Custom View Settings

Question #5 *Topic 4*

You create a canvas app.
You need to make the app available to other people in your company.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Grant access to individual users in your company.

B. Share the app with a Microsoft Exchange distribution list.

C. Grant access to a Microsoft Teams team.

D. Share the app with a Microsoft Azure Active Directory security group.

Correct Answer: *AD*
After you build a canvas app that addresses a business need, specify which users in your organization can run the app and which can modify and even reshare it.
Specify each user by name, or specify a security group in Azure Active Directory.
Incorrect Answers:
C: You can share an app you've created by embedding it directly into Microsoft Teams. When completed, users can select + to add your app to any of your team channels or conversations in the team you are in. The app appears as a tile under Tabs for your team.
Reference:
https://docs.microsoft.com/en-us/powerapps/maker/canvas-apps/share-app

DRAG DROP -

You create a custom field on the Account entity.

Members of TeamA must have full access to the field. Members of TeamB must have no access to the field.

You need to configure security.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
Add TeamA to the field security profile.	
Create a field security profile and set all the permissions for the custom attribute to **Yes**.	
Add TeamB to the field security profile.	
Create a field security profile and set all the permissions for the custom attribute to **No**.	
Enable field-level security for the field.	

Correct Answer:

Actions	Answer Area
Add TeamA to the field security profile.	Enable field-level security for the field.
Create a field security profile and set all the permissions for the custom attribute to **Yes**.	Create a field security profile and set all the permissions for the custom attribute to **Yes**.
Add TeamB to the field security profile.	Add TeamA to the field security profile.
Create a field security profile and set all the permissions for the custom attribute to **No**.	
Enable field-level security for the field.	

Step 1: Enable field security for the field

Step 2: Create a field security profile and set all the permissions for the custom attribute to Yes.

Step 3: Add TeamA to the field security profile.

Note: Field-level security is available for the default fields on most out-of-box entities, custom fields, and custom fields on custom entities.

Field-level security is managed by the security profiles. To implement field-level security, a system administrator performs the following tasks.

1. Enable field security on one or more fields for a given entity.

2. Associate one more existing security profiles, or create one or more new security profiles to grant the appropriate access to specific users or teams.

HOTSPOT -

A company uses two SQL Server environments and two Common Data Service environments.

The company policy states that only specific administrators can create environments. SQL Server and Common Data Service groups must be distinct.

You need to assign security access.

What should you assign? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Role	Security access
Admin users for SQL environments	Environment Maker Environment Admin System Administrator and Environment Security group Power Platform Administrator and Environment Security group
Admin users for Common Data Service environments	Environment Maker Environment Admin Global Administrator System Administrator
Users that create Common Data Service apps	System Customizer Environment Maker Environment Admin System Administrator
Users that create SQL apps	System Customizer Environment Maker Environment Admin System Administrator

Correct Answer:

Answer Area

Role	Security access
Admin users for SQL environments	Environment Maker Environment Admin **System Administrator and Environment Security group** Power Platform Administrator and Environment Security group
Admin users for Common Data Service environments	Environment Maker **Environment Admin** Global Administrator System Administrator
Users that create Common Data Service apps	System Customizer **Environment Maker** Environment Admin System Administrator
Users that create SQL apps	**System Customizer** Environment Maker Environment Admin System Administrator

Box 1: System Administrator and Environment Security group

Security model for the databases

When a database is created, the users who have environment roles assigned to them, will continue to maintain those privileges.

Users with Environment Admin role are now assigned to System Administrator role. Users with Environment Maker continue to possess the same role.

Question #8 *Topic 4*

You have a Power Platform solution that uses Common Data Service.

You need to secure all fields that support field-level security.

Which field can you secure?

A. createdon

B. accountid

C. owninguser

D. cr7b_accountid

Correct Answer: *D*

Which fields can be secured?

Although most attributes can be secured, there are system attributes, such as IDs, timestamps, and record tracking attributes, that can't. Below are a few examples of attributes that can't be enabled for field security. ownerid, processid, stageid, accountid, contactid createdby, modifiedby, OwningTeam, OwningUser createdon, EntityImage_Timestamp, modifiedon, OnHoldTime, overriddencreatedon statecode, statuscode

Reference:

https://docs.microsoft.com/en-us/power-platform/admin/field-level-security

Previous Questions Next Questions