Project: Creating Password Policies and Allowing User to Change Password
Project Completed By: Brionna Morris
Cloud Service Provider (CSP): Amazon Web Services (AWS)
Areas and Services of Focus: Identity and Access Management (IAM), password policies, least privilege, security, users, roles, policies, multi-factor authentication, root user.

Introduction:

In this project document I provide information on various services and definitions of critical components within the AWS environment. The beginning focuses on the fundamentals of Identity and Access Management and near the end, I focus on a project task to gain hands-on experience in working with the services within the AWS environment, specifically IAM (Identity and Access Management).

What is Identity and Access Management:

Identity and Access Management (IAM) is a service within AWS and other cloud service providers (CSPs) that allow administrators to manage users, user groups, roles, and policies. In more succinct terms it allows organizations to manage, secure, and define user roles and privileges. It also ensures that the right individuals have the right access.

IAM, in terms of security, allows administrators and/or engineers to implement best practices such as least privilege, multi-factor authentication, single sign-on, as well as implementing password policies and resetting user passwords. IAM is important for organizational security and compliance.

What are users, roles, user groups, and policies:

- **Users**: A user is a person or application that has been granted access to AWS resources within the organization. These are additional accounts created by the root user, but not accessed through the root user account. Users can be created by other users if those permissions have been assigned.

- **User Groups**: A user group is created to manage multiple users within a group that are typically assigned the same policies. One example would be a team of marketing individuals needing access to a storage database of social media posts. An admin, or individual with permissions to create user groups could create a Marketing User Group that grants access to the database. It is important to know that user groups cannot be added to other user groups, only individuals.

- **Roles**: Roles are similar to users, however they are not assigned or associated to a user, application or service. Roles are created for users, applications, and services to access when needed (assuming they have the privilege). These are identities that have specific permissions and have temporary security credentials to gain access.

- **Policies**: All policies in the AWS environment are JSON documents. These policies are necessary to manage access and permissions for users, applications, and/or services. These policies determine what is allowed or denied. There are different types of policies such as:

  - **Identity-Based**
  - **Resource-Based**
  - **Access Control Lists (ACLs)**
  - **And many more**...

IAM Best Practices vs Security Best Practices:

Identity and Access Management (IAM) allows teams to implement security and compliance within their organization. Some IAM Best Practices include, but are not limited to:

- Principles of Least Privilege
- Using IAM Groups
- Granting Read Only Access
- Password Policies and MFA enforcement

These are all practices necessary to ensure a secure cloud environment for the organization and the individuals within the organization.

In terms of cybersecurity best practices, many are similar to those in the cloud and can be implemented in the cloud. Some additional examples include:

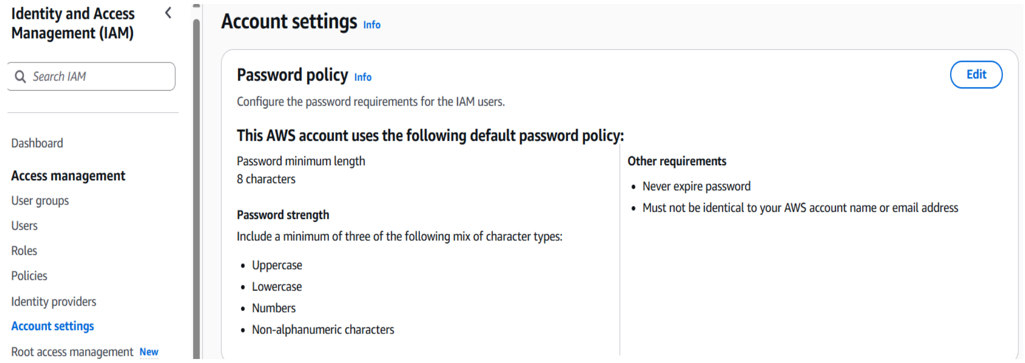
- Zero-Trust Architecture
- Cybersecurity Awareness Training
- Network Segmentation
- Secure Cloud Configurations

These are a short number of best practices, but are integral to a secure environment.

