

SC-300^{Q&As}

Microsoft Identity and Access Administrator

Pass Microsoft SC-300 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/sc-300.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

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-AzureADMSInvitation cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Implement Azure AD Connect.

Correct Answer: A

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

QUESTION 2

You need to implement the planned changes for litware.com. What should you configure?

- A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com
- B. Azure AD Connect to include the litware.com domain
- C. staging mode in Azure AD Connect for the litware.com domain

Correct Answer: C

QUESTION 3

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

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

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

What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments after from the Role settings details

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

Correct Answer: D

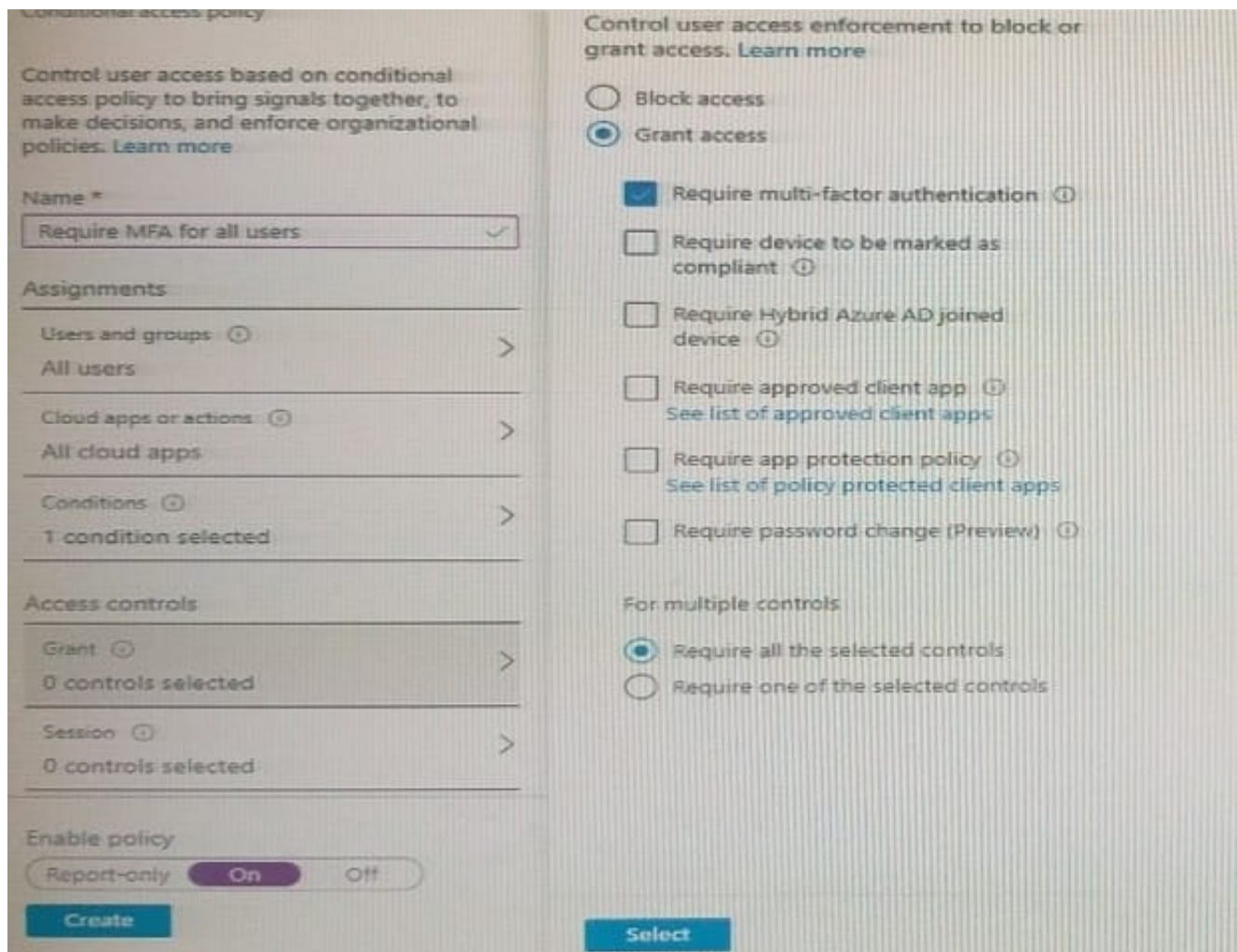
Reference: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 4

HOTSPOT

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)



You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)

Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s), 0 Group

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

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

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	Membership
User Administrator				
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin3	Admin3@m365x629615.onmicrosoft.com	User	Directory	Direct

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

Hot Area:

- | | Yes | No |
|--|-----------------------|-----------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve The activation request. | <input type="radio"/> | <input type="radio"/> |
| Admin2 can request activation of the User Administrator role for a period of two hours. | <input type="radio"/> | <input type="radio"/> |
| If Admin3 connects to the Azure Active Directory admin Center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using Multi-factor authentication (MFA) twice. | <input type="radio"/> | <input type="radio"/> |

Correct Answer:

- | | Yes | No |
|--|----------------------------------|----------------------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve The activation request. | <input checked="" type="radio"/> | <input type="radio"/> |
| Admin2 can request activation of the User Administrator role for a period of two hours. | <input checked="" type="radio"/> | <input type="radio"/> |
| If Admin3 connects to the Azure Active Directory admin Center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using Multi-factor authentication (MFA) twice. | <input type="radio"/> | <input checked="" type="radio"/> |

QUESTION 5

HOTSPOT

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.

Hot Area:

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

<input type="checkbox"/>	An app registration in Azure AD
<input type="checkbox"/>	Azure AD Application Proxy
<input type="checkbox"/>	An enterprise application in Azure AD
<input type="checkbox"/>	A managed identity in Azure AD

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

<input type="checkbox"/>	Azure AD Application Proxy
<input type="checkbox"/>	A compliance policy
<input type="checkbox"/>	A conditional access policy
<input type="checkbox"/>	An OAuth policy

Correct Answer:

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

<input type="checkbox"/>	An app registration in Azure AD
<input type="checkbox"/>	Azure AD Application Proxy
<input checked="" type="checkbox"/>	An enterprise application in Azure AD
<input type="checkbox"/>	A managed identity in Azure AD

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

<input type="checkbox"/>	Azure AD Application Proxy
<input type="checkbox"/>	A compliance policy
<input checked="" type="checkbox"/>	A conditional access policy
<input type="checkbox"/>	An OAuth policy

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>

[Latest SC-300 Dumps](#)

[SC-300 Exam Questions](#)

[SC-300 Braindumps](#)