Medus Labs

Application Overview

This application allows you to create and manage ‘labs’ for the purposes of learning how to use all of the services and infrastructure available on Amazon Web Services. Each lab is made up of a group of 1 to 30 users, and each user will have a unique login. When using this application, you can also delete individual labs, users within them, and erase any leftover work, like items stored in an S3 Bucket. The following is a guide to using the application.

Contents

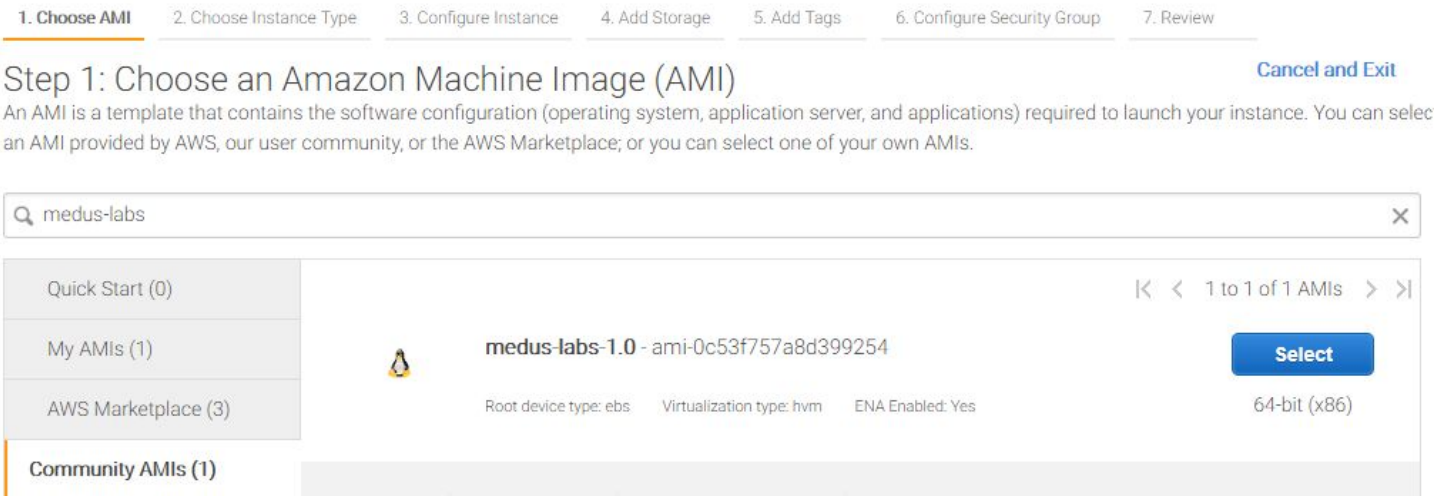
Setup Guide

Installation

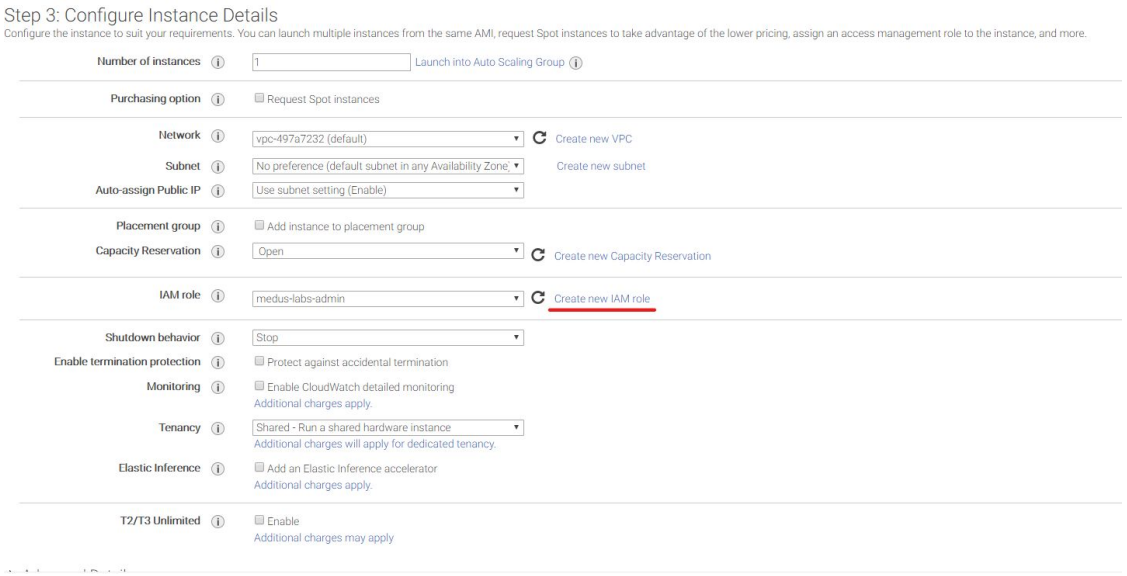
Medus Labs has been designed to be cloud native, and easily manageable for any end user. At present, the distribution of the application is via a valid AWS AMI (Amazon Machine Image) for use with AWS EC2.

Navigate to your AWS Console, and select the EC2 service. Click ‘Launch Instance’ to begin the process.

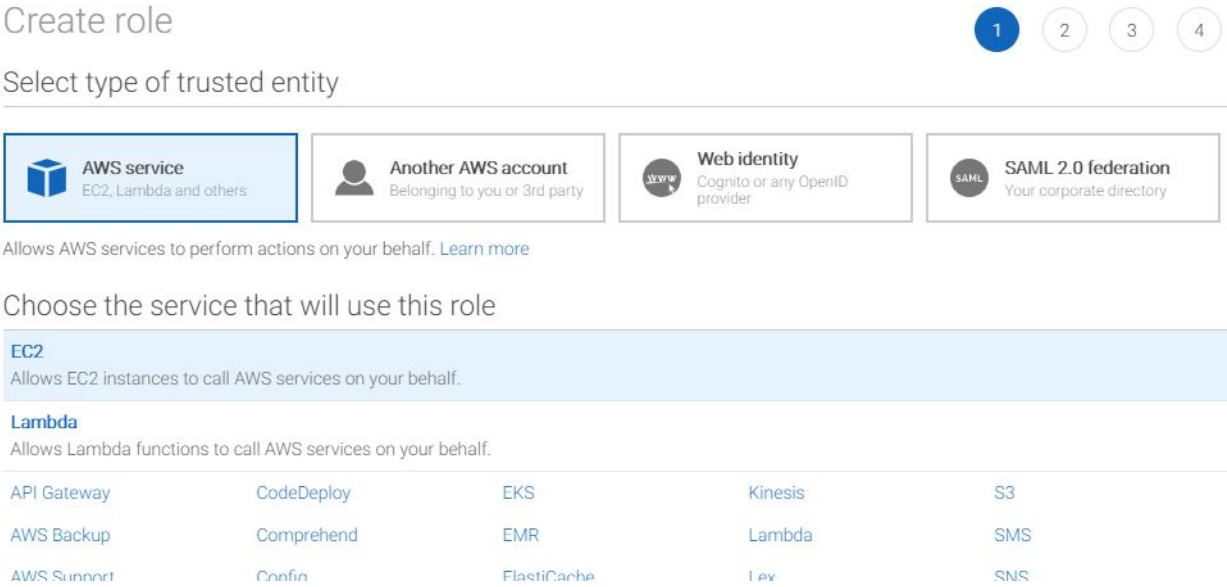
When prompted for an AMI to use, use the search facility and select the ‘medus-labs’ image.



