

## Exam Questions SC-300

Microsoft Identity and Access Administrator

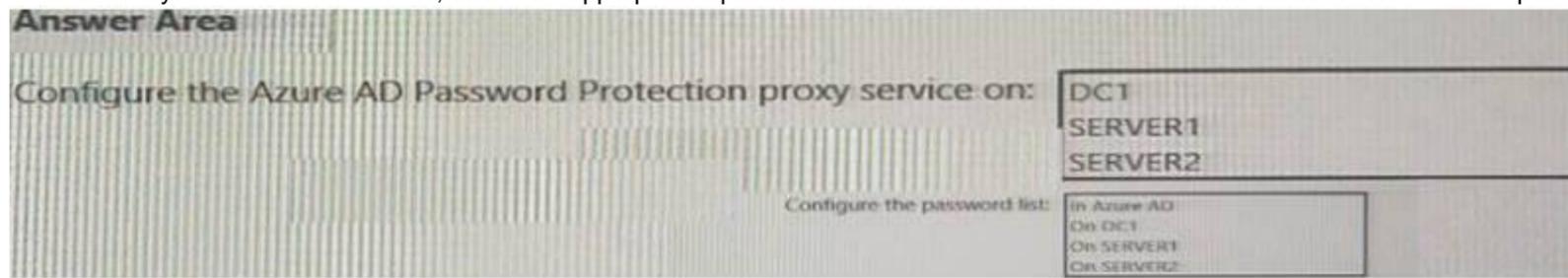
<https://www.2passeasy.com/dumps/SC-300/>



**NEW QUESTION 1**

- (Exam Topic 1)

You need to implement password restrictions to meet the authentication requirements. You install the Azure AD password Protection DC agent on DC1. What should you do next? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

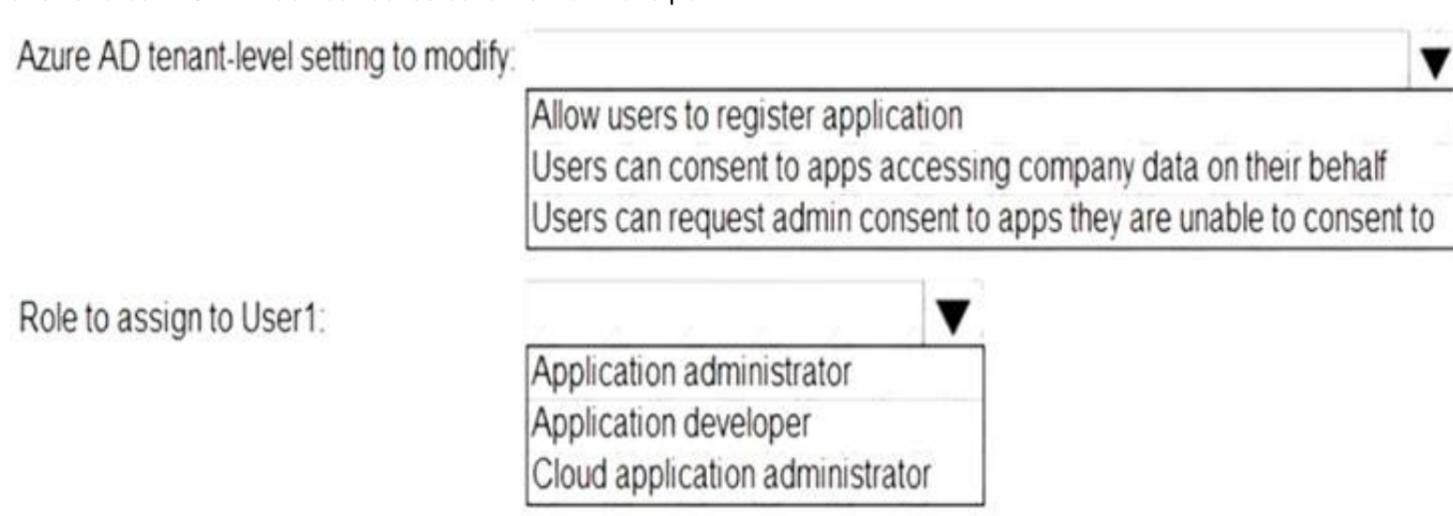
**Answer:** A

**Explanation:**  
 Server1 On DC1

**NEW QUESTION 2**

- (Exam Topic 1)

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
 Graphical user interface, text Description automatically generated  
 Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

**NEW QUESTION 3**

- (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 4**

- (Exam Topic 3)

You need implement the planned changes for application access to organizational data. What should you configure?

