

PRACTICE QUESTIONS

Microsoft

AB-650

Microsoft 365 and AI Services Administrator Associate

SHARED BY [u/ab650_notes](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 18, 2026
EXAM	Microsoft AB-650, Microsoft 365 and AI Services Administrator Associate

Shared by [u/ab650_notes](#) on aiexamcerts

10 practice questions for the Microsoft AB-650 exam, Microsoft 365 and AI Services Administrator Associate, each followed by its answer and a short explanation. More free sets and the full practice exam: aiexamcerts.com/microsoft/ab-650. Spotted a mistake? Email support@aiexamcerts.com with the exam code AB-650 and the question number.

1. Which setting controls how the organization's name and profile information appear across Microsoft 365?

- A Device groups in the Defender portal
- B Hub site navigation in SharePoint only, which controls the menus across team sites
- C Organization profile settings in the Microsoft 365 admin center
- D Message trace results in Exchange

Answer: C

The organization profile settings in the Microsoft 365 admin center hold the tenant's name and profile details that services display. Defender device groups, SharePoint hub navigation and message trace results do not hold this profile information.

2. Which two practices help an administrator monitor the health of Microsoft 365 services? (Choose two.)

- A Subscribe to service health notifications
- B Review service health incidents in the admin center regularly
- C Turn off all notifications to reduce alert noise
- D Check only the local Outlook cache on one computer
- E Delete old service advisories to keep the list short

Answer: A, B

Subscribing to notifications delivers incidents and advisories as they happen, and reviewing service health in the admin center confirms the current status. Turning off notifications and deleting advisories hide problems, and one computer's Outlook cache says nothing about tenant-wide service health.

3. Sign-ins from unfamiliar locations are flagged as risky for certain users. Which Microsoft Entra feature detects risky sign-ins and users?

- A Exchange mailbox audit logging
- B A SharePoint site template
- C The Teams app catalog
- D Microsoft Entra ID Protection

Answer: D

Microsoft Entra ID Protection calculates sign-in and user risk from signals such as unusual locations and feeds policies that respond to it. Mailbox audit logs, site templates and the app catalog do not evaluate sign-in risk.

4. A Conditional Access policy can require multifactor authentication for sign-ins that meet conditions such as a specific application or location.
- A True
 - B False

Answer: A (True)

Conditional Access evaluates conditions such as the user, application, location and risk, then applies a grant control such as requiring multifactor authentication. The statement is true.

5. Users must be blocked from choosing common or easily guessed passwords. Which Microsoft Entra capability does this?
- A Microsoft Entra Password Protection with a banned password list
 - B Disabling all password changes for every user
 - C One shared password for each department
 - D Setting passwords to never expire for all users, so that no password is ever checked again

Answer: A

Microsoft Entra Password Protection checks new passwords against a global and custom banned password list, so common or guessable choices are rejected. Disabling password changes, shared department passwords and never-expiring passwords each weaken the account security the requirement is meant to protect.

6. Self-service password _____ (SSPR) lets users reset their own forgotten password without contacting an administrator.

Answer: reset

Self-service password reset is the Microsoft Entra feature that lets users prove their identity and set a new password themselves. The word in the feature name is reset. It is configured separately from password protection.

7. A user cannot sign in after a password reset, and the administrator needs to see the failure reasons. Where should the administrator look?
- A The Teams call quality dashboard
 - B The Microsoft Entra sign-in logs
 - C The SharePoint storage metrics
 - D The Exchange transport rules list

Answer: B

The Microsoft Entra sign-in logs record each sign-in attempt with its result and failure reason, such as an invalid password or a blocked policy. Call quality, storage metrics and transport rules do not record sign-in outcomes.

8. A team member needs a privileged role only for short periods and must have approval before activation. Which configuration fits?
- A A permanent Global Administrator assignment for the person
 - B A shared administrator password stored in a team document
 - C An eligible assignment in Privileged Identity Management with activation approval
 - D A guest invitation with the admin role, sent to a personal email address outside the company

Answer: C

Privileged Identity Management provides eligible assignments that are activated only when needed, for a limited time and optionally after approval, with an audit trail. Permanent assignments keep standing privilege, a shared password cannot be attributed to one person, and a guest invitation is not a role grant model.

9. A regional helpdesk should manage users in one region only, not across the whole tenant. Which Microsoft Entra object scopes the administrator's role?
- A A shared mailbox
 - B A Teams channel
 - C A SharePoint hub site that groups related team sites under one navigation
 - D An administrative unit

Answer: D

An administrative unit is a container of users or groups, and a role assigned on it applies only to the members of that unit. A shared mailbox, a Teams channel and a hub site cannot scope an Entra administrator role.

10. Which two statements about groups in Microsoft 365 and Microsoft Entra are correct? (Choose two.)
- A A Microsoft 365 group provides a shared mailbox, a site and a team together
 - B A security group can grant access to resources but does not provide a group mailbox
 - C Dynamic membership is available only for on-premises groups
 - D Guest users cannot be members of any group
 - E Each group must have exactly one owner by policy

Answer: A, B

A Microsoft 365 group bundles a mailbox, a SharePoint site and optionally a team, while a security group controls access to resources without a mailbox. Dynamic membership applies to cloud groups, guests can be group members, and no policy requires exactly one owner.