

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

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Azure Active Directory (Azure AD).

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Set-MsolCompanySettings
- B. Set-MsolDomainFederationSettings
- C. Update-MsolFederatedDomain
- D. Set-MsolDomain

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

- ⇒ A device named Device1
- ⇒ Users named User1, User2, User3, User4, and User5
- ⇒ Groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

- A. Group1 and Group4 only
- B. Group1, Group2, Group3, Group4, and Group5
- C. Group1 and Group2 only
- D. Group1 only
- E. Group1, Group2, Group4, and Group5 only



You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click the Exhibit tab.)

#### Guest user access

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

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 settings

Admins and users in the guest inviter role can invite ⓘ

Yes

No

Members can invite ⓘ

Yes

No

Guests can invite ⓘ

Yes

No

Email One-Time Passcode for guests ⓘ

[Learn more](#)

Yes

No

Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

Yes

No

#### Collaboration restrictions

Allow invitations to be sent to any domain (most inclusive)

Deny invitations to the specified domains

Allow invitations only to the specified domains (most restrictive)

A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrikam.com	A user in fabrikam.com

Which users will be emailed a passcode?

- A. User2 only
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

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.

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 Identity Governance blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Licenses blade in the Azure Active Directory admin center
- D. the Set-WindowsProductKey cmdlet

**HOTSPOT -**

You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.

Users are invited to collaborate with contoso.com as shown in the following table.

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

From the External collaboration settings in the Azure Active Directory admin center, you configure the Collaboration restrictions settings as shown in the following exhibit.

**Collaboration restrictions**

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

 Delete

**TARGET DOMAINS**

Outlook.com

From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input checked="" type="radio"/>

You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.

Name	Type	Directly assigned license
User1	User	<i>None</i>
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	<i>None</i>
Group3	Mail-enabled security group	<i>None</i>

Which objects can you add as members to Group3?

- A. User2 and Group2 only
- B. User2, Group1, and Group2 only
- C. User1, User2, Group1 and Group2
- D. User1 and User2 only
- E. User2 only

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

B. redirection URL

C. username

D. shared key

E. password

DRAG DROP -

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

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

Select and Place:

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

[Hide Solution](#) [Discussion](#)

Correct Answer:	Actions	Answer Area
	Sign in to the Microsoft 365 admin center.	Create a self-signed user account in the Azure AD tenant.
	Create a self-signed user account in the Azure AD tenant.	Sign in to the Microsoft 365 admin center.
	From the Microsoft 365 admin center, add the domain name.	Respond to the Become the admin message.
	Respond to the Become the admin message.	Create a TXT record in the contoso.com DNS zone.
	From the Microsoft 365 admin center, remove the domain name.	
	Create a TXT record in the contoso.com DNS zone.	

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

In the tenant, you create the groups shown in the following table.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

Which members can you add to GroupA and GroupB? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

GroupA:

- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

GroupB:

- User1 only
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

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 Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

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 password writeback.

Does this meet the goal?

A. Yes

B. No

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 Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

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 pass-through authentication.

Does this meet the goal?

A. Yes

B. No

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 Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

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 conditional access policies.

Does this meet the goal?

A. Yes

B. No

#### NOTES

You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1. Department1 has the users shown in the Users exhibit. (Click the Users tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

### Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory

+ Add member Remove member Bulk operations Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Search users Add filters

2 users found

Name	User principal name	User type	Directory synced
User1	User1@m365x629615.onmicrosoft.com	Member	No
User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

### Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

+ Add Remove Refresh Columns Preview features Got feedback?

Search groups Add filters

Name	Group Type	Membership Type
Group1	Security	Assigned
Group2	Security	Assigned

Department1 has the user administrator assignments shown in the Assignments exhibit. (Click the Assignments tab.)

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

### User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)

Dashboard > ContosoAzureAD > Groups > Group2

### Group2 | Members

Group

+ Add members Remove Refresh Bulk operations Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Direct members

Name	User type
User3	Member
User4	Member

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

### Statements

### Yes

### No

Admin1 can reset the passwords of User3 and User4.