- A. authentication methods
- B. the User consent settings
- C. access packages
- D. an application proxy

**Answer:** D

### NEW QUESTION 5

- (Exam Topic 3)

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Number of authentication methods required:

Authentication methods that can be used:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Number of authentication methods required:

Authentication methods that can be used:

### NEW QUESTION 6

- (Exam Topic 4)

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: C

Explanation:

MFA and SSPR are both required. However, MFA is required first. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

### NEW QUESTION 7

- (Exam Topic 4)

HOTSPOT

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

### 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 8**

- (Exam Topic 4)

You have a Microsoft 365 tenant and an Active Directory domain named adatum.com. You deploy Azure AD Connect by using the Express Settings. You need to configure self-service password reset (SSPR) to meet the following requirements:

- > When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.
- > Passwords must be synced between the tenant and the domain regardless of where the password was reset.

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

NOTE: Each correct selection is worth one point.

From the Password reset blade in the Azure Active Directory admin center, configure:

Authentication methods
Notifications
Properties
Registration

From Azure AD Connect, enable:

Federation with Active Directory Federation Services (AD FS)
Pass-through authentication
Password hash synchronization
Password writeback

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions>

**NEW QUESTION 9**

- (Exam Topic 4)

You have an Azure Active Directory Premium P2 tenant. You create a Log Analytics workspace.

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

What should you do first?

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

**Answer:** C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-lo>

**NEW QUESTION 10**

- (Exam Topic 4)

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

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

You have an 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 10**

- (Exam Topic 4)

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

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

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

Answer: C

**Explanation:**

Reference:

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

**NEW QUESTION 12**

- (Exam Topic 4)

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

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

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

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

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

Solution: You configure 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 17**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	None

You have the Device Settings shown in the following exhibit.

User1 has the devices shown in the following table.

Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

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

NOTE: Each correct selection is worth one point.

**Statements**

**Yes No**

User1 can join four additional Windows 10 devices to Azure AD.

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

Admin2 is a local administrator on Device3.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes  
 Users may join 5 devices to Azure AD.  
 Box 2: Yes  
 Box 3: No  
 An additional local device administrator has not been applied Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

**NEW QUESTION 22**

- (Exam Topic 4)  
 You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

For which resources can you create an access review?

- A. Group1, App1, Contributor, and Role1
- B. Hotel and Contributor only
- C. Group1, Role1, and Contributor only
- D. Group1 only

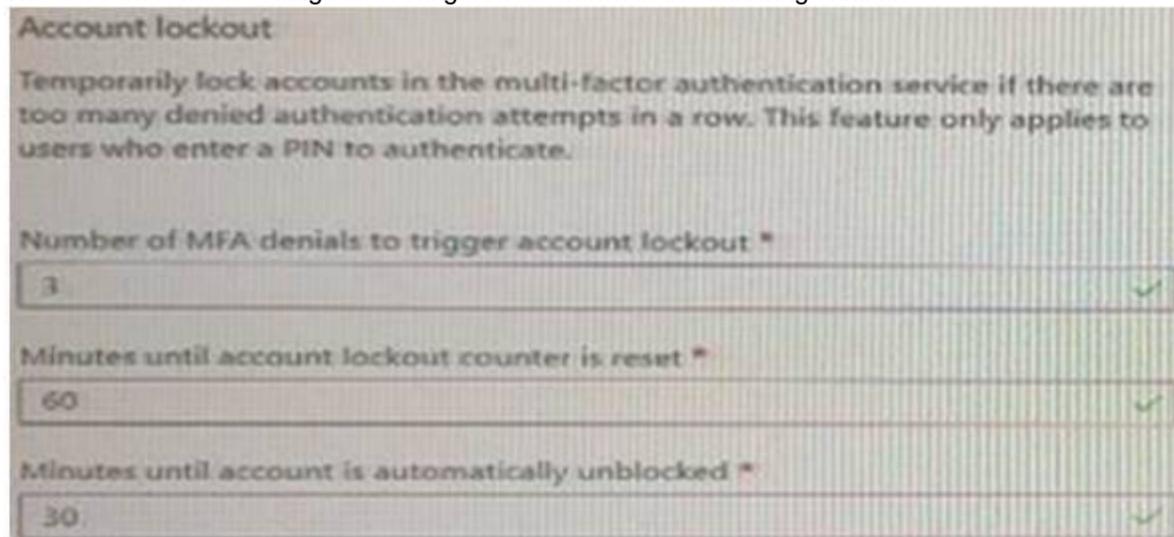
**Answer:** A

**Explanation:**

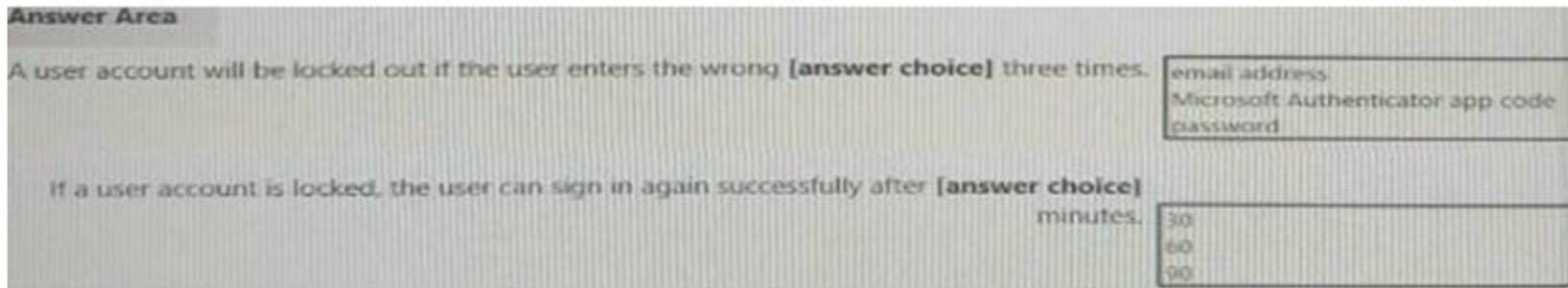
Access reviews require an Azure AD Premium P2 license.  
 Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.  
 Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.  
 Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-securi> <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

**NEW QUESTION 25**

- (Exam Topic 4)  
 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.



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. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

App code 60

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#account-lockout>

**NEW QUESTION 27**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

In Azure AD, you add a new enterprise application named App1. Which groups can you assign to App1?

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

**Answer:** C

**NEW QUESTION 31**

- (Exam Topic 4)

Your company has a Microsoft 365 tenant.

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

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

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

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

NOTE: Each correct selection is worth one point.

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

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

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

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

directory/conditional-access/require-managed-devices

**NEW QUESTION 34**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

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

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

**Answer:** A

**NEW QUESTION 39**

- (Exam Topic 4)

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
Sign in to the Microsoft 365 admin center.	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;"> <span>⬅</span>  <span>➡</span> </div> <div style="text-align: center;"> <span>⬆</span>  <span>⬇</span> </div> </div>
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 41**

- (Exam Topic 4)

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

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

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

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

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

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

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 45**

- (Exam Topic 4)

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

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

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

- Block external user from signing in to this directory: No

- > Remove external user: Yes
  - > Number of days before removing external user from this directory: 90
- What should you configure on the Identity Governance blade?
- A. Access packages
  - B. Settings
  - C. Terms of use
  - D. Access reviews

**Answer: B**

**Explanation:**

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

**NEW QUESTION 48**

- (Exam Topic 4)

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

- > A device named Device1
  - > Users named User1, User2, User3, User4, and User5
  - > Groups named Group1, Group2, Group3, Group4, and Group5
- The groups are configured as shown in the following table.

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

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 49**

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Service to install on Server4:

<input type="checkbox"/>	Azure AD Application Proxy
<input type="checkbox"/>	The Azure AD Password Protection DC agent
<input type="checkbox"/>	The Azure AD Password Protection proxy service
<input type="checkbox"/>	Web Application Proxy in Windows Server

Rule to configure on Firewall1:

<input type="checkbox"/>	Allow incoming HTTPS connections from Azure AD to Server4.
<input type="checkbox"/>	Allow incoming IPsec connections from Azure AD to Server4.
<input type="checkbox"/>	Allow outbound HTTPS connections from Server4 to Azure AD.
<input type="checkbox"/>	Allow outbound IPsec connections from Server4 to Azure AD.

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 54**

- (Exam Topic 4)

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com. Several users use their contoso.com email address for self-service sign up to Azure Active Directory (Azure AD). You gain global administrator privileges to the Azure AD tenant that contains the self-signed users. You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services. Which PowerShell cmdlet should you run?

- A. Set-MsolCompanySettings
- B. Set-MsolDomainFederationSettings
- C. Update-MsolFederatedDomain
- D. Set-MsolDomain

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup>

**NEW QUESTION 57**

- (Exam Topic 4)

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

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

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

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

Can assign users to App1:

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

Can register App2 in Azure AD:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 61**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role. SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal. You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of nonadministrative users. The solution must use the principle of least privilege. Which role should you assign to SecAdmin1?

- A. Authentication administrator
- B. Helpdesk administrator
- C. Privileged authentication administrator
- D. Security operator

**Answer:** C

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

**NEW QUESTION 64**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1. A contractor uses the credentials of user1@outlook.com. You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com. What should you do?

- A. Run the New-AzADUser cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Create a guest user account in contoso.com.

**Answer:** D

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-usersportal>

**NEW QUESTION 68**

- (Exam Topic 4)

You have a Microsoft 365 tenant. All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services. Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request. You need to block the users automatically when they report an MFA request that they did not initiate. Solution: From the Azure portal, you configure the Block/unblock users settings for multi-factor authentication (MFA). Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

You need to configure the fraud alert settings. Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

**NEW QUESTION 70**

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

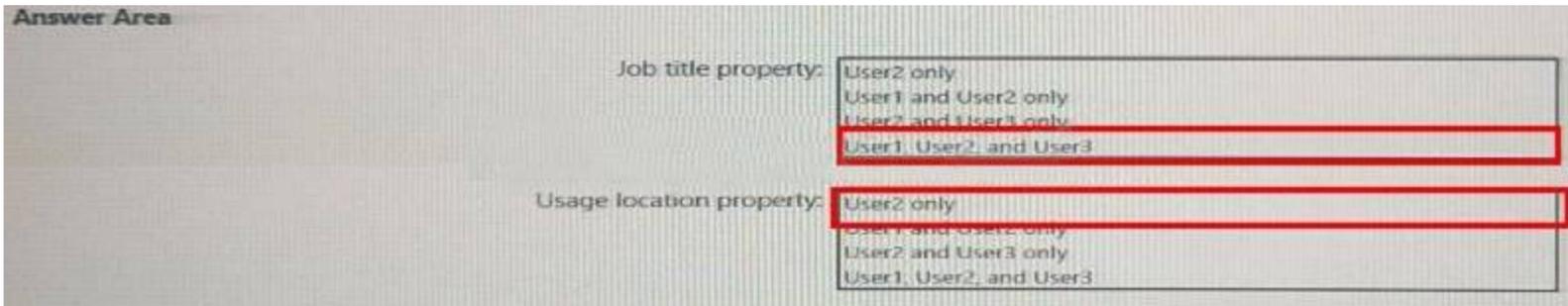
Job title property:  User2 only  
 User1 and User2 only  
 User2 and User3 only  
 User1, User2, and User3

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 75**

- (Exam Topic 4)

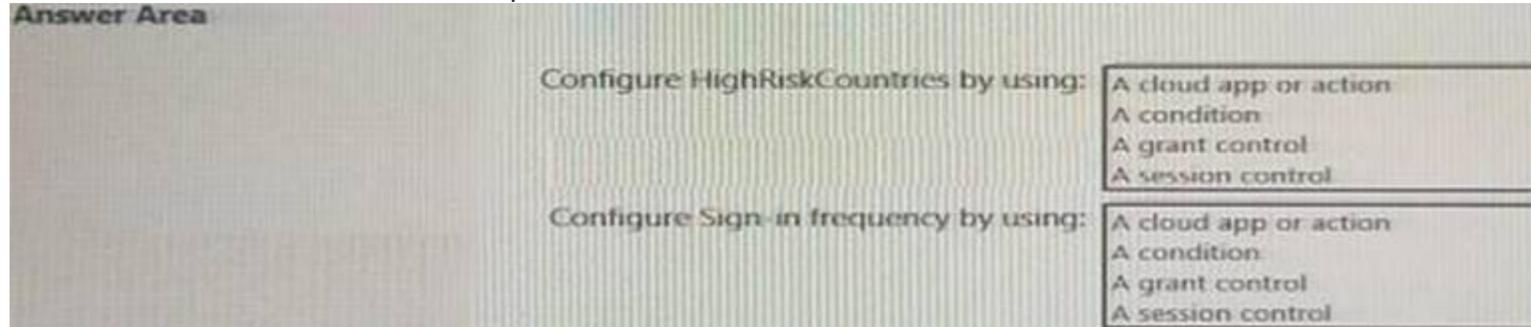
You have a Microsoft 365 tenant.

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.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 80**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain that sync to an Azure Active Directory (Azure AD) tenant. The tenant contains the shown in the following table.

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

All the users work remotely.

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

**PROVISION FROM ACTIVE DIRECTORY**



**Azure AD Connect cloud provisioning**

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

**Azure AD Connect sync**

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

**USER SIGN IN**



Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

Connectivity from the on-premises domain to the internet is lost. Which user can sign in to Azure AD?

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

Answer: B

**NEW QUESTION 85**

- (Exam Topic 4)

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

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

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

Answer: B

**NEW QUESTION 88**

- (Exam Topic 4)

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click the Exhibit tab.)

**Custom smart lockout**

Lockout threshold ⓘ  ✓

Lockout duration in seconds ⓘ  ✓

**Custom banned passwords**

Enforce custom list ⓘ  Yes  No

Custom banned password list ⓘ  ✓

**Password protection for Windows Server Active Directory**

Enable password protection on Windows Server Active Directory ⓘ  Yes  No

Mode ⓘ  Enforced  Audit

You are evaluating the following passwords:

- > Pr0jectlitw@re
- > T@ilw1nd
- > C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

Answer: C

**Explanation:**

Reference:

<https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation>

**NEW QUESTION 89**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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

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

The domain controllers are prevented from communicating to the internet. You implement Azure AD Password Protection on Server1 and Server2. You deploy a new server named Server4 that runs Windows Server 2019. You need to ensure that Azure AD Password Protection will continue to work if a single server fails. What should you implement on Server4?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 92**

- (Exam Topic 4)

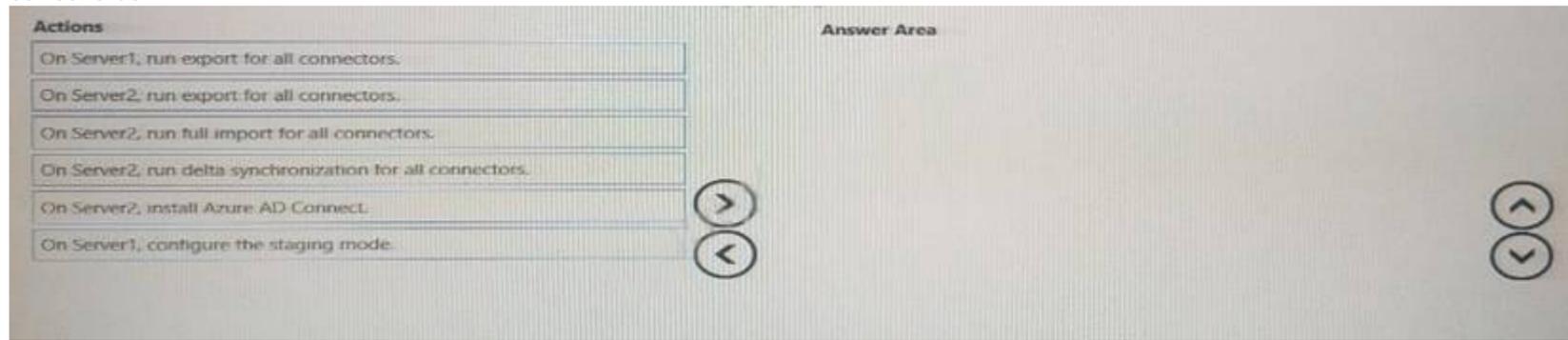
Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

Attire AD Connect is installed on a server named Server 1.

You deploy a new server named Server2 that runs Windows Server 2019.

You need to implement a failover server for Azure AD Connect. The solution must minimize how long it takes to fail over if Server1 fails.

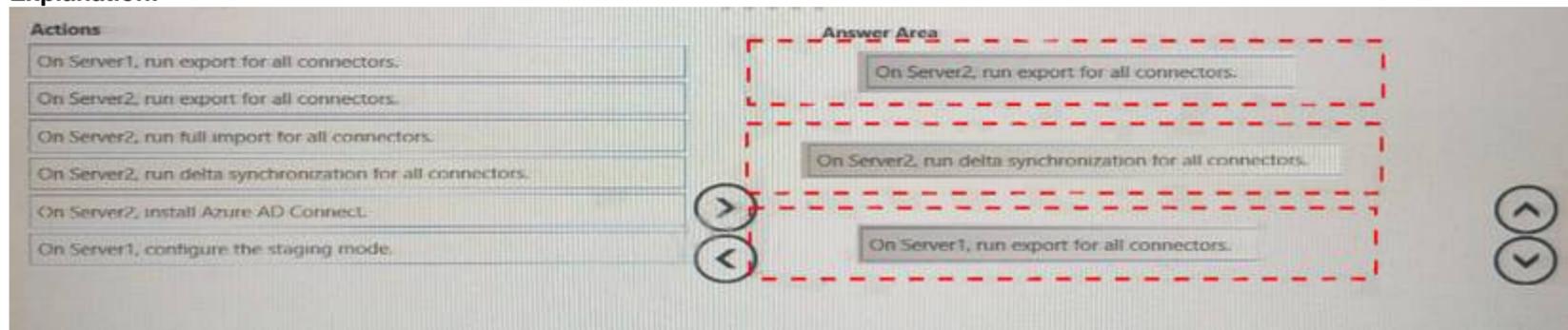
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



**NEW QUESTION 96**

- (Exam Topic 4)

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

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

User1 is the owner of Group1.

You create an access review that has the following settings:

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

Which users can perform access reviews for User3?

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

- C. User1 only
- D. User1 and User2 only

Answer: B

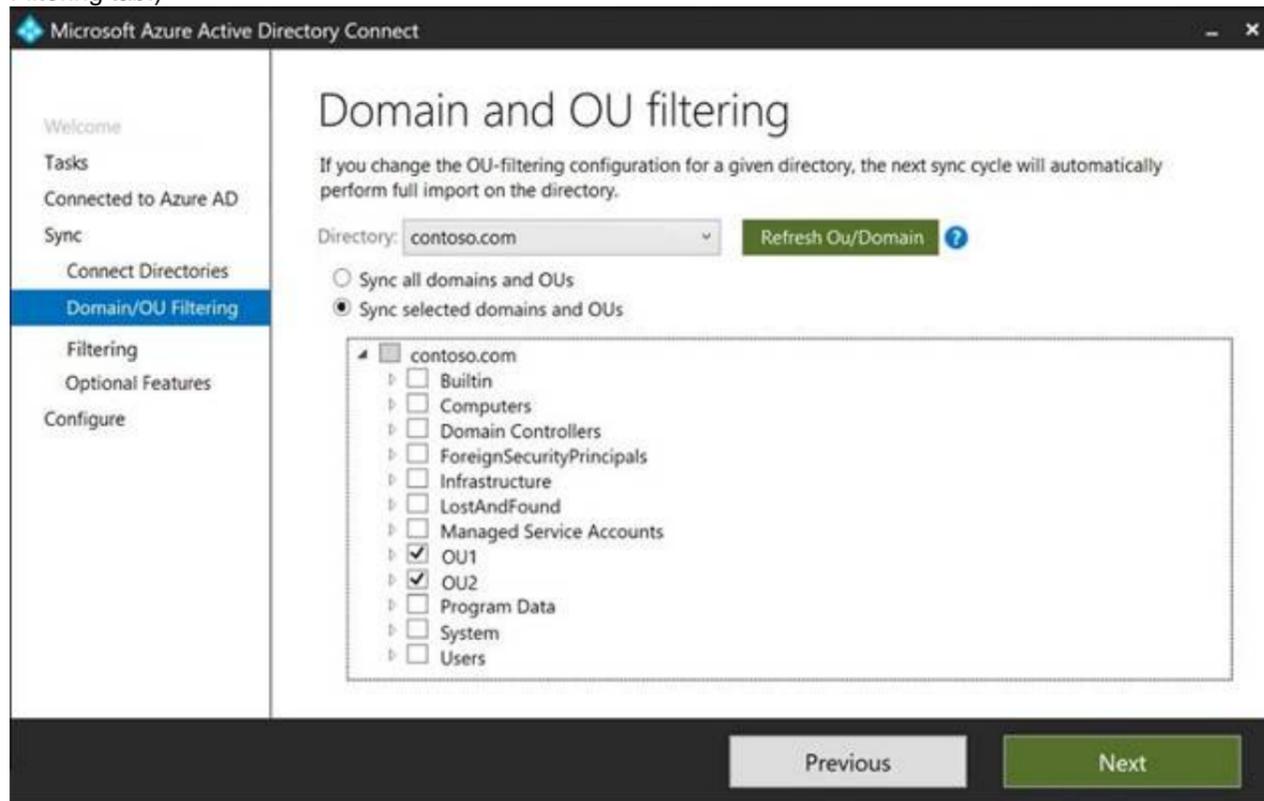
**NEW QUESTION 97**

- (Exam Topic 4)

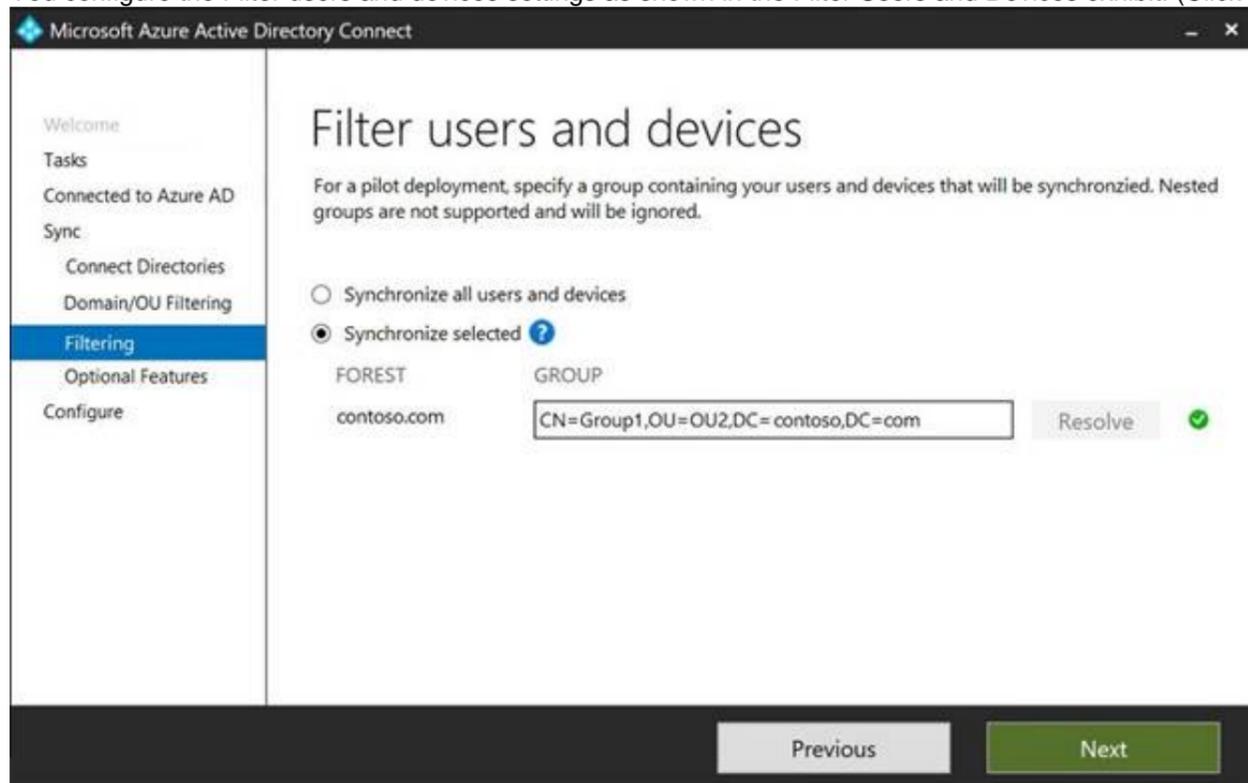
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

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

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



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



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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

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

Reference:

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

**NEW QUESTION 98**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

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

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

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

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

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app>

**NEW QUESTION 103**

- (Exam Topic 4)

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

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

You have a Microsoft 365 tenant.

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

### Create an access review

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

Review name \*

Description

Start date \*

Frequency

Duration (in days)

End  Never  End by  Occurrences

Number of times

End date

Users Scope  Everyone

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

Reviewers

(Preview) Fallback reviewers

Upon completion settings

**Start**

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

- A. Yes
- B. No

**Answer: A**

**Explanation:**

Reference:  
 D18912E1457D5D1DDCDBD40AB3BF70D5D  
<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

**NEW QUESTION 106**

- (Exam Topic 4)  
 You have an Azure Active Directory (Azure AD) tenant. You create an enterprise application collection named HR Apps that has the following settings:

- Applications: Appl. App?, App3
  - Owners: Admin 1
  - Users and groups: HRUsers
- 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. From Properties, change User assignment required to No.
- C. From Permissions, review the User consent permissions.
- D. From Single sign on, configure a sign-on method.

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 108**

- (Exam Topic 4)

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:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

**NEW QUESTION 111**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange only run email clients that use Modern authentication protocols.

What should you implement?

You need to ensure that use Modern authentication

- A. a compliance policy in Microsoft Endpoint Manager
- B. a conditional access policy in Azure Active Directory (Azure AD)
- C. an application control profile in Microsoft Endpoint Manager
- D. an OAuth policy in Microsoft Cloud App Security

**Answer:** B

**NEW QUESTION 112**

- (Exam Topic 4)

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

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

Dashboard > ContosoAzureAD > Department1 Administrative Unit

### Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory

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

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

Search users | Add filters

2 users found

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

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

Dashboard > ContosoAzureAD > Department1 Administrative Unit

### Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

>> + Add | Remove | Refresh | Columns | Preview features | Got feedback?

Search groups | Add filters

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

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

## User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
<b>User Administration</b>			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

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

## Group2 | Members

Group

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

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

Direct members

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 117**

- (Exam Topic 4)

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.

To classify leaked credentials as high-risk, use:

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

To trigger remediation, use:

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

To mitigate the risk, select:

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Graphical user interface, text, application, email Description automatically generated

Reference:

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

**NEW QUESTION 118**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

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

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

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

NOTE: Each correct selection is worth one point.

GroupA:

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

GroupB:

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:

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

**NEW QUESTION 123**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

### Money Back Guarantee

#### **SC-300 Practice Exam Features:**

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