Vendor: Microsoft

Exam Code:SC-300

Exam Name: Microsoft Identity and Access Administrator

Version: Demo

QUESTION 1

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.

Correct Answer: C

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-unblock https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

---

QUESTION 2

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.

Correct Answer: B

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

---

QUESTION 3

Your company purchases 2 new Microsoft 365 ES subscription and an app named App.

You need to create a Microsoft Defender for Cloud Apps access policy for App1.

What should you do you first? (Choose Correct Answer based on Microsoft Identity and Access Administrator at microsoft.com)

A. Configure a Token configuration for App1.

B. Add an API permission for App.

C. Configure a Conditional Access policy to use app-enforced restrictions.

D. Configure a Conditional Access policy to use Conditional Access App Control.

Correct Answer: C

https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad To create a Microsoft Defender for Cloud Apps access policy for App1, you should configure a Conditional Access policy to use app-enforced restrictions. This will allow you to control access to your cloud apps based on conditions such as user, device, location, and app state. You can also use app-enforced restrictions to control access to your cloud apps based on the state of the app, such as whether it\\'s running on a managed or unmanaged device.

QUESTION 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 Account lockout settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

You need to configure the fraud alert settings.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

---

QUESTION 5

HOTSPOT

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

1.

Users that are assigned Role1 can create or delete instances of Azure Container Apps.

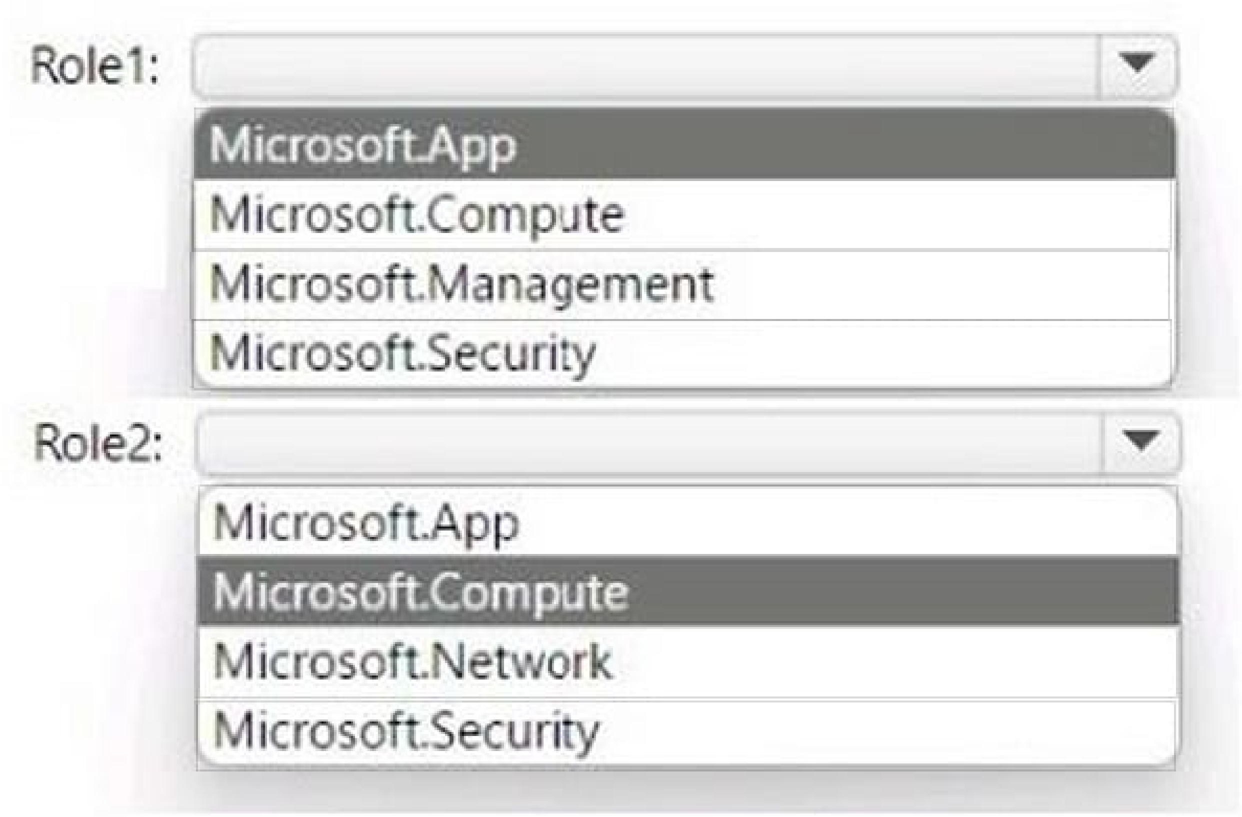
2.

