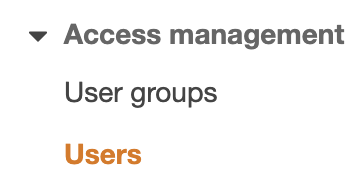
**Introduction**

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

**Instructions**

1. From the **Identity & Access Management** console, click on **Users** in the sidebar menu:



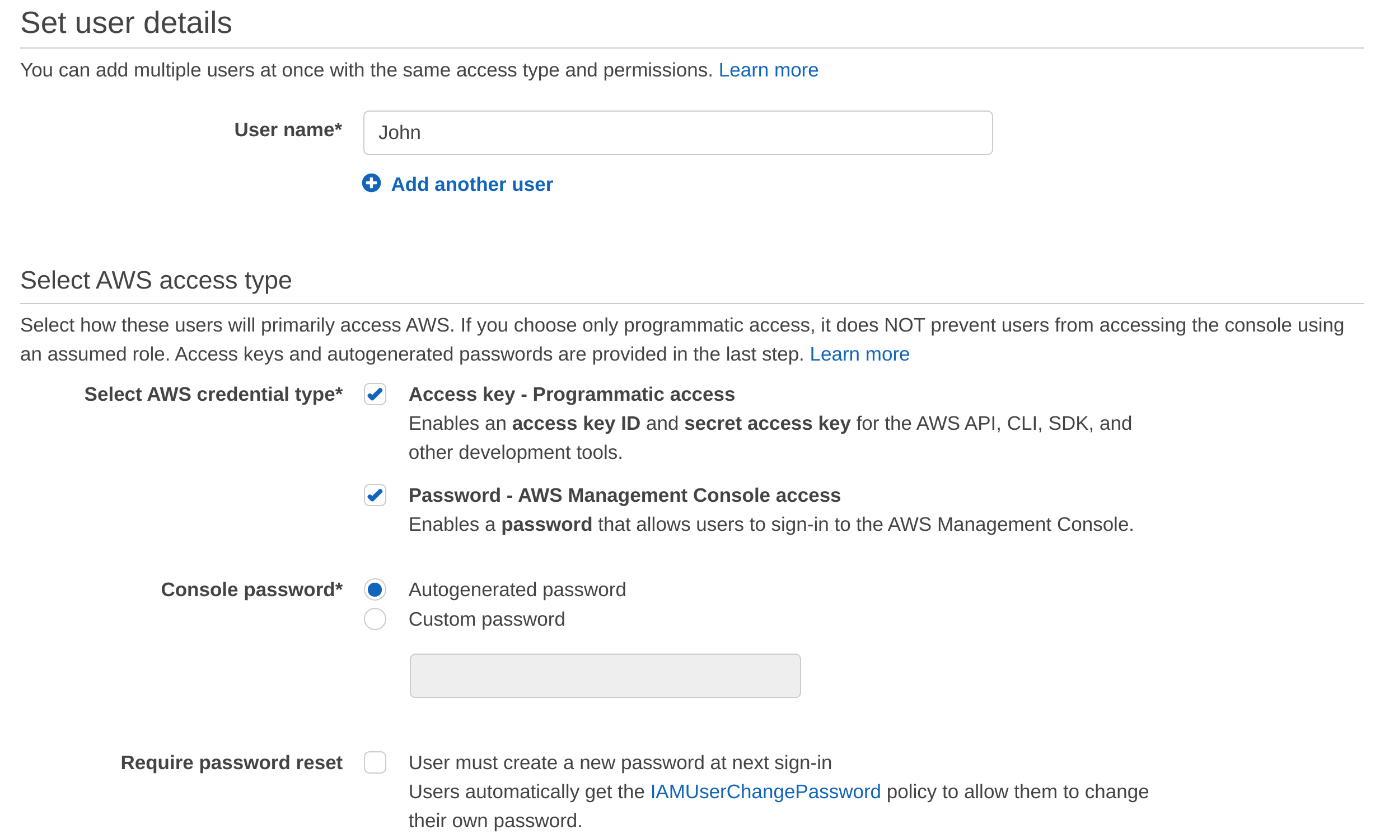
2. Click **Add users**to begin creating a new user:



*Note:* You can create up to 10 users at a time with usernames that don't exceed 64 characters.

3. Enter the following values in the form:

* **User name**: *John* (Name must be case sensitive)
* **Access key - Programmatic access**: Checked
* **Password - AWS Management Console access**: Checked
* **Console password**: **Autogenerated password**
* **Require password reset**: Unchecked



4. Click **Next: Permissions** to advance to the next step.

5. Click**Next: Tags**. Skip this page and click on **Next: Review**.

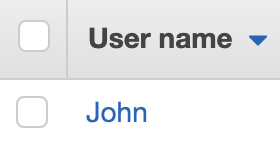
You will add the user to the DevOps Group later.

6. Click **Create User.**

7. Click**Download .csv**for downloading a CSV file containing the security credentials and then click **Close**:



8. Review the newly-created user in the **IAM Console**:



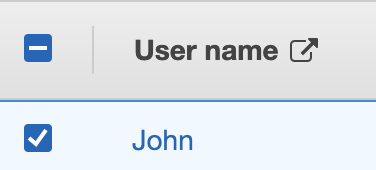
You will now add John to the DevOps Group.

9. Click **User groups** > **DevOps** to open the DevOps group details view:

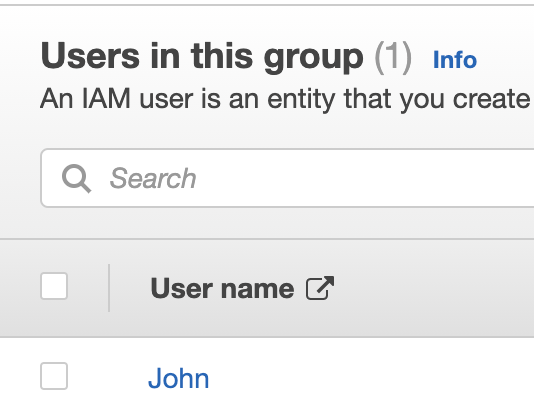


10. Click **Add Users**.

11. Check **John** and click **Add Users**:



Observe that John is now in the DevOps group:



**Summary**

In this lab step, you used the IAM Management console to create an IAM user and attach it to an IAM group.

VALIDATION CHECKS

**2Checks**

Check again

**Created IAM User**

Check that an IAM User with the specified name exists

AWS Identity and Access Management (IAM)

**Added IAM User to IAM Group**

Added the IAM User to the IAM Group

AWS Identity and Access Management (IAM)