

Secure the Application

Configure access controls for restricted course content based on user groups

- An **ACL file** is uploaded and applied to the relevant data source.



Figure 1 View of ACL file

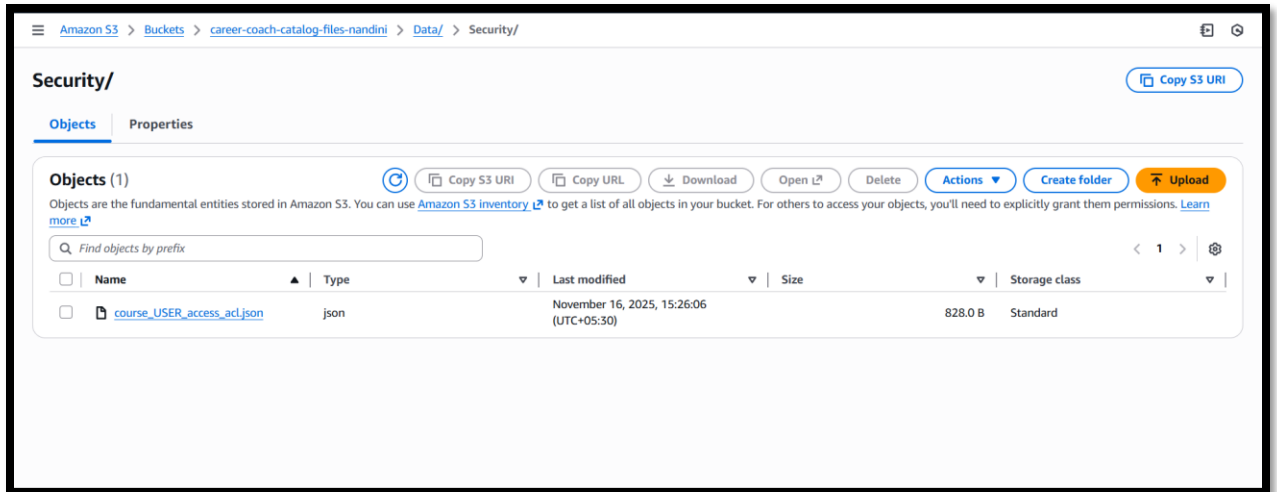


Figure 2 ACL file is uploaded to s3 bucket

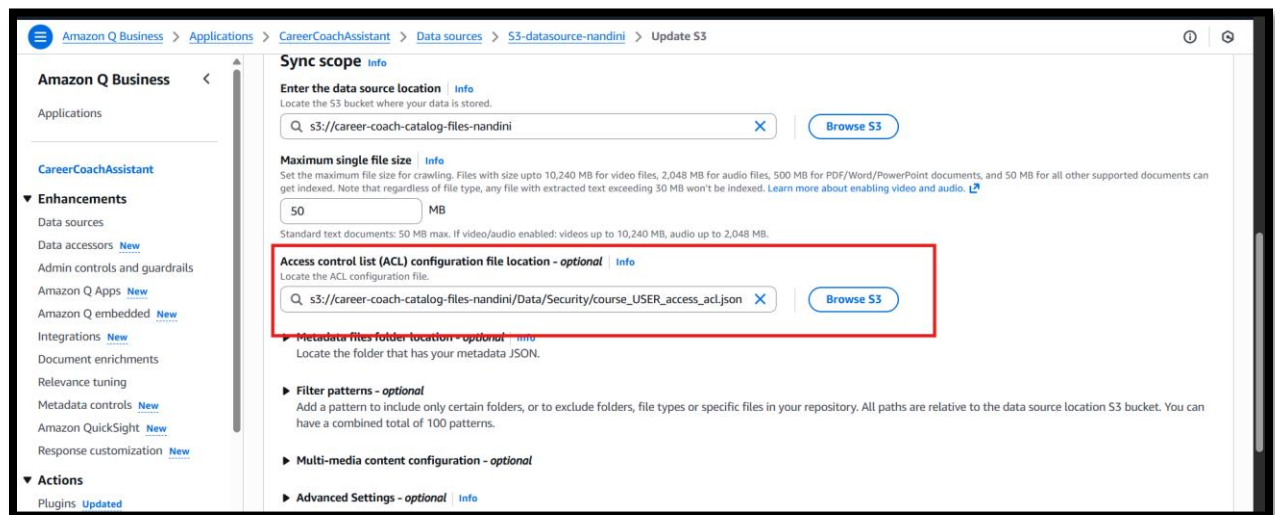


Figure 3 Located the above ACL file in ACL configuration of s3 data source

- Verification shows restricted courses are visible only to approved users.