Users that are assigned Role2 can enforce adaptive network hardening rules.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



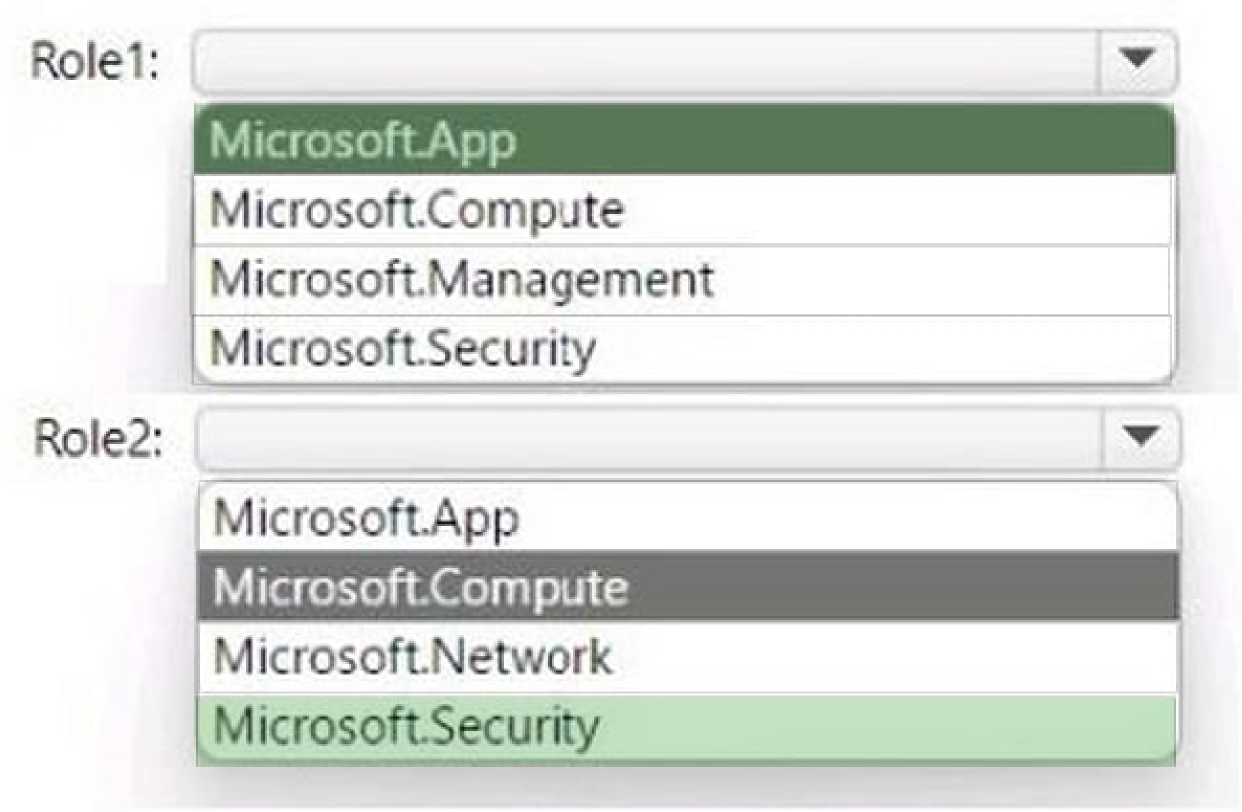
Role1:

- Microsoft.App
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

Role2:

- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security

Correct Answer:



Role1:

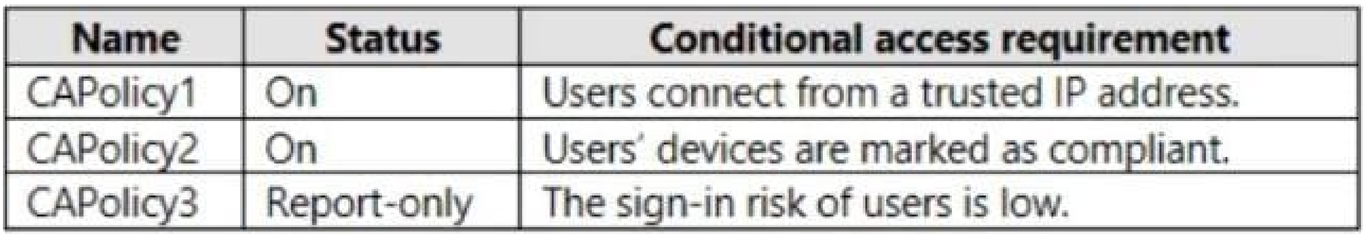
- [✓ Microsoft.App]
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

Role2:

- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- [✓ Microsoft.Security]

QUESTION 6

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



Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

You need to evaluate which policies will be applied to User1 when User1 attempts to sign-in from various IP addresses. Which feature should you use?

