Microsoft

(MS-500)

Microsoft 365 Security Administration

Total: **524 Questions**

Link:

Question: 1

You have several Conditional Access policies that block noncompliant devices from connecting to services. You need to identify which devices are blocked by which policies.
What should you use?

A. the Setting compliance report in the Microsoft Endpoint Manager admin center
B. Sign-ins in the Azure Active Directory admin center
C. Activity log in the Cloud App Security portal
D. Audit logs in the Azure Active Directory admin center

Answer: B

Explanation:

AAD > Monitoring > Sign-in logs

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access

Question: 2

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 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant.
Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled

User writeback: Disabled -

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.
Solution: You modify the Azure AD app and attribute filtering settings.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:

The answer is NO, sourceanchor attribute is used to identify the objects. This is that MS says: "The sourceAnchor attribute is defined as an attribute immutable during the lifetime of an object. It uniquely identifies an object as being the same object on-premises and in Azure AD. The attribute is also called immutableId and the two names are used interchangeable."

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-design-

concepts#:~:text=%20To%20switch%20from%20objectGUID%20to%20ConsistencyGuid%20as,of%20the%20ms-DS-ConsistencyGuid%20attribute%20in%20your...%20More%20

Question: 3

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 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant.
Azure AD Connect has the following settings:

- ⇨ Source Anchor: objectGUID
- ⇨ Password Hash Synchronization: Disabled
- ⇨ Password writeback: Disabled
- ⇨ Directory extension attribute sync: Disabled
- ⇨ Azure AD app and attribute filtering: Disabled
- ⇨ Exchange hybrid deployment: Disabled
- ⇨ User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.
Solution: You modify the Password Hash Synchronization settings.
Does that meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Leaked credentials detection in Azure AD Identity Protection requires Password Hash Sync enabled in Azure AD Connect

References:

https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

Question: 4

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 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant.
Azure AD Connect has the following settings:

- ⇨ Source Anchor: objectGUID
- ⇨ Password Hash Synchronization: Disabled
- ⇨ Password writeback: Disabled
- ⇨ Directory extension attribute sync: Disabled
- ⇨ Azure AD app and attribute filtering: Disabled
- ⇨ Exchange hybrid deployment: Disabled
- ⇨ User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Protect against leaked credentials and add resilience against outages

If your organization uses a hybrid identity solution with pass-through authentication or federation, then you should enable password hash sync for the following two reasons:

The Users with leaked credentials report in the Azure AD management warns you of username and password pairs, which have been exposed on the "dark web." An incredible volume of passwords is leaked via phishing, malware, and password reuse on third-party sites that are later breached. Microsoft finds many of these leaked credentials and will tell you, in this report, if they match credentials in your organization – but only if you enable password hash sync!

Question: 5

HOTSPOT -
You have a Microsoft 365 subscription that uses a default domain name of contoso.com.
The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

multi-factor authentication
users service settings

app passwords (learn more)

● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

verification options (learn more)

Methods available to users:

☐ Call to phone
■ Text message to phone
■ Notification through mobile app
■ Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

☐ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60): 14

In contoso.com, you create the users shown in the following table.

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enforced
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My Apps portal	

Answer:

Answer Area

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

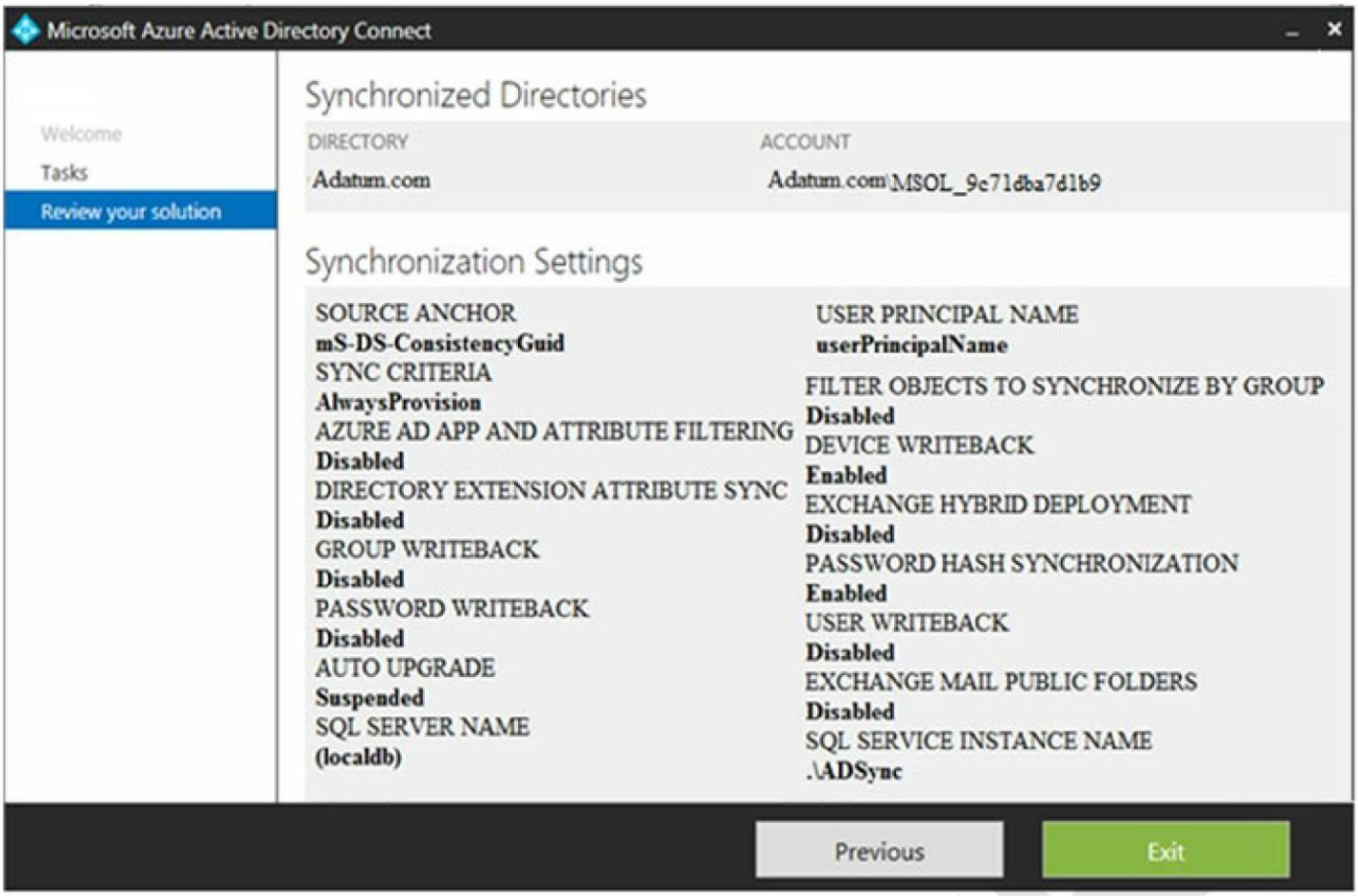
Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My Apps portal	

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

Question: 6

HOTSPOT -
You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



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

If you reset a password in Azure AD of a synced user, the new password will **[answer choice]**.
- be overwritten
- be synced to Active Directory
- be subject to the Active Directory password policy

If you join a computer to Azure AD, **[answer choice]**.
- an object will be provisioned in the Computers container
- an object will be provisioned in the RegisteredDevices container
- the device object in Azure will be deleted during synchronization

Answer:

Answer Area

If you reset a password in Azure AD of a synced user, the new password will **[answer choice]**.
- be overwritten
- be synced to Active Directory
- be subject to the Active Directory password policy

If you join a computer to Azure AD, **[answer choice]**.
- an object will be provisioned in the Computers container
- an object will be provisioned in the RegisteredDevices container
- the device object in Azure will be deleted during synchronization

Explanation:

1. be overwritten until the password is changed again on-prem

2. Object will be provisioned in the RegisteredDevices container

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization#:~:text=An%20administrator%20can,manually%20updated%20password.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

Question: 7 You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Endpoint Manager.
You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network. What should you do first?

A. From the Azure Active Directory admin center, create a new certificate
B. Enable Application Proxy in Azure AD
C. From Active Directory Administrative Center, create a Dynamic Access Control policy D.
From the Azure Active Directory admin center, configure authentication methods

Answer: A

Explanation:

to configure conditional access for VPN connectivity, you need to: Create

a VPN certificate in the Azure portal.

Download the VPN certificate.

Deploy the certificate to your VPN server.

Reference:
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10

Question: 8 You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you create a new user. You plan to assign the Reports reader role to the user.
You need to view the permissions of the Reports reader role.
Which admin center should you use?

A. Microsoft 365 Defender
B. Azure Active Directory
C. Microsoft Defender for Identity
D. Microsoft Defender for Cloud Apps

Answer: B

Explanation:

You can view the Role permissions either from Microsoft 365 Admin Center OR Azure Active Directory.

Question: 9

You have a Microsoft 365 E5 subscription.
You need to ensure that users who are assigned the Exchange administrator role have time-limited permissions and must use multi-factor authentication (MFA) to request the permissions.
What should you use to achieve the goal?

A. Microsoft 365 Compliance permissions
B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
C. Microsoft Azure AD group management
D. Microsoft 365 user management

Answer: B

Explanation:

Correct answer is B. “Time-limited permissions” is the key here.

Question: 10

Your company has a Microsoft 365 subscription.
The company does not permit users to enroll personal devices in mobile device management (MDM). Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.
The users must be prevented from backing up the app's data to iCloud.
What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
B. an app protection policy in Microsoft Endpoint Manager
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
D. a device compliance policy in Microsoft Endpoint Manager

Answer: B

Explanation:

The requirement is specifically about blocking users from backing up data from the app to iCloud. This is accomplished with Intune App protection.

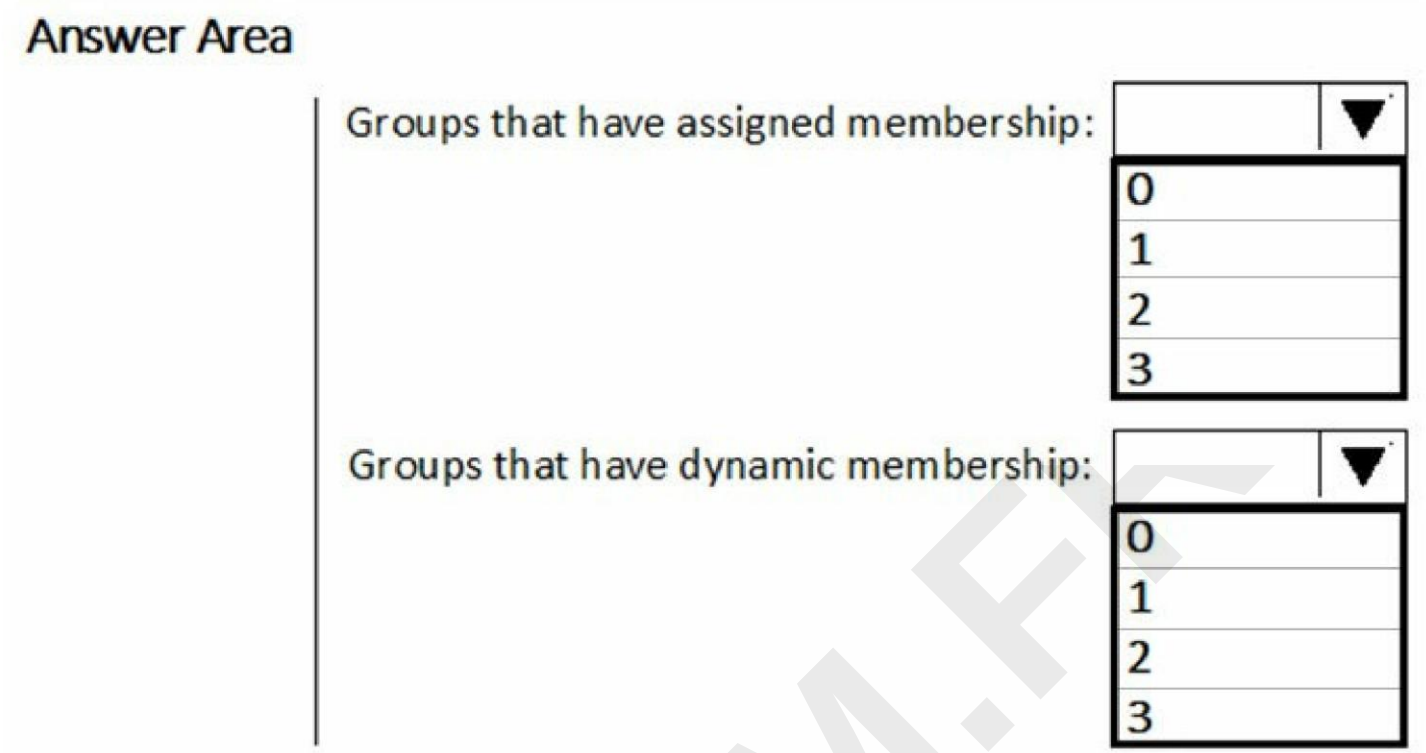
Don't forget, though that app protection does not block these users from logging in with their web browser and copying data out. You can prevent this by adding a conditional access policy which only allows access through the app, which you have protected with your shiny new app protection policy.

Question: 11

HOTSPOT -
You have a Microsoft 365 E5 subscription.
Users and device objects are added and removed daily. Users in the sales department frequently change their device.
You need to create three following groups:

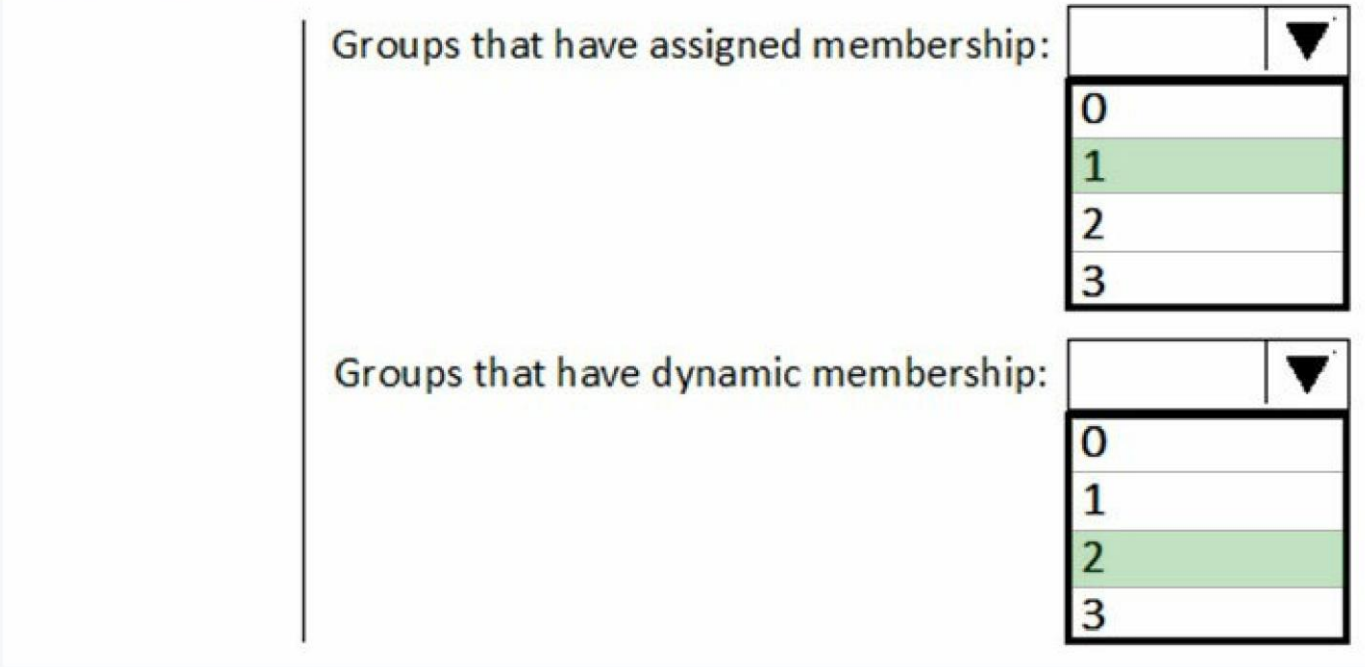
Name	Requirement
Group1	All the devices of users where the `Department` attribute is set to `Sales`
Group2	All the users where the `Department` attribute is set to `Sales`
Group3	All the devices where the `deviceOwnership` attribute is set to `Company`.

The solution must minimize administrative effort.
What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:

Answer Area



Explanation:
Group 1 has to be assigned because you can't create a device group based on the device owners' attributes. Group 2 can be dynamic because a user does have a department attribute.
Group 3 can be dynamic because a device does have a deviceownership attribute.

Question: 12 Your company has a main office and a Microsoft 365 subscription.
You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.
What should you include in the configuration?

A. a user risk policy
B. a sign-in risk policy
C. a named location in Azure Active Directory (Azure AD)
D. an Azure MFA Server

Answer: C

Explanation:

Named locations

With named locations, you can create logical groupings of IP address ranges or countries and regions.

You can access your named locations in the Manage section of the Conditional Access page.

