



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ---- Guaranteed.



SC-300 MCQs  
SC-300 Exam Questions  
SC-300 Practice Test  
SC-300 TestPrep  
SC-300 Study Guide



[killexams.com](http://killexams.com)

**Microsoft**

# SC-300

*Microsoft Identity and Access Administrator*

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/SC-300>



### Question: 29

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>

### Question: 30

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>

### Question: 31

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



<a href="#">Federation</a>	Disabled	0 domains
<a href="#">Seamless single sign-on</a>	Disabled	0 domains
<a href="#">Pass-through authentication</a>	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>

### Question: 32

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

### Question: 33

HOTSPOT

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	

**Answer: B**

Explanation:

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>

**Question: 34**

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. Entitlement management settings
- C. Terms of use
- D. Access reviews setting

**Answer: B**

Explanation:

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

### Question: 35

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

You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the past.

For how long does Azure AD store events in the sign-in logs?

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

### Answer: B

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-dataretention#how-long-does-azure-ad-store-the-data>

### Question: 36

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 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>

## Question: 37

### HOTSPOT

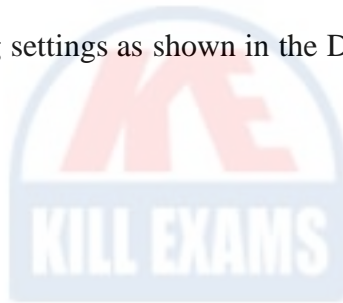
Your network contains an on-premises Active Directory domain named contoso.com.

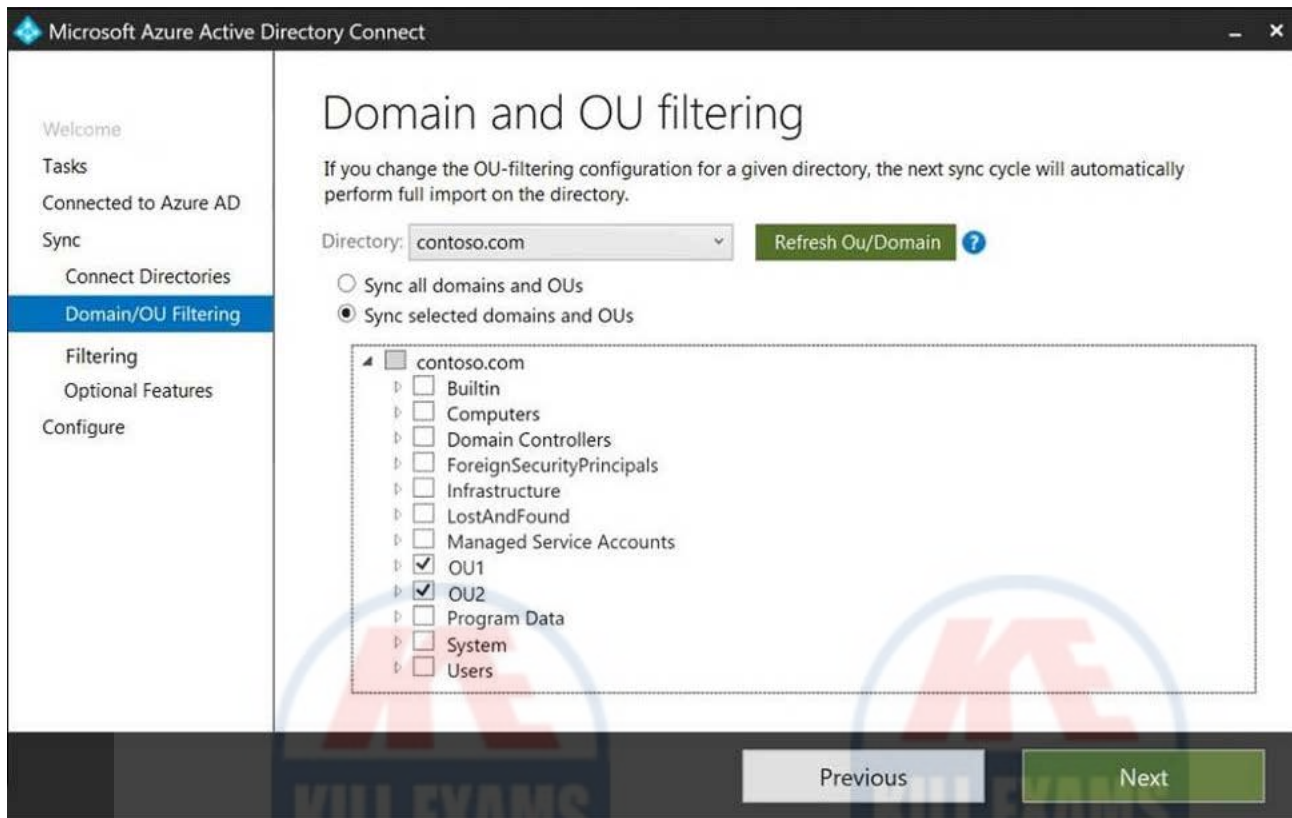
The domain contains the objects shown in the following table.

