

[Download Full Version SC-300 Exam Dumps\(Updated in March/2023\)](#)

Correct Answer: A

QUESTION 39

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant-

Users sign in to computers that run Windows 10 and are joined to the domain.

You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).

You need to configure the computers for Azure AD Seamless SSO.

What should you do?

- A. Enable Enterprise State Roaming.
- B. Configure Sign-in options.
- C. Install the Azure AD Connect Authentication Agent.
- D. Modify the Intranet Zone settings.

Correct Answer: D

QUESTION 40

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

Correct Answer: A

QUESTION 41

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

[SC-300 Exam Dumps](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#) [SC-300 Q&As](#)

<https://www.ensurepass.com/SC-300.html>

[Download Full Version SC-300 Exam Dumps\(Updated in March/2023\)](#)

- B. redirection URL
- C. username
- D. shared key
- E. password

Correct Answer: AB

QUESTION 42

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.

You create an Azure Sentinel instance and configure the Azure Active Directory connector.

You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.

What should you do first?

- A. Add an Azure Sentinel data connector.
- B. Configure the Notify settings in Azure AD Identity Protection.
- C. Create an Azure Sentinel playbook.
- D. Modify the Diagnostics settings in Azure AD.

Correct Answer: A

QUESTION 43

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

QUESTION 44

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

[Download Full Version SC-300 Exam Dumps\(Updated in March/2023\)](#)

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you modify the Diagnostics settings.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

QUESTION 45

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

QUESTION 46

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

And 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?

- 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.

Correct Answer: A

[Download Full Version SC-300 Exam Dumps\(Updated in March/2023\)](#)

QUESTION 47

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.)

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

Correct Answer: A

QUESTION 48

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.

Correct Answer: A

QUESTION 49

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.

[Download Full Version SC-300 Exam Dumps\(Updated in March/2023\)](#)

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 Administrative units blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Groups blade in the Azure Active Directory admin center
- D. the Sec-MsolUserLicense cmdlet

Correct Answer: D

QUESTION 50

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.

Correct Answer: C

QUESTION 51

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

Correct Answer: A

QUESTION 52

Note: This question is part of a series of questions that present the same scenario. Each question

[SC-300 Exam Dumps](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#) [SC-300 Q&As](#)

<https://www.ensurepass.com/SC-300.html>