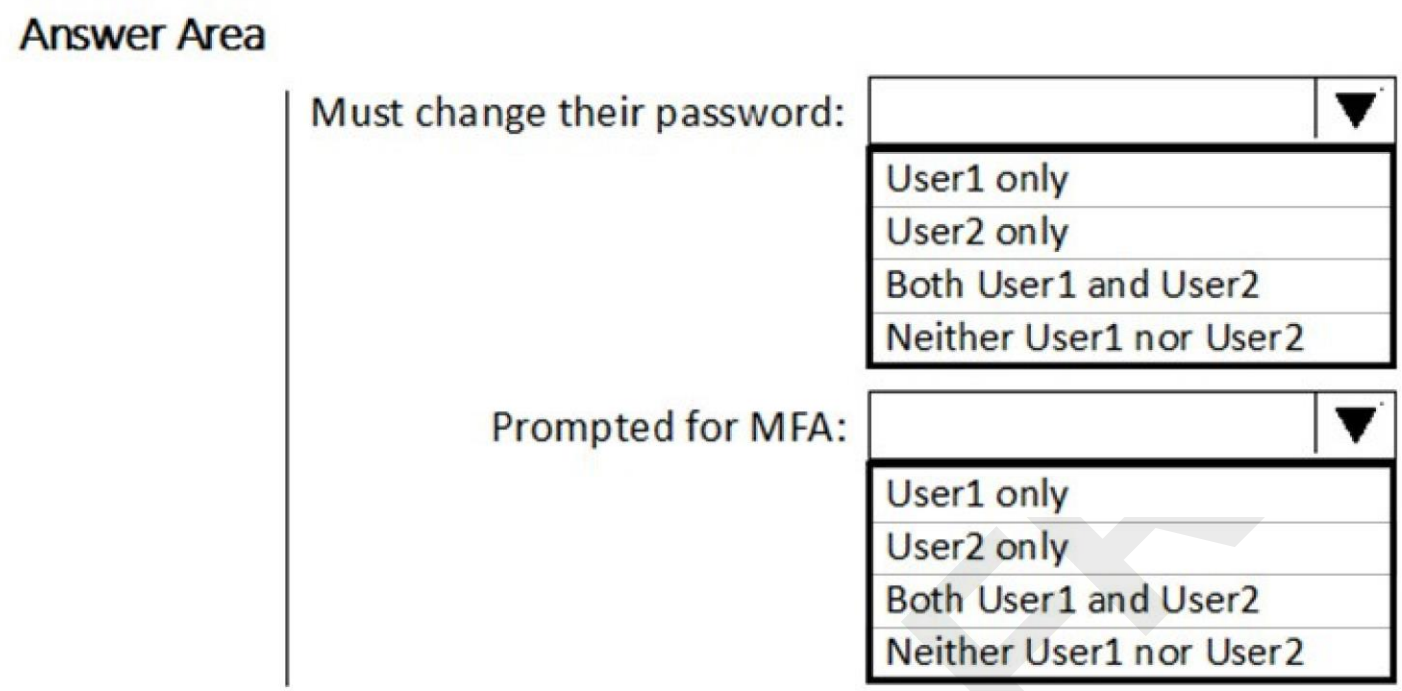
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Question: 13 HOTSPOT -

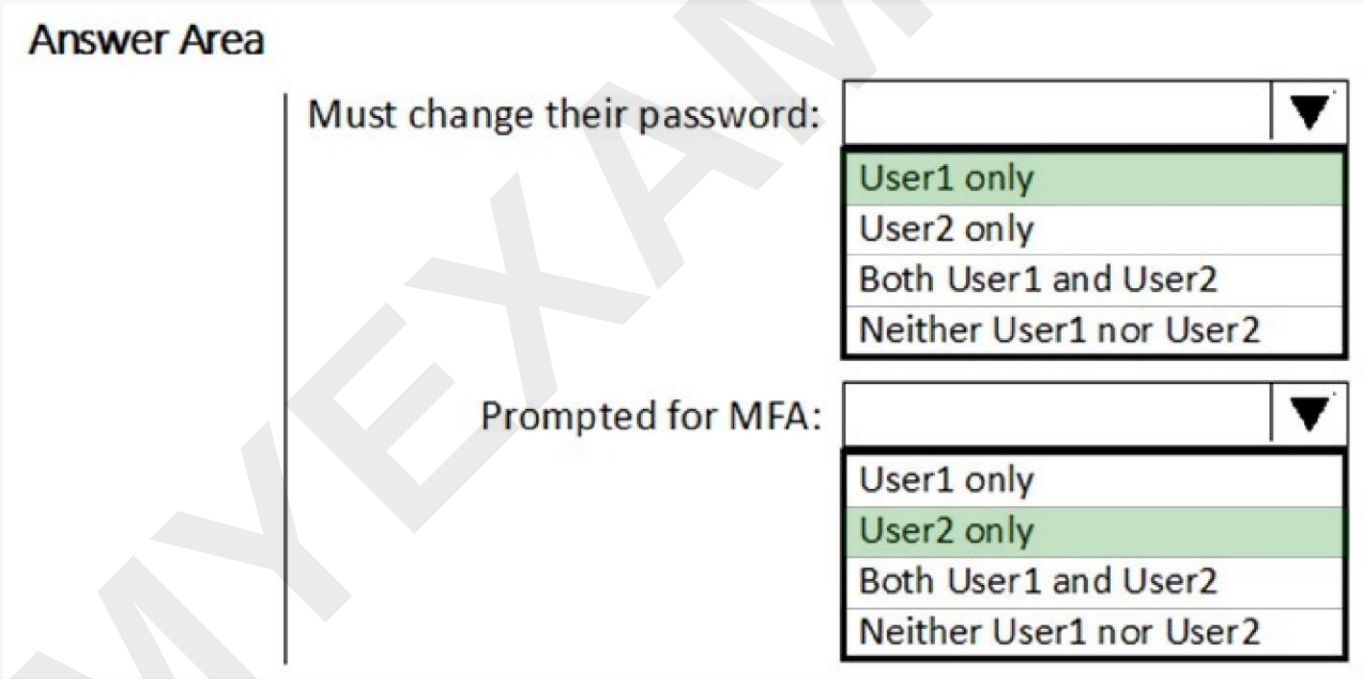
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:☞
Assignments: Include Group1, Exclude Group2
☞ Conditions: User risk of Low and above
☞ Access: Allow access, Require password change
You need to identify how the policy affects User1 and User2.
What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:



Explanation:
Box 1: User1 only -

The Azure AD Identity Protection user risk policy is excluded from Group2. Exclusion overrides inclusion.
Therefore, the policy will not affect User2. Thus, only
User 1 needs to change the Password.

Box 2: User2 only -
MFA will be triggered for User 2.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

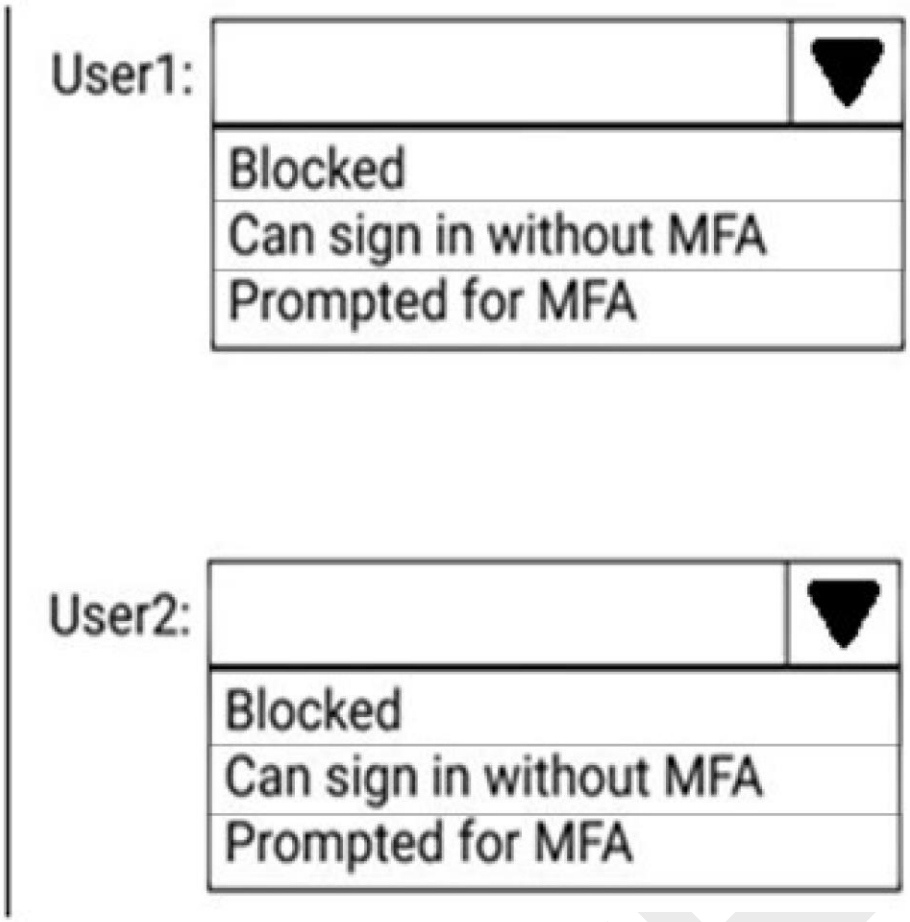
Question: 14

HOTSPOT -
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

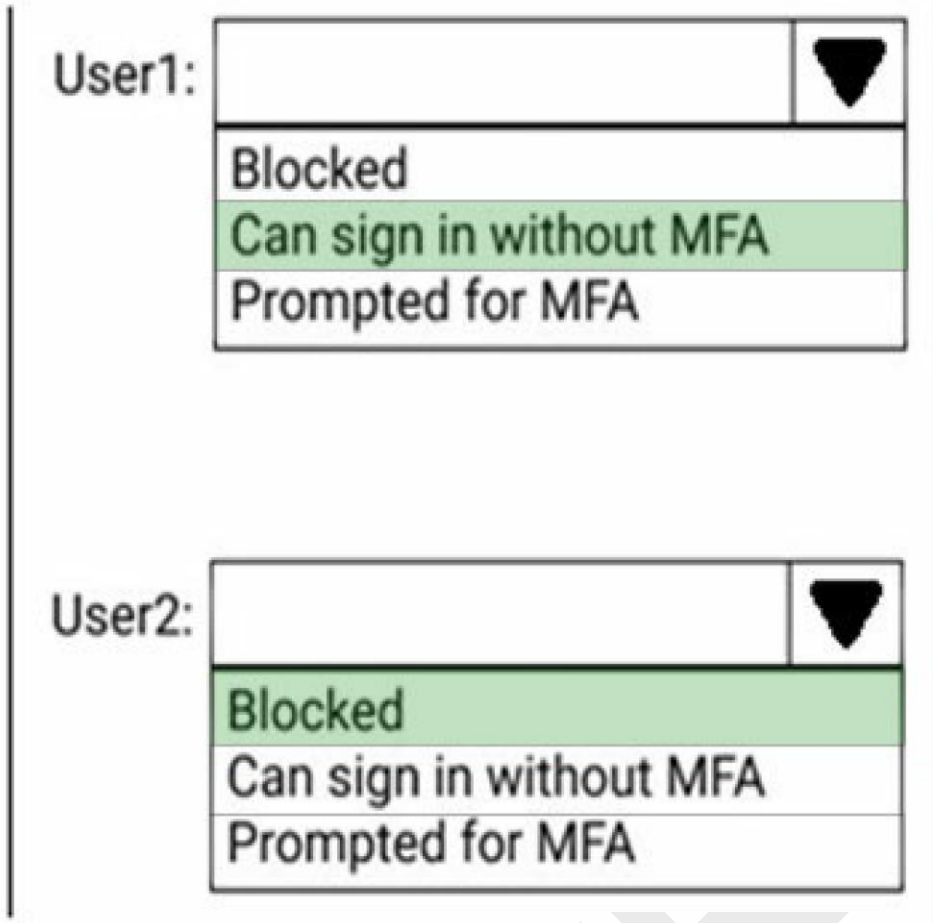
You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
Assignments: Include Group1, Exclude Group2
Conditions: Sign-in risk of Low and above
Access: Allow access, Require multi-factor authentication
You need to identify how the policy affects User1 and User2.
What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

User1 - Can sign in without MFA

User 2 - Blocked

Users must register for Azure AD MFA and SSPR before they face a situation requiring remediation. Users not registered are blocked and require administrator intervention.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

Question: 15

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 on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
Solution: You use the Security event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

Question: 16

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 on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the Directory Service event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

Question: 17

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 on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the System event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:

certainly No. needs an Application.

References:

https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

Question: 18

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 on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
Solution: You use the Application event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: A

Explanation:

References:

https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

https://learn.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors#troubleshoot-other-error-messages

Question: 19

You have a Microsoft 365 E5 subscription.
Some users are required to use an authenticator app to access Microsoft SharePoint Online.
You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.
What should you do?

A. From the Microsoft 365 Security admin center, download a report.
B. From Azure Log Analytics, query the logs.
C. From the Microsoft 365 Security admin center, perform an audit log search.
D. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

Answer: D

Explanation:

The user sign-ins report provides information on the sign-in pattern of a user, the number of users that have signed in over a week, and the status of these sign- ins.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.
2. From the Azure Active Directory admin center, view the sign-ins.
Other incorrect answer options you may see on the exam include the following:
1. From the Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.
2. From the Azure Active Directory admin center, view the audit logs.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Question: 20

HOTSPOT -
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

You implement Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
From PIM, you review the Application Administrator role and discover the users shown in the following table.

Name	Assignment type
UserA	Permanent
UserB	Eligible
UserC	Eligible

The Application Administrator role is configured to use the following settings in PIM:
- Activation maximum duration (hours): 1 hour
- Require justification on activation: No
- Require ticket information on activation: No
- On activation, require Azure MFA: No
- Require approval to activate: Yes
- Approvers: None

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
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	○	○
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	○	○
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	○	○

Answer:

Answer Area

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	○	○
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	○	○
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	○	○

Explanation:

yes

yes

no

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?source=recommendations

Question: 21

You have a Microsoft 365 E5 subscription.
Some users are required to use an authenticator app to access Microsoft SharePoint Online.
You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.
What should you do?

A. From the Azure Active Directory admin center, view the sign-ins.
B. From the Microsoft 365 Security admin center, download a report.
C. From the Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.
D. From the Azure Active Directory admin center, view the authentication methods.

Answer: A

Explanation:
The user sign-ins report provides information on the sign-in pattern of a user, the number of users that have signed in over a week, and the status of these sign- ins.

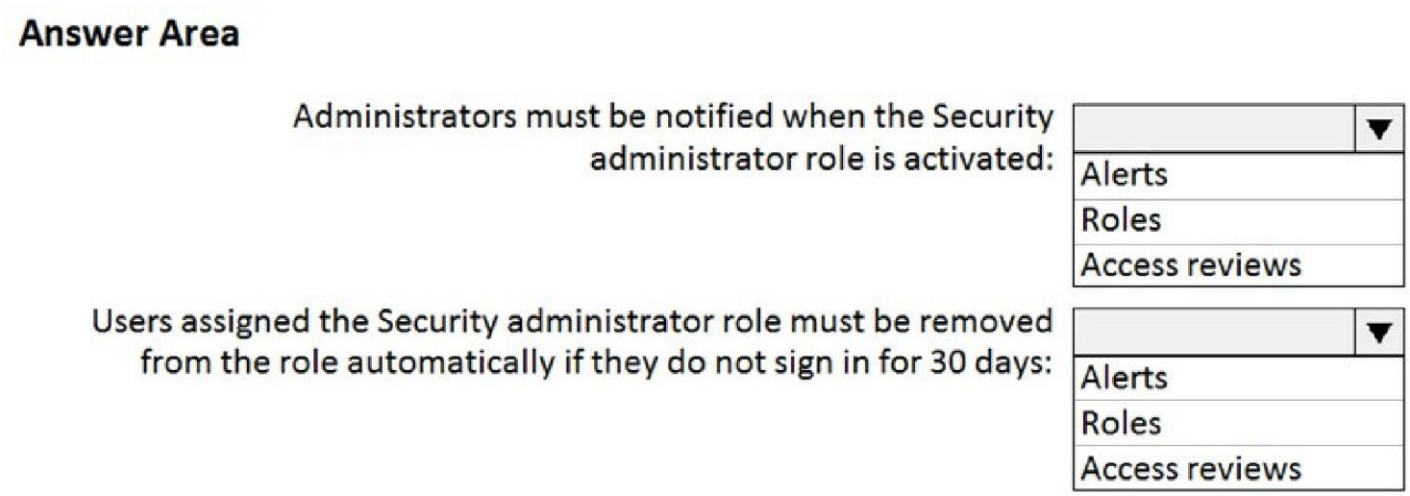
Note:
There are several versions of this question in the exam. The question has two possible correct answers: 1. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins. 2. From the Azure Active Directory admin center, view the sign-ins.

Other incorrect answer options you may see on the exam include the following: 1.
From Azure Log Analytics, query the logs.
2. From the Microsoft 365 Compliance center, perform an audit log search.
3. From the Microsoft 365 Defender portal, download a report.

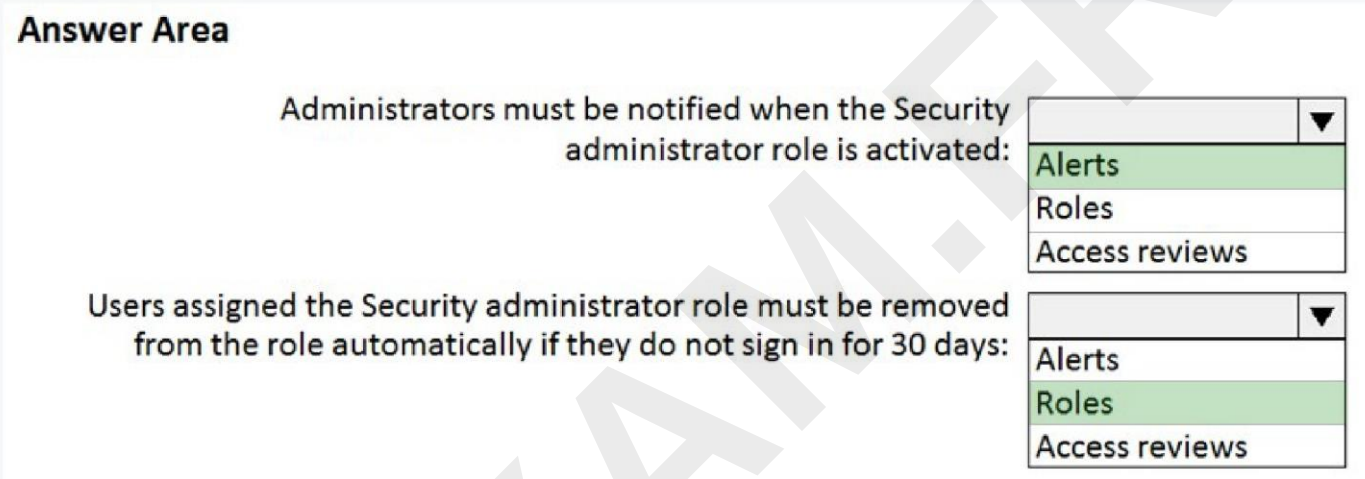
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Question: 22

HOTSPOT -
You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.
You need to recommend an Azure AD Privileged Identity Management (PIM) solution that meets the following requirements:
☞ Administrators must be notified when the Security administrator role is activated.
☞ Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days.
Which Azure AD PIM setting should you recommend configuring for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:



Explanation:

