

# IAM Automation Lab Documentation

Cletus Nehinlalei Mangu  
cletus.mangu@amalitechtraining.org  
GTP Programming and Ops Challenge

May 4, 2025

## Lab Overview

This lab aims to automate Identity and Access Management (IAM) tasks on a Linux machine using a Bash script. The script handles user and group provisioning, home directory configuration, password policies, and email notifications. All activities are logged for auditability.

## Objectives

- Automate user and group creation from a CSV file.
- Assign full names and group memberships.
- Apply password complexity and enforce password resets.
- Secure each user's home directory.
- Log all actions to a file.
- Send notification emails and validate password complexity.

## Environment

- **OS:** Ubuntu 22.04 LTS
- **Tools:** bash, useradd, groupadd, chage, passwd, mailutils
- **Privileges:** Root or sudo required

## Input File Format

The script accepts a CSV file named `users.txt` | `users.csv` in the following format:

<code>username , fullname , group</code>
--

## Script Overview: `iam_setup.sh`

### Main Features

- Checks and creates groups if they do not exist.
- Adds users with full name, group, home directory.

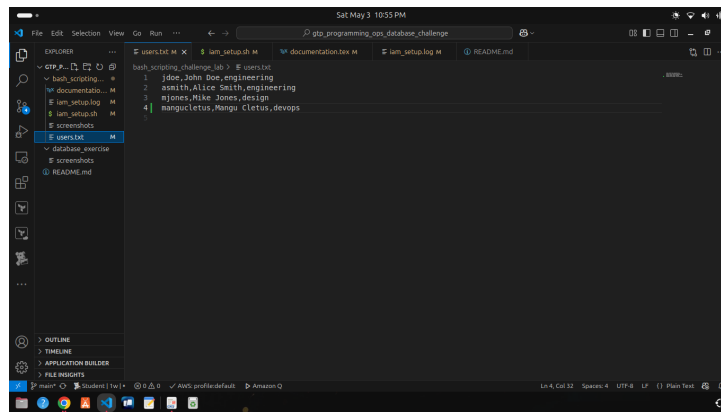


Figure 1: Sample users.txt format

- Assigns temporary password and enforces reset.
- Validates password complexity.
- Locks down home directory permissions using `chmod 700`.
- Sends email notifications to users.
- Logs all actions to `iam_setup.log`.

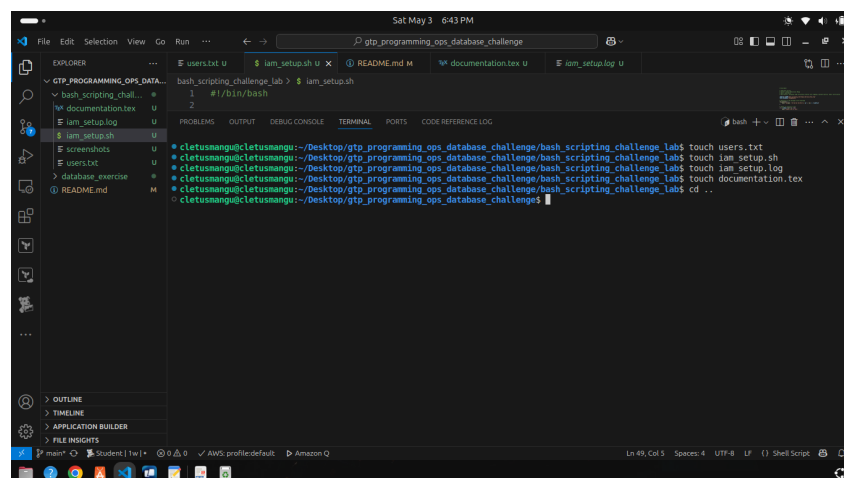


Figure 2: Script displayed in terminal

## Running the Script

### 1. Make Script Executable

```
chmod +x iam_setup.sh
```

### 2. Install Dependencies (Optional)

```
sudo apt update  
sudo apt install mailutils -y
```

### 3. Execute the Script

```
sudo ./iam_setup.sh users.txt
```

```

cletusmanguctetus@~/Desktop/gtp_programming_ops_database_challenge/bash_scripting_challenge_lab$ sudo ./iam_setup.sh users.txt
[sudo] password for cletusmanguctetus:
[2025-05-03 23:11:41] Created group: engineering
[2025-05-03 23:11:41] Created user: jdoe, Fullname: John Doe, Group: engineering
[2025-05-03 23:11:41] Password set for jdoe
[2025-05-03 23:11:41] Password reset on first login enforced for jdoe
[2025-05-03 23:11:41] Permissions set to 700 on /home/jdoe
[2025-05-03 23:11:41] Email sent to jdoe@gmail.com
[2025-05-03 23:11:41] Group already exists: engineering
[2025-05-03 23:11:41] Created user: asmith, Fullname: Alice Smith, Group: engineering
[2025-05-03 23:11:41] Password set for asmith
[2025-05-03 23:11:41] Password reset on first login enforced for asmith
[2025-05-03 23:11:41] Permissions set to 700 on /home/asmith
[2025-05-03 23:11:41] Email sent to asmith@gmail.com
[2025-05-03 23:11:41] Created group: design
[2025-05-03 23:11:41] Created user: mjones, Fullname: Mike Jones, Group: design
[2025-05-03 23:11:41] Password set for mjones
[2025-05-03 23:11:41] Password reset on first login enforced for mjones
[2025-05-03 23:11:41] Permissions set to 700 on /home/mjones
[2025-05-03 23:11:41] Email sent to mjones@gmail.com
[2025-05-03 23:11:42] Created group: devops
[2025-05-03 23:11:42] Created user: manguctetus, Fullname: Mangu Cletus, Group: devops
[2025-05-03 23:11:42] Password set for manguctetus
[2025-05-03 23:11:42] Password reset on first login enforced for manguctetus
[2025-05-03 23:11:42] Permissions set to 700 on /home/manguctetus
[2025-05-03 23:11:42] Email sent to manguctetus@gmail.com
cletusmanguctetus@~/Desktop/gtp_programming_ops_database_challenge/bash_scripting_challenge_lab$

