

# Microsoft

## Exam Questions SC-300

Microsoft Identity and Access Administrator



### 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 meet the authentication requirements for leaked credentials. What should you do?

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

**Answer:** C

**Explanation:**

Reference:

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

### NEW QUESTION 3

- (Exam Topic 1)

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE:Each correct selection is worth one point.

Azure AD Connect settings to modify:

Directory Extensions
Domain Filtering
Optional Features

Assign Azure AD licenses to:

An Azure Active Directory group that has only nested groups
An Azure Active Directory group that has the Assigned membership type
An Azure Active Directory group that has the Dynamic User membership type

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Litware recently added a custom user attribute named `LWLicense` to the `litware.com` Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the `LWLicense` attribute. Users who have the appropriate value for `LWLicense` must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

NEW QUESTION 4

- (Exam Topic 2)  
You create a Log Analytics workspace.  
You need to implement the technical requirements for auditing. What should you configure in Azure AD?

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

Answer: B

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

NEW QUESTION 5

- (Exam Topic 2)  
You need to meet the technical requirements for license management by the helpdesk administrators.  
What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Object to create for each branch office:

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

Tool to use:

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Answer Area

Object to create for each branch office:

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

Tool to use:

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

#### NEW QUESTION 6

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 7

- (Exam Topic 2)

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

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

**Answer:** C

#### Explanation:

Reference:

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

#### NEW QUESTION 8

- (Exam Topic 2)

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

- A. From the Microsoft Azure Active Directory Connect wizard, selectCustomize synchronization options.
- B. From PowerShell, runSet-ADSyncScheduler.
- C. From PowerShell, runStart-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, selectChange user sign-in.

**Answer:** A

#### Explanation:

You need to selectCustomize synchronization optionsto configure Azure AD Connect to sync the Adatum organizational unit (OU).

#### NEW QUESTION 9

- (Exam Topic 3)

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

AH 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. Prom 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 10

- (Exam Topic 3)

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





 Save  Discard  Delete |  Got feedback?

Enabled for users to sign-in?  ☒ Yes ☐ No

Name   

Homepage URL   



Logo    

User access URL   


Application ID   

Object ID   

Terms of Service Url   

Privacy Statement Url   

Reply Url   

User assignment required?  ☐ Yes ☒ No

Visible to users?  ☒ Yes ☐ No

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

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

All users

No one

Only users listed on the Owners blade

Only users listed on the Users and groups blade

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

all users

no one

only users listed on the Owners blade

only users listed on the Users and groups blade

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 10**

- (Exam Topic 3)

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

- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

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

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

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

**Answer: C**

**Explanation:**

Reference:

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

**NEW QUESTION 11**

- (Exam Topic 3)

You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click theExhibittab.)

## Guest user access

### Guest user access restrictions (Preview) ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☒ Guest users have limited access to properties and memberships of directory objects
- ☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

## Guest invite settings

### Admins and users in the guest inviter role can invite ⓘ

☒ Yes ☐ No

### Members can invite ⓘ

☒ Yes ☐ No

### Guests can invite ⓘ

☐ Yes ☒ No

### Email One-Time Passcode for guests ⓘ

[Learn more](#)

☒ Yes ☐ No

### Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

☒ Yes ☐ No

## 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)

A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrkam.com	A user in fabrikam.com

Which users will be emailed a passcode?

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

**Answer:** A

### Explanation:

Reference:

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

## NEW QUESTION 16

- (Exam Topic 3)

You have a Microsoft 365 tenant.

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

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

- A. Application Insights in Azure Monitor
- B. access reviews in Azure AD
- C. Cloud App Discovery in Microsoft Cloud App Security
- D. enterprise applications in Azure AD

**Answer:** C

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs>

#### NEW QUESTION 20

- (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 21

- (Exam Topic 3)

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 23

- (Exam Topic 3)

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

You receive more than 100 email alerts each day for tailed Azure AD user sign-in attempts. You need to ensure that a new security administrator receives the alerts instead of you. Solution: From Azure monitor, you modify the action group.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 25

- (Exam Topic 3)

You have a Microsoft 365 tenant.

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

What should you do first?

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

**Answer:** A

#### NEW QUESTION 26

- (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

## Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on activation	No
Require justification on active assignment	Yes

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

# Add assignments

Privileged Identity Management | Azure AD roles

Membership   Setting

Assignment type ⓘ

- ☒ Eligible
- ☐ Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts \*

01/01/2021 

12:00:00 AM

Assignment ends \*

01/31/2021 

11:59:00 PM

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

## Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

#### Answer Area

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

#### NEW QUESTION 28

- (Exam Topic 3)

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.

You need to ensure that the IT department users only have access to the Security administrator role when required.

What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments after from the Role settings details
- B. Expire active assignments after from the Role settings details
- C. Assignment type to Active
- D. Assignment type to Eligible

**Answer: D**

#### Explanation:

Reference:

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

#### NEW QUESTION 31

- (Exam Topic 3)

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 verification code from the Microsoft Authenticator app
- B. security questions
- C. voice
- D. SMS

**Answer: B**

#### NEW QUESTION 34

- (Exam Topic 3)

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

All users who run applications registered in Azure AD are subject to conditional access policies. You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

- A. a cloud apps or actions condition
- B. a user risk condition
- C. a client apps condition
- D. a sign-in risk condition

**Answer: C**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

#### NEW QUESTION 37

- (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 40

- (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 43

- (Exam Topic 3)

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.

☐☐

User2 can access the enterprise application.

☐☐

User3 can accept the invitation and gain access to the SharePoint site.

☐☐

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 46

- (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 47

- (Exam Topic 3)

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**

#### NEW QUESTION 50

- (Exam Topic 3)

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

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections. What should you include in the recommendation?

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

**Answer: C**

#### NEW QUESTION 52

- (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 56

- (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 \***  ✓

**Description ⓘ**


**Start date \***  

**Frequency**  ▼

**Duration (in days) ⓘ**  14

**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 ⓘ**  
[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 58

- (Exam Topic 3)

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 63**

- (Exam Topic 3)

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 66**

- (Exam Topic 3)

Your company has an Azure Active Directory (Azure AD) tenant named Contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

To allow access for users who have fabrikam.com email addresses, configure:

An access package assignment in Identity Governance
An access package policy in Identity Governance
A conditional access policy in Azure AD
The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

An access package assignment in Identity Governance
An access package policy in Identity Governance
A conditional access policy in Azure AD
The External collaboration settings in Azure AD

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

An access package assignment in Identity Governance

An access package policy in Identity Governance

A conditional access policy in Azure AD

The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

An access package assignment in Identity Governance

An access package policy in Identity Governance

A conditional access policy in Azure AD

The External collaboration settings in Azure AD

NEW QUESTION 68

- (Exam Topic 3)  
You have an Azure Active Directory (Azure AD) tenant.  
You need to review the Azure AD sign-ins log to investigate sign ins that occurred in the past. For how long does Azure AD store events in the sign-in log?

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

Answer: B

NEW QUESTION 70

- (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 73

- (Exam Topic 3)  
You configure a new Microsoft 365 tenant to use a default domain name of contosso.com.  
You need to ensure that you can control access to Microsoft 365 resource-, by using conditional access policy. What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MI A) registration policy1.
- D. Configure password protection for Windows Server Active Directory.

Answer: B

NEW QUESTION 78

- (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 79

- (Exam Topic 3)  
You have a Microsoft 365 tenant.  
You need to identify users who have leaked credentials. The solution must meet the following requirements.

- Identity sign-ins by users who are suspected of having leaked credentials.
  - Tag the sign-ins as a high risk event.
  - Immediately enforce a control to mitigate the risk, while still allowing the user to access applications. What should you use? To answer, select the appropriate options in the answer area.
- NOTE: Each correct selection is worth one point.

Answer Area

To classify leaked credentials as high-risk, use:

Azure Active Directory (Azure AD) Identity Protection

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Identity Governance

Self-service password reset (SSPR)

To trigger remediation, use:

Client apps not using Modern authentication

Device state

Sign-in risk

User location

User risk

To mitigate the risk, select:

Apply app-enforced restrictions

Block access

Grant access but require app protection policy

Grant access but require multi-factor authentication

Grant access but require password change

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:  
Answer Area

To classify leaked credentials as high-risk, use:

Azure Active Directory (Azure AD) Identity Protection

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Identity Governance

Self-service password reset (SSPR)

To trigger remediation, use:

Client apps not using Modern authentication

Device state

Sign-in risk

User location

User risk

To mitigate the risk, select:

Apply app-enforced restrictions

Block access

Grant access but require app protection policy

Grant access but require multi-factor authentication

Grant access but require password change

NEW QUESTION 84

- (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 all their respective domain names for email addresses.  
You plan to create an access package named package1 that will be accessible only to the Fabrikam and Litware users.  
You need to configure connected organizations for Fabrikam and Litware so that any of their users can request access by using package1.  
What is the minimum number of connected organizations that you should create.

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

Answer: C

NEW QUESTION 87

- (Exam Topic 3)

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 90

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### SC-300 Practice Exam Features:

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

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