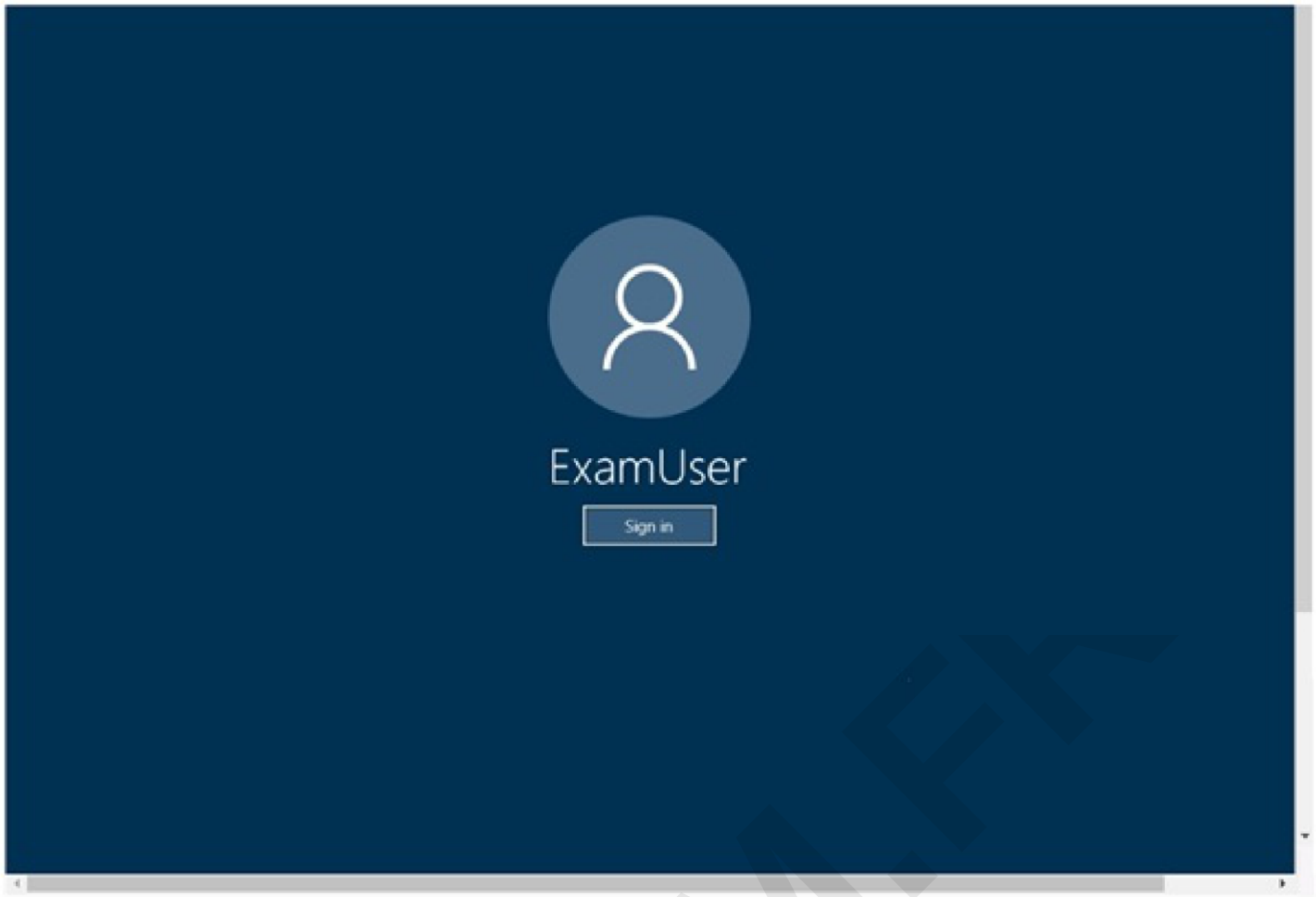
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?tabs=new

Question: 23

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks

in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:

Microsoft 365 Password:
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab instance: 11032396 -
You need to ensure that a user named Lee Gu can manage all the settings for Exchange Online. The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

See explanation below.

Explanation:
1. In the Exchange Administration Center (EAC), navigate to Permissions > Admin Roles.
2. Select the group: Organization Management and then click on Edit.
3. In the Members section, click on Add.

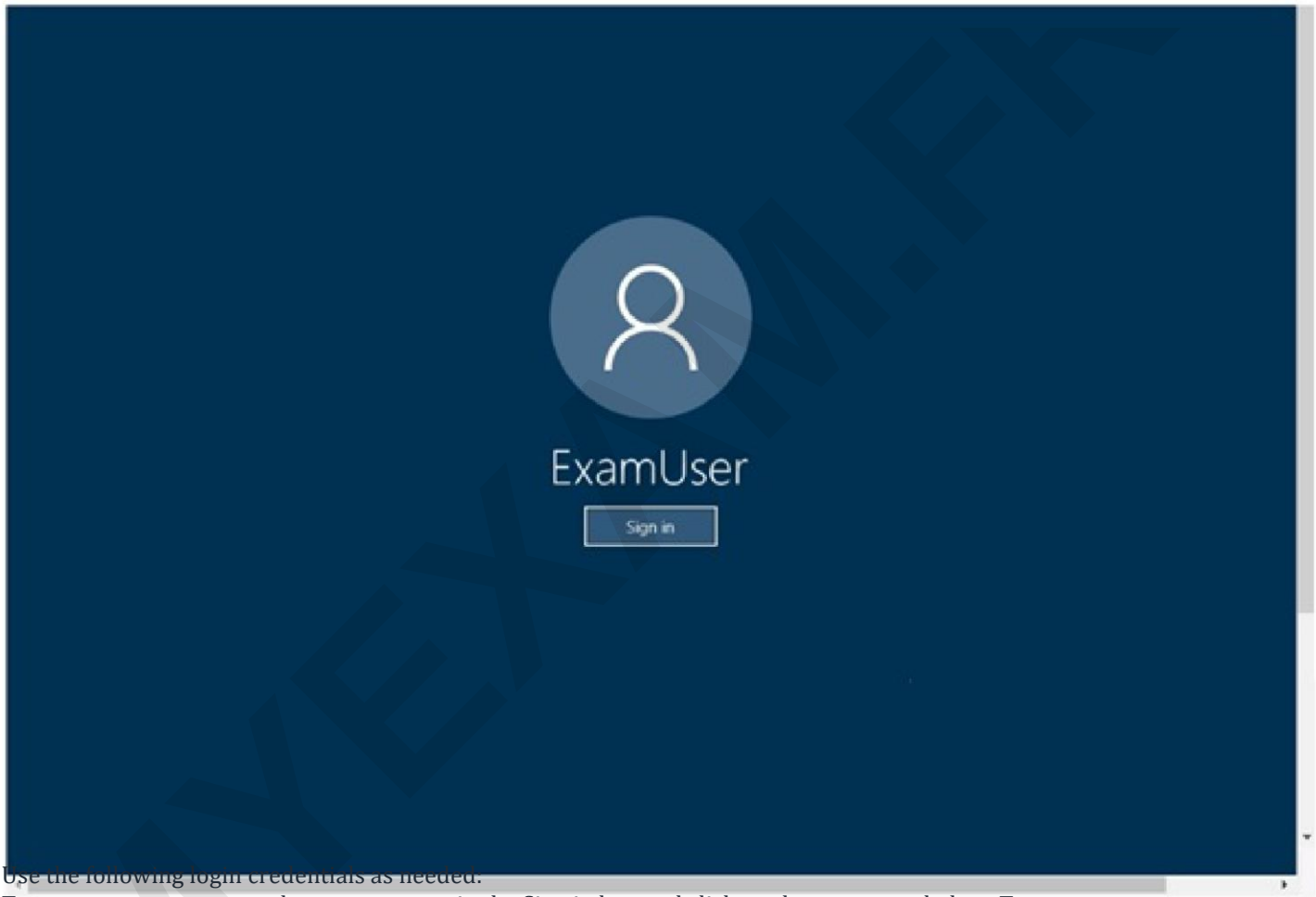
4. Select the users, USGs, or other role groups you want to add to the role group, click on Add, and then click on OK.
5. Click on Save to save the changes to the role group.

Reference:
https://help.bittitan.com/hc/en-us/articles/115008104507-How-do-I-assign-the-elevated-admin-role-Organization-Management-to-the-account-that-is-performing-a-Public-Folder-migration-
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

Question: 24

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below. To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:

Microsoft 365 Password:
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab instance: 11032396 -
You need to ensure that each user can join up to five devices to Azure Active Directory (Azure AD). To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

See explanation below.

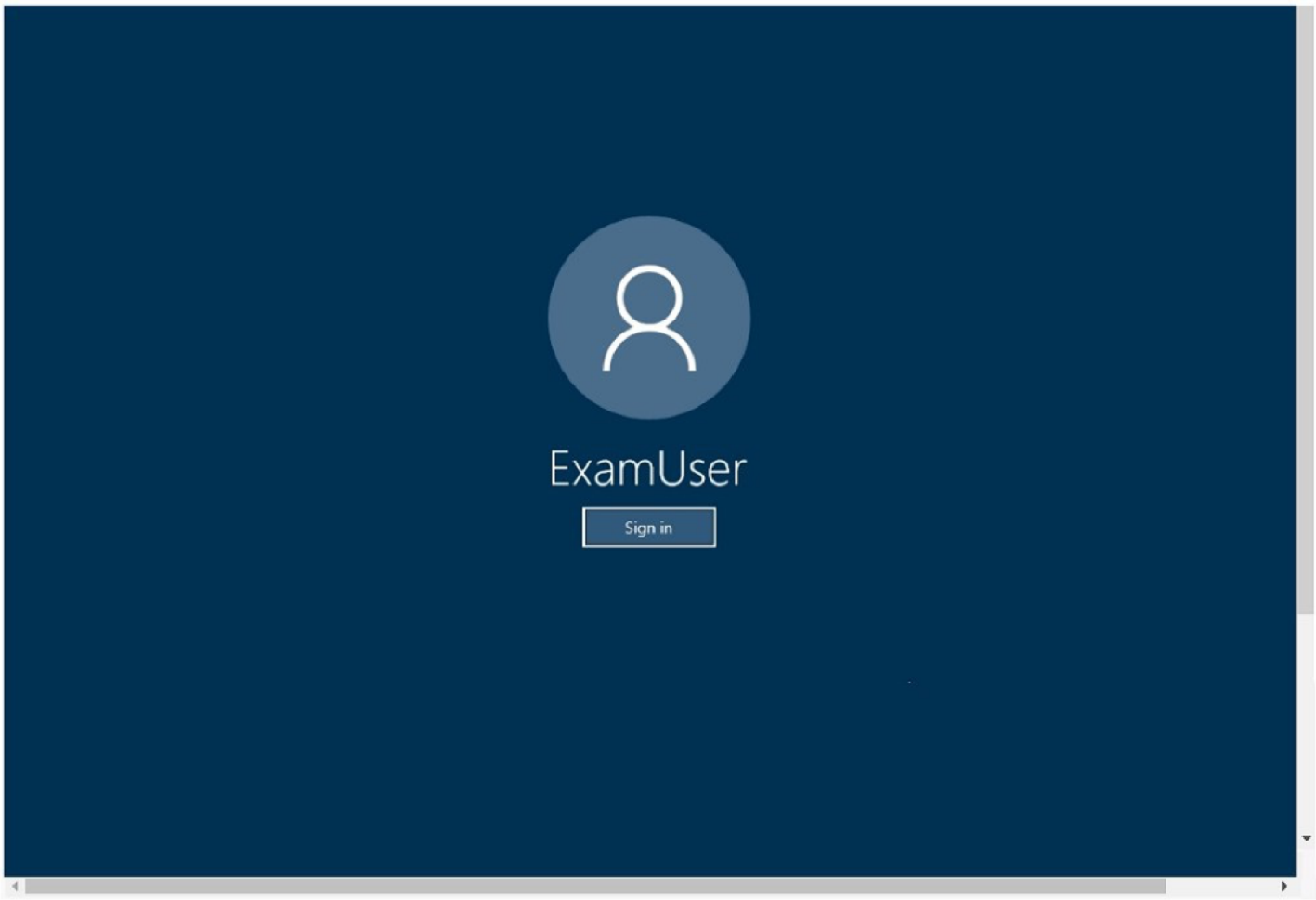
Explanation:
1. After signing into the Microsoft 365 admin center, click Admin centers > Azure Active Directory > Devices.
2. Navigate to Device Settings.
3. Set the Users may join devices to Azure AD setting to All.
4. Set the Additional local administrators on Azure AD joined devices setting to None.
5. Set the Users may register their devices with Azure AD setting to All.
6. Leave the Require Multi-Factor Auth to join devices setting on it default setting.
7. Set the Maximum number of devices setting to 5.
8. Set the Users may sync settings and app data across devices setting to All.
9. Click the Save button at the top left of the screen.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal https://docs.microsoft.com/en-us/microsoft-365/compliance/use-your-free-azure-ad-subscription-in-office-365?view=o365-worldwide

Question: 25

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:

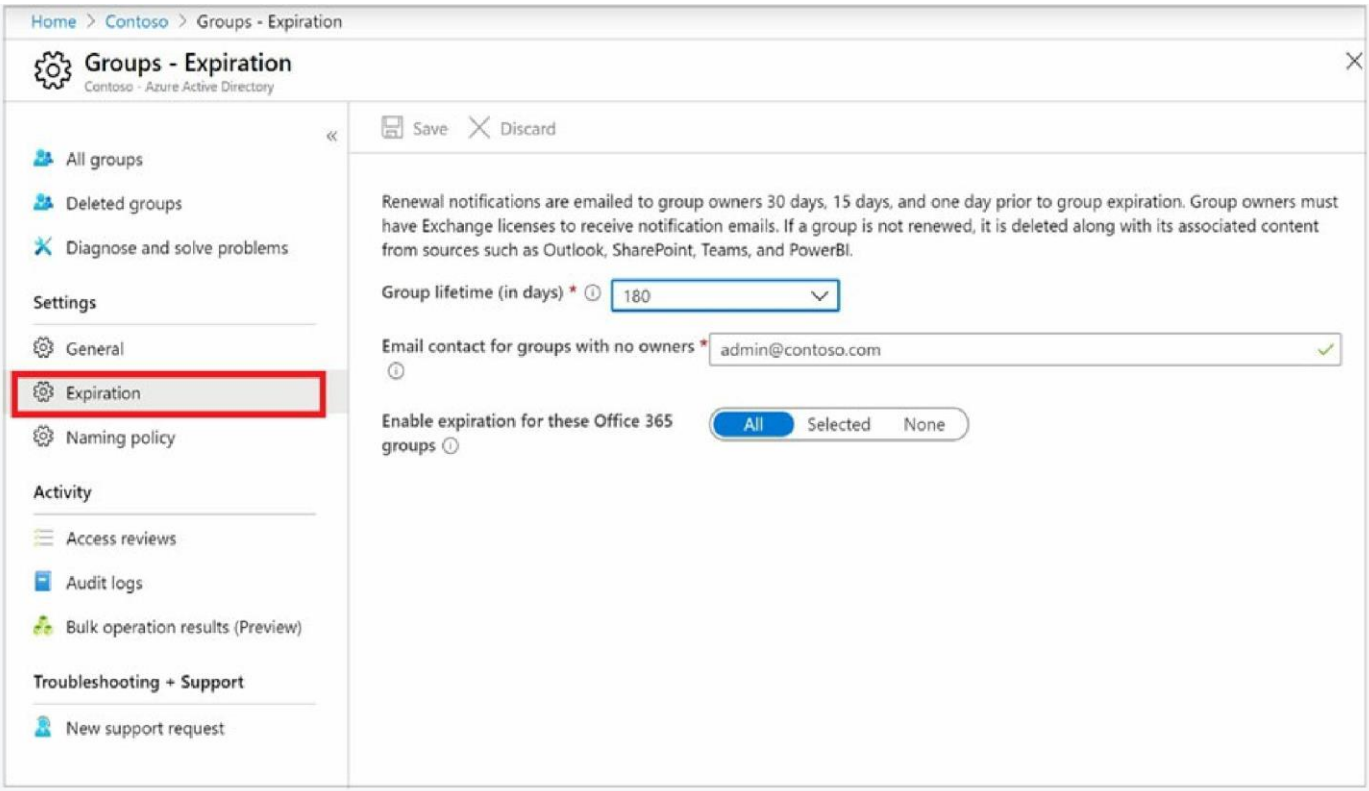
Microsoft 365 Password:
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

Lab instance: 11032396 -
You need to ensure that group owners renew their Office 365 groups every 180 days. To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

See explanation below.

Explanation:
Set group expiration -
1. Open the Azure AD admin center with an account that is a global administrator in your Azure AD organization.
2. Select Groups, then select Expiration to open the expiration settings.



3. On the Expiration page, you can:
➪ Set the group lifetime in days. You could select one of the preset values, or a custom value (should be 31 days or more).

➪ Specify an email address where the renewal and expiration notifications should be sent when a group has no owner.

➪ Select which Office 365 groups expire. You can set expiration for:➪ All Office 365 groups
➪ A list of Selected Office 365 groups
➪ None to restrict expiration for all groups
Save your settings when you're done by selecting Save.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-lifecycle

Question: 26

SIMULATION -
You need to ensure that unmanaged mobile devices are quarantined when the devices attempt to connect to Exchange Online.
To complete this task, sign in to the Microsoft 365 portal.

Answer:

See explanation below.

Explanation:
You need to configure the Exchange ActiveSync Access Settings.
1. Go to the Exchange admin center.
2. Click on Mobile in the left navigation pane.
3. On the Mobile Device Access page, click the Edit button in the Exchange ActiveSync Access Settings area.
4. Select the Quarantine option under When a mobile device that isn't managed by a rule or personal exemption connects to Exchange.
5. Optionally, you can configure notifications to be sent to administrators and a message to be sent to the mobile device user when a device is quarantined.

6. Click Save to save the changes.

Question: 27

SIMULATION -
You need to ensure that all users must change their password every 100 days. To complete this task, sign in to the Microsoft 365 portal.

Answer:

See explanation below.

Explanation:
You need to configure the Password Expiration Policy.
1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Settings section then select the Settings option. 3. Click on Security and Privacy.
4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled Set user passwords to expire after a number of days is ticked. 6. Enter 100 in the Days before passwords expire field.
7. Click Save changes to save the changes.

Question: 28

SIMULATION -
You need to ensure that a user named Grady Archie can monitor the service health of your Microsoft 365 tenant. The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft 365 portal.

Answer:

See explanation below.

Explanation:
You need to assign the Service Administrator role to Grady Archie.
1. In the Microsoft 365 Admin Center, type Grady Archie into the Search for users, groups, settings or tasks search box.
2. Select the Grady Archie user account from the search results.
3. In the Roles section of the user account properties, click the Edit link.
4. Select the Customized Administrator option. This will display a list of admin roles.
5. Select the Service admin role.
6. Click Save to save the changes.

Reference:
https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

Question: 29

You configure several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.
You need to allow a user named User1 to view Defender for Office 365 reports from the Threat management dashboard.
Which role provides User1 with the required role permissions?

A. Security administrators
B. Information Protection administrator
C. Message center reader
D. Service administrator

Answer: A

Explanation:
In order to view and use the reports described in this article, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:
☞ Organization Management
☞ Security Administrator
☞ Security Reader
☞ Global Reader
Note:
There are several versions of this question in the exam. The question has two possible correct answers: 1. Security Administrator
2. Security Reader
Other incorrect answer options you may see on the exam include the following:
☞ Compliance administrator
☞ Exchange administrator

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo

Question: 30

You have a Microsoft 365 subscription that contains a user named User1.
You plan to use Compliance Manager.
You need to ensure that User1 can assign Compliance Manager roles to users. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Compliance Manager Assessor
B. Global Administrator
C. Portal Admin
D. Compliance Manager Administrator

Answer: B

Explanation:
The Global Admin can manage role assignments in Compliance Manager.
Incorrect Answers:
C: Portal Admin is for the now deprecated classic portal.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/working-with-compliance-manager?view=o365-worldwide

Question: 31

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user

named User1.
You have a Data Subject Request (DSR) case named Case1.
You need to allow User1 to export the results of Case1. The solution must use the principle of least privilege. Which role should you assign to User1 for Case1?

