DUMPSARENA

Microsoft 365 Security Administration

Microsoft MS-500

Version Demo

Total Demo Questions: 20

Total Premium Questions: 638

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 2, New Update	268
Topic 3, Case Study 1	5
Topic 4, Case Study 2	4
Topic 5, Case Study 3	5
Topic 6, Case Study 4	2
Topic 7, Case Study 5	2
Topic 8, Case Study 6	2
Topic 9, Mixed Questions	350
Total	638

QUESTION NO: 1

You need to create a group that will be used to provide limited access to SharePoint resources for users.

Which of the following options are available to you to create the group? (Choose two.)

A. Using the M365 admin center, create an O365 group

B. Using the M365 admin center, create a security group

C. Using the M365 admin center, create a distribution list

D. Using Azure AD admin center, create a security group

E. Using Azure AD admin center, create an O365 group

ANSWER: B D

Explanation:

To control access to resources you must use a security group.

Reference:

https://docs.microsoft.com/en-US/microsoft-365/admin/create-groups/compare-groups?WT.mc_id=365AdminCSH&view=o365-worldwide

QUESTION NO: 2

You have a Microsoft 365 Enterprise E5 subscription.

You use Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). You plan to use Microsoft Office 365 Attack simulator.

What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA)

B. Configure Office 365 Advanced Threat Protection (ATP)

C. Create a Conditional Access App Control policy for accessing Office 365

D. Integrate Office 365 Threat Intelligence and Microsoft Defender ATP

ANSWER: A

Explanation:

Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

QUESTION NO: 3

Which of the following components are required for Azure AD Hybrid Identity with Password Hash Sync? (Choose two.)

A. Azure AD Connect

B. Federation Proxy

C. Federation Server

D. Authentication Agent

E. Active Directory

ANSWER: A E

Explanation:

Reference: https://docs.microsoft.com/en-za/azure/security/fundamentals/choose-ad-authn

QUESTION NO: 4

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user.

You plan to assign the Reports reader role to the user.

You need to view the permissions of the Reports reader role.

Which admin center should you use?

A. Azure Active Directory

B. Cloud App Security

C. Security & Compliance

D. Microsoft 365

ANSWER: A

QUESTION NO: 5

You are configuring a 3rd party DLP solution for your organization. You need to give the DLP system the ability to decrypt any data item that has been protected by a AIP label. You want to solution to be operational immediately.

What should you do? (Choose three.)

A. Run the Enable-AipServiceSuperUserFeature PowerShell cmdlet

B. Run the Add-AipServiceSuperUser PowerShell cmdlet

C. Run the Set-AipServiceSuperUserGroup PowerShell cmdlet

D. Run the New-AzureADUser PowerShell cmdlet

E. Run the Add-AzureADGroupMember PowerShell cmdlet

ANSWER: A B D

Explanation:

Enable the feature; create a user; add the user to the feature

You can also create a group, add the user to the group and assign the group to the feature, but AIP caches group membership and only updates it periodically – it won't be available immediately as is required by the question.

Reference:

https://docs.microsoft.com/en-us/powershell/module/azuread/add-azureadgroupmember?view=azureadps-2.0

QUESTION NO: 6

You create an alert policy as in the exhibit. (Choose all that apply.)

A. User1 copies File1 every 5 minutes. An alert is triggered after 10 minutes.

B. User1 copies File1 every 5 minutes. An alert is triggered after 50 minutes.

C. User1 copies File1 every 5 minutes. An alert is triggered after 60 minutes.

D. Five users all copy File1 every 5 minutes. An alert is triggered after 10 minutes.

E. Five users all copy File1 every 5 minutes. An alert is triggered after 50 minutes.

F. Five users all copy File1 every 5 minutes. An alert is triggered after 60 minutes.

ANSWER: C F

Explanation:

The alert triggers after the threshold is met or exceeded and the window has expired.

View alerts shows how many times the conditions (filter) was met within the window period.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

QUESTION NO: 7

You have an Azure Active Directory (Azure AD) tenant that has a Microsoft 365 subscription.

You recently configured the tenant to require multi-factor authentication (MFA) for risky sign-ins.

You need to review the users who required MFA.

What should you do?