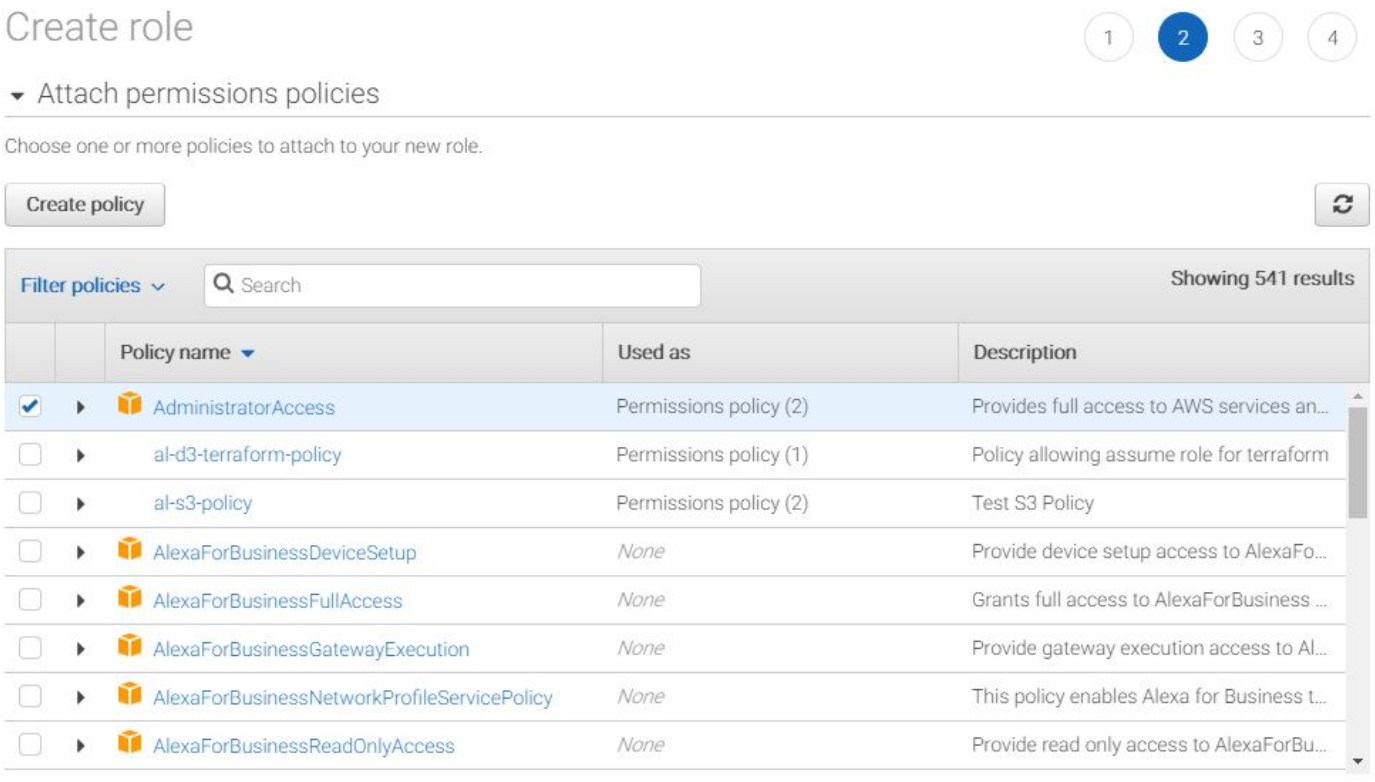
Once selected, it is best to create a new IAM role. Click ‘Create new IAM Role’ to take this action.



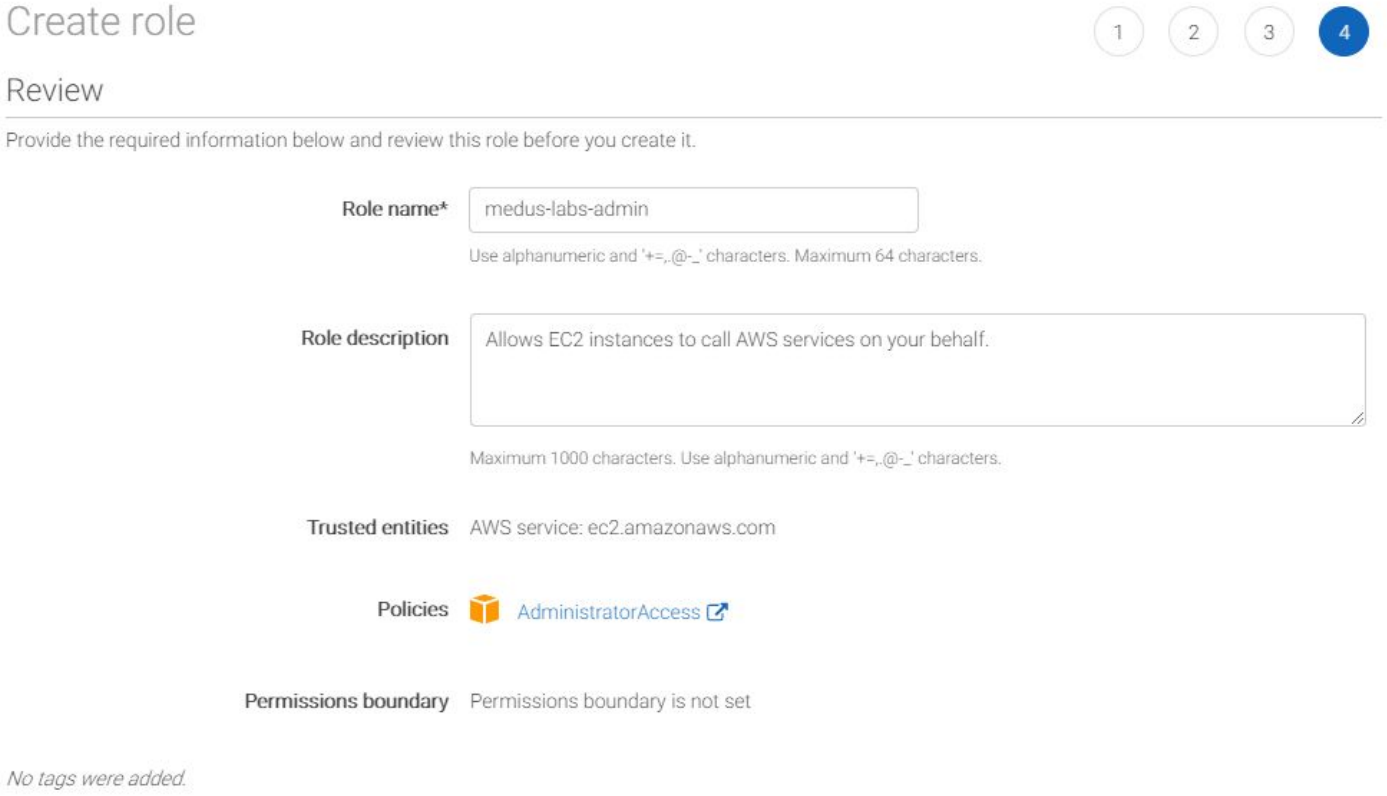
Select the relevant AWS Service - In this case, EC2.



