



AltorCloud

Back 2 Basics

Cloud Remediation 101 -
AWS Make sure MFA is
enabled for users

Users MFA Enabled

Provider	AWS
Service	IAM
Description	Ensures a multi-factor authentication device is enabled for all users within the account
More Info	User accounts should have an MFA device setup to enable two-factor authentication
AWS Link	<u>http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_ManagingPasswordPolicies.html</u>
Recommended Action	Enable an MFA device for the user account

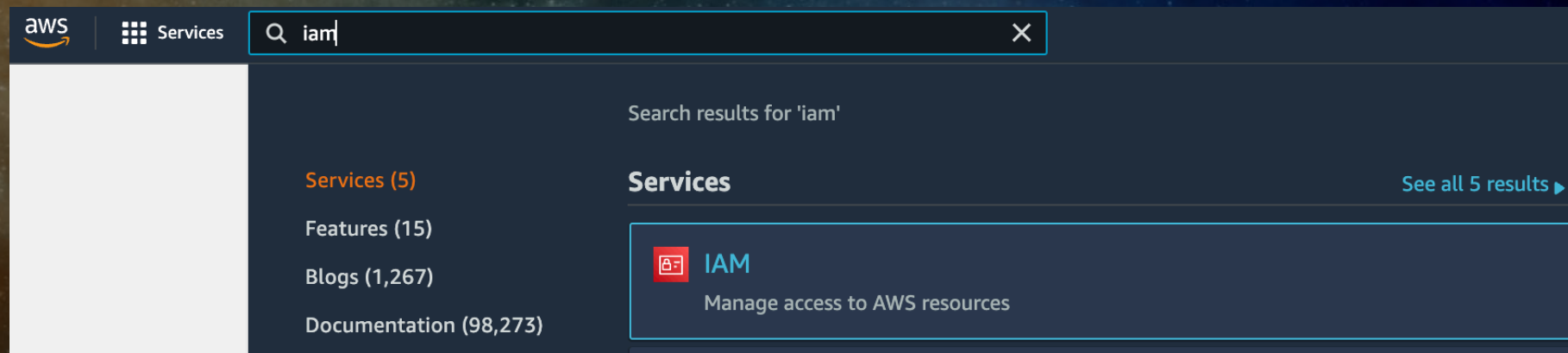


1

Log in to the AWS Management Console.

2

Select the "Services" option and search for IAM.




The screenshot shows the AWS console search interface. At the top left is the AWS logo. Next to it is a 'Services' button with a grid icon. To the right is a search bar containing the text 'iam' and a clear button (X). Below the search bar, the text 'Search results for 'iam'' is displayed. On the left side, there is a list of categories: 'Services (5)', 'Features (15)', 'Blogs (1,267)', and 'Documentation (98,273)'. On the right side, under the heading 'Services', there is a result for 'IAM' with a red icon and the description 'Manage access to AWS resources'. A link 'See all 5 results' is located at the top right of the results section.

aws Services Q iam X

Search results for 'iam'

Services (5)
Features (15)
Blogs (1,267)
Documentation (98,273)

Services See all 5 results ▶

 IAM
Manage access to AWS resources

3

Scroll down the left navigation panel and choose "Users".

Dashboard

▼ **Access management**

User groups

Users

Roles


Policies

Identity providers

Account settings

4

Select the "User" that needs to be verified and click on the "Username" to access the selected "IAM User".



IAM > Users

Users (Selected 1/12) [Info](#) Refresh Delete Add users

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Console last sign-in
<input checked="" type="checkbox"/>	Admin	Administrator	Never	None	10 minutes ago	None



Users > SecondAdmin

Summary

User ARN arn:aws:iam::[redacted]:user/SecondAdmin

Path /

Creation time 2022-02-21 19:03 UTC+0530

Permission **Security credentials** **Access Advisor**

Sign-in credentials

Summary • Console sign-in link: <https://qlicket.signin.aws.amazon.com/console>

Console password Enabled (never signed in) | [Manage](#)

Assigned MFA device Not assigned | [Manage](#)

Signing certificates None

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)


Click on the "Security Credentials" under the configuration page.

Scroll down the "Security Credentials" tab and check the "Assigned MFA device". Check the "Multi-factor authentication (MFA)" section for any active devices. If "Not assigned" is showing against "Assigned MFA device" then a multi-factor authentication device is not enabled for the selected user account.

6



Sign-in credentials

Summary	• Console sign-in link: https://102604287607.signin.aws.amazon.com/console
Console password	Enabled (last signed in 4 days) Manage
Assigned MFA device	Not assigned Manage
Signing certificates	None 



7

Repeat step number
2 - 6 to check other
IAM users.

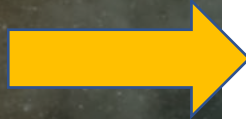




On the "Security Credentials" page, scroll down and click on the "Multi-factor authentication (MFA)," and click on the "Manage" link to enable a multi-factor authentication device.

Summary	• Console sign-in link: https://102604287607.signin.aws.amazon.com/console
Console password	Enabled (last signed in 4 days) Manage
Assigned MFA device	Not assigned Manage 
Signing certificates	None 

Click on the "Virtual MFA device" and click on "Continue".



Manage MFA device ✕

Choose the type of MFA device to assign:

- Virtual MFA device**
Authenticator app installed on your mobile device or computer
- U2F security key**
YubiKey or any other compliant U2F device
- Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)

Cancel Continue

Now install the AWS MFA compatible application on mobile device or computer. Once the application is installed click on the "Show QR code" and scan the code with pre-installed application.

10

Set up virtual MFA device ✕

1. Install a compatible app on your mobile device or computer

See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)



11

Enter two consecutive MFA codes generated from application in "MFA code 1" and "MFA code 2" and click on the "Assign MFA" button.

3. Type two consecutive MFA codes below

MFA code 1

532249

MFA code 2

139397

Cancel

Previous

Assign MFA

12

On successful setup will get the following message "You have successfully assigned virtual MFA".

Set up virtual MFA device



✔ You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.

Close

13

Repeat steps 8 - 12 to enable a multi-factor authentication device for all other IAM users.



Thank You

Please fill out the Contact us form for a free assessment and get a free Security eBook in the process

<https://altorcloud.com/contact/>

-  **Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software**
No Starch Press
-  **Real-World Bug Hunting**
No Starch Press
-  **Malware Data Science: Attack Detection and Attribution**
No Starch Press
-  **Practical Forensic Imaging**
No Starch Press
-  **Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation**
No Starch Press
-  **Pentesting Azure Applications: The Definitive Guide to Testing and Securing Deployments**
No Starch Press
-  **Rootkits and Bootkits**
No Starch Press
-  **Practical IoT Hacking**
No Starch Press
-  **Serious Cryptography: A Practical Introduction to Modern Encryption**
No Starch Press
-  **The Tangled Web: A Guide to Securing Modern Web Applications**
No Starch Press
-  **Black Hat Go**
No Starch Press
-  **The Ghidra Book**
No Starch Press
-  **Ethical Hacking**
No Starch Press
-  **How to Hack Like a Ghost**
No Starch Press
-  **Crypto Dictionary**
No Starch Press
-  **Black Hat Python, 2nd Edition**
No Starch Press
-  **Cyberjutsu**
No Starch Press
-  **Foundations of Information Security**
No Starch Press