

## Exam Questions SC-300

Microsoft Identity and Access Administrator

<https://www.2passeasy.com/dumps/SC-300/>



### NEW QUESTION 1

- (Exam Topic 1)

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.

What should you configure?

- A. named locations that have a private IP address range
- B. named locations that have a public IP address range
- C. trusted IPs that have a public IP address range
- D. trusted IPs that have a private IP address range

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

Location offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure Client Address space: List the IP address ranges that you want routed to the local on-premises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

### NEW QUESTION 2

- (Exam Topic 1)

You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.

What should you do first?

- A. Modify the User consent settings for the enterprise applications.
- B. Create a catalog.
- C. Create a program.
- D. Modify the Admin consent requests settings for the enterprise applications.

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

### NEW QUESTION 3

- (Exam Topic 1)

You need to meet the authentication requirements for leaked credentials. What should you do?

- A. Enable federation with PingFederate in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Enable password hash synchronization in Azure AD Connect.
- D. Configure an authentication method policy in Azure AD.

**Answer: C**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>

### NEW QUESTION 4

- (Exam Topic 1)

You need to configure app registration in Azure AD to meet the delegation requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Azure AD tenant-level setting to modify:

Allow users to register application

Users can consent to apps accessing company data on their behalf

Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

Application administrator

Application developer

Cloud application administrator

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

**NEW QUESTION 5**

- (Exam Topic 1)

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

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

To manage Azure AD built-in role assignments, use:

Global administrator
Privileged role administrator
Security administrator
User access administrator

To manage Azure built-in role assignments, use:

Global administrator
Privileged role administrator
Security administrator
User access administrator

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal> <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

**NEW QUESTION 6**

- (Exam Topic 1)

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.

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

Azure AD Connect settings to modify:

Directory Extensions
Domain Filtering
Optional Features

Assign Azure AD licenses to:

An Azure Active Directory group that has only nested groups
An Azure Active Directory group that has the Assigned membership type
An Azure Active Directory group that has the Dynamic User membership type

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

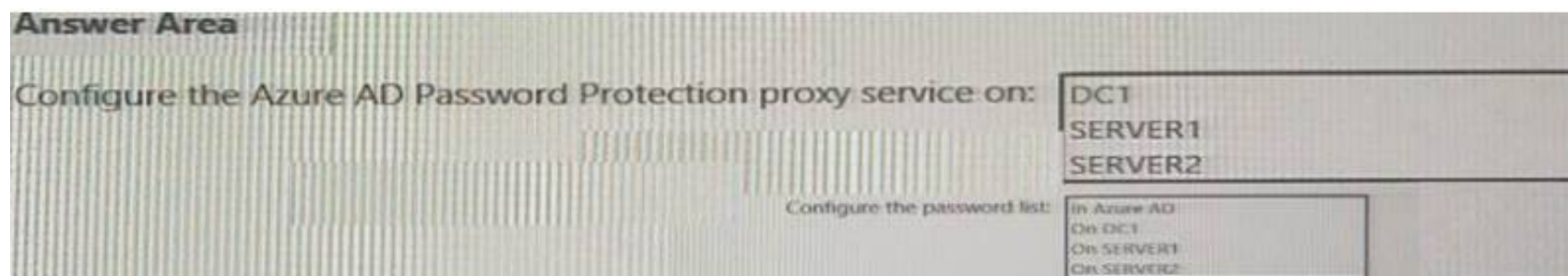
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

**NEW QUESTION 7**

- (Exam Topic 1)

You need to implement password restrictions to meet the authentication requirements. You install the Azure AD password Protection DC agent on DC1.

What should you do next? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
 Server1 On DC1

#### NEW QUESTION 8

- (Exam Topic 2)

You need to allocate licenses to the new users from A. Datum. The solution must meet the technical requirements. Which type of object should you create?

- A. a distribution group
- B. a Dynamic User security group
- C. an administrative unit
- D. an OU

**Answer:** C

#### NEW QUESTION 9

- (Exam Topic 2)

You create a Log Analytics workspace.

You need to implement the technical requirements for auditing. What should you configure in Azure AD?

- A. Company branding
- B. Diagnostics settings
- C. External Identities
- D. App registrations

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

#### NEW QUESTION 10

- (Exam Topic 2)

You need to locate licenses to the A. Datum users. The solution must need the technical requirements. Which type of object should you create?

- A. A Dynamo User security group
- B. An OU
- C. A distribution group
- D. An administrative unit

**Answer:** D

#### NEW QUESTION 10

- (Exam Topic 2)

You need to meet the technical requirements for the probability that user identities were compromised. What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The users must first:

- ☒ Provide consent for any app to access the data of Contoso.
- ☒ Register for multi-factor authentication (MFA).
- ☒ Register for self-service password reset (SSPR).

You must configure:

- ☒ A sign-in risk policy
- ☒ A user risk policy
- ☒ An Azure AD Password Protection policy



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

**NEW QUESTION 13**

- (Exam Topic 2)

You need to meet the planned changes for the User administrator role. What should you do?

- A. Create an access review.
- B. Modify Role settings
- C. Create an administrator unit.
- D. Modify Active Assignments.

**Answer:** B

**Explanation:**

Role Setting details is where you need to be: Role setting details - User Administrator Privileged Identity Management | Azure AD roles

Default Setting State

Require justification on activation Yes Require ticket information on activation No On activation, require Azure MFA Yes Require approval to activate No

Approvers None

**NEW QUESTION 14**

- (Exam Topic 2)

You need to meet the technical requirements for license management by the helpdesk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Object to create for each branch office:	<input type="checkbox"/> An administrative unit <input type="checkbox"/> A custom role <input type="checkbox"/> A Dynamic User security group <input type="checkbox"/> An OU
Tool to use:	<input type="checkbox"/> Azure Active Directory admin center <input type="checkbox"/> Active Directory Administrative Center <input type="checkbox"/> Active Directory module for Windows PowerShell <input type="checkbox"/> Microsoft 365 admin center

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text Description automatically generated

**NEW QUESTION 19**

- (Exam Topic 3)

You need to resolve the issue of the sales department users. What should you configure for the Azure AD tenant?

- A. the User settings
- B. the Device settings
- C. the Access reviews settings
- D. Security defaults

**Answer:** B

**NEW QUESTION 24**

- (Exam Topic 3)

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Number of authentication methods required:  ▼

Authentication methods that can be used:  ▼

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Number of authentication methods required: 2

Authentication methods that can be used: Email and phone only

#### NEW QUESTION 27

- (Exam Topic 3)

You need to resolve the issue of the guest user invitations. What should you do for the Azure AD tenant?

- A. Configure the Continuous access evaluation settings.
- B. Modify the External collaboration settings.
- C. Configure the Access reviews settings.
- D. Configure a Conditional Access policy.

**Answer:** B

#### NEW QUESTION 29

- (Exam Topic 3)

You need to implement the planned changes for Package1. Which users can create and manage the access review?