A. eDiscovery Manager
B. Security Operator
C. eDiscovery Administrator
D. Global Reader

Answer: A

Explanation:

An E-Discovery Administrator role is superior in terms of RBAC than E-Discovery Manager.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?view=o365-worldwide#step-1-assign- ediscovery-permissions-to-potential-case-members

Question: 32

HOTSPOT -
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You create and enforce an Azure Active Directory (Azure AD) Identity Protection user risk policy that has the following settings:
- Assignments: Include Group1, Exclude Group2
- User-risk: User risk level of Medium and above
- Access: Allow access, Require password change

The users attempt to sign in. The risk level for each user is shown in the following table.

User	User risk level
User1	High
User2	Medium
User3	High

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 must change his password.	○	○
User2 must change his password.	○	○
User3 must change his password.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 must change his password.	○	○
User2 must change his password.	○	○
User3 must change his password.	○	○

Explanation:
Box 1: Yes.
User1 is in Group1 which the policy applies to.

Box 2: No -
User2 is in Group2 which is excluded from the policy.

Box 3: No -
User3 is in Group1 which is included in the policy and Group2 which is excluded from the policy. In this case, the exclusion wins so the policy does not apply to
User3.

Question: 33

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription. You need to allow a user named User1 to view ATP reports from the Threat management dashboard. Which role provides User1 with the required role permissions?

A. Compliance administrator
B. Security reader
C. Message center reader
D. Reports reader

Answer: B

Explanation:

What permissions are needed to view the Defender for Office 365 reports?

You need to be a member of one of the following role groups in the Security & Compliance Center:

Organization Management

Security Administrator

Security Reader

Global Reader

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-atp?

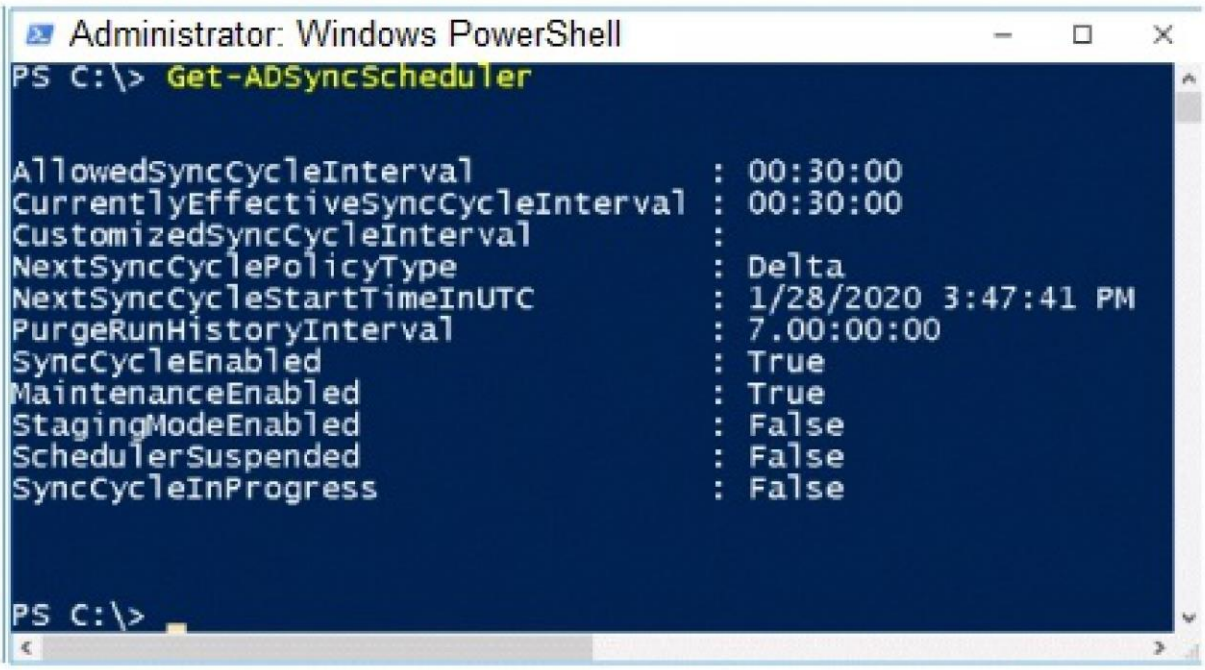
view=o365-worldwide#what-permissions-are-needed-to-view-the- atp-reports

Question: 34 HOTSPOT

-

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD) as shown in the following exhibit.

The synchronization schedule is configured as shown in the following exhibit:



Use the drop-down menus to select the answer choice that answers each question based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Which employees can authenticate by using Azure AD?

- Only employees who have an Azure AD user account
- Employees who have an Azure AD user account and a synced on-premises account
- Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

- Fix the synchronization server and install Azure AD Connect in staging mode
- Fix the synchronization server and install an additional authentication agent
- Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
- Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

Answer:

Answer Area

Which employees can authenticate by using Azure AD?

- Only employees who have an Azure AD user account
- Employees who have an Azure AD user account and a synced on-premises account
- **Only employees who have a synced on-premises account**

What should you do to remove the warning for pass-through authentication?

- Fix the synchronization server and install Azure AD Connect in staging mode
- **Fix the synchronization server and install an additional authentication agent**
- Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
- Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

Question: 35

HOTSPOT -
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Compliance administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure Active Directory (Azure AD) Identity Protection.
You need to identify which users can perform the following actions:☞
Configure a user risk policy.
☞ View the risky users report.
Which users 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

Configure a user risk policy:

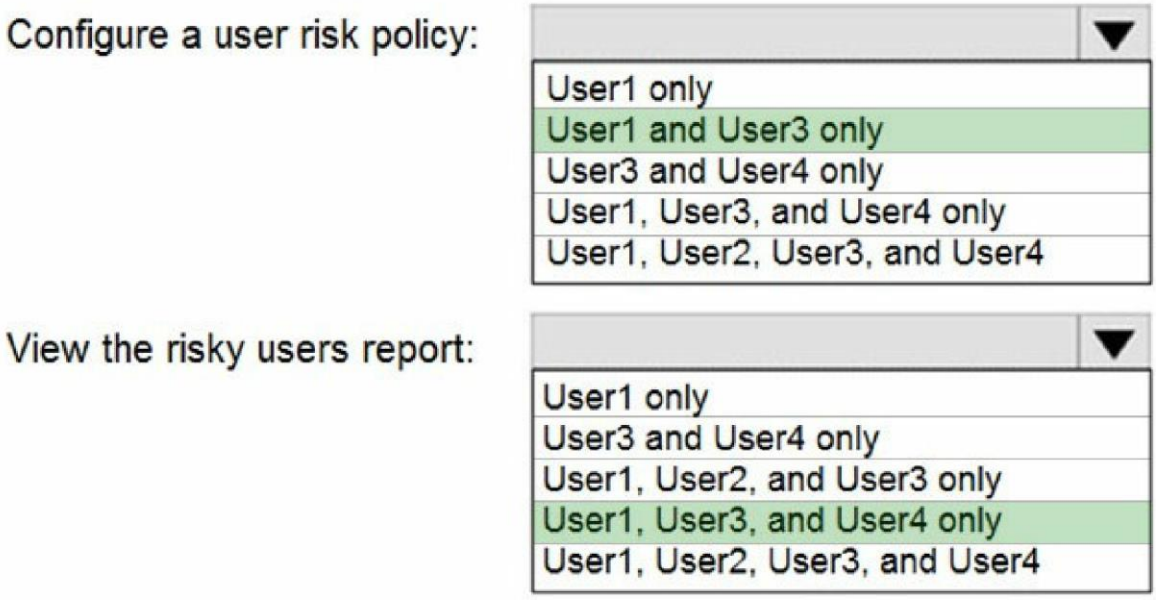
- User1 only
- User1 and User3 only
- User3 and User4 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

View the risky users report:

- User1 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

Answer:

Answer Area



Explanation:

1.- User1 and User3

2.- User1, User3, User4

Global administrator.Full access to Identity Protection

Compliance Administrator. Can't access to Security in the AAD blade.

Security administrator.Full access to Identity Protection

Security operator. View all Identity Protection reports and Overview blade

"Currently (3/21), the security operator role cannot access the Risky sign-ins report."

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

Question: 36 HOTSPOT

-

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

Name	Role
Admin1	Groups administrator
Admin2	User administrator

You add internal as a blocked word in the group naming policy for contoso.com.
You add Contoso- as prefix in the group naming policy for contoso.com.
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 create a Microsoft 365 group named Distribution.	○	○
Admin2 can create a Microsoft 365 group named Contoso-FinanceInternal.	○	○
Admin2 can create a security group named Contoso-internal.	○	○

Answer:

Answer Area

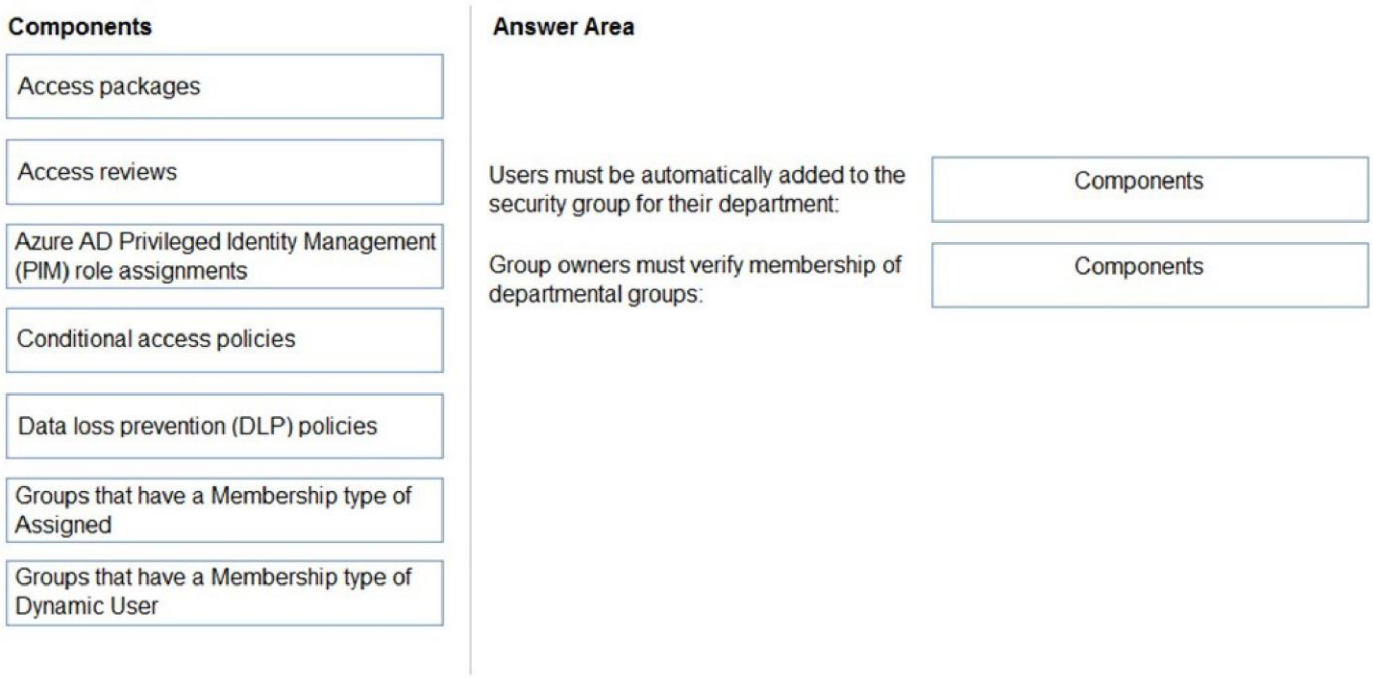
Statements	Yes	No
Admin1 can create a Microsoft 365 group named Distribution.	○	○
Admin2 can create a Microsoft 365 group named Contoso-FinanceInternal.	○	○
Admin2 can create a security group named Contoso-internal.	○	○

Explanation:
User Admin and Global Admin are exempt from group password policies.

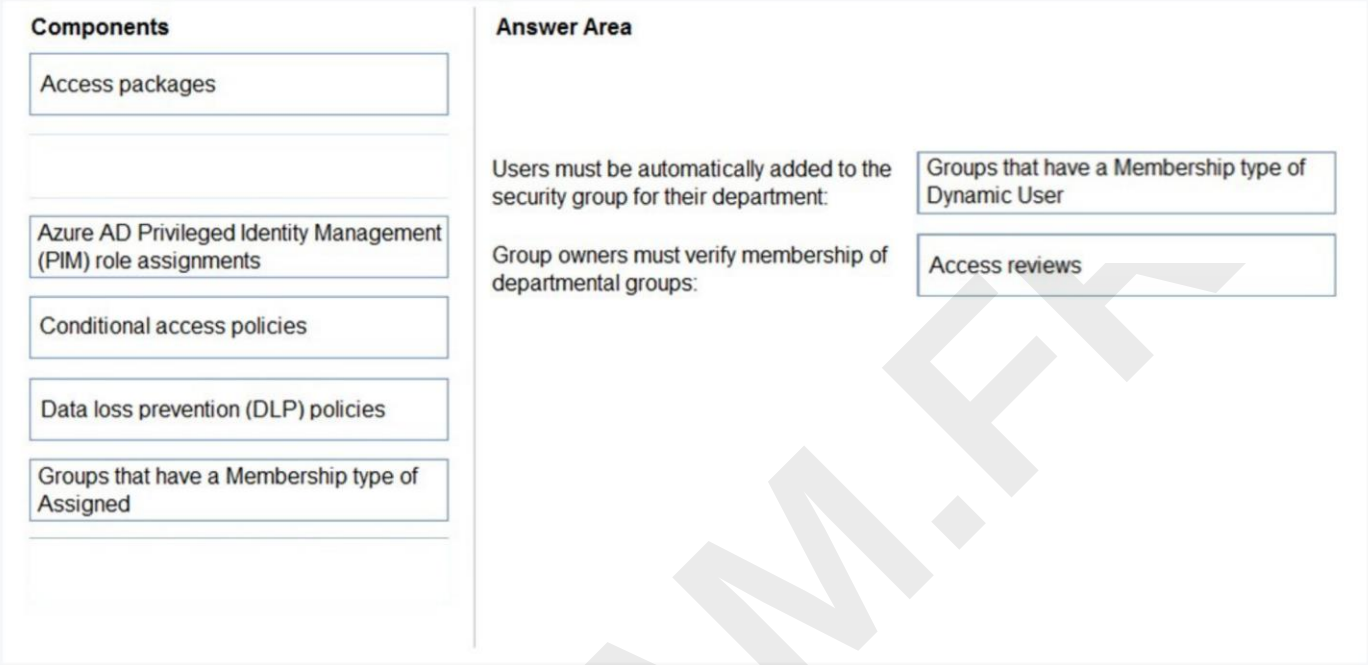
Reference:
https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide

Question: 37

DRAG DROP -
You have a Microsoft 365 tenant.
User attributes are synced from your company's human resources (HR) system to Azure Active Directory (Azure AD).
The company has four departments that each has its own Microsoft SharePoint Online site. Each site must be accessed only by the users from its respective department.
You are designing an access management solution that has the following requirements:☞ Users must be added automatically to the security group of their department.
☞ All security group owners must verify once quarterly that only the users in their department belong to their group.
Which components should you recommend to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may only 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.
Select and Place:



Answer:



Explanation:

Reference:
https://cloudbuild.co.uk/tag/create-a-dynamic-security-group-in-azure-ad/ https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question: 38

HOTSPOT -
You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager. The Compliance policy settings are configured as shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ — Compliant / **Not Compliant**

Enhanced jailbreak detection ⓘ — Enabled / **Disabled**

Compliance status validity period (days) ⓘ — 30

On February 25, 2020, you create the device compliance policies shown in the following table.

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

On March 1. 2020, users enroll Windows 10 devices in Microsoft Endpoint Manager as shown in the following table

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

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 March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Answer:

Answer Area

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Explanation:
Box 1: Yes -
Device2 is in Group2 so Policy2 applies.

Device2 is not compliant with Policy2. However, the device won't be marked as non-compliant until 10 days after the device was enrolled.

Box 2: Yes -
Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

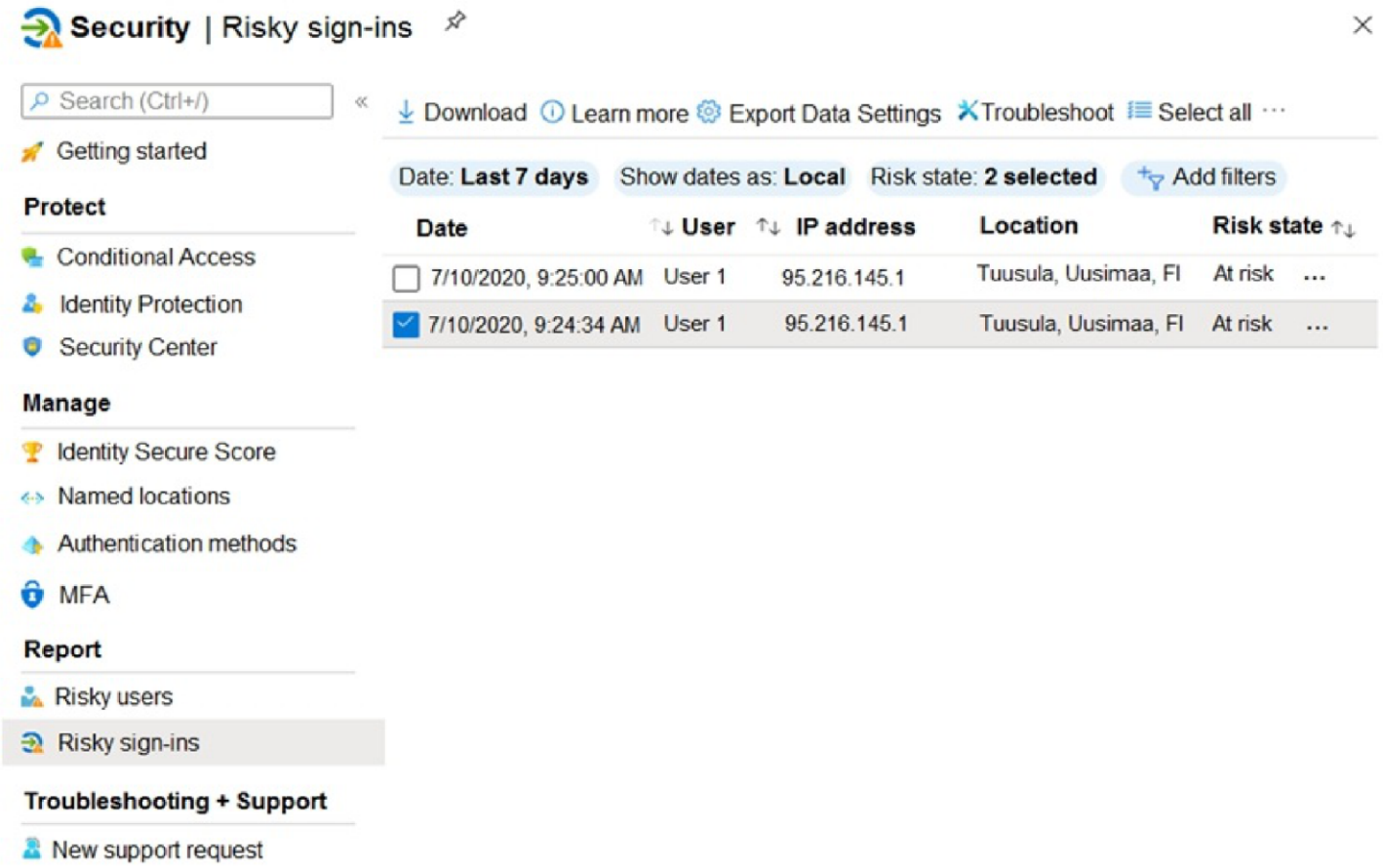
Device1 is compliant with Policy1 but non-compliant with Policy2. However, the device won't be marked as non-compliant until 10 days after the device was enrolled.