A. Access reviews

B. Identity Secure Score

C. The What If tool

D. the Microsoft 365 network connectivity test tool

Correct Answer: C

QUESTION 7

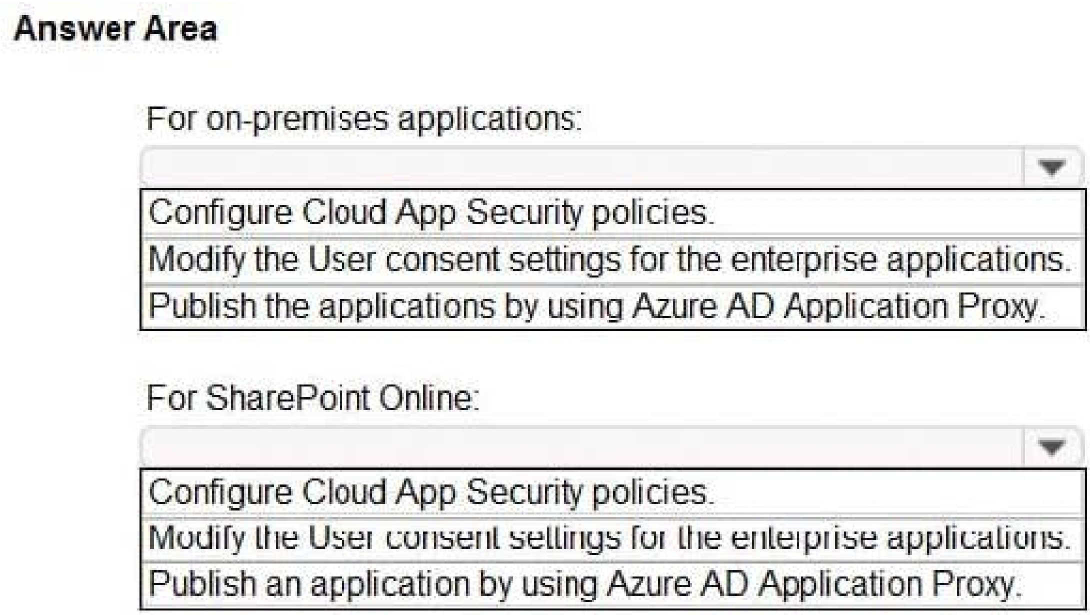
HOTSPOT

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

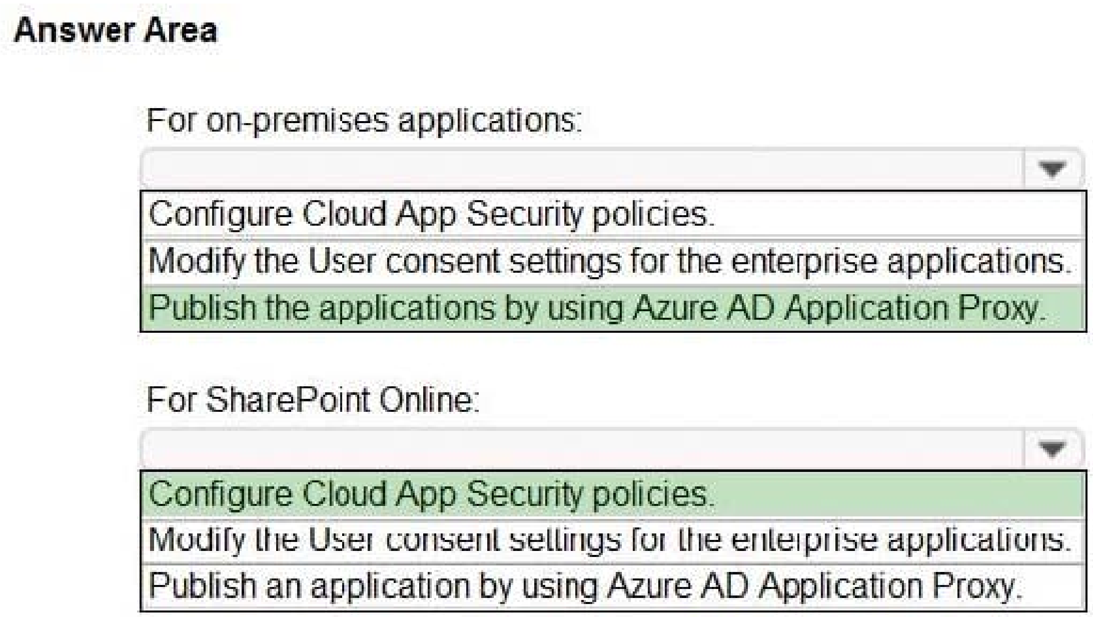
For on-premises applications:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

Correct Answer:



Answer Area

For on-premises applications:

▼

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- [✓ Publish the applications by using Azure AD Application Proxy.]