- A. User3 only
- B. User4 only
- C. User5 only
- D. User3 and User4
- E. User3 and User5
- F. User4and User5

**Answer:** E

#### NEW QUESTION 33

- (Exam Topic 3)

You need to implement the planned changes for litware.com. What should you configure?

- A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com
- B. Azure AD Connect to include the litware.com domain
- C. staging mode in Azure AD Connect for the litware.com domain

**Answer:** C

#### NEW QUESTION 38

- (Exam Topic 3)

You need implement the planned changes for application access to organizational data. What should you configure?

- A. authentication methods
- B. the User consent settings
- C. access packages
- D. an application proxy

**Answer:** B

#### NEW QUESTION 41

- (Exam Topic 3)

You need to resolve the issue of I-.Group1. What should you do first?

- A. Recreate the IT-Group 1 group.
- B. Change Membership type of IT-Group1 to Dynamic Device
- C. Add an owner to IT\_Group1.
- D. Change Membership type of IT-Group1 to Dynamic User

**Answer:** A

#### NEW QUESTION 46

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. An administrator deletes User1.

You need to identify the following:

- How many days after the account of User1 is deleted can you restore the account?
- Which is the least privileged role that can be used to restore User1?

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

Answer Area

Number of days:

Role:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Number of days:

Role:

NEW QUESTION 50

- (Exam Topic 4)

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for tailed Azure AD user sign-in attempts. You need to ensure that a new security administrator receives the alerts instead of you. Solution: From Azure AD, you create an assignment for the Insights at administrator role. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 54

- (Exam Topic 4)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	None
User2	None
Admin1	Application administrator
Admin2	Authentication administrator

The User settings for enterprise applications have the following configuration.

- Users can consent to apps accessing company data on their behalf:
- Users can consent to apps accessing company data for the groups they
- Users can request admin consent to apps they are unable to consent to: Yes
- Who can review admin consent requests: Admin2, User2

User1 attempts to add an app that requires consent to access company data. Which user can provide consent?

- A. User1
- B. User2
- C. Admin1
- D. Admin2

Answer: C

NEW QUESTION 56

- (Exam Topic 4)

Your company requires that users request access before they can access corporate applications. You register a new enterprise application named MyApp1 in Azure Active Dilatory (Azure AD) and configure single sign-on (SSO) for MyApp1. Which settings should you configure next for MyApp1?

- A. Self-service
- B. Provisioning
- C. Roles and administrators
- D. Application proxy

Answer: A

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

NEW QUESTION 59

- (Exam Topic 4)  
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 an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant. You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes. You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD. Solution: You configure Azure AD Password Protection. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 61

- (Exam Topic 4)  
You have a Microsoft 365 E5 subscription and an Azure subscription. You need to meet the following requirements:

- Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.
- Delegate the ability to create new virtual machines.

What should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features

Azure AD built-in roles

Azure AD managed identities

Azure role-based access control (Azure RBAC)

Answer Area

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:

Delegate the ability to create new virtual machines:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Features

Azure AD built-in roles

Azure AD managed identities

Azure role-based access control (Azure RBAC)

Answer Area

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:

Delegate the ability to create new virtual machines:

NEW QUESTION 63

- (Exam Topic 4)  
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 tenant. You have 100 IT administrators who are organized into 10 departments. You create the access review shown in the exhibit. (Click the Exhibit tab.)



## Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name \*

Description

Start date \*

Frequency

Duration (in days)

End  End by

Number of times

End date

Users  
 Scope ☒ Everyone

Review role membership (permanent and eligible) \*  
 Application Administrator and 72 others

Reviewers

(Preview) Fallback reviewers

Upon completion settings

**Start**

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You set Reviewers to Member (self).

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

## NEW QUESTION 66

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant.

You create an enterprise application collection named HR Apps that has the following settings:

- Applications: Appl. App?, App3
- Owners: Admin 1
- Users and groups: HRUsers

Three apps have the following Properties settings:

- Enabled for users to sign in: Yes
- User assignment required: Yes
- Visible to users: Yes

Users report that when they go to the My Apps portal, they only see App1 and App2-You need to ensure that the users can also see App3. What should you do from App3?

What should you do from App3?

- A. From Users and groups, add HRUsers.
- B. From Properties, change User assignment required to No.
- C. From Permissions, review the User consent permissions.
- D. From Single sign on, configure a sign-on method.

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal> <https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces>

#### NEW QUESTION 70

- (Exam Topic 4)

You have a Microsoft 365 ES subscription that user Microsoft Defender for Cloud Apps and Yammer. You need prevent users from signing in to Yammer from high-risk locations.

What should you do in the Microsoft Defender for Cloud Apps portal?

- A. Create an access Policy.
- B. Create an activity policy.
- C. Unsanction Yammer.
- D. Create an anomaly detection policy.

**Answer:** A

#### NEW QUESTION 72

- (Exam Topic 4)

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Administrative units blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Groups blade in the Azure Active Directory admin center
- D. the Sec-MsolUserLicense cmdlet

**Answer:** C

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0>

#### NEW QUESTION 73

- (Exam Topic 4)

You have an Azure AD tenant that contains the users shown in The following table.

Name	Role
User1	User Administrator
User2	Password Administrator
User3	Security Reader
User4	User

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method.

Which users must use security questions when resetting their password?

- A. User4 only
- B. User3and User4only
- C. User1 and User4only
- D. User1, User3, and User4 only
- E. User1, User2, User3. and User4

**Answer:** B

#### NEW QUESTION 77

- (Exam Topic 4)

You have a Microsoft Exchange organization that uses an SMTP' address space of contoso.com.

Several users use their contoso.com email address for self-service sign up to Azure Active Directory (Azure AD).

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Set-MsolCompanySettings
- B. Set-MsolDomainFederationSettings
- C. Update-MselfederatedDomain
- D. Set-MsolDomain

**Answer:** A

#### Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup>

#### NEW QUESTION 82

- (Exam Topic 4)

You have an Azure AD tenant

You configure User consent settings to allow users to provide consent to apps from verified publishers. You need to ensure that the users can only provide consent to apps that require low impact permissions. What should you do?

- A. Create an access package.
- B. Configure permission classifications.
- C. Create an enterprise application collection.
- D. Create an access review.

**Answer: B**

#### NEW QUESTION 86

- (Exam Topic 4)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Application Administrator

You need to compare the role permissions of each user. The solution must minimize administrative effort. What should you use?

- A. the Microsoft 365 Defender portal
- B. the Microsoft 365 admin center
- C. the Microsoft Entra admin center
- D. the Microsoft Purview compliance portal

**Answer: C**

#### NEW QUESTION 91

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.

Azure AD Connect is configured in Azure AD as shown in the following exhibit.

### PROVISION FROM ACTIVE DIRECTORY



#### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

#### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

### USER SIGN IN



Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

Connectivity from the on-premises domain to the internet is lost. Which users can sign in to Azure AD?

