of current members.

If the project group is using disk quotas (see *Administer disk space*), this operation is carried out by a the systems team, so there may be a short delay. Otherwise, it happens at once.

Temporarily stop a user from using any time in your project

This is called *deactivating* a user. A user who has been deactivated cannot use any of your budgets. This means that they cannot do any work, in effect, so we recommend that you use this facility with care.

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you are working on.
3. Click *Administer Users*.
4. Select the user or users you wish to deactivate.
5. Click *Deactivate*.

To reactivate the users, do the same, but click *Activate* instead.

Remove one or more users from your project

Before doing this, bear in mind that it will result in all their files in your project being deleted. Are you sure that this is what you want? If so:

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to work on. This will display a screen with a variety of options for managing the project.
3. Click *Administer Users*.
4. A list of all your users will be displayed. Tick the box next to the user (or users) in question, then go to the bottom and click *Remove User from Project*.

SAFE will now ask you to confirm your action. If you do, all the files and directories in your project which belong to the users will be deleted, and the users will be removed from any of your project groups, so that they will not be able to use your time. In addition, if a user does not belong to any other project, their account on the service machine will be closed.

Send a mailing to all users in your project

1. Login to SAFE.
2. Go to the menu *Projects Managed* and select the *project* you wish to work on. This will display a screen with a variety of options for managing the project.
3. By *Project mailings* click on *View*
4. You will see a list of all of the previous project mailings, and the option to compose a new one.
5. Select *Compose*
6. To change the mailing or content, you can use the *Edit Subject* and *Edit* buttons. Once you have changed the text select *Update*.
7. To send the mail click *Send*.

   There is an option to *Start Over* - this will wipe the content of the email.

   The *Abort* option will take you out of the mailing page completely.

1.5.4 Tracking your Project Usage

Check the current state of your project's time and space

1. Login to SAFE.
2. Go to the menu *Projects managed* and select the *project* you wish to work on.
3. Under *Project groups* you can see the current state of each project group's budgets. If it uses disk quotas, you will see these, together with how much of is in use.

If a project group's use of a quota is getting close to the maximum, it is highlighted in pink.

The budget values displayed are updated every morning, and the values shown for disk use are updated four times a day. For this reason, these values may not all be completely up-to-date. If there is a lot of activity in your project, the numbers shown could be significantly different from the current ones.

Track what your project's users and project groups are doing

This can be done using the Report Generator:

1. Login to SAFE.
2. Go to the menu *Service information* and select *Report generator*
3. Choose a report format: HTML, PDF or CSV (comma-separated values — good for input to Excel, *etc.*)
4. Select the start and end dates of the period you are interested in.
5. Select *Project Information*. (Only PIs and project managers see this section).
6. Select the information you need.
7. Click *Generate Report*.

Request automatic project reports

1. Login to SAFE.
2. Go to the menu *Projects Managed* and select the *project* you wish to work on. This will display a screen with a variety of options for managing the project.
3. Click on *Update*
4. Enter the email addresses which the reports should be sent to in *Recipients for automatic reports*.
5. Set the *Frequency of Automatic Reports* to the preferred frequency.
6. Click *Update* to confirm the changes.

Check how much space my project's users are occupying

Use the Report Generator (see *Request automatic project reports*), and select *User disk use*. The Report Generator displays the history of disk use—to see the current use, make sure that the reporting period includes the present moment. The disk usage values known to the database are updated four times a day, so if there is a lot of activity in your project, the numbers shown could be significantly different from the current ones.

There's an unresolvable problem with this: if a user has an account which belongs to more than one project, the disk usage shown for that account will be the total that the account is using in all those projects combined.

Request more resources (kAUs and disk space)

If you need more homespace or workspace, contact the Turing's Research Computing Service helpdesk. We will always receive such requests sympathetically, and it is likely that we will be able to allocate some more to your project.

1.6 Atiras, Secure Safe Haven and Intel cluster

This chapter contains information about the Alan Turing Institute Remote Access Service (Atiras), a Secure Safe Haven with an Intel cluster. It explains:

- *Key components*
- *Requesting access to Atiras*

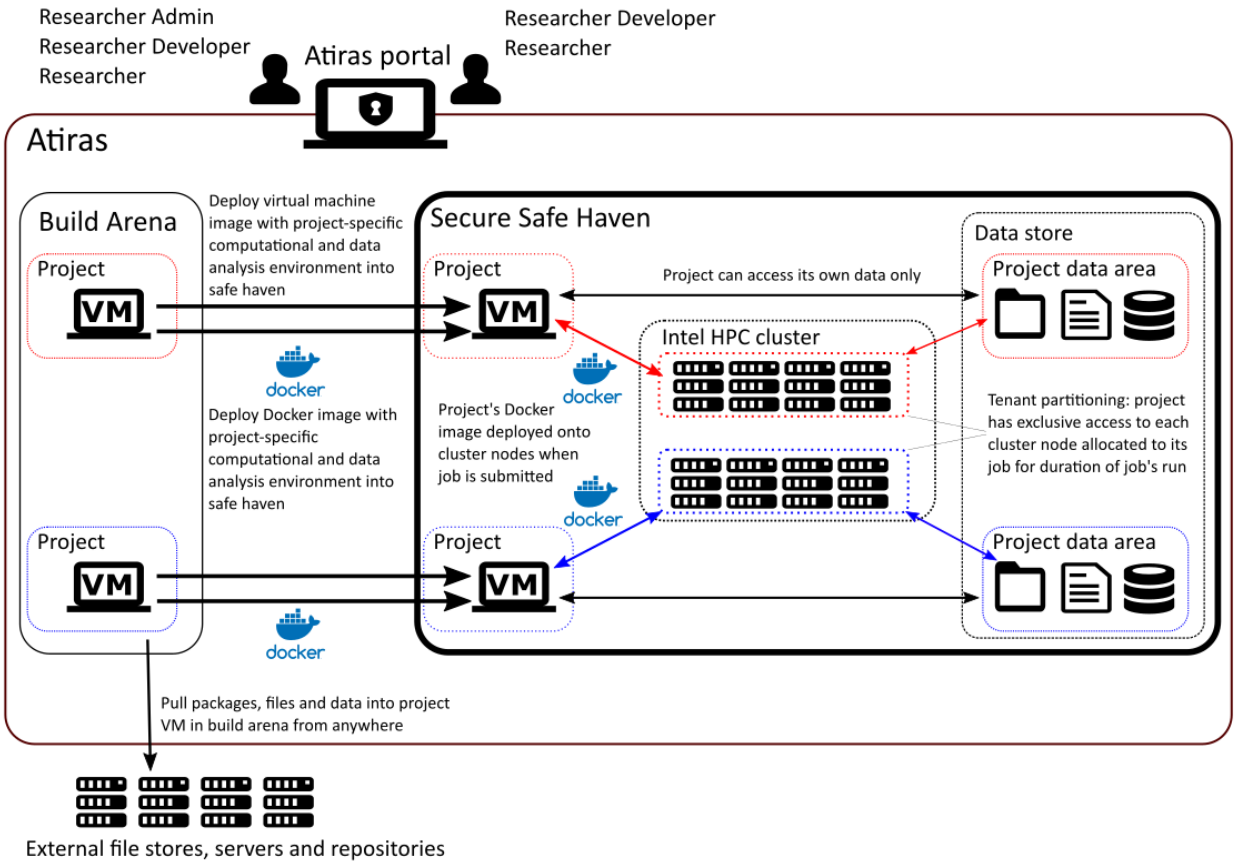
- *Early Access Service*

1.6.1 Important note

Atiras is under development. As a consequence, aspects of its design, behaviour and usage are liable to change.

1.6.2 Key components

The **Alan Turing Institute Remote Access Service (Atiras)** provides a service for running computational and data analysis tasks upon project data held within a secure environment. Atiras consists of the following components.



