



Microsoft

Exam Questions SC-300

Microsoft Identity and Access Administrator

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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.

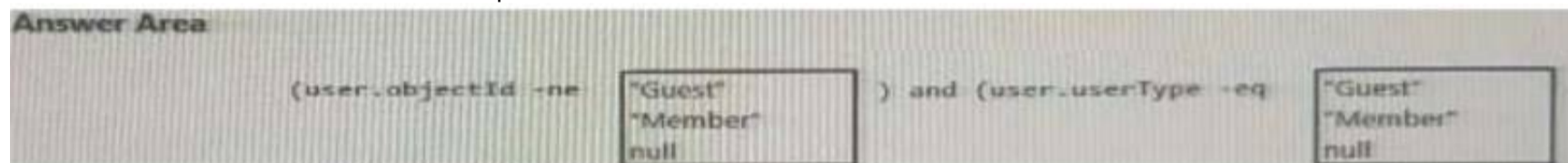
NEW QUESTION 2

- (Exam Topic 1)

You need to 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 3

- (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 4

- (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 5

- (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 6

- (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 7

- (Exam Topic 2)

You need to meet the planned changes and technical requirements for App1. What should you implement?

- A. a policy set in Microsoft Endpoint Manager
- B. an app configuratifton policy in Microsoft Endpoint Manager
- C. an app registration in Azure AD
- D. Azure AD Application Proxy

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

NEW QUESTION 8

- (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 9

- (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:

An administrative unit
A custom role
A Dynamic User security group
An OU

Tool to use:

Azure Active Directory admin center
Active Directory Administrative Center
Active Directory module for Windows PowerShell
Microsoft 365 admin center

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated

NEW QUESTION 10

- (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 10

- (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 13

- (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 14

- (Exam Topic 3)

You need to resolve the recent security incident issues.

What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. Each policy type 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.

Policy Types

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

Answer Area

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy Types

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

Answer Area

Leaked credentials: A user risk policy

A sign-in from a suspicious browser: A sign-in risk policy

Resources accessed from an anonymous IP address: A sign-in risk policy

NEW QUESTION 15

- (Exam Topic 4)

Your network contains an on-premises Active Directory Domain services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

Name	Description
OU1	Syncs with Azure AD
OU2	Does NOT sync with Azure AD

You need to create a break-glass account named BreakGlass.

Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Location:

Azure AD

OU1

OU2

Role:

Billing Administrator

Global Administrator

Owner


Privileged Role Administrator

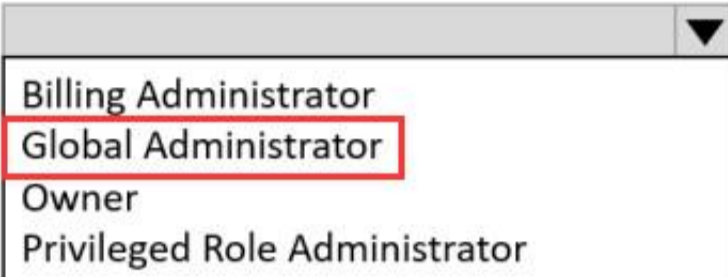
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Location: 

Role: 

NEW QUESTION 17

- (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 Block/unblock users 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 21

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain.

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain.

The VPN server does NOT support Azure Multi-Factor Authentication (MFA). You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

- A. Azure AD Application Proxy
- B. an Azure AD Password Protection proxy
- C. Network Policy Server (NPS)
- D. a pass-through authentication proxy

Answer: C

NEW QUESTION 25

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You purchase the app governance add-on license. You need to enable app governance integration. Which portal should you use?

- A. the Microsoft Defender for Cloud Apps portal
- B. the Microsoft 365 admin center
- C. Microsoft 365 Defender
- D. the Azure Active Directory admin center
- E. the Microsoft Purview compliance portal

Answer: A

NEW QUESTION 27

- (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

And 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 29

- (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

 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

Answer: A

Explanation:

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

NEW QUESTION 34

- (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 37

- (Exam Topic 4)
 You have an Azure Active Directory (Azure Azure) tenant that contains the objects shown in the following table.
 • A device named Device1
 • Users named User1, User2, User3, User4, and User5
 • Five 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, Group4
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	Group5
Group5	Microsoft 365	Assigned	User5

How many licenses are used if you assign the Microsoft Office 365 Enterprise E5 license to Group1?

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

Answer: B

Explanation:

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

NEW QUESTION 40

- (Exam Topic 4)
 You have an Azure AD tenant.
 You need to bulk create 25 new user accounts by uploading a template file. Which properties are required in the template file?