- A. User1 and User3 only
- B. User1 only
- C. User1, User2, and User3
- D. User1 and User2 only

**Answer: A**



**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations>

**NEW QUESTION 92**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate. Solution: From the Azure portal, you configure the Fraud alert settings for multi-factor authentication (MFA). Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

> Automatically block users who report fraud.

> Code to report fraud during initial greeting. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

**NEW QUESTION 94**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that has multi-factor authentication (MFA) enabled. The account lockout settings are configured as shown in the following exhibit.

**Account lockout**

Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.

Number of MFA denials to trigger account lockout \*

3

Minutes until account lockout counter is reset \*

60

Minutes until account is automatically unblocked \*

30

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**

A user account will be locked out if the user enters the wrong [answer choice] three times.

If a user account is locked, the user can sign in again successfully after [answer choice] minutes.

email address  
 Microsoft Authenticator app code  
 password  
 30  
 60  
 90

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

App code 60

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#account-lockout>

**NEW QUESTION 95**

- (Exam Topic 4)

You have an Azure AD tenant and a .NET web app named App1. You need to register App1 for Azure AD authentication.

What should you configure for App1?

- A. the executable name
- B. the bundle ID
- C. the package name
- D. the redirect URI

**Answer: D**

**NEW QUESTION 97**



- (Exam Topic 4)

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements.

- Identify sign-ins by users who are suspected of having leaked credentials.
- Tag the sign-ins as a high risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications. What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To classify leaked credentials as high-risk, use:

Azure Active Directory (Azure AD) Identity Protection
Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Identity Governance
Self-service password reset (SSPR)

To trigger remediation, use:

Client apps not using Modern authentication
Device state
Sign-in risk
User location
User risk

To mitigate the risk, select:

Apply app enforced restrictions
Block access
Grant access but require app protection policy
Grant access but require password change

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

**NEW QUESTION 100**

- (Exam Topic 4)

Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?

- A. a named network location  
 B. the Microsoft Authenticator app  
 C. Windows Hello for Business authentication  
 D. FIDO2 tokens

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

**NEW QUESTION 105**

- (Exam Topic 4)

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company is developing a web service named App1.

You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.

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.

Actions	Answer Area
Create an app registration.	
Add a group claim.	
Add app permissions.	
Grant admin consent.	
Add delegated permissions.	

Navigation buttons: > < (bottom left) and ^ v (bottom right)

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

> Create an app registration:

Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.

> Grant admin consent:

Higher-privileged permissions require administrator consent.

> Add app permissions:

After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity. Encoded inside the access token is every permission that your app has been granted for that resource.

Reference:

<https://docs.microsoft.com/en-us/graph/auth/auth-concepts>

**NEW QUESTION 110**

- (Exam Topic 4)

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 tenant.

You have 100 IT administrators who are organized into 10 departments. You create the access review shown in the exhibit. (Click the Exhibit tab.)

**Create an access review**

Access reviews allow reviewers to attest to whether users still need to be in a role.

**Review name \*** Admin review ✓

**Description ⓘ**

**Start date \*** 12/18/2020

**Frequency** Monthly

**Duration (in days) ⓘ** 14

**End ⓘ** Never End by Occurrences

**Number of times** 0

**End date** 01/17/2021

**Users**

**Scope** Everyone

**Review role membership (permanent and eligible) \***  
 Application Administrator and 72 others

**Reviewers**

**Reviewers** (Preview) Manager

**(Preview) Fallback reviewers ⓘ**  
 Megan Bowen

✓ Upon completion settings

**Start**

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You modify the properties of the IT administrator user accounts. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

Reference:  
D18912E1457D5D1DDCBD40AB3BF70D5D  
<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

### NEW QUESTION 112

- (Exam Topic 4)

You need to support the planned changes and meet the technical requirements for MFA.

Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Feature:

Grace period:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Feature:

Grace period:

### NEW QUESTION 115

- (Exam Topic 4)

You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.

You need to configure External collaboration settings for the tenant to meet the following requirements: |

\*Guest users must be prevented from querying staff email addresses.

\*Guest users must be able to access the tenant only if they are invited by User1.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

Guest user access restrictions:

Guest invite restrictions:

Enable guest self-service sign up via user flows:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box1 = User access is restricted to properties and memberships of their own directory objects (most restrictive). This setting ensures that guest users are prevented from querying staff email addresses and can access the tenant only if they are invited by User1.

Box2 = Only users assigned to specific admin roles can invite guest users. This setting ensures that guest users can access the tenant only if they are invited by User1.

Box3 = This setting enables guest users to sign up for the tenant only if they are invited by User1.

### NEW QUESTION 120

- (Exam Topic 4)

You have an Azure AD tenant that contains the users shown in the following table.

Name	User risk level
User1	Low
User2	Medium
User3	High

You have the Azure AD Identity Protection policies shown in the following table.

Type	Users	User risk	Sign-in risk	Controls
User risk policy	All users	Low and above	Unconfigured	Block access
Sign-in risk policy	All users	Unconfigured	High	Block access

You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.

User	Action
User1	Confirm user compromised
User2	Confirm sign-in safe
User3	Dismiss user risk
User2	Confirm user compromised

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>
User2 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>
User3 can sign in from an anonymous IP address.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input checked="" type="radio"/>
User2 can sign in by using multi-factor authentication (MFA).	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in from an anonymous IP address.	<input type="radio"/>	<input checked="" type="radio"/>

### NEW QUESTION 123

- (Exam Topic 4)

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for tailed Azure AD user sign-in attempts. You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure monitor, you create a data collection rule. Does this meet the goal?

- A. Yes
- B. No



Answer: B

#### NEW QUESTION 125

- (Exam Topic 4)

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts. You need to ensure that a new security administrator receives the alerts instead of you. Solution: From Azure AD, you modify the Diagnostics settings.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

#### NEW QUESTION 126

- (Exam Topic 4)

You have an Azure AD tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	Not applicable

Azure Multi-Factor Authentication (MFA) is enabled for all users.

User1 triggers a medium severity alert that requires additional investigation.

You need to force User1 to reset his password the next time he signs in. the solution must minimize administrative effort.

What should you do?

- A. Configure a sign-in risk policy.
- B. Mark User1 as compromised.
- C. Reconfigure the user risk policy to trigger on medium or low severity.
- D. Reset the Azure MFA registration for User1.

Answer: B

#### NEW QUESTION 128

- (Exam Topic 4)

You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.

You enable combined registration in interrupt mode. You create a new user named User1.

Which two authentication methods can User1 use to complete the combined registration process? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a FIDO2 security key
- B. a hardware token
- C. a one-time passcode email
- D. Windows Hello for Business
- E. the Microsoft Authenticator app

Answer: AE

#### NEW QUESTION 131

- (Exam Topic 4)

A user named User1 receives an error message when attempting to access the Microsoft Defender for Cloud Apps portal.