Atiras portal

The Atiras portal is a web browser-based remote desktop gateway by which researchers can access the Secure Safe Haven and build arena. It allows the use of virtual machines within Atiras via either a command-line terminal or a graphical desktop.

Secure Safe Haven

The Secure Safe Haven provides a project with virtual machines customised with software required by that project and connected to the project's data held within the Secure Safe Haven. These virtual machines allow the project's researchers to run computational and data analysis tasks, access the project's data held within the Secure Safe Haven, and submit jobs to the Intel cluster (these virtual machines also serve as login nodes for the Intel cluster).

Virtual machines do not allow outbound or inbound connections to hosts external to the Secure Safe Haven.

Each virtual machine runs CentOS Linux release 7.5.

Intel cluster

The Intel cluster, within the Secure Safe Haven, is a cluster of 32 Intel Xeon compute nodes. Each node has 2 CPUs, a 1 x Skylake Gold 6148F (Omnipath-enabled) CPU and 1 x Skylake Gold 6148 CPU. Each CPU has 20 physical cores, with hyperthreading this provides 40 virtual cores per CPU. The cluster, in total, has 1280 physical cores. Each node has 192GB of memory and 8TB of local storage. 300TB of storage is shared across the cluster via NFS. 33TB is shared via BeeGFS.

If a project-specific Docker image has been developed for the project (see below) then this will be deployed upon nodes within the Intel cluster when the project's researchers submit jobs to the cluster.

Nodes do not allow outbound or inbound connections to hosts external to the Secure Safe Haven.

Each node runs CentOS Linux release 7.5.

Project data areas

Each project has a data area in the Secure Safe Haven. These are available in fixed sizes, for example 10GB, 50GB, or 100GB. The size available to a project depends upon both the data a project wants to hold within the Secure Safe Haven and the data they expect to produce from their analyses.

Build arena

Complementing the Secure Safe Haven, but sitting outside of it, is the **build arena**. The build arena provides a project with a project-specific virtual machine. The project's researcher administrators and researcher developers have administrator rights sufficient to install and configure the computational and data analysis environment required by their project's researchers.

This virtual machine also allows researcher administrators and researcher developers to build a Docker image. This Docker image can contain a computational and data analysis environment which can be deployed upon nodes within the Intel cluster when the project's researchers submit jobs to the cluster.

Once a virtual machine has been configured, it is deployed, by EPCC's Systems Development Team, into the Secure Safe Haven, where it becomes available as a virtual machine for a project's researchers. Depending on the project, a researcher developer may retain administrator rights on the deployed virtual machine to be able to make configuration changes and fixes for the project's researchers.

If a Docker image has been prepared, then it, too, is deployed into the Secure Safe Haven, so that it can be deployed upon nodes within the Intel cluster when a project's researchers submit jobs.

The virtual machine allow outbound connections to hosts external to Atiras, to allow for software to be downloaded and installed in their virtual machine, and their Docker image constructed.

Each virtual machine runs CentOS Linux release 7.5. They are configured with 4 CPUs, 16GB memory and ~60GB disk space to allow for software assembly and testing. Once deployed into the Secure Safe Haven the number of cores, available RAM and disk space are extended.

1.6.3 Requesting access to Atiras

This section explains how you request access to Atiras.

If you are a researcher wanting to access a virtual machine for your project within the Secure Safe Haven, you will need:

1. An account for the Atiras portal to access the Secure Safe Haven.
2. An account for a virtual machine in the Secure Safe Haven.

If you are one of your project's researcher administrators or researcher developers wanting to access a virtual machine for your project within the build arena, you will need:

1. An account for the Atiras portal to access the build arena.

2. An account for a virtual machine in the build arena.

Note: if you are a research administrator or researcher developer wanting to access virtual machines both in the build arena and Secure Safe Haven then you will need all 4 accounts.

You can request user accounts for each of these using your account on the Turing's SAFE.

Instructions on getting an account for the Turing's SAFE and using a *Project Code* to request access to the Turing's research computing resources, including Atiras, are in the *SAFE for Individual Users* section of this User Guide.

This *Project Code* entry can be obtained by contacting the Turing's Research Computing Service Manager via an email to research-computing-support@turing.ac.uk.

If your request for access is successful, you will receive emails from the Turing's SAFE with the information for your user accounts for the Atiras portal, the Secure Safe Haven and the build arena.

Access is via the Atiras portal

1.6.4 Early Access Service

Atiras is currently being run for the Turing's researchers as an Early Access Service. The purpose of this Early Access Service is to establish how best to later configure the service to meet the needs of the Turing's researchers. The Early Access Service will be replaced at a future date.

This section explains how Atiras's Early Access Service operates:

- There is one SAFE *Project Code* for the Early Access Service.
- This *Project Code* can be obtained by contacting the Turing's Research Computing Service Manager via an email to research-computing-support@turing.ac.uk.
- There are no limitations on user disk quotas.
- There is no batch queuing software provided. A job will only execute if there are resources available. If sufficient resources are not available then the user will have to try and submit later.
- There is no procedure in place for resolving disagreements on resource usage and allocations.
- There is **no** backup on any of the 3 filesystems users have access to.
- There is **no** disaster recovery.

1.7 Connecting to Atiras

This chapter explains how to connect to the Alan Turing Remote Access Service (Atiras) and, once connected, to the virtual machines within the Secure Safe Haven and the build arena.

If you are a researcher wanting to access a virtual machine for your project within the Secure Safe Haven, you need:

1. An account for the Atiras portal to access the Secure Safe Haven.
2. An account for a virtual machine in the Secure Safe Haven.

If you are one of your project's researcher administrators or researcher developers wanting to access a virtual machine for your project within the build arena, you need:

1. An account for the Atiras portal to access the build arena.
2. An account for a virtual machine in the build arena.

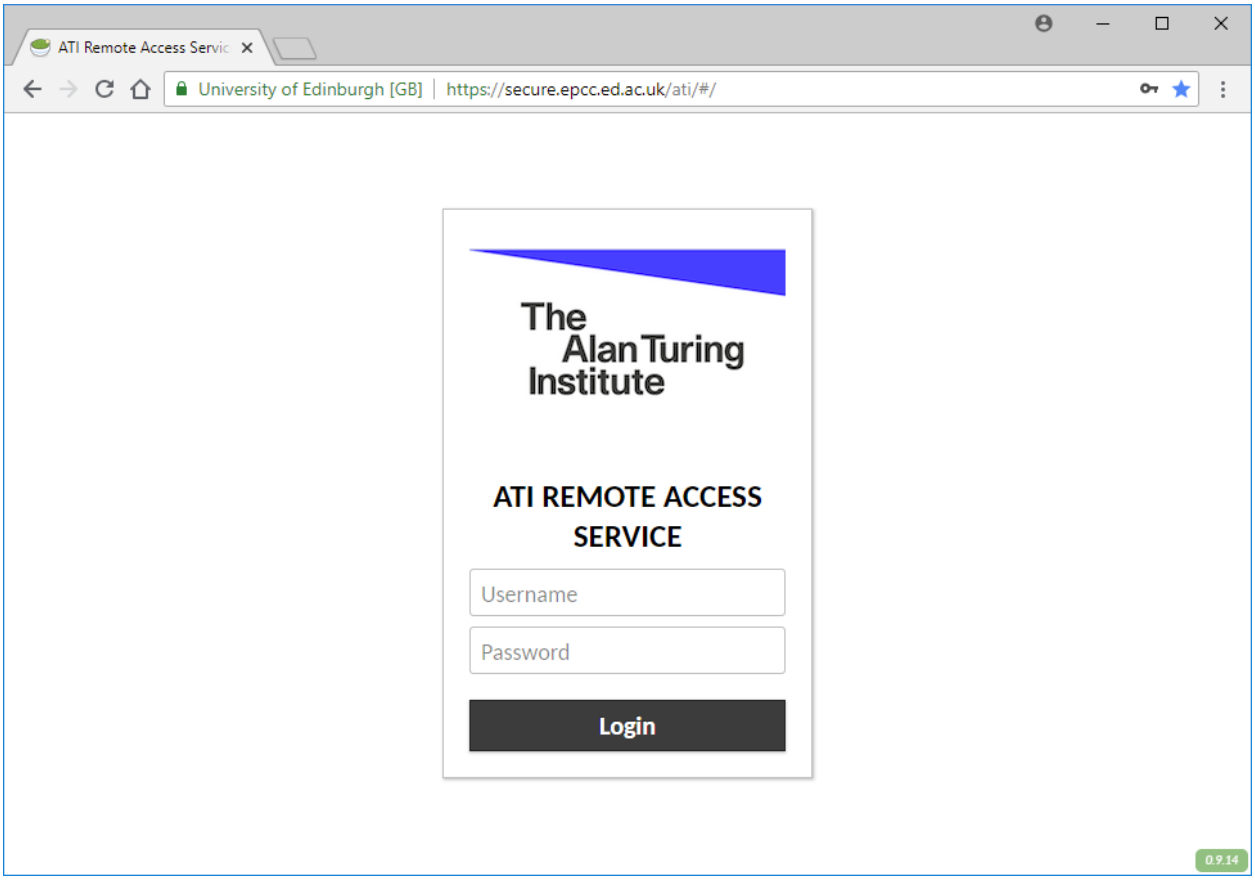
See the chapter *Atiras, Secure Safe Haven and Intel cluster* for instructions on how to get these user accounts.