A. From the Microsoft 365 admin center, review a Security & Compliance report

B. From the Security & Compliance admin center, run an audit log search and download the results to a CSV file

C. From the Azure Active Directory admin center, review the Authentication methods activities

D. From the Azure Active Directory admin center, download the sign-ins to a CSV file

ANSWER: D

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting

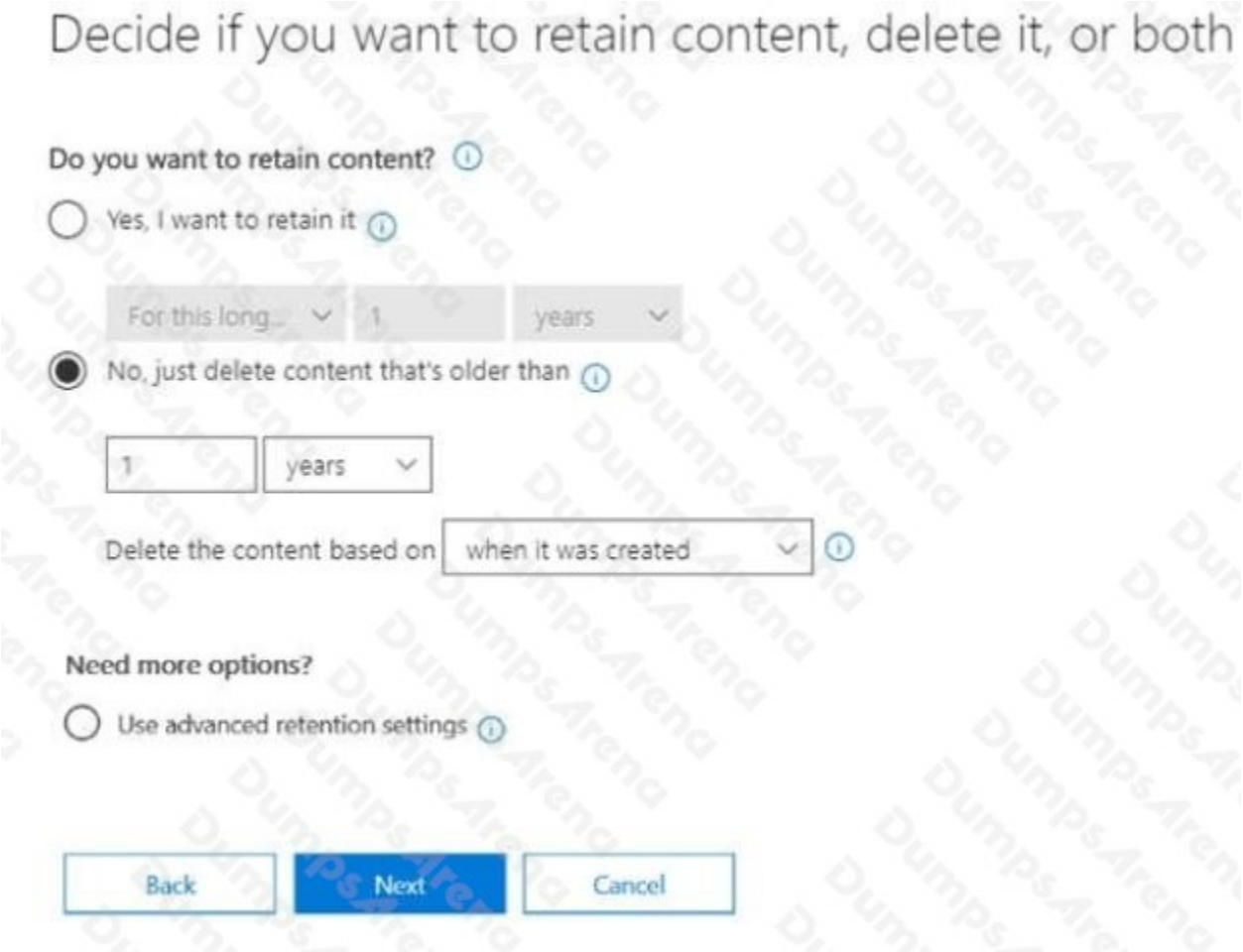
QUESTION NO: 8 - (HOTSPOT)

HOTSPOT

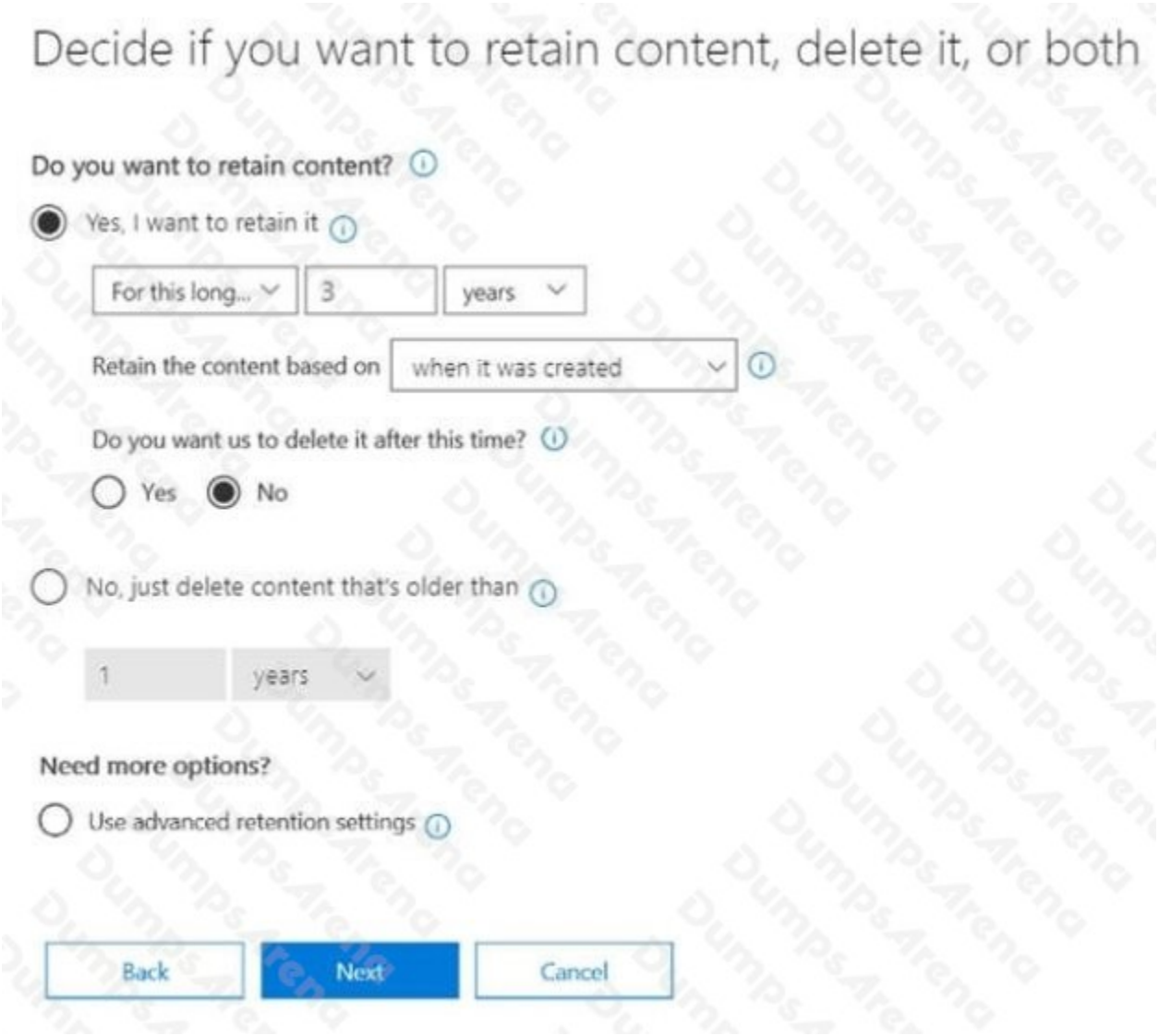
You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.



