
**Vendor:** Microsoft

**Exam Code:** MS-500

**Exam Name:** Microsoft 365 Security Administration

**Version:** DEMO

**QUESTION 1**
**Case Study 1 - Fabrikam, Inc**
**Overview**
Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

**Existing Environment**
**Network Infrastructure**
The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

**Problem Statements**
Fabrikam identifies the following issues:
- Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.
- Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

**Requirements**
**Planned Changes**
Fabrikam plans to implement the following changes:
- Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory
- Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

**Application Administration**
Fabrikam identifies the following application requirements for managing workload applications:
- User administrators will work from different countries
- User administrators will use the Azure Active Directory admin center
- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

**Security Requirements**
Fabrikam identifies the following security requirements:
- Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
- Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
- Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
- The location of the user administrators must be audited when the administrators authenticate to Azure AD Email messages that include attachments containing malware must be delivered without the attachment
- The principle of least privilege must be used whenever possible

Hotspot Question

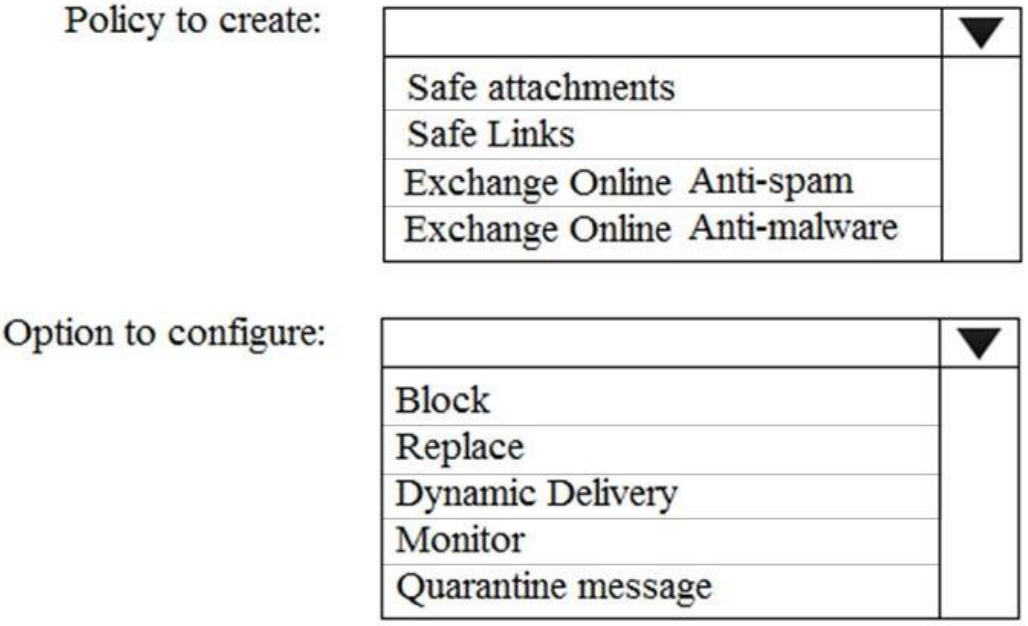
You need to recommend an email antimalware solution that meets the security requirements.

What should you include in the recommendation? To answer, select the appropriate options in

the answer area.

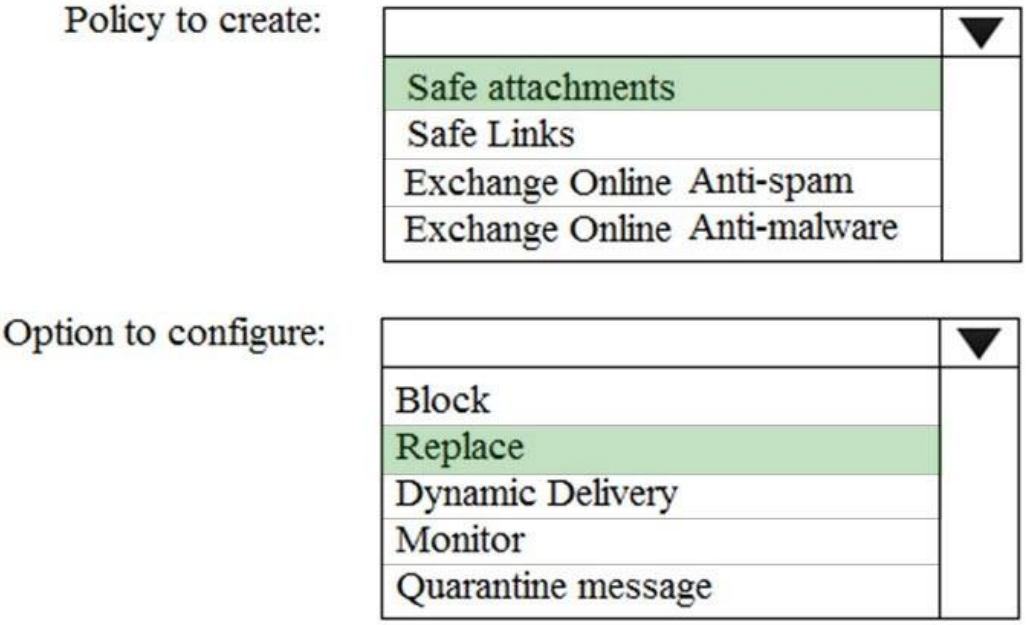
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**