- A. `accountEnabled`, `givenName`, `surname`, and `userPrincipalName`
- B. `accountEnabled`, `displayName`, `userPrincipalName`, and `passwordProfile`
- C. `displayName`, `identityIssuer`, `usageLocation`, and `userType`
- D. `accountEnabled`, `passwordProfile`, `usageLocation`, and `userPrincipalName`

- A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 44

- (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-MsolFederatedDomain`
D. `Set-MsolDomain`

Answer: A

Explanation:

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

NEW QUESTION 45

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:

- Block external users from signing in to this directory: Yes
- Remove external user Yes
- Number of days before removing external user from this directory: 30

On March 1, 2022, you create an access package named Package1 that has the following settings:

- Resource roles
 - o Name: All Company
 - o Type: Group and Team
 - o Role: Member
- Lifecycle

o Access package assignment expire: On date o Assignment expiration date: April 1, 2022

On March 1, 2022, you assign Package1 to the guest users shown in the following table.

Name	Email address
Guest1	guest1@outlook.com
Guest2	guest2@outlook.com

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1(2022, you invite a guest user named Guest3 to contoso.com. On April 4, 2022, you add Guest3 to the All Company group.

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
On May 5, 2022, the Guest1 account is in contoso.com.	<input type="radio"/>	<input type="radio"/>
On May 5, 2022, the Guest2 account is in contoso.com.	<input type="radio"/>	<input type="radio"/>
On May 5, 2022, the Guest3 account is in contoso.com.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

NEW QUESTION 50

- (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 54

- (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 57

- (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 60

- (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 63

- (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 64

- (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 65

- (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:

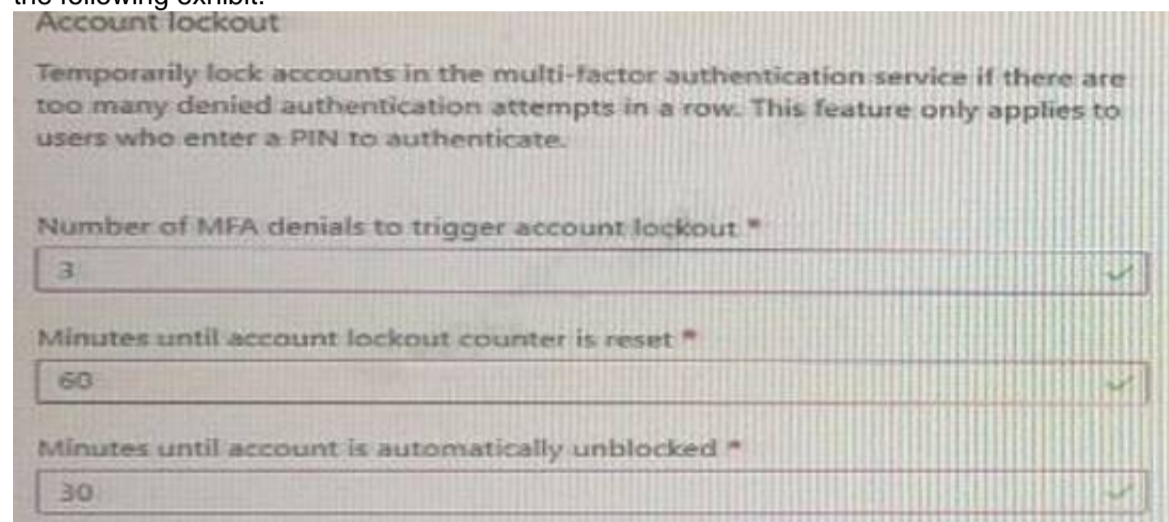
Reference:

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

NEW QUESTION 67

- (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.

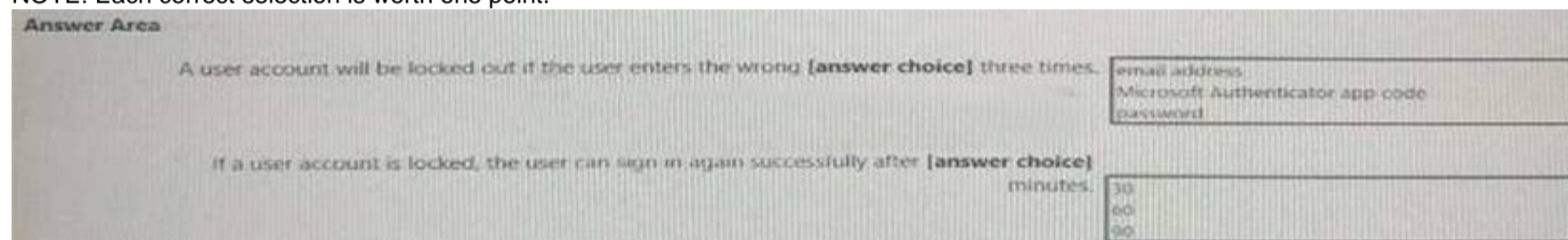


The screenshot shows the 'Account lockout' settings in the Azure AD portal. It includes a description: 'Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.' Below this are three settings, each with a dropdown menu and a green checkmark icon:

- 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.



The screenshot shows the 'Answer Area' for the question. It contains two statements with dropdown menus for '[answer choice]':

- A user account will be locked out if the user enters the wrong [answer choice] three times. The dropdown menu has options: email address, Microsoft Authenticator app code, and password.
- If a user account is locked, the user can sign in again successfully after [answer choice] minutes. The dropdown menu has options: 30, 60, and 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 71

- (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 75

- (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.