```

Figure 3: Executing the IAM script

## Logging and Password Enforcement

### Logging

All actions are recorded in iam\_setup.log:

```

[2025-05-03 14:20:12] Created group: engineering
[2025-05-03 14:20:14] Created user: jdoe
[2025-05-03 14:20:15] Set password for jdoe

```

```

1 [2025-05-03 23:11:41] Created group: engineering
2 [2025-05-03 23:11:41] Created user: jdoe, Fullname: John Doe, Group: engineering
3 [2025-05-03 23:11:41] Password set for jdoe
4 [2025-05-03 23:11:41] Password reset on first login enforced for jdoe
5 [2025-05-03 23:11:41] Permissions set to 700 on /home/jdoe
6 [2025-05-03 23:11:41] Email sent to jdoe@gmail.com
7 [2025-05-03 23:11:41] Group already exists: engineering
8 [2025-05-03 23:11:41] Created user: asmith, Fullname: Alice Smith, Group: engineering
9 [2025-05-03 23:11:41] Password set for asmith
10 [2025-05-03 23:11:41] Password reset on first login enforced for asmith
11 [2025-05-03 23:11:41] Permissions set to 700 on /home/asmith
12 [2025-05-03 23:11:41] Email sent to asmith@gmail.com
13 [2025-05-03 23:11:41] Created group: design
14 [2025-05-03 23:11:41] Created user: mjones, Fullname: Mike Jones, Group: design
15 [2025-05-03 23:11:41] Password set for mjones
16 [2025-05-03 23:11:41] Password reset on first login enforced for mjones
17 [2025-05-03 23:11:41] Permissions set to 700 on /home/mjones
18 [2025-05-03 23:11:41] Email sent to mjones@gmail.com
19 [2025-05-03 23:11:42] Created group: devops
20 [2025-05-03 23:11:42] Created user: manguctetus, Fullname: Mangu Cletus, Group: devops
21 [2025-05-03 23:11:42] Password set for manguctetus
22 [2025-05-03 23:11:42] Password reset on first login enforced for manguctetus
23 [2025-05-03 23:11:42] Permissions set to 700 on /home/manguctetus
24 [2025-05-03 23:11:42] Email sent to manguctetus@gmail.com
25

```

Figure 4: View of log file output

### Password Policy

The temporary password must meet:

- Minimum 8 characters

- At least 1 uppercase, 1 lowercase, and 1 digit

```
chage -d 0 username
```

```

53
54 # Function to check password complexity
55 check_password_complexity() {
56     local password="$1"
57     if [[ ${#password} -lt 8 ]]; then return 1; fi
58     [[ "$password" =~ [A-Z] ]] && [[ "$password" =~ [a-z] ]] && [[ "$password" =~ [0-9] ]]
59     return 0
60 }
61

```

Figure 5: Password policy applied and enforced

## Permissions

Each user's home directory is restricted:

```
chmod 700 /home/username
```

```

98
99 # Enforce password reset
100 chage -d 0 $username
101 log_action "Password reset on first login enforced for $username"
102
103 # Set secure home directory permissions
104 chmod 700 "/home/$username"
105 log_action "Permissions set to 700 on /home/$username"
106

```

Figure 6: Verifying permissions for home directory

## Optional: Email Notification

```
echo "Welcome to the system, $FULLNAME." | mail -s "Account Created"
➔ $USERNAME@gmail.com
```

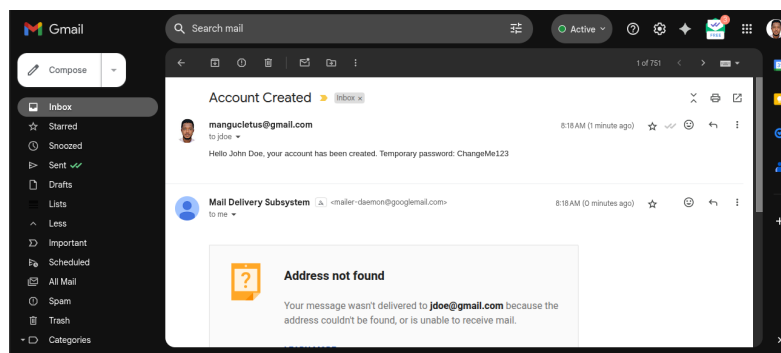


Figure 7: Email notification sent from script

## Project Directory Structure

```

bash_scripting_challenge_lab/
|-- iam_setup.sh
|-- users.txt
|-- iam_setup.log

```

```
|-- README.md
'-- screenshots/
    |-- users_txt_content.png
    |-- script_in_terminal.png
    |-- run_script.png
    |-- password_policy.png
    |-- log_output.png
    |-- home_dir_permissions.png
    '-- email_notification.png
```

## Author

**Cletus Nehinlalei Mangu**

Email: [cletus.mangu@amalitechtraining.org](mailto:cletus.mangu@amalitechtraining.org)

GitHub: <https://github.com/mangucletus>