SECURING MULTI-VENDOR CLOUDS

LABS 2 - Deploying MFA for single sign-on to an individual AWS account

ABSTRACT

This lab document contains a step-by-step guide to configuring MFA for single sign-on to an individual AWS Account. It will provide attendees with instructions on how to deploy Conditional Access policies to enable MFA to AWS Console.

Luciana Blanchard

Written for **Securing Multi-vendor Clouds** a series of events for **Microsoft Partners** created by Luciana Blanchard.
Luciana.blanchard@microsoft.com

Contents

1. Getting started

Azure AD supports single sign-on integration with AWS SSO. With AWS SSO you can connect Azure AD to AWS in one place and centrally govern access across hundreds of accounts and AWS SSO integrated applications. This enables seamless Azure AD sign-in experience for users to use the AWS Console.

The following Microsoft security solution procedure uses Conditional Access policies to implement multifactor authentication for SSO to AWS Console.

This lab covers the following steps:

1. Create a Conditional Access policy for AWS Console application.
2. Test sign-in to AWS Console with multi factor authentication.

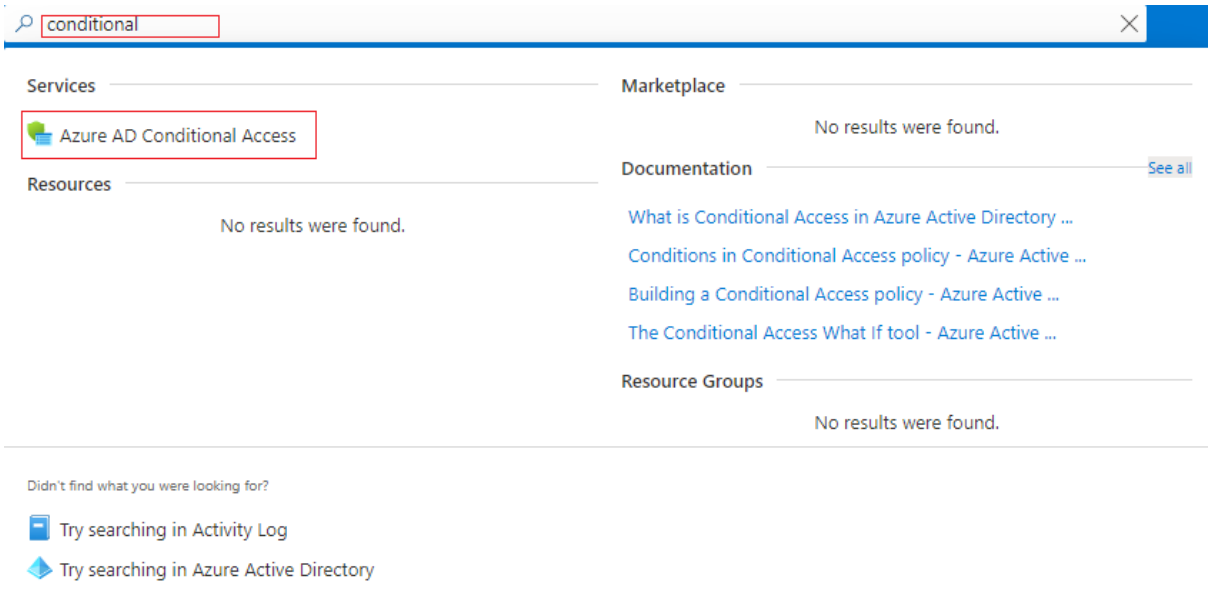
2. Pre-requisites

This lab is part of a series, prior to attempting this lab you must follow the steps in **Lab 1 - Deploying Azure AD for single sign-on to an individual AWS account.** This will help you setup the environment and components required to successfully complete this lab.