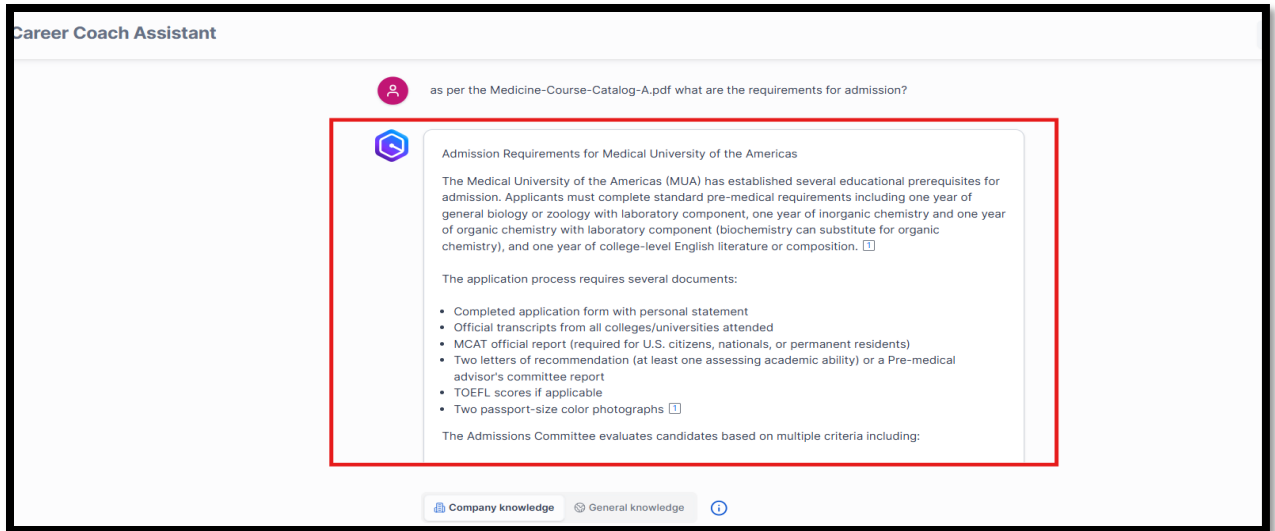


Figure 4 Response of q chat for query when logged in as career.coach.one



Figure 5 verifying answer in pdf document at desktop

Correct Answer found

- Verification shows restricted courses are not accessible to denied users.