Next, you are required to assign a policy to the new IAM role you are creating. This is heavily customisable, but selecting the ‘AdministratorAccess’ policy will ensure the application works effectively.

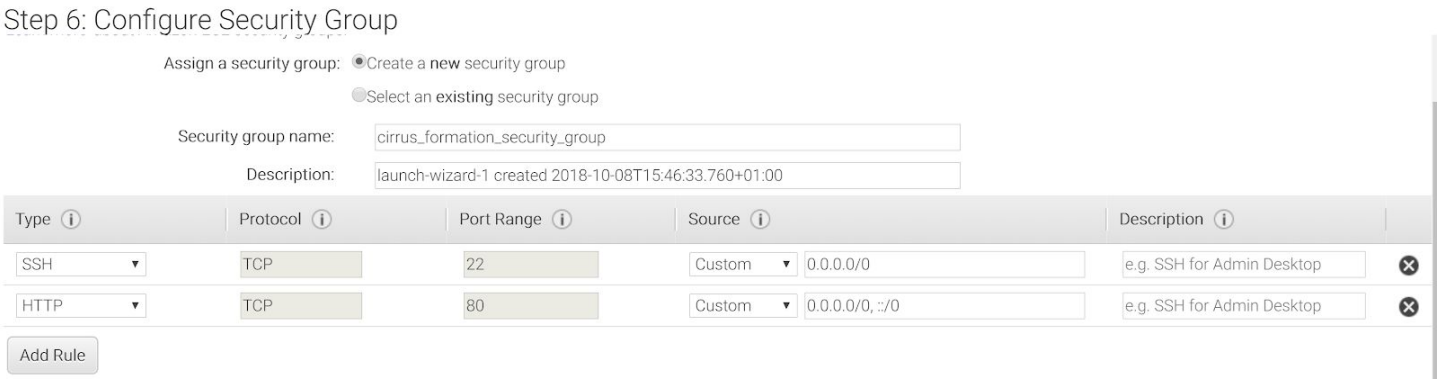


Once you proceed, you will be given the opportunity to review the role. We would advise giving the newly created IAM role a name which is easily distinguishable to prevent confusion in the future.



Once the role has been created, you'll be taken back to the 'Configure Instance Details' pane. Click the small 'refresh' icon next to 'Create new IAM role' and select the new role which will now appear in the dropdown selection.

Proceed until the 'Configure Security Group' section. It is vital to add a new rule (HTTP) to ensure you can access the UI of the Medus Labs application. Once added, your rules should look similar to the below:



Once the EC2 has built and is deemed as 'running' in the AWS Console, navigate to:

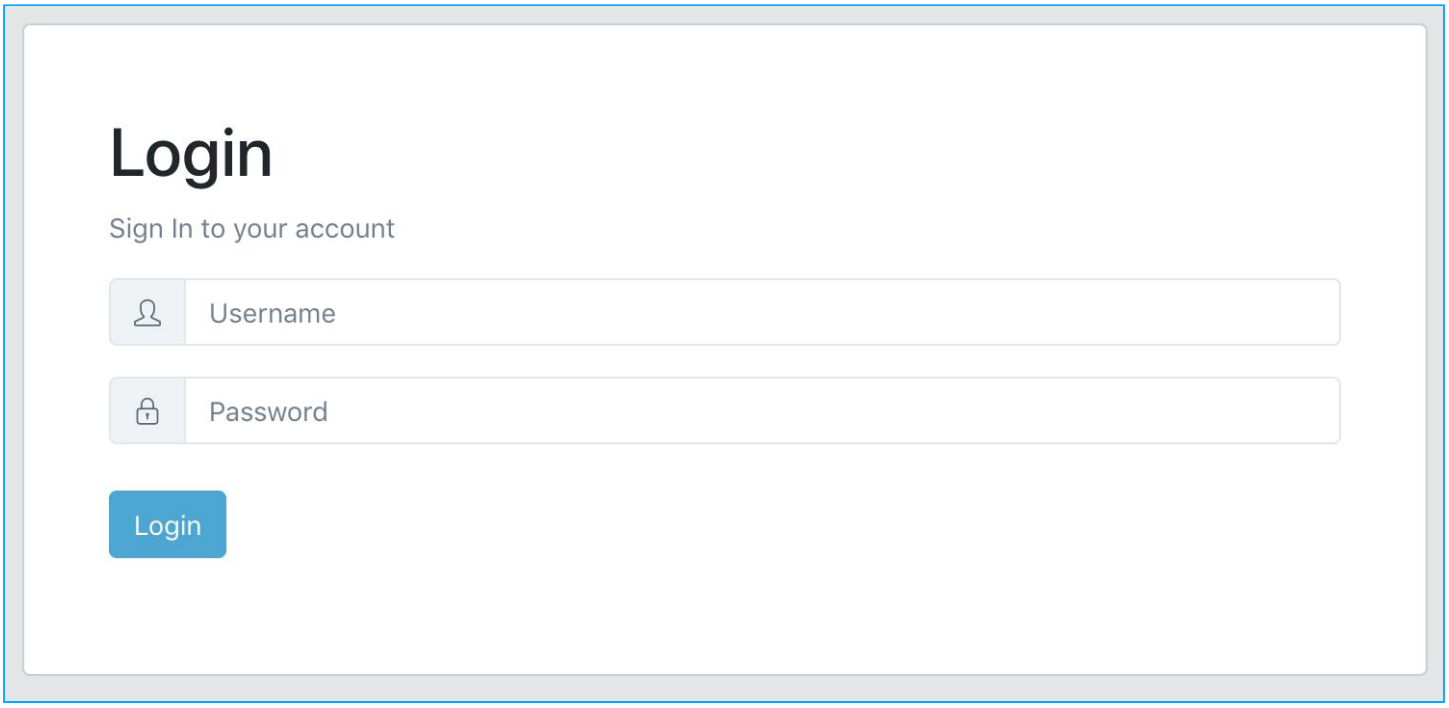
*http://**<EC2 IPv4 Address>**:8080* (the EC2 IPv4 address is visible on the AWS Console).

Once the application is running, the last step is to configure the application with your AWS Access Keys. This is a secure way of allowing the application to integrate with your AWS Environment. To achieve this, open an SSH connection to your EC2, and execute "aws configure", providing the required details.

Once complete, the application is ready to use.

UI Guide

Signing in



When you first access the application you will immediately be redirected to the login page. The default username is admin, and the default password can be found in a newly generated S3 bucket on the AWS Console. It is not possible to create a user or set of credentials from this login page.

Navigation Bar

Upon logging in, you are first presented with the dashboard. From here you can navigate to the four main areas of the application: Users, Labs, Accounts and Cleanup.