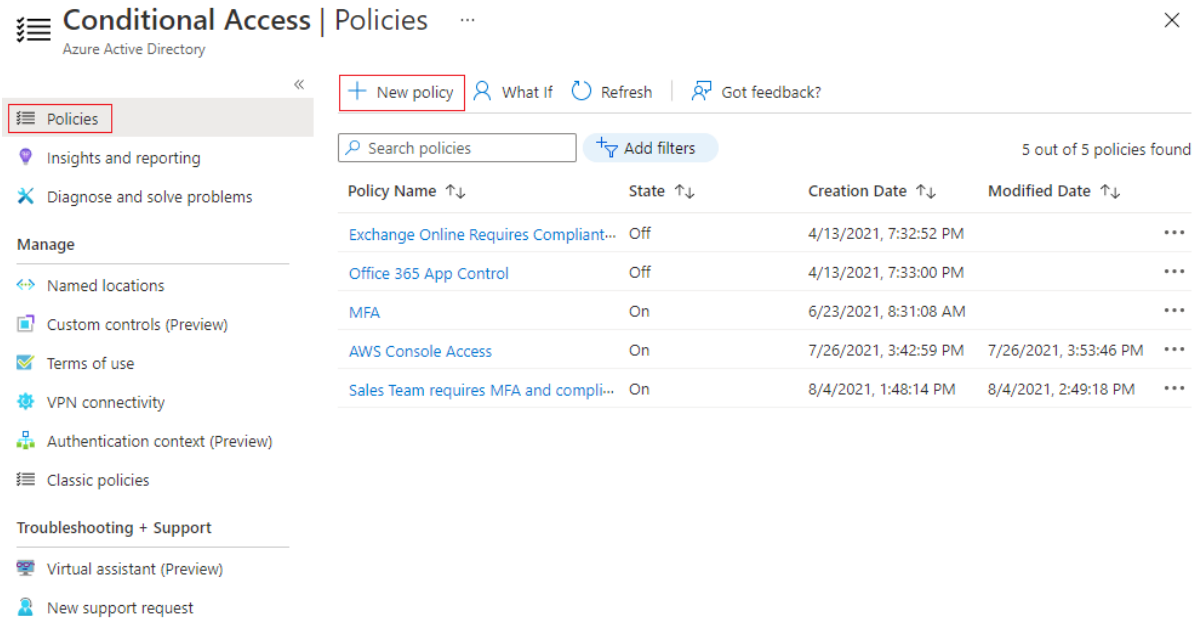
3. Create a Conditional Access Policy for AWS Console application

3.1 Sign in to the **Azure portal** using the admin username and password obtained during the creation of the tenant in **Part 0 - Getting Started - Lab Guide - Securing Multi-vendor Clouds**, **How to create a new M365 Demo Tenant** section.