Admin1 can add User1 to Group 2



Admin 2 can reset the password of User1.



#### HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled.

You are creating a conditional access policy as shown in the following exhibit.

## New

### Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users.

[Learn more](#)

#### Name \*

Policy1

#### Assignments

Users and groups ⓘ

#### Include

#### Exclude

- None
- All users
- Select users and groups

All guest users (preview) ⓘ

Directory roles (preview) ⓘ

Users and groups

#### Select ⓘ

1 user

US User1  
user1@sk200922outlook.onm... \*\*\*

#### Access controls

Grant ⓘ



0 controls selected

Session ⓘ



0 controls selected

#### Enable policy

Report-only

On

Off

**Create**

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.

Hot Area:

#### Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice]

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting



To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice]

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting



You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click the Exhibit tab.)

Custom smart lockout

Lockout threshold ⓘ

5



Lockout duration in seconds ⓘ

3600



Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

Contoso  
Litware  
Tailwind  
project  
Zettabyte  
MainStreet



Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

You are evaluating the following passwords:

- Pr0jectlitw@re
- T@ilw1nd
- C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role.

SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.

You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. Authentication administrator
- B. Helpdesk administrator** 
- C. Privileged authentication administrator
- D. Security operator

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.

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 verification code from the Microsoft Authenticator app 
- B. security questions
- C. voice
- D. SMS

Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?

- A. a named network location
- B. the Microsoft Authenticator app
- C. Windows Hello for Business authentication
- D. FIDO2 tokens

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

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. atypical travel
- D. leaked credentials

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

- A. a cloud apps or actions condition
- B. a user risk condition
- C. a client apps condition
- D. a sign-in risk condition

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured

B. an Azure AD conditional access policy that has session controls configured

C. an Azure AD conditional access policy that has client apps conditions configured

D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain.

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. an Azure AD Password Protection proxy

C. Network Policy Server (NPS)

D. a pass-through authentication proxy

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain.

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. an Azure AD Password Protection proxy

C. Network Policy Server (NPS)

D. a pass-through authentication proxy

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

A. Azure AD Connect

B. Azure AD Application Proxy

C. Password Change Notification Service (PCNS)

D. the Azure AD Password Protection proxy service

**HOTSPOT -**

You have a Microsoft 365 tenant.

Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).

You need to receive an alert if a registered application gains read and write access to the user's email.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Tool to use:

Azure AD Identity Protection  
Identity Governance  
**Microsoft Cloud App Security** →  
Microsoft Endpoint Manager

Policy type to create:

App discovery  
App protection  
Conditional access  
**OAuth app** →  
Sign-in risk  
User risk

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

You create an enterprise application collection named HR Apps that has the following settings:

☞ Applications: App1, App2, App3

☞ Owners: Admin1

☞ Users and groups: HRUsers

All 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 Single sign-on, configure a sign-on method.
  - C. From Properties, change User assignment required to No.
  - D. From Permissions, review the User consent permissions.

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

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. Application Insights in Azure Monitor
- B. access reviews in Azure AD
- C. Cloud App Discovery in Microsoft Cloud App Security**
- D. enterprise applications in Azure AD

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that has the default App registrations settings. The tenant contains the users shown in the following table.

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.

You need to identify who can assign users to App1, and who can register App2 in Azure AD.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Can assign users to App1:

Admin1 only  
Admin3 only  
**Admin1 and Admin3 only** →  
Admin1, Admin2, and Admin3 only  
Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

Admin1 only  
Admin3 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3 only  
**Admin1, Admin2, Admin3, and User1** →

HOTSPOT -

You have an on-premises datacenter that contains the hosts shown in the following table.

Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

You have an Azure Active Directory (Azure AD) tenant that syncs to the Active Directory forest. Multi-factor authentication (MFA) is enforced for Azure AD.

You need to ensure that you can publish App1 to Azure AD users.

