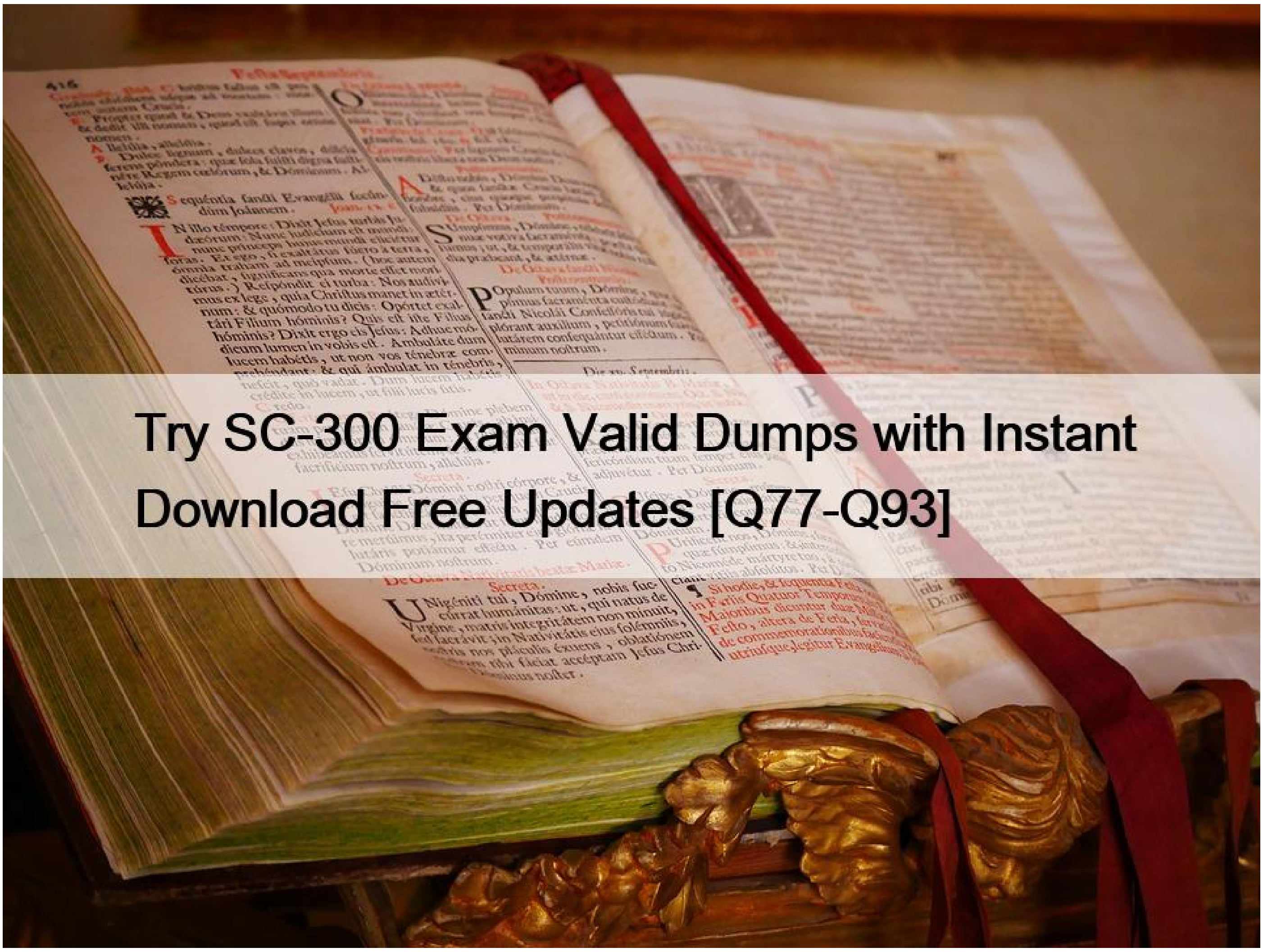
Try SC-300 Exam Valid Dumps with Instant Download Free Updates [Q77-Q93

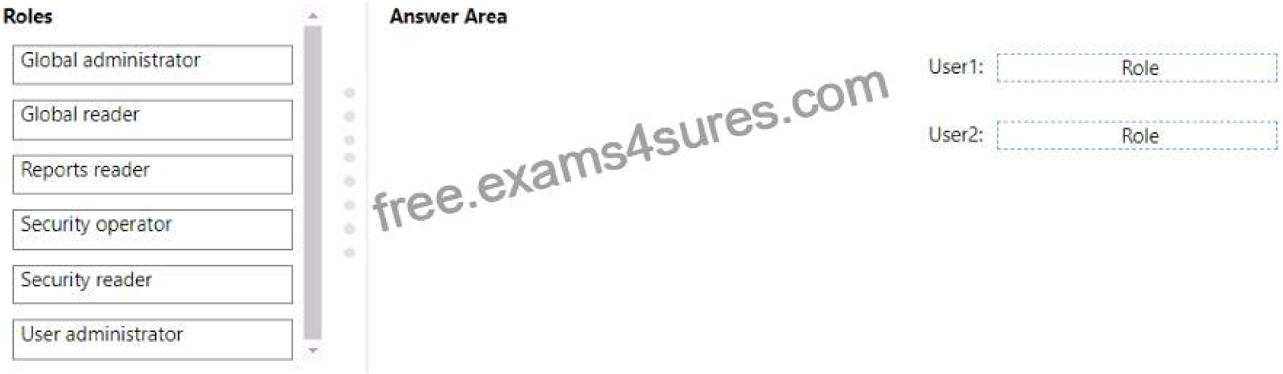


Try SC-300 Exam Valid Dumps with Instant Download Free Updates
SC-300 Dumps First Attempt Guaranteed Success

NO.77 You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.



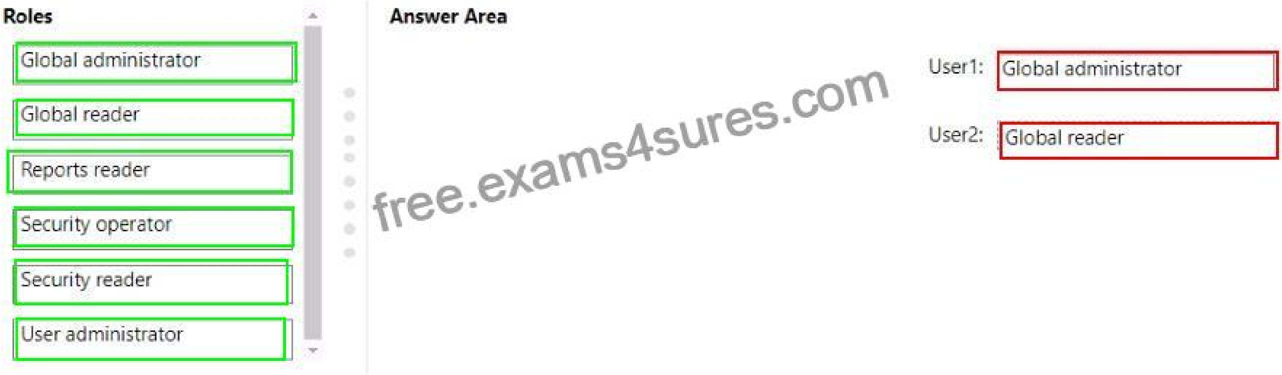
Roles

- Global administrator
- Global reader
- Reports reader
- Security operator
- Security reader
- User administrator

Answer Area

User1: Role

User2: Role



Roles

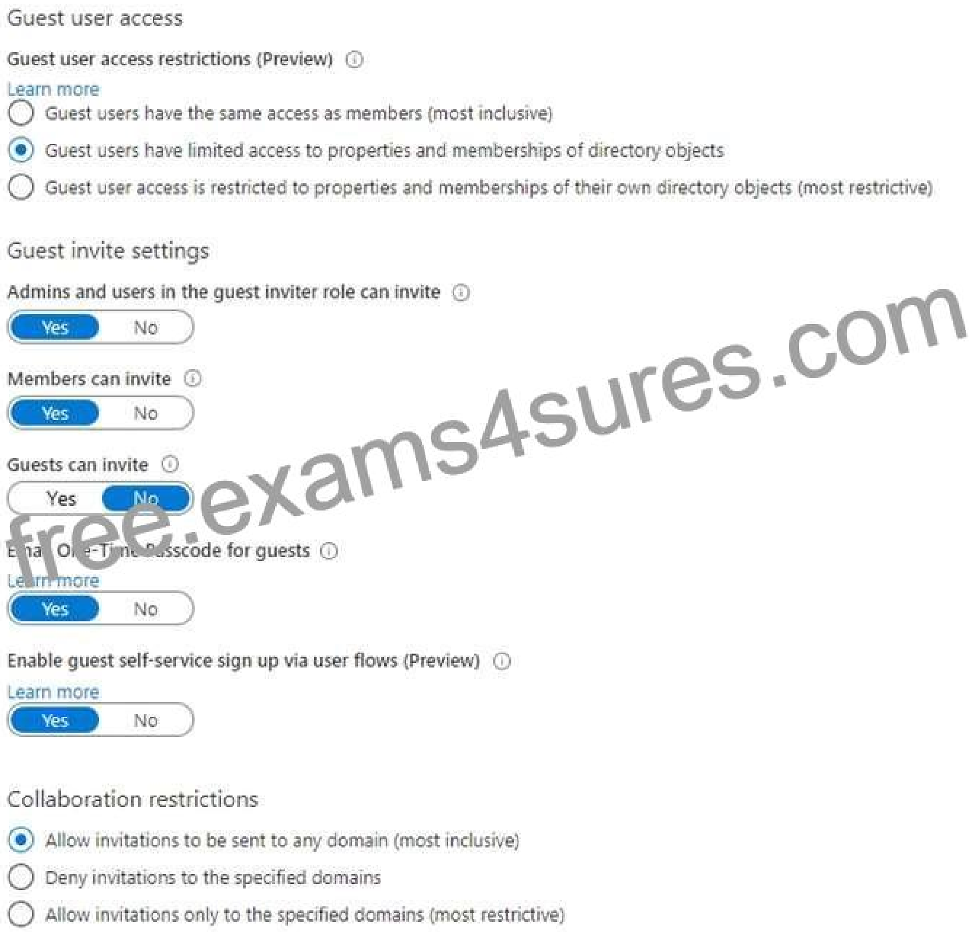
- Global administrator
- Global reader
- Reports reader
- Security operator
- Security reader
- User administrator

Answer Area

User1: Global administrator

User2: Global reader

NO.78 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 the Exhibit tab.)



