

## SC-300 Dumps

### Microsoft Identity and Access Administrator

<https://www.certleader.com/SC-300-dumps.html>



### NEW QUESTION 1

- (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:

- ☐ 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.

### 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 Azure Sentinel data connectors.
- D. Add an Azure Sentinel playbook.

**Answer: A**

### NEW QUESTION 3

- (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.

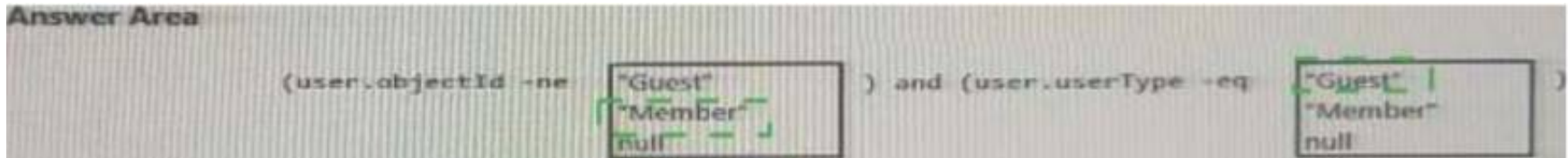
**Answer Area**

(user.objectId -ne "Guest"  
"Member"  
null) and (user.userType -eq "Guest"  
"Member"  
null)

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



#### NEW QUESTION 4

- (Exam Topic 3)

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

What should you do first?

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

**Answer: D**

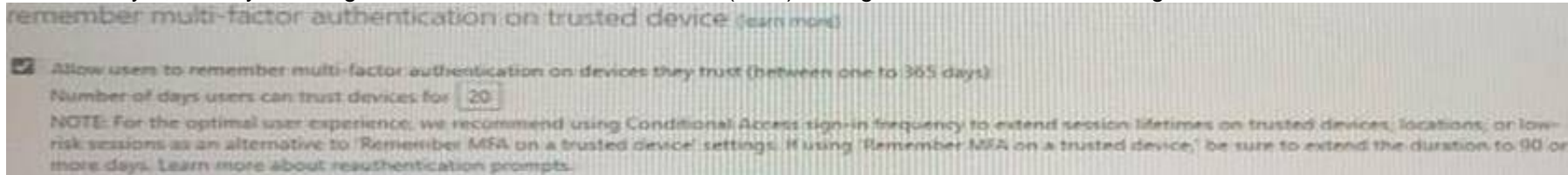
#### NEW QUESTION 5

- (Exam Topic 3)

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 6**

- (Exam Topic 3)

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 User2 to be eligible for the application administrator role.

For User1, you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click Assignment tab)

**Add assignments**  
Privileged Identity Management | Azure AD roles

Membership Setting

Assignment type ⓘ  
☒ Eligible  
☐ Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts \*

01/01/2021 12:00:00 AM

Assignment ends \*

01/31/2021 11:59:00 PM

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

**Answer Area**

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

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area

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

**NEW QUESTION 7**

- (Exam Topic 3)

Your company requires that users request access before they can access corporate applications.

You register a new enterprise application named MyApp1 in Azure Active Directory (Azure AD) and configure single sign-on (SSO) for MyApp1.

Which settings should you configure next for MyApp1?

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

**Answer: C**

**NEW QUESTION 8**

- (Exam Topic 3)

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 9**

- (Exam Topic 3)

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

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

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

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

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

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

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Reference:

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

**NEW QUESTION 10**

- (Exam Topic 3)

You have a Microsoft 365 tenant.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

## NEW QUESTION 10

- (Exam Topic 3)

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: D**

## NEW QUESTION 15

- (Exam Topic 3)

You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group 1 tab.)

```
PS C:\> Get-AzureADGroup -SearchString Admin | Get-AzureADGroupOwner

ObjectID      DisplayName UserPrincipalName  UserType
-----
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin        admin@m365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -SearchString Admin | Get-AzureADGroupMember | ft displayname

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

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

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

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| The members of Group3 can access App1 without first being approved by User1. | <input type="radio"/>            | <input checked="" type="radio"/> |
| After you configure self-service for App1, the owner of Group1 is User1.     | <input type="radio"/>            | <input checked="" type="radio"/> |
| App1 appears in the Microsoft Office 365 app launcher of User4.              | <input checked="" type="radio"/> | <input type="radio"/>            |

NEW QUESTION 20

- (Exam Topic 3)

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

**Account lockout**

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

Number of MFA denials to trigger account lockout \*

3 ✓

Minutes until account lockout counter is reset \*

60 ✓

Minutes until account is automatically unblocked \*

30 ✓

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE: Each correct selection is worth one point.

Answer Area

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

email address  
Microsoft Authenticator app code  
password

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

30  
60  
90

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

**Answer Area**

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

email address  
Microsoft Authenticator app code  
password

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

30  
60  
90

NEW QUESTION 24

- (Exam Topic 3)

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 Subscription!
- C. Managed Application Contributor for Subscription!
- D. Cloud application administrator in Azure AD

**Answer:** A

#### NEW QUESTION 26

- (Exam Topic 3)

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 28

- (Exam Topic 3)

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 theExhibittab.)



## Create an access review

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

Review name \*

Description

Start date \*

Frequency

Duration (in days)

End ☐ Never ☐ End by ☐ Occurrences

Number of times

End date

Users

Scope ☒ Everyone

Review role membership (permanent and eligible) \*

[Application Administrator and 72 others](#)

Reviewers

Reviewers

(Preview) Fallback reviewers

✓ Upon completion settings

Start

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

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

Solution: You create a separate access review for each role.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

### Explanation:

Reference:

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

## NEW QUESTION 29

- (Exam Topic 3)

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

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

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

What is a valid authentication method available to users?

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

**Answer: A**

## NEW QUESTION 34

- (Exam Topic 3)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.  
You have a Microsoft 365 tenant.  
You have 100 IT administrators who are organized into 10 departments. You create the access review shown in the exhibit. (Click the Exhibit tab.)

### Create an access review

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

**Review name \*** Admin review ✓

**Description ⓘ**

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

**Frequency** Monthly

**Duration (in days) ⓘ** 14

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

**Number of times** 0

**End date** 01/17/2021

**Users**

**Scope** ☒ Everyone

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

**Reviewers**

**Reviewers** (Preview) Manager

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

Upon completion settings

**Start**

You discover that all access review requests are received by Megan Bowen.  
You need to ensure that the manager of each department receives the access reviews of their respective department.  
Solution: You modify the properties of the IT administrator user accounts. Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

#### Explanation:

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

### NEW QUESTION 36

- (Exam Topic 3)

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

**Answer: A**

#### NEW QUESTION 41

- (Exam Topic 3)

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 44

- (Exam Topic 3)

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 49

- (Exam Topic 3)

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 sequenced? 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 |
|---|-------------|
| Register a custom domain name of contoso.com. |             |
| Create a new TXT record in DNS.               |             |
| Set the domain to primary.                    |             |
| Delete the contoso.onmicrosoft.com domain.    |             |
| Verify the domain name.                       |             |

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

| Actions                                       | Answer Area                                   |
|---|---|
| Register a custom domain name of contoso.com. | Create a new TXT record in DNS.               |
| Create a new TXT record in DNS.               | Register a custom domain name of contoso.com. |
| Set the domain to primary.                    | Set the domain to primary.                    |
| Delete the contoso.onmicrosoft.com domain.    | Verify the domain name.                       |
| Verify the domain name.                       |   |



NEW QUESTION 52

- (Exam Topic 3)

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

You plan to bulk invite Azure AD business-to-business (B2B) collaboration users.

Which two parameters must you include when you create the bulk invite? Each correct answer presents part of the solution

NOTE:Each correct selection is worth one point.

- A. email address
- B. redirection URL
- C. username
- D. shared key
- E. password

Answer: AB

Explanation:

Reference:

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

NEW QUESTION 57

- (Exam Topic 3)

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com. You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed 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            |
|---|------------------------|
| <div>Sign in to the Microsoft 365 admin center.</div>                   |                        |
| <div>Create a self-signed user account in the Azure AD tenant.</div>    |                        |
| <div>From the Microsoft 365 admin center, add the domain name.</div>    | <div>⬅️ ➡️ ⬆️ ⬆️</div> |
| <div>Respond to the Become the admin message.</div>                     |                        |
| <div>From the Microsoft 365 admin center, remove the domain name.</div> |                        |
| <div>Create a TXT record in the contoso.com DNS zone.</div>             |                        |

A.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

NEW QUESTION 61

- (Exam Topic 3)

You have a Microsoft 365 tenant.

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

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

What should you configure?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 65

- (Exam Topic 3)

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:** A

#### NEW QUESTION 67

- (Exam Topic 3)

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 71**

- (Exam Topic 3)

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:** A

**NEW QUESTION 76**

- (Exam Topic 3)

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 79**

- (Exam Topic 3)

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

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

users can request access by using package 1.

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

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

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

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

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

**Answer:** C

**NEW QUESTION 81**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SC-300 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SC-300-dumps.html>