

Question: 371

CertyIQ

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You create an access review for Azure Active Directory (Azure AD) roles.

You need to ensure that users who do not respond to review requests are removed automatically from the roles.

The solution must minimize administrative effort.

Which two settings should you modify? To answer, select the settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Reviewers

Reviewers

Members (self)



^ Upon completion settings

Auto apply results to resource ⓘ

Enable

Disable

If reviewers don't respond ⓘ

No change



Action to apply on denied guest users ⓘ

Remove user's membership from the resource



(Preview) At end of review, send notification to

+ Select User(s) or Group(s)

^ Advanced settings

Show recommendations ⓘ

Enable

Disable

Require reason on approval ⓘ

Enable

Disable

Mail notifications ⓘ

Enable

Disable

Reminders ⓘ

Enable

Disable

Additional content for reviewer email ⓘ

HOTSPOT

-

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. An administrator deletes User1.

You need to identify the following:

- How many days after the account of User1 is deleted can you restore the account?
- Which is the least privileged role that can be used to restore User1?

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

NOTE: Each correct selection is worth one point.

Answer Area

Number of days:

▼
15
30
90
180

Role:

▼
User administrator
Network administrator
Helpdesk administrator
Domain name administrator

Question: 373

HOTSPOT

You have an Azure AD tenant that contains the groups shown in the following exhibit.

You have an Azure AD tenant that contains the groups shown in the following exhibit.

☐	Name	Group Type	Membership Type	Source	Security enabled
☐	All Company	Microsoft 365	Assigned	Cloud	No
☐	Group1	Microsoft 365	Assigned	Cloud	Yes
☐	Group2	Security	Assigned	Cloud	Yes
☐	Group3	Security	Dynamic	Cloud	Yes
☐	Group4	Security	Assigned	Windows Server AD	Yes

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

You can add a managed identity to <answer choice>.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

You can add an Azure AD cloud user to <answer choice>.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

Question: 375

DRAG DROP

You have a Microsoft 365 E5 subscription.

You need to perform the following tasks:

- Identify the locations and IP addresses used by Azure AD users to sign in.
- Review the Azure AD security settings and identify improvement recommendations.
- Identify changes to Azure AD users or service principals.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Resources

Audit logs

Identity secure score

Provisioning logs

Sign-in logs

Answer Area

Identify the locations and IP addresses used by Azure AD users to sign in:

Identify changes to Azure AD users or service principals:

Review the Azure AD security settings and identify improvement recommendations:

Question: 376

CertyIQ

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect. ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled. The tenant contains the users shown in the following table.

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

AdatumUsers	Security	Assigned	None	User1, User2
-------------	----------	----------	------	--------------

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:

- Phone
 - Security questions
 - The Microsoft Authenticator app
 - Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
 - The principle of least privilege must be used.
- You need to implement the planned changes for Package1.
Which users can create and manage the access review?

- A. User3 only
- B. User4 only
- C. User5 only
- D. User3 and User4
- E. User3 and User5
- F. User4 and User5

Question: 377

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Name	Role
User1	<i>None</i>
User2	<i>None</i>
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

•Users must provide one authentication method to reset their password by using SSPR. Available methods must include:

- Email
- Phone
- Security questions
- The Microsoft Authenticator app

•Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.

•The principle of least privilege must be used.

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.Configure a Conditional Access policy.

C.Modify the External collaboration settings.

D.Configure the Access reviews settings.