- Identity 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 79

- (Exam Topic 4)

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

- > Pa55w0rd12
- > Pa55w0rd12
- > Pa55w0rd12
- > Pa55w.rd12
- > Pa55w.rd123
- > Pa55w.rd123
- > Pa55w.rd123
- > Pa55word12
- > Pa55word12
- > Pa55word12
- > Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.

What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Tracked sign-in attempts:

	▼
4	
5	
10	
11	

Unlock by:

	▼
Clearing the browser cache	
Signing in by using inPrivate browsing mode	
Performing a self-service password reset (SSPR)	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, table Description automatically generated

Reference:

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

NEW QUESTION 84

- (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 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 restrictions:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows:

No

Yes

- 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 88

- (Exam Topic 4)

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Configure password protection for Windows Server Active Directory.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

NEW QUESTION 91

- (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 94

- (Exam Topic 4)
Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.
You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync.
What should you do in Azure AD Connect?

- A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
- B. Configure a Full Import run profile.
- C. Create an inbound synchronization rule for the Active Directory Domain Services connector.
- D. Configure an Export run profile.

Answer: C

Explanation:
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

NEW QUESTION 99

- (Exam Topic 4)
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon 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 monitor, you create a data collection rule. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 104

- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site!. Site! hosts PDF files
You need to prevent users from printing the files directly from Sitel.

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

- A. activity policy
- B. file policy
- C. access policy
- D. session policy

Answer: D

NEW QUESTION 105

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.

Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Which objects can you add as eligible in Azure Privileged identity Management (PIM) for an Azure AD role?

- A. User1 only
- B. User1 and Identity1 only
- C. User1, Guest1, and Identity
- D. User1 and Guest1 only

Answer: D

Explanation:

Reference:

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

NEW QUESTION 109

- (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 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 *

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

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 add each manager as a fallback reviewer. 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 115

- (Exam Topic 4)

You have a Microsoft 365 subscription. The subscription contains users that use Microsoft Outlook 2016 and Outlook 2013 clients. You need to implement tenant restrictions. The solution must minimize administrative effort. What should you do first?

- A. Upgrade the Outlook 2013 clients to Outlook 2016.
- B. Configure the Outlook 2013 clients to use modern authentication.
- C. Upgrade all the Outlook clients to Outlook 2019.
- D. From the Exchange admin center, configure Organization Sharing.

Answer: A

NEW QUESTION 118

- (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 123

- (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 127

- (Exam Topic 4)

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

Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure AD Identity Protection.

Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure the user risk policy:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

- 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/identity-protection/overview-identity-protection>

NEW QUESTION 132

- (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 137

- (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 141

- (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 Microsoft Azure app connector. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 146

- (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. security questions
- C. voice
- D. an app password

Answer: A

Explanation:

Reference:

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

NEW QUESTION 149

- (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 154

- (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 159

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
 You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.
 What should you do first?

- A. From the Microsoft Defender for Cloud Apps portal, unsanctioned Facebook.
- B. Create an app configuration policy in Microsoft Endpoint Manager.
- C. Create a Defender for Cloud Apps access policy.
- D. Create a Conditional Access policy.

Answer: C

NEW QUESTION 160

- (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)

[Show advanced expiration settings](#)

Access Reviews

Require access reviews * ☒ Yes ☐ No

Starting on ⓘ

Review frequency ⓘ **Annually** **Bi-annually** Quarterly Monthly Weekly

Duration (in days) ⓘ ✓
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 162

- (Exam Topic 4)

You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.

Users are invited to collaborate with contoso.com as shown in the following table.

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

From the External collaboration settings in the Azure Active Directory admin center, you configure the Collaboration restrictions settings as shown in the following exhibit.

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)

 Delete

☒ TARGET DOMAINS

☐ Outlook.com

From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.
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 accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes
Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.
Box 2: Yes
Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.
Box 3. No
Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

NEW QUESTION 166

- (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 168

- (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 172

- (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 174

- (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



NEW QUESTION 179

- (Exam Topic 4)
You have a Microsoft 365 E5 tenant. You purchase a cloud app named App1.
You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud app Security.
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

From Microsoft Cloud App Security, create a session policy.

Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
A picture containing application Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app> <https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad>

NEW QUESTION 181

- (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 185

- (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: A**

Explanation:

(user.department

-eq

-eq

-match

-ne

-notin

null

\$null

"null"

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.

Correct Order

Actions

On Server1, run export for all connectors.

On Server2, run export for all connectors.

On Server2, run full import for all connectors.

On Server2, run delta synchronization for all connectors.

On Server2, install Azure AD Connect.

On Server1, configure the staging mode.

>

<

Answer Area

>

<

- Answer: A**

Explanation:

Explanation:

Actions

- On Server1, run export for all connectors.
- On Server2, run export for all connectors.
- On Server2, run full import for all connectors.
- On Server2, run delta synchronization for all connectors.
- On Server2, install Azure AD Connect.
- On Server1, configure the staging mode.