**Answer Area**



**Explanation:**
Block Prevents messages with detected malware attachments from proceeding.
Sends messages with detected malware to quarantine in Office 365 where a security administrator or analyst can review and release (or delete) those messages.
Blocks future messages and attachments automatically Safeguard your organization from repeated attacks using the same malware attachments.
Replace Removes detected malware attachments.
Notifies recipients that attachments have been removed.
Sends messages with detected malware to quarantine in Office 365 where a security administrator or analyst can review and release (or delete) those messages Raise visibility to recipients that attachments were removed because of detected malware.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-attachments-policies?view=o365-worldwide

**QUESTION 2**
**Case Study 2 - Litware, Inc**
**Overview**
Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

**Existing Environment**
**Internal Network Infrastructure**
The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address range shown in the following table.

| Location | IP address range |
|---|---|
| Chicago office internal network | 192.168.0.0/20 |
| Chicago office perimeter network | 172.16.0.0/24 |
| Chicago office external network | 131.107.83.0/28 |
| San Francisco office internal network | 192.168.16.0/20 |
| San Francisco office perimeter network | 172.16.16.0/24 |
| San Francisco office external network | 131.107.16.218/32 |

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:
- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

| Office | Name | Configuration |
|---|---|---|
| Chicago | DC1 | Domain controller |
| Chicago | DC2 | Domain controller |
| San Francisco | DC3 | Domain controller |
| Chicago | Server1 | SIEM-server |

You need to enable and configure Microsoft Defender for Endpoint to meet the security requirements. What should you do?

A. Configure port mirroring
B. Create the ForceDefenderPassiveMode registry setting
C. Download and install the Microsoft Monitoring Agent
D. Run WindowsDefenderATPOnboardingScript.cmd

**Answer:** C
**Explanation:**
The Server is 2016 need to go with MMA
Windows Server 2008 R2 SP1, Windows Server 2012 R2, and Windows Server 2016
You can onboard Windows Server 2008 R2 SP1, Windows Server 2012 R2, and Windows Server 2016 to Defender for Endpoint by using any of the following options:

Option 1: Onboard by installing and configuring Microsoft Monitoring Agent (MMA)
Option 2: Onboard through Azure Security Center
Option 3: Onboard through Microsoft Endpoint Configuration Manager version 2002 and later

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/configure-server-endpoints

**QUESTION 3**
**Case Study 3 - Contoso, Ltd**
**Overview**
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, and New York.
The company has the offices shown in the following table.

| Location | Employees | Laptops | Desktops computers | Mobile devices |
|---|---|---|---|---|
| Montreal | 2, 500 | 2, 800 | 300 | 3, 100 |
| Seattle | 1, 000 | 1, 100 | 200 | 1, 500 |
| New York | 300 | 320 | 30 | 400 |

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

**Existing Environment**
**Infrastructure**
The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.
The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.
Each client computer has a single volume.
Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

| Location | IP address space | Public NAT segment |
|---|---|---|
| Montreal | 10.10.0.0/16 | 190.15.1.0/24 |
| Seattle | 172.16.0.0/16 | 194.25.2.0/24 |
| New York | 192.168.0.0/16 | 198.35.3.0/24 |

Named locations are defined in Azure AD as shown in the following table.

| Name | IP address range | Trusted |
|---|---|---|
| Montreal | 10.10.0.0/16 | Yes |
| New York | 192.168.0.0/16 | No |

Which role should you assign to User1?