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]

Enable Email One-Time Passcode for guests ⓘ

Learn more

[✓ Yes] No

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

Learn more

[✓ Yes] No

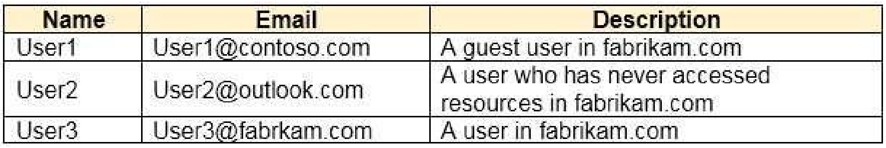
Collaboration restrictions

● 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?

- User2 only
- User1 only
- User1 and User2 only
- User1, User2, and User3

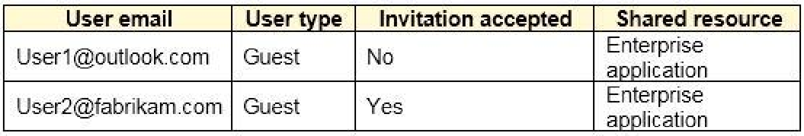
Explanation/Reference:

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

NO.79 You have a Microsoft 365 tenant named contoso.com.

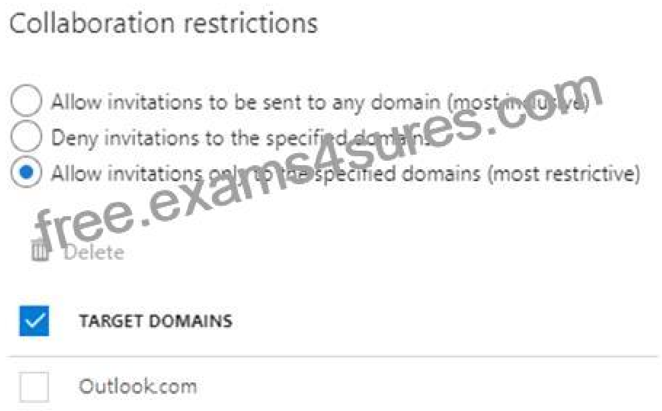
Guest user access is enabled.

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)

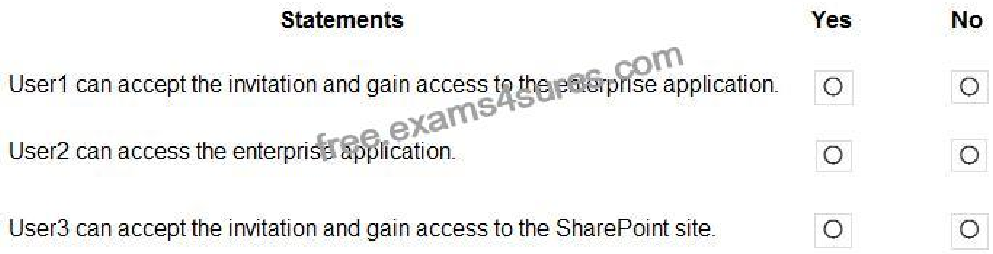
☑ TARGET DOMAINS

□ Outlook.com

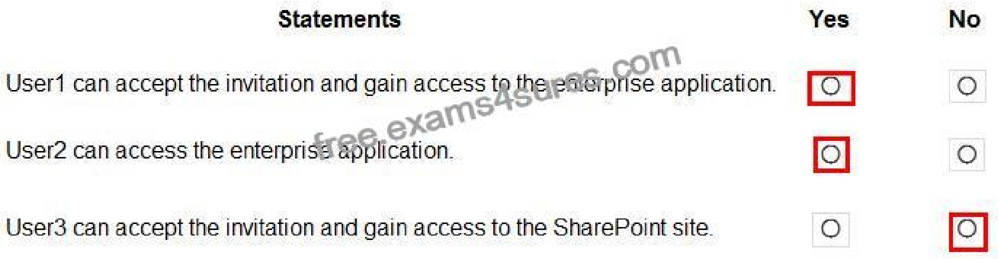
From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.

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.	○	○



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.	○	[✓ ○]

NO.80 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?
* Yes
* No
Reference:

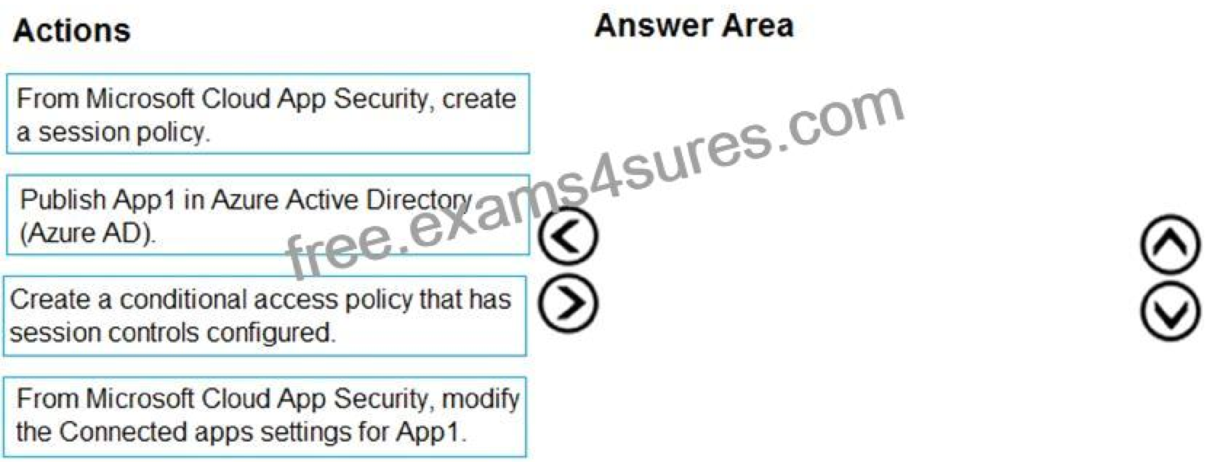
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