3.2 In the Azure search box, type **Conditional Access,** select **Azure AD Conditional Access.**

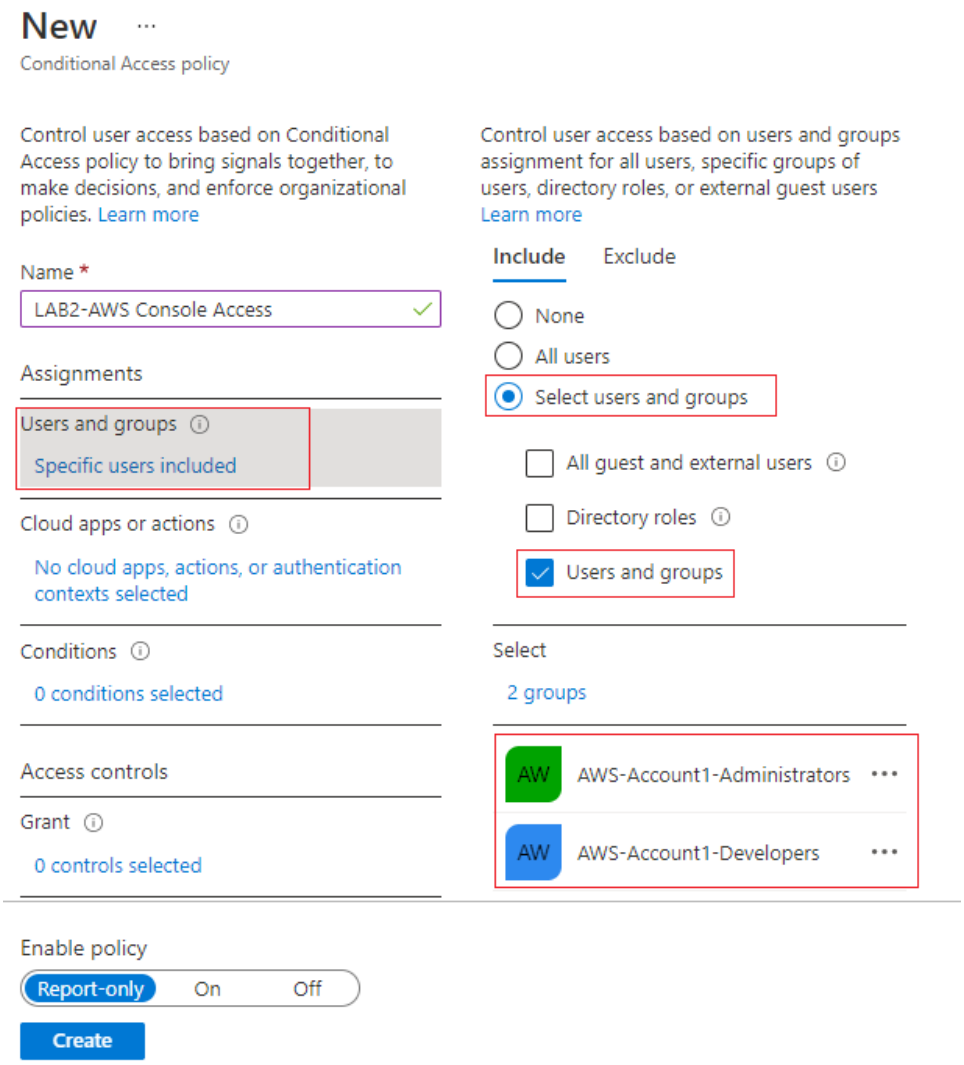


3.3 On the **Conditional Access** page, select **Policies,** then select **New policy.**



3.4 On the **New Policy** page, perform the following steps:

a) Give a descriptive **Name** for the new policy (for example, **LAB2-AWS Console Access**).
b) Select **Users and Groups,** select **Select Users and Groups** box, then select **Users and Groups** box.
c) In the search box, type **AWS-Account1-Administrators** (this is the group you created on **LAB 1 - Deploying Azure AD for single sign-on to an individual AWS account**), click on the group name to select it.
d) In the search box, type **AWS-Account1-Developers** (this is the group you created on **LAB 1 - Deploying Azure AD for single sign-on to an individual AWS account**), click on the group name to select it.
e) Click **Select.**