Answer Area

- On Server2, run export for all connectors.
- On Server2, run delta synchronization for all connectors.
- On Server1, run export for all connectors.

NOTE: Each correct selection is worth one point.

Options	Answer Area
<div>Admin1</div> <div>All guest and external users</div> <div>All users</div> <div>Directory roles</div> <div>None</div>	<div>Include: <input type="text"/></div> <div>Exclude: <input type="text"/></div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

A white background with black text Description automatically generated

NEW QUESTION 195

- (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 200

- (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 201

- (Exam Topic 4)

You have the Azure resources show in the following table.

Name	Description
User1	User account
Group1	Security group that uses the Dynamic user membership type
VM1	Virtual machine with a system-assigned managed identity
App1	Enterprise application
RG1	Resource group

To Which identities can you assign the Contributor role for RG1?

- A. User1 only
B. User1 and Group1 only
C. User1 and VM1 only
D. User1, VM1, and App1 only
E. User1, Group1, VM1, and App1

Answer: E

NEW QUESTION 203

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com that has Email one-time passcode for guests set to Yes.

You invite the guest users shown in the following table.

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users:

Guest1 only

Guest2 only

Guest3 only

Guest1 and Guest2 only

Guest2 and Guest3 only

Guest1, Guest2, and Guest3

Valid for:

30 minutes

60 minutes

24 hours

48 hours

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Users:

Guest1 only

Guest2 only

Guest3 only

Guest1 and Guest2 only

Guest2 and Guest3 only

Guest1, Guest2, and Guest3

Valid for:

30 minutes

60 minutes

24 hours

48 hours

NEW QUESTION 204

- (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 209

- (Exam Topic 4)

You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group1 tab.)

```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

ObjectId                DisplayName  UserPrincipalName      UserType
-----
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin        admin@M365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -searchstring "group1" | GetAzureADGroupMember | ft displayname

DisplayName
-----
User1
User4
Group3
```

You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click the App1 Properties tab.)

[Dashboard](#) > [ContosoAzureAD](#) > [Enterprise applications](#) > [App1](#)

App1| Properties

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators (Prev.

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-ins

Save Discard Delete Got feedback?

Enabled for users to sign-in?

Yes No

Name

App1

Homepage URL

https://app1.m365x629615.onmicrosoft.com/

Logo

AP

Select a file

User access URL

https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...

Application ID

09df58d6-d29d-40de-b0d0-321fdc63c665

Object ID

03709d22-7e61-4007-a2a0-04dbdff269cd

Terms of Service Url

Publisher did not provide this information

Privacy Statement Url

Publisher did not provide this information

Reply URL

https://contoso.com/App1/login

User assignment required?

Yes No

Visible to users?

Yes No

You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click the App1 Self-service tab.)

App1 | Self-service
Enterprise application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Pre...

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Allow users to request access to this application? ⓘ

To which group should assigned users be added? ⓘ

Require approval before granting access to this application? ⓘ

Who is allowed to approve access to this application? ⓘ

To which role should users be assigned in this application? * ⓘ

Yes No

Select Group Group1

Yes No

Select approvers 1 users selected

Default Access

Select approvers

Search

User1
User1@m365x629615.onmicrosoft.com
Selected

User2
User2@m365x629615.onmicrosoft.com

User3
User3@m365x629615.onmicrosoft.com

User4
User4@m365x629615.onmicrosoft.com

Select approvers

Selected approvers

User1
User1@m365x629615.onmicrosoft.com

Remove

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
The members of Group3 can access App1 without first being approved by User1.	<input type="radio"/>	<input type="radio"/>
After you configure self-service for App1, the owner of Group1 is User1.	<input type="radio"/>	<input type="radio"/>
App1 appears in the Microsoft Office 365 app launcher of User4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

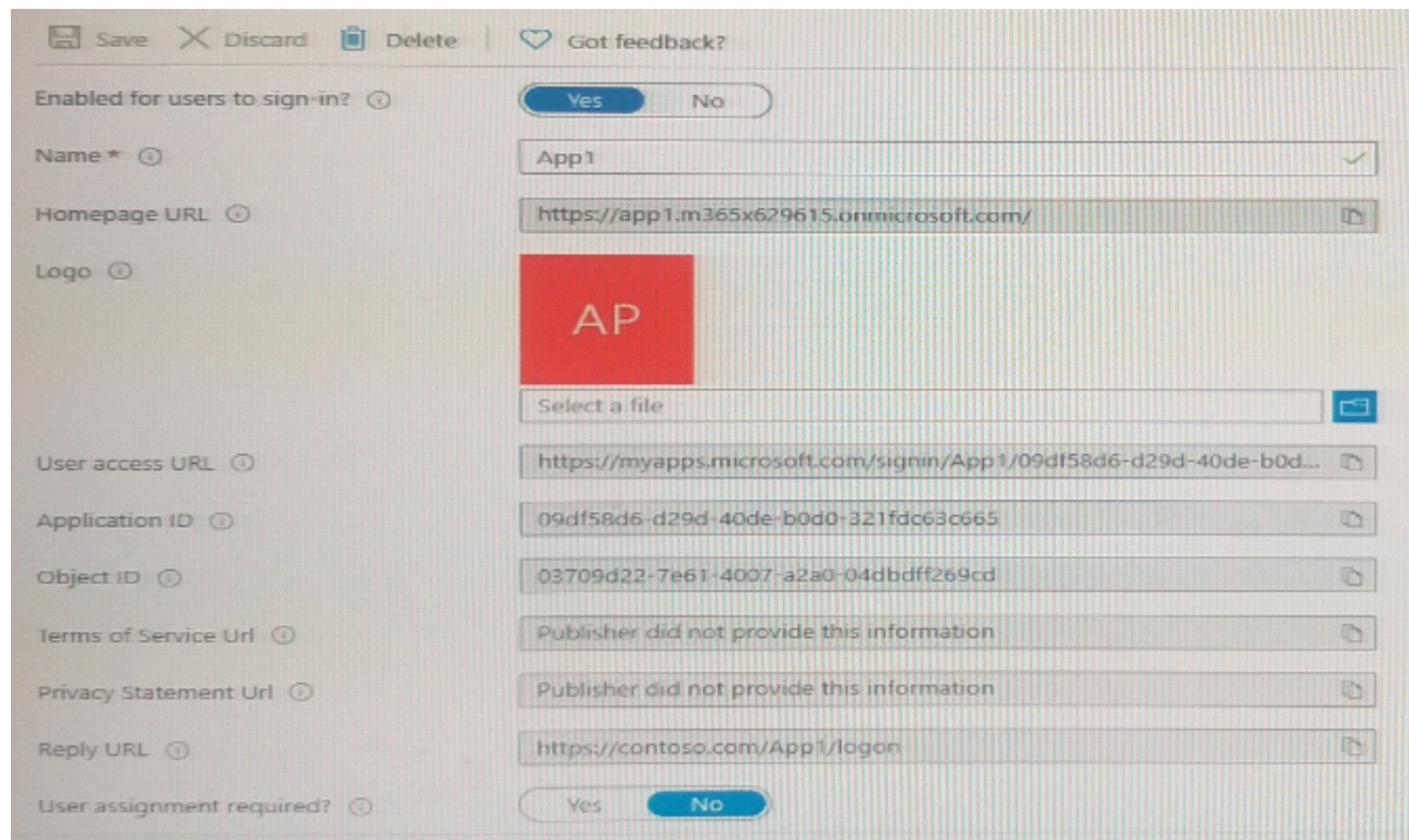
Answer: A

Explanation:

- No No Yes
- a) When you assign a group to an application, only users in the group will have access. The assignment does not cascade to nested groups.
b) Tested in lab, existing owners will be replaced. Also direct assignment (resource owner) is path of least privilege. (replicated in test)
c) Application setting 'visible to users' is set to No, then no users see this application on their My Apps portal and O365 launcher.
- Reference
- a) <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>
b) maybe
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage-groups>
c) <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users>

NEW QUESTION 213

- (Exam Topic 4)
You have a custom cloud app named App1 that is registered in Azure Active Directory (Azure AD). App1 is configured as shown in the following exhibit.



The screenshot shows the configuration page for an application named 'App1'. The 'Enabled for users to sign-in?' toggle is set to 'Yes'. The 'Name' is 'App1'. The 'Homepage URL' is 'https://app1.m365x629615.onmicrosoft.com/'. The 'Logo' is a red square with 'AP' in white. The 'User access URL' is 'https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...'. The 'Application ID' is '09df58d6-d29d-40de-b0d0-321fdc63c665'. The 'Object ID' is '03709d22-7e61-4007-a2a0-04dbdff269cd'. The 'Terms of Service Url' and 'Privacy Statement Url' are both 'Publisher did not provide this information'. The 'Reply URL' is 'https://contoso.com/App1/login'. The 'User assignment required?' toggle is set to '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.

[answer choice] can access App1 from the homepage URL.

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

Both questions have the same drop-down menu options: All users, No one, Only users listed on the Owners blade, Only users listed on the Users and groups blade.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 217

- (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 221

- (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

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

Save

Discard

Got feedback?

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 225

- (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 228

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to ensure that users can request access to Site. the solution must meet the following requirements.

- Automatically approve requests from users based on their group membership.
- Automatically remove the access after 30 days What should you do?

- A. Create a Conditional Access policy.
B. Create an access package.
C. Configure Role settings in Azure AD Privileged Identity Management.
D. Create a Microsoft Defender for Cloud Apps access policy.

Answer: B

NEW QUESTION 231

- (Exam Topic 4)

You have a Microsoft 365 ES subscription that contains a user named User1. User1 is eligible for the Application administrator role. User1 needs to configure a new connector group for an application proxy. What should you to activate the role for User1?

- A. the Microsoft Defender for Cloud Apps portal
B. the Microsoft 365 admin center

- C. the Azure Active Directory admin center
- D. the Microsoft 365 Defender portal

Answer: C

NEW QUESTION 235

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com that contains the resources shown in the following table. You create a user named Admin 1.

Name	Description
Au1	Administrative unit
CAPolicy1	Conditional Access policy
Package1	Access package

You need to ensure that Admin can enable Security defaults for contoso.com. What should you do first?

- A. Configure Identity Governance.
- B. Delete Package1.
- C. Delete CAPolicy1.
- D. Assign Admin1 the Authentication administrator role for Au1

Answer: D

Explanation:

To enable Security defaults for contoso.com, you should first sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator. Then, browse to Azure Active Directory > Properties and select Manage security defaults. Set the Enable security defaults toggle to Y select Save. After that, you can assign Admin1 the Identity Administrator role for Au1 to enable them to manage security defaults for the tenant.
<https://practical365.com/what-are-azure-ad-security-defaults-and-should-you-use-them/>

NEW QUESTION 238

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3. You need to configure the users as shown in the following table.

User	Configuration
User1	<ul style="list-style-type: none">User administrator roleDevice Administrators roleIdentity Governance Administrator role
User2	<ul style="list-style-type: none">Records Management roleQuarantine Administrator role group
User3	<ul style="list-style-type: none">Endpoint Security Manager roleIntune Role Administrator role

Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal 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.

Portals

Azure Active Directory admin center

Exchange admin center

Microsoft 365 compliance center

Microsoft Endpoint Manager admin center

SharePoint admin center

Answer Area

User1:

User2:

User3:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 239

- (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 241

- (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 242

- (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

Global administrator

Global reader

Reports reader

Security operator

Security reader

User administrator

Answer Area

User1:

Role

User2:

Role

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Roles

Global administrator

Global reader

Reports reader

Security operator

Security reader

User administrator

Answer Area

User1:

Global administrator

User2:

Global reader

NEW QUESTION 243

- (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 244

- (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 246

- (Exam Topic 4)

You have an Azure subscription.

From Entitlement management, you plan to create a catalog named Catalog1 that will contain a custom extension.

What should you create first and what should you use to distribute Catalog1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First create:

An Azure Automation account

A managed account

An Azure Automation account

An Azure logic app

Distribute Catalog1 by using:

A playbook

A playbook

A workflow

An access package

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

First create:

An Azure Automation account

A managed account

An Azure Automation account

An Azure logic app

Distribute Catalog1 by using:

A playbook

A playbook

A workflow

An access package

NEW QUESTION 248

- (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 pass-through authentication. Does this meet the goal?

- A. Yes
B. No

Answer: A

Explanation:

Reference:

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


NEW QUESTION 252

- (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?](#)

+ Add filters

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

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"/> User3	Member
<input type="checkbox"/> 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

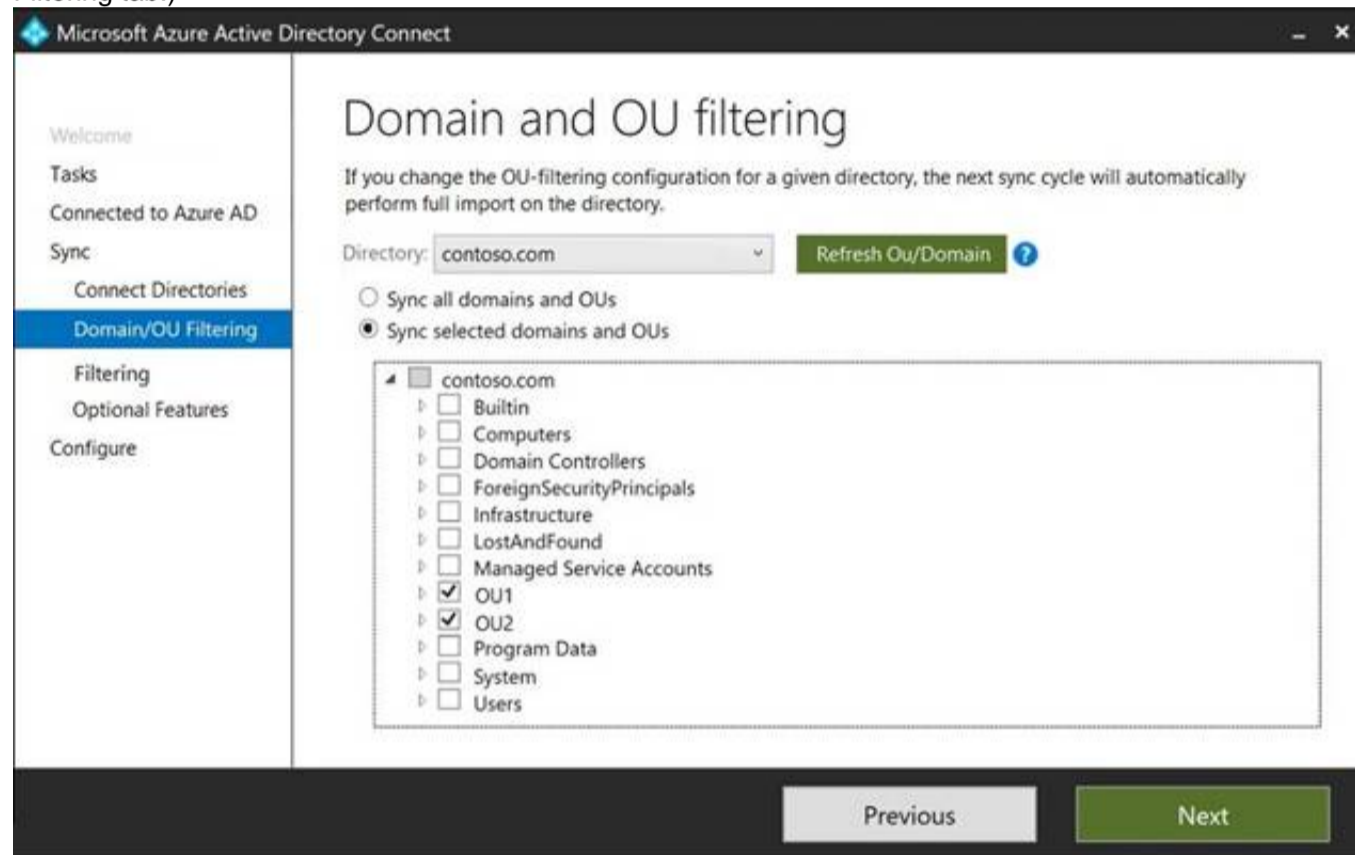
NEW QUESTION 255

- (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.

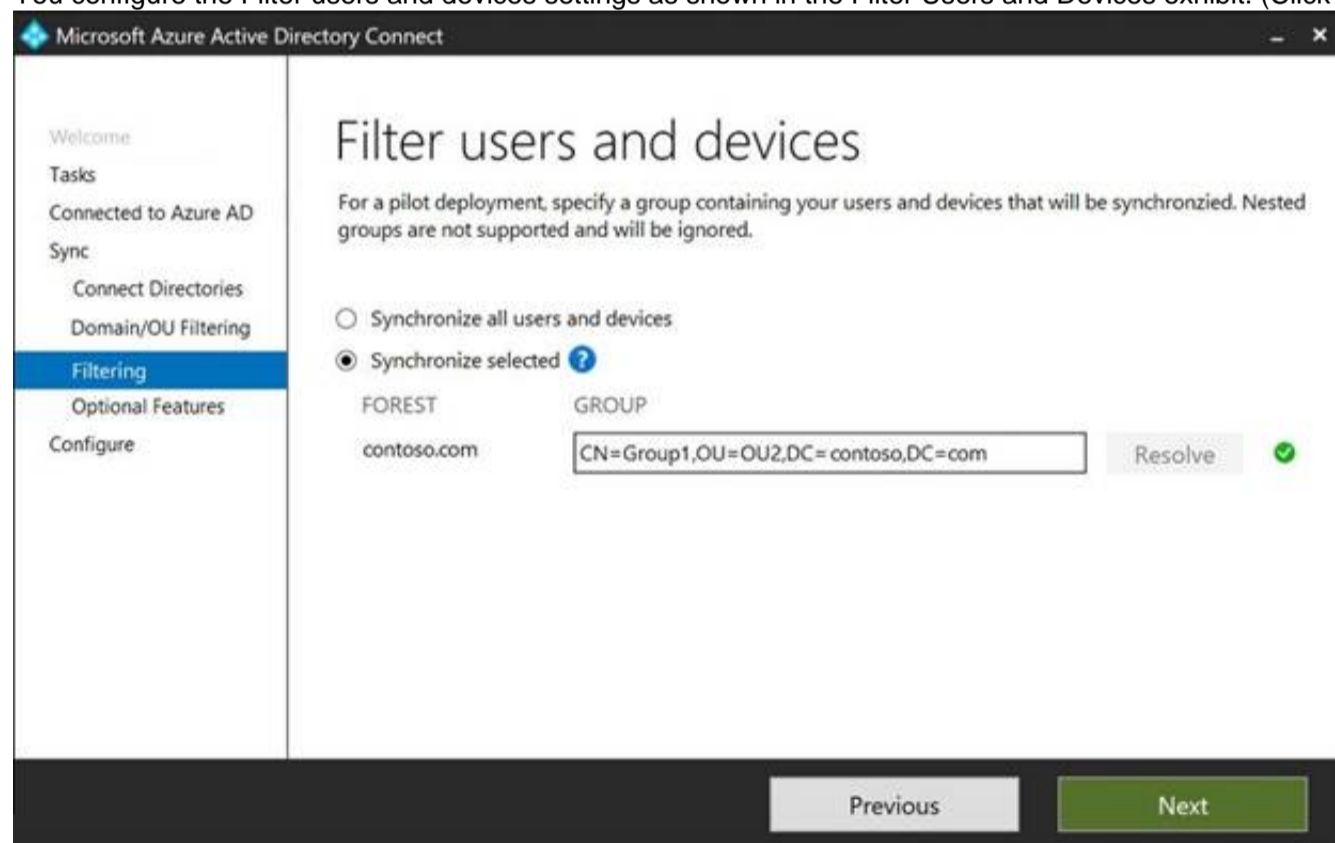
Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

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.)