Box 3: No -
Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.
Device1 is compliant with Policy1 but non-compliant with Policy2. th

March 12 -
is more than 10 days after the device was enrolled so it will now be marked as non-compliant by Policy2.

Question: 39

You have a Microsoft 365 tenant.
From the Azure Active Directory admin center, you review the Risky sign-ins report as shown in the following exhibit.



You need to ensure that you can see additional details including the risk level and the risk detection type. What should you do?

A. Purchase Microsoft 365 Enterprise E5 licenses.

B. Activate an instance of Microsoft Defender for Identity.

C. Configure Diagnostic settings in Azure Active Directory (Azure AD). D. Deploy Azure Sentinel and add a Microsoft Office 365 connector.

Answer: A

Explanation:

As per the link you need a AAD premium P2license to do some good stuff, and in other articles to get more risk info

As per the link you need a AAD premium P2 license to get more risk info - AAD P2 is part of the Microsoft E5 license.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#license-requirements

Question: 40

You have a Microsoft 365 E5 subscription.
You plan to create a conditional access policy named Policy1. You need to be able to use the sign-in risk level condition in Policy1. What should you do first?

A. Connect Microsoft Endpoint Manager and Microsoft Defender for Endpoint. B. From the Azure Active Directory admin center, configure the Diagnostics settings. C. From the Endpoint Management admin center, create a device compliance policy.

D. Onboard Azure Active Directory (Azure AD) Identity Protection.

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk

Question: 41

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Type	Member of
User1	Member	Group1
User2	Member	Group2
User3	Guest	Group1

You assign an enterprise application named App1 to Group1 and User2.
You configure an Azure AD access review of App1. The review has the following settings:
- Review name: Review1
- Start date: 01`"15`"2020
- Frequency: One time
- End date: 02`"14`"2020
- Users to review: Assigned to an application
- Scope: Everyone
- Applications: App1
- Reviewers: Members (self)
- Auto apply results to resource: Enable
- Should reviewer not respond: Take recommendations

On February 15, 2020, you review the access review report and see the entries shown in the following table:

Name	User requires access to App1	Last sign in
User1	Yes	February 14, 2020
User2	No response	February 1, 2020
User3	No response	January 3, 2020

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 February 20, 2020, User1 can access App1.	○	○
On February 20, 2020, User2 can access App1.	○	○
On February 20, 2020, User3 can access App1.	○	○

Answer:

Answer Area

Statements	Yes	No
On February 20, 2020, User1 can access App1.	○	○
On February 20, 2020, User2 can access App1.	○	○
On February 20, 2020, User3 can access App1.	○	○

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/perform-access-review

Question: 42

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 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.
Solution: You enable SSPR for Group3.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and
Cloud application administrators. Therefore, we must enable SSPR for User3 by applying it to Group2 and not Group3 as User4 is in Group3. User4 would thus be affected if we enable it on Group3.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

Question: 43

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 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.
Solution: You enable SSPR for Group2.
Does that meet the goal?

A. Yes

B. No

Answer: A

Explanation:
By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and
Cloud application administrators.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-re set-policy-differences

Question: 44

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.
Solution: You enable SSPR for Group1.
Does that meet the goal?

A. Yes

B. No

Answer: B

Explanation:
By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and
Cloud application administrators. Thus, we must enable SSPR for User3 by applying it to Group2.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-re set-policy-differences

Question: 45

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Group	Role
User1	Group1	User administrator
User2	Group1	Security operator
User3	Group2	Security reader
User4	None	Global administrator

You enable self-service password reset for Group1 and configure security questions as the only authentication method for self-service password reset.
You need to identity which user must answer security questions to reset their password. Which user should you identify?

A. User1
B. User2
C. User3
D. User4

Answer: B

Explanation:
Self-service password reset (SSPR) is only enabled for Group1 (User1 and User2). User1 cannot use security questions for SSPR because User1 has an administrative security role. Therefore, only User2 can use SSPR with security questions as the authentication method.

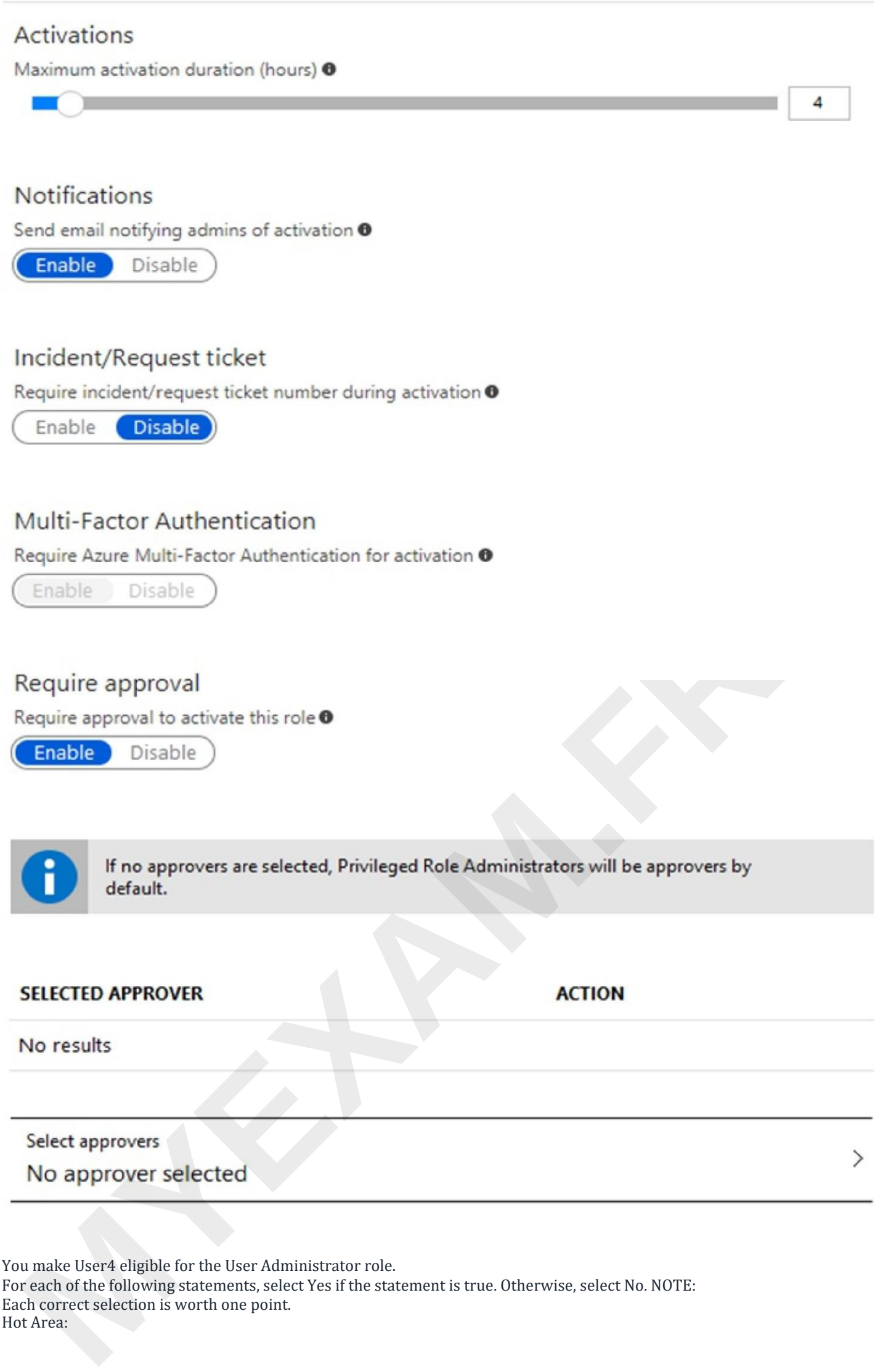
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

Question: 46

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Permanent role assignment
User1	Global Administrator
User2	Security Administrator
User3	Privileged Role Administrator
User4	None

The User Administrator role is configured in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.



You make User4 eligible for the User Administrator role.
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 receives an email notification when User4 activates the User Administrator role.	○	○
User2 receives an email notification when User4 activates the User Administrator role.	○	○
User3 receives an email notification when User4 requests activation of the User Administrator role.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	○	○
User2 receives an email notification when User4 activates the User Administrator role.	○	○
User3 receives an email notification when User4 requests activation of the User Administrator role.	○	○

Question: 47

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1.
The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.
For User1, you select Confirm user compromised.
User1 can still sign in.
You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.
Solution: You configure the user risk policy to block access when the user risk level is high.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

In my opinion it should be A, since it is only blocking high risk users and lower risk users are not affected

Question: 48

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 E5 subscription that contains a user named User1.

The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.
For User1, you select Confirm user compromised.
User1 can still sign in.
You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.
Solution: You configure the sign-in risk policy to block access when the sign-in risk level is high.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk

Question: 49

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 E5 subscription that contains a user named User1.
The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.
For User1, you select Confirm user compromised.
User1 can still sign in.
You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.
Solution: From the Access settings, you select Block access for User1.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk

Question: 50

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 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.
Solution: You create a conditional access policy for User1, User2, and User3. Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:

SSPR is not enforced/configured via Conditional Access Policy.

It is part of the "Password Reset" menu in AAD.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#enable-self-service-password-reset

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

Question: 51

You have a Microsoft 365 tenant that is linked to a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.
You need to enable Azure AD Seamless Single Sign-On (Azure AD SSO) for contoso.com. What should you use?

A. Azure AD Connect
B. the Microsoft 365 Defender portal
C. the Microsoft 365 Security admin center
D. the Microsoft 365 admin center

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

Question: 52

You have a Microsoft 365 subscription.
You need to recommend a passwordless authentication solution that uses biometric authentication. What should you include in the recommendation?

A. Windows Hello for Business
B. a smart card
C. the Microsoft Authenticator app
D. a PIN

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Question: 53

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.
You plan to deploy a hybrid Azure Active Directory (Azure AD) tenant that has Azure AD Identity Protection risk policies enabled.
You need to configure Azure AD Connect to support the planned deployment.
Which Azure AD Connect authentication method should you select?

A. Federation with AD FS
B. Federation with PingFederate
C. Password Hash Synchronization
D. Pass-through authentication

Answer: C

Explanation:

One of the protection risk policies is a “Use risk policy”. It will require a password change. For this to work in a hybrid environment:Make sure you have PHS, Password Writeback and SSPR enabled

Honestly, I don't understand the fact that answers to such trivial questions are wrong. This exam is full of wrong answers, any idea how to change it?

Question: 54

You have several Conditional Access policies that block noncompliant devices from connecting to services. You need to identify which devices are blocked by which policies.
What should you use?

A. the Device compliance report in the Microsoft Endpoint Manager admin center
B. the Device compliance trends report in the Microsoft Endpoint Manager admin center
C. Activity log in the Cloud App Security portal
D. the Conditional Access Insights and Reporting workbook in the Azure Active Directory admin center

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

Question: 55

You have a Microsoft 365 subscription named contoso.com.
You need to configure Microsoft OneDrive for Business external sharing to meet the following requirements:☞
Enable file sharing for users that have a Microsoft account.
☞ Block file sharing for anonymous users.
What should you do?

A. From Advanced settings for external sharing, select Allow or block sharing with people on specific domains and add contoso.com.
B. From the External sharing settings for OneDrive, select Only people in your organization.
C. From the External sharing settings for OneDrive, select Existing external users.
D. From the External sharing settings for OneDrive, select New and existing external users.

Answer: D

Explanation:

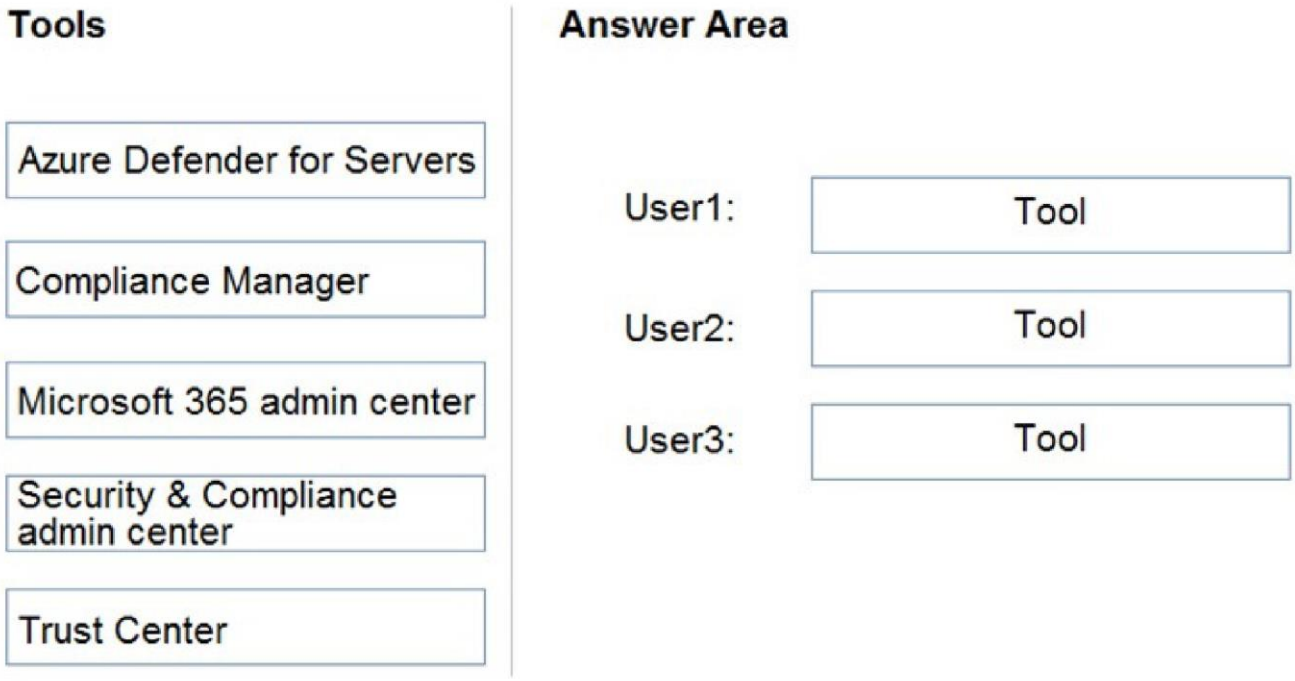
Reference:
https://www.sharepointdiary.com/2020/09/enable-external-sharing-in-onedrive-for-business.html

Question: 56

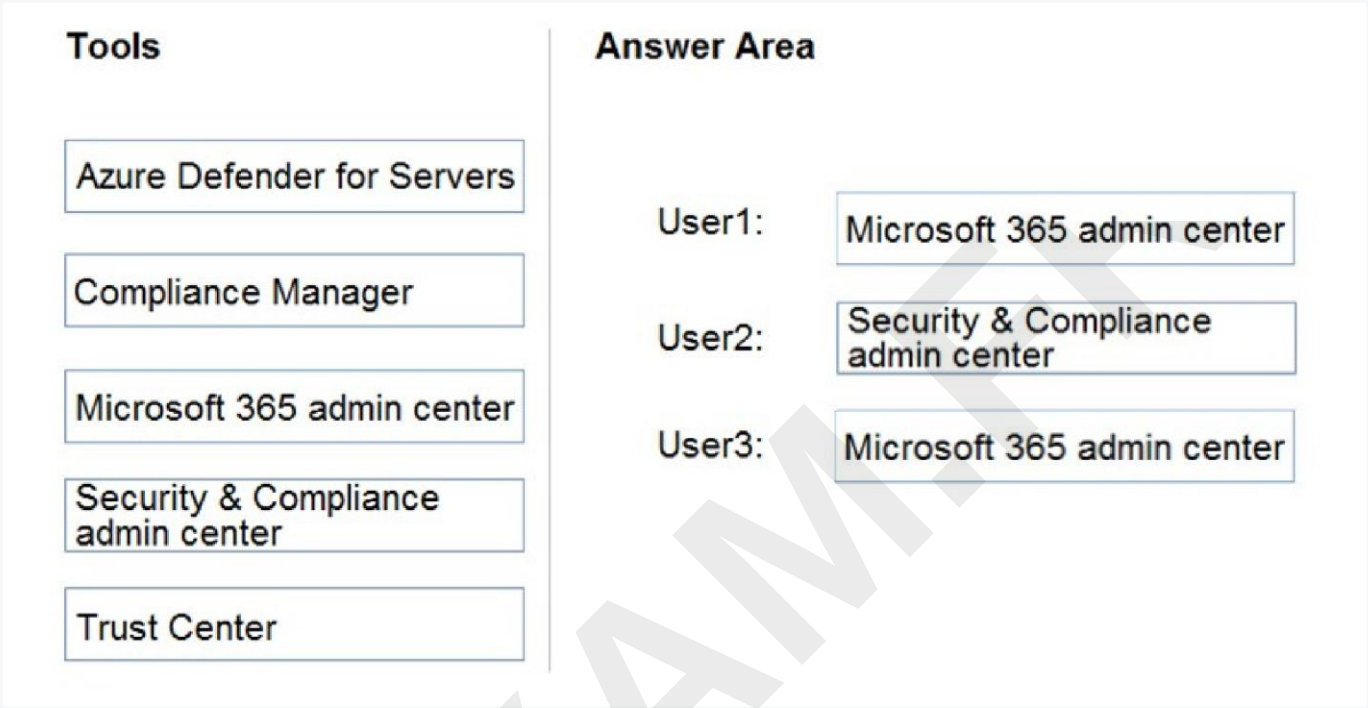
DRAG DROP -
You have a Microsoft 365 E5 tenant that contains three users named User1, User2, and User3. You need to assign roles or role groups to the users as shown in the following table.