Access to, and usage of, Atiras, and virtual machines within the Secure Safe Haven and build arena is done entirely from within a web browser, via the Atiras portal.

1.7.1 Use web browser to access the Atiras portal

Visit https://secure.epcc.ed.ac.uk/ati/ in your web browser.

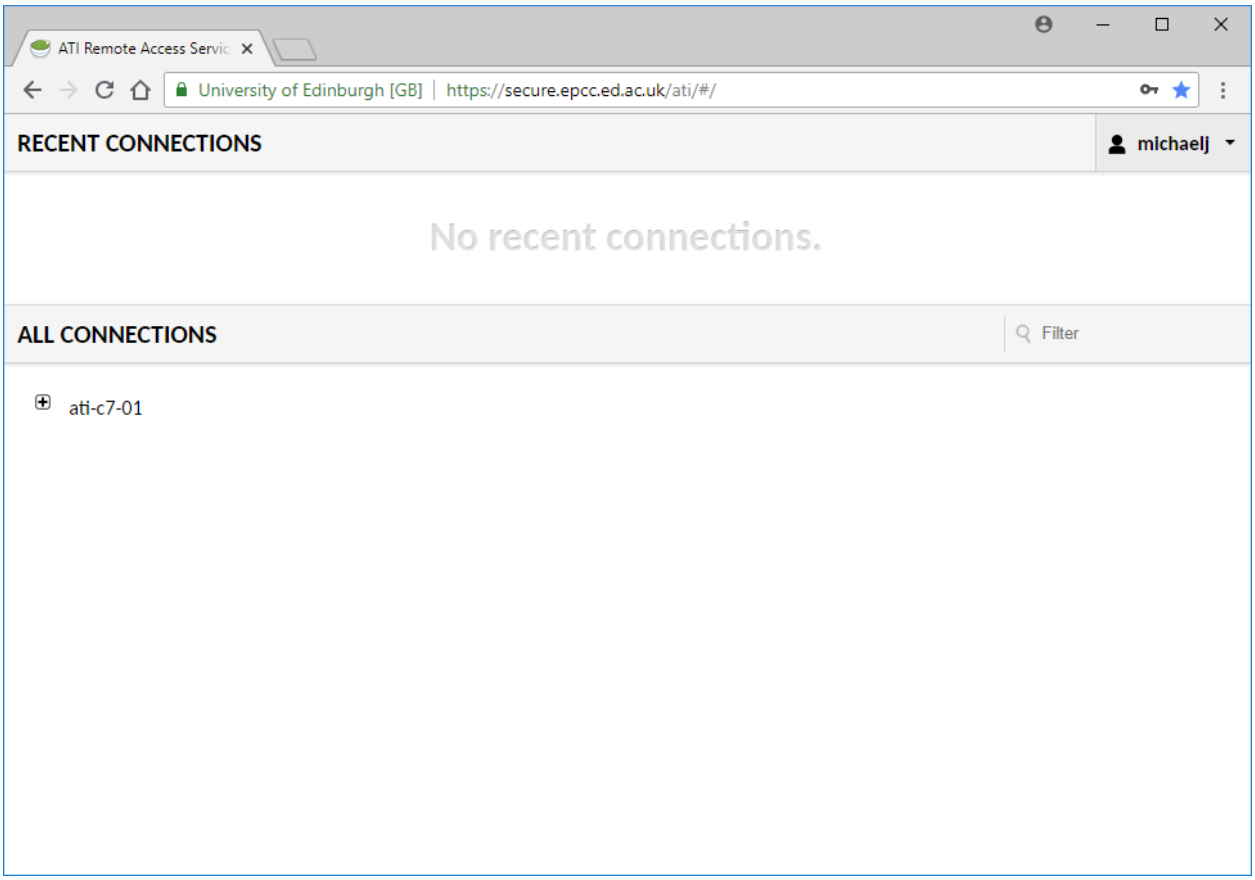
The Atiras portal will appear:



If you want to access the Secure Safe Haven then enter your **Atiras portal Secure Safe Haven** username and password and click 'Login'.

If you want to access the build arena then enter your **Atiras portal build arena** username and password and click 'Login'.

You will be presented with your home page. When logging in for the first time the home page will look something like:



1.7.2 View your available connections

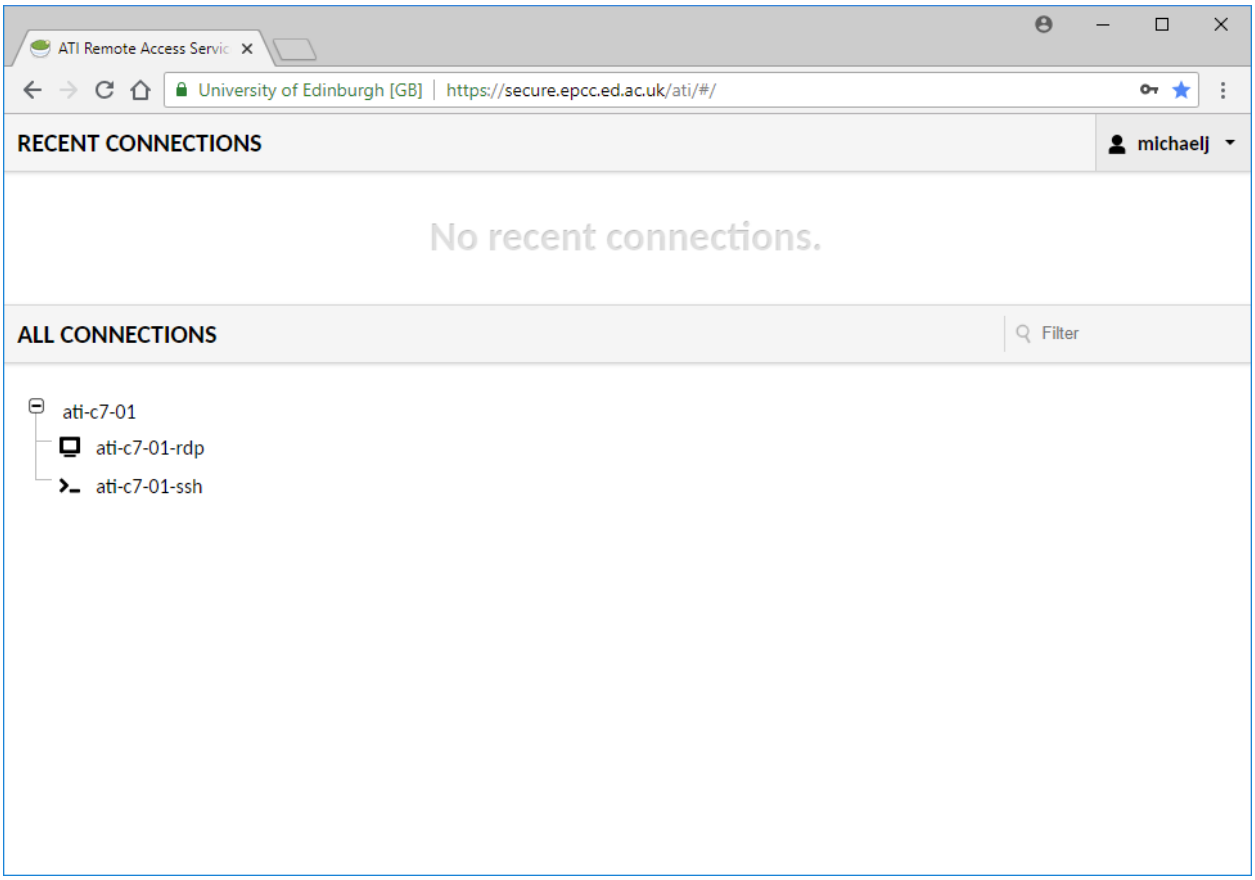
The home page shows your *connections*, the virtual machine which you can connect to:

