

Microsoft

Exam Questions SC-300

Microsoft Identity and Access Administrator



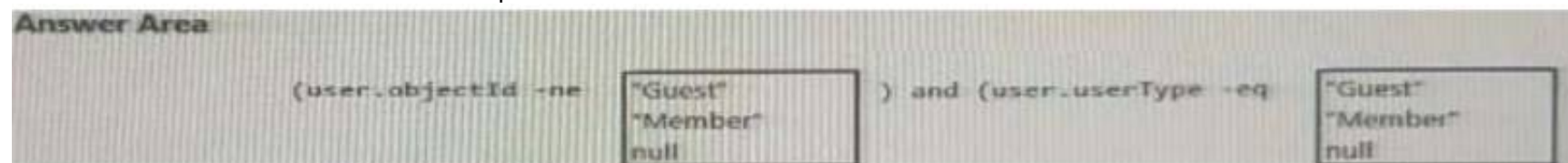
NEW QUESTION 1

- (Exam Topic 1)

You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, drag the appropriate values to the correct targets. Each value 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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Null "Member"

NEW QUESTION 2

- (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 3

- (Exam Topic 1)

You need to configure the detection of multi-staged attacks to meet the monitoring requirements. What should you do?

- A. Customize the Azure Sentinel rule logic.
- B. Create a workbook.
- C. Add Azure Sentinel data connectors.
- D. Add an Azure Sentinel playbook.

Answer: A

NEW QUESTION 4

- (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 5

- (Exam Topic 2)

You need to sync the ADatum users. The solution must meet the technical requirements. What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Answer: A

Explanation:

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

NEW QUESTION 6

- (Exam Topic 4)

You have an Azure AD tenant named Contoso that contains a terms of use (ToU) named Terms1 and an access package. Contoso users collaborate with an external organization named Fabrikam. Fabrikam users must accept Terms1 before being allowed to use the access package. You need to identify which users accepted or declined Terms1. What should you use?

- A. provisioning logs
- B. the Usage and Insights report
- C. sign-in logs
- D. audit logs

Answer: D

NEW QUESTION 7

- (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 AI) 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 8

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest. The tenant-uses through authentication.

A corporate security policy states the following:

- Domain controllers must never communicate directly to the internet.
- Only required software must be- installed on servers.

The Active Directory domain contains the on-premises servers shown in the following table.

Name	Description
Server1	Domain controller (PDC emulator)
Server2	Domain controller (infrastructure master)
Server3	Azure AD Connect server
Server4	Unassigned member server

You need to ensure that users can authenticate to Azure AD if a server fails.

On which server should you install an additional pass-through authentication agent?

- A. Server2
- B. Server4
- C. Server1
- D. Server3

Answer: C

Explanation:

Reference:

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

NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled. You are creating a conditional access policy as shown in the following exhibit.

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Policy1 ✓

Assignments

Users and groups ⓘ>
Specific users included

Cloud apps or actions ⓘ>
All cloud apps

Conditions ⓘ>
0 conditions selected

Access controls

Grant ⓘ>
0 controls selected

Session ⓘ>
0 controls selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. [Learn more](#)

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest users (preview) ⓘ

☐ Directory roles (preview) ⓘ

☒ Users and groups

Select ⓘ>
1 user

US User1
user1@sk200922outlook.onm...

...

Enable policy

Report-only **On** Off

Create

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.

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

Conditions settings

Enable policy setting

Grant settings

Sessions settings

Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.

Conditions settings

Enable policy setting

Grant settings

Sessions settings

Users and groups setting

- A. Mastered
- B. Not Mastered

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all>

NEW QUESTION 11

- (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 ES subscription. You create a user named User1.

You need to ensure that User1 can update the status of identity Secure Score improvement actions. Solution: You assign the Security Operator role User1.

Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 15

- (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. User3 and User4 only

C. User1 and User4 only

D. User1, User3, and User4 only

E. User1, User2, User3. and User4

Answer: B

NEW QUESTION 16

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.

You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.

You need to download the Azure AD log that contains conditional access policy data. What should you export from Azure AD?

A. sign-ins in JSON format

B. sign-ins in CSV format

C. audit logs in JSON format

D. audit logs in CSV format

Answer: C

Explanation:

Reference:

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

NEW QUESTION 19

- (Exam Topic 4)

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

Name	Role
Admin1	Cloud application administrator
Admin2	Application administrator
Admin3	Security administrator
User1	None

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1 requires admin consent to access Azure AD before the app can be used.