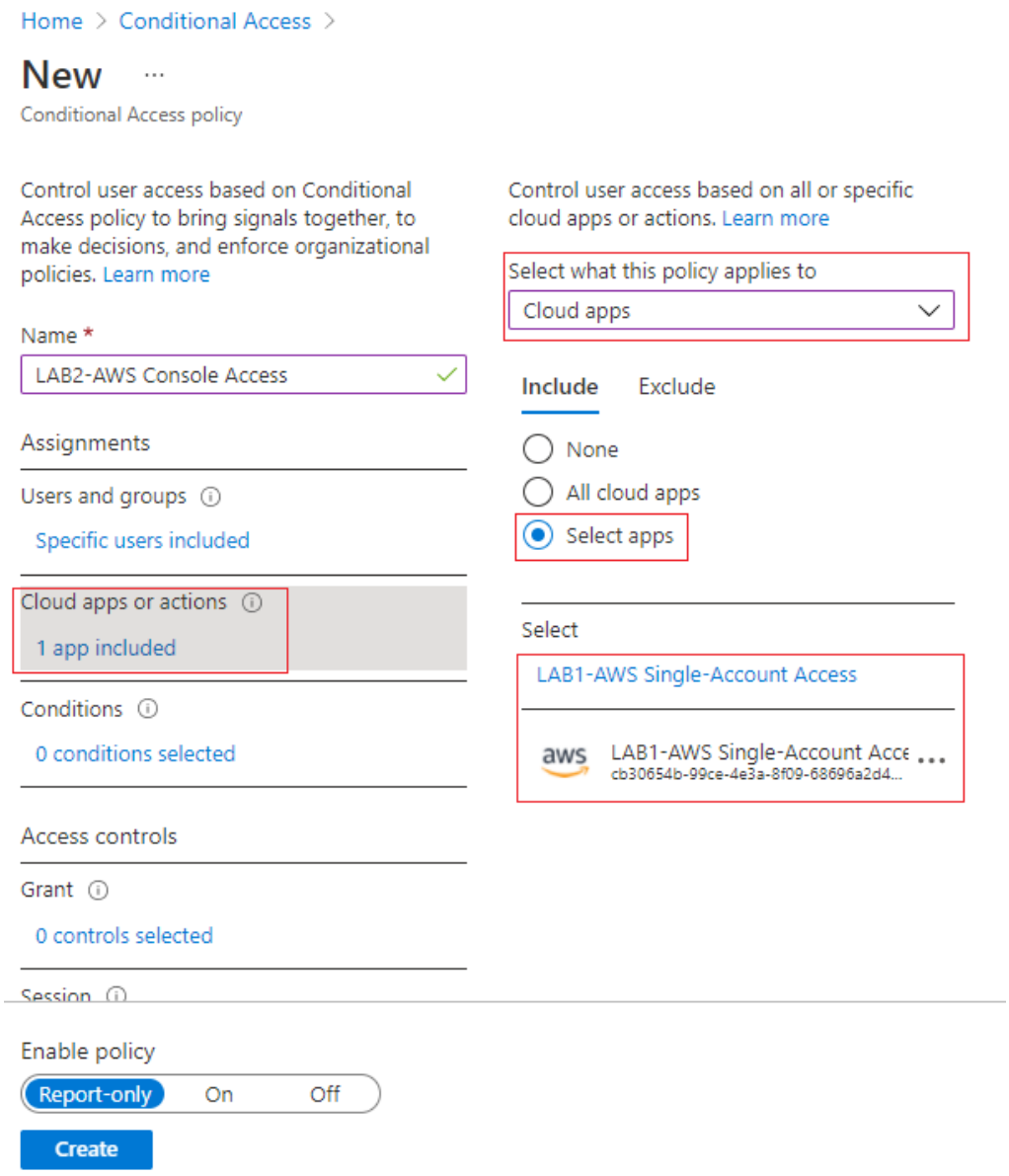
f) In the **Cloud apps or actions** section, select **No cloud apps, actions, or authentication context selected**.

g) In the **Select what this policy applies to** filed, leave the default **Cloud apps**.