Project Details and Photos:

The photos below represent the steps taken during the process of setting the password policy and managing the user's accounts settings to change their own password. (Note: The photos below do not represent the actual policy implemented on the user account. It is merely to show the options available and the steps taken to make the changes).

STEP ONE: Log into the AWS console and navigate to the Identity and Access Management (IAM) service.



Configure the password requirements for the IAM users.

This AWS account uses the following default password policy:

Password minimum length
8 characters

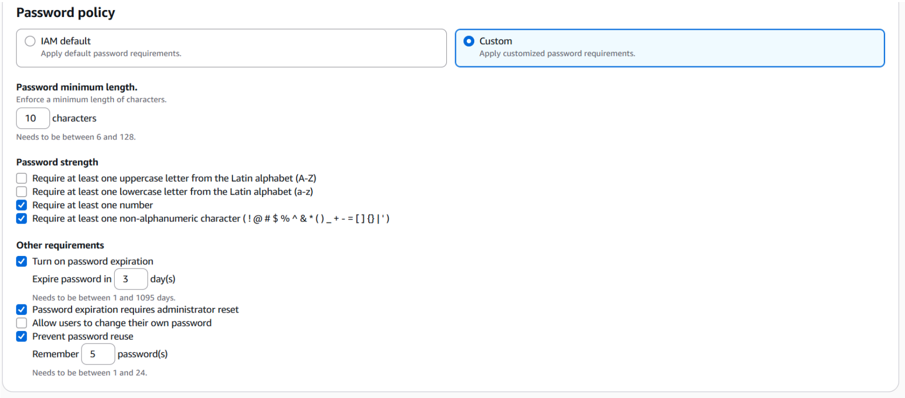
Password strength
Include a minimum of three of the following mix of character types:

- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

STEP TWO: Instead of selecting IAM default (basic settings), select Custom to set a new password policy that adds additional security. You are able to modify the password strength and add additional requirements for users to access their accounts. This makes it harder for threat actors to access the system environment. However, there are other security methods such as multi-factor authentication, available and recommended to implement.



Password policy

○ IAM default
Apply default password requirements.

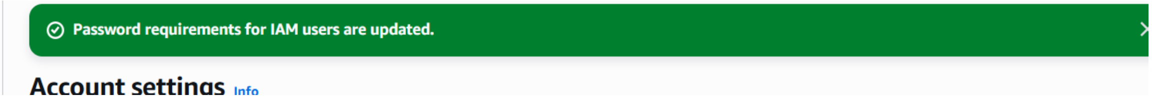
● Custom
Apply customized password requirements.

Password minimum length.
Enforce a minimum length of characters.
10 characters
Needs to be between 6 and 128.

Password strength
- □ Require at least one uppercase letter from the Latin alphabet (A-Z)
- □ Require at least one lowercase letter from the Latin alphabet (a-z)
- ☑ Require at least one number
- ☑ Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] {} | ')

Other requirements
- ☑ Turn on password expiration
  Expire password in 3 day(s)
  Needs to be between 1 and 1095 days.
- ☑ Password expiration requires administrator reset
- □ Allow users to change their own password
- ☑ Prevent password reuse
  Remember 5 password(s)
  Needs to be between 1 and 24.

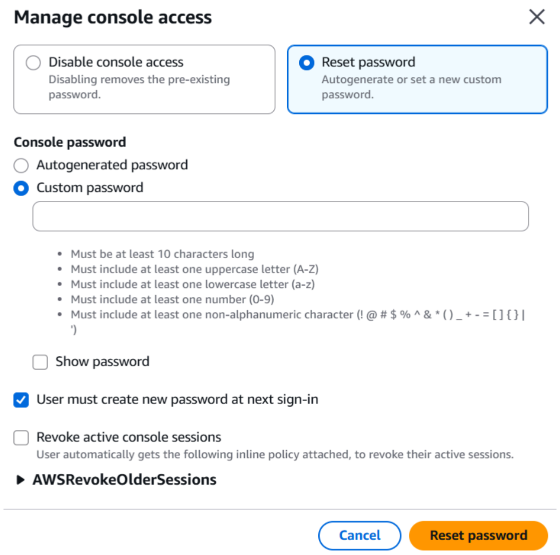
STEP THREE: Once you have saved your custom password requirements, you should receive a notification that the requirements for your IAM users have been updated.