Policy2 is configured as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Hot Area:

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	○	○
If a user deletes a Microsoft OneDrive file created on January 1,2018, an administrator can recover the file on April 15, 2019	○	○
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	○	○

ANSWER:

Explanation:

Policy2 is in effect as it has the longer retention period.

Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-ofretention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence

QUESTION NO: 9 - (DRAG DROP)

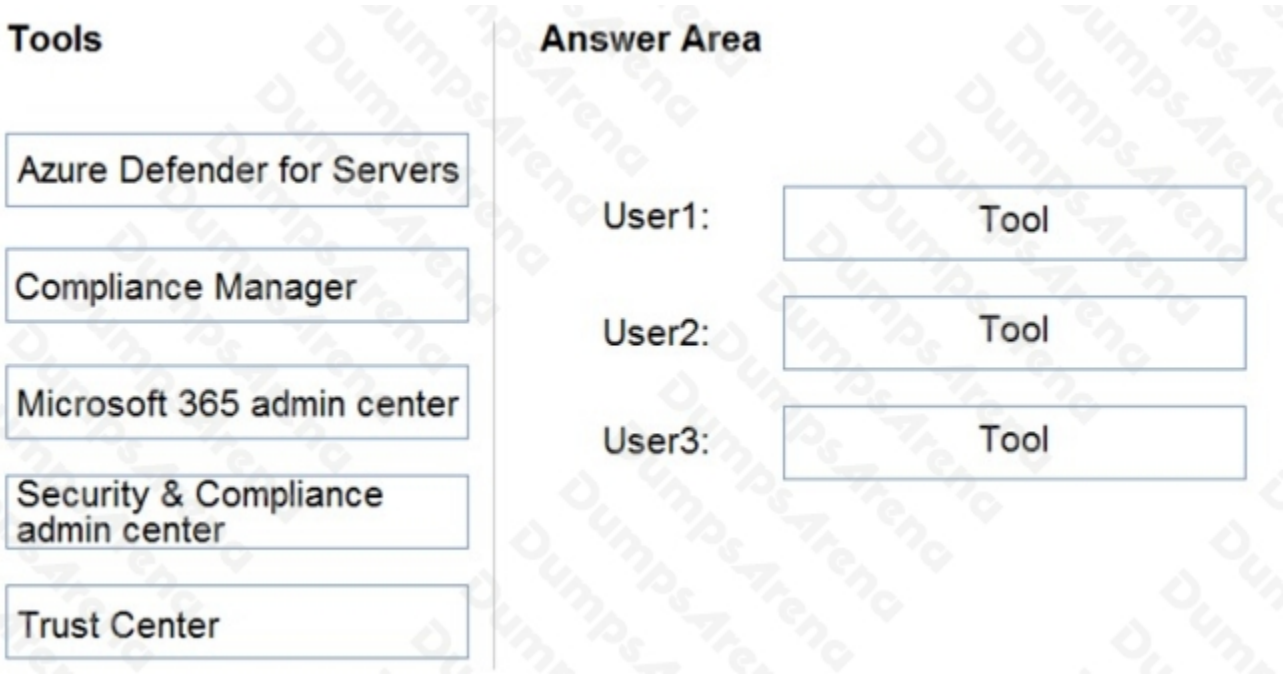
You have a Microsoft 365 E5 tenant that contains three users named User1, User2, and User3.

You need to assign roles or role groups to the users as shown in the following table.

User	Role or role group
User1	SharePoint admin
User2	Data Investigator
User3	User admin

What should you use to assign a role or role group to each user? To answer, drag the appropriate tools to the correct roles or role groups. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



ANSWER:

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

QUESTION NO: 10 - (SIMULATION)

SIMULATION

You need to ensure that a user named Allan Deyoung uses multi-factor authentication (MFA) for all authentication requests.

