

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	3
2. Pre-requisites	3
3. Create a Conditional Access Policy for AWS Console application.....	3
4. Test Sign-in to AWS Console with Multifactor Authentication.....	8

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.

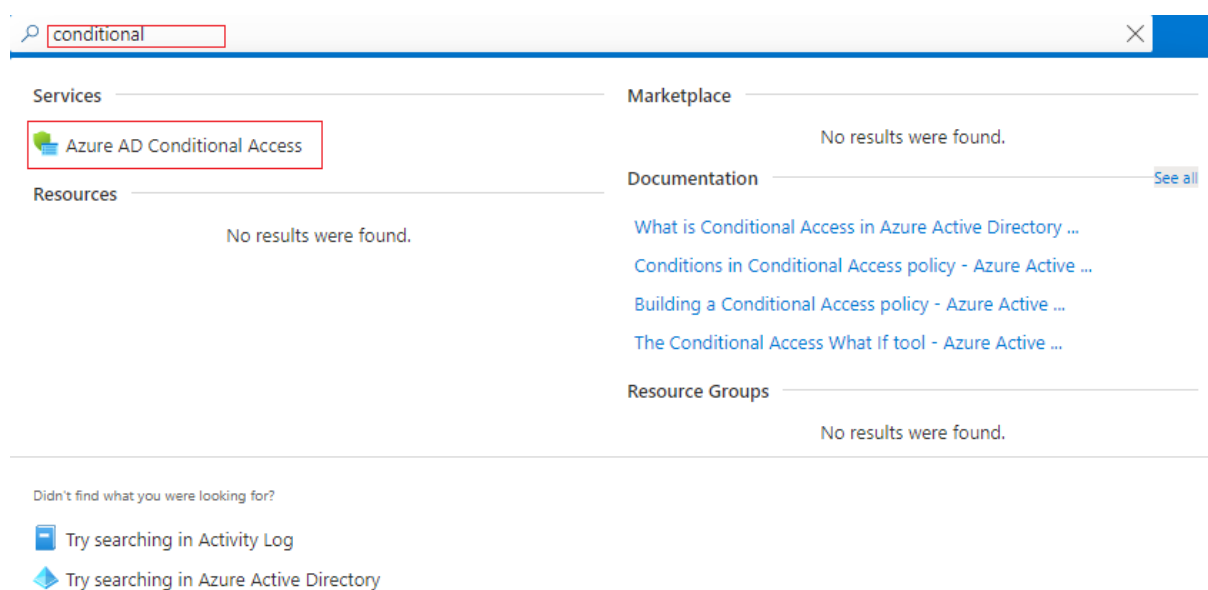
2. Pre-requisites

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**.

Conditional Access | Policies ...

Azure Active Directory

« **+ New policy** What If Refresh Got feedback?

Search policies Add filters 5 out of 5 policies found

Policy Name ↑↓	State ↑↓	Creation Date ↑↓	Modified Date ↑↓
Exchange Online Requires Compliant...	Off	4/13/2021, 7:32:52 PM	...
Office 365 App Control	Off	4/13/2021, 7:33:00 PM	...
MFA	On	6/23/2021, 8:31:08 AM	...
AWS Console Access	On	7/26/2021, 3:42:59 PM	7/26/2021, 3:53:46 PM ...
Sales Team requires MFA and compli...	On	8/4/2021, 1:48:14 PM	8/4/2021, 2:49:18 PM ...

Manage

- Insights and reporting
- Diagnose and solve problems
- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context (Preview)
- Classic policies
- Troubleshooting + Support
- Virtual assistant (Preview)
- New support request

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

- Give a descriptive **Name** for the new policy (for example, **LAB2-AWS Console Access**).
- Select **Users and Groups**, select **Select Users and Groups** box, then select **Users and Groups** box.
- 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.
- 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.
- Click **Select**.

New ...