User	Role or role group
User1	SharePoint admin
User2	Data Investigator
User3	User admin

What should you use to assign a role or role group to each user? To answer, drag the appropriate tools to the correct roles or role groups. Each tool 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.
Select and Place:



Answer:



Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

Question: 57

Your network contains an on-premises Active Directory domain named contoso.local that has a forest functional level of Windows Server 2008 R2.
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to install Azure AD Connect and enable single sign-on (SSO).
You need to prepare the domain to support SSO. The solution must minimize administrative effort.

What should you do?

A. Raise the forest functional level to Windows Server 2016.
B. Modify the UPN suffix of all domain users.
C. Populate the mail attribute of all domain users.
D. Rename the domain.

Answer: B

Explanation:

"You can solve the ".local" problem by registering new UPN suffix or suffixes in AD DS to match the domain (or domains) you verified in Microsoft 365. "

Reference:

https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide

Question: 58

HOTSPOT -
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Department	Microsoft 365 role
Admin1	IT	Groups admin
Admin2	IT	User admin
Admin3	Research	User admin
Admin4	Finance	Groups admin

For contoso.com, you create a group naming policy that has the following configuration:
<Department> - <Group name>
You plan to create the groups shown in the following table.

Name	Type
IT-Group1	Microsoft 365
Finance-Group2	Security

Which user can be used to create each group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

IT-Group1:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin4 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Finance-Group2:

- Admin4 only
- Admin1 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Answer:

Answer Area

IT-Group1:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin4 only
- Admin1, Admin2, and Admin3 only
- **Admin1, Admin2, Admin3, and Admin4**

Finance-Group2:

- Admin4 only
- Admin1 and Admin4 only
- Admin2, Admin3, and Admin4 only
- **Admin1, Admin2, Admin3, and Admin4**

Explanation:

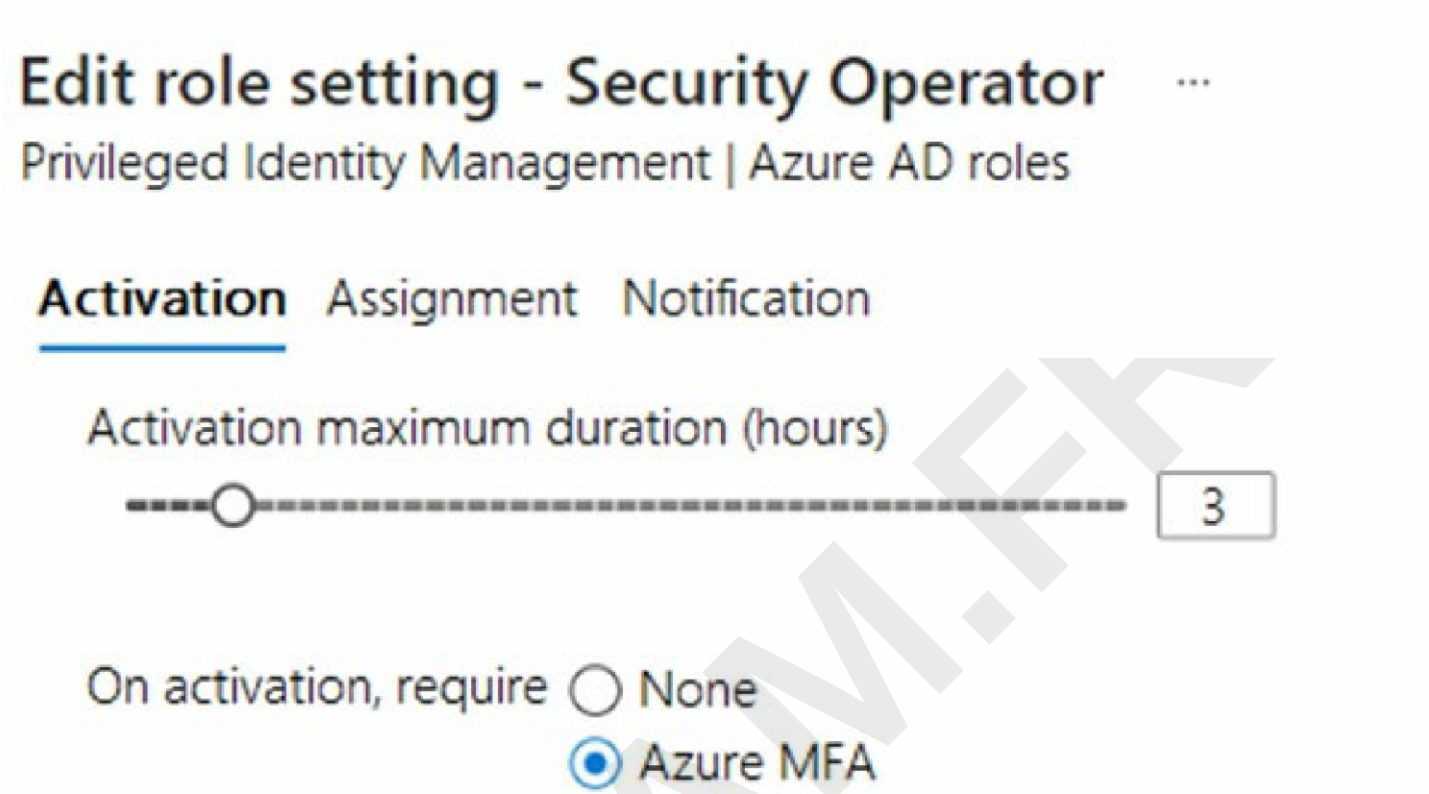
Reference:
https://office365itpros.com/2020/01/22/using-groups-admin-role/ https://docs.microsoft.com/en-us/azure/ac tive-directory/roles/permissions-reference

Question: 59

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

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

You configure the Security Operator role in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.



You add assignments to the Security Operator role as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

Which users can activate the Security Operator role?

A. User2 only
B. User3 only
C. User1 and User2 only

D. User2 and User3 only
E. User1, User2, and User3

Answer: C

Explanation:

Because:1. Active assignments don't require the member to activate the role before usage. Members assigned as active have the privileges assigned ready to use. This type of assignment is also available to customers that don't use Azure AD PIM2. https://learn.microsoft.com/en-us/answers/questions/529070/user-mfa-is-disabled-however-pim-activation-is-ask.html

Active assignments don't require the member to activate the role before usage.
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

Question: 60

You have a Microsoft 365 tenant.
You need to implement a policy to enforce the following requirements:
☞ If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint
Online only from a web browser. The user must be prevented from downloading files or syncing files from SharePoint Online.
☞ If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files.
What should you create?

A. a conditional access policy in Azure AD that has Client apps conditions configured
B. a conditional access policy in Azure AD that has Session controls configured
C. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured
D. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured

Answer: B

Explanation:

Because the Application enforced restrictions..

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

Question: 61

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains two users named User1 and User2.
You need to assign Role Based Access Control (RBAC) roles to User1 and User2 to meet the following requirements:
☞ Use the principle of least privilege.
☞ Enable User1 to view sync errors by using Azure AD Connect Health.
☞ Enable User2 to configure Azure Active Directory Connect Health Settings.
Which two roles should you assign? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The Monitoring Reader role in Azure AD Connect Health to User1
B. The Security reader role in Azure AD to User1
C. The Reports reader role in Azure AD to User1
D. The Contributor role in Azure AD Connect Health to User2
E. The Monitoring Contributor role in Azure AD Connect Health to User2
F. The Security operator role in Azure AD to User2

Answer: AD

Explanation:

For the second role I would select the Contributor role in AAC Connect Health (Option D) rather than the Monitoring Contributor role (option E), which doesn´t exist in the latest documentation, AFAIKhttps://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations#manage-access-with-azure-rbac https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#connect-health

Question: 62

You have a Microsoft 365 subscription that contains a user named User1. You need to assign User1 permissions to search Microsoft Office 365 audit logs. What should you use?

A. the Azure Active Directory admin center
B. the Exchange admin center
C. the Microsoft 365 Defender portal
D. the Microsoft 365 Compliance center

Answer: B

Explanation:
To give a user the ability to search the audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only
Audit Logs or Audit Logs role, and then add the user as a member of the new role group.

Incorrect:
Not D: If you assign a user the View-Only Audit Logs or Audit Logs role on the Permissions page in the compliance portal, they won't be able to search the audit log. You have to assign the permissions in Exchange Online. This is because the underlying cmdlet used to search the audit log is an Exchange Online cmdlet. You can also use the Exchange admin center (EAC).

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-complianc e

Question: 63

You have a Microsoft 365 tenant that has modern authentication enabled.
You have Windows 10, MacOS, Android, and iOS devices that are managed by using Microsoft Endpoint Manager. Some users have older email client applications that use Basic authentication to connect to Microsoft Exchange Online.
You need to implement a solution to meet the following security requirements:
☞ Allow users to connect to Exchange Online only by using email client applications that support modern

authentication protocols based on OAuth 2.0.
☞ Block connections to Exchange Online by any email client applications that do NOT support modern authentication.
What should you implement?

A. a conditional access policy in Azure Active Directory (Azure AD)
B. an application control profile in Microsoft Endpoint Manager
C. a compliance policy in Microsoft Endpoint Manager
D. an OAuth app policy in Microsoft Defender for Cloud Apps

Answer: A

Explanation:
Block clients that don't support multi-factor with a Conditional Access policy.
Note: Clients that do not use modern authentication can bypass Conditional Access policies, so it's important to block these.
Incorrect:
Not D: OAuth app policies enable you to investigate which permissions each app requested and which users authorized them for Office 365, Google Workspace, and Salesforce. You're also able to mark these permissions as approved or banned.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies

Question: 64

HOTSPOT -
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a user named User1 and multiple Windows
10 devices. The devices are Azure AD joined and protected by using BitLocker Drive Encryption (BitLocker).
You need to ensure that User1 can perform the following actions:☞
View BitLocker recovery keys.
☞ Configure the usage location for the users in the tenant.
The solution must use the principle of least privilege.
Which two roles should you assign to User1 in the Microsoft 365 admin center? To answer, select the appropriate roles in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

- [ ] Cloud device admin
- [ ] Desktop Analytics admin
- [ ] Intune Administrator
- [ ] Printer admin
- [ ] Printer tech

Global

- [ ] Global Administrator

Identity

- [ ] Application admin
- [ ] Application developer
- [ ] Authentication admin
- [ ] Cloud application admin
- [ ] Conditional Access admin
- [ ] Domain Name Administrator
- [ ] External identity provider admin

Answer:

Answer Area

- [ ] Cloud device admin
- [ ] Desktop Analytics admin
- [ ] Intune Administrator
- [ ] Printer admin
- [ ] Printer tech

Global

- [ ] Global Administrator

Identity

- [ ] Application admin
- [ ] Application developer
- [ ] Authentication admin
- [ ] Cloud application admin
- [ ] Conditional Access admin
- [ ] Domain Name Administrator
- [ ] External identity provider admin

Explanation:
Box 1: Helpdesk admin -
View BitLocker recovery keys.

Helpdesk Admins can read bitlocker metadata and key on devices Note:
One of the following should be enough:

Global admins -

Intune Service Administrators -

Security Administrators -

Security Readers -

Helpdesk Admins -

Box 2: User Administrator -
Configure the usage location for the users in the tenant.
The User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.
The User Administrator cam manage all user properties including User Principal Name

Update (FIDO) device keys -

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Question: 65 HOTSPOT

-
Your on-premises network contains an Active Directory domain that syncs to Azure Active Directory (Azure AD) by using Azure AD Connect. The functional level of the domain is Windows Server 2019.
You need to deploy Windows Hello for Business. The solution must meet the following requirements:
☞ Ensure that users can access Microsoft 365 services and on-premises resources.
☞ Minimize administrative effort.
How should you deploy Windows Hello for Business and which type of trust should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

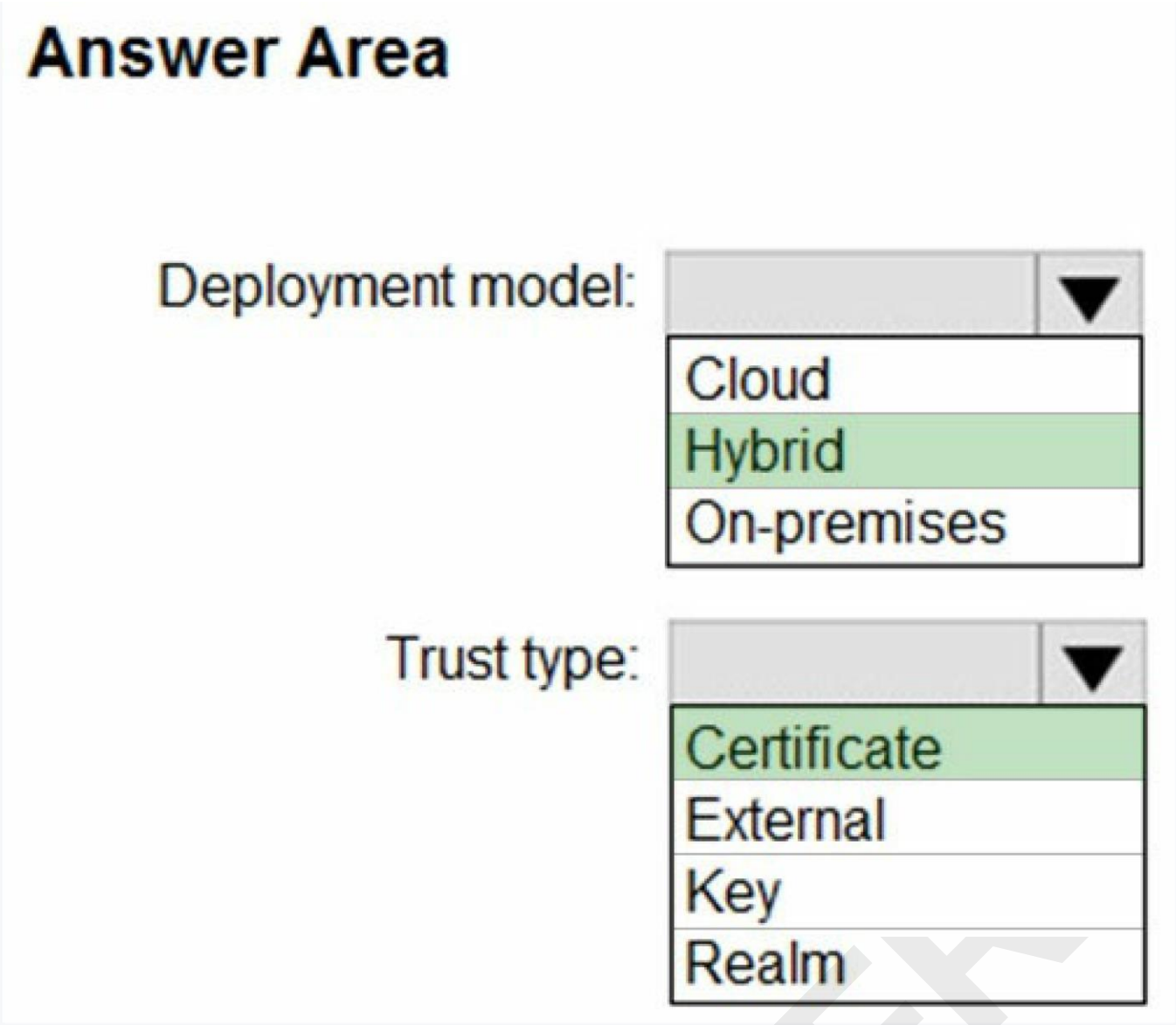
Deployment model:

- Cloud
- Hybrid
- On-premises

Trust type:

- Certificate
- External
- Key
- Realm

Answer:



Explanation:
Box 1: Hybrid -
Hybrid environments are distributed systems that enable organizations to use on-premises and Azure-based identities and resources.

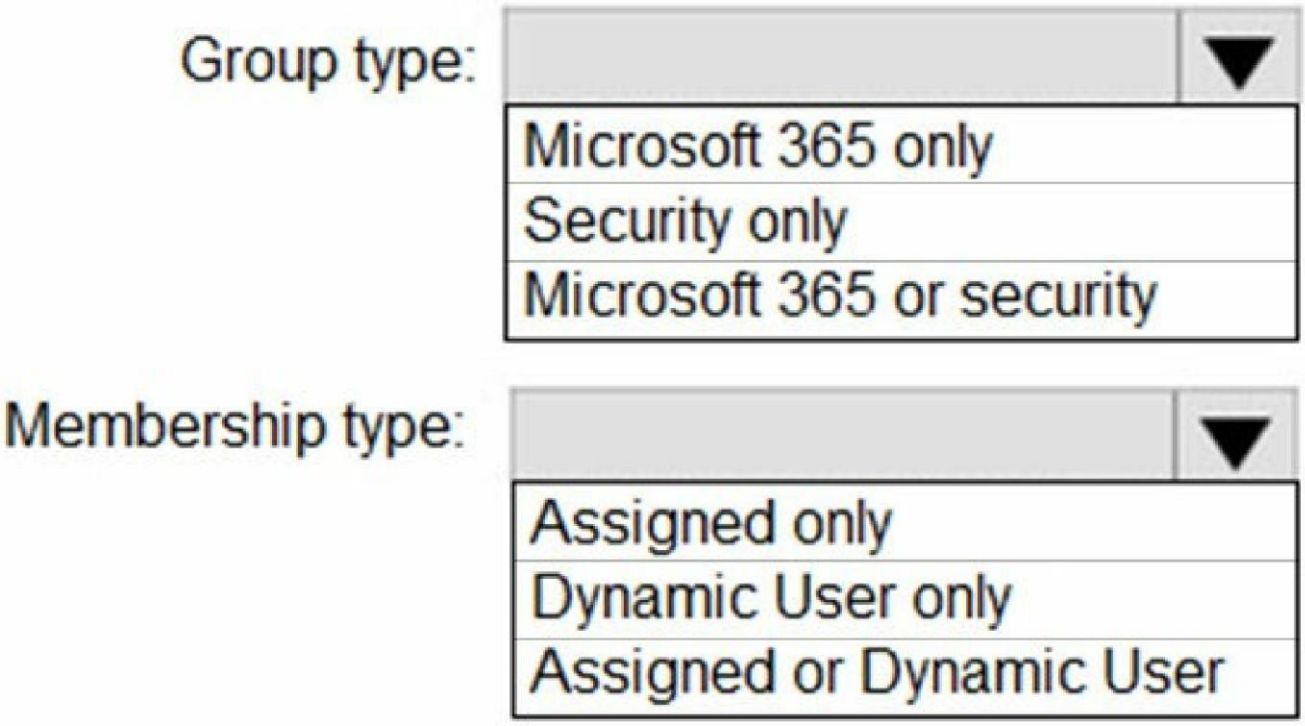
Box 2: Certificate -
The Windows Hello for Business deployment depends on an enterprise public key infrastructure as trust anchor for authentication. Domain controllers for hybrid deployments need a certificate in order for Windows devices to trust the domain controller.

Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cert-t rust-prereqs

Question: 66

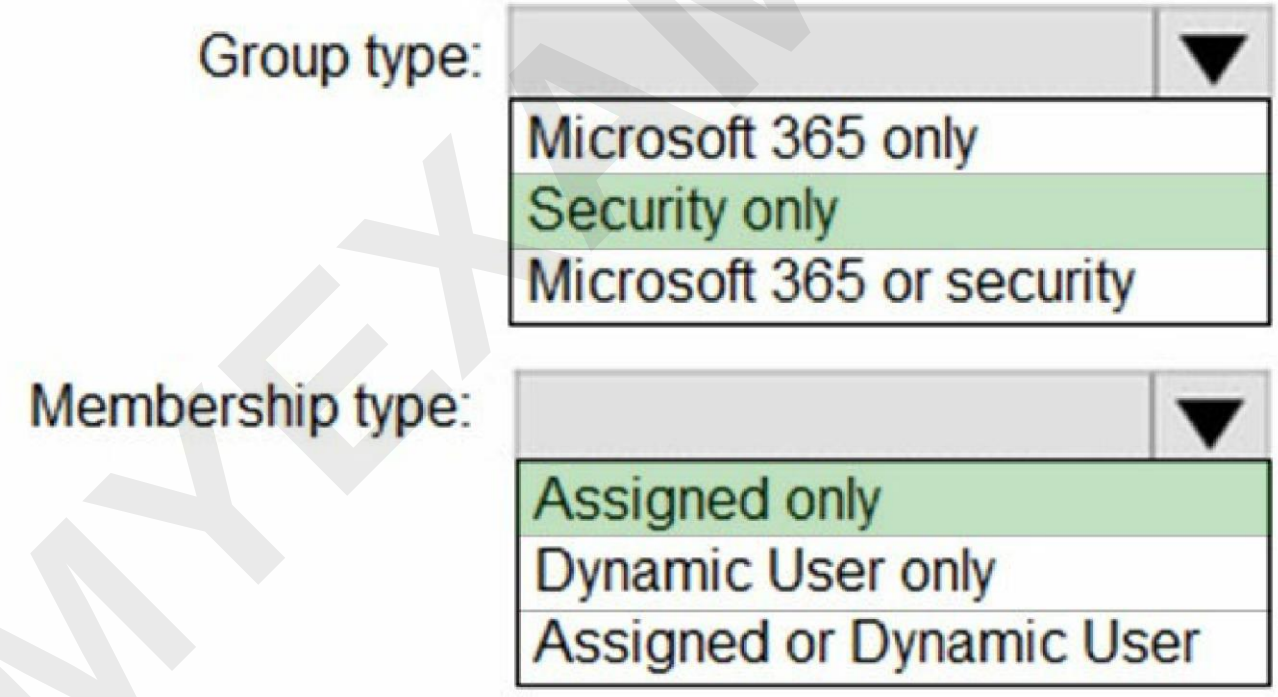
HOTSPOT -
You have a Microsoft 365 E5 subscription.
You need to create a role-assignable group. The solution must ensure that you can nest the group. How should you configure the group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:
Box 1: Security only -
You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.

Incorrect:
Not supported:
Adding Security groups to Microsoft 365 groups.
Adding Microsoft 365 groups to Security groups or other Microsoft 365 groups.

Box 2: Assigned only -
The membership type for role-assignable groups must be Assigned and can't be an Azure AD dynamic group.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal

Question: 67

HOTSPOT -
You create device groups in Microsoft Defender for Endpoint as shown in the following table.

Name	Rank	Membership rule
Group1	1	Name Starts with Device
Group2	2	Tag Equals Tag1
Group3	3	Name Starts with Computer and OS is Windows 10

You onboard three devices to Microsoft Defender for Endpoint as shown in the following table.

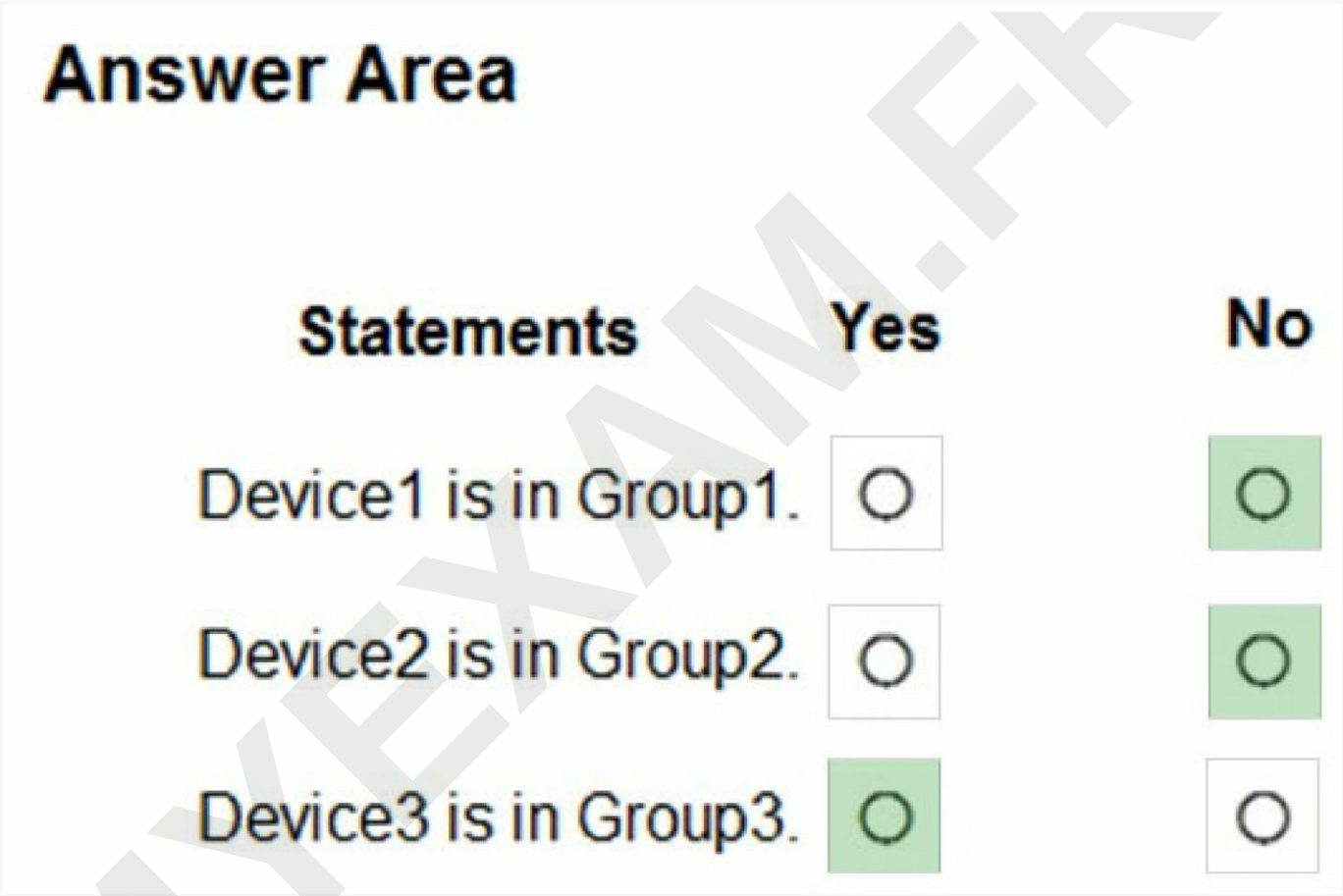
Name	Operating system
Device1	Windows 10
Device2	MacOS
Computer3	Windows 10

After the devices are onboarded, you perform the following actions:➪
Add a tag named Tag1 to Device1.
➪ Rename Computer3 as 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
Device1 is in Group1.	○	○
Device2 is in Group2.	○	○
Device3 is in Group3.	○	○

Answer:



Explanation:
Box 1: No -
The Group1 membership rule 'Name Start with Device' applies to Device1.
However, the higher ranked Group2 membership rule 'Tag Equals Tag1' also applies to Device1, and overrules

the lower ranked rule.

Note: Specify the matching rule that determines which device group belongs to the group based on the device name, domain, tags, and OS platform. If a device is also matched to other groups, it's added only to the highest ranked device group.

Box 2: No -
The Group1 membership rule 'Name Start with Device' applies Device2. No other rule applies.

Box 3: Yes -
The Group3 rule applies for Computer3.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups

Question: 68

You have a Microsoft 365 E5 subscription that contains 100 users. Each user has a computer that runs Windows 10 and either an Android mobile device or an iOS mobile device. All the devices are registered with Azure Active Directory (Azure AD).
You enable passwordless authentication for all the users.
You need to ensure that the users can sign in to the subscription by using passwordless authentication. What should you instruct the users to do on their mobile device first?

A. Install a device certificate.
B. Install a user certificate.
C. Install the Microsoft Authenticator app.
D. Register for self-service password reset (SSPR).

Answer: C

Explanation:
The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.

Note: Microsoft Authenticator App
You can allow your employee's phone to become a passwordless authentication method. You may already be using the Microsoft Authenticator App as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordles s

Question: 69

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Azure Multi-Factor Authentication (Azure MFA)
User1	Group1	None
User2	Group1	User authenticates by using a text message.
User3	Group1	User authenticates by using the Microsoft Authenticator app.
User4	Group1	User authenticates by using passwordless authentication.

You enable the authentication methods registration campaign and configure the Microsoft Authenticator method for Group1.
Which users will be prompted to configure authentication during sign in?

A. User1 only
B. User2 only
C. User2 and User3 only
D. User1 and User2 only
E. User2 and User3 only
F. User1, User2, and User3 only

Answer: D

Explanation:
You can nudge users to set up Microsoft Authenticator during sign-in. Users will go through their regular sign-in, perform multifactor authentication as usual, and then be prompted to set up Microsoft Authenticator. You can include or exclude users or groups to control who gets nudged to set up the app. This allows targeted campaigns to move users from less secure authentication methods to Microsoft Authenticator.

Incorrect:
Not C, Not E, Not F: Not User3 since the user must not have already set up Microsoft Authenticator for push notifications on their account.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-registration-campaign

Question: 70

HOTSPOT -
You have a Microsoft 365 subscription that contains three users named User1, User2, and User3. You have the named locations shown in the following table.

Name	IP address range	Trusted
NY	192.168.2.0/27	Yes
DC	192.168.1.0/27	No
LA	192.168.3.0/27	No

You configure an Azure Multi-Factor Authentication (MFA) trusted IP address range of 192.168.1.0/27. You have the Conditional Access policies shown in the following table.

Name	Assignments: Users and groups	Assignments: Cloud apps or actions	Conditions: Locations	Access controls: Grant
CA1	All users	Microsoft Forms	All trusted locations	Grant access: Require multi-factor authentication
CA2	All users	Microsoft Planner	NY	Block access

The users have the IP addresses shown in the following table.

User	IP address
User1	192.168.1.16
User2	192.168.2.16
User3	192.168.3.16

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:

Statements	Yes	No
User1 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	○	○
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○

Answer:

Statements	Yes	No
User1 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	○	○
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○

Explanation:
Box 1: No -
User1 has IP address 192.168.1.16, which is in DC named location. DC is not trusted. CA1 applies. Access will not be granted.

Box 2: No -
User2 has IP address 192.168.2.16, which is in NY named location. NY is trusted. However, CA2 blocks Microsoft Planner NY access.

Box 3: No -
User3 is in LA. LA is not trusted.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-polic ies

Question: 71

Your network contains an on-premises Active Directory domain. The domain contains a domain controller named DC1.
You have a Microsoft 365 E5 subscription.
You install the Microsoft Defender for Identity sensor on DC1.
You need to configure enhanced threat detection in Defender for Identity. The solution must ensure that the

following events are collected from DC1:
☞ 4726 - User Account Deleted
☞ 4728 - Member Added to Global Security Group
☞ 4776 - Domain Controller Attempted to Validate Credentials for an Account (NTLM) What should you do on DC1?

A. Install the Azure Monitor agent.
B. Install System Monitor (SYSMON).
C. Configure the Windows Event Collector service.
D. Configure the Advanced Audit Policy Configuration policy.

Answer: D

Explanation:
Windows Event logs -
Defender for Identity detection relies on specific Windows Event logs that the sensor parses from your domain controllers. For the correct events to be audited and included in the Windows Event log, your domain controllers require accurate Advanced Audit Policy settings.

For the correct events to be audited and included in the Windows Event Log, your domain controllers require accurate Advanced Audit Policy settings. Incorrect
Advanced Audit Policy settings can lead to the required events not being recorded in the Event Log and result in incomplete Defender for Identity coverage.

Note: Relevant Windows Events -
For Active Directory Federation Services (AD FS) events
1202 - The Federation Service validated a new credential
1203 - The Federation Service failed to validate a new credential 4624
- An account was successfully logged on
4625 - An account failed to log on

For other events -
1644 - LDAP search
4662 - An operation was performed on an object
4726 - User Account Deleted
4728 - Member Added to Global Security Group
4729 - Member Removed from Global Security Group
4730 - Global Security Group Deleted
4732 - Member Added to Local Security Group
4733 - Member Removed from Local Security Group
4741 - Computer Account Added
4743 - Computer Account Deleted
4753 - Global Distribution Group Deleted
4756 - Member Added to Universal Security Group
4757 - Member Removed from Universal Security Group
4758 - Universal Security Group Deleted
4763 - Universal Distribution Group Deleted
4776 - Domain Controller Attempted to Validate Credentials for an Account (NTLM) 7045 -
New Service Installed
8004 - NTLM Authentication

Reference:
https://docs.microsoft.com/en-us/defender-for-identity/prerequisites https://docs.microsoft.com/en-us/defen der-for-identity/configure-windows-event-collection

Question: 72

You have a Microsoft 365 E5 subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
A user named User1 is eligible for the User Account Administrator role. You need User1 to request to activate the User Account Administrator role. From where should User1 request to activate the role?

A. the My Access portal
B. the Microsoft 365 Defender portal
C. the Microsoft 365 admin center
D. the Azure Active Directory admin center

Answer: D

Explanation:

the Azure Active Directory admin center -> Azure portal ->Privileged Identity Management

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role

Question: 73

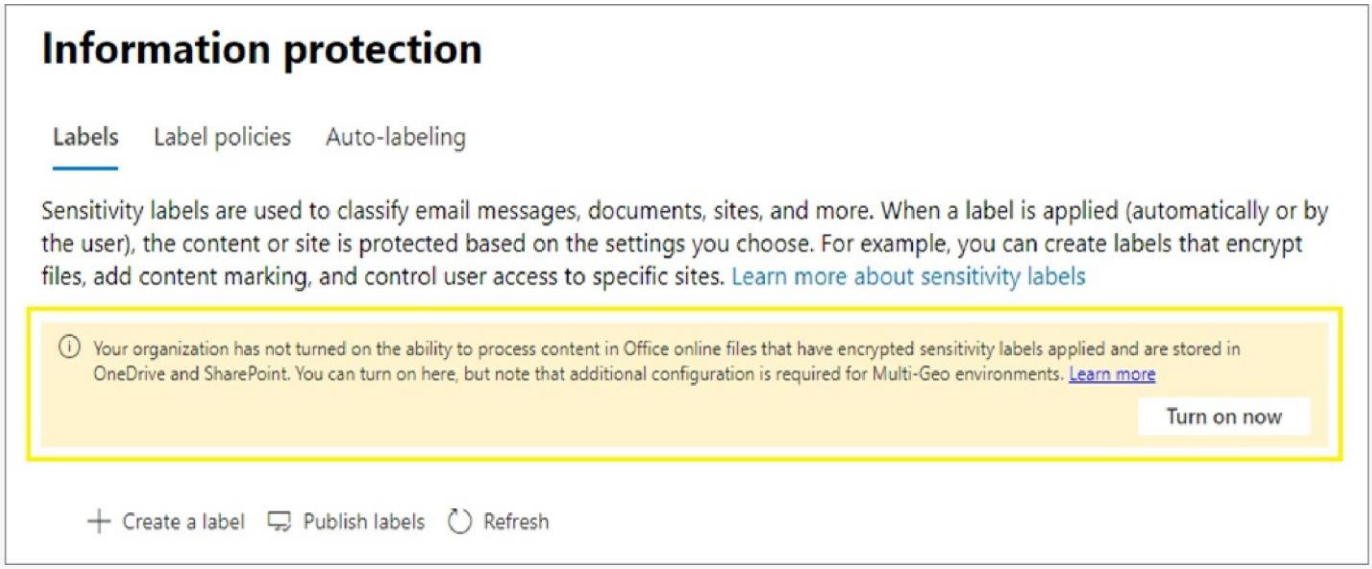
You have a Microsoft 365 E5 subscription.
You need to enable support for sensitivity labels in Microsoft SharePoint Online. What should you use?

A. the SharePoint admin center
B. the Microsoft 365 admin center
C. the Microsoft 365 Compliance center
D. the Azure Active Directory admin center

Answer: C

Explanation:
Use the Microsoft Purview compliance portal to enable support for sensitivity labels
This option is the easiest way to enable sensitivity labels for SharePoint and OneDrive, but you must sign in as a global administrator for your tenant.