To complete this task, sign in to the Microsoft 365 admin center.

ANSWER: See explanation below.

Explanation:

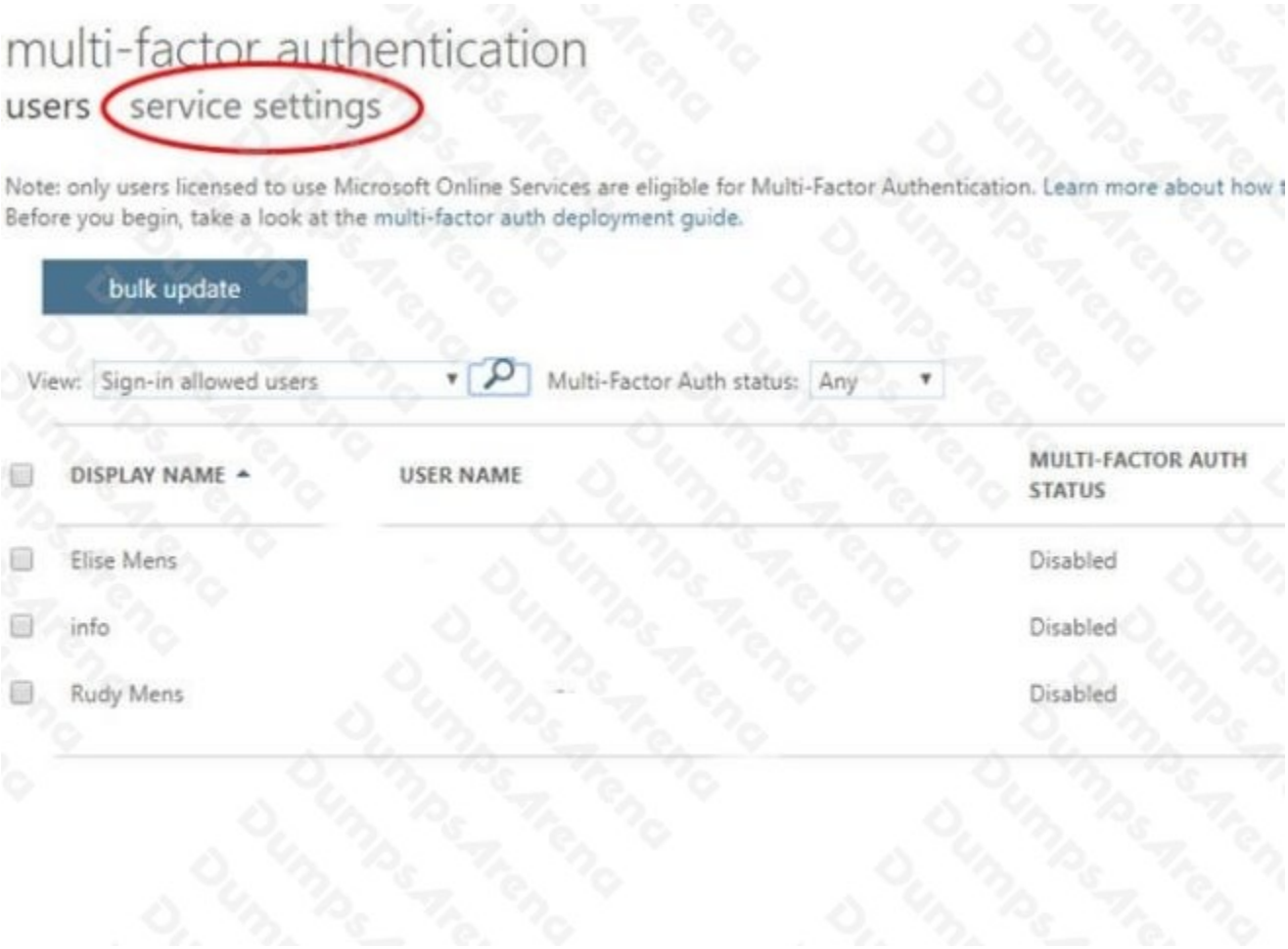
1. Open the Admin Center and go to Users > Active Users

2. Open Multi-factor authentication

Don’t select any user yet, just open the Multi-factor authentication screen. You will find the button in the toolbar.