You configure the Admin consent requests strong as shown in the following exhibit. Admin consent requests.

Users can request admin consent to apps they are unable to consent to ☒ Yes ☐ No

Who can review admin consent requests ☐ ?

Reviewer type	Reviewers
Users	4 users selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests ☒ Yes ☐ No

Selected users will receive request expiration reminders ☒ Yes ☐ No

Consent request expires after (days) ☐ ?

Admin1, Admin2, Admin3, and User1 are added as reviewers.

Which users can review and approve the admin consent requests?

- A. Admm1 only
- B. Admm1 and Admin2 only
- C. Admm1 Admm2 and Admin3 only
- D. Admln1, Admin2. and User1 only
- E. Admm1 Admm2. Admm3, and User1

Answer: B

NEW QUESTION 22

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role. SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal. You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of nonadministrative users. The solution must use the principle of least privilege. Which role should you assign to SecAdmin1?

- A. Authentication administrator
- B. Helpdesk administrator
- C. Privileged authentication administrator
- D. Security operator

Answer: C

Explanation:

Reference:

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

NEW QUESTION 27

- (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 28

- (Exam Topic 4)

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

You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. home prions
- B. mobile app notification
- C. a mobile app code
- D. an email to an address in your organization

Answer: C

NEW QUESTION 29

- (Exam Topic 4)

You have a Microsoft 365 tenant.

In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

- A. an access policy in Microsoft Cloud App Security.
- B. Terms and conditions in Microsoft Endpoint Manager.
- C. a conditional access policy in Azure AD
- D. a compliance policy in Microsoft Endpoint Manager

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

NEW QUESTION 33

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

- > A device named Device1
- > Users named User1, User2, User3, User4, and User5
- > Groups named Group1, Group2, Group3, Group4, and Group5 The groups are configured as shown in the following table.

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

NEW QUESTION 38

- (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-logout>

NEW QUESTION 42

- (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 43

- (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:

- Create an app registration.
- Add a group claim.
- Add app permissions.
- Grant admin consent.
- Add delegated permissions.

Answer Area

> <

^ v

- 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 48

- (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:
An authentication method policy
A Conditional Access policy
An MFA registration policy
The Multi-Factor Authentication Server settings

Grace period:
7 days
14 days
28 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Feature:
An authentication method policy
A Conditional Access policy
An MFA registration policy
The Multi-Factor Authentication Server settings

Grace period:
7 days
14 days
28 days

NEW QUESTION 51

- (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 ES subscription. You create a user named User1.

You need to ensure that User1 can update the status of identity Secure Score improvement actions. Solution: You assign the Exchange Administrator role to User1.

- A. Yes
- B. No

Answer: B

NEW QUESTION 52

- (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 Account lockout 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 57

- (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 61

- (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 62

- (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 65

- (Exam Topic 4)

You create a conditional access policy that blocks access when a user triggers a high-severity sign-in alert. You need to test the policy under the following conditions;

- A user signs in from another country.
- A user triggers a sign-in risk.

What should you use to complete the test?

- A. the Conditional Access What If tool
- B. sign-ins logs in Azure AD
- C. access reviews in Azure AD
- D. the activity logs in Microsoft Defender for Cloud Apps

Answer: A

NEW QUESTION 68

- (Exam Topic 4)

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

Name	Role
Admin1	Account Administrator
Admin2	Service Administrator
Admin3	SharePoint Administrator

You need to implement Azure AD Privileged Identity Management (PIM). Which users can use PIM to activate their role permissions?

- A. Admin1 only
- B. Admin2 only
- C. Admin3 only
- D. Admin1 and Admin2 only
- E. Admin2 and Admin3 only
- F. Admin1, Admin2, and Admin3

Answer: D

NEW QUESTION 72

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

The users have the devices shown in the following table. You create the following two Conditional Access policies:

- Name: CAPolicy1
- Assignments

o Users or workload identities: Group 1

o Cloud apps or actions: Office 365 SharePoint Online o Conditions

Filter for devices: Exclude filtered devices from the policy Rule syntax: device.displayName -starts With "Device*"

o Access controls Grant: Block access

Session: 0 controls selected o Enable policy: On

- Name: CAPolicy2
- Assignments

o Users or workload identities: Group2

o Cloud apps or actions: Office 365 SharePoint Online o Conditions: 0 conditions selected

- Access controls

o Grant: Grant access

Require multifactor authentication o Session:

0 controls selected

- Enable policy: On

All users confirm that they can successfully authenticate using MFA.