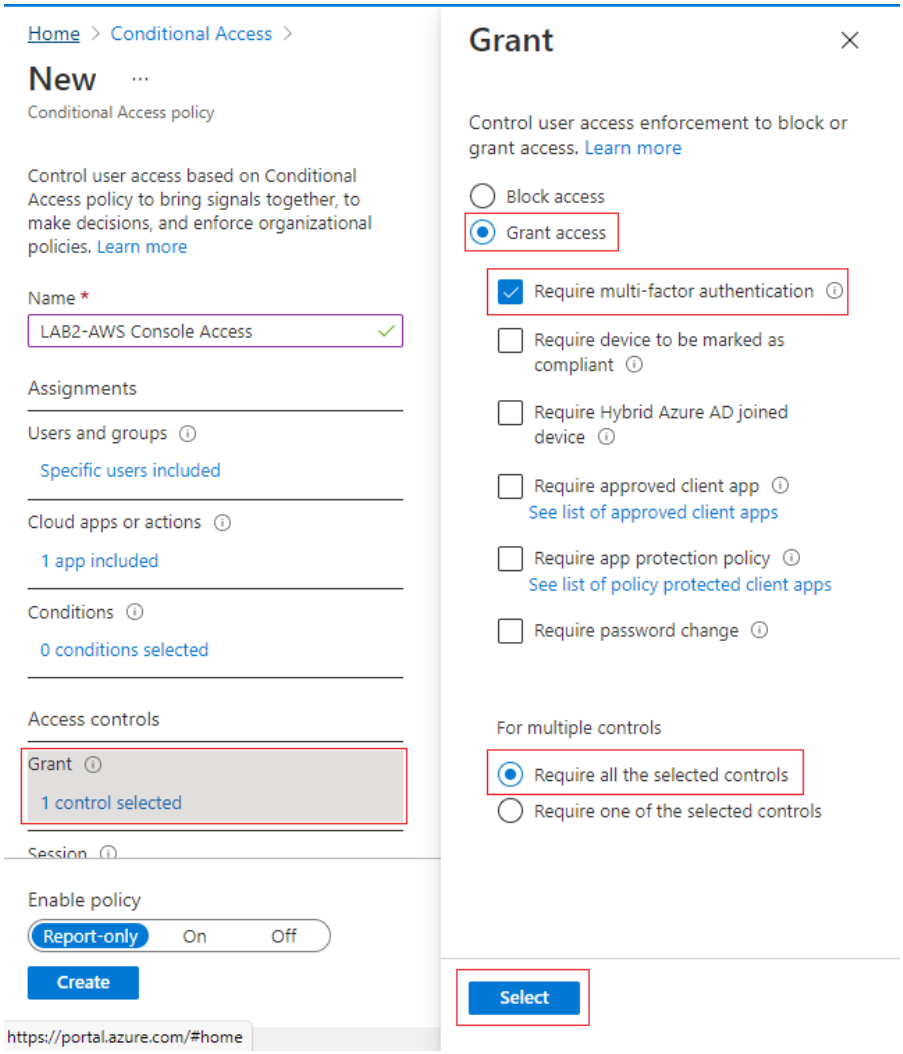
h) Select **Include,** select **Select apps**.

i) Select **None** to select an application.

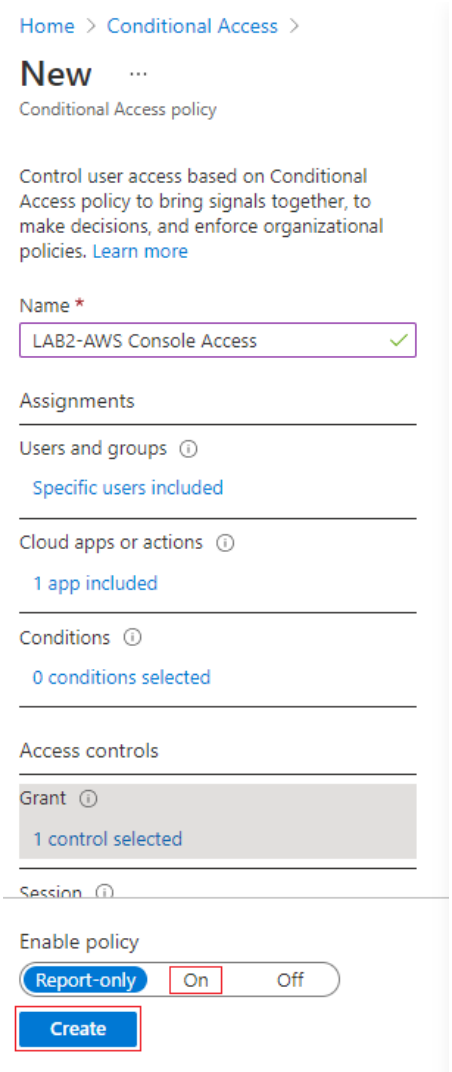
j) In the **Select Cloud apps** search box, type the name of the Enterprise Application you created in **LAB 1 - Deploying Azure AD for single sign-on to an individual AWS account.** Click on the application name and click **Select** at the bottom of the page.



k) In the **Grant** section, select **0 controls selected**.
l) Select **Grant access,** then select **Require multi-factor authentication.**
m) Click **Select** at the bottom of the page.