3. Open the Service settings

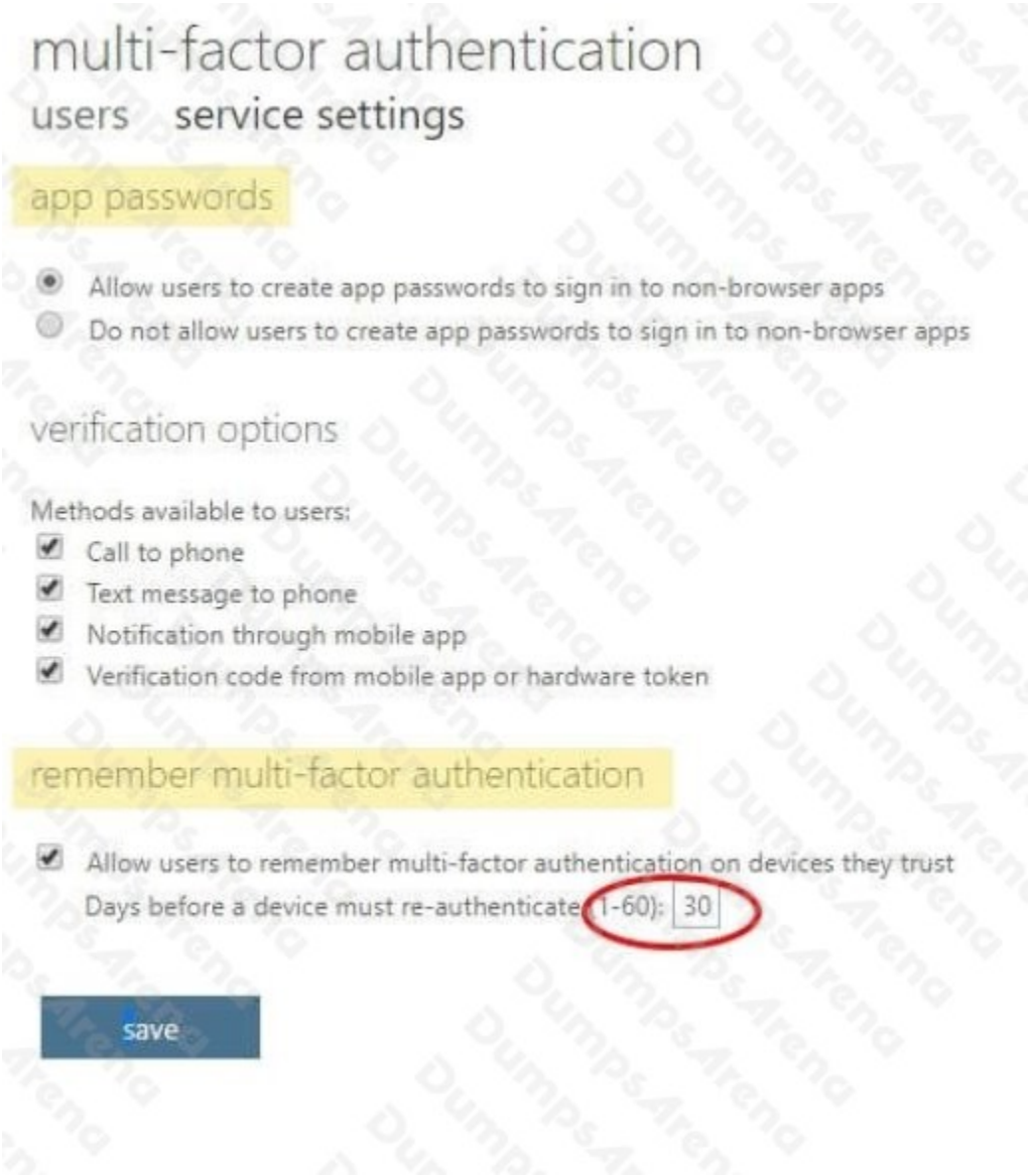
Before we start enabling MFA for the users, we first go through the service settings. The button to the settings screen doesn't stand out, but it's just below the title



4. Setup MFA Office 365

A few settings are important here:

▪ Make sure you check the App password. Otherwise, users can't authenticate in some applications (like the default mail app in Android). ▪ Also, take a look at the remember function. By default, it is set to 14 days.