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 access Site1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

NEW QUESTION 75

- (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 76

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provide product information to users that connect to App1 anonymously.

You need to provide App1 with Access to db1. The solution must meet the following requirements:

* Credentials must only be available to App1.

* Administrative effort must be minimized. Which type of credentials should you use?

- A. a user-assigned managed identity
- B. an Azure AD user account
- C. A SQL Server account
- D. a system-assigned managed identity

Answer: D

NEW QUESTION 78

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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

You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD.

Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.

You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency. What should you do?

- A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
- B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.
- C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
- D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

Answer: A

NEW QUESTION 79

- (Exam Topic 4)

You have an Azure AD tenant that contains a user named User1 and a registered app named App1. User1 deletes the app registration of App1.

You need to restore the app registration.

What is the maximum number of days you have to restore the app registration from when it was deleted?

- A. 14
- B. 30
- C. 60

D. 180

Answer: B

NEW QUESTION 81

- (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 dateNumber of daysNumber of hours (Preview)Never

Assignments expire after (number of days)

365

Show advanced expiration settings

Access Reviews

Require access reviews *

YesNo

Starting on ⓘ

03/01/2022📅

Review frequency ⓘ

AnnuallyBi-annuallyQuarterlyMonthlyWeekly

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 82

- (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 84

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains the following group:

- > Name: Group1
- > Members: User1, User2
- > Owner: User3

On January 15, 2021, you create an access review as shown in the exhibit. (Click the Exhibit tab.)

Create an access review

Review name *

Description

Start date *

Frequency

Duration (in days) 14

End ☐ Never ☒ End by ☐ Occurrences

Number of times

End date *

Users

Users to review

Scope ☐ Guest users only ☒ Everyone

Group *

Reviewers

Reviewers

Programs

Link to program

☐ Upon completion settings

☐ Advanced settings

Start

Users answer the Review1 question as shown in the following table.

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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 February 5, 2021, User1 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with low confidence

Reference:

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

NEW QUESTION 88

- (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 91

- (Exam Topic 4)

You have an Azure Ad tenant that contains the users show in the following table.

Name	Usage location	Department	Job title
User1	United States	Sales	Associate
User2	Finland	Sales	SalesRep
User3	Australia	Sales	Manager