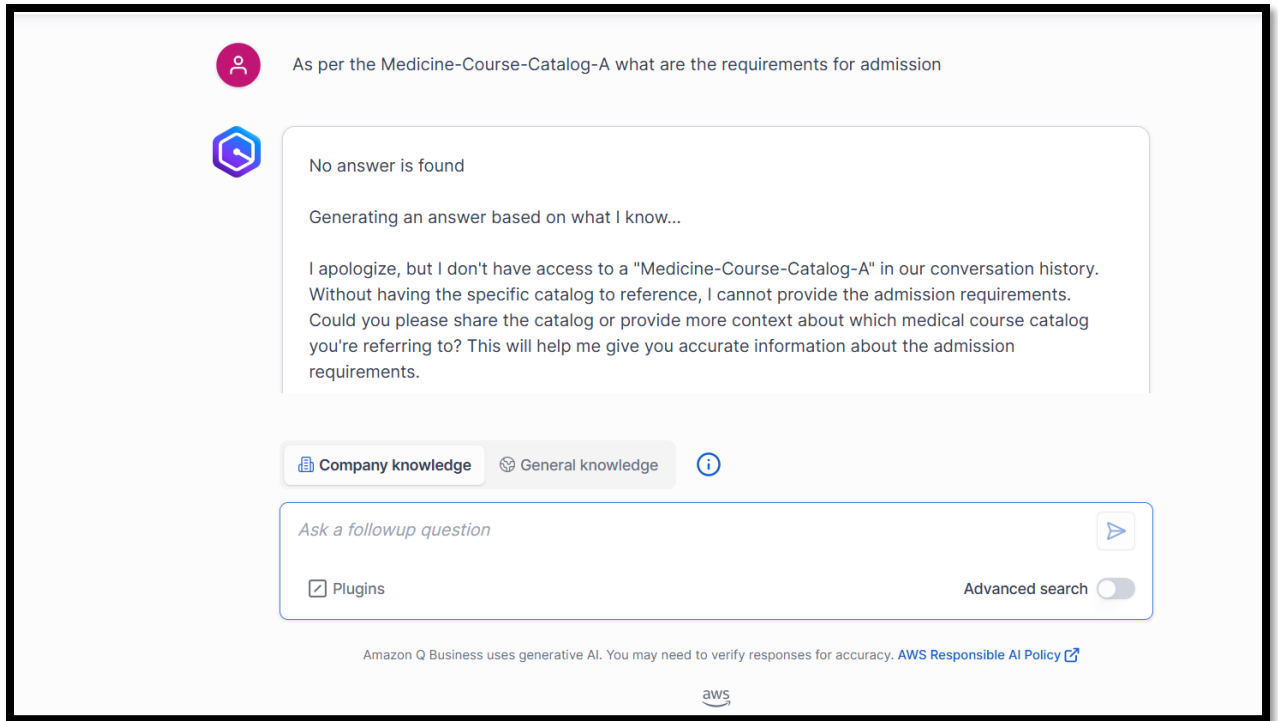


Figure 4 Response for career.coach.two user

- Screenshots of both access success and denied scenarios are included.

[ACL ACCESS DEMO IN WEBAPPLICATION](#)

Please click the above link for the video demo

Implement content moderation by defining restricted keywords.

- A Global Controls list in Amazon Q is configured to block specific keywords (e.g., Gambling, Casino).
- A screenshot of keyword blocking configuration is provided.

The screenshot shows the 'Blocked words' configuration section within the 'Chat orchestration settings' in Amazon Q. The section is titled 'Blocked words' with an 'info' link. Below the title, it states: 'Define blocked words for the application. The application will not mention them in any responses.' There is a text input field labeled 'Enter blocked words' and an 'Add' button. Below the input field, it says 'You can block 15 more words.' At the bottom, there are five buttons with 'X' icons, each representing a blocked word: 'Gambling', 'Casino', 'Self-harm', 'Attack', and 'Hacking'. The entire configuration area is highlighted with a red border. At the bottom right of the settings panel, there are 'Cancel' and 'Save' buttons.

Figure 6 Configuring the Keyword blocking

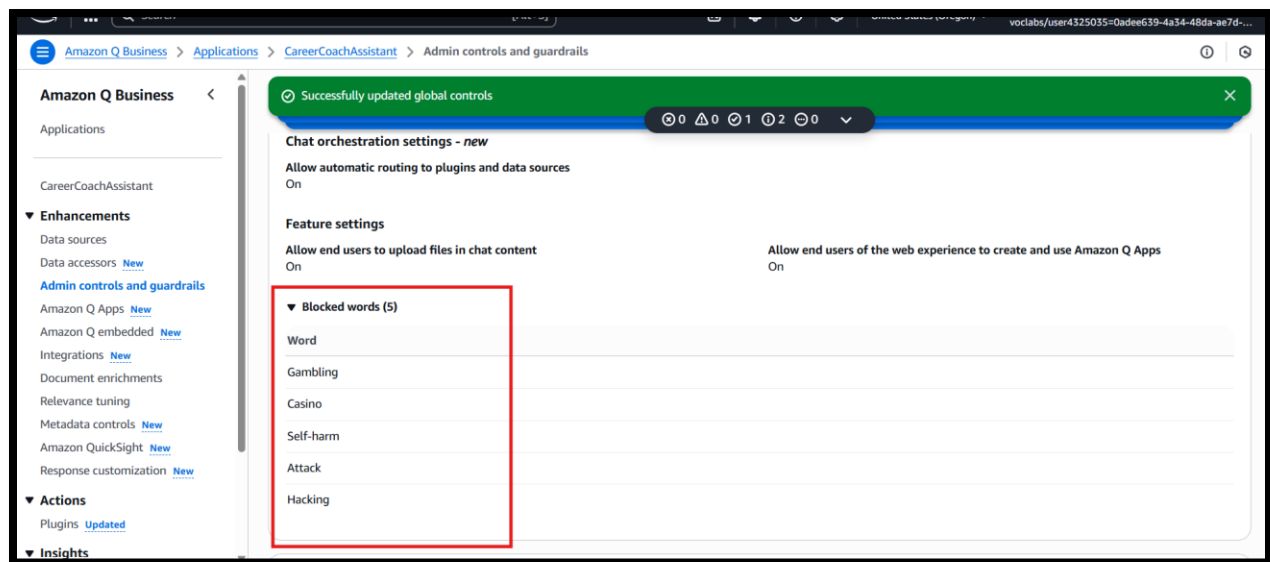


Figure 7 Screenshot of blocked keywords configuration after save