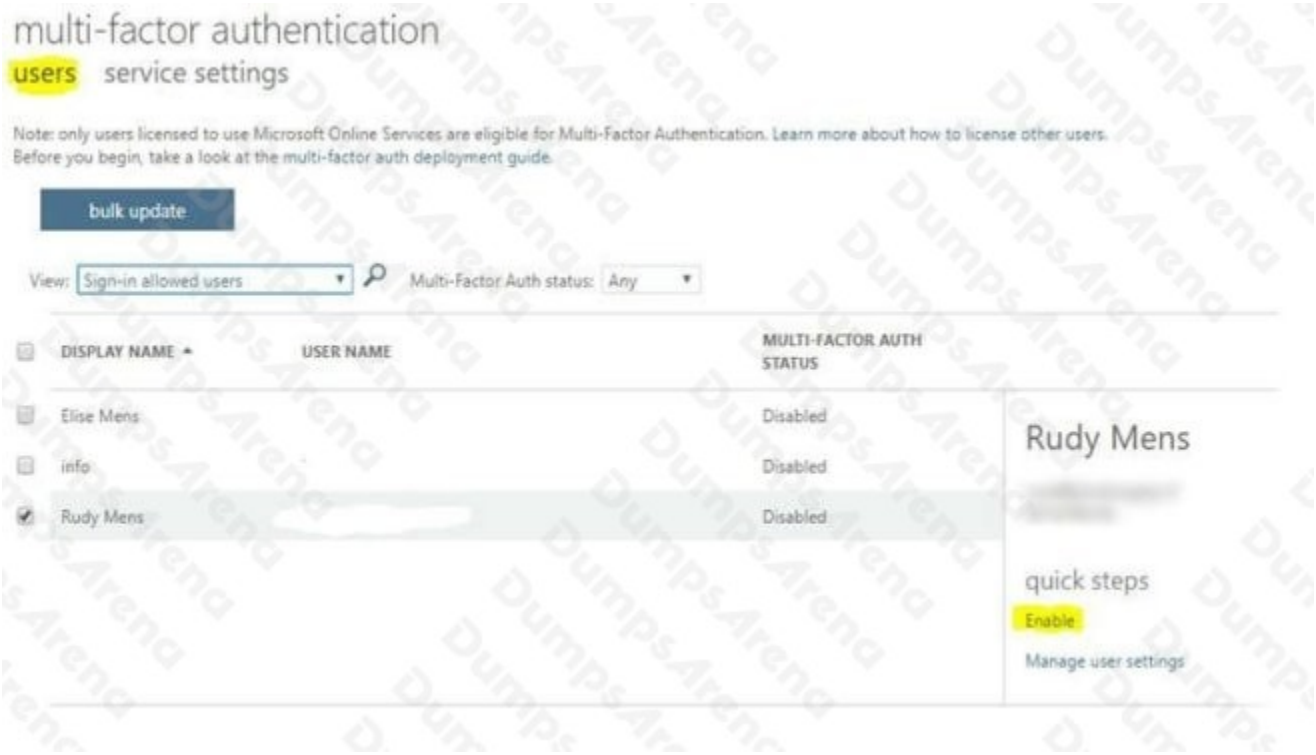


5. Enable MFA for Office 365 users

After you have set the settings to your liking click on save and then on users (just below the title Multi-factor authentication).

You see the list of your users again. Here you can select single or multiple users to enable MFA.

At the moment you enable Office 365 MFA for a user it can get the setup screen as soon as the users browse to one of the Office 365 products.



Reference:

https://lazyadmin.nl/office-365/how-to-setup-mfa-in-office-365/

QUESTION NO: 11 - (DRAG DROP)

DRAG DROP

You have a Microsoft 365 E5 subscription.

All computers run Windows 10 and are onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You create a Microsoft Defender ATP machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

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:

ANSWER:

Explanation:

QUESTION NO: 12

You are receiving email messages with "Unhealthy Identity Synchronization Notification" in the subject line.

Which of the following tools would you use to investigate this issue by first reviewing the DirSync status?

A. IdFix

B. Office 354 Admin Center

C. Azure AD Connect wizard

D. Active Directory Users and Computers

E. Azure portal

ANSWER: B

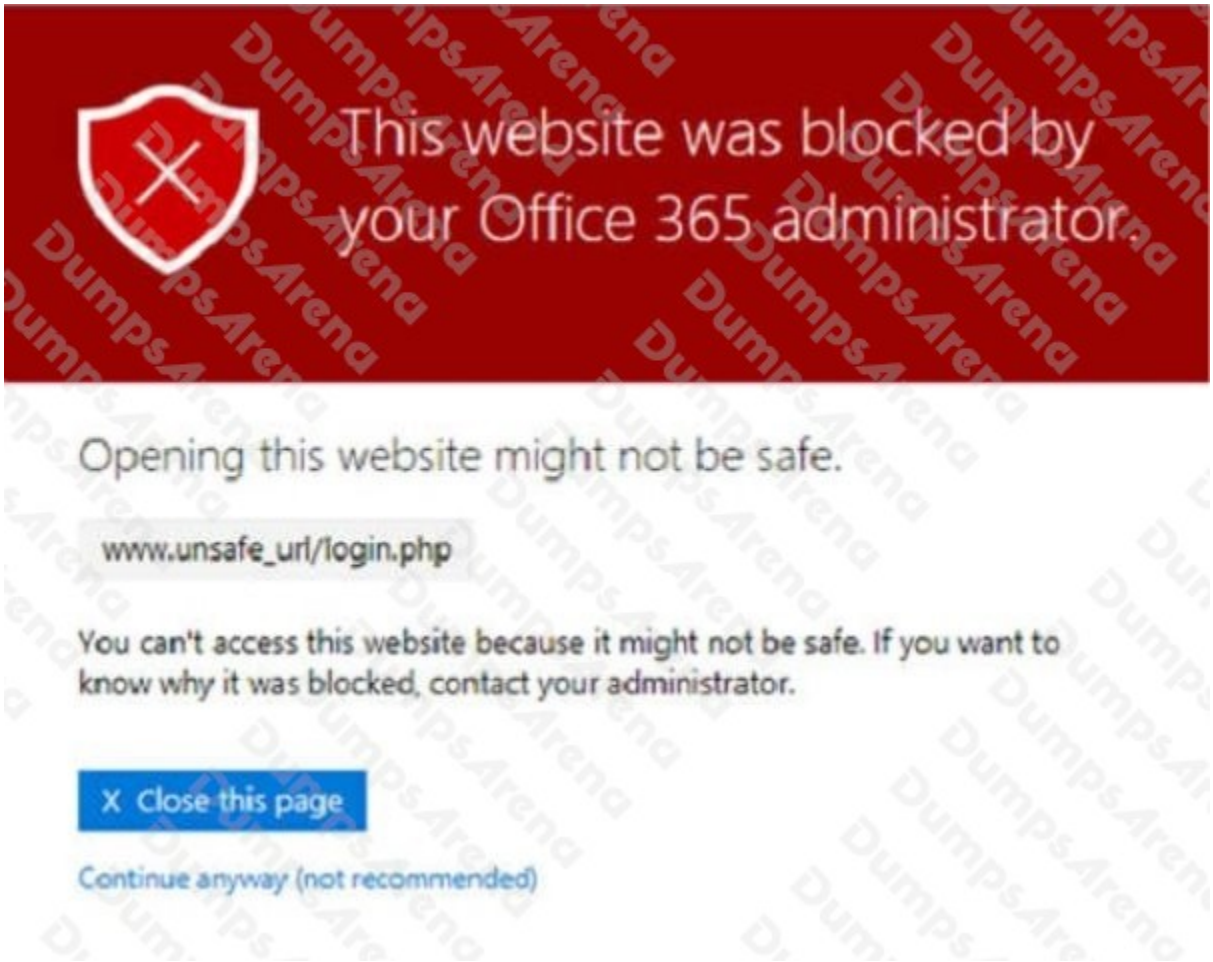
Explanation:

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/identify-directory-synchronization-errors

QUESTION NO: 13

A user phones to complain that his browser is not allowing him to visit a URL that is normally used for business saying that "This website was blocked by your Office 365 administrator." as in the exhibit.