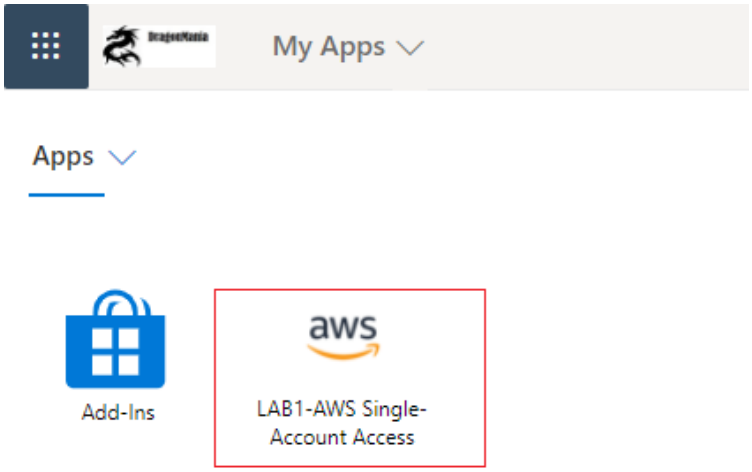
n) On the **New Conditional Access policy page,** under **Enable policy**, select **On**.
o) Select **Create.**



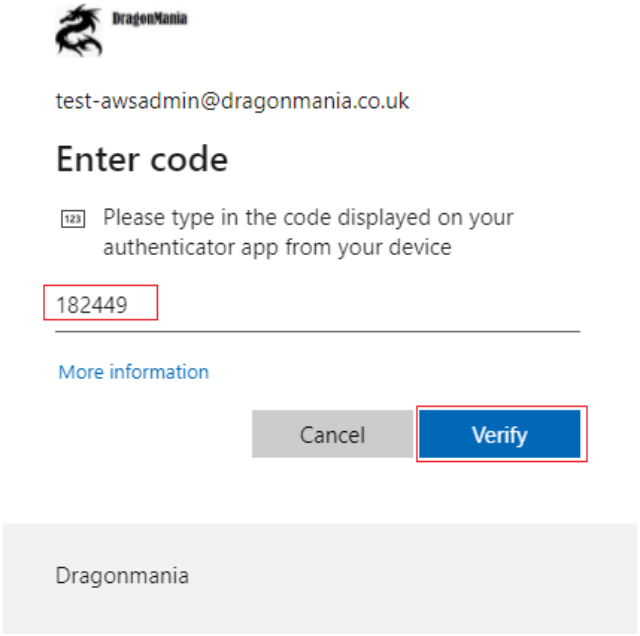
4. Test Sign-in to AWS Console with Multifactor Authentication

*Please note that it may take a few minutes for the changes carried out in section 3 to take effect. You may want to wait 5 minutes after creating the Conditional Access policy before you test it.

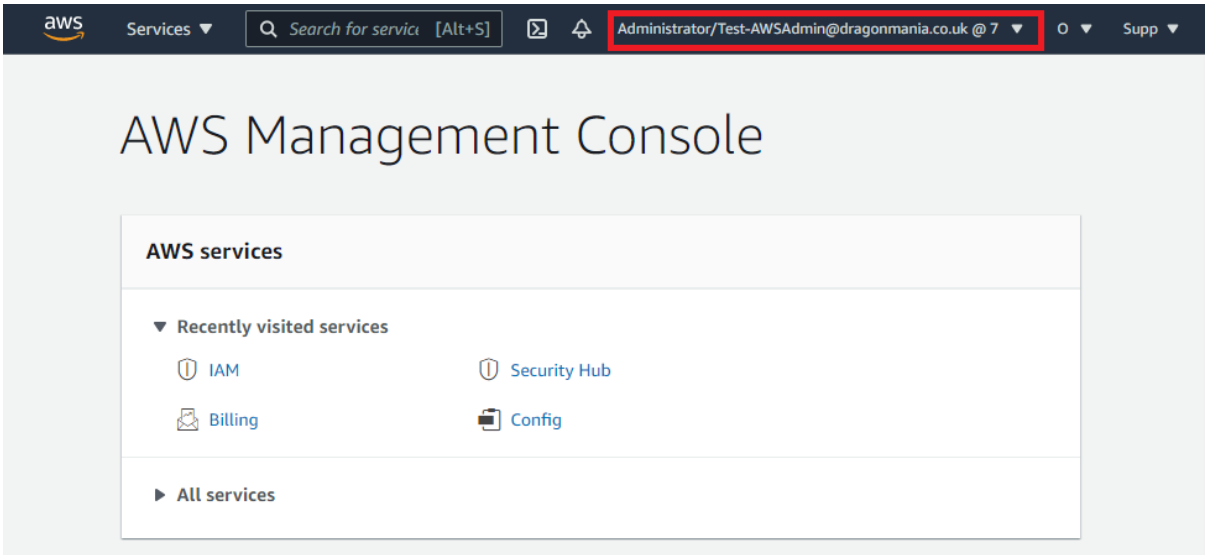
4.1 Open a **New InPrivate** browser window, go to https://myapplications.microsoft.com/
4.2 Log on using the **Test-AWSAdmin** account you created in **LAB1 - Deploying Azure AD for single sign-on to an individual AWS account.**
4.3 If you haven't done so yet, you will be prompted to setup **Microsoft Authenticator,** follow the steps on screen to configure it.
4.4 Select the **Enterprise Application** you created in **LAB1 - Deploying Azure AD for single sign-on to an individual AWS account.**