You need to identify the cause of the error. The solution must minimize administrative effort. What should you use?

- A. Log Analytics
- B. sign-in logs
- C. audit logs
- D. provisioning logs

Answer: B

#### NEW QUESTION 134

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription. You need to perform the following tasks:

- Identify the locations and IP addresses used by Azure AD users to sign in
- Review the Azure AD security settings and identify improvement recommendations.
- Identify changes to Azure AD users or service principle.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource 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.

Resources	Answer Area
Audit logs	Identify the locations and IP addresses used by Azure AD users to sign in:
Identity secure score	Identify changes to Azure AD users or service principals:
Provisioning logs	Review the Azure AD security settings and identify improvement recommendations:
Sign-in logs	

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

Resources	Answer Area
Audit logs	Identify the locations and IP addresses used by Azure AD users to sign in:
Identity secure score	Identify changes to Azure AD users or service principals:
Provisioning logs	Review the Azure AD security settings and identify improvement recommendations:
Sign-in logs	

#### NEW QUESTION 138

- (Exam Topic 4)

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users. From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users. You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort. What should you use?

- A. the Identity Governance blade in the Azure Active Directory admin center  
 B. the Set-AzureAdUser cmdlet  
 C. the Licenses blade in the Azure Active Directory admin center  
 D. the Set-WindowsProductKey cmdlet

Answer: C

#### NEW QUESTION 143

- (Exam Topic 4)

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM). While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights. You need to ensure that the IT department users only have access to the Security administrator role when required. What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments after from the Role settings details  
 B. Expire active assignments after from the Role settings details  
 C. Assignment type to Active  
 D. Assignment type to Eligible

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

#### NEW QUESTION 147

- (Exam Topic 4)

You have an Azure AD tenant that contains an access package named Package1 and a user named User1. Package1 is configured as shown in the following exhibit.

## Expiration

Access package assignments expire ⓘ

On date **Number of days** Number of hours (Preview) Never

Assignments expire after (number of days)

365

[Show advanced expiration settings](#)

## Access Reviews

Require access reviews \*

**Yes** No

Starting on ⓘ

03/01/2022 ⓘ

Review frequency ⓘ

Annually **Bi-annually** Quarterly Monthly Weekly

Duration (in days) ⓘ

90 ✓

Maximum 175

Reviewers ⓘ

- ☒ Self-review  
☐ Specific reviewer(s)  
☐ Manager

You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege. Which role should you assign to User1?

- A. Privileged role administrator  
 B. User administrator  
 C. External Identity Provider administrator  
 D. Security administrator

**Answer: A**

## NEW QUESTION 150

- (Exam Topic 4)

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 tenant.

You have 100 IT administrators who are organized into 10 departments. You create the access review shown in the exhibit. (Click the Exhibit tab.)

## Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name \*

Description

Start date \*

Frequency

Duration (in days)

End ☒ Never ☐ End by ☐ Occurrences

Number of times

End date

Users

Scope ☒ Everyone

Review role membership (permanent and eligible) \*

[Application Administrator and 72 others](#)

Reviewers

Reviewers

(Preview) Fallback reviewers

Upon completion settings

Start

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You create a separate access review for each role. Does this meet the goal?

- A. Yes
- B. No

Answer: B

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

## NEW QUESTION 155

- (Exam Topic 4)

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com. You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 users.

Which four 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.

### Actions

Delete the contoso.onmicrosoft.com domain.

Register a custom domain name of contoso.com.

Set the domain to primary.

Create a new TXT record in DNS.

Verify the domain name.

### Answer Area





- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Table Description automatically generated with medium confidence

Reference:

<https://practical365.com/configure-a-custom-domain-in-office-365/>

**NEW QUESTION 157**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to conned to Microsoft Exchange Online.

You need to ensure that users can connect t to Exchange only run email clients that use Modern authentication protocols.

What should you implement?

You need to ensure that use Modern authentication

- A. a compliance policy in Microsoft Endpoint Manager
- B. a conditional access policy in Azure Active Directory (Azure AD)
- C. an application control profile in Microsoft Endpoint Manager
- D. an OAuth policy in Microsoft Cloud App Security

**Answer:** C

**NEW QUESTION 161**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named conto.so.com that has Azure AD Identity Protection enabled. You need to Implement a sign-in risk remediation policy without blocking access.

What should you do first?

- A. Configure access reviews in Azure AD.
- B. Enforce Azure AD Password Protection.
- C. implement multi-factor authentication (MFA) for all users.
- D. Configure self-service password reset (SSPR) for all users.

**Answer:** C

**Explanation:**

MFA and SSPR are both required. However, MFA is required first. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

**NEW QUESTION 166**

- (Exam Topic 4)

You have an Azure subscription that contains the custom roles shown in the following table.

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role. Which roles can you clone to create Role3?

- A. Role2 only
- B. built-in Azure subscription roles only
- C. built-in Azure subscription roles and Role2 only
- D. built-in Azure subscription roles and built-in Azure AD roles only
- E. Role1, Role2 built-in Azure subscription roles, and built-in Azure AD roles

**Answer:** C

**NEW QUESTION 168**

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click the Exhibit tab.)

## Guest user access

### Guest user access restrictions (Preview) ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☒ Guest users have limited access to properties and memberships of directory objects
- ☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

## Guest invite settings

### Admins and users in the guest inviter role can invite ⓘ

☒ Yes ☐ No

### Members can invite ⓘ

☒ Yes ☐ No

### Guests can invite ⓘ

☐ Yes ☒ No

### Email One-Time Passcode for guests ⓘ

[Learn more](#)

☒ Yes ☐ No

### Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

☒ Yes ☐ No

## Collaboration restrictions

- ☒ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive)

A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrkam.com	A user in fabrikam.com

Which users will be emailed a passcode?

- A. User2 only
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

**Answer:** A

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

## NEW QUESTION 169

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User1, and User3,

You create a group named Group1. You add User2 and User3 to Group1.

You configure a role in Azure AD Privileged identity Management (PIM) as shown in the application administrator exhibit. (Click the application Administrator tab.)

Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group(s)

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on activation	No
Require justification on active assignment	Yes

Group1 is configured as the approver for the application administrator role. You configure User2to be eligible for the application administrator role. For User1, you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click Assignment tab)

Add assignments

Privileged Identity Management | Azure AD roles

Membership

Setting

Assignment type ⓘ

Eligible

Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts \*

01/01/2021

12:00:00 AM

Assignment ends \*

01/31/2021

11:59:00 PM

For each of the following statement, select Yes if the statement is true, Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input checked="" type="radio"/>



You have a Microsoft 365 E5 subscription.  
 You need to create a Microsoft Defender for Cloud Apps session policy. What should you do first?

- A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.
- B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance
- C. From the Azure Active Directory admin center, create a Conditional Access policy.
- D. From the Microsoft Defender for Cloud Apps portal, create a continuous report.