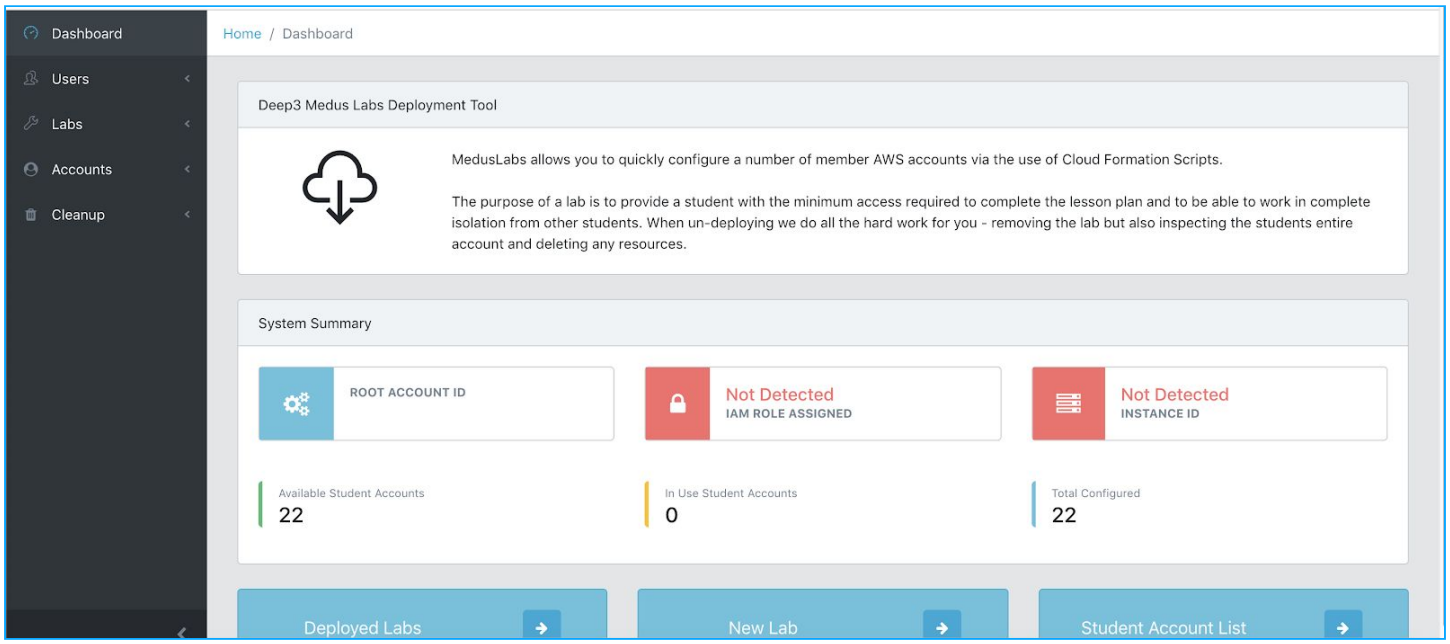
The Users page provides a list of all users who have access to the application, as well as the ability to edit or delete them. Initially this list will contain just the admin. You can also create more application user / a set of credentials from this page. Please note that users refers to users registered with this application, **NOT** the AWS accounts generated in the accounts area of the application.

The Labs pages allow you to create, monitor and delete labs. A ‘lab’ is a specific environment in which student accounts are allocated. Each lab has a theme, usually tailored toward a certain aws technology. For more information on Labs please consult the relevant section of this documentation

The Accounts pages allow you to create and list accounts for student use / allocation into labs. Doing this requires an email address client that allows the + operator. Please note that it is not possible to delete a generated AWS account via this application - it can only be emptied of data. For more information on Accounts please consult the relevant section of this documentation

The Cleanup page allows you delete all the data from the application - contents of s3 buckets, saved data with other Amazon Services and so on. This can be considered a kind of factory reset. For more information on Cleanup please consult the relevant section of this documentation

Dashboard



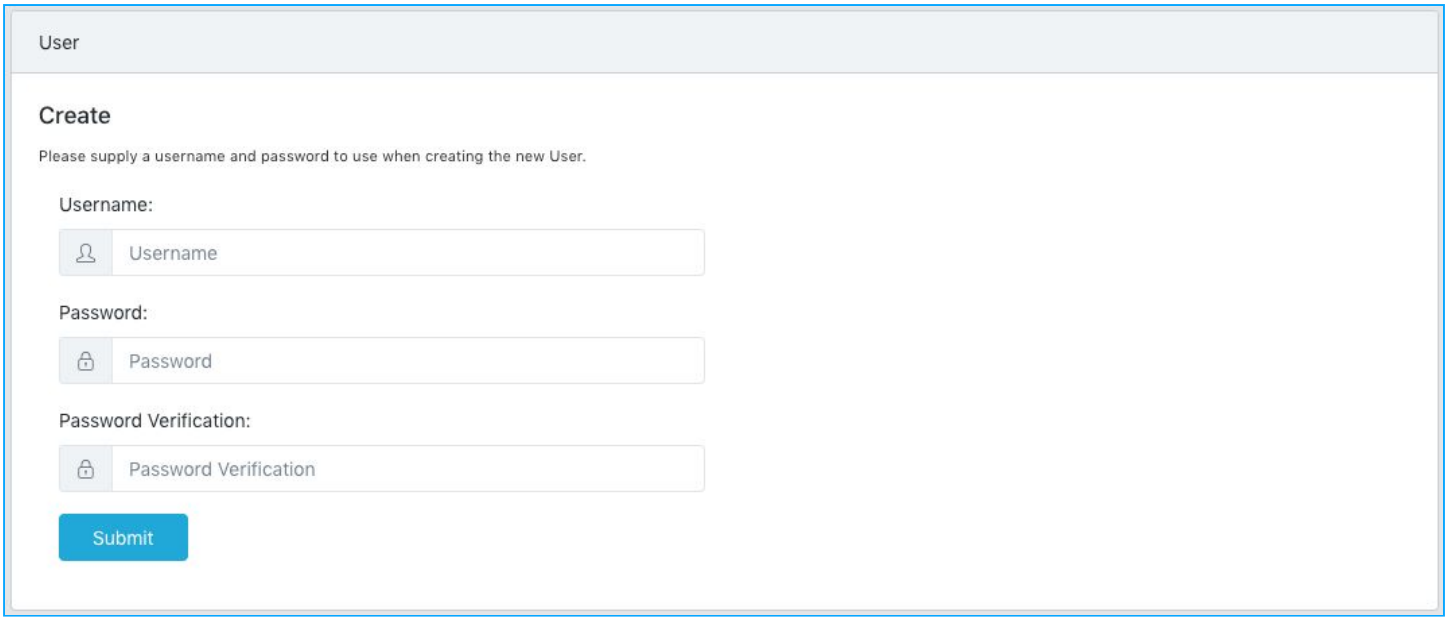
The dashboard is the landing page upon each signin. On first sign-in this page is empty of any student accounts.