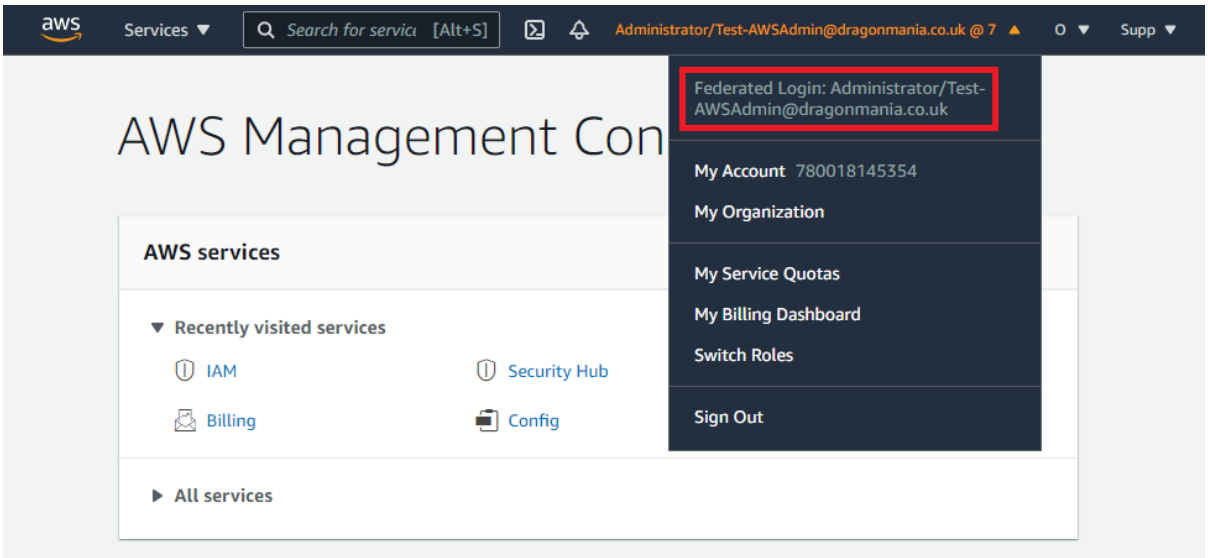
4.5 When prompted, type in the code displayed on your authenticator app from your device, then select **Verify**.



4.6 Once the sign-in is successful, you will be redirected to **AWS Console** as an Administrator.



4.7 If you select the arrow next to the user name to expand it, you will see the user is a federated user. This account is a full admin in AWS according to the role assignments configured in **LAB1 - Deploying Azure AD for single sign-on to an individual AWS account**, so play around and see what you can do (for example, create a new user, create a S3 bucket, etc.)



Congratulations! You have now successfully completed this lab. We hope you found this lab, and the associated lab materials useful. We look forward to seeing what you build as a result of attending this lab!

Lab Complete.