A. Global administrator
B. User administrator
C. Privileged role administrator
D. Security administrator

**Answer:** C
**Explanation:**
Privileged Role Administrator can manage role assignments in Azure Active Directory, as well as within Azure AD Privileged Identity Management.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

**QUESTION 4**
You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.

You need to ensure that users can only share files with users at specified partner companies. The solution must minimize administrative effort.

What should you do?

A. Limit external sharing by domain.
B. Set External sharing to New and existing guests.
C. Allow only users in specific security groups to share externally.
D. Set File and folder links to Specific people.

**Answer:** A
**Explanation:**
Limiting domains
You can limit domains by allowing only the domains you specify or by allowing all domains except those you block.
To limit domains at the organization level
1. Go to Sharing in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.
2. Under Advanced settings for external sharing, select the Limit external sharing by domain check box, and then select Add domains.
3. To create an allowlist (most restrictive), select Allow only specific domains; to block only the

domains you specify, select Block specific domains.
4. List the domains (maximum of 3000) in the box provided, using the format domain.com.
5. Etc.
Reference:
https://docs.microsoft.com/en-us/sharepoint/restricted-domains-sharing

**QUESTION 5**
You have an Azure Sentinel workspace.
You need to manage incidents based on alerts generated by Microsoft Cloud App Security.
What should you do first?

A. From the Cloud App Security portal, configure security extensions.
B. From the Cloud App Security portal, configure app connectors.
C. From the Cloud App Security portal, configure log collectors.
D. From the Microsoft 365 compliance center, add and configure a data connector.

**Answer:** A
**Explanation:**
Integrating with Microsoft Sentinel
In the Defender for Cloud Apps portal, under the Settings cog, select Security extensions.
On the SIEM agents tab, select add (+), and then choose Microsoft Sentinel.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

**QUESTION 6**
You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a Microsoft Office 365 connector.
You need to use a Fusion rule template to detect multistage attacks in which users sign in by using compromised credentials, and then delete multiple files from Microsoft OneDrive.
Based on the Fusion rule template, you create an active rule that has the default settings.
What should you do next?

A. Add data connectors.
B. Add a workbook.
C. Add a playbook.
D. Create a custom rule template.

**Answer:** B
**Explanation:**
Create an automation rule
Create a playbook
Add actions to a playbook
Attach a playbook to an automation rule or an analytics rule to automate threat response
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

**QUESTION 7**
You configure several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.
You need to allow a user named User1 to view Microsoft Defender for Office 365 reports in the Threat management dashboard.
Which role provides User1 with the required role permissions?

A. Security reader
B. Compliance administrator
C. Information Protection administrator
D. Exchange administrator

**Answer:** A
**Explanation:**
In order to view and use the reports described in this article, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:
- Organization Management
- Security Administrator
- Security Reader
- Global Reader
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Security Administrator
2. Security Reader
Other incorrect answer options you may see on the exam include the following:
- Compliance administrator
- Exchange administrator
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo

**QUESTION 8**
Your network contains an on-premises Active Directory domain. The domain contains a domain controller named DC1.
You have a Microsoft 365 E5 subscription.
You install the Microsoft Defender for Identity sensor on DC1.
You need to configure enhanced threat detection in Defender for Identity.
The solution must ensure that the following events are collected from DC1:

- 4726 - User Account Deleted
- 4728 - Member Added to Global Security Group
- 4776 - Domain Controller Attempted to Validate Credentials for an Account (NTLM)

What should you do on DC1?

A. Install the Azure Monitor agent.
B. Install System Monitor (SYSMON).
C. Configure the Windows Event Collector service.
D. Configure the Advanced Audit Policy Configuration policy.

**Answer:** D
**Explanation:**
Windows Event logs
Defender for Identity detection relies on specific Windows Event logs that the sensor parses from your domain controllers. For the correct events to be audited and included in the Windows Event log, your domain controllers require accurate Advanced Audit Policy settings.
For the correct events to be audited and included in the Windows Event Log, your domain controllers require accurate Advanced Audit Policy settings.
Note: Relevant Windows Events
For Active Directory Federation Services (AD FS) events:
1202 - The Federation Service validated a new credential

1203 - The Federation Service failed to validate a new credential
4624 - An account was successfully logged on
4625 - An account failed to log on

Reference:
https://docs.microsoft.com/en-us/defender-for-identity/prerequisites
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection

**QUESTION 9**
You have a Microsoft 365 E5 subscription that contains 100 users. Each user has a computer that runs Windows 10 and either an Android mobile device or an iOS mobile device. All the devices are registered with Azure Active Directory (Azure AD).
You enable passwordless authentication for all the users.
You need to ensure that the users can sign in to the subscription by using passwordless authentication.
What should you instruct the users to do on their mobile device first?