- If you entered your **Atiras portal Secure Safe Haven** username then you will see your project's Secure Safe Haven virtual machine.
- If you entered your **Atiras portal build arena** username then you will seeyour project's build arena virtual machine.

The home page shows:

- 'RECENT CONNECTIONS' shows screen shots of virtual machines you have recently connected to (i.e. logged in to). When you log in for the first time, 'RECENT CONNECTIONS' will show 'No recent connections', as shown above.
- 'ALL CONNECTIONS' shows a list of all the virtual machines you can connect to. For example, `ati-c7-01` above.

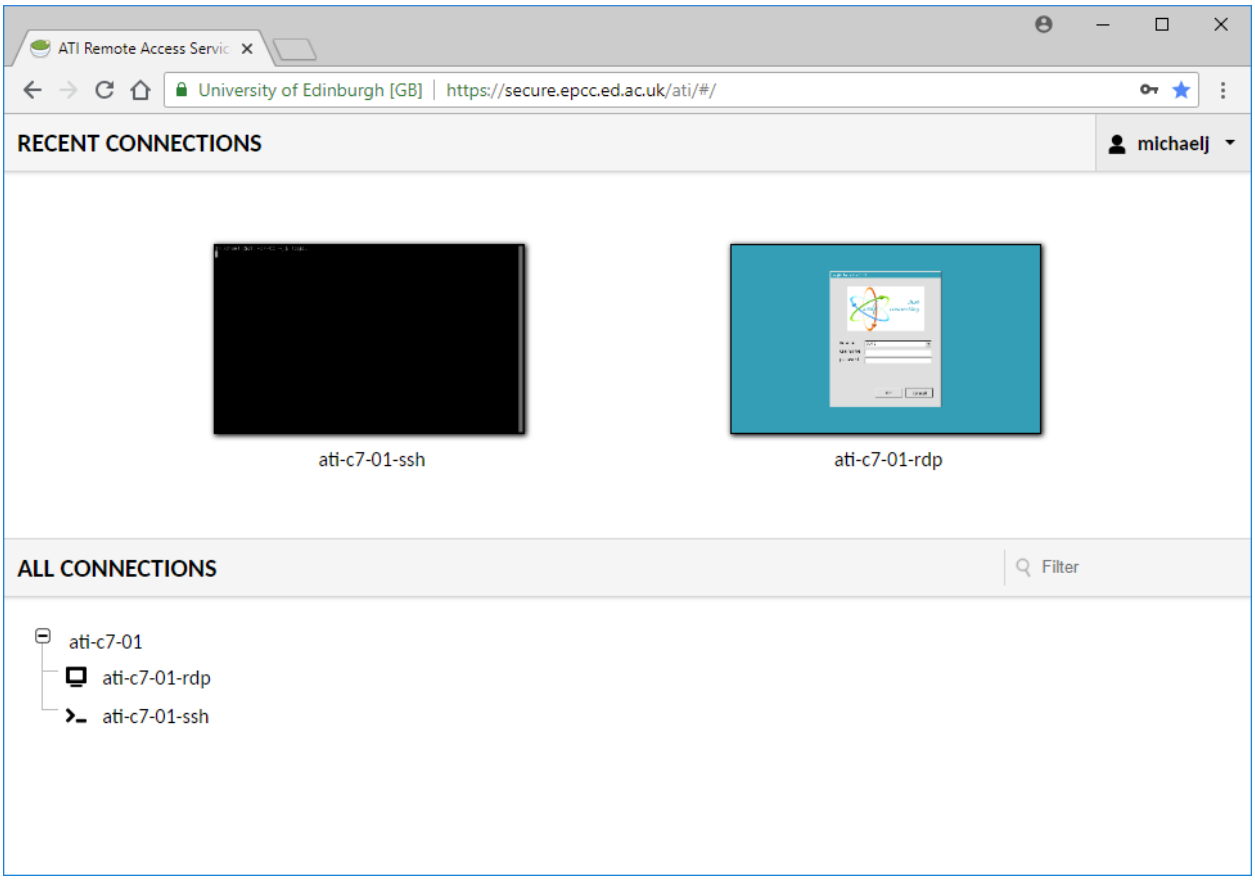
Clicking on virtual machine names in 'ALL CONNECTIONS' shows connection options for that virtual machine e.g.



There are two types of connection option:

- RDP (remote desktop protocol), suffix `-rdp` (for example `ati-c7-01-rdp`). This connection allows you to use the virtual machine via a remote desktop.
- SSH (secure shell), suffix `-ssh` (for example `ati-c7-01-ssh`). This connection allows you to use the virtual machine via a command-line terminal.