Once populated, the System Summary card offers a brief snapshot of the application including AWS configurables Root Account ID, the IAM Role of the account and the instance ID. There is also a summary of the available student accounts - either **Available** or **In Use.**

The root account ID refers to AWS Account of the admin user, not any of the accounts generated via the application.

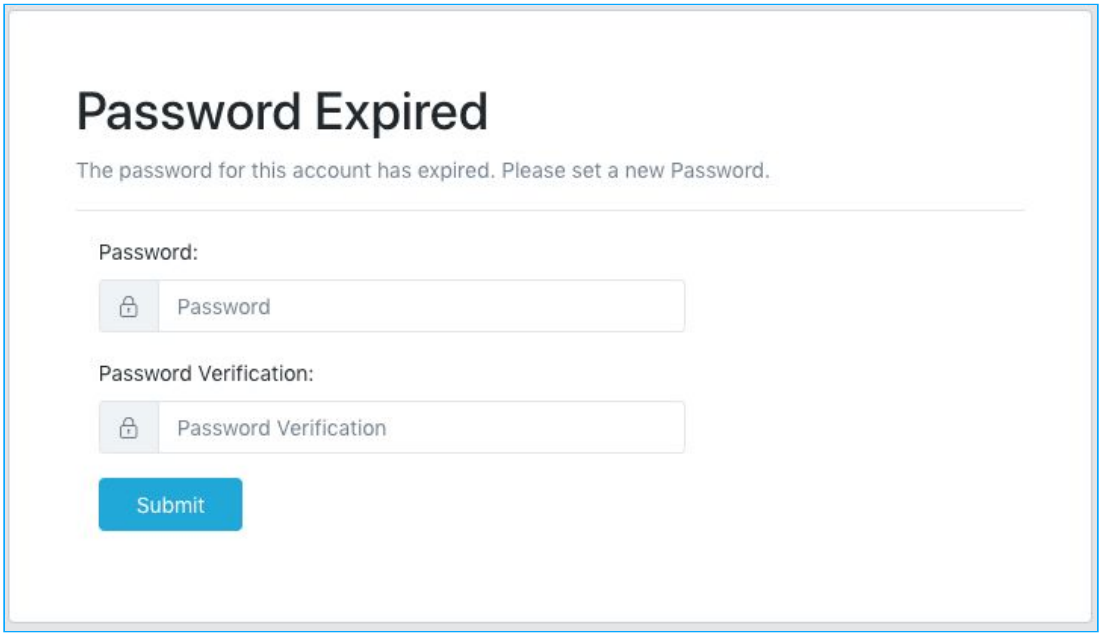
Users

To set up other users for this application you need to navigate to the Users > Create page.

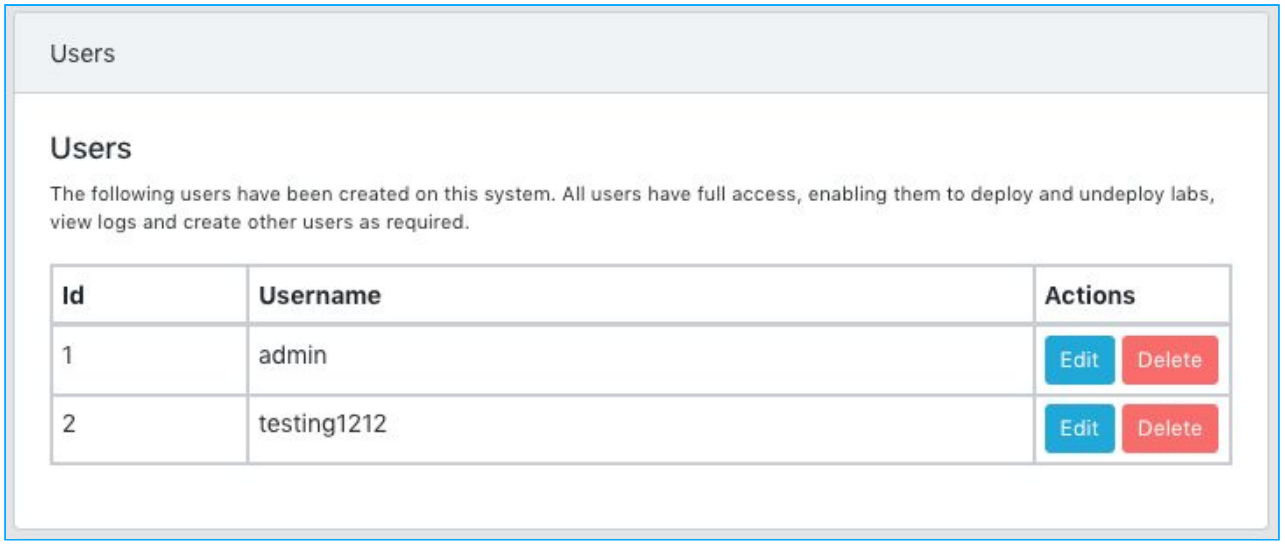


Once the form is submitted the user is primed for general use. The root account ID will be identical to that of the admin, and the user will have all the privileges granted to the administrator. Due caution should be exercised in this regard as this means any created user can wipe clean the data in the application.

The created user will have to supply a new password of their choosing once they've logged in.



The created user(s) along with the original admin user are now viewable in the list tab. From here you can edit a username and password or delete a user altogether.