A. Install a device certificate.
B. Install a user certificate.
C. Install the Microsoft Authenticator app.
D. Register for self-service password reset (SSPR).

**Answer:** C
**Explanation:**
The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.
Note: Microsoft Authenticator App
You can allow your employee's phone to become a passwordless authentication method. You may already be using the Microsoft Authenticator App as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

**QUESTION 10**
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

| Name | Member of | Azure Multi-Factor Authentication (Azure MFA) |
|---|---|---|
| User1 | Group1 | None |
| User2 | Group1 | User authenticates by using a text message. |
| User3 | Group1 | User authenticates by using the Microsoft Authenticator app. |
| User4 | Group1 | User authenticates by using passwordless authentication. |

You enable the authentication methods registration campaign and configure the Microsoft Authenticator method for Group1.
Which users will be prompted to configure authentication during sign in?

A. User1 only
B. User2 only
C. User2 and User3 only

D. User1 and User2 only
E. User2 and User3 only
F. User1, User2, and User3 only

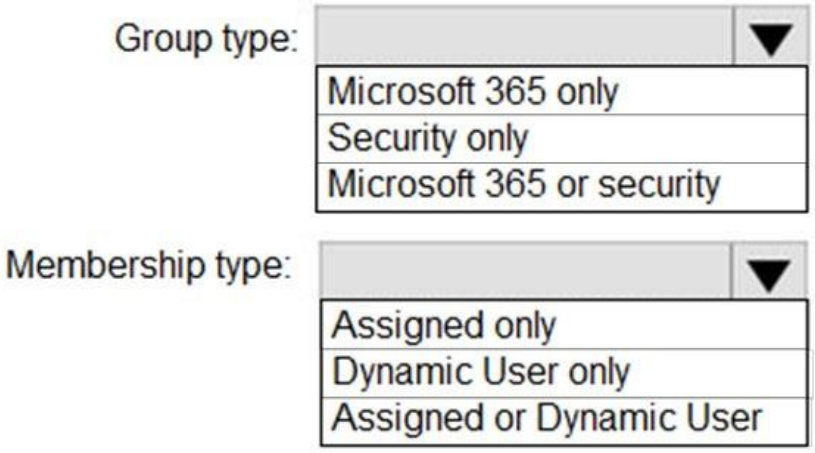
**Answer:** D
**Explanation:**
You can nudge users to set up Microsoft Authenticator during sign-in. Users will go through their regular sign-in, perform multifactor authentication as usual, and then be prompted to set up Microsoft Authenticator. You can include or exclude users or groups to control who gets nudged to set up the app. This allows targeted campaigns to move users from less secure authentication methods to Microsoft Authenticator.
Incorrect:
Not C, Not E, Not F: Not User3 since the user must not have already set up Microsoft Authenticator for push notifications on their account.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-registration-campaign

**QUESTION 11**
Hotspot Question

You have a Microsoft 365 E5 subscription.
You need to create a role-assignable group. The solution must ensure that you can nest the group.

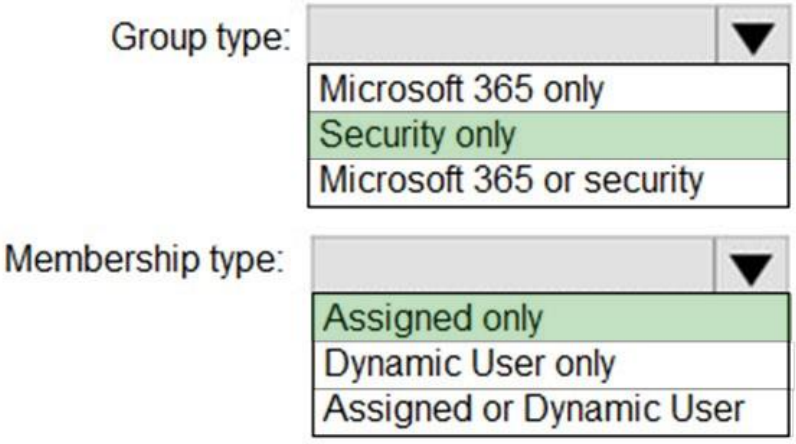
How should you configure the group? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**