**Answer:** A

#### NEW QUESTION 171

- (Exam Topic 4)

Your company has a Microsoft 365 tenant.

All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.

The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.

You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution must minimize administrative effort.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

<p>Ensure that the users can connect to Service1 without being prompted for authentication:</p>	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px 5px; text-align: right;">▼</div> <div style="padding: 5px;"> <p>An app registration in Azure AD</p> <p>Azure AD Application Proxy</p> <p>An enterprise application in Azure AD</p> <p>A managed identity in Azure AD</p> </div> </div>
<p>Ensure that the users can access Service1 only from the Azure AD-joined computers:</p>	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px 5px; text-align: right;">▼</div> <div style="padding: 5px;"> <p>Azure AD Application Proxy</p> <p>A compliance policy</p> <p>A conditional access policy</p> <p>An OAuth policy</p> </div> </div>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices>

#### NEW QUESTION 173

- (Exam Topic 4)

You have an Azure AD tenant that contains two users named User1 and User2. You plan to perform the following actions:

- Create a group named Group 1.
- Add User1 and User 2 to Group1.
- Assign Azure AD roles to Group1. You need to create Group1.

Which two settings can you use? Each correct answer presents a complete solution NOTE: Each correct selection is worth one point

- A. Group type: Microsoft 365 Membership type: Dynamic User
- B. Group type: Security Membership type: Dynamic Device
- C. Group type Security Membership type: Dynamic User
- D. Group type Security Membership type: Assigned
- E. Group type: Microsoft 365 Membership type: Assigned

**Answer:** DE

#### NEW QUESTION 175

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.

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



**Answer Area**

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

(user.department

-eq  
-eq  
-match  
-ne  
-notin

null  
null  
\$null  
"null"

## NEW QUESTION 178

- (Exam Topic 4)

You have an Azure subscription.

Azure AD logs are sent to a Log Analytics workspace.

You need to query the logs and graphically display the number of sign-ins per user.

How should you complete the query? To answer, select the appropriate options in the answer area.

```
SignInLogs
| where ResultType == 0
|  login_count = count() by Identity

extend
print
project
render
summarize

 columnchart

extend
print
project
render
summarize
```

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

**Box 1 = SigninLogs**

```
Box = SigninLogs
| where ResultType == 0
```

```
| summarize(login_count = count()) by identity
```

```
| summarize login
| render piechart
```

This query retrieves the sign-in logs, filters the successful sign-ins, summarizes the count of sign-ins per user, and renders the result as a pie chart.  
 Box 2 = Render

#### NEW QUESTION 181

- (Exam Topic 4)

You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.

You need to ensure that the support team can reset passwords and manage multi-factor authentication (MFA) settings for only the executives. The solution must use the principle of least privilege.

Which object type and Azure Active Directory (Azure AD) role should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Object type:

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

Role:

- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Object type:

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

Role:

- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

#### NEW QUESTION 183

- (Exam Topic 4)

Your company has an Azure Active Directory (Azure AD) tenant named contosri.com. The company has the business partners shown in the following table.

Name	Description
Fabrikam, Inc.	An Azure AD tenant that has two verified domains named fabrikam.com and adatum.com
Litware, Inc.	A third-party identity provider that uses the domain names of litwareinc.com and contoso.com

users can request access by using package 1.

Users at Fabrikam and Litware use ail then respective domain names for email addresses.

You plan to create an access package named package1 that will be accessible only to the Fabrikam and Litware users.

You need to configure connected organizations for Fabrikam and litware so that any of their users can request access by using package1.

What is the minimum of connected organization that you should create.

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C

#### NEW QUESTION 188

- (Exam Topic 4)

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.  
 The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.  
 You plan to implement multi-factor authentication (MFA).  
 Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. an app password
- C. Windows Hello for Business
- D. SMS

**Answer: C**

**Explanation:**

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.  
 After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.  
 Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods> <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

**NEW QUESTION 190**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.  
 A contractor uses the credentials of user1@outlook.com.  
 You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.  
 What should you do?

- A. Run the New-AzADUser cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Create a guest user account in contoso.com.

**Answer: D**

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-usersportal>

**NEW QUESTION 191**

- (Exam Topic 4)

You plan to deploy a new Azure AD tenant.  
 Which multifactor authentication (MFA) method will be enabled by default for the tenant?

- A. Microsoft Authenticator
- B. SMS
- C. voice call
- D. email OTP

**Answer: B**

**NEW QUESTION 195**

- (Exam Topic 4)

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.  
 User1 has the devices shown in the following table.

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings: ➤ Name: Terms1

- Display name: Contoso terms of use
- Require users to expand the terms of use: On
- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: December 10, 2020
- Frequency: Monthly

On November 15, 2020, User1 accepts Terms1 on Device3.

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 197

- (Exam Topic 4)

Your on-premises network contains an Active Directory domain that uses Azure AD Connect to sync with an Azure AD tenant. You need to configure Azure AD Connect to meet the following requirements:

- User sign-ins to Azure AD must be authenticated by an Active Directory domain controller.
- Active Directory domain users must be able to use Azure AD self-service password reset (SSPR). What should you use for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Authentication by the domain controller:

Federation with Active Directory Federation Services (AD FS)

Federation with Active Directory Federation Services (AD FS)

Pass-through authentication

Password hash synchronization

SSPR:

Password hash synchronization

Device writeback

Group writeback

Password hash synchronization

Password writeback

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



## Answer Area

Authentication by the domain controller: Federation with Active Directory Federation Services (AD FS) ▼

Federation with Active Directory Federation Services (AD FS)

Pass-through authentication

Password hash synchronization

SSPR: Password hash synchronization ▼

Device writeback

Group writeback

Password hash synchronization

Password writeback

### NEW QUESTION 200

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You need to ensure that User1 can create new catalogs and add resources to the catalogs they own. What should you do?

- A. From the Roles and administrators blade, modify the Service support administrator role.
- B. From the identity Governance blade, modify the Entitlement management settings.
- C. From the Identity Governance blade, modify the roles and administrators for the General catalog
- D. From the Roles and administrators blade, modify the Groups administrator role.

Answer: B

### NEW QUESTION 204

- (Exam Topic 4)

Your company has an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

You have the app registrations shown in the following table.

App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

A company policy prevents changes to user permissions.

Which user can create appointments in the calendar of each user at the company?

- A. User1
- B. User2
- C. User3
- D. User4

Answer: B

### NEW QUESTION 206

- (Exam Topic 4)

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can create or delete instances of Azure Container Apps.
- Users that are assigned Role2 can enforce adaptive network hardening rules.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role1:   
 Microsoft.App  
 Microsoft.Compute  
 Microsoft.Management  
 Microsoft.Security

Role2:   
 Microsoft.App  
 Microsoft.Compute  
 Microsoft.Network  
 Microsoft.Security

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Role1:   
 Microsoft.App  
 Microsoft.Compute  
 Microsoft.Management  
 Microsoft.Security

Role2:   
 Microsoft.App  
 Microsoft.Compute  
 Microsoft.Network  
 Microsoft.Security

NEW QUESTION 207

- (Exam Topic 4)

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center. You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.