You know that your M365 security policies was recently updated.

Where would you start your investigation?

A. Microsoft Defender ATP

B. Azure ATP

C. Office ATP

D. Microsoft Secure Score

ANSWER: C

Explanation:

URL blocking is part of O365 ATP Safe Links

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links-warning-pages

QUESTION NO: 14

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Office 365 enabled.

You need to review the zero-hour auto purge (ZAP) configuration for the subscription.

Which two threat policies should you review? Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point,

A. Safe links Built-in protection (Microsoft)

B. Office365 AntiPhish Default (Default)

C. Anti-spam outbound policy (Default)

D. Anti-malware (Default) Default

E. Anti-spam inbound policy

F. Safe attachments Built-in protection (Microsoft)

ANSWER: C D

QUESTION NO: 15

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a

Microsoft Office 365 connector.

You need to assign built-in role-based access control (RBAC) roles to achieve the following tasks:

Create and run playbooks.

Manage incidents.

The solution must use the principle of least privilege.

Which two roles should you assign? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Automation Operator

B. Azure Sentinel responder

C. Automation Runbook Operator

D. Azure Sentinel contributor

E. Logic App contributor

ANSWER: D E

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/roles

QUESTION NO: 16

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response(s) to the question or statement below. Each answer is worth one point.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your organization uses SharePoint Online to share files with internal team members as well as occasionally share files with external users. Your CISO is concerned that users in the Retail department is could potentially share files that contain credit card numbers with external recipients from their SharePoint online site. You are tasked to remove external sharing for files where this is already happening, and also prevent it from happening in future. You decide to use Microsoft Cloud App Security to accomplish the task.

Which section of the policy would you use to configure only files that contain credit card numbers should be matched with this policy?

