

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

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

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

|                               |
|-------------------------------|
| Global administrator          |
| Privileged role administrator |
| Security administrator        |
| User access administrator     |

To manage Azure built-in role assignments, use:

|                               |
|-------------------------------|
| Global administrator          |
| Privileged role administrator |
| Security administrator        |
| User access administrator     |

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 2

- (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 3

- (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 4

- (Exam Topic 3)

You need to modify the settings of the User administrator role to meet the technical requirements. Which two actions should you perform for the role? Each correct

answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Select Require justification on activation
- B. Set all assignments to Active
- C. Set all assignments to Eligible
- D. Modify the Expire eligible assignments after setting.
- E. Select Require ticket information on activation.

**Answer:** AB

#### NEW QUESTION 5

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 6

- (Exam Topic 4)

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

| Name | Description                        |
|------|------------------------------------|
| OU1  | Syncs with Azure AD                |
| OU2  | Does <b>NOT</b> sync with Azure AD |

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

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

NOTE: Each correct selection is worth one point.

#### Answer Area

Location:

Azure AD  
OU1  
OU2

Role:

Billing Administrator  
Global Administrator  
Owner  
Privileged Role Administrator

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area

Location:

▼

Azure AD

OU1

OU2

Role:

▼

Billing Administrator

Global Administrator

Owner

Privileged Role Administrator

### NEW QUESTION 7

- (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 8

- (Exam Topic 4)

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

A corporate security policy states the following:

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

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

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

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

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

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

**Answer:** C

#### Explanation:

Reference:

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

### NEW QUESTION 9

- (Exam Topic 4)

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 10

- (Exam Topic 4)

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

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

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

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

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

Solution: You configure Azure AD Password Protection. Does this meet the goal?

A. Yes

B. No

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 4)

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

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

A. 14 days

B. 30 days

C. 90 days

D. 365 days

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-dataretention# how-long-does-azure-ad-store-the-data>

#### NEW QUESTION 15

- (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 set Reviewers to Member (self).

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

## NEW QUESTION 16

- (Exam Topic 4)

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

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

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

Three apps have the following Properties settings:

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

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

What should you do from App3?

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

**Answer: A**

**Explanation:**

Reference:

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

#### NEW QUESTION 19

- (Exam Topic 4)

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

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

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

Answer: A

#### NEW QUESTION 23

- (Exam Topic 4)

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

## New

Conditional access policy

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

Name \*

Policy1 ✓

### Assignments

Users and groups ⓘ  
 Specific users included >

Cloud apps or actions ⓘ  
 All cloud apps >

Conditions ⓘ  
 0 conditions selected >

### Access controls

Grant ⓘ  
 0 controls selected >

Session ⓘ  
 0 controls selected >

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

### Include

Exclude

- ☐ None
- ☐ All users
- ☒ Select users and groups

- ☐ All guest users (preview) ⓘ
- ☐ Directory roles (preview) ⓘ
- ☒ Users and groups

Select ⓘ

1 user >

US User1  
 user1@sk200922outlook.onm... ⋮

Enable policy

Report-only On Off

Create

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

NOTE: Each correct selection is worth one point.

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

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

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

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

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

## NEW QUESTION 25

- (Exam Topic 4)

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

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

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

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

Does this meet the goal?

- A. Yes  
B. No

**Answer: B**

## NEW QUESTION 26

- (Exam Topic 4)

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

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

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

- A. sign-ins in JSON format  
B. sign-ins in CSV format  
C. audit logs in JSON format  
D. audit logs in CSV format

**Answer: C**

**Explanation:**

Reference:

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

## NEW QUESTION 30

- (Exam Topic 4)

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

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

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

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



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

Who can review admin consent requests ☐

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

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

Selected users will receive request expiration reminders ☒ Yes ☐ No

Consent request expires after (days)

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

Which users can review and approve the admin consent requests?

- A. Admm1 only
- B. Admm1 and Admin2 only
- C. Admm1 Admm2 and Admin3 only
- D. Admin1, Admin2. and User1 only
- E. Admm1 Admm2. Admm3, and User1

**Answer: B**

### NEW QUESTION 33

- (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 34

- (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 39

- (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 40

- (Exam Topic 4)

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM). You need to identify users that are eligible for the Cloud Application Administrator role. Which blade in the Privileged Identity Management settings should you use?

- A. Azure resources
- B. Privileged access groups
- C. Review access
- D. Azure AD roles

**Answer: D**

#### NEW QUESTION 42

- (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 46

- (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 49

- (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 50

- (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 54**

- (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 55**

- (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 57

- (Exam Topic 4)  
You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User1, and User3,  
You create a group named Group1. You add User2 and User3 to Group1.  
You configure a role in Azure AD Privileged identity Management (PIM) as shown in the application administrator exhibit. (Click the application Administrator tab.)

| Role setting details - Application Administrator        |                         |
|---|-------------------------|
| Privileged Identity Management   Azure AD roles         |                         |
| Edit  |                         |
| Activation  |                         |
| Setting   | State                   |
| Activation maximum duration (hours)                     | 5 hour(s)               |
| Require justification on activation                     | Yes                     |
| Require ticket information on activation                | No                      |
| Require approval to activate                            | Yes                     |
| Approvers   | 0 Member(s), 1 Group(s) |
| Assignment  |                         |
| Setting   | State                   |
| Allow permanent eligible assignment                     | No                      |
| Expire eligible assignments after                       | 3 month(s)              |
| Allow permanent active assignment                       | No                      |
| Expire active assignments after                         | 1 month(s)              |
| Require Azure Multi-Factor Authentication on activation | No                      |
| Require justification on active assignment              | Yes                     |



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

### Add assignments

Privileged Identity Management | Azure AD roles

Membership

Setting

Assignment type ⓘ  

Eligible

Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts \*

01/01/2021

12:00:00 AM

Assignment ends \*

01/31/2021

11:59:00 PM

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 62

- (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 66

- (Exam Topic 4)

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

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

**Answer:** C

**Explanation:**

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods> <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

**NEW QUESTION 68**

- (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 71

- (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 75

- (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<br>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 80

- (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.<br>Enable Azure AD Privileged Identity Management (PIM).<br>Modify security defaults. |
|--|

User:

|  |
|--|
| User1 only<br>User2 only<br>User3 only<br>User1 and User2 only<br>User1 and User3 only<br>User2 and User3 only |
|--|

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

### Answer Area

Configuration:

|   |
|---|
| Enable access reviews.<br>Enable Azure AD Privileged Identity Management (PIM).<br><b>Modify security defaults.</b> |
|---|

User:

|   |
|---|
| <b>User1 only</b><br>User2 only<br>User3 only<br>User1 and User2 only<br>User1 and User3 only<br>User2 and User3 only |
|---|

### NEW QUESTION 85

- (Exam Topic 4)

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

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

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

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

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



NOTE: Each correct selection is worth one point.

Answer Area

User1:

User3 only  
 User2 and User3 only  
 User3 and User5 only  
 User2, User3, and User5 only  
 User3, User4 and User5 only  
 User2, User3, User4, and User5

User4:

User3 only  
 User2 and User3 only  
 User3 and User5 only  
 User1, User2, and User3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:

User3 only  
 User2 and User3 only  
 User3 and User5 only  
 User2, User3, and User5 only  
 User3, User4 and User5 only  
 User2, User3, User4, and User5

User4:

User3 only  
 User2 and User3 only  
 User3 and User5 only  
 User1, User2, and User3 only

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 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 93

- (Exam Topic 4)

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

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

The subscription contains the users shown in the following table.

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

On June1, Admin4 performs the following actions:

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

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

### Answer Area

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

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

### Answer Area

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

### NEW QUESTION 96

- (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 99

- (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 100

- (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 103

- (Exam Topic 4)

HOTSPOT

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



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

## Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

### Activation

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

### Assignment

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

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

NOTE: Each correct selection is worth one point.

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

- 8 hours
- 15 days
- 1 month

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

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

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Reference:

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

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

#### NEW QUESTION 106

- (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 109

- (Exam Topic 4)

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

| User  | Configuration   |
|-------|---|
| User1 | <ul style="list-style-type: none"> <li>User administrator role</li> <li>Device Administrators role</li> <li>Identity Governance Administrator role</li> </ul> |
| User2 | <ul style="list-style-type: none"> <li>Records Management role</li> <li>Quarantine Administrator role group</li> </ul>  |
| User3 | <ul style="list-style-type: none"> <li>Endpoint Security Manager role</li> <li>Intune Role Administrator role</li> </ul>                                      |

Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

| Portals                                 | Answer Area                 |
|---|-----------------------------|
| Azure Active Directory admin center     |                             |
| Exchange admin center                   | User1: <input type="text"/> |
| Microsoft 365 compliance center         | User2: <input type="text"/> |
| Microsoft Endpoint Manager admin center | User3: <input type="text"/> |
| SharePoint admin center                 |                             |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated



#### NEW QUESTION 112

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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

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

Which policy type should you create?

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

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 114

- (Exam Topic 4)

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

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

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

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

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

Solution: You configure pass-through authentication. Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

#### Explanation:

Reference:

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

#### NEW QUESTION 118

- (Exam Topic 4)

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

You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc. Fabrikam uses a domain named fabrikam.com.

Fabrikam users must be removed automatically from the tenant when access is no longer required. You need to configure the following settings:

- Block external user from signing in to this directory: No
- Remove external user: Yes
- Number of days before removing external user from this directory: 90

What should you configure on the Identity Governance blade?

- A. Access packages
- B. Entitlement management settings
- C. Terms of use
- D. Access reviews setting

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 122

- (Exam Topic 4)

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

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

Dashboard > ContosoAzureAD > Department1 Administrative Unit

## Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory


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

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

Search users

Add filters

2 users found

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

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

Dashboard > ContosoAzureAD > Department1 Administrative Unit

## Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

+ Add Remove Refresh Columns Preview features Got feedback?

Search groups

Add filters

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

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

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

## User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

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

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

Dashboard > ContosoAzureAD > Groups > Group2

## Group2 | Members

Group

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

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

Direct members

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

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

| Statements   | Yes                   | No                    |
|--|-----------------------|-----------------------|
| Admin1 can reset the passwords of User3 and User4. | <input type="radio"/> | <input type="radio"/> |
| Admin1 can add User1 to Group 2                    | <input type="radio"/> | <input type="radio"/> |
| Admin 2 can reset the password of User1.           | <input type="radio"/> | <input type="radio"/> |

- A. Mastered  
 B. Not Mastered

Answer: A

**Explanation:**

Reference:

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

**NEW QUESTION 125**

- (Exam Topic 4)

You create a new Microsoft 365 E5 tenant.

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

What should you configure?

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

Answer: A

**NEW QUESTION 129**

- (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.)

Microsoft Azure Active Directory Connect

Welcome

Tasks

Connected to Azure AD

Sync

Connect Directories

**Domain/OU Filtering**

Filtering

Optional Features

Configure

## Domain and OU filtering

If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.

Directory:

☐ Sync all domains and OUs  
☒ Sync selected domains and OUs

- contoso.com
  - ☐ Builtin
  - ☐ Computers
  - ☐ Domain Controllers
  - ☐ ForeignSecurityPrincipals
  - ☐ Infrastructure
  - ☐ LostAndFound
  - ☐ Managed Service Accounts
  - ☒ OU1
  - ☒ OU2
  - ☐ Program Data
  - ☐ System
  - ☐ Users



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 130

- (Exam Topic 4)

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

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

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

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

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

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

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

Group1:

1

500

525

Group2:

1

100

295

395

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Group1:

1

500

525

Group2:

1

100

295

395

NEW QUESTION 131

.....



## 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