What should you create?

- A. an access package that targets users outside your directory
- B. an access package that targets users in your directory
- C. a group-based access review that targets guest users
- D. an application-based access review that targets guest users

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

NEW QUESTION 211

- (Exam Topic 4)

You have an on-premises datacenter that contains the hosts shown in the following table.

Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

You have an Azure Active Directory (Azure AD) tenant that syncs to the Active Directory forest. Multi-factor authentication (MFA) is enforced for Azure AD.

You need to ensure that you can publish App1 to Azure AD users.

What should you configure on Server and Firewall1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Service to install on Server4:

Azure AD Application Proxy
The Azure AD Password Protection DC agent
The Azure AD Password Protection proxy service
Web Application Proxy in Windows Server

Rule to configure on Firewall1:

Allow incoming HTTPS connections from Azure AD to Server4.
Allow incoming IPsec connections from Azure AD to Server4.
Allow outbound HTTPS connections from Server4 to Azure AD.
Allow outbound IPsec connections from Server4 to Azure AD.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy

#### NEW QUESTION 212

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	<b>None</b>

You have the Device Settings shown in the following exhibit.

Devices | Device settings

Default Directory - Azure Active Directory

Save Discard Got feedback?

All devices

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Diagnose and solve problems

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Users may join devices to Azure AD

All Selected None

Selected

No member selected

Users may register their devices with Azure AD

All None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication

Yes No

We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user

5

Additional local administrators on all Azure AD joined devices

Manage Additional local administrators on All Azure AD joined devices

User1 has the devices shown in the following table.

Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

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

NOTE: Each correct selection is worth one point.



Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	<input type="radio"/>	<input type="radio"/>
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to <b>Yes</b> .	<input type="radio"/>	<input type="radio"/>
Admin2 is a local administrator on Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

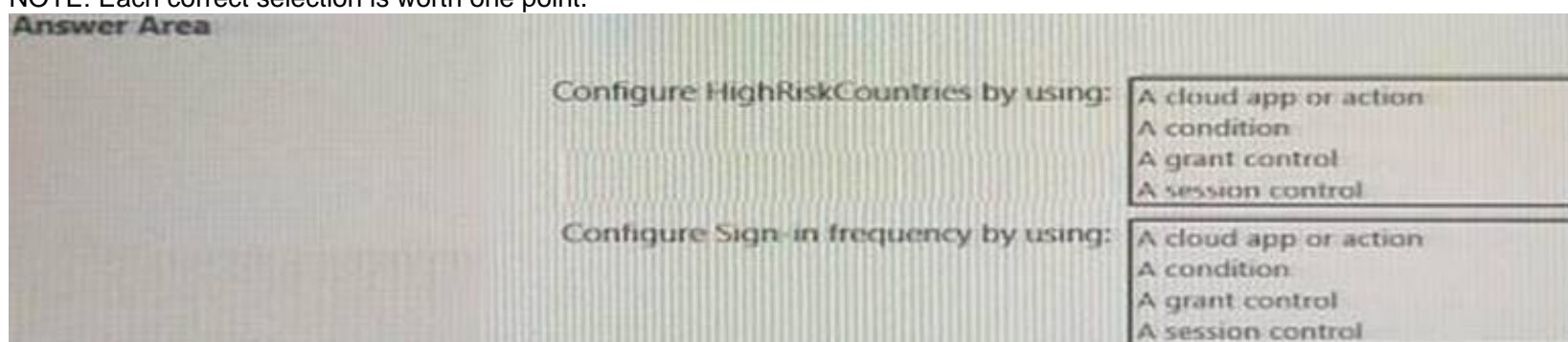
**Answer:** A

**Explanation:**

Box 1: Yes  
 Users may join 5 devices to Azure AD. Box 2: Yes  
 Box 3: No  
 An additional local device administrator has not been applied Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

**NEW QUESTION 213**

- (Exam Topic 4)  
 You have a Microsoft 365 tenant.  
 You create a named location named HighRiskCountries that contains a list of high-risk countries.  
 You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country. What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.



- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated  
 Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

**NEW QUESTION 218**

- (Exam Topic 4)  
 You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 is the owner of Group1.  
 You create an access review that has the following settings:

- > Users to review: Members of a group
- > Scope: Everyone
- > Group: Group1
- > Reviewers: Members (self)

Which users can perform access reviews for User3?

- A. User1, User2, and User3  
 B. User3 only  
 C. User1 only  
 D. User1 and User2 only

**Answer:** B



#### NEW QUESTION 221

- (Exam Topic 4)

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 an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure password writeback. Does this meet the goal?

A. Yes

B. No

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

#### NEW QUESTION 224

- (Exam Topic 4)

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 an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure conditional access policies. Does this meet the goal?

A. Yes

B. No

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

#### NEW QUESTION 227

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant. For the tenant. Users can register applications Is set to No.

A user named Admin1 must deploy a new cloud app named App1.

You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

A. Application developer in Azure AD

B. App Configuration Data Owner for Subscription1

C. Managed Application Contributor for Subscription1

D. Cloud application administrator in Azure AD

**Answer: A**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

#### NEW QUESTION 232

- (Exam Topic 4)

You have an Azure subscription that contains the key vaults shown in the following table.

Name	In resource group	Number of days to retain deleted key vaults	Purge protection
KeyVault1	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

The subscription contains the users shown in the following table.

Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

On June1, Admin4 performs the following actions:

- Deletes a certificate named Certificate1 from Key Vault1
- Deletes a secret named Secret1 from KeyVault2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	<input type="radio"/>	<input type="radio"/>
Admin2 can purge Certificate1 on June 12.	<input type="radio"/>	<input type="radio"/>
Admin3 can purge Certificate1 on June 14.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

### Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can purge Certificate1 on June 12.	<input type="radio"/>	<input checked="" type="radio"/>
Admin3 can purge Certificate1 on June 14.	<input type="radio"/>	<input checked="" type="radio"/>

### NEW QUESTION 233

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies. You need to block access to cloud apps when a user is assessed as high risk.

Which type of policy should you create in the Microsoft Defender for Cloud Apps?

- A. OAuth app policy  
 B. anomaly detection polio  
 C. access policy  
 D. activity policy

Answer: C

### NEW QUESTION 236

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You need to Identity users who have leaked credentials. The solution must meet the following requirements:

- Identity sign-ms by users who are suspected of having leaked credentials.
- Flag the sign-ins as a high-risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications. What should you use? To answer, select the appropriate options m the answer area.