NO.81 You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud app Security.

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



Actions

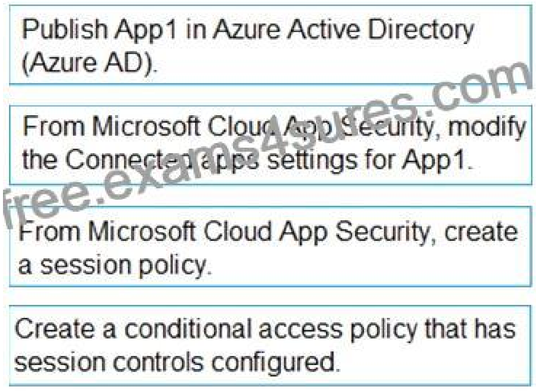
From Microsoft Cloud App Security, create a session policy.

Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

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

Answer Area

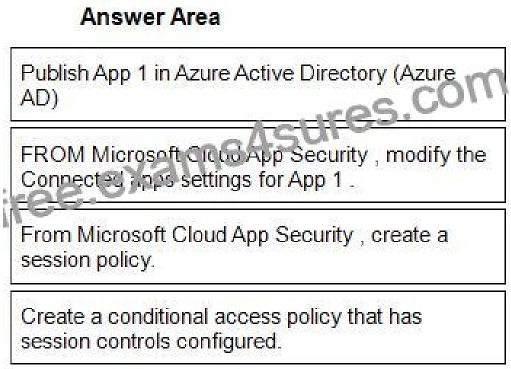


Publish App1 in Azure Active Directory (Azure AD).

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

From Microsoft Cloud App Security, create a session policy.

Create a conditional access policy that has session controls configured.



Answer Area

Publish App 1 in Azure Active Directory (Azure AD)

FROM Microsoft Cloud App Security , modify the Connected apps settings for App 1 .

From Microsoft Cloud App Security , create a session policy.

Create a conditional access policy that has session controls configured.

1 &#8211; Publish App 1 in Azure Active Directory (Azure AD)

2 &#8211; FROM Microsoft Cloud App Security , modify the Connected apps settings for App 1 .

3 &#8211; From Microsoft Cloud App Security , create a session policy.

4 &#8211; Create a conditional access policy that has session controls configured.

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app

https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

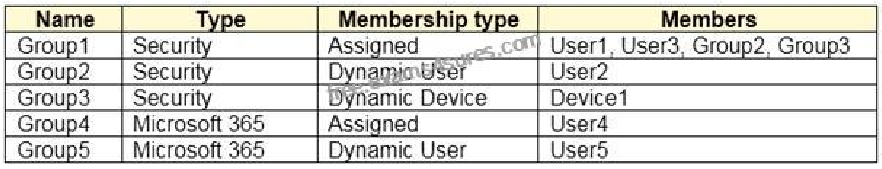
NO.82 You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

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.

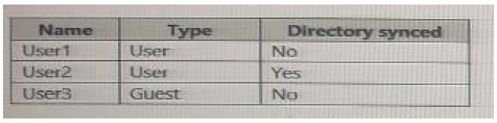


Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?
* Group1 and Group4 only
* Group1, Group2, Group3, Group4, and Group5
* Group1 and Group2 only
* Group1 only
* Group1, Group2, Group4, and Group5 only
Reference:

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

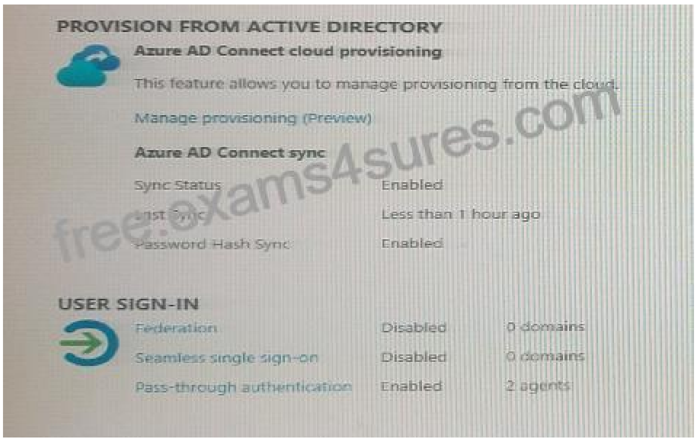
NO.83 Your network contains an on-premises Active Directory domain that sync to an Azure Active Directory (Azure AD) tenant. The tenant contains the shown in the following table.



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

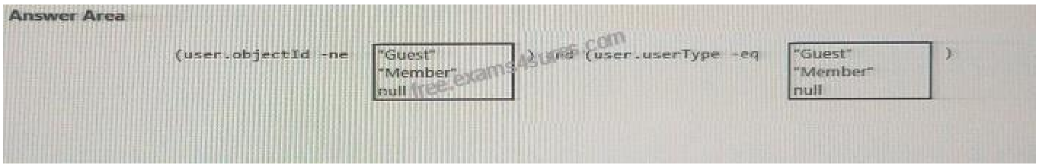
Connectivity from the on-premises domain to the internet is lost.

Which user can sign in to Azure AD?
* User1 only
* User1 and User 3 only
* User1, and User2 only
* User1, User2, and User3

NO.84 You need to create the LWGroup1 group to meet the management requirements.

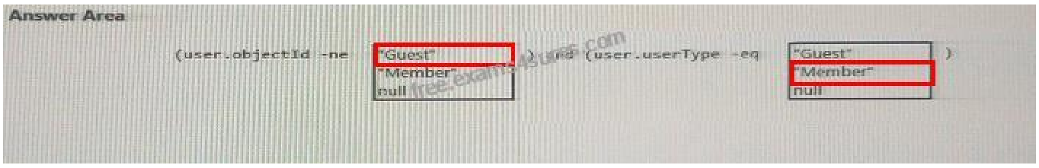
How should you complete the dynamic membership rule? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You many need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer Area

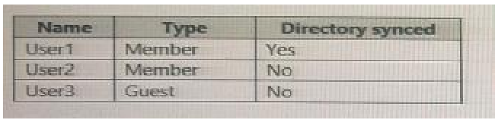
```
(user.objectId -ne  "Guest"   ) and (user.userType -eq  "Guest"   )
                    "Member"                            "Member"
                    null                                null
```



Answer Area

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

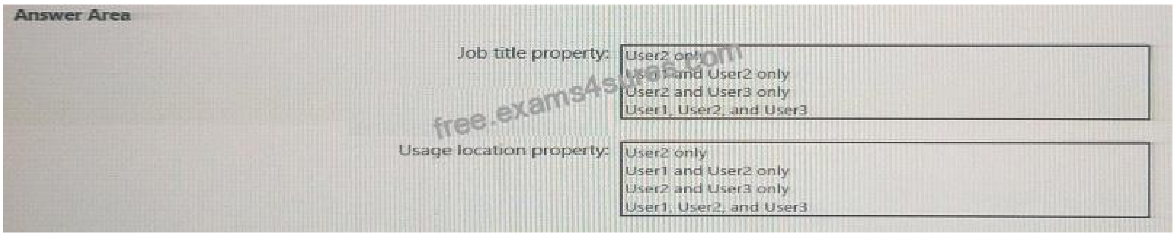
NO.85 You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



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

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

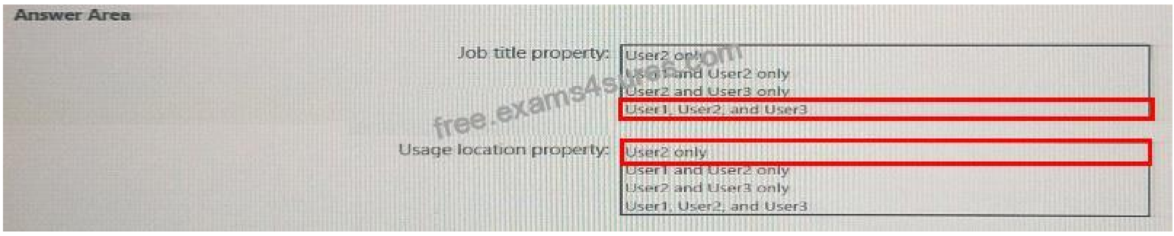
NOTE: Each correct selection is worth one point.



Answer Area

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

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



Answer Area

Job title property:
- User2 only
- User1 and User2 only
- User2 and User3 only
- [✓ User1, User2, and User3]

Usage location property:
- [✓ User2 only]
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

NO.86 Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

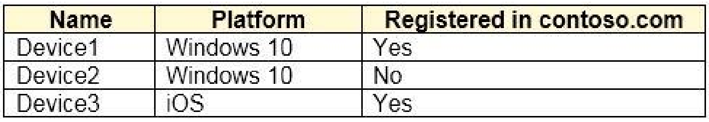
The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?
* a named network location
* the Microsoft Authenticator app
* Windows Hello for Business authentication
* FIDO2 tokens
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

NO.87 You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

User1 has the devices shown in the following table.



Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

Name: Terms1

Display name: Contoso terms of use

Require users to expand the terms of use: On

Require users to consent on every device: On

Expire consents: On

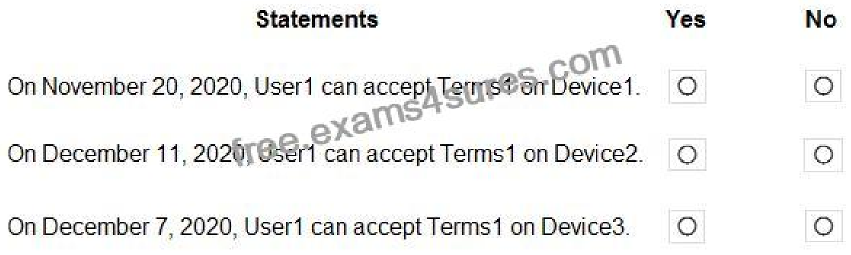
Expire starting on: December 10, 2020

Frequency: Monthly

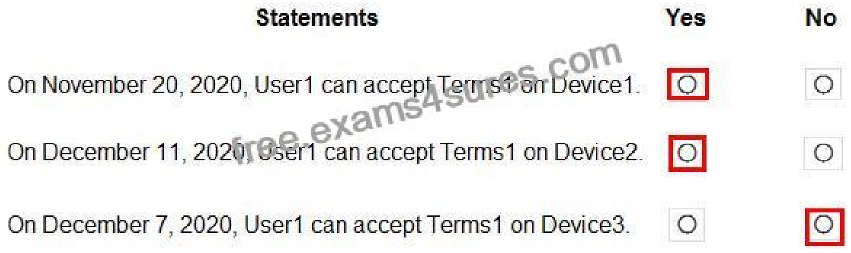
On November 15, 2020, User1 accepts Terms1 on Device3.

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
On November 20, 2020, User1 can accept Terms1 on Device1.	○	○
On December 11, 2020, User1 can accept Terms1 on Device2.	○	○
On December 7, 2020, User1 can accept Terms1 on Device3.	○	○



Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	[✓ ○]	○
On December 11, 2020, User1 can accept Terms1 on Device2.	[✓ ○]	○
On December 7, 2020, User1 can accept Terms1 on Device3.	○	[✓ ○]

NO.88 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.

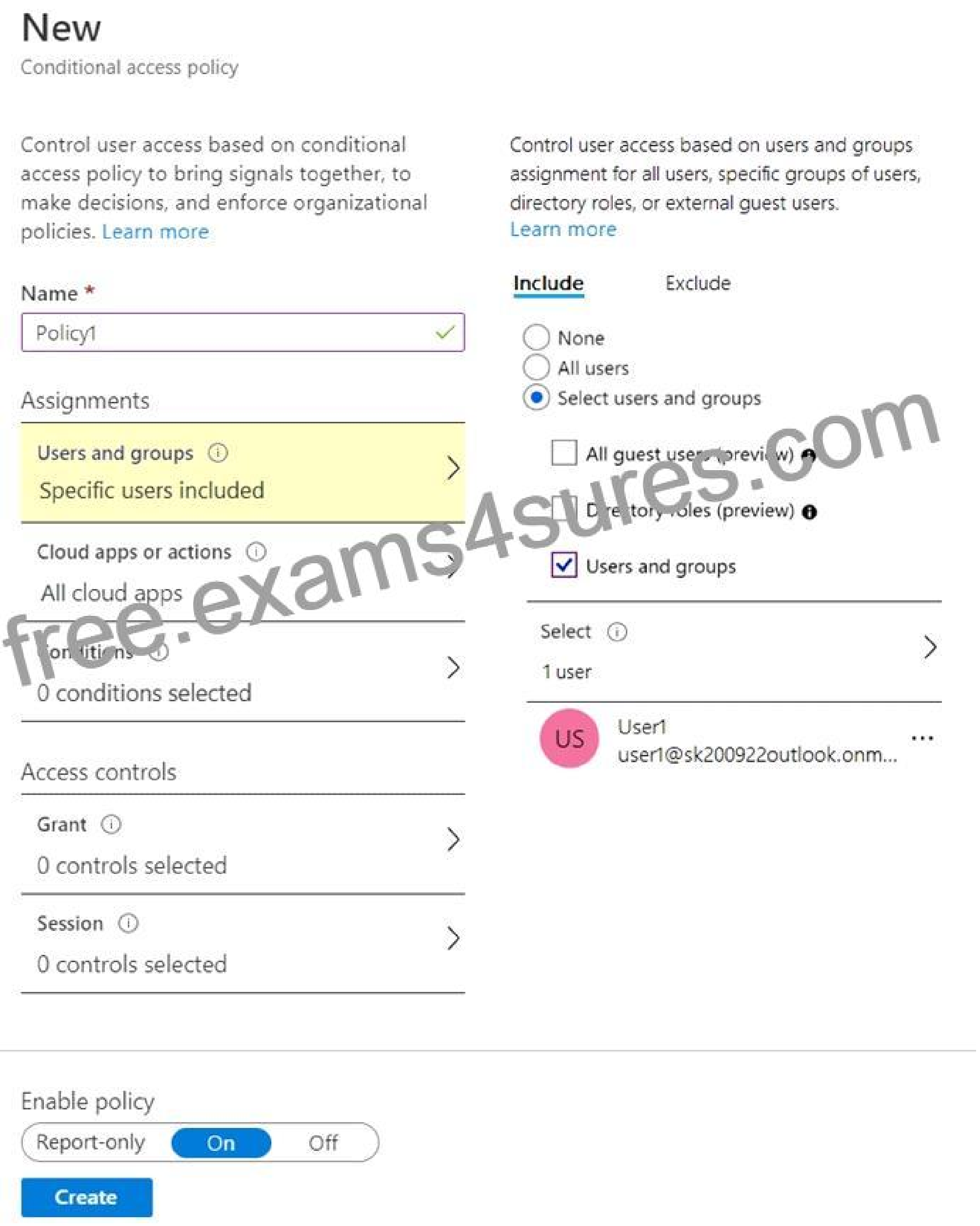
Which two parameters must you include when you create the bulk invite? Each correct answer presents part of the solution NOTE: Each correct selection is worth one point.
* email address
* redirection URL
* username

* shared key
* password
Reference:

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

NO.89 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

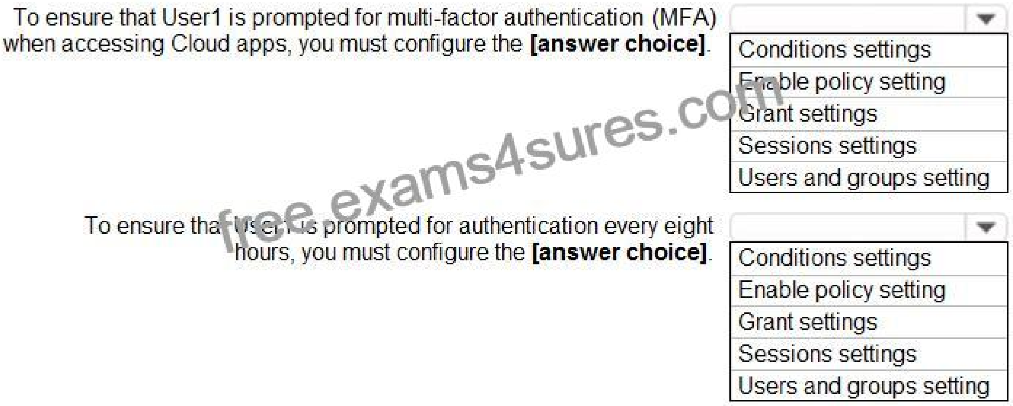
US User1
user1@sk200922outlook.onm...

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.

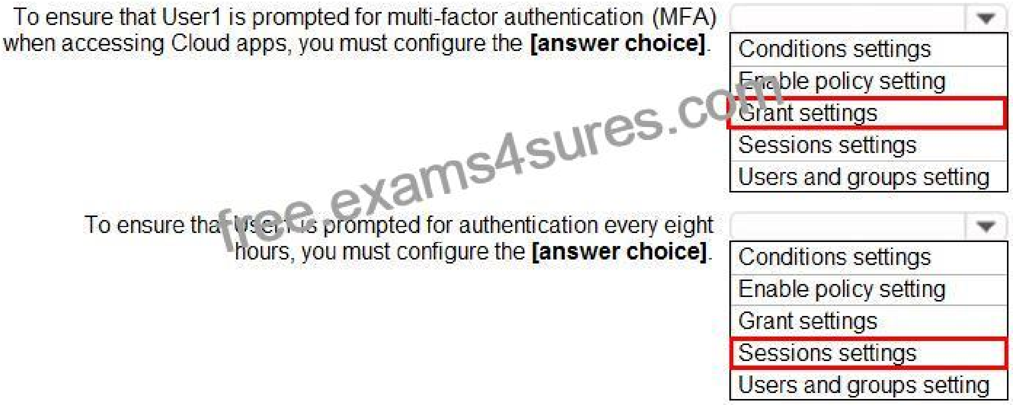


To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

- 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



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

Reference:

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

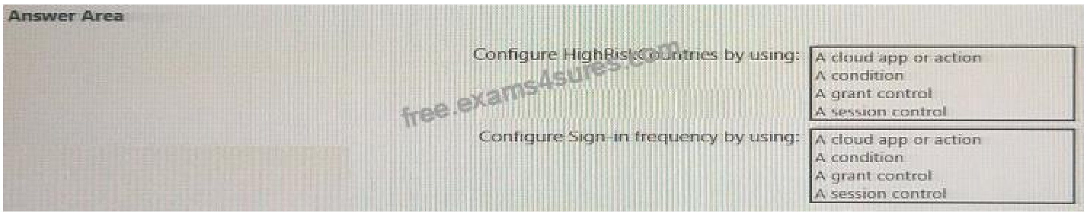
NO.90 You have a Microsoft 36S tenant.

You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



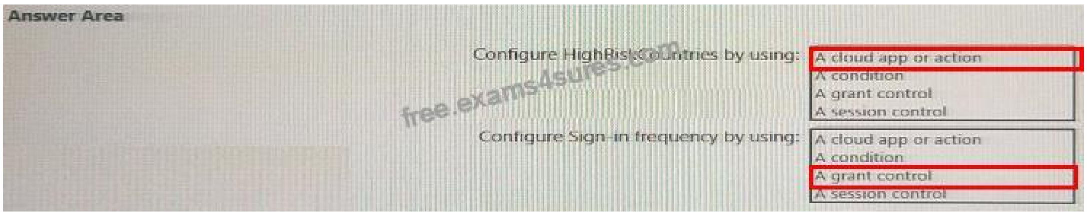
Answer Area

Configure HighRiskCountries by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control



Answer Area

Configure HighRiskCountries by using:
- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:
- A cloud app or action
- A condition
- A grant control
- A session control

NO.91 Your company requires that users request access before they can access corporate applications.

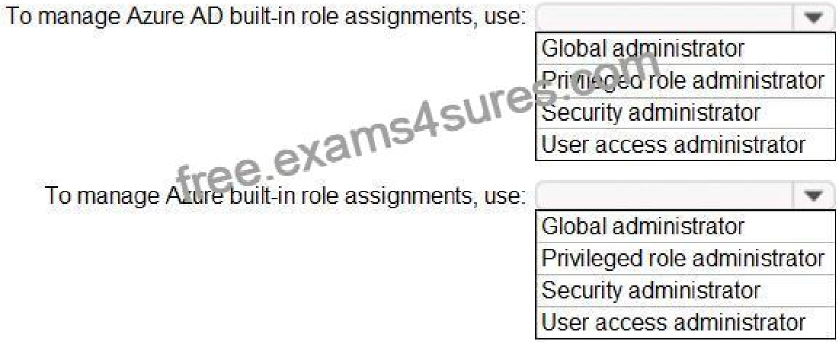
You register a new enterprise application named MyApp1 in Azure Active Dilatory (Azure AD) and configure single sign-on (SSO) for MyApp1.

Which settings should you configure next for MyApp1?
* Self-service
* Provisioning
* Roles and administrators
* Application proxy

NO.92 You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

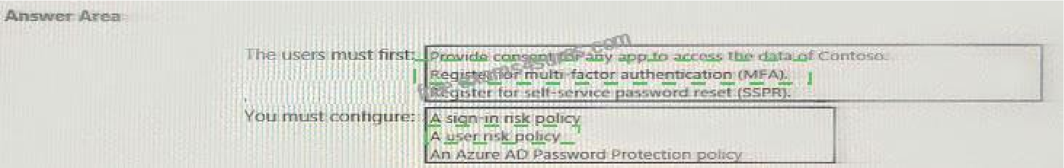
What should you do? To answer, select the appropriate options in the answer area.

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

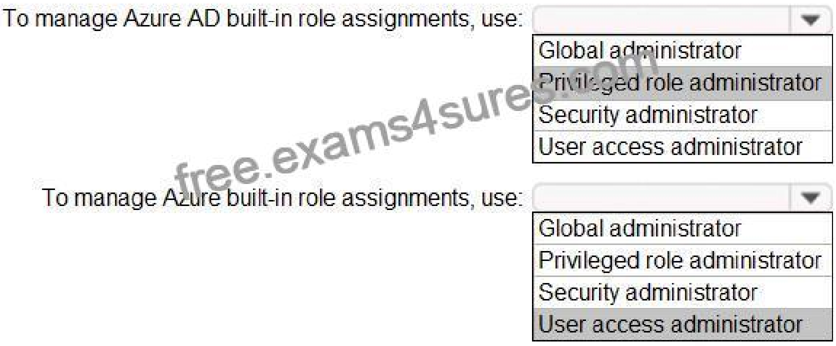


Answer Area

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

Explanation



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

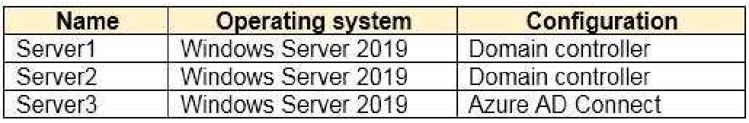
Reference:

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

NO.93 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?
* Azure AD Connect
* Azure AD Application Proxy
* Password Change Notification Service (PCNS)
* the Azure AD Password Protection proxy service
Explanation/Reference:

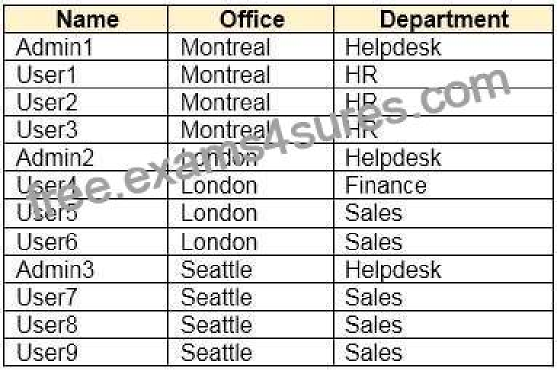
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises- deploy Implement access management for apps Testlet 1 Case Study Overview Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.



Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

* Microsoft Office 365 Enterprise E5

* Enterprise Mobility + Security

* Windows 10 Enterprise E3

* Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

* The users in the London office have the Microsoft 365 Phone System license unassigned.

* The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

* Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

* The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

* The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

* Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

* When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

* Implement self-service password reset (SSPR).

* Analyze Azure audit activity logs by using Azure Monitor.

* Simplify license allocation for new users added to the tenant.

* Collaborate with the users at Fabrikam on a joint marketing campaign.

* Configure the User administrator role to require justification and approval to activate.

* Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

* For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

* All users must be synced from AD DS to the contoso.com Azure AD tenant.

* App1 must have a redirect URI pointed to https://contoso.com/auth- response.

* License allocation for new users must be assigned automatically based on the location of the user.

* Fabrikam users must have access to the marketing department&#8217;s SharePoint site for a maximum of 90 days.

* Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

* The helpdesk administrators must be able to manage licenses for only the users in their respective office.

* Users must be forced to change their password if there is a probability that the users&#8217; identity was compromised.

100% Guarantee Download SC-300 Exam Dumps PDF Q&A:
https://www.exams4sures.com/Microsoft/SC-300-practice-exam-dumps.html]