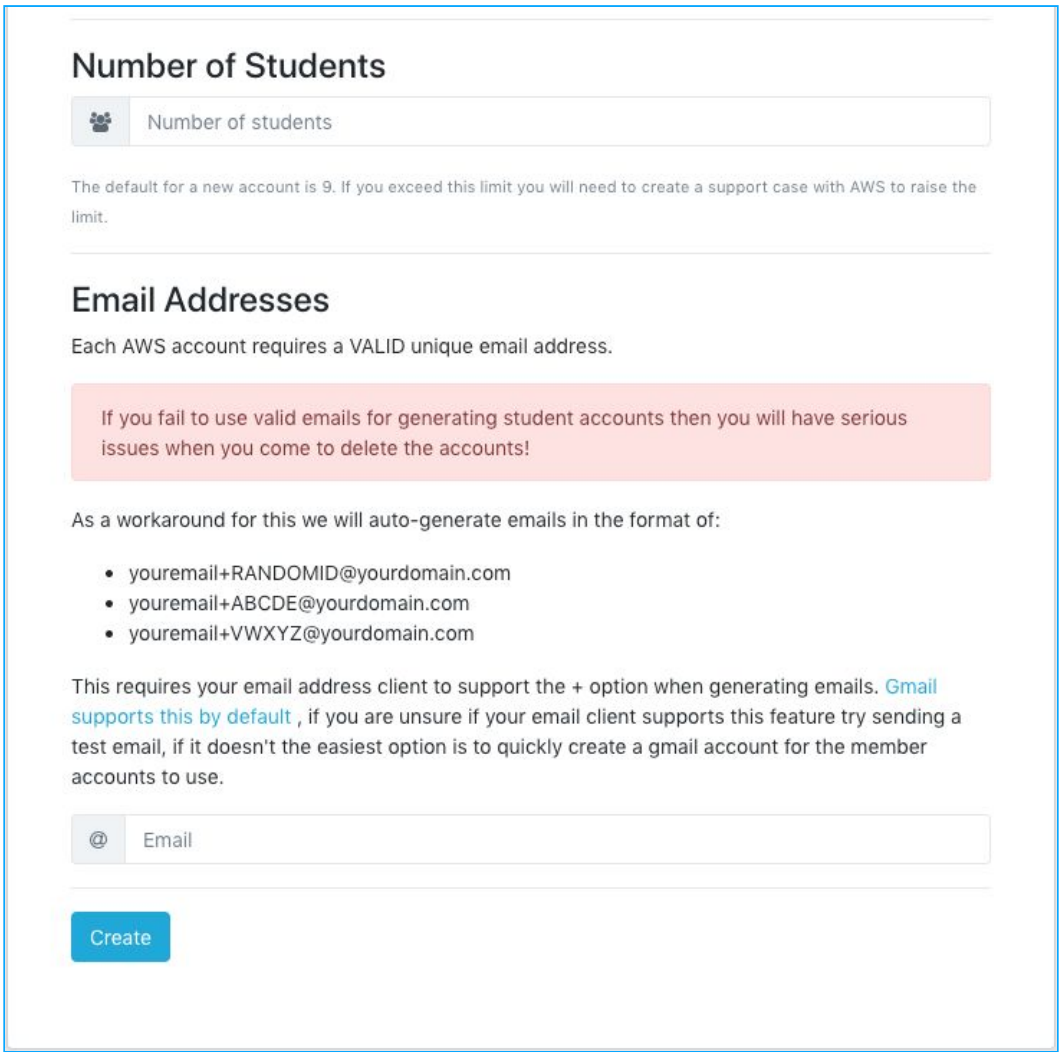
Accounts

Medus Labs allows for and automates the deployment of multiple AWS accounts, primarily for short term, lab style usage. Each AWS account requires a unique email address, but using an email provider with the '+' operator enabled streamlines this process, meaning only a single base email address is required to create 1-9 accounts. The use of AWS organisations allows one parent account to create these accounts (referred to in this application and guide as student accounts). For more information on AWS Organisations please visit https://aws.amazon.com/organizations/faqs/.

These student accounts are full AWS accounts that live under the umbrella of the parent account. It is possible to login to any of these generated accounts (known as 'switching role' on the AWS console) from the AWS console, and has associated logs in CloudFormation for debugging and troubleshooting purposes.

There is a default limit on the number of accounts that can be created, which is set at 9. To create more in a single instance / against one parent account you will need to raise a support case with AWS. The AWS support team usually respond and deal with a case such as this in under 24 hours.

Setting Up New Accounts



Opting to create new accounts will redirect you to the account creation modal. All that needs to be supplied is an email address which has a + operator supporting provider, and the number of accounts you wish to create. Once successfully created, the student accounts will be visible in the List tab:

Account	AWS Account ID
AWSLabsAccount 1	653641107383
AWSLabsAccount 1	738046251894
AWSLabsAccount 1	784068573597
AWSLabsAccount 10	836296355426
AWSLabsAccount 11	579620622192
AWSLabsAccount 12	148261647506
AWSLabsAccount 13	222442387547
AWSLabsAccount 14	558098001826

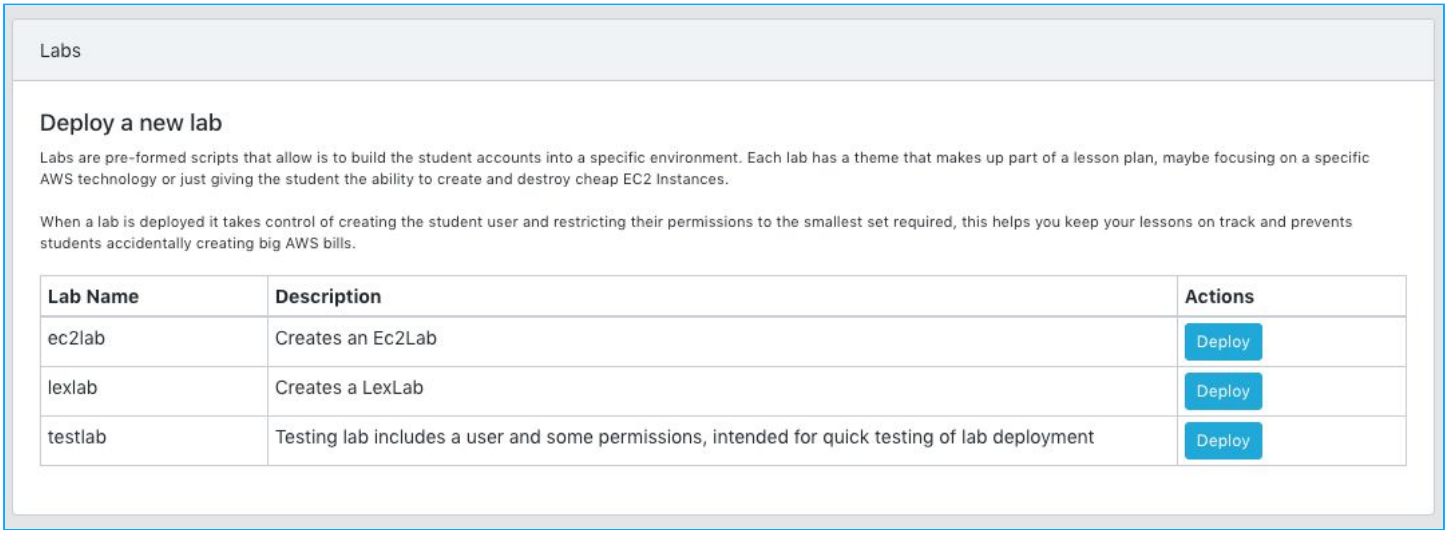
It should be noted that at this point these accounts are not strictly usable - none of them have an IAM user account assigned to them that would allow them to make use of AWS services. As part of the lab deployment process, an IAM user account is created and assigned to each account selected to be included in the new lab. This IAM user will, as previously mentioned, have restricted permissions so that students cannot perform actions outside the scope of a given lesson plan. For more information on IAM users please visit https://aws.amazon.com/iam/faqs/?nc=sn&loc=5.