To classify leaked credentials as high-risk, use:

Azure Active Directory (Azure AD) Identity Protection
Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Identity Governance
Self-service password reset (SSPR)

To trigger remediation, use:

Client apps not using Modern authentication
Device state
Sign-in risk
User location
User risk

To mitigate the risk, select:

Apply app enforced restrictions
Block access
Grant access but require app protection policy
Grant access but require password change

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To classify leaked credentials as high-risk, use:

Azure Active Directory (Azure AD) Identity Protection
Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Identity Governance
Self-service password reset (SSPR)

To trigger remediation, use:

Client apps not using Modern authentication
Device state
Sign-in risk
User location
User risk

To mitigate the risk, select:

Apply app enforced restrictions
Block access
Grant access but require app protection policy
Grant access but require password change

#### NEW QUESTION 239

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU).

What should you configure?

- A. an access review
- B. the terms or use
- C. a linked subscription
- D. a user flow

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing>

#### NEW QUESTION 244

- (Exam Topic 4)

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

... ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD > User Administrator >

## Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

### Activation

SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

### Assignment

SETTING	STATE
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every [answer choice].

- 8 hours
- 15 days
- 1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a [answer choice].

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- privileged role administrator only

- A. Mastered
- B. Not Mastered

Answer: A

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

### NEW QUESTION 246

- (Exam Topic 4)

You have a Microsoft 365 tenant.

Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).



You need to receive an alert if a registered application gains read and write access to the users' email. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Tool to use:

- Azure AD Identity Protection
- Identity Governance
- Microsoft Cloud App Security
- Microsoft Endpoint Manager

Policy type to create:

- App discovery
- App protection
- Conditional access
- OAuth app
- Sign-in risk
- User risk

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy>

#### NEW QUESTION 247

- (Exam Topic 4)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The tenant has the authentication methods shown in the following table.

Method	Target	Enabled
FIDO2	Group2	Yes
Microsoft Authenticator app	Group1	Yes
SMS	Group3	Yes

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User2 only
- E. User2 and User3 only

**Answer:** D

#### NEW QUESTION 250

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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.

Roles	Answer Area
Global administrator	User1: <input type="text" value="Role"/>
Global reader	User2: <input type="text" value="Role"/>
Reports reader	
Security operator	
Security reader	
User administrator	

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Roles	Answer Area
Global administrator	User1: <input type="text" value="Global administrator"/>
Global reader	User2: <input type="text" value="Global reader"/>
Reports reader	
Security operator	
Security reader	
User administrator	

#### NEW QUESTION 251

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.

A contractor uses the credentials of user1@outlook.com.

You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.

What should you do?

- A. Run the New-AzureADMSInvitation cmdlet.  
 B. Configure the External collaboration settings.  
 C. Add a WS-Fed identity provider.  
 D. Implement Azure AD Connect.

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal> <https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0>

#### NEW QUESTION 254

- (Exam Topic 4)

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

- A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured  
 B. an Azure AD conditional access policy that has session controls configured  
 C. an Azure AD conditional access policy that has client apps conditions configured  
 D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad>

**NEW QUESTION 256**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

In Azure AD, you add a new enterprise application named Appl. Which groups can you assign to App1?

- A. Group1 and Group2 only
- B. Group2 only
- C. Group3 only
- D. Group1 only
- E. Group1 and Group4

**Answer:** C

**NEW QUESTION 258**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

- A. Application Insights in Azure Monitor
- B. access reviews in Azure AD
- C. Cloud App Discovery in Microsoft Cloud App Security
- D. enterprise applications in Azure AD

**Answer:** C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs>

**NEW QUESTION 261**

- (Exam Topic 4)

You create a new Microsoft 365 E5 tenant.

You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).

What should you configure?

- A. a sign-in risk policy
- B. a user risk policy
- C. an MFA registration policy

**Answer:** A

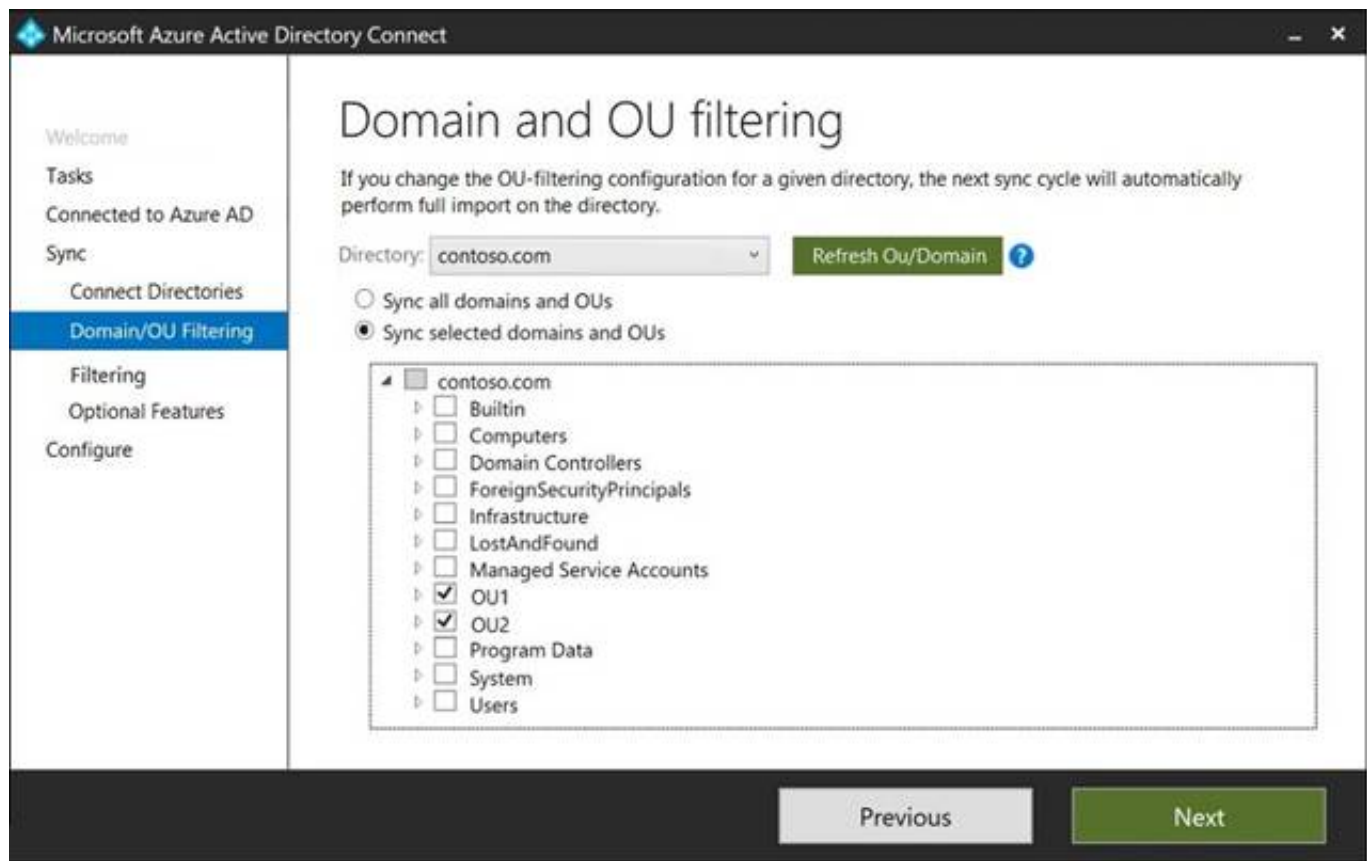
**NEW QUESTION 263**

- (Exam Topic 4)