You create a dynamic user group and configure the following rule syntax.

```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

Which users will be added to the group?

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

Answer: D

NEW QUESTION 96

- (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 E5 subscription. You create a user named User1.

You need to ensure that User1 can update the status of identity Secure Score improvement actions. Solution: You assign the User Administrator role to User1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 101

- (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 104

- (Exam Topic 4)
You have a hybrid Microsoft 365 subscription that contains the users show in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Application Administrator
Admin3	Cloud Application Administrator
Admin4	Application Developer
User1	None

You plan to deploy an on-premises app1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.
You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which user should perform the installation, and which role should you assign to Users1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

User that should perform the installation:

Admin3

Admin1

Admin2

Admin3

Admin4

Assign User1 the role of:

Application Developer

Application Administrator

Application Developer

Cloud Application Administrator

Global Administrator

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User that should perform the installation:

Admin3

Admin1

Admin2

Admin3

Admin4

Assign User1 the role of:

Application Developer

Application Administrator

Application Developer

Cloud Application Administrator

Global Administrator

NEW QUESTION 105

- (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 113

- (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.

Ensure that the users can connect to Service1 without being prompted for authentication:

▼

An app registration in Azure AD
 Azure AD Application Proxy
 An enterprise application in Azure AD
 A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

▼

Azure AD Application Proxy
 A compliance policy
 A conditional access policy
 An OAuth policy

- 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 117

- (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 122

- (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
| where ResultType == 0
| summarize login_count = count() by identity
| 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 125

- (Exam Topic 4)
You have an Azure AD tenant that contains a user named Admin1.
Admin1 uses the Require password change for high-risk user's policy template to create a new Conditional Access policy.
Who is included and excluded by default in the policy assignment? To answer, drag the appropriate options to the correct target. Each option 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.

Options

Admin1

All guest and external users

All users

Directory roles

None

Answer Area

Include:

Exclude:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A white background with black text Description automatically generated

NEW QUESTION 127

- (Exam Topic 4)
You have a Microsoft 365 tenant.

You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor. What should you do first?

- A. Run the Get-AzureADAuditDirectoryLogs cmdlet.
- B. Create an Azure AD workbook.
- C. Run the Set-AzureADTenantDetail cmdlet.
- D. Modify the Diagnostics settings for Azure AD.

Answer: D

NEW QUESTION 129

- (Exam Topic 4)

Your company has an Azure Active Directory (Azure AD) tenant named contoso.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 all their 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 number of connected organizations that you should create.

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

Answer: C

NEW QUESTION 134

- (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 138

- (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 141

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1.

You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principal of least privilege.

Which role should you assign to User1?

- A. Privileged role administrator
- B. Identify Governance administrator
- C. User administrator
- D. User Access Administrate

Answer: B

NEW QUESTION 146

- (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	None

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 Yes .	<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 147

- (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.

Answer Area

Configure HighRiskCountries by using:

A cloud app or action

A condition

A grant control

A session control

Configure Sign-in frequency by using:

A cloud app or action

A condition

A grant control

A session control

- 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 151

- (Exam Topic 4)

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

Name	Member of administrative unit
User1	AU1
User2	AU1
User3	AU1
User4	AU2
User5	Not a member of an administrative unit

The users are assigned the roles shown in the following table.

User	Role	Role scope
User1	Password Administrator	Organization
User2	Global Reader	Organization
User3	None	Not applicable
User4	Password Administrator	AU1
User5	None	Not applicable

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

User3 only

User3 only

User2 and User3 only

User3 and User5 only

User2, User3, and User5 only

User3, User4 and User5 only

User2, User3, User4, and User5

User4:

User3 only

User3 only

User2 and User3 only

User3 and User5 only

User1, User2, and User3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:

User3 only

User3 only

User2 and User3 only

User3 and User5 only

User2, User3, and User5 only