## Answer Area




**Explanation:**
Box 1: Security only
You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.

Box 2: Assigned only
The membership type for role-assignable groups must be Assigned and can't be an Azure AD dynamic group.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal

**QUESTION 12**
**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

**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.**

You have a Microsoft 365 subscription and are planning to install AD Connect to support an Active Directory hybrid identity solution. Your company is using a 3rd party authentication solution that requires smartcards. You need to choose an authentication method for the Azure AD hybrid identity solution. What do you do?

Solution: You configure Pass-through authentication.

Does that meet the goal?

A. Yes

B. No

**Answer:** B
**Explanation:**
Pass-through authentication is not compatible with 3rd MFA solutions or smartcards.
Pass-through authentication should be used when the password validation must be on-premise, as it relies on local Active Directory for authentication. It is set up by installing an agent on an on-premise server that allows Azure AD to validate local AD passwords and usernames.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

**QUESTION 13**
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

| Name | Platform | Device encryption | Enrolled in Microsoft Intune |
|---|---|---|---|
| Device1 | Windows 10 | Enabled | Yes |
| Device2 | Android | Enabled | Yes |
| Device3 | iOS | Enabled | Yes |
| Device4 | macOS | Enabled | Yes |

You Plan to use the encryption report in Microsoft Endpoint Manager to view devices that have encryption enabled.

Which devices will be included in the encryption report?

A. Device1 only
B. Device1 and Device2 Only
C. Device1 and Device4 Only
D. Device1, Device2 and Device4 Only
E. Device1, Device2, Device 3 and Device 4

**Answer:** D
**Explanation:**
Encryption of data storage on a device: Supported on Android 4.0 and later, or KNOX 4.0 and later.
MacOS, Windows 10: There is an Intune setting: Encryption of data storage on a device
There is no Intune encryption setting for iOS/iPadOS.

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-mac-os

**QUESTION 14**
You have a Microsoft 365 E5 subscription.
You create a sensitivity label named Label1 and publish Label1 to all users and groups.
You have the following files on a computer:

```
- File1.doc
```

- File2.docx
- File3.xlsx
- File4.txt

You need to identify which files can have Label1 applied. Which files should you identify?

A. File2.docx only
B. File1.doc, File2.docx, File3xlsx, and File4.txt
C. File1.doc, File2.docx, and File3.xlsx only
D. File2.docx and File3.xlsx only

**Answer:** C
**Explanation:**
Office files are ok: .doc, .docx, and .xlsx.
Note: Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels

**QUESTION 15**
You have a Microsoft 365 E5 subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
A user named User1 is eligible for the User Account Administrator role.
You need User1 to request to activate the User Account Administrator role.
From where should User1 request to activate the role?

A. the My Access portal
B. the Microsoft 365 Defender portal
C. the Azure Active Directory admin center
D. the Microsoft 365 admin center

**Answer:** C
**Explanation:**
The Azure Active Directory admin center -> Azure portal -> Privileged Identity Management
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role

**QUESTION 16**
You have a Microsoft 365 tenant that has modern authentication enabled. You have Windows 10, MacOS. Android, and iOS devices that are managed by using Microsoft Endpoint Manager.
Some users have older email client applications that use Basic authentication to connect to Microsoft Exchange Online. You need to implement a solution to meet the following security requirements:

- Allow users to connect to Exchange Online only by using email client applications that support modern authentication protocols based on OAuth 2.0.
- Block connections to Exchange Online by any email client applications that do NOT support modern authentication.

What should you implement?

A. a conditional access policy in Azure Active Directory (Azure AD)
B. an OAuth app policy m Microsoft Defender for Cloud Apps
C. a compliance policy in Microsoft Endpoint Manager
D. an application control profile in Microsoft Endpoint Manager

**Answer:** A
**Explanation:**
Block clients that don't support multi-factor with a Conditional Access policy.
Note: Clients that do not use modern authentication can bypass Conditional Access policies, so it's important to block these.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies

**QUESTION 17**
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 contains 100 users and has dynamic user membership. All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.
You create a sensitivity label named Label and publish Label1 as the default label for Group1.
You need to ensure that the users in Group1 must apply Label1 to their email and documents.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Install the Azure Information Protection unified labeling client on the Windows 10 devices.
B. From the Microsoft 365 Compliance center, modify the settings of the Label1 policy.
C. Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices.
D. From the Microsoft 365 Compliance center, create an auto-labeling policy.
E. From the Azure Active Directory admin center, set Membership type for Group1 to Assigned.