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

LAB2-AWS Console Access ✓

Assignments

Users and groups ⓘ

Specific users included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users [Learn more](#)

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select

2 groups

AW

AWS-Account1-Administrators ...

AW

AWS-Account1-Developers ...

Enable policy

Report-only

On

Off

Create

- 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.

[Home](#) > [Conditional Access](#) >

New ...

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

LAB2-AWS Console Access ✓

Assignments

Users and groups ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

[0 controls selected](#)

Session ⓘ

Enable policy

Report-only On Off

Create

Control user access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

☐ None

☐ All cloud apps

☒ **Select apps**

Select

[LAB1-AWS Single-Account Access](#)



LAB1-AWS Single-Account Acce ...
cb30654b-99ce-4e3a-8f09-68696a2d4...

- 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.

Home > Conditional Access >

New

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

LAB2-AWS Console Access ✓

Assignments

Users and groups ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[1 app included](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

[1 control selected](#)

Session ⓘ

Enable policy

Report-only On Off

Create

<https://portal.azure.com/#home>

Grant

Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy ⓘ
[See list of policy protected client apps](#)

☐ Require password change ⓘ

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

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

Home > Conditional Access >

New

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

LAB2-AWS Console Access ✓

Assignments

Users and groups ⓘ

Specific users included

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Enable policy

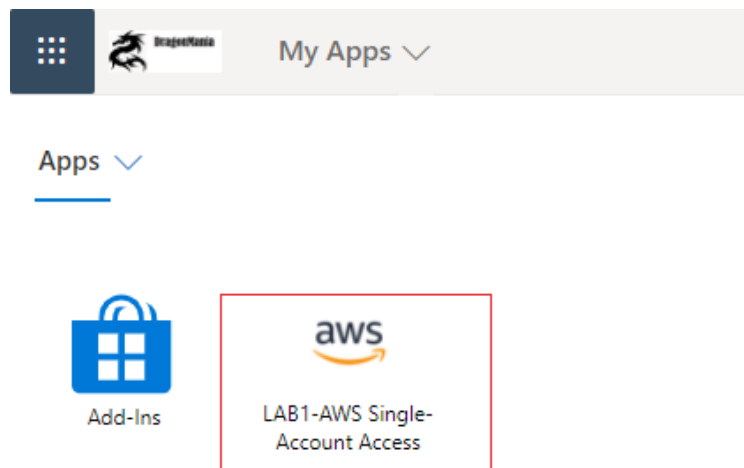
Report-only On Off

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.

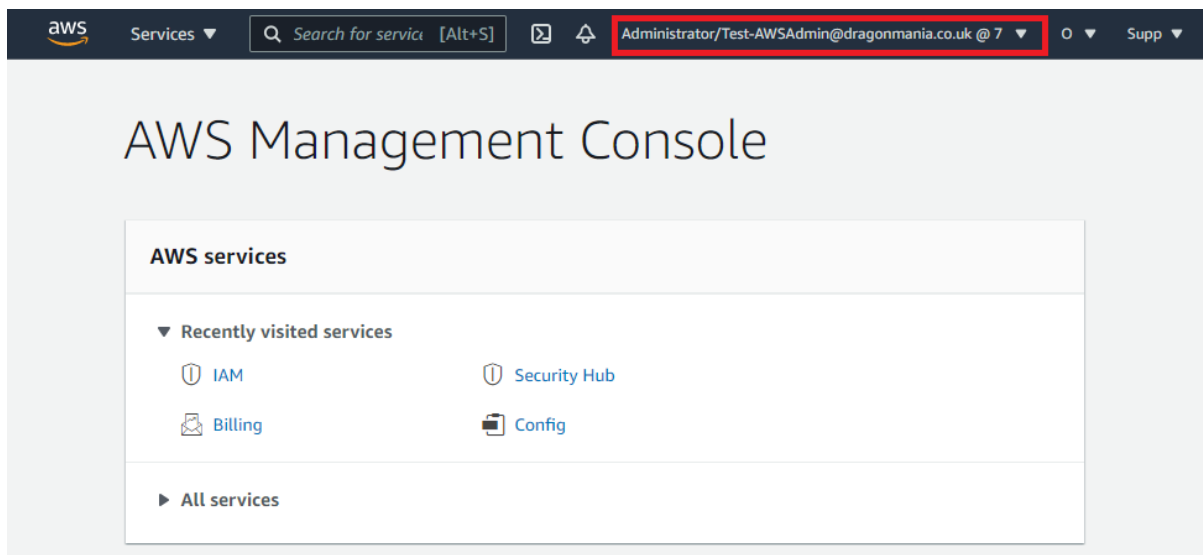
- 4.1 Open a **New InPrivate** browser window, go to <https://myapplications.microsoft.com/>
- 4.2 Log on using the **Test-AWSAdmin** account you created in **LAB1 - Deploying Azure AD for single sign-on to an individual AWS account**.
- 4.3 If you haven't done so yet, you will be prompted to setup **Microsoft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



