

Question: 52

CertyIQ

HOTSPOT

-

You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role. You need to configure External collaboration settings for the tenant to meet the following requirements:

- Guest users must be prevented from querying staff email addresses.
- Guest users must be able to access the tenant only if they are invited by User1.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Guest user access restrictions:

Guest users have the same access as members (most inclusive)

Guest users have limited access to properties and memberships of directory objects

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite restrictions:

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

Member users and users assigned to specific admin roles can invite guest users including guests with member

Only users assigned to specific admin roles can invite guest users

No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service
sign up via user flows:

No
Yes

Question: 170

CertyIQ

HOTSPOT

-

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can manage application security groups.
- Users that are assigned Role2 can manage Azure Firewall.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role1:

	▼
Microsoft.App	
Microsoft.Computer	
Microsoft.Network	
Microsoft.Security	

Role2:

	▼
Microsoft.App	
Microsoft.Management	
Microsoft.Network	
Microsoft.Security	

Question: 172

CertyIQ

DRAG DROP

-

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Defender for Cloud Apps.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Publish App1 in Azure AD.

Create a conditional access policy that has session controls configured.

From Microsoft Defender for Cloud Apps, create a session policy.

From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.



Question: 173

CertyIQ

HOTSPOT

-

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

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

Existing Environment. Litware Environment
Litware has an AD DS forest named litware.com

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:
 - Email

- 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 implement the planned changes for SSPR.
What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Number of authentication methods required:

▼

1
2
3
4

Authentication methods that can be used:

▼

Microsoft Authenticator only
Security questions only
Email and phone only
Phone and Microsoft Authenticator only
Email, phone, and Microsoft Authenticator only
Email, phone, Microsoft Authenticator, and security questions