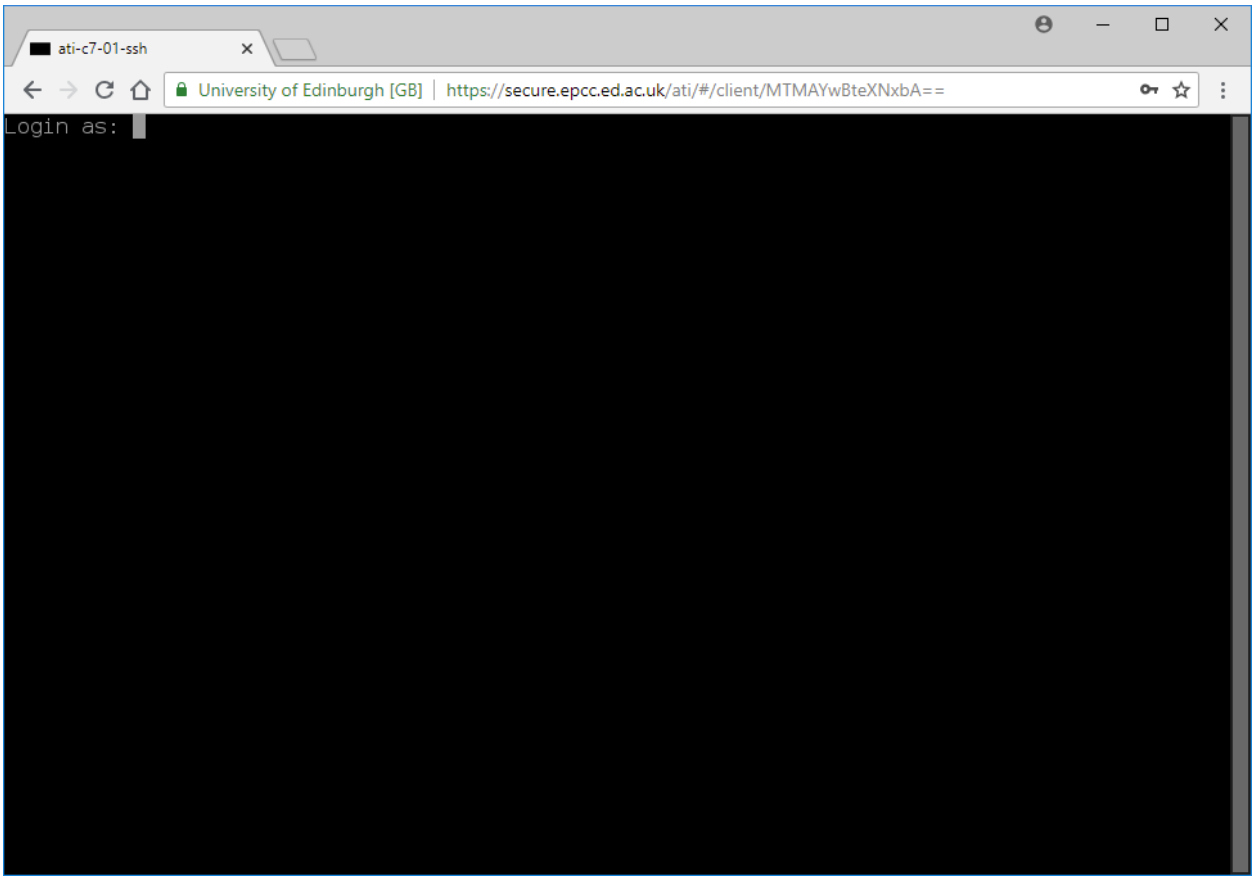
On subsequent sessions, you will see your recent connections e.g.



1.7.3 Connect via SSH (secure shell) session

To connect to a virtual machine via an SSH session, right-click on the `-ssh` connection for that virtual machine and select "Open link in new tab". This can be done under either 'ALL CONNECTIONS' or, for virtual machines to which you have connected before, under 'RECENT CONNECTIONS'.

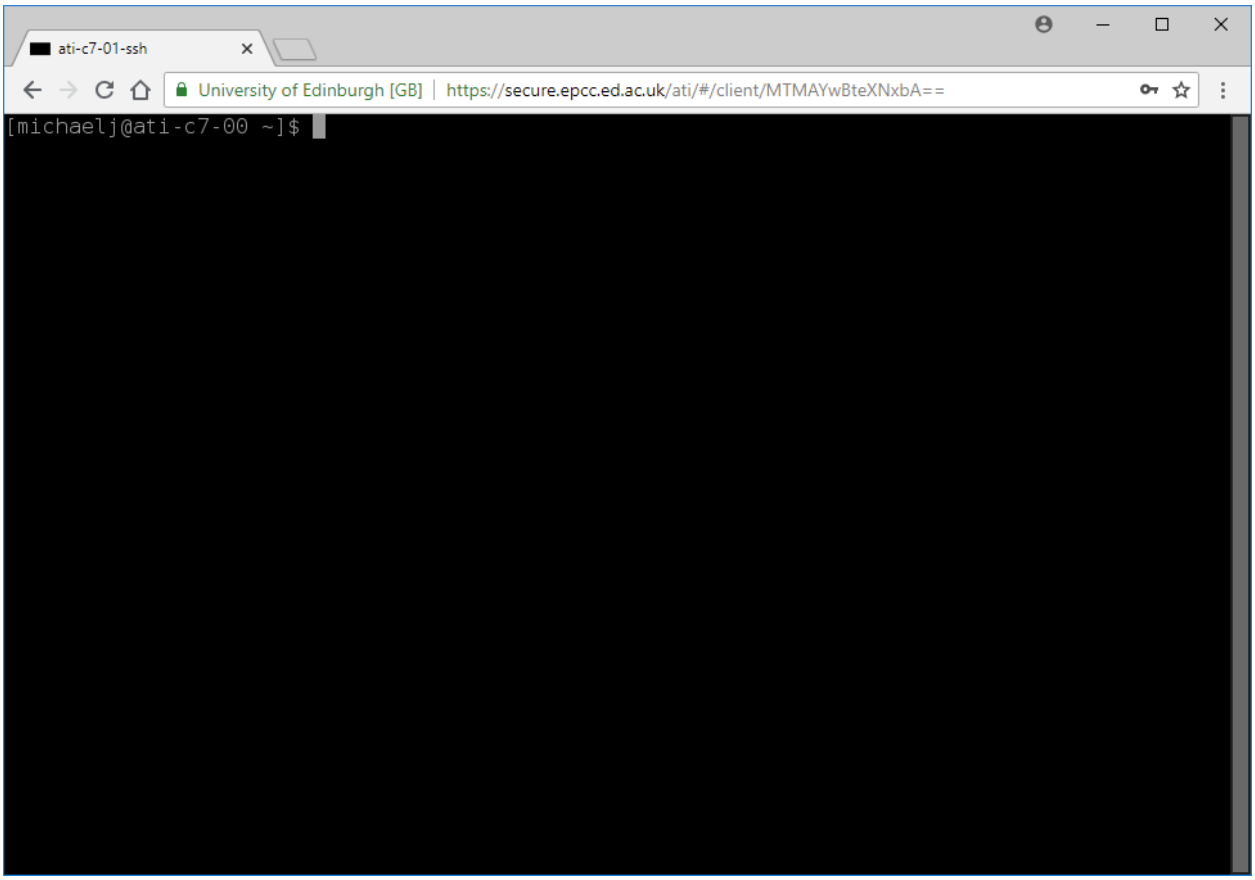
You will be shown a command-line terminal with a login prompt e.g.



If accessing the Secure Safe Haven, enter your **Secure Safe Haven virtual machine** username and password and press ENTER.

If accessing the build arena, enter your **build arena virtual machine** username and password and press ENTER.