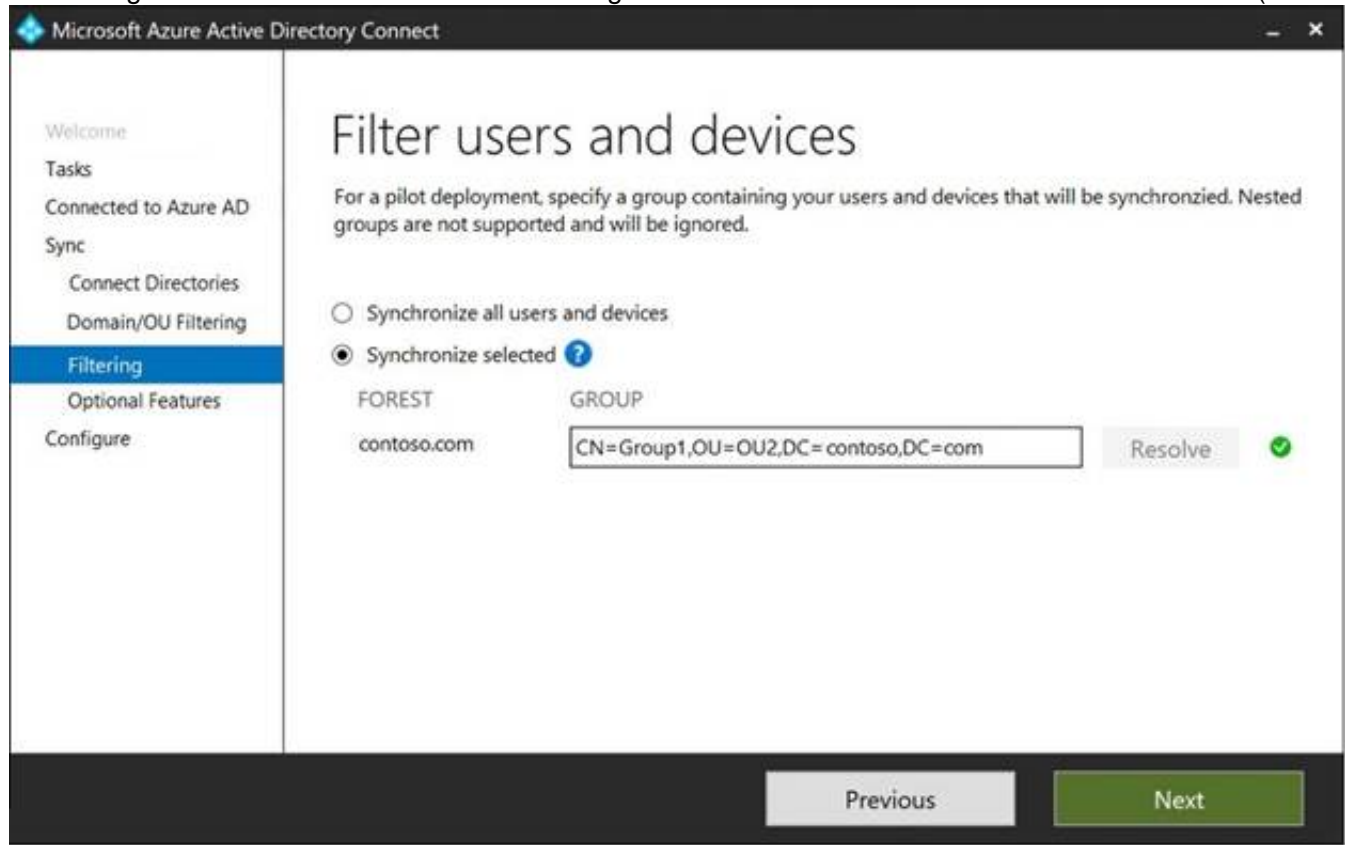
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

You install Azure AD Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering exhibit. (Click the Domain and OU Filtering tab.)



You configure the Filter users and devices settings as shown in the Filter Users and Devices exhibit. (Click the Filter Users and Devices tab.)



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

Statements	Yes	No
User1 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated  
Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.  
Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

NEW QUESTION 267

- (Exam Topic 4)  
You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.



Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

For which groups can you create an access review?

- A. Group1 only
- B. Group1 and Group4 only
- C. Group1 and Group2 only
- D. Group1, Group2, Group4, and Group5 only
- E. Group1, Group2, Group3, Group4 and Group5

**Answer:** D

**Explanation:**

You cannot create access reviews for device groups. Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

**NEW QUESTION 268**

- (Exam Topic 4)

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 an Amazon Web Services (AWS) account a Google Workspace subscription, and a GitHub account You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the GitHub app connector Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 272**

- (Exam Topic 4)

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 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate. Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

You need to configure the fraud alert settings. Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

**NEW QUESTION 273**

- (Exam Topic 4)

You have an Azure subscription that contains the following virtual machine Name: VM1

Azure region: East US

System-assigned managed identity: Disabled

You create the managed identities shown in the following table.

Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

You perform the following actions:

- Assign Managed1 to VM1.
- Create a resource group named RG1 in the West US region.

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	<input type="radio"/>	<input type="radio"/>
You can assign Managed3 to V1.	<input type="radio"/>	<input type="radio"/>
You can assign VM1 the Owner role for RG1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	<input checked="" type="radio"/>	<input type="radio"/>
You can assign Managed3 to V1.	<input checked="" type="radio"/>	<input type="radio"/>
You can assign VM1 the Owner role for RG1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 278

- (Exam Topic 4)  
You have a Microsoft 365 tenant.  
You have an Active Directory domain that syncs to the Azure Active Directory {Azure AD} tenant. Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.  
You plan to manage access to external applications by using Azure AD.  
You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.  
What should you use to gather the information?

- A. Cloud App Discovery in Microsoft Defender for Cloud Apps
- B. enterprise applications in Azure AD
- C. access reviews in Azure AD
- D. Application Insights in Azure Monitor

Answer: A

NEW QUESTION 283

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-300 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-300 Product From:

<https://www.2passeasy.com/dumps/SC-300/>

## Money Back Guarantee

### SC-300 Practice Exam Features:

- \* SC-300 Questions and Answers Updated Frequently
- \* SC-300 Practice Questions Verified by Expert Senior Certified Staff
- \* SC-300 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SC-300 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year