Labs

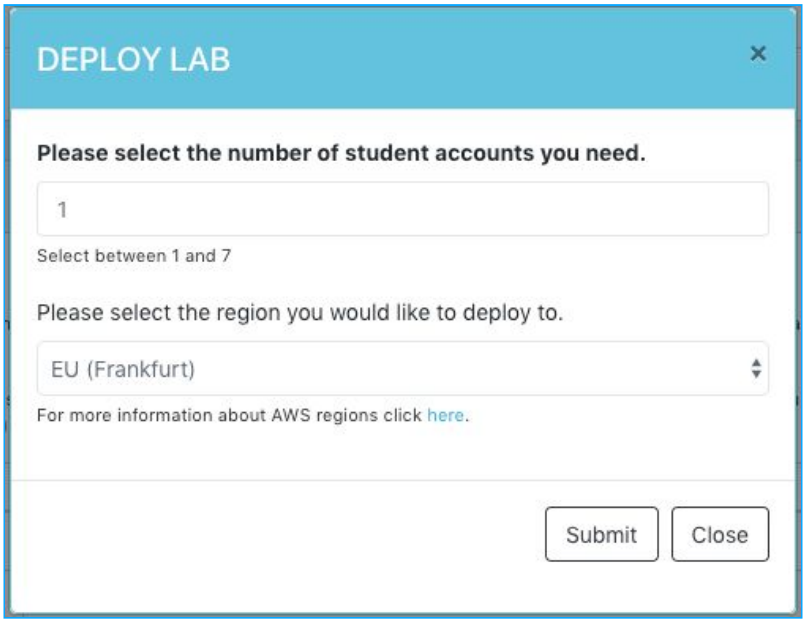
Labs are pre-formed scripts that allow us to load student accounts into a specific environment. The two labs provided by default are EC2Lab & Lexlab. Amazon EC2 is a cloud computing service and Lex is a chatbot service. Deploying a lab passes control of the account's permissions to the lab itself, restricting its permissions to the smallest set necessary, in the EC2 case only allowing minimal EC2 access and no access to any other AWS service. More 'labs' can be added by adding scripts to the cloudFormationScripts directory in the API. Describing the process of creating a script is out of scope for this guide.

There are no preconfigured labs loaded by default in Medus Labs. You must deploy and delete each one manually. Each lab requires at least one student to be assigned to it. One student account can not be assigned to two concurrent labs.

New Lab



Opting to deploy a new lab will provide you with a list of the possible, loaded lab scripts available for selection. Clicking deploy will take you to the deployment modal:

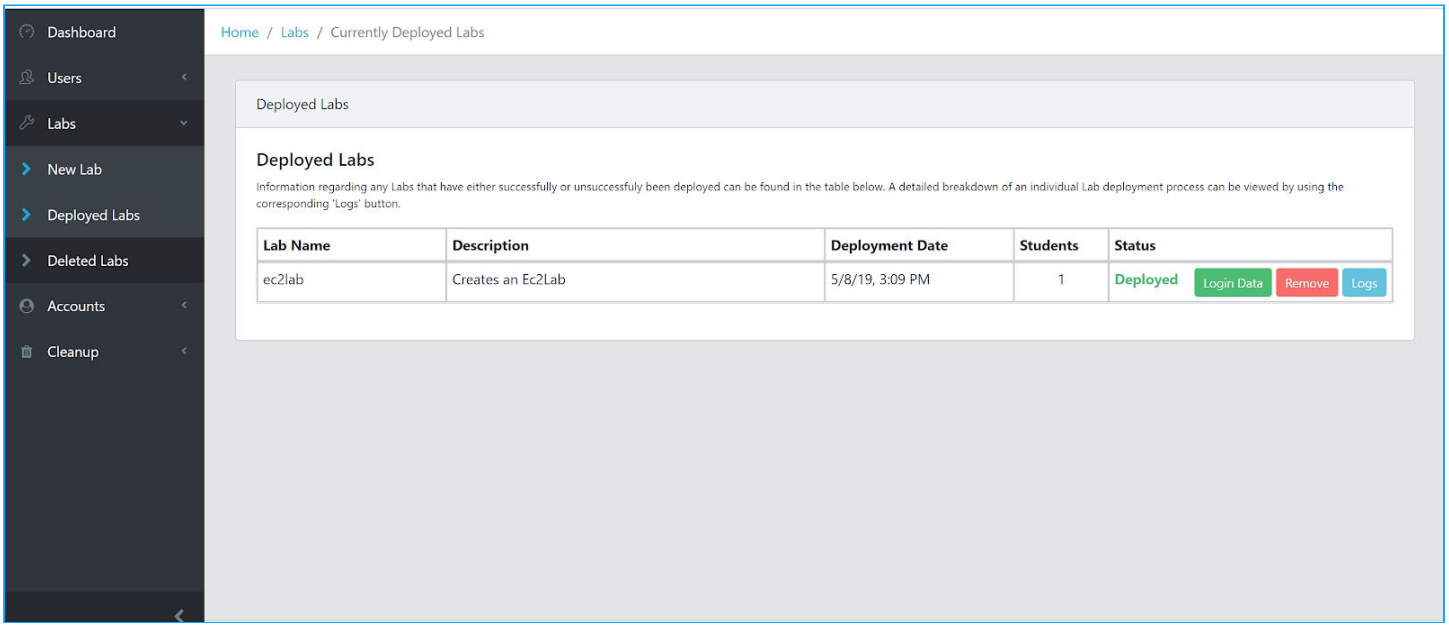


The list of available regions for a lab corresponds to the regions where the service associated with a given lab is available. For more information on AWS regions please visit here: https://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/getting-started.html#select-region

A lab may fail to deploy for numerous reasons, most commonly due to too many requests being made from a single account at once. For more detailed troubleshooting information on why a lab did not successfully deploy, you can consult the logs tab for a failed lab, or check the Cloudformation logs which will have more in depth logging information. For more information on AWS Cloudformation please visit here:

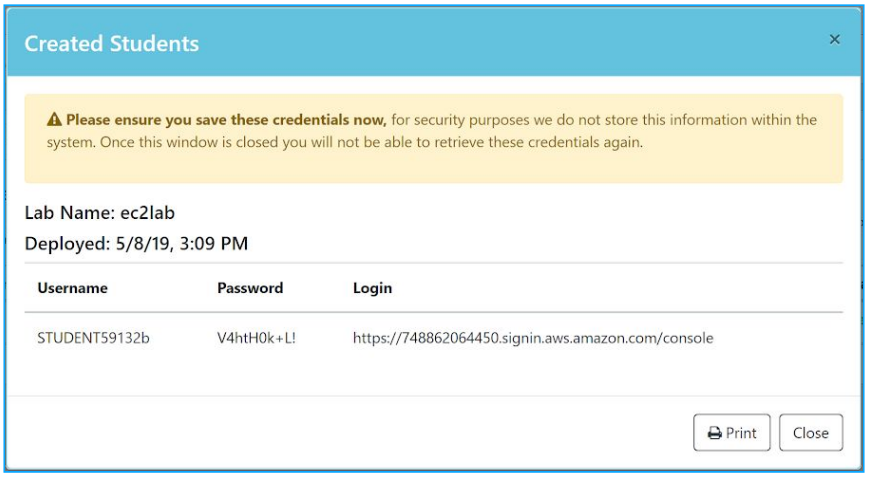
https://aws.amazon.com/blogs/devops/view-cloudformation-logs-in-the-console/

Once successfully deployed, the lab is viewable in the deployed labs section:



Note the Login Data button in the status column. Clicking on this button will reveal a modal window displaying all of the lab's student accounts login information: A randomly generated Username, Password, and console link to navigate to login. From here the students will have full use of an AWS account with its associated permissions.

