- **Vendor:** Microsoft
- **Exam Code:** SC-300
- **Exam Name:** Microsoft Identity and Access Administrator

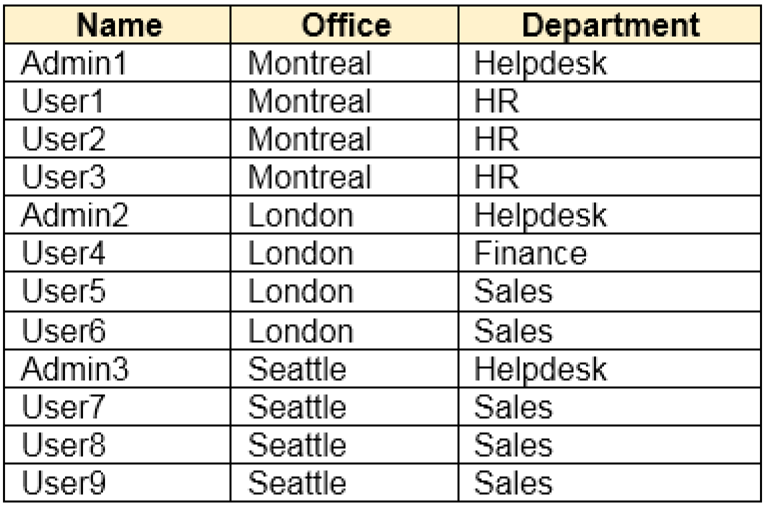
QUESTION 54
Case Study 1 - Contoso, Ltd
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

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

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



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

Existing Environment. Microsoft 365/Azure Environment

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

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

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

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

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

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

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

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to https://contoso.com/auth- response.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

You need to meet the planned changes for the User administrator role.
What should you do?

A. Create an access review.
B. Create an administrative unit.
C. Modify Active assignments.
D. Modify Role settings.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=new

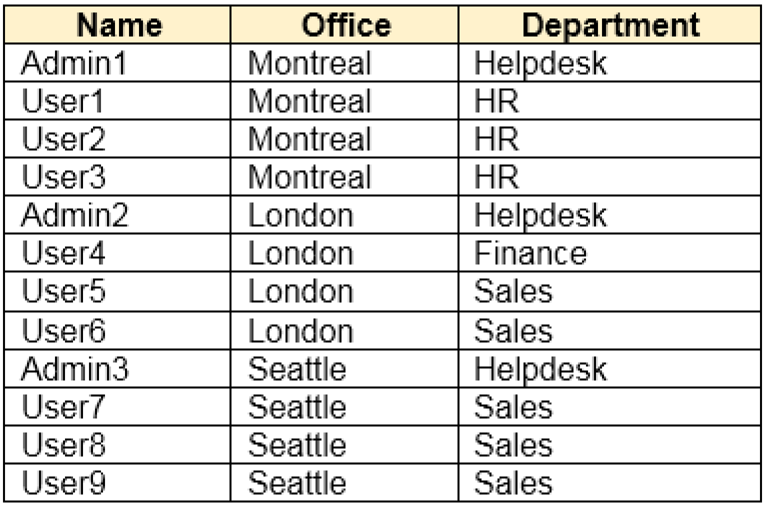
QUESