

## Exam Questions SC-300

Microsoft Identity and Access Administrator

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



### NEW QUESTION 1

- (Exam Topic 1)

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

What should you configure?

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

**Answer: B**

#### Explanation:

Reference:

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

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

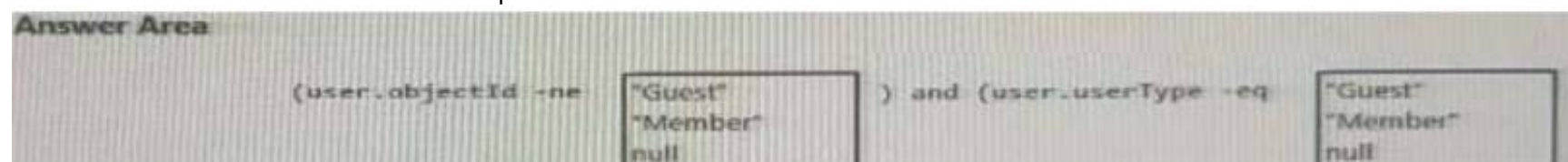
### NEW QUESTION 2

- (Exam Topic 1)

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

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

**Answer: C**

#### Explanation:

Reference:

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

#### NEW QUESTION 5

- (Exam Topic 1)

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

Azure AD tenant-level setting to modify:

Allow users to register application Users can consent to apps accessing company data on their behalf Users can request admin consent to apps they are unable to consent to
--

Role to assign to User1:

Application administrator Application developer Cloud application administrator
---

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Graphical user interface, text Description automatically generated

Reference:

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

#### NEW QUESTION 6

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 7

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 8

- (Exam Topic 1)

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

For on-premises applications:

Configure Cloud App Security policies. Modify the User consent settings for the enterprise applications. Publish the applications by using Azure AD Application Proxy.
--

For SharePoint Online:

Configure Cloud App Security policies. Modify the User consent settings for the enterprise applications. Publish an application by using Azure AD Application Proxy.
--

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

For on-premises applications:

<input type="checkbox"/> Configure Cloud App Security policies. <input type="checkbox"/> Modify the User consent settings for the enterprise applications. <input type="checkbox"/> Publish the applications by using Azure AD Application Proxy.
---

For SharePoint Online:

<input type="checkbox"/> Configure Cloud App Security policies. <input type="checkbox"/> Modify the User consent settings for the enterprise applications. <input type="checkbox"/> Publish an application by using Azure AD Application Proxy.
---

#### NEW QUESTION 9

- (Exam Topic 2)

You create a Log Analytics workspace.

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

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

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 10

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 10

- (Exam Topic 2)

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

- A. a policy set in Microsoft Endpoint Manager
- B. an app configuratfon 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 13

- (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 16

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

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

Default Setting State

Require justification on activation Yes Require ticket information on activation No On activation, require Azure MFA Yes Require approval to activate No  
 Approvers None

#### NEW QUESTION 21

- (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 26

- (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).

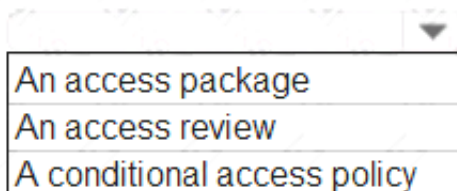
#### NEW QUESTION 29

- (Exam Topic 2)

You need to implement the planned changes and technical requirements for the marketing department. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

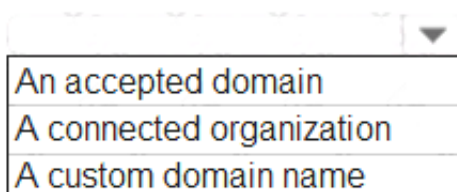
To configure user access:



A screenshot of a dropdown menu with the following options:

- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:



A screenshot of a dropdown menu with the following options:

- An accepted domain
- A connected organization
- A custom domain name

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Reference:

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

#### NEW QUESTION 33

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 36

- (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:

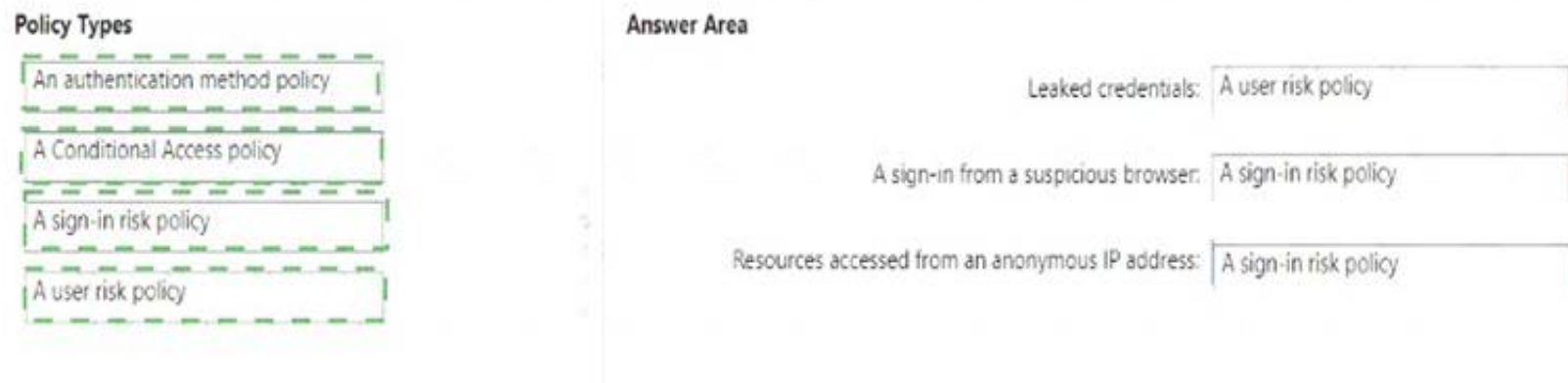
A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:



#### NEW QUESTION 39

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 42

- (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 46

- (Exam Topic 4)

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

You receive more than 100 email alerts each day for 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 create an assignment for the Insights at administrator role. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 47

- (Exam Topic 4)

You have an Azure AD tenant that contains a user named User1. User1 needs to manage license assignments and reset user passwords. Which role should you assign to User1?

- A. License administrator
- B. Helpdesk administrator
- C. Billing administrator
- D. User administrator

**Answer:** D

#### NEW QUESTION 51

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain that syncs to an Azure AD tenant. Users sign in to computers that run Windows 10 and are joined to the domain.

You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO). You need to configure the Windows 10 computers to support Azure AD Seamless SSO. What should you do?

- A. Modify the Local intranet zone settings

- B. Configure Sign-in options from the Settings app.
- C. Enable Enterprise State Roaming.
- D. Install the Azure AD Connect Authentication Agent.

**Answer: B**

#### NEW QUESTION 56

- (Exam Topic 4)

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

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

You have a Microsoft 365 tenant.

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

#### Create an access review

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

**Review name \*** Admin review ✓

**Description ⓘ**

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

**Frequency** Monthly ✓

**Duration (in days) ⓘ** 14

**End ⓘ** **Never** End by Occurrences

**Number of times** 0

**End date** 01/17/2021

**Users**

**Scope** ☒ Everyone

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

**Reviewers**

**Reviewers** (Preview) Manager ✓

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

▼ Upon completion settings

**Start**

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

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

Solution: You set Reviewers to Member (self).

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### NEW QUESTION 59

- (Exam Topic 4)

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

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

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

What should you use?

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



D. the Sec-MsolUserLicense cmdlet

**Answer:** C

**Explanation:**

Reference:

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

### NEW QUESTION 63

- (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

**Include**      Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest users (preview) ⓘ

☐ Directory roles (preview) ⓘ

☒ Users and groups

Select ⓘ >

1 user

US User1  
user1@sk200922outlook.onm...

**Enable policy**

Report-only   **On**   Off

Create

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

NOTE: Each correct selection is worth one point.

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

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

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

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

## NEW QUESTION 68

- (Exam Topic 4)

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

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

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method. Which users must use security questions when resetting their password?

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

**Answer: B**

## NEW QUESTION 70

- (Exam Topic 4)

Your company purchases 2 new Microsoft 365 ES subscription and an app named App. You need to create a Microsoft Defender for Cloud Apps access policy for App1.

What should you do you first? (Choose Correct Answer based on Microsoft Identity and Access Administrator at microsoft.com)

- Configure a Token configuration for App1.
- Add an API permission for App.
- Configure a Conditional Access policy to use app-enforced restrictions.
- Configure a Conditional Access policy to use Conditional Access App Control.

**Answer: C**

**Explanation:**

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

To create a Microsoft Defender for Cloud Apps access policy for App1, you should configure a Conditional Access policy to use app-enforced restrictions. This will allow you to control access to your cloud apps based on conditions such as user, device, location, and app state. You can also use app-enforced restrictions to control access to your cloud apps based on the state of the app, such as whether it's running on a managed or unmanaged device.

## NEW QUESTION 71

- (Exam Topic 4)

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

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

In Azure AD Identity Protection, you configure a user risk policy that has the following settings:

- Assignments: o Users: Group1
- o User risk: Low and above

• Controls:

o Access: Block access

• Enforce policy: On

In Azure AD Identity Protection, you configure a sign-in risk policy that has the following settings:

- Assignments: o Users: Group2

o Sign-in risk: Low and above

• Controls:

o Access: Require multi-factor authentication

• Enforce policy. On the following settings: ng settings:

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 from an anonymous IP address.	<input type="radio"/>	<input type="radio"/>
User2 can sign in from an anonymous IP address.	<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 from an anonymous IP address.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in from an anonymous IP address.	<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 72

- (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 73

- (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 75

- (Exam Topic 4)

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

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Application Administrator

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

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

**Answer:** C

#### NEW QUESTION 80

- (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 81

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

Users authorize third-party cloud apps to access their data.

You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.

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

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

**Answer:** C

### NEW QUESTION 83

- (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 85

- (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 87

- (Exam Topic 4)

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

You need to review the Azure AD sign-ins log to investigate sign ins that occurred in the past. For how long does Azure AD store events in the sign-in log?

- A. 14 days
- B. 30 days
- C. 90 days
- D. 365 days

**Answer: B**

#### NEW QUESTION 88

- (Exam Topic 4)

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

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

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text, application Description automatically generated

- > Create an app registration:

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

- > Grant admin consent:

Higher-privileged permissions require administrator consent.

- > Add app permissions:

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

Reference:

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

#### NEW QUESTION 90

- (Exam Topic 4)

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

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

You have a Microsoft 365 tenant.

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

## Create an access review

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

Review name \*

Description

Start date \*

Frequency

Duration (in days)

End ☐ Never ☐ End by ☐ Occurrences

Number of times

End date

Users

Scope ☒ Everyone

Review role membership (permanent and eligible) \*

[Application Administrator and 72 others](#)

Reviewers

Reviewers

(Preview) Fallback reviewers

Upon completion settings

Start

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

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

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

- A. Yes
- B. No

Answer: A

### Explanation:

Reference:

D18912E1457D5D1DDCBD40AB3BF70D5D

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

## NEW QUESTION 92

- (Exam Topic 4)

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

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

You have a Microsoft 365 ES subscription. You create a user named User1.

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

- A. Yes
- B. No

Answer: B

## NEW QUESTION 97

- (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 99**

- (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 102**

- (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 106**

- (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 107

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant. You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. atypical travel
- D. leaked credentials

**Answer: D**

### Explanation:

Reference:

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

## NEW QUESTION 112

- (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 113

- (Exam Topic 4)

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

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

For which users can you configure the Job title property and the Usage location property in Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Job title property: ☐ User2 only  
☐ User1 and User2 only  
☐ User2 and User3 only  
☐ User1, User2, and User3

Usage location property: ☐ User2 only  
☐ User1 and User2 only  
☐ User2 and User3 only  
☐ User1, User2, and User3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Job title property: ☐ User2 only  
☐ User1 and User2 only  
☐ User2 and User3 only  
☒ User1, User2, and User3

Usage location property: ☐ User2 only  
☐ User1 and User2 only  
☐ User2 and User3 only  
☒ User1, User2, and User3

### NEW QUESTION 115

- (Exam Topic 4)

You have an Azure AD tenant that contains a user named User1 and the conditional access policies shown in the following table.

Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

You need to evaluate which policies will be applied User1 when User1 attempts to sign-in from various IP addresses. Which feature should you use?

- A. Access reviews
- B. Identity Secure Score
- C. The What If tool
- D. the Microsoft 365 network connectivity test tool

**Answer:** C

### NEW QUESTION 117

- (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 121

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table. The users have the devices shown in the following table. You create the following two Conditional Access policies:

- Name: CAPolicy1
- Assignments



o Users or workload identities: Group 1  
o Cloud apps or actions: Office 365 SharePoint Online o Conditions  
Filter for devices: Exclude filtered devices from the policy Rule syntax: device.displayName -starts With "Device\*"  
o Access controls Grant: Block access  
Session: 0 controls selected o Enable policy: On

- Name: CAPolicy2
- Assignments

o Users or workload identities: Group2  
o Cloud apps or actions: Office 365 SharePoint Online o Conditions: 0 conditions selected

- Access controls

o Grant: Grant access  
Require multifactor authentication o Session:  
0 controls selected

- Enable policy: On

All users confirm that they can successfully authenticate using MFA.  
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

NEW QUESTION 125

- (Exam Topic 4)

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

Name	Role
User1	None
User2	Privileged Authentication Administrator
User3	Global Administrator

In Azure AD Privileged Identity Management (PIM), you configure the Global Administrator role as shown in the following exhibit.

Edit

Setting	State
Activation maximum duration (hours)	1 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

#### Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

User 1 is eligible for the Global Administrator role.

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 requires Azure Multi-Factor Authentication (MFA) to activate the Global Administrator role.	<input type="radio"/>	<input type="radio"/>
User2 can approve all activation requests for the Global Administrator role.	<input type="radio"/>	<input type="radio"/>
User2 and User3 can edit the Global Administrator role assignment.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

#### Answer Area

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can approve all activation requests for the Global Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
User2 and User3 can edit the Global Administrator role assignment.	<input type="radio"/>	<input checked="" type="radio"/>

#### NEW QUESTION 127

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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

Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

The domain controllers are prevented from communicating to the internet. You implement Azure AD Password Protection on Server1 and Server2. You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails. What should you implement on Server4?

- A. Azure AD Connect
- B. Azure AD Application Proxy
- C. Password Change Notification Service (PCNS)
- D. the Azure AD Password Protection proxy service

**Answer: D**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premisesdep>

**NEW QUESTION 129**

- (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 134**

- (Exam Topic 4)

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

**Expiration**

Access package assignments expire ⓘ

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

Assignments expire after (number of days)

365

[Show advanced expiration settings](#)

**Access Reviews**

Require access reviews \*

**Yes** No

Starting on ⓘ

03/01/2022 ⓘ

Review frequency ⓘ

Annually **Bi-annually** Quarterly Monthly Weekly

Duration (in days) ⓘ

90 ✓

Maximum 175

Reviewers ⓘ

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

You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege.

Which role should you assign to User1?

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

**Answer: A**

**NEW QUESTION 135**

- (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 137

- (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	Answer Area
Delete the contoso.onmicrosoft.com domain.	<div> <div>⬅️</div> <div>➡️</div> <div>⬆️</div> <div>⬇️</div> </div>
Register a custom domain name of contoso.com.	
Set the domain to primary.	
Create a new TXT record in DNS.	
Verify the domain name.	

- 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 140**

- (Exam Topic 4)

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

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

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

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

**Answer:** C

**NEW QUESTION 143**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

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

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

**Answer:** A

**NEW QUESTION 145**

- (Exam Topic 4)

Your company has a Microsoft 365 tenant.

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

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

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

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

NOTE: Each correct selection is worth one point.



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

▼

An app registration in Azure AD

Azure AD Application Proxy

An enterprise application in Azure AD

A managed identity in Azure AD

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

▼

Azure AD Application Proxy

A compliance policy

A conditional access policy

An OAuth policy

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 149**

- (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**

**Answer Area**

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.

⬅

➡

⬆

⬇

- 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 152**

- (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 155

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the following:

- An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
- A Microsoft SharePoint Online site named Site1
- A Microsoft Teams team named Team1

You need to create an entitlement management workflow to manage Site1 and Team1. What should you do first?

- A. Create an access package.
- B. Create a catalog.
- C. Create an administrative unit.
- D. Configure an app registration.

Answer: A

#### NEW QUESTION 156

- (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 Google Workspace app connector. Does this meet the goal?

- A. Yes
- B. No

Answer: B

#### NEW QUESTION 159

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Object type:

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

Role:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

Object type:

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

Role:

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

### NEW QUESTION 163

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)

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

Name \*

Require MFA for all users ✓

Assignments

Users and groups ⓘ

All users >

Cloud apps or actions ⓘ

All cloud apps >

Conditions ⓘ

1 condition selected >

Access controls

Grant ⓘ

0 controls selected >

Session ⓘ

0 controls selected >

Enable policy

Report-only On Off

Create

Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ

[See list of approved client apps](#)

☐ Require app protection policy ⓘ

[See list of policy protected client apps](#)

☐ Require password change (Preview) ⓘ

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)



Privileged Identity Management > ContosoAzureAD > User Administrator >

### Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

**Activation**

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s), 0 Group

**Assignment**

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

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

### User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

**Eligible assignments** Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	Membership
User Administrator				
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin3	Admin3@m365x629615.onmicrosoft.com	User	Directory	Direct

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

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

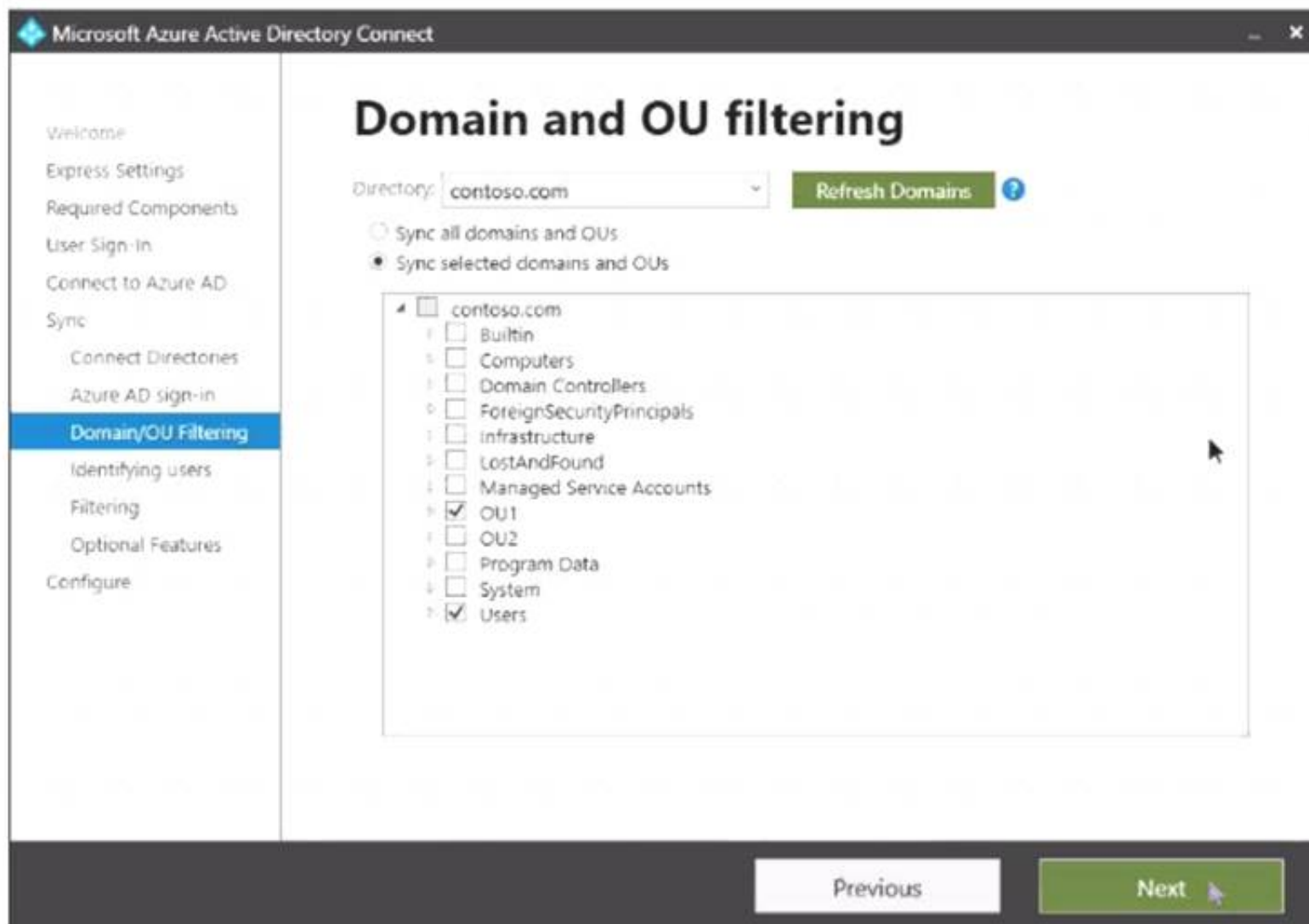
Explanation:  
Yes Yes Yes

NEW QUESTION 166  
- (Exam Topic 4)

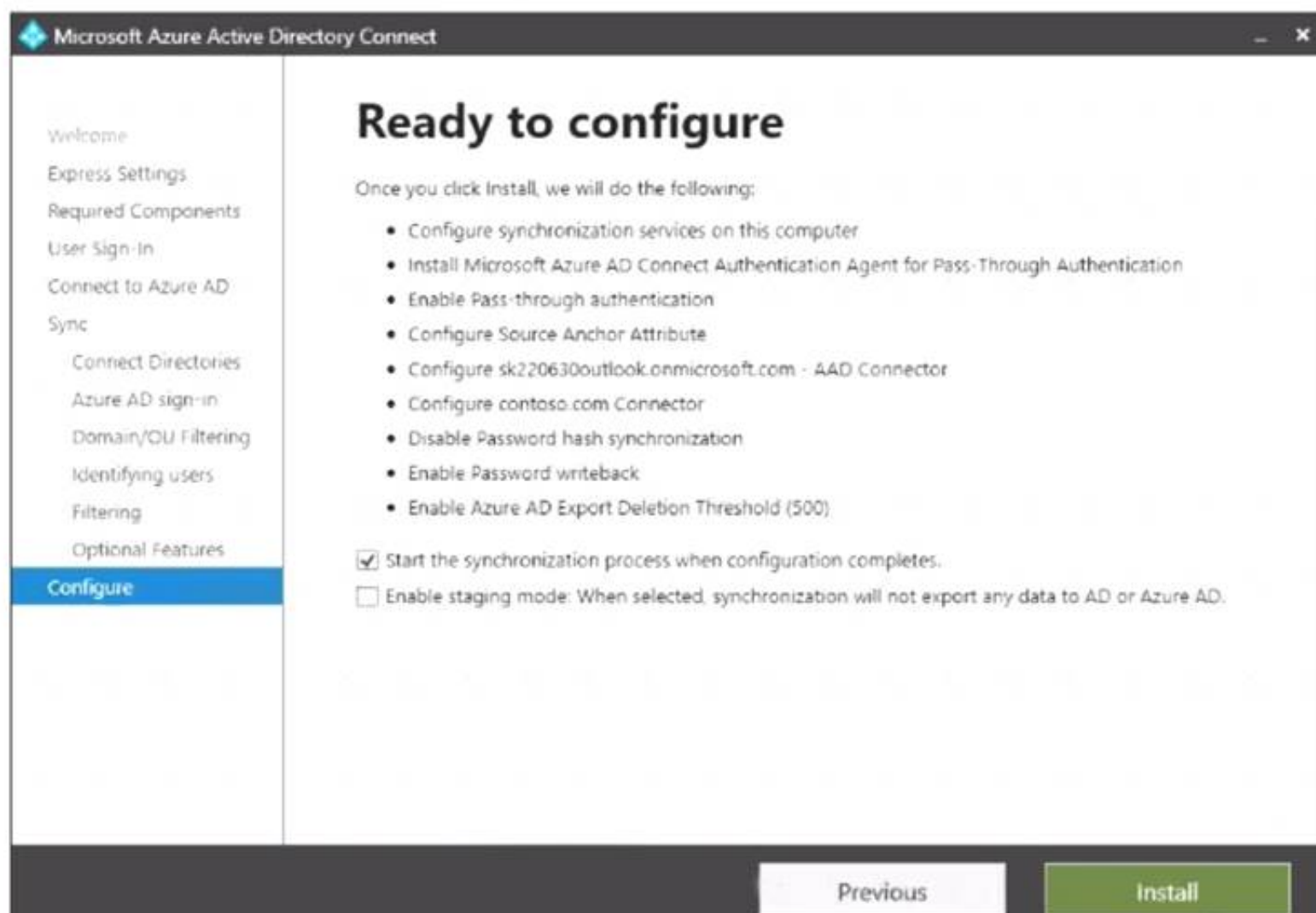
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

Name	Organizational unit (OU)
User1	OU1
User2	OU2

In Azure AD Connect. Domain/OU Filtering is configured as shown in the following exhibit.



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



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 use self-service password reset (SSPR) to reset his password.	<input type="radio"/>	<input type="radio"/>
If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	<input type="radio"/>	<input type="radio"/>
User2 can be added to a Microsoft SharePoint Online site as a member.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area		
Statements	Yes	No
User1 can use self-service password reset (SSPR) to reset his password.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can be added to a Microsoft SharePoint Online site as a member.	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 171

- (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 176

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps. You need to group related apps into categories in the My Apps portal.

What should you create?

- A. tags  
B. collections  
C. naming policies  
D. dynamic groups

Answer: B

Explanation:

Reference:

<https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps-portal-2dae6b8a>

#### NEW QUESTION 177

- (Exam Topic 4)

You plan to deploy a new Azure AD tenant.

Which multifactor authentication (MFA) method will be enabled by default for the tenant?

- A. Microsoft Authenticator

- B. SMS
- C. voice call
- D. email OTP

**Answer:** B

#### NEW QUESTION 179

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a web app named App1. Guest users are regularly granted access to App1.

You need to ensure that the guest users that have NOT accessed App1 during the past 30 days have their access removed the solution must minimize administrative effort.

What should you configure?

- A. a compliance policy
- B. an access review for application access
- C. a guest access review
- D. a Conditional Access policy

**Answer:** C

#### NEW QUESTION 182

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that has the default App registrations settings. The tenant contains the users shown in the following table.

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD. You need to identify who can assign users to App1, and who can register App2 in Azure AD.

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

Can assign users to App1:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users> <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

#### NEW QUESTION 186

- (Exam Topic 4)

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

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

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

**Answer:** B

#### NEW QUESTION 190

- (Exam Topic 4)

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

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

You have the app registrations shown in the following table.

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

A company policy prevents changes to user permissions.

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

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

**Answer: B**

### NEW QUESTION 193

- (Exam Topic 4)

You have an Azure subscription.

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Role1:

Microsoft.App  
Microsoft.Compute  
Microsoft.Management  
Microsoft.Security

Role2:

Microsoft.App  
Microsoft.Compute  
Microsoft.Network  
Microsoft.Security

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Role1:

Microsoft.App  
Microsoft.Compute  
Microsoft.Management  
Microsoft.Security

Role2:

Microsoft.App  
Microsoft.Compute  
Microsoft.Network  
Microsoft.Security



#### NEW QUESTION 198

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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

What should you create?

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

**Answer: C**

#### Explanation:

Reference:

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

#### NEW QUESTION 203

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Service to install on Server4:

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

Rule to configure on Firewall1:

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

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Reference:

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

#### NEW QUESTION 205

- (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 209

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.

You create an Azure Sentinel instance and configure the Azure Active Directory connector.



You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection. What should you do first?

- A. Add an Azure Sentinel data connector.
- B. Configure the Notify settings in Azure AD Identity Protection.
- C. Create an Azure Sentinel playbook.
- D. Modify the Diagnostics settings in Azure AD.

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection>

**NEW QUESTION 211**

- (Exam Topic 4)

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

Name	Role
User1	Security administrator
User2	Privileged authentication administrator
User3	Service support administrator

User2 reports that he can only configure multi-factor authenticating (MFA) to use the Microsoft Authenticator app.

You need to ensure that User2 can configure alternate MFA methods.

Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.

**Answer Area**

Configuration:

▼

Enable access reviews.

Enable Azure AD Privileged Identity Management (PIM).

Modify security defaults.

User:

▼

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

User2 and User3 only

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area

Configuration:

▼

Enable access reviews.
Enable Azure AD Privileged Identity Management (PIM).
Modify security defaults.

User:

▼

User1 only
User2 only
User3 only
User1 and User2 only
User1 and User3 only
User2 and User3 only

### NEW QUESTION 216

- (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.

☐ ☐

Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.

☐ ☐

Admin2 is a local administrator on Device3.

☐ ☐

- 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 218

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

#### Answer Area

User1:

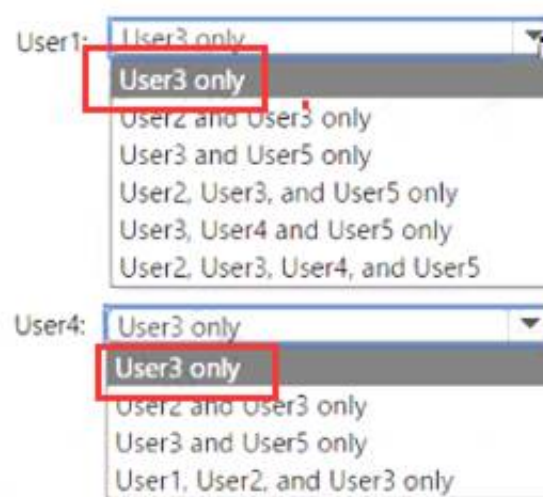
User4:

- A. Mastered  
 B. Not Mastered

Answer: A

#### Explanation:

## Answer Area



### NEW QUESTION 222

- (Exam Topic 4)

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

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

User1 is the owner of Group1.

You create an access review that has the following settings:

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

Which users can perform access reviews for User3?

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

**Answer: B**

### NEW QUESTION 223

- (Exam Topic 4)

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

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

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

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

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

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

- A. Yes
- B. No

**Answer: B**

#### Explanation:

Reference:

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

### NEW QUESTION 226

- (Exam Topic 4)

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

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

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

Which role should you assign to Admin1?

- A. Application developer in Azure AD
- B. App Configuration Data Owner for Subscription1
- C. Managed Application Contributor for Subscription1
- D. Cloud application administrator in Azure AD

**Answer: A**

#### Explanation:

Reference:

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



#### NEW QUESTION 231

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain that sync to an Azure Active Directory (Azure AD) tenant. The tenant contains the 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 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 user can sign in to Azure AD?

- A. User1 only
- B. User1 and User 3 only
- C. User1, and User2 only
- D. User1, User2, and User3

**Answer: B**

#### NEW QUESTION 235

- (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 238

- (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 242

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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

- Identity sign-ms by users who are suspected of having leaked credentials.

- Flag the sign-ins as a high-risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications. What should you use? To answer, select the appropriate options in the answer area.

To classify leaked credentials as high-risk, use:

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

To trigger remediation, use:

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

To mitigate the risk, select:

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

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

To classify leaked credentials as high-risk, use:

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

To trigger remediation, use:

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

To mitigate the risk, select:

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

#### NEW QUESTION 247

- (Exam Topic 4)

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

In the tenant, you create the groups shown in the following table.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

Which members can you add to GroupA and GroupB? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

GroupA:

User1 only
User1 and Group1 only
User1, Group1, and Group2 only
User1, Group1, and Group4 only
User1, Group1, Group2, and Group3 only
User1, Group1, Group2, Group3, and Group4

GroupB:

User1 only
User1 and Group4 only
User1, Group1, and Group4 only
User1, Group1, Group2, and Group4 only
User1, Group1, Group2, Group3, and Group4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/>

#### NEW QUESTION 250

- (Exam Topic 4)

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

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

What should you configure?

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

**Answer:** C

**Explanation:**

Reference:

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

#### NEW QUESTION 252

- (Exam Topic 4)

HOTSPOT

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



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

## Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

### Activation

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

### Assignment

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

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

NOTE: Each correct selection is worth one point.

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

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

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Reference:

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

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

#### NEW QUESTION 256

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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



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

NOTE: Each correct selection is worth one point.

Tool to use:

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

Policy type to create:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

#### NEW QUESTION 261

- (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 265

- (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 270

- (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 272

- (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 273

- (Exam Topic 4)

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

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

You have a Microsoft 365 E5 subscription. You create a user named User1.

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

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 276

- (Exam Topic 4)

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

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

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

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

**NEW QUESTION 278**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to be notified if a user downloads more than 50



files in one minute from Site1.

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

- A. session policy
- B. anomaly detection policy
- C. activity policy
- D. file policy

Answer: C

#### NEW QUESTION 279

- (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

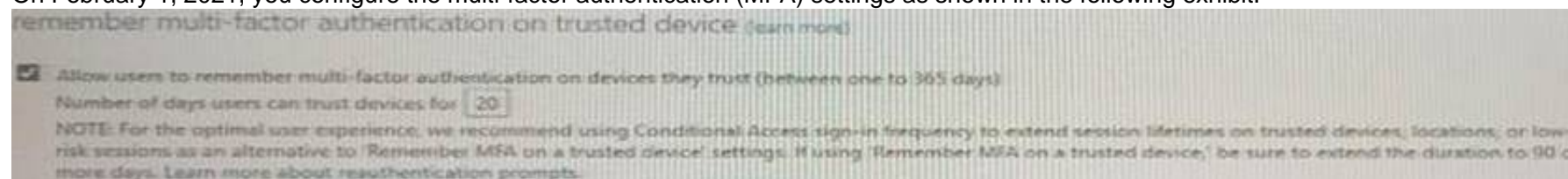
#### NEW QUESTION 282

- (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 285

- (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 290

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 293

- (Exam Topic 4)

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

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

You have the locations shown in the following table.

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

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

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

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

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

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

© Session: 0 controls selected

- Enable policy: On

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 295

- (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 297

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

## Money Back Guarantee

### SC-300 Practice Exam Features:

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