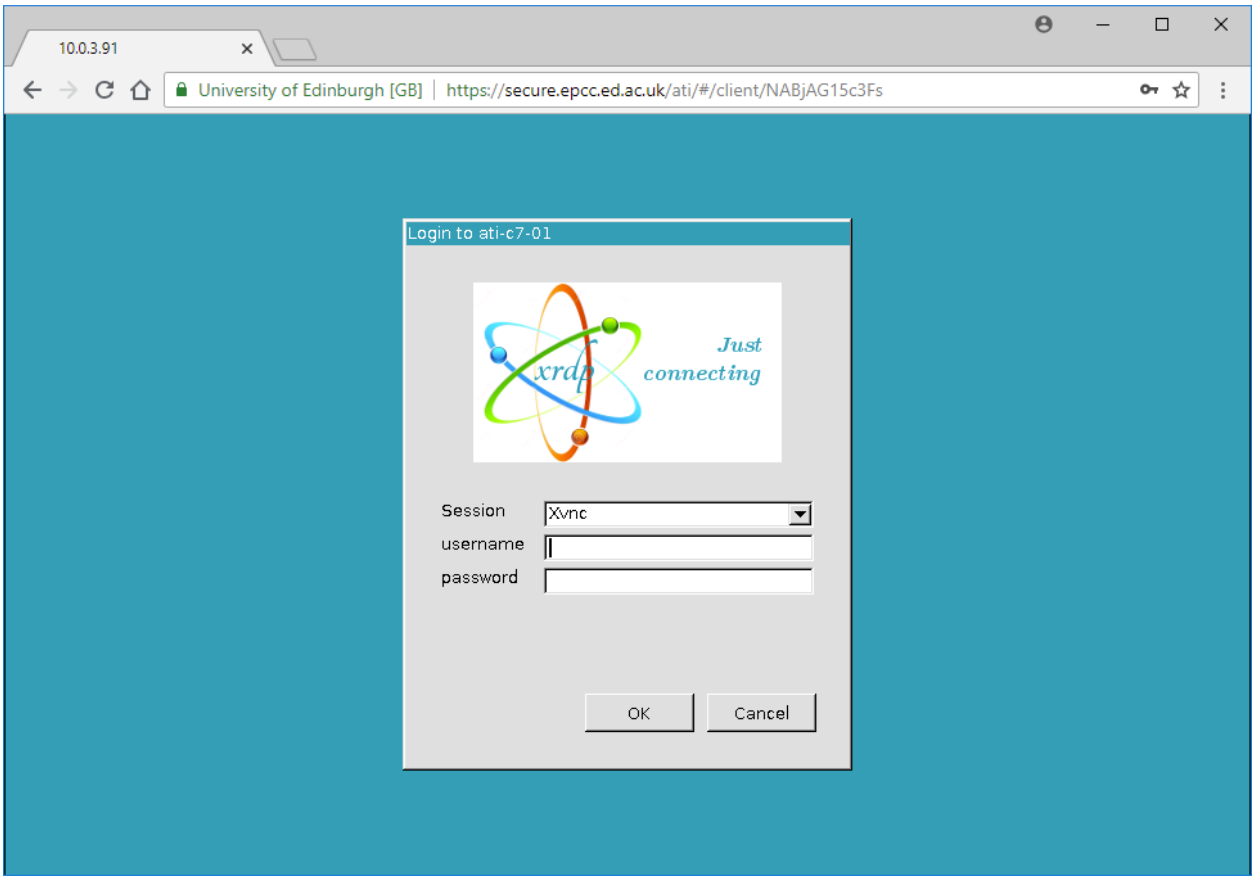
You will be presented with a bash prompt e.g.



1.7.4 Connect via RDP (remote desktop) session

To connect to a virtual machine via an RDP session, right-click on the `-rdp` connection for that virtual machine and select "Open link in new tab". This can be done under either 'ALL CONNECTIONS' or, for virtual machines to which you have connected before, under 'RECENT CONNECTIONS'.

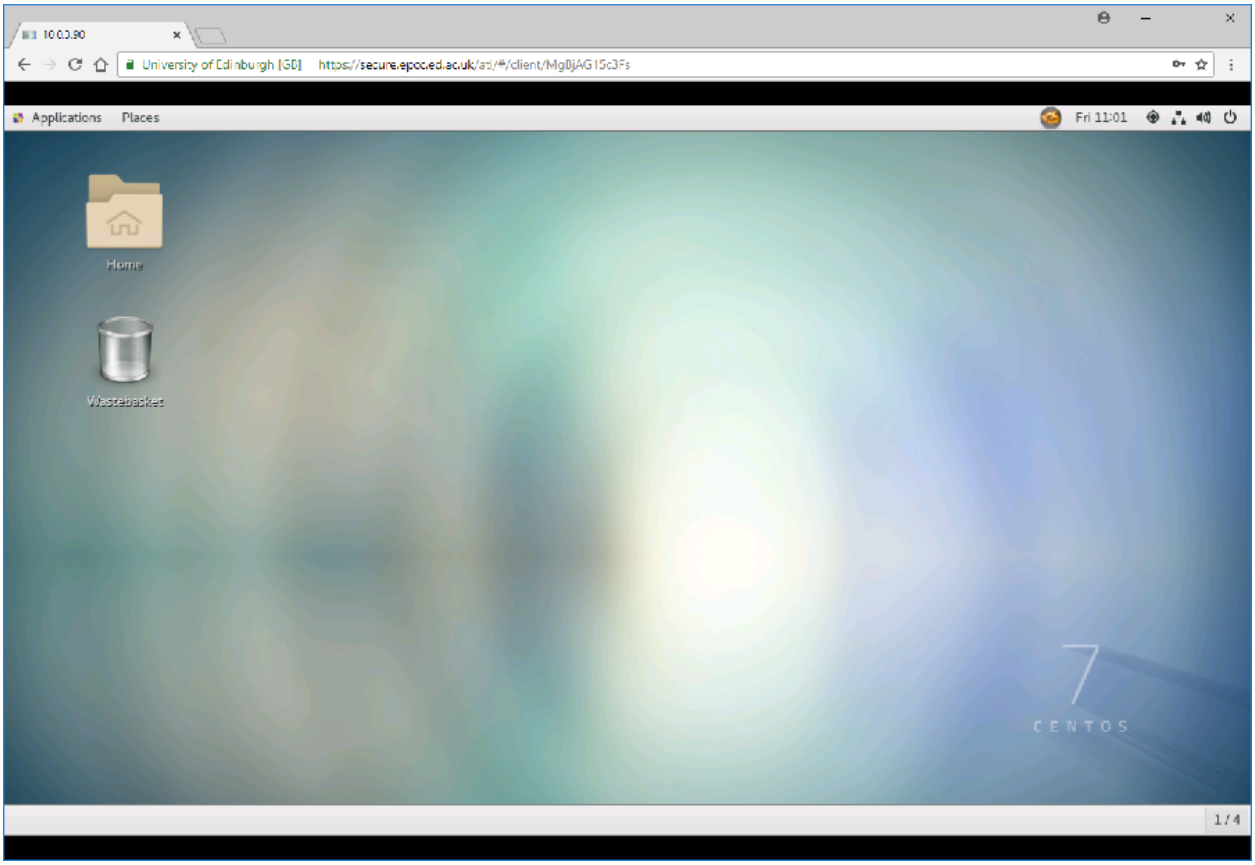
You will be shown a login dialog e.g.



If accessing the Secure Safe Haven, enter your **Secure Safe Haven virtual machine** username and password click 'OK'.

If accessing the build arena, enter your **build arena virtual machine** username and password and click 'OK'.

You will be presented with a desktop e.g.



Note: the first time you log into a virtual machine via RDP you may have to work through a few screens to configure your local environment (e.g. select your preferred language etc).

1.7.5 Disconnect from SSH (secure shell) session

Enter:

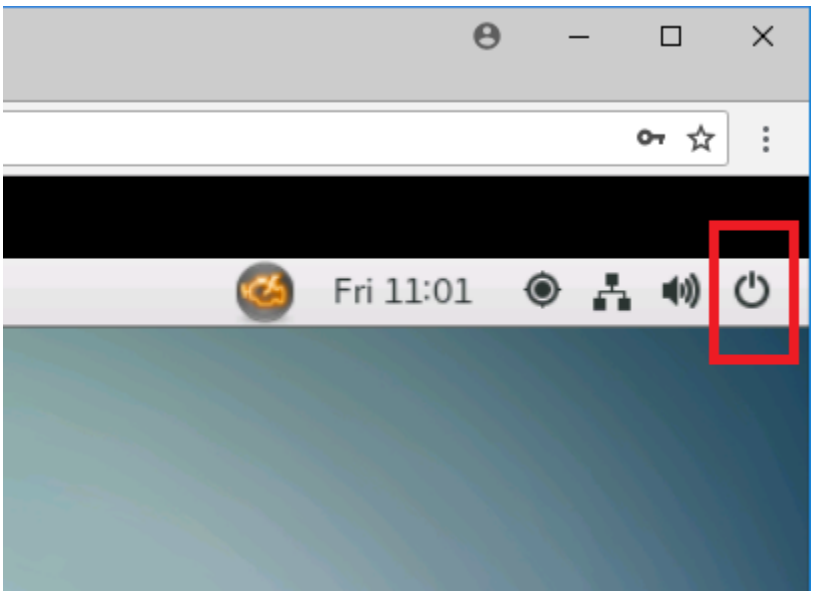
```
exit
```

Or, press CTRL-D.