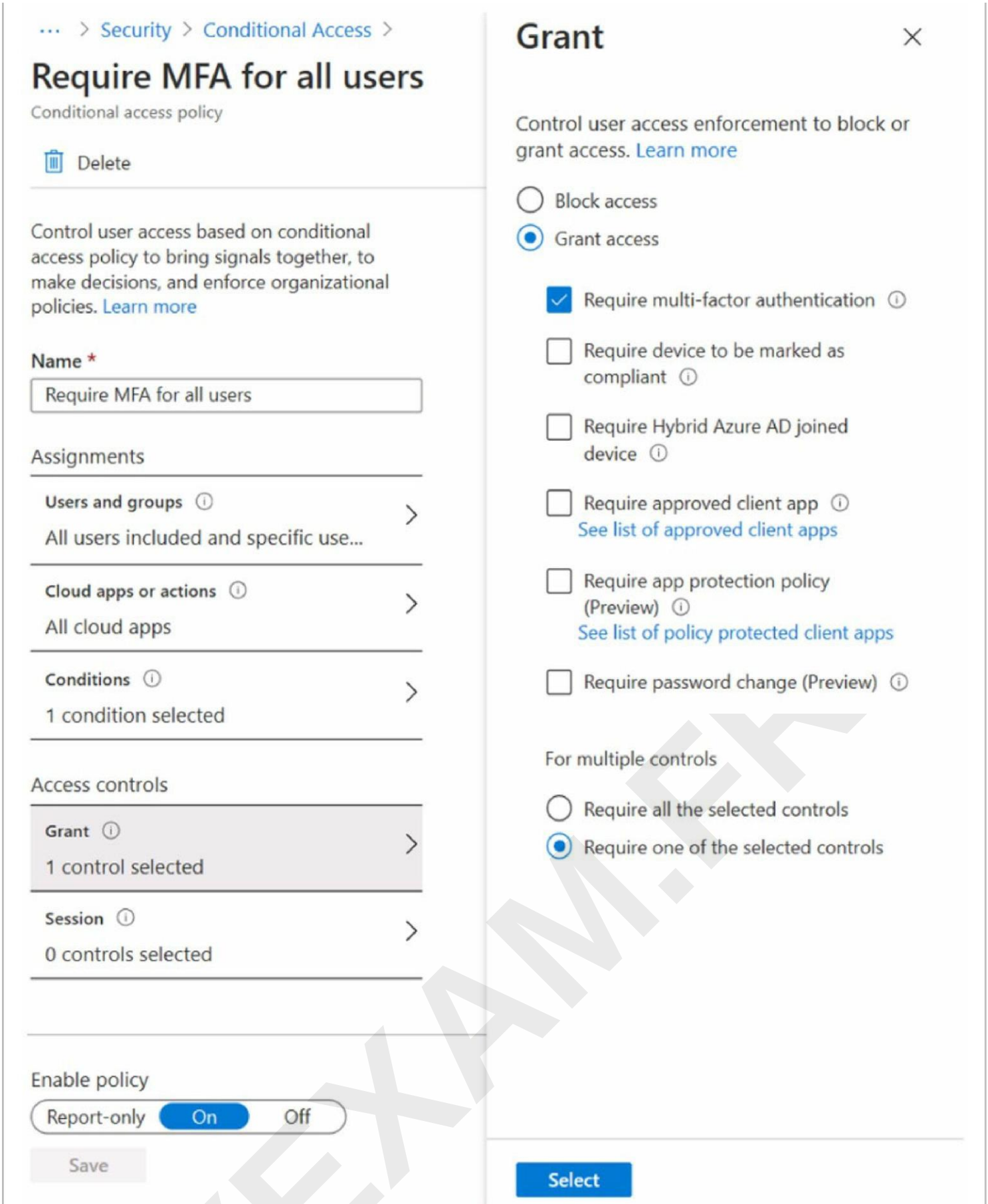
1. Sign in to the Microsoft Purview compliance portal as a global administrator, and navigate to Solutions > Information protection > Labels
2. If you see a message to turn on the ability to process content in Office online files, select Turn on now:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files

Question: 74

HOTSPOT -
You have a Microsoft 365 tenant.
A conditional access policy is configured for the tenant as shown in the Policy exhibit. (Click the Policy tab.)



The User Administrator role is configured as shown in the Role setting exhibit. (Click the Role setting tab.)

User Administrator | Role settings

Privileged Identity Management | Azure AD roles

Edit

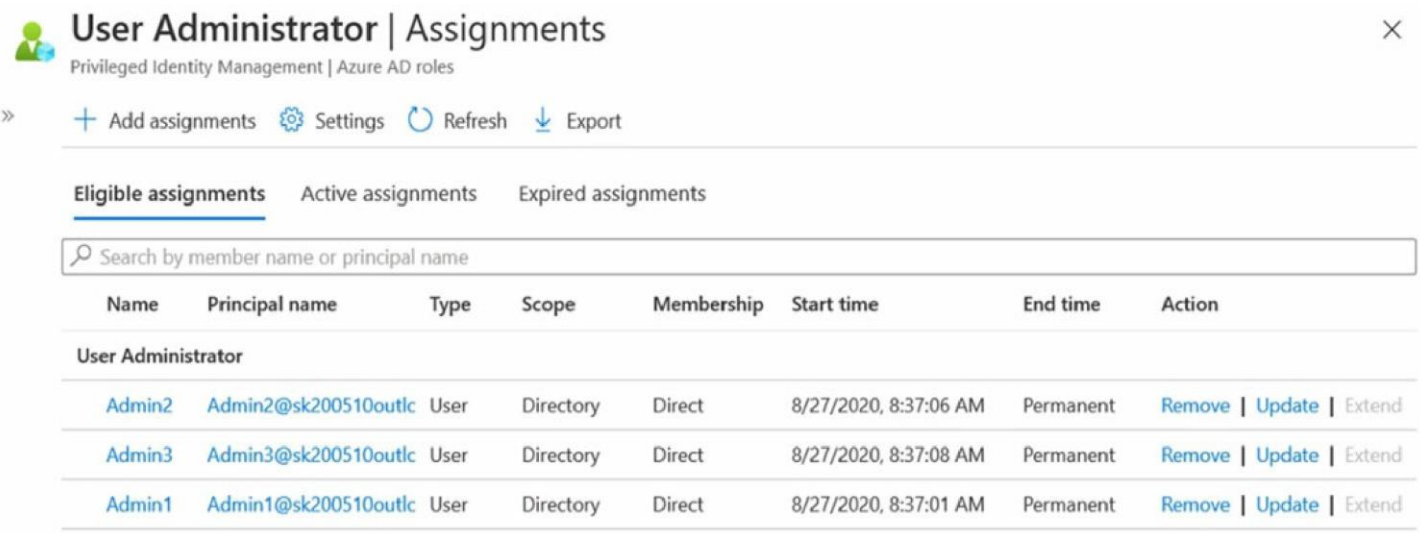
Activation

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	1 Member(s), 0 Group(

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication o...	Yes
Require justification on active assignment	Yes

The User Administrator role has the assignments shown in the Assignments exhibit. (Click the Assignments tab.)



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:

Statements	Yes	No
Before Admin1 can perform a task that requires the User Administrator role, the approver must approve the activation request.	○	○
Admin2 can request that the User Administrator role be activated for a period of two hours.	○	○
Admin3 will be prompted to authenticate by using Azure Multi-Factor Authentication (MFA) when the user signs in to the Azure Active Directory admin center, and again when the user activates the User Administrator role	○	○

Answer:

Statements	Yes	No
Before Admin1 can perform a task that requires the User Administrator role, the approver must approve the activation request.	○	○
Admin2 can request that the User Administrator role be activated for a period of two hours.	○	○
Admin3 will be prompted to authenticate by using Azure Multi-Factor Authentication (MFA) when the user signs in to the Azure Active Directory admin center, and again when the user activates the User Administrator role	○	○

Explanation:
Box 1: Yes -
In this scenario the User Administrator role is require justification on active assignment.

Require justification -
You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the
Require justification on activation box.

Box 2: Yes -
Activation maximum duration is 8 hours.

Box 3: Yes -
Require multifactor authentication
Privileged Identity Management provides enforcement of Azure AD Multi-Factor Authentication on activation

and on active assignment.

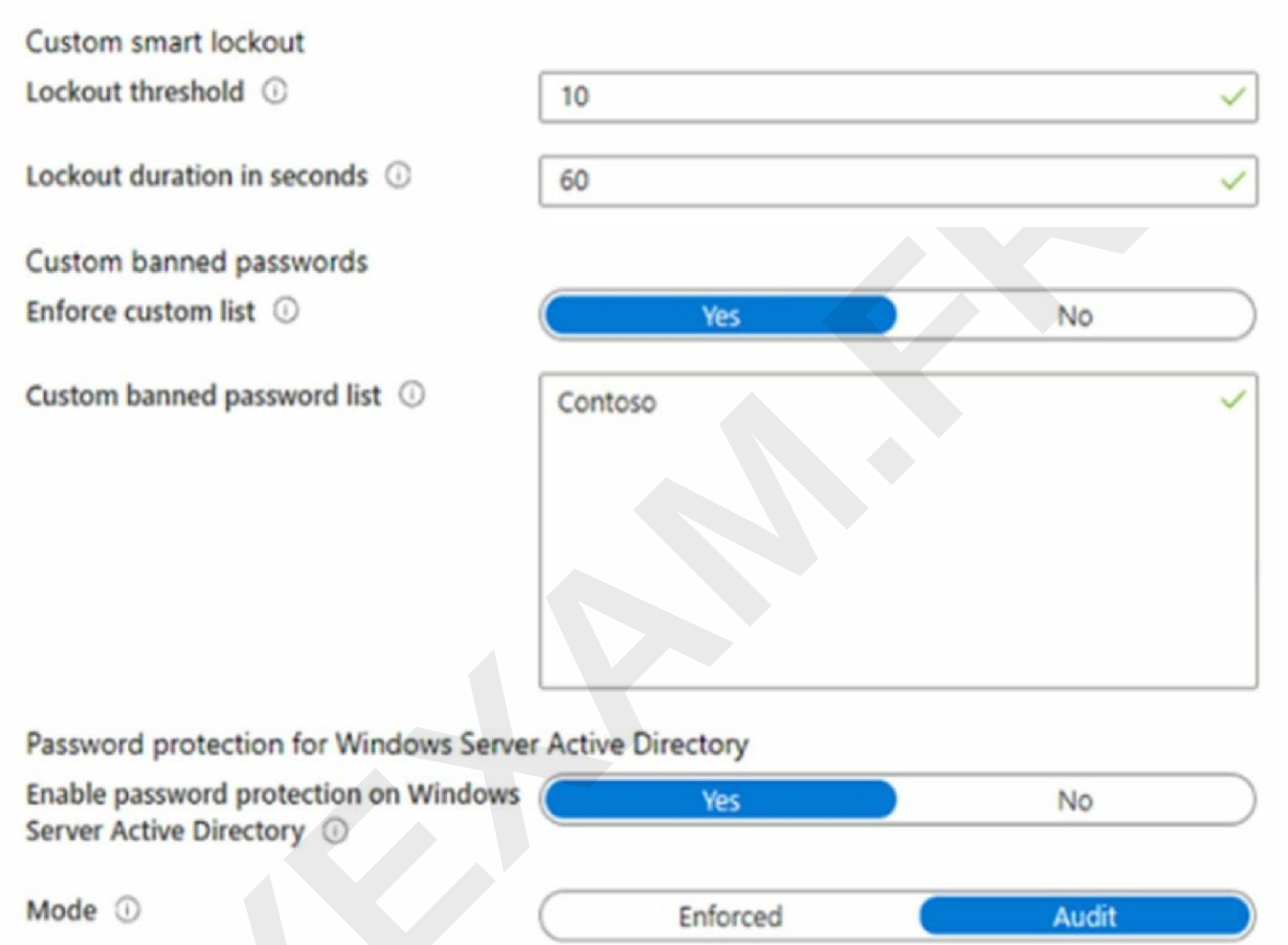
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

Question: 75

HOTSPOT -
Your company has a Microsoft 365 E5 subscription and a hybrid Azure Active Directory named contoso.com.
Contoso.com includes the following users:

Name	Password	Source
User1	CoNtOsO.Password	Azure Active Directory
User2	P1AiNPWD	Azure Active Directory
User3	MyV3rrYC0mplexPWD	Windows Server Active Directory (AD)

You configure Password protection for Contoso.com as shown in the following exhibit.



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:

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	○	○
User2 can change his password to C0NT0$0C0NT0$0.	○	○
User3 can change his password to myCONTOSOc0mp1exPWD.	○	○

Answer:

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	●	○
User2 can change his password to C0NT0$0C0NT0$0.	●	○
User3 can change his password to myCONTOSOc0mp1exPWD.	○	●

Explanation:
Box 1: Yes -
Note: The following considerations and limitations apply to the custom banned password list: The custom banned password list can contain up to 1000 terms.
The custom banned password list is case-insensitive.
The custom banned password list considers common character substitution, such as "o" and "0", or "a" and "@".
The minimum string length is four characters, and the maximum is 16 characters.

Box 2: Yes -
The $ character is OK when it used instead of an S.

Box 3: No -

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection

Question: 76

You have a Microsoft 365 E5 subscription that contains a user named User1.
You need to ensure that User1 can use the Microsoft 365 compliance center to search audit logs and identify which users were added to Microsoft 365 role groups. The solution must use the principle of least privilege.
To which role group should you add User1?

A. View-Only Organization Management
B. Security Reader
C. Organization Management
D. Compliance Management

Answer: D

Explanation:

Compliance Management. Assigned RolesAudit LogsCompliance AdminData Loss PreventionInformation Rights ManagementJournalingMessage TrackingRetention ManagementTransport RulesView-Only Audit LogsView-Only ConfigurationView-Only Recipients View-Only Organization ManagementAssigned RolesView-Only ConfigurationView-Only Recipientscorrect Answer- D

https://admin.exchange.microsoft.com/#/adminRoles click the roles and check permissions. compliance management and org management have access. but compliance management is least priveliged. not to be confused with ordinary audit logs those require reports reader.

Question: 77

HOTSPOT
-

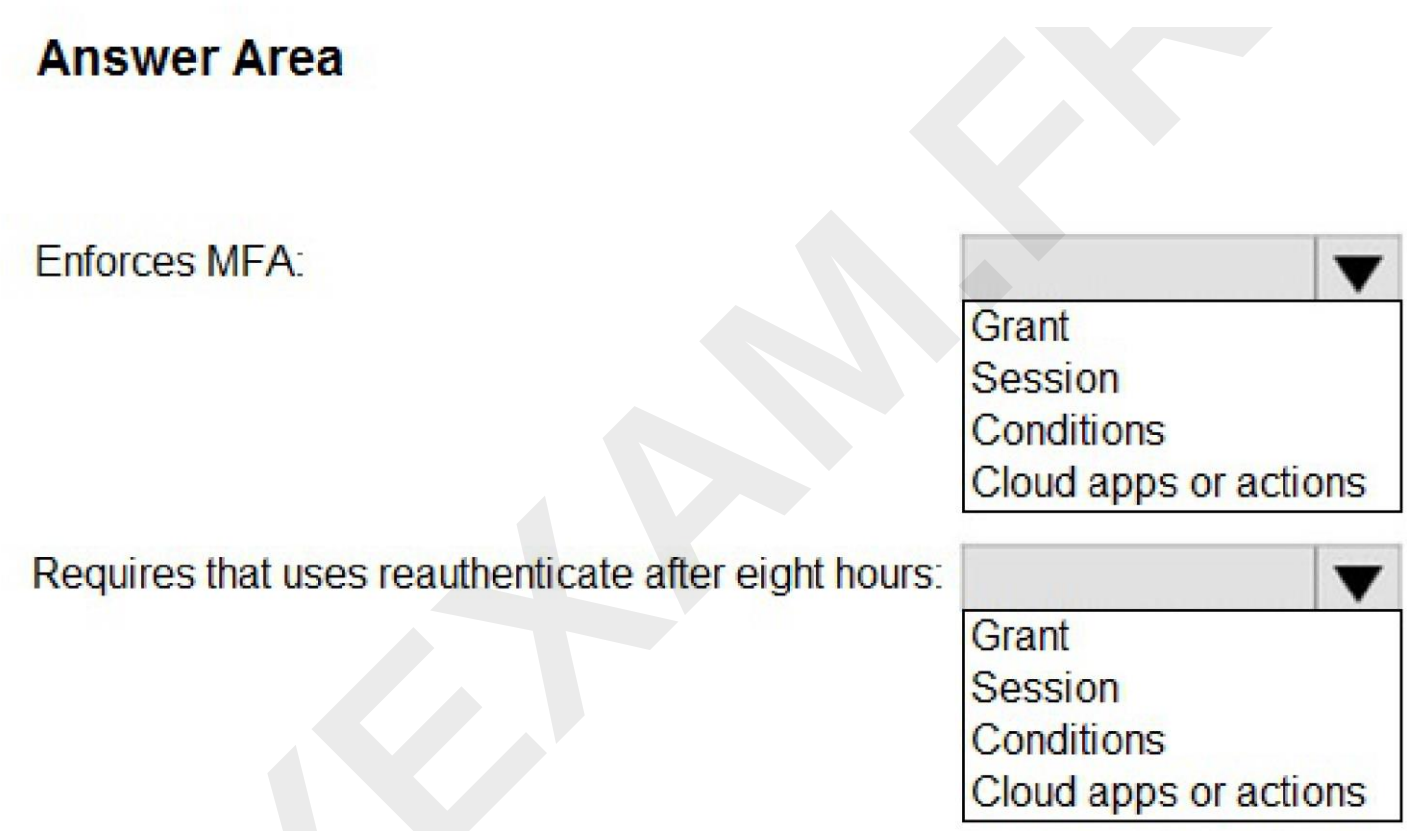
You have a Microsoft 365 E5 subscription.

You need to create a conditional access policy named Policy1 that meets the following requirements:

•Enforces multi-factor authentication (MFA)
•Requires that users reauthenticate after eight hours

Which settings should you configure in Policy1 for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area

Enforces MFA: [Grant / Session / Conditions / Cloud apps or actions]

Requires that uses reauthenticate after eight hours: [Grant / Session / Conditions / Cloud apps or actions]

Explanation:

grant

session

Question: 78 HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains three users named Use1, User2, and User3.

You have Azure Active Directory (Azure AD) roles that have the role activation settings shown in the following table.

You have Azure AD roles that have the role assignment settings shown in the following table.

Name	Require justification on activation	Require approval to activate	Approver
Role1	No	Yes	User1
Role2	Yes	No	*Not applicable*

The Azure AD roles have eligible users assigned as shown in the following table.

Name	Allow permanent eligible assignment	Allow permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

Name	Eligible assignment
Role1	User1, User2
Role2	User3

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE:
Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can approve his own Role1 assignment request.	○	○
User1 can approve the Role2 assignment request of User3.	○	○
User1 must provide a justification to approve the Role1 assignment request of User2.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can approve his own Role1 assignment request.	○	○
User1 can approve the Role2 assignment request of User3.	○	○
User1 must provide a justification to approve the Role1 assignment request of User2.	○	○

Question: 79

You have a hybrid Azure Active Directory (Azure AD) tenant that has pass-through authentication enabled. You plan to implement Azure AD Identity Protection and enable the user risk policy.
You need to configure the environment to support the user risk policy.

What should you do first?

A. Enable the sign-in risk policy.

B. Enforce the multi-factor authentication (MFA) registration policy. C. Configure a conditional access policy.

D. Enable password hash synchronization.

Answer: D

Explanation:

"For users to self-remediate risk though, they must register for Azure AD Multifactor Authentication before they become risky. For more information, see the article Plan an Azure Active Directory Multi-Factor Authentication deployment. Use the Identity Protection multifactor authentication registration policy to help get your users registered for Azure AD Multifactor Authentication before they need to use it. "So Enable MFA will be the correct answer.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/how-to-deploy-identity-protection

Question: 80

You configure several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view Defender for Office 365 reports from the Threat management dashboard.

Which role provides User1 with the required role permissions?

A. Reports reader
B. Exchange administrator
C. Security administrators
D. Compliance administrator

Answer: C

Explanation:

only Security Administrator role mentions Defender 365.