What should you configure on Server and Firewall1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Service to install on Server4:

Azure AD Application Proxy →  
The Azure AD Password Protection DC agent  
The Azure AD Password Protection proxy service  
Web Application Proxy in Windows Server

Rule to configure on Firewall1:

Allow incoming HTTPS connections from Azure AD to Server4.  
Allow incoming IPsec connections from Azure AD to Server4.  
Allow outbound HTTPS connections from Server4 to Azure AD. →  
Allow outbound IPsec connections from Server4 to Azure AD.

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD.

Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.

You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.

What should you do?

- A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
- B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.
- C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
- D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

You have a custom cloud app named App1 that is registered in Azure Active Directory (Azure AD).

App1 is configured as shown in the following exhibit.

Save Discard Delete | Got feedback?

Enabled for users to sign-in?  Yes  No

Name  

Homepage URL  

Logo   
 

User access URL  

Application ID  

Object ID  

Terms of Service Url  

Privacy Statement Url  

Reply Url  

User assignment required?  Yes  No

Visible to users?  Yes  No

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.

Hot Area:

#### Answer Area

[answer choice] can access App1 from the homepage URL.

All users 

No one

Only users listed on the Owners blade

Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

all users 

no one

only users listed on the Owners blade

only users listed on the Users and groups blade

You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

For which groups can you create an access review?

- A. Group1 only
- B. Group1 and Group4 only
- C. Group1 and Group2 only
- D. Group1, Group2, Group4, and Group5 only
- E. Group1, Group2, Group3, Group4 and Group5

You have a Microsoft 365 tenant.

In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

- A. an access policy in Microsoft Cloud App Security.
- B. Terms and conditions in Microsoft Endpoint Manager.
- C. a conditional access policy in Azure AD
- D. a compliance policy in Microsoft Endpoint Manager

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 is the owner of Group1.

You create an access review that has the following settings:

- ⇒ Users to review: Members of a group
- ⇒ Scope: Everyone
- ⇒ Group: Group1
- ⇒ Reviewers: Members (self)

Which users can perform access reviews for User3?

- A. User1, User2, and User3
- B. User3 only
- C. User1 only
- D. User1 and User2 only

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.

You need to ensure that the IT department users only have access to the Security administrator role when required.

What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments after from the Role settings details
- B. Expire active assignments after from the Role settings details
- C. Assignment type to Active
- D. Assignment type to Eligible

#### HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

User1 has the devices shown in the following table.

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

- ⇒ Name: Terms1
- ⇒ Display name: Contoso terms of use
- ⇒ Require users to expand the terms of use: On
- ⇒ Require users to consent on every device: On
- ⇒ Expire consents: On
- ⇒ Expire starting on: December 10, 2020
- ⇒ Frequency: Monthly

On November 15, 2020, User1 accepts Terms1 on Device3.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input type="radio"/>

You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

... ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD > User Administrator >

#### Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

##### Activation

SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

##### Assignment

SETTING	STATE
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

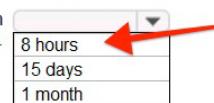
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

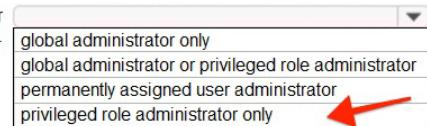
##### Answer Area

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every [answer choice]



8 hours  
15 days  
1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a [answer choice]



global administrator only  
global administrator or privileged role administrator  
permanently assigned user administrator  
privileged role administrator only

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.

You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.

What should you create?

- A. an access package that targets users outside your directory
- B. an access package that targets users in your directory
- C. a group-based access review that targets guest users
- D. an application-based access review that targets guest users

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 \* Admin review

Description ⓘ

Start date \* 12/18/2020

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never End by Occurrences

Number of times 0

End date 01/17/2021

Users Scope Everyone

Review role membership (permanent and eligible) \*

Application Administrator and 72 others

Reviewers Reviewers (Preview) Manager

(Preview) Fallback reviewers ⓘ Megan Bowen

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 create a separate access review for each role.

Does this meet the goal?