User3, User4 and User5 only

User2, User3, User4, and User5

User4:

User3 only

User3 only

User2 and User3 only

User3 and User5 only

User1, User2, and User3 only

NEW QUESTION 154

- (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 159

- (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-ins 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 163

- (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 166

- (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 167

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1. You need to meet the following requirements:

- Prevent User1 from being added as an owner of newly registered apps.
- Ensure that User1 can manage the application proxy settings.
- Ensure that User2 can register apps.
- Use the principle of least privilege. Which role should you assign to User1?

- A. Application developer
- B. Cloud application administrator
- C. Service support administrator
- D. Application administrator

Answer: D

NEW QUESTION 170

- (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>

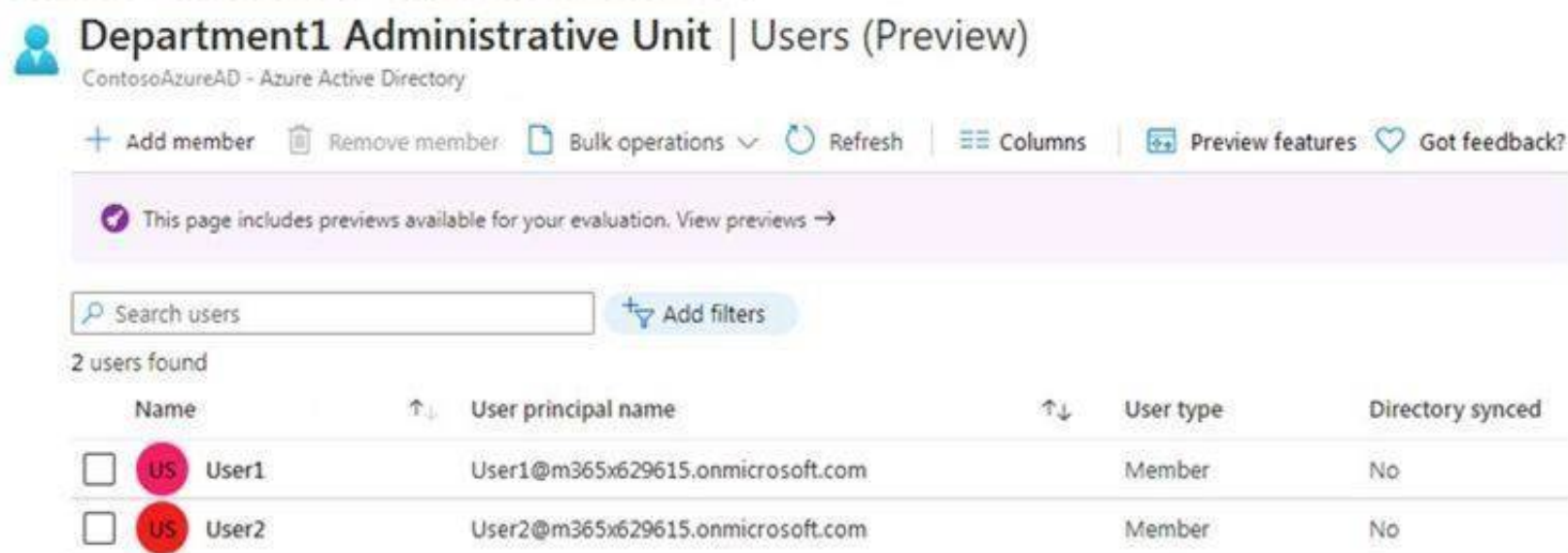
NEW QUESTION 175

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1.

Department1 has the users shown in the Users exhibit. (Click the Users tab.)

[Dashboard](#) > [ContosoAzureAD](#) > [Department1 Administrative Unit](#)



Department1 Administrative Unit | Users (Preview)
 ContosoAzureAD - Azure Active Directory

+ Add member Remove member Bulk operations Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. [View previews](#) →

Search users Add filters

2 users found

Name	User principal name	User type	Directory synced
<input type="checkbox"/> User1	User1@m365x629615.onmicrosoft.com	Member	No
<input type="checkbox"/> User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

» + Add Remove Refresh Columns Preview features Got feedback?

Search groups Add filters

Name	Group Type	Membership Type
<input type="checkbox"/> GR Group1	Security	Assigned
<input type="checkbox"/> GR Group2	Security	Assigned

Department1 has the user administrator assignments shown in the Assignments exhibit. (Click the Assignments tab.)

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

» + Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)

Dashboard > ContosoAzureAD > Groups > Group2

Group2 | Members

Group

» + Add members Remove Refresh Bulk operations Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Direct members

Name	User type
<input type="checkbox"/> US User3	Member
<input type="checkbox"/> US User4	Member

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
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input type="radio"/>
Admin1 can add User1 to Group 2	<input type="radio"/>	<input type="radio"/>
Admin 2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

NEW QUESTION 179

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3. You have two Azure AD roles that have the Activation settings shown in the following table.

Name	Required justification on activation	Require approval to activate	Approvers
Role1	No	Yes	User1
Role2	Yes	No	None

The Azure AD roles have the Assignment settings shown in the following table.

Role	Allow permanent eligible assignment	Allow Permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have the eligible users shown in the following table.

Role	Eligible assignment
Role1	User1, User2
Role2	User3

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
If User1 requests Role1, the request will be approved automatically.	<input type="radio"/>	<input type="radio"/>
User1 can approve the request of User3 for Role2.	<input type="radio"/>	<input type="radio"/>
User1 must provide justification to approve the request of User2 for Role1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can approve the request of User3 for Role2.	<input type="radio"/>	<input checked="" type="radio"/>
User1 must provide justification to approve the request of User2 for Role1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 182

- (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 185

- (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 186

- (Exam Topic 4)

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

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

You have the locations shown in the following table.

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

The tenant contains a named location that has the following configurations:

- Name: location1
- Mark as trusted location: Enabled
- IPv4 range: 10.10.0.0/16

MFA has a trusted IP address range of 193.17.17.0/24.

You have a Conditional Access policy that has the following settings:

- Name: CAPolicy1
- Assignments
 - o Users or workload identities: Group 1
 - o Cloud apps or actions: All cloud apps
- * Conditions
 - * Locations All trusted locations
- Access controls
 - o Grant
 - Grant access: Require multi-factor authentication
- Session: 0 controls selected
- Enable policy: On

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
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 188

- (Exam Topic 4)

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

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

You create an access review for Group1 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

You create an access review for Group2 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

What is the minimum number of Azure AD Premium P2 licenses required for each group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Group1:

1

500

525

Group2:

1

100

295

395

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Group1:

▼

1

500

525

Group2:

▼

1

100

295

395

NEW QUESTION 192
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The SC-300 Practice Test Here](#)