**Answer:** DE
**Explanation:**
How to configure auto-labeling policies for SharePoint, OneDrive, and Exchange?
Note: When you create a sensitivity label, you can automatically assign that label to files and emails when it matches conditions that you specify.
There are two different methods for automatically applying a sensitivity label to content in Microsoft 365:
* Client-side labeling when users edit documents or compose (also reply or forward) emails: Use a label that's configured for auto-labeling for files and emails (includes Word, Excel, PowerPoint, and Outlook).
* Service-side labeling when content is already saved (in SharePoint or OneDrive) or emailed (processed by Exchange Online): Use an auto-labeling policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

**QUESTION 18**
**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

**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.**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

| Name | Azure Active Directory (Azure AD) role | Security group |
|---|---|---|
| User1 | Directory writers | Group1, Group3 |
| User2 | Security administrator | Group1, Group2 |
| User3 | Azure Information Protection administrator | Group2, Group3 |
| User4 | Cloud application administrator | Group3, Group4 |

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.

Solution: You enable SSPR for Group3.

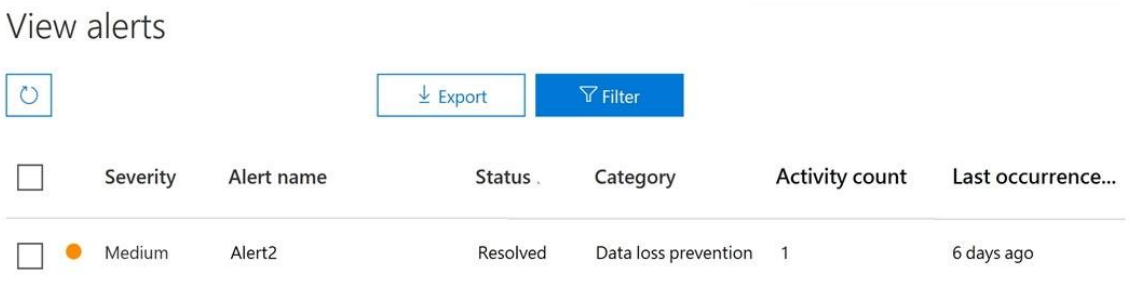
Does that meet the goal?

A. Yes
B. No

**Answer:** B
**Explanation:**
By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and Cloud application administrators. Therefore, we must enable SSPR for User3 by applying it to Group2 and not Group3 as User4 is in Group3. User4 would thus be affected if we enable it on Group3.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

**QUESTION 19**
You have a Microsoft 365 alert named Alert?
as shown in the following exhibit.




You need to manage the status of Alert. To which status can you change Alert2?

A. The status cannot be changed.
B. investigating only
C. Active or investigating only
D. Investigating, Active, or Dismissed
E. Dismissed only

**Answer:** D
**Explanation:**
After you investigate the alert, choose Manage alert to change the status (Active, Investigating, Dismissed, or Resolved). You can also add comments and assign the alert to someone in your organization.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

**QUESTION 20**
You have a Microsoft 365 subscription.

You receive a General Data Protection Regulation (GDPR) request for the custom dictionary of a user.

From the Microsoft 365 Compliance center, you need to create a content search.

How should you configure the content search?

A. Condition: Type Operator Equals any of Value Documents
B. Condition: Type Operator Equals any of Value Office Roaming Service
C. Condition: Title Operator Equals any of Value. Normal. dot
D. Condition: file type Operator Equals any of Value: dic

**Answer:** B
**Explanation:**
You can use the UDS case tool to search for and export usage data that's generated by the Office Roaming Service. Roaming is a service that stores Office-related settings, such as Office theme, custom dictionary, language settings, developer mode, and auto correct.
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-manage-gdpr-data-subject-requests-with-the-dsr-case-tool

# Thank You for Trying Our Product

## Braindump2go Certification Exam Features:


★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.


★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

**10% Discount Coupon Code:** **ASTR14**