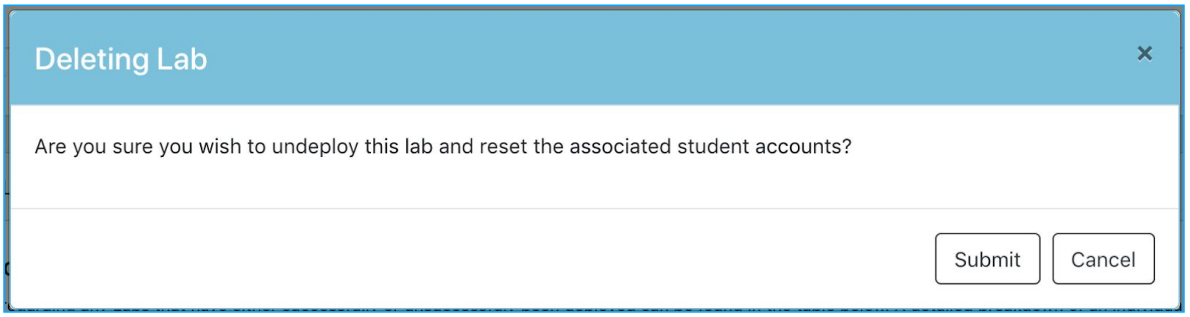
This lab login data is viewable once only. It is therefore advisable to print out this data and distribute it to the students using the lab environment as it can not be recovered. If a student or student loses their login details the only course of action is to remove the lab to make their accounts available for use in another lab.



As noted in the screengrab above, the details are not stored within the application itself as this would represent a significant vulnerability

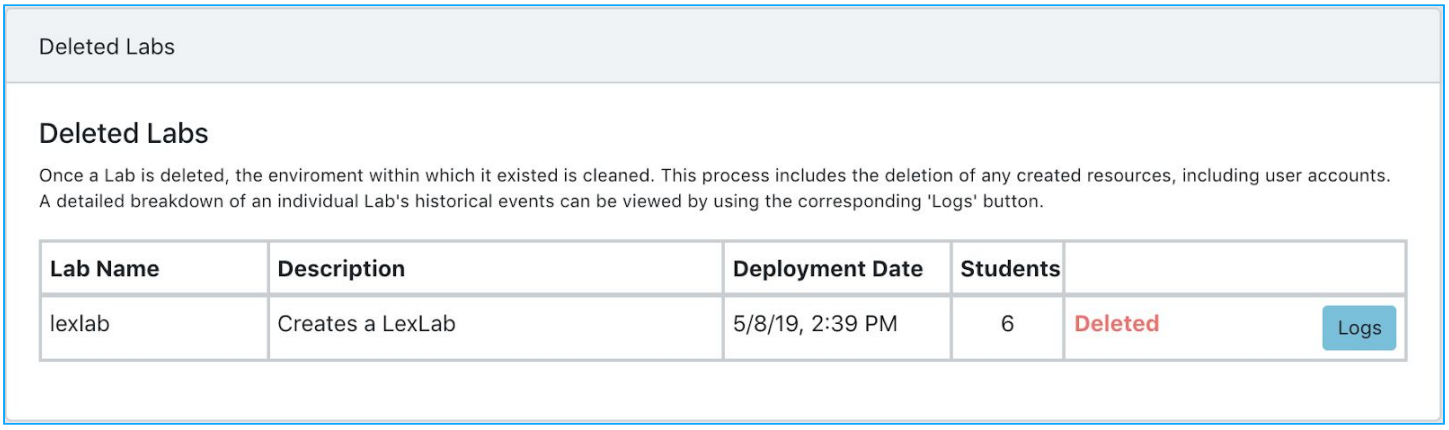
Deleting a Lab

Once a lesson has concluded, you can navigate to the deployed labs section and delete an individual lab, and make the student accounts allocated to it available for use in another lab. This will also prevent students from continuing to use the accounts. Conversely if the lab is not deleted then students will be free to use the IAM accounts indefinitely, and their accounts cannot be reallocated. The application has no timeout feature, and no labs will be deleted automatically. It is the responsibility of the user to manage these resources within the application.



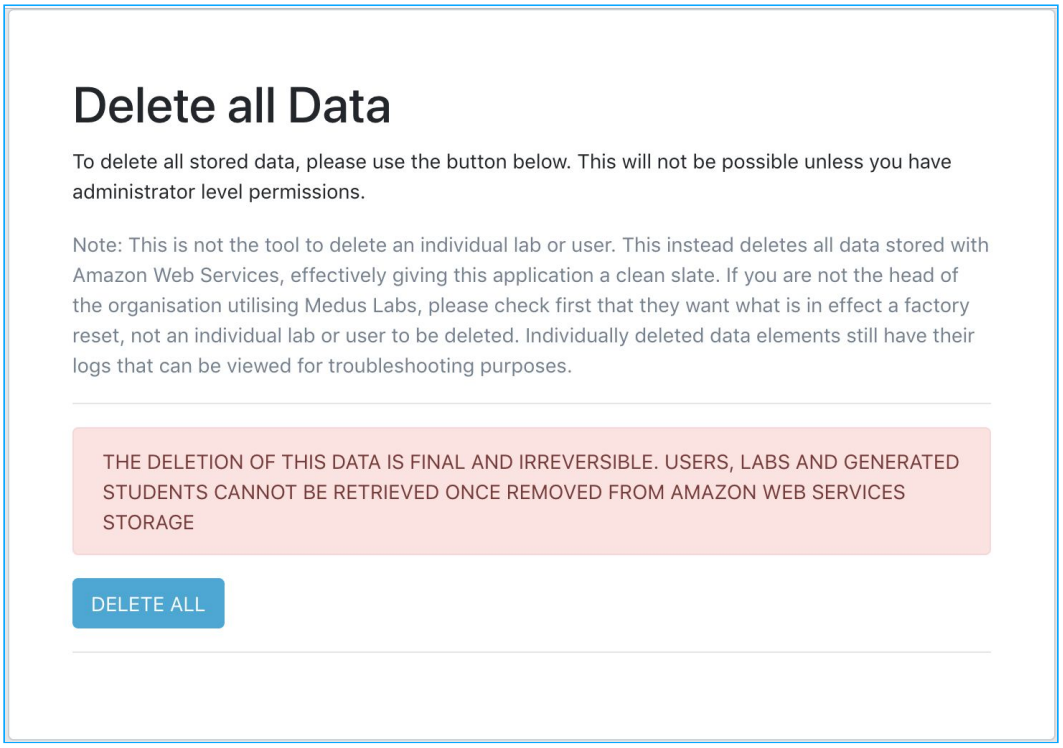
The removal of a lab is not instantaneous; it will take time to coordinate the reset with AWS. A lab will appear as **removing** in the deployed labs sections whilst this is in progress:

Once this process has finished the lab will no longer be viewable in the deployed labs section. It can then be viewed in the deleted labs section. Any resources used within the accounts in a deleted lab have been cleared.



Cleanup

The Cleanup section of the website allows you to perform a factory reset on the application. This will clear the application of generated AWS accounts, and any resources they may have used. It will also remove all deployed labs. This process is irreversible, so it is recommended that you verify you have no further use for the accounts nor the resources stored within them. This is also another reason not to give students direct access to the Medus-Labs application.



The deletion of all AWS resources is done in sequence, one after the other. A modal window is displayed illustrating the number of accounts successfully deleted: