

# Microsoft

## Exam Questions SC-300

Microsoft Identity and Access Administrator



**NEW QUESTION 1**

- (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.

Azure AD tenant-level setting to modify:

Allow users to register application

Users can consent to apps accessing company data on their behalf

Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

Application administrator

Application developer

Cloud application administrator

- 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 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 create the LWGroup1 group to meet the management requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

(user.objectId -ne

"Guest"

"Member"

null

) and (user.userType -eq

"Guest"

"Member"

null

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Null "Member"

**NEW QUESTION 4**

- (Exam Topic 1)

You need to configure the detection of multi staged attacks to meet the monitoring requirements. What should you do?

- A. Customize the Azure Sentinel rule logic.
- B. Create a workbook.
- C. Add an Azure Sentinel playbook.
- D. Add Azure Sentinel data connectors.

Answer: D

**NEW QUESTION 5**

- (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 6**

- (Exam Topic 2)

You need to implement the planned changes and technical requirements for the marketing department. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure user access:

An access package

An access review

A conditional access policy

To enable collaboration with fabrikam.com:

An accepted domain

A connected organization

A custom domain name

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:

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

**NEW QUESTION 7**

- (Exam Topic 2)

You need to meet the technical requirements for the probability that user identities were compromised. What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The users must first:

Provide consent for any app to access the data of Contoso.

Register for multi-factor authentication (MFA).

Register for self-service password reset (SSPR).

You must configure:

A sign-in risk policy

A user risk policy

An Azure AD Password Protection policy

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:

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

#### NEW QUESTION 8

- (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: B**

#### Explanation:

Role Setting details is where you need to be: Role setting details - User Administrator Privileged Identity Management | Azure AD roles

Default Setting State

Require justification on activation Yes Require ticket information on activation No On activation, require Azure MFA Yes Require approval to activate No

Approvers None

#### NEW QUESTION 9

- (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 10

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 3)

You need to implement the planned changes for Package!. Which users can create and manage the access review?

- A. User3 only
- B. User4 only
- C. User5 only
- D. User3 and User4
- E. User3 and User5
- F. User4and User5

**Answer: C**

#### NEW QUESTION 14

- (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.

You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync.

What should you do in Azure AD Connect?

- A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
- B. Configure a Full Import run profile.
- C. Create an inbound synchronization rule for the Active Directory Domain Services connector.
- D. Configure an Export run profile.

**Answer: C**

#### Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

#### NEW QUESTION 19

- (Exam Topic 4)

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

⏪

⏩

⏴

⏵

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
A picture containing application Description automatically generated  
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>

NEW QUESTION 20

- (Exam Topic 4)  
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 plan to create an access package named package1 that will be accessible only to the users at Fabrikam. 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.

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:**  
Text Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-re> <https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cr>

NEW QUESTION 21

- (Exam Topic 4)  
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. An administrator deletes User1. You need to identify the following:  
• How many days after the account of User1 is deleted can you restore the account?  
• Which is the least privileged role that can be used to restore User1?  
What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>



**Answer Area**



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**



**NEW QUESTION 25**

- (Exam Topic 4)

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

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

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

What is a valid authentication method available to users?

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

**Answer:** A

**NEW QUESTION 29**

- (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 33**

- (Exam Topic 4)

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Identity Governance blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Licenses blade in the Azure Active Directory admin center
- D. the Set-WindowsProductKey cmdlet

**Answer:** C

**NEW QUESTION 36**

- (Exam Topic 4)

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 41**

- (Exam Topic 4)

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

- Name: Group1
- Members: User1, User2
- Owner: User3

On January 15, 2021, you create an access review as shown in the exhibit. (Click the Exhibit tab.)

## Create an access review

**Review name \***

**Description ⓘ**

**Start date \***

**Frequency**

**Duration (in days) ⓘ**

**End ⓘ** ☐ Never ☒ End by ☐ Occurrences

**Number of times**

**End date \***

**Users**

**Users to review**

**Scope** ☐ Guest users only ☒ Everyone

**Group \***

**Reviewers**

**Reviewers**

**Programs**

**Start**

Users answer the Review1 question as shown in the following table.

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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 February 5, 2021, User1 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered



**Answer:** A

**Explanation:**

A screenshot of a computer Description automatically generated with low confidence

Reference:

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

**NEW QUESTION 43**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You have an Active Directory domain that syncs to the Azure Active Directory {Azure AD) tenant. 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. Cloud App Discovery in Microsoft Defender for Cloud Apps

B. enterprise applications in Azure AD

C. access reviews in Azure AD

D. Application Insights in Azure Monitor

**Answer:** A

**NEW QUESTION 48**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users 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 AD 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 users can sign in to Azure AD?

A. User1 and User3 only

B. User1 only

C. User1, User2, and User3

D. User1 and User2 only

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 50**

- (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.	<input type="radio"/>	<input type="radio"/>
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to <b>Yes</b> .	<input type="radio"/>	<input type="radio"/>
Admin2 is a local administrator on Device3.	<input type="radio"/>	<input type="radio"/>

- 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 55**

- (Exam Topic 4)

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



New

Conditional access policy

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

Name \*

Policy1

Assignments

Users and groups ⓘ

Specific users included

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only

On

Off

Create

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 and external users ⓘ

Directory roles ⓘ

Users and groups

Select

1 user

US

User1

user1@sk200922outlook.onm...

...

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

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

Conditions settings

Enable policy setting

Grant settings

Sessions settings

Users and groups setting

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

Conditions settings

Enable policy setting

Grant settings

Sessions settings

Users and groups setting

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 56

- (Exam Topic 4)

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

- Pa55w0rd12
- Pa55w0rd12
- Pa55w0rd12
- Pa55w.rd12
- Pa55w.rd123
- Pa55w.rd123
- Pa55w.rd123
- Pa55word12
- Pa55word12
- Pa55word12
- Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.  
What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

Tracked sign-in attempts:

	▼
4	
5	
10	
11	

Unlock by:

	▼
Clearing the browser cache	
Signing in by using inPrivate browsing mode	
Performing a self-service password reset (SSPR)	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Graphical user interface, text, table Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

NEW QUESTION 61

- (Exam Topic 4)  
You have a Microsoft 365 tenant.  
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.  
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.  
You need to block the users automatically when they report an MFA request that they did not initiate. Solution: From the Azure portal, you configure the Fraud alert settings for multi-factor authentication (MFA). Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:  
The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.  
The following fraud alert configuration options are available:

- > Automatically block users who report fraud.
- > Code to report fraud during initial greeting. Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

NEW QUESTION 63

- (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.

Account lockout

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

Number of MFA denials to trigger account lockout \*

3

Minutes until account lockout counter is reset \*

60

Minutes until account is automatically unblocked \*

30

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



**Answer Area**

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

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

email address

Microsoft Authenticator app code

password

30

60

90

- 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 65**

- (Exam Topic 4)  
 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 AD, you create an assignment for the Insights at administrator role. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 67**

- (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 68**

- (Exam Topic 4)  
**HOTSPOT**  
 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.	<input type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 70

- (Exam Topic 4)  
You have a Microsoft 365 tenant.  
In Azure Active Directory (Azure AD), you configure the terms of use.  
You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.  
What should you configure?

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

Answer: C

Explanation:

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

NEW QUESTION 72

- (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

Sign in to the Microsoft 365 admin center.

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.

Answer Area

⏮

⏭

⏮

⏭

- 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 74

- (Exam Topic 4)  
You have a Microsoft 365 subscription that contains the following:

- An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
- A Microsoft SharePoint Online site named Site1
- A Microsoft Teams team named Team1

You need to create an entitlement management workflow to manage Site1 and Team1. What should you do first?

- A. Create an access package.
- B. Create a catalog.
- C. Create an administrative unit.
- D. Configure an app registration.

Answer: A

NEW QUESTION 75

- (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 76**

- (Exam Topic 4)

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 79**

- (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 83**

- (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 85**

- (Exam Topic 4)

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

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

**Answer:** B

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

**NEW QUESTION 88**

- (Exam Topic 4)

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

Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure AD Identity Protection.  
Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Configure the user risk policy:

User3 only

User3 and User4 only

User1, User2, and User3 only

User1, User3, and User4 only

User1, User2, User3, and User4

View the risky users report:

User3 only

User3 and User4 only

User1, User2, and User3 only

User1, User3, and User4 only

User1, User2, User3, and User4

- 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/identity-protection/overview-identity-protection>

**NEW QUESTION 89**

- (Exam Topic 4)

You have an Azure subscription that contains the custom roles shown in the following table.

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role. Which roles can you clone to create Role3?

- A. Role2 only
- B. built-in Azure subscription roles only
- C. built-in Azure subscription roles and Role2 only
- D. built-in Azure subscription roles and built-in Azure AD roles only
- E. Role1, Role2 built-in Azure subscription roles, and built-in Azure AD roles

**Answer:** A

**NEW QUESTION 91**

- (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 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 98

- (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.)

The screenshot shows the 'Domain and OU filtering' configuration window in Microsoft Azure Active Directory Connect. The left sidebar has tabs for 'Welcome', 'Tasks', 'Connected to Azure AD', 'Sync', 'Connect Directories', 'Domain/OU Filtering' (selected), 'Filtering', 'Optional Features', and 'Configure'. The main area is titled 'Domain and OU filtering' and contains the following elements:

- A message: 'If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.'
- A 'Directory:' dropdown menu set to 'contoso.com' and a 'Refresh Ou/Domain' button.
- Two radio buttons: 'Sync all domains and OUs' (unselected) and 'Sync selected domains and OUs' (selected).
- A tree view showing the directory structure for 'contoso.com'. The 'OU1' and 'OU2' checkboxes are selected, while others are not.
- 'Previous' and 'Next' buttons at the bottom.