A. Create a filter

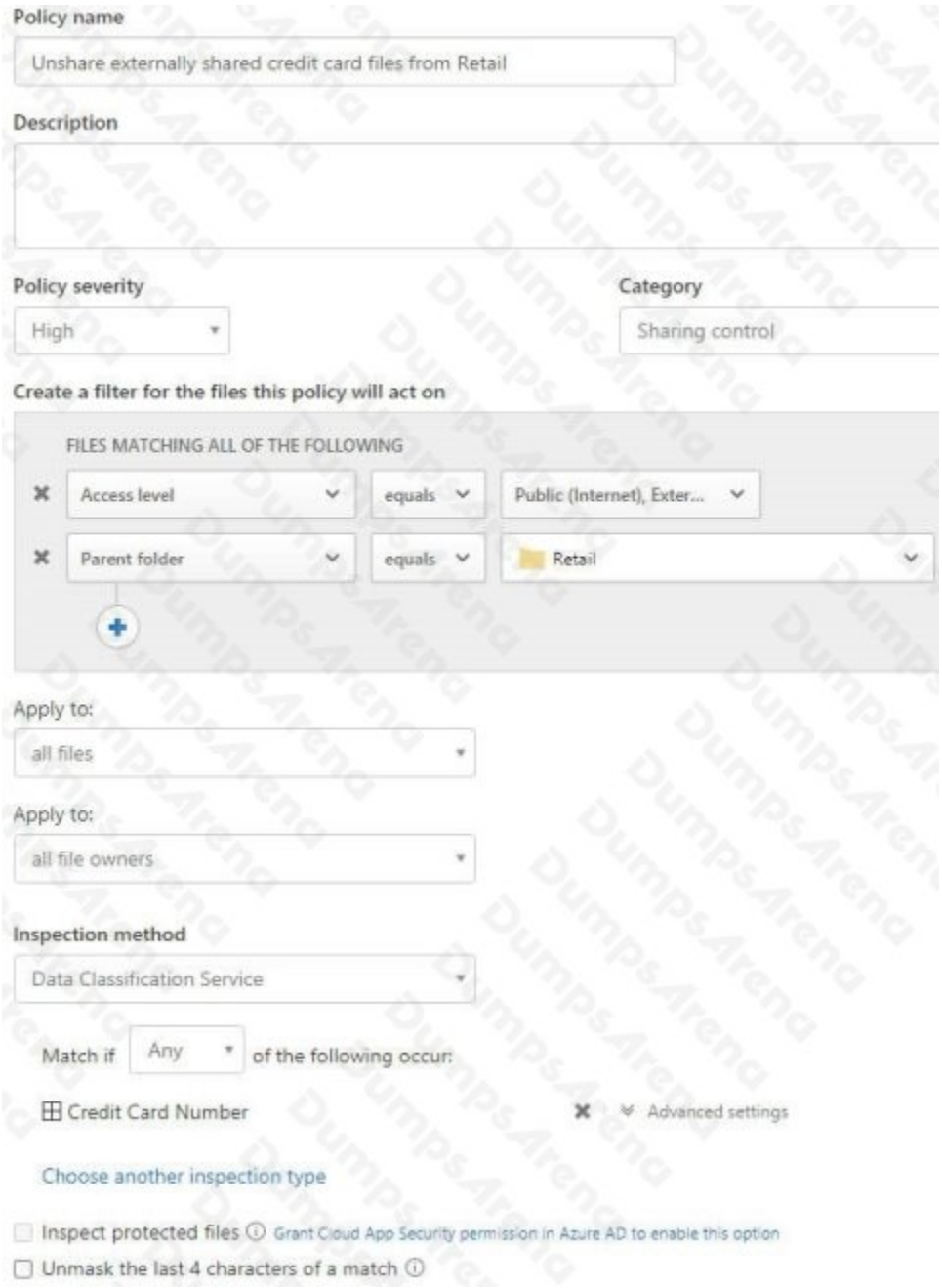
B. Apply to

C. Inspection method

D. Governance actions

ANSWER: C

Explanation:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies

QUESTION NO: 17 - (SIMULATION)

SIMULATION

You need to ensure that all users must change their password every 100 days.

To complete this task, sign in to the Microsoft 365 portal.

ANSWER: See explanation below.

Explanation:

You need to configure the Password Expiration Policy.

1. Sign in to the Microsoft 365 Admin Center.

2. In the left navigation pane, expand the Settings section then select the Settings option.

3. Click on Security and Privacy.

4. Select the Password Expiration Policy.

5. Ensure that the checkbox labelled Set user passwords to expire after a number of days is ticked.

6. Enter 100 in the Days before passwords expire field.

7. Click Save changes to save the changes.

QUESTION NO: 18 - (HOTSPOT)

HOTSPOT

You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain EU Social Security Numbers (SSN) or Equivalent ID.

- Prevent any email messages that contain credit card numbers from being sent outside your organization.

- Block the external sharing of Microsoft OneDrive content that contains EU passport numbers. - Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

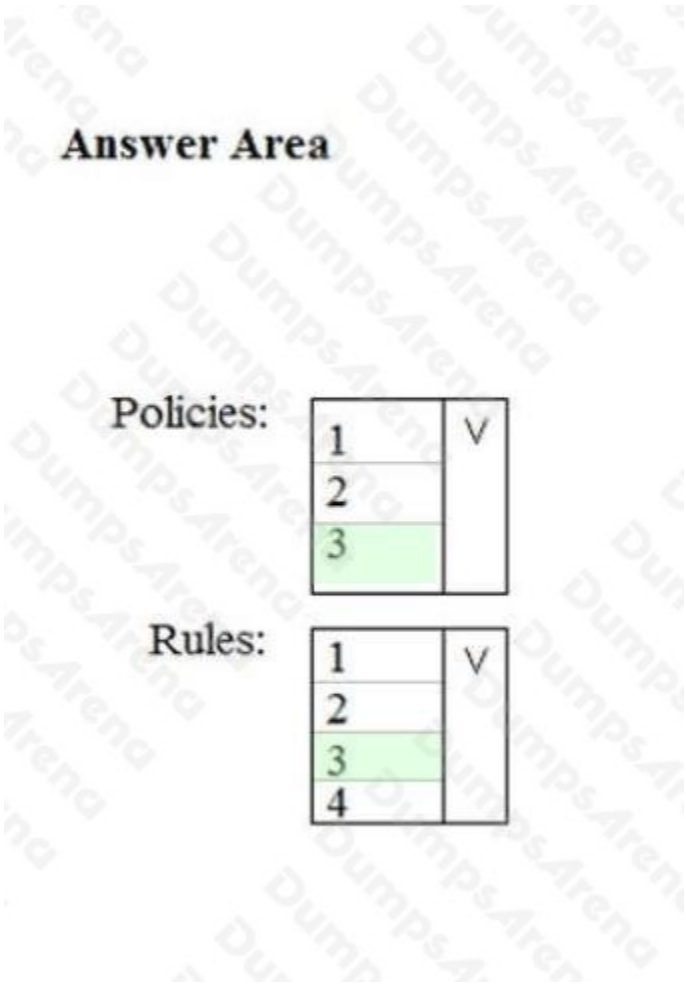
Policies:

1	V
2	
3	

Rules:

1	V
2	
3	
4	

ANSWER:



Explanation:

QUESTION NO: 19

You are using Attack Surface Reduction (ASR) in Microsoft 365 security center to help reduce your Windows 10 attack surfaces.

Which of the following is a prerequisite requirement for deploying ASR to Windows 10 devices?

A. Intune

B. Configuration Manager

C. Defender ATP

D. M365 license assignment

E. Device Guard

ANSWER: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/learn/modules/m365-security-management-endpoints/attack-surface-reduction

QUESTION NO: 20

You need to create Group3.

What are two possible ways to create the group?

A. a Microsoft 365 group in the Microsoft 365 admin center

B. a mail-enabled security group in the Microsoft 365 admin center

C. a security group in the Microsoft 365 admin center

D. a distribution list in the Microsoft 365 admin center

E. a security group in the Azure AD admin center

ANSWER: A D