A. Yes

B. No

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)  14

End

Number of times

End date

Users Scope  Everyone

Review role membership (permanent and eligible) \*  
[Application Administrator and 72 others](#)

Reviewers

(Preview) Fallback reviewers

Upon completion settings

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

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 \* Admin review ✓

Description ⓘ

Start date \* 12/18/2020

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never End by Occurrences

Number of times 0

End date 01/17/2021

Users Scope Everyone

Review role membership (permanent and eligible) \* Application Administrator and 72 others

Reviewers Reviewers (Preview) Manager

(Preview) Fallback reviewers ⓘ Megan Bowen

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 set Reviewers to Member (self).

Does this meet the goal?

A. Yes

B. No

#### Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

#### Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.



Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5



Enterprise Mobility + Security

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

#### Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

#### Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirement. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the user's identity was compromised.

#### Question

You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

#### Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

#### Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

#### Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom catalogs and custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

#### Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

#### Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

#### Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

\*

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

#### Question

You need to meet the authentication requirements for leaked credentials.

What should you do?

- A. Enable password hash synchronization in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Configure an authentication method policy in Azure AD.
- D. Enable federation with PingFederate in Azure AD Connect.

User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

\*

Enterprise Mobility + Security

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the user's identity was compromised.

#### Question

HOTSPOT -

You need to meet the technical requirements for the probability that user identities were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

The users must first:

Provide consent for any app to access the data of Contoso.
Register for multi-factor authentication (MFA).
Register for self-service password reset (SSPR).

You must configure:

A sign-in risk policy
A user risk policy
An Azure AD Password Protection policy

System			
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

#### Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom catalogs and custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

#### Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

#### Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

#### Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

#### HOTSPOT -

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

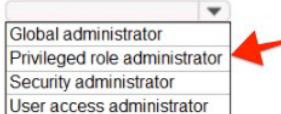
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

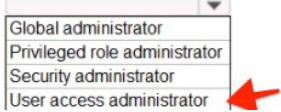
Hot Area:

#### Answer Area

To manage Azure AD built-in role assignments, use:



To manage Azure built-in role assignments, use:



#### Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

#### Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

#### Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

#### Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

#### Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom catalogs and custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

#### Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

#### Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

#### Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

\*

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

#### Question

##### HOTSPOT -

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.

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

NOTE: Each correct selection is worth one point.

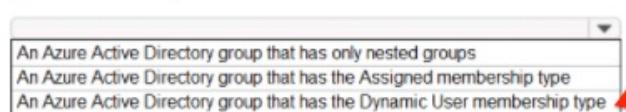
Hot Area:

#### Answer Area

Azure AD Connect settings to modify:



Assign Azure AD licenses to:



Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom catalogs and custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

#### Question

HOTSPOT -

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

For on-premises applications:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- Publish the applications by using Azure AD Application Proxy.



For SharePoint Online:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.



Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

#### Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

#### Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

#### Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

#### Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom catalogs and custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

#### Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

#### Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

#### Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

-

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

#### Question

You need to configure the detection of multi-staged attacks to meet the monitoring requirements.

What should you do?

A. Customize the Azure Sentinel rule logic.

B. Create a workbook.

C. Add Azure Sentinel data connectors.

D. Add an Azure Sentinel playbook.

### Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

#### Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

#### Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirement. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the user's identity was compromised.

#### Question

You create a Log Analytics workspace.

You need to implement the technical requirements for auditing.

What should you configure in Azure AD?

A. Company branding

B. Diagnostics settings

C. External Identities

D. App registrations

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

-

Enterprise Mobility + Security

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the user's identity was compromised.

### Question

You need to meet the planned changes and technical requirements for App1.

What should you implement?

- A. a policy set in Microsoft Endpoint Manager
- B. an app configuration policy in Microsoft Endpoint Manager
- C. an app registration in Azure AD
- D. Azure AD Application Proxy

#### Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

#### Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

#### Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirement. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the user's identity was compromised.

#### Question

HOTSPOT -

You need to implement the planned changes and technical requirements for the marketing department.

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

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

To configure user access:

- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:

- An accepted domain
- A connected organization
- A custom domain name