Password requirements for IAM users are updated.

Account settings Info

STEP FOUR: Once you have completed the previous step, click Users and select the user account that you will make changes to. Once selected, click the Security credentials tab, select manage console access and reset password. At this stage you will need to select preferences such as creating a temporary password for the user and allowing them to change their password upon sign in.



Manage console access

○ Disable console access
Disabling removes the pre-existing password.

● Reset password
Autogenerate or set a new custom password.

Console password
- ○ Autogenerated password
- ● Custom password

  - Must be at least 10 characters long
  - Must include at least one uppercase letter (A-Z)
  - Must include at least one lowercase letter (a-z)
  - Must include at least one number (0-9)
  - Must include at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')

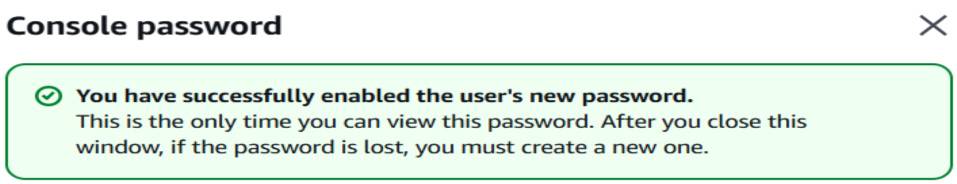
  □ Show password

☑ User must create new password at next sign-in

□ Revoke active console sessions
User automatically gets the following inline policy attached, to revoke their active sessions.

▸ AWSRevokeOlderSessions

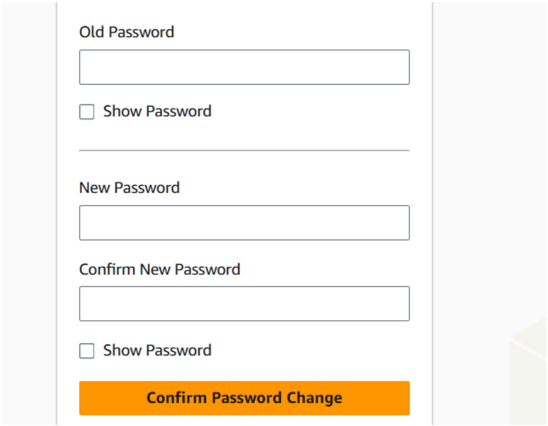
STEP FIVE: Once you have implemented password reset changes for the user(s), you should receive a notification that the new password has been enabled.



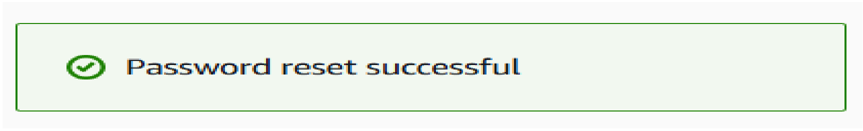
Console password

You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

STEP SIX: Log out of the root user account. If you are using AWS to build projects or practice working with the services within the cloud provider platform, log into the user account that you created. If you are creating the password changes for a user they will need to log into their account with the custom password you created. For this example, I have access to the root user and user account where I will change the password. When trying to login, a notification will appear asking to add the old password and the new password.



STEP SEVEN: In the final step, you should receive a notification that a new password for the user was created successfully. Depending on the password policy changes made in previous steps, the user should expect to change their password soon and will not be able to reuse an old password.



Password reset successful

Conclusion:
Overall, the tasks for this project were easy to complete. The primary tasks were to set a custom password policy and modify the user's account to change their password from the password created for the user from the root user account
.

Resources:
[AWS Documentation for Account Password Policy for IAM Users]