The screenshot shows the 'Domain and OU filtering' configuration window in Microsoft Azure Active Directory Connect. The left sidebar has tabs: Welcome, Tasks, Connected to Azure AD, Sync, Connect Directories, **Domain/OU Filtering**, Filtering, Optional Features, and Configure. The main area is titled 'Domain and OU filtering' and includes a note: 'If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.' Below this, the 'Directory' is set to 'contoso.com' with a 'Refresh Ou/Domain' button. Two radio buttons are present: 'Sync all domains and OUs' (unselected) and 'Sync selected domains and OUs' (selected). A tree view shows the directory structure with 'contoso.com' expanded, listing various OUs. 'OU1' and 'OU2' are checked, while others are unchecked. At the bottom are 'Previous' and 'Next' buttons.

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



The screenshot shows the 'Filter users and devices' configuration window in Microsoft Azure Active Directory Connect. The left sidebar is the same as the previous exhibit, with the 'Filtering' tab selected. The main area is titled 'Filter users and devices' and includes a note: 'For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.' Below this, two radio buttons are present: 'Synchronize all users and devices' (unselected) and 'Synchronize selected' (selected). Under 'Synchronize selected', there are two input fields: 'FOREST' (containing 'contoso.com') and 'GROUP' (containing 'CN=Group1,OU=OU2,DC=contoso,DC=com'). A 'Resolve' button and a green checkmark are next to the GROUP field. At the bottom are 'Previous' and 'Next' buttons.

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 257

- (Exam Topic 4)
You have an Azure Active Directory Premium P2 tenant. You create a Log Analytics workspace.
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 Set-AzureADTenantDetail cmdlet.
- B. Create an Azure AD workbook.
- C. Modify the Diagnostics settings for Azure AD.
- D. Run the Get-AzureADAuditDirectoryLogs cmdlet.

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-lo>

NEW QUESTION 260

- (Exam Topic 4)
You have a Microsoft 365 tenant and an Active Directory domain named adatum.com. You deploy Azure AD Connect by using the Express Settings.
You need to configure self-service password reset (SSPR) to meet the following requirements:
> When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.
> Passwords must be synced between the tenant and the domain regardless of where the password was reset.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

From the Password reset blade in the Azure Active Directory admin center, configure:

Authentication methods

Notifications

Properties

Registration

From Azure AD Connect, enable:

Federation with Active Directory Federation Services (AD FS)

Pass-through authentication

Password hash synchronization

Password writeback

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

directory/authentication/concept-authentication-security-questions

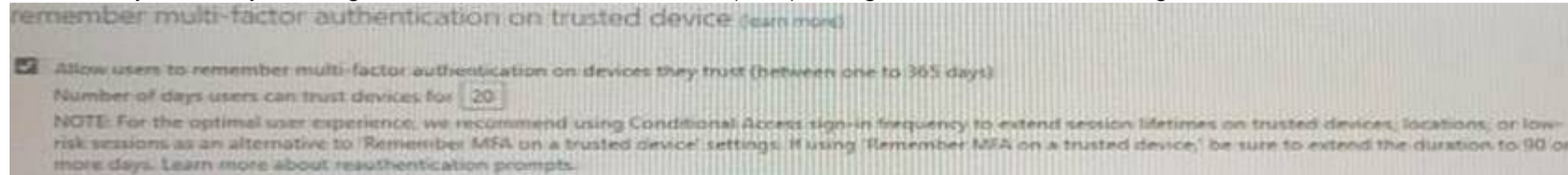
NEW QUESTION 264

- (Exam Topic 4)

You create the Azure Active Directory (Azure AD) users shown in the following table.

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.



The users authentication to Azure AD on their devices as shown in the following table.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

On February 26, 2021, what will the multi-factor auth status be for each user?

A)

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B)

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C)

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D)

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

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 271

- (Exam Topic 4)

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click the Exhibit tab.)

Custom smart logout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

You are evaluating the following passwords:

- > Pr0jectlitw@re
- > T@ilw1nd
- > C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

Answer: C

Explanation:

Reference:
<https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation>

NEW QUESTION 274

- (Exam Topic 4)

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

Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

For which resources can you create an access review?

- A. Group1, App1, Contributor, and Role1
- B. Hotel and Contributor only
- C. Group1, Role1, and Contributor only
- D. Group1 only

Answer: A

Explanation:

Access reviews require an Azure AD Premium P2 license.
 Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-access-reviews-overview>

NEW QUESTION 276

- (Exam Topic 4)

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resource-, by using conditional access policy. What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Configure password protection for Windows Server Active Directory.

Answer: B

NEW QUESTION 281

- (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 Amazon Web Services app connector. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 284

- (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. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

Answer: D

Explanation:

Reference:

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

NEW QUESTION 287

.....

Relate Links

100% Pass Your SC-300 Exam with ExamBible Prep Materials

<https://www.exambible.com/SC-300-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>