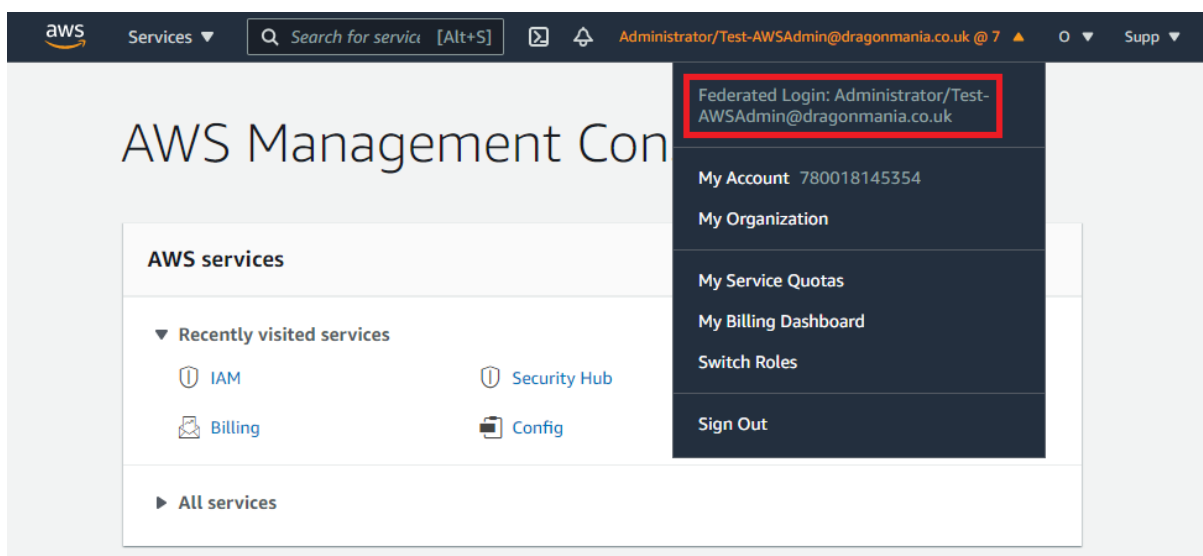
4.5 When prompted, type in the code displayed on your authenticator app from your device, then select **Verify**.

The screenshot shows the login interface of the DragonMania application. At the top is the DragonMania logo. Below it is the email address 'test-awsadmin@dragonmania.co.uk'. The main heading is 'Enter code'. Below this is a prompt: 'Please type in the code displayed on your authenticator app from your device'. A text input field contains the code '182449', which is highlighted with a red rectangular box. Below the input field is a link for 'More information'. At the bottom right are two buttons: 'Cancel' and 'Verify'. The 'Verify' button is highlighted with a red rectangular box. At the very bottom of the page is a grey bar with the text 'Dragonmania'.

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.