For SharePoint Online:

▼

- [✓ Configure Cloud App Security policies.]
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

Reference: https://docs.microsoft.com/en-us/sharepoint/app-enforced-restrictions https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

---

QUESTION 8

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the User Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 9

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

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain.

The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. an Azure AD Password Protection proxy

C. Network Policy Server (NPS)

D. a pass-through authentication proxy

Correct Answer: C

QUESTION 10

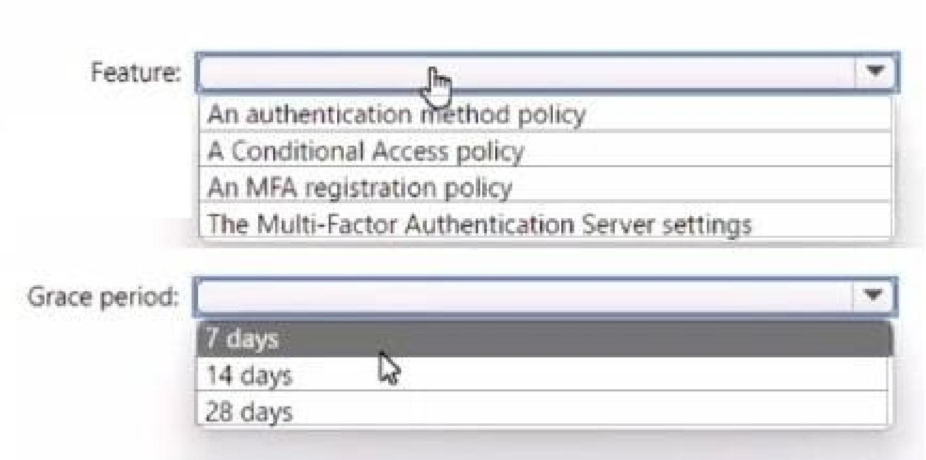
HOTSPOT

You need to support the planned changes and meet the technical requirements for MFA.

Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.

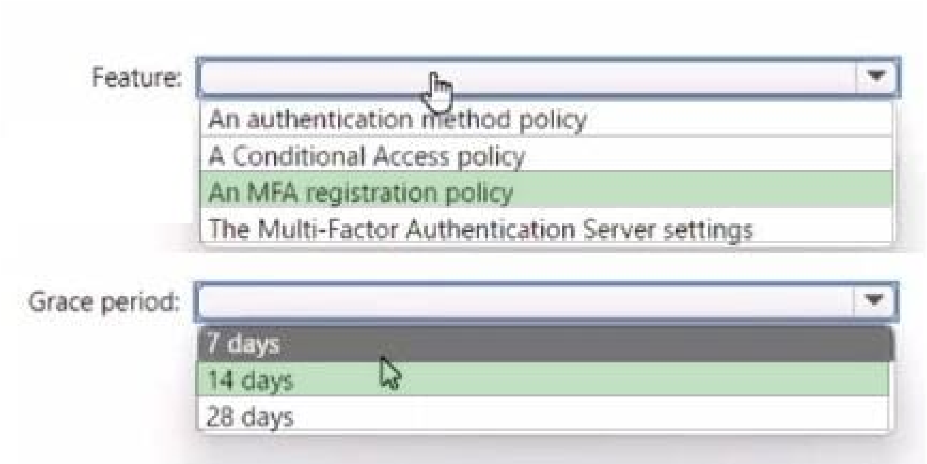
NOTE: Each correct selection is worth one point.

Hot Area:



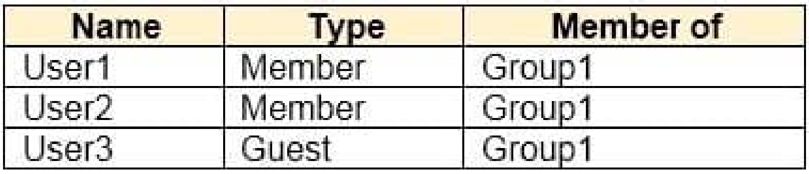
Feature:
An authentication method policy
A Conditional Access policy
An MFA registration policy
The Multi-Factor Authentication Server settings
Grace period:
7 days
14 days
28 days

Correct Answer:


Feature:
An authentication method policy
A Conditional Access policy
An MFA registration policy
The Multi-Factor Authentication Server settings
Grace period:
7 days
14 days
28 days

QUESTION 11

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:

1.

Users to review: Members of a group

2.

Scope: Everyone

3.

Group: Group1

4.

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

Correct Answer: B

QUESTION 12

You need to resolve the issue of the guest user invitations. What should you do for the Azure AD tenant?

A. Configure the Continuous access evaluation settings.

B. Modify the External collaboration settings.

C. Configure the Access reviews settings.

D. Configure a Conditional Access policy.

Correct Answer: B