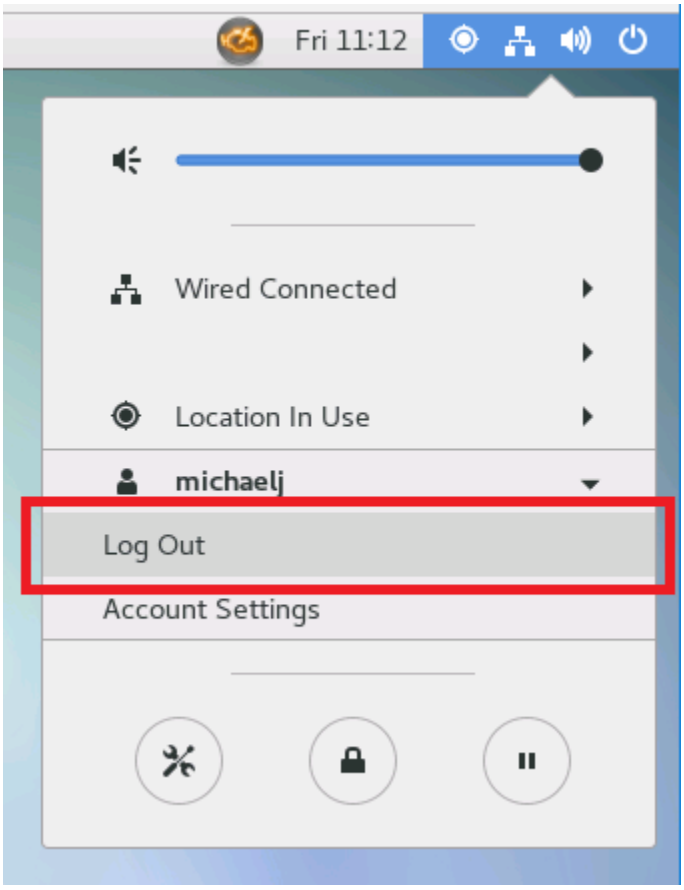
You will then be presented with a number of options, see *After disconnecting from a session*.

1.7.6 Disconnect from RDP (remote desktop) session

Click the button icon on the top right hand side of the desktop:



You will be presented with a dialog box. Click your user name then select 'Log Out':

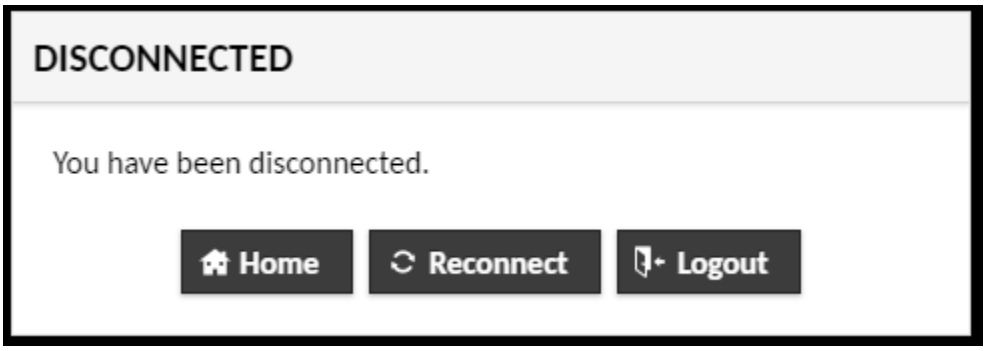


A 'Log Out <your-virtual-machine-username>' dialog box will appear. Click 'Log Out'.

You will then be presented with a number of options, see *After disconnecting from a session*.

1.7.7 After disconnecting from a session

Once you exit from an RDP or SSH session you will be shown a 'DISCONNECTED' dialog:



There are three options:

- Return to the Atiras portal home page: Click 'Home'.
- Reconnect session: Click 'Reconnect'.
- Logout from the Atiras portal: Click 'Logout'.

1.7.8 Change your Atiras portal password

You can change your Atiras portal password as follows:

1. Click the menu labelled by your username at the top-right of the page.
2. Select 'Settings'.
3. **Fill in the following fields:**
    - 'Current Password'
    - 'New Password'
    - 'Confirm New Password'
4. Click 'Update Password'.

1.7.9 Change your virtual machine password

If running a SSH (secure shell) session, or from terminal window in an RDP (remote desktop) session

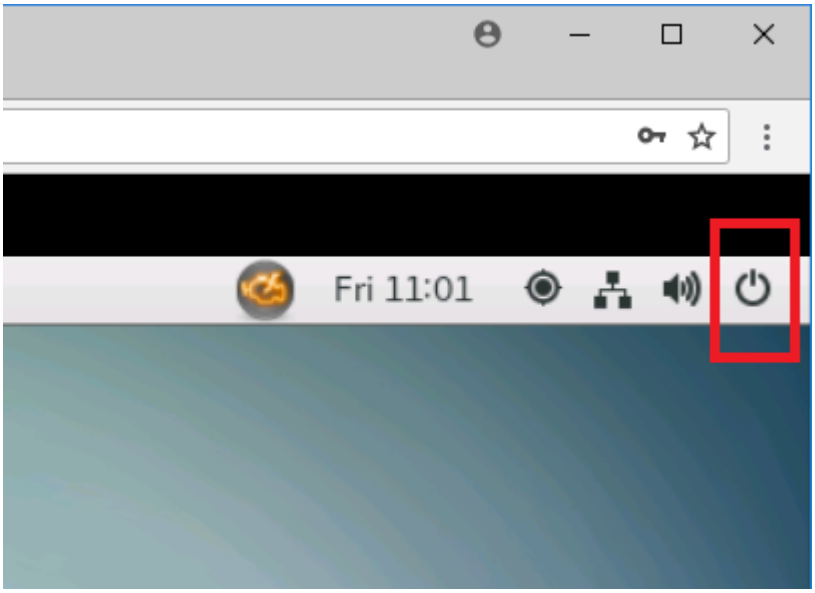
1. Run:

```
passwd
```

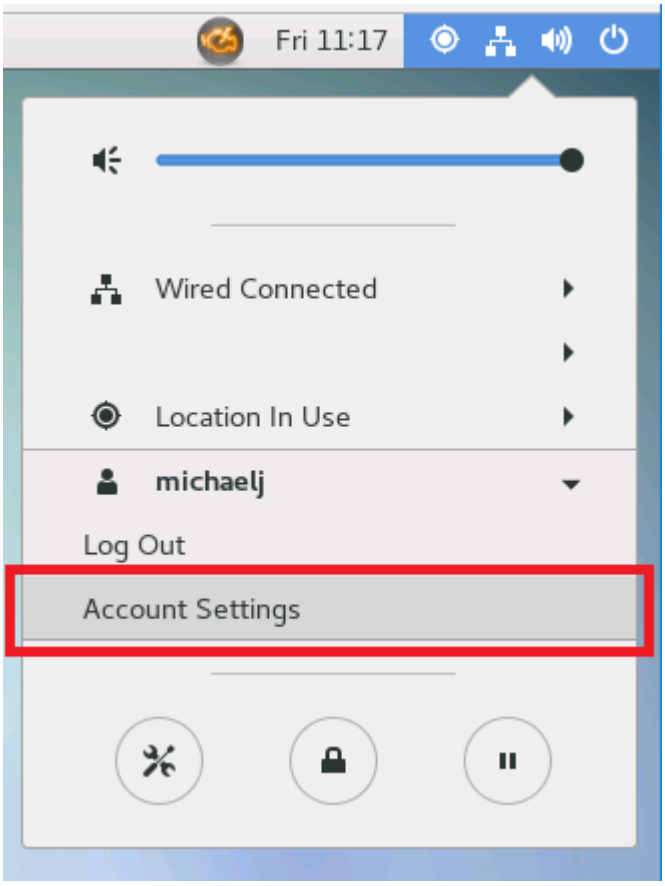
2. You will be prompted to enter your old password.
3. You will be prompted to enter your new password twice.