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.

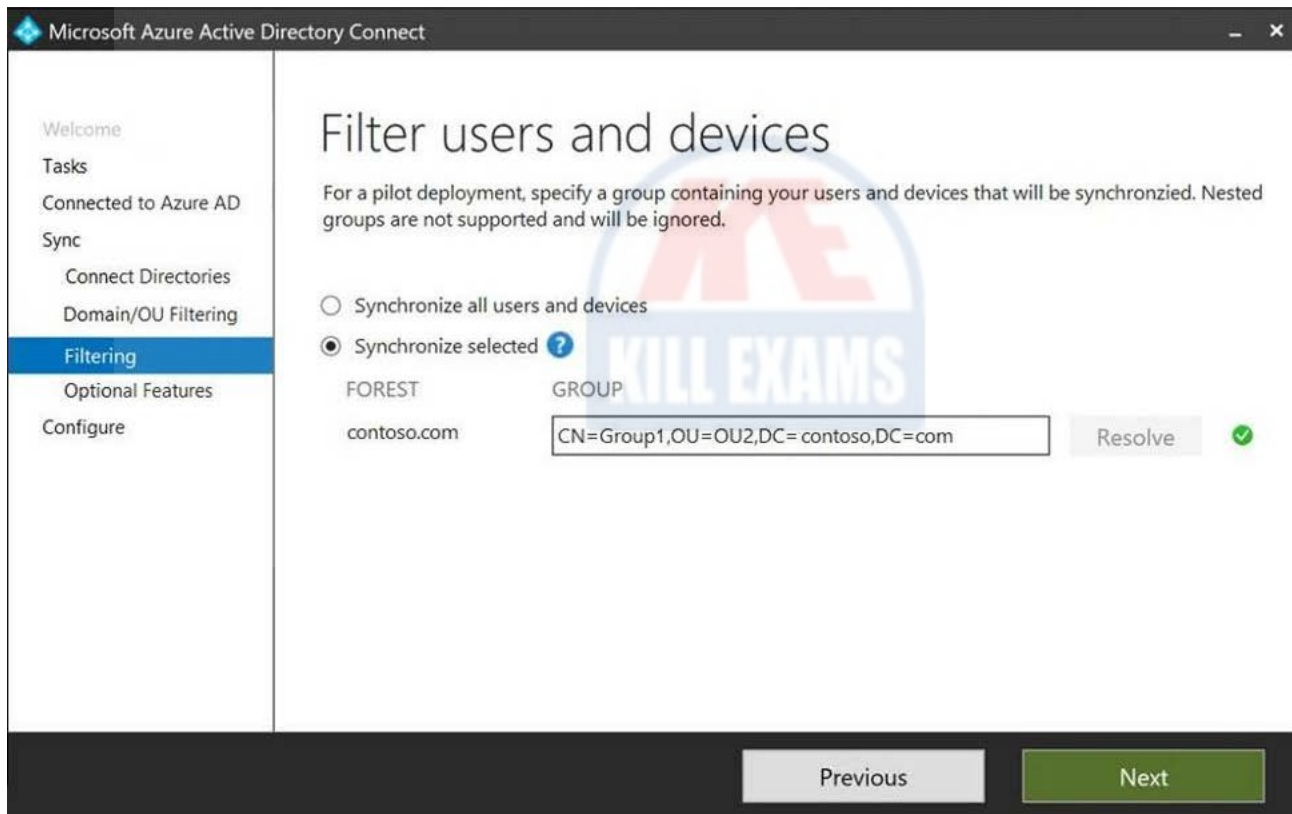
You install Azure AD Connect.

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.

User2 syncs to Azure AD.

Group2 syncs to Azure AD.

### Answer: B

Explanation:

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>

### Question: 38

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 notification through the Microsoft Authenticator app
- B. an app password
- C. Windows Hello for Business
- D. SMS

### Answer: C

Explanation:

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and

Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Reference:

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

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

### Question: 39

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.

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 Notifications 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>

### Question: 40

HOTSPOT

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

**Answer: B**

Explanation:

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

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



## Exam Questions Based on Current Exam Objectives

Killexams.com provides exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these questions, candidates will become cover the structure, difficulty level, and topic coverage of the actual exam, helping them prepare more effectively and efficiently.

## Comprehensive Exam MCQs (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

## Realistic Practice Tests (Online & Desktop)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Exam Simulator. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

## Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

## Regularly Updated Content

Our question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying relevant material and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.