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

The screenshot shows the 'Filter users and devices' configuration window in Microsoft Azure Active Directory Connect. The left sidebar is the same as the previous window, with 'Filtering' selected. The main area is titled 'Filter users and devices' and contains the following elements:

- A message: 'For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.'
- Two radio buttons: 'Synchronize all users and devices' (unselected) and 'Synchronize selected' (selected).
- Fields for 'FOREST' (set to 'contoso.com') and 'GROUP' (set to 'CN=Group1,OU=OU2,DC=contoso,DC=com').
- A 'Resolve' button and a green checkmark icon.
- 'Previous' and 'Next' buttons at the bottom.

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 103**

- (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 106**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

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

You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD.

Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.

You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency. What should you do?

- A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
- B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.
- C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
- D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

**Answer:** A

**NEW QUESTION 110**

- (Exam Topic 4)

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 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 (MFA) registration policy1.
- D. Configure password protection for Windows Server Active Directory.

**Answer:** B

**NEW QUESTION 115**

- (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:

- Identify sign-ins by users who are suspected of having leaked credentials.
- Flag 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.

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:**

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

#### NEW QUESTION 117

- (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 121

- (Exam Topic 4)

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

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

You have a Microsoft 365 tenant.

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

## Create an access review

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

Review name \*

Description

Start date \*

Frequency

Duration (in days)

End ☐ Never ☐ End by ☐ Occurrences

Number of times

End date

Users

Scope ☒ Everyone

Review role membership (permanent and eligible) \*

[Application Administrator and 72 others](#)

Reviewers

Reviewers

(Preview) Fallback reviewers

Upon completion settings

**Start**

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

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

Solution: You set Reviewers to Member (self).

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

### NEW QUESTION 126

- (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 129

- (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 133

- (Exam Topic 4)

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

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

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

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

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

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

- A. Yes
- B. No

Answer: B

NEW QUESTION 136

- (Exam Topic 4)

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com. You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 users.

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

Actions

Delete the contoso.onmicrosoft.com domain.

Register a custom domain name of contoso.com.

Set the domain to primary.

Create a new TXT record in DNS.

Verify the domain name.

Answer Area

<

>

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated with medium confidence

Reference:

<https://practical365.com/configure-a-custom-domain-in-office-365/>

NEW QUESTION 140

- (Exam Topic 4)

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company is developing a web service named App1.

You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.

Which three actions should yon 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

Create an app registration.

Add a group claim.

Add app permissions.

Grant admin consent.

Add delegated permissions.

Answer Area

>

<

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A



**Explanation:**

Graphical user interface, text, application Description automatically generated

> Create an app registration:

Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.

> Grant admin consent:

Higher-privileged permissions require administrator consent.

> Add app permissions:

After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity. Encoded inside the access token is every permission that your app has been granted for that resource.

Reference:

<https://docs.microsoft.com/en-us/graph/auth/auth-concepts>

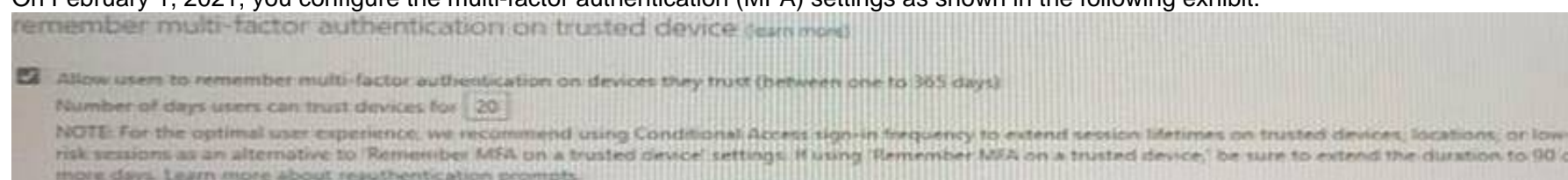
**NEW QUESTION 144**

- (Exam Topic 4)

You create the Azure Active Directory (Azure AD) users shown in the following table.

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.



The users authentication to Azure AD on their devices as shown in the following table.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

On February 26, 2021, what will the multi-factor auth status be for each user?

A)

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B)

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C)

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D)

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

**NEW QUESTION 149**

- (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 \*

Admin review

Description ⓘ

Start date \*

12/18/2020

Frequency

Monthly

Duration (in days) ⓘ

14

End ⓘ

Never

End by

Occurrences

Number of times

0

End date

01/17/2021

Users

Scope

Everyone

Review role membership (permanent and eligible) \*

Application Administrator and 72 others

Reviewers

Reviewers

(Preview) Manager

(Preview) Fallback reviewers ⓘ

Megan Bowen

Upon completion settings

Start

You discover that all access review requests are received by Megan Bowen.  
 You need to ensure that the manager of each department receives the access reviews of their respective department.  
 Solution: You add each manager as a fallback reviewer. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

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

**NEW QUESTION 153**

- (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 156

.....

## 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](#)**