Alternatively, if running an RDP (remote desktop) session:

1. Click the button icon on the top right hand side of the desktop:



2. You will be presented with a dialog box. Click your user name then select 'Account Settings':



3. Click '<your-virtual-machine-username>' on the row of user names.
4. Click the button (with five blobs) next to the 'Password' field.
5. **Fill in the following fields:**
    - 'Current Password'

- 'New Password'
- 'Verify New Password'

6. Click 'Change'.

1.7.10 Logout from the Atiras portal

To logout from the Atiras portal when on the home page:

1. Click the menu labelled by your username at the top-right of the page.
2. Select 'Logout'.

1.8 Using the build arena

This chapter explains how to use, and configure, a virtual machine for your project in the build arena of Atiras to both:

- Install and configure the computational and data analysis environment required by your project's researchers.
- Build a Docker image containing a computational and data analysis environment which can be deployed upon nodes within the Intel cluster when your project's researchers submit jobs to the cluster.

The virtual machine allows outbound connections to hosts external to Atiras, to allow you to download software and install it on your virtual machine, and to build a Docker image.

The virtual machine runs CentOS Linux release 7.5.

See the chapter *Connecting to Atiras* for instructions on how to connect to a virtual machine in the build arena.

1.8.1 Run commands as administrator

To run commands as administrator, run:

```
sudo su -
```

You will be prompted for a password:

```
[sudo] password for <your-virtual-machine-username>
```

Enter your virtual machine password.

The prompt should change to the administrator prompt:

```
#
```

1.8.2 Get software/data/documentation into the virtual machine

The virtual machine supports a number of standard ways to get content - including software, data (for example sample data, test data, but *not secure or sensitive project data*), and documentation - into your virtual machine. This includes tools to:

- Access files from URLs, and interact with REST endpoints: `curl`, `wget`
- Securely transfer files: `scp`, `sftp`
- Securely log into remote hosts:, `ssh`

- Interact with source code repositories: `git`, `svn`, `cvs`

If using your virtual machine via RDP, then Mozilla Firefox web browser is also available:

- Either, run:

```
firefox
```

- Or, select Applications => Firefox

1.8.3 Deploy a virtual machine, and Docker image, into the Secure Safe Haven

Once you have configured the virtual machine, and, optionally, a Docker image, with the software needed by the researchers on your project, it can be deployed within the Secure Safe Haven. The process is as follows:

1. Request that the virtual machine, and Docker image (if applicable), be deployed into the Secure Safe Haven.
2. EPCC's Systems Development Team (SDT) audits your virtual machine in accordance with the required security standards of both your project and the Secure Safe Haven. If they have any concerns, suggestions, or requirements they will pass these back to you for you to act upon.
3. If you have built a Docker image, SDT will audit that also.
4. SDT shuts down your virtual machine in the build arena.
5. SDT copies your virtual machine into the Secure Safe Haven, connects it to your project's data area and starts it up. It is now available as a virtual machine for use by your project's researchers.
6. If you have built a Docker image, SDT deploys the image into the Secure Safe Haven, configuring the Secure Safe Haven so that the Docker image is deployed upon nodes within the Intel cluster when your researchers submit jobs.
7. SDT restarts the virtual machine in the build arena.

1.8.4 Default text editors

By default, each build arena virtual machine provides two text editors:

- ViM: `vi` or `vim`.
- GNU nano: `nano`.

1.9 Using the Secure Safe Haven

This chapter explains how to use a virtual machine for your project in the Secure Safe Haven of Atiras.

The virtual machine is customised with software required by your project and is connected to your project's data held within the Secure Safe Haven. The virtual machine allows you to run computational and data analysis tasks, access your data held within the Secure Safe Haven, and submit jobs to the Intel cluster (these virtual machines also serve as login nodes for the Intel cluster).

See the chapter *Connecting to Atiras* for instructions on how to connect to a virtual machine in the Secure Safe Haven.

1.9.1 Access project data

Your project data will be available as NFS mounts on your virtual machine. These will be in the `/mnt/` directory.

1.9.2 Submit a job to the Intel cluster

The Secure Safe Haven uses the Slurm workload manager to run jobs on the Intel cluster.

You can submit jobs to the Intel cluster using the `qsub` command.

1.9.3 Data security within the Intel cluster

These are planned

Local disks on compute nodes are purged at the end of each run.

File permissions on `/tmp` directories are such that other projects won't be able to access any temporary data that has been deposited there by you. Furthermore, the contents of `/tmp` are deleted on a regular basis to avoid project-specific data inadvertently being left there.

The job scheduler is configured so that two projects never share the same compute node at the same time.

1.9.4 Troubleshooting: no internet connections

Virtual machines in the Secure Safe Haven do not allow outbound or inbound connections to hosts external to the Secure Safe Haven.

1.10 Success Stories

This chapter contains information about research enabled using the Alan Turing Institute's Research Computing Service.

- Mike Jackson, Rosa Filgueira and Anna Roubickova, "Analysing historical newspapers and books using Apache Spark and Cray Urika-GX", EPCC blog, August 2019. A blog post on further explorations of 15th-19th century books data and 18th-early 20th century newspapers data using the Turing's Cray Urika-GX service.
- Mike Jackson, Rosa Filgueira and Anna Roubickova, "Analysing Historical Newspapers and Books Using Apache Spark and Cray Urika-GX", Alan Turing Institute / EPCC, The University of Edinburgh, 16 August 2019 (`PDF`). A report on further explorations of 15th-19th century books data and 18th-early 20th century newspapers data using the Turing's Cray Urika-GX service.
- Rosa Filgueira, "Spark-based genome analysis on Cray-Urika and Cirrus clusters", EPCC blog, 16 January 2019. A comparison of using Urika and Cirrus for analysis of cancer genomes.
- Rosa Filgueira and Mike Jackson, "Analysing humanities data using Cray Urika-GX", EPCC News 84, November 2018, p12-13.
- Alessandra Cabassi and Junyang Wang, "High performance, large-scale regression", October 2018. A summary of work conducted in the High performance, large-scale regression project, part of the Turing's Summer Internship programme 2018, sponsored by Cray Inc, using a case study of flight arrivals and departures for all commercial flights within the USA, from October 1987 to April 2008, a dataset of over 120 million rows of data.
- Rosa Filgueira, "Analysing humanities data using Cray Urika-GX", EPCC blog, 11 October 2018. A blog post on exploring 15th-19th century books data and 18th-early 20th century newspapers data using the Turing's Cray Urika-GX service.
- Rosa Filgueira and Mike Jackson, "Analysing Humanities Data using Cray Urika-GX", Alan Turing Institute / EPCC, The University of Edinburgh, 31 July 2018 (`PDF`). A report on exploring 15th-19th century books data and 18th-early 20th century newspapers data using the Turing's Cray Urika-GX service.

CHAPTER 2

Related services

As an alternative to using the Alan Turing Institute Research Computing Service, you may also want to consider Cirrus, an EPSRC Tier-2 National HPC Facility available for users in both academia and industry for computational, simulation, modelling, and data science challenges.

hpc-uk provides information about organisations across the UK, including EPCC, that offer access to HPC infrastructures and related services such as training.

CHAPTER 3

About this documentation

This documentation is based on the Cirrus Documentation which itself draws on the Sheffield Iceberg Documentation and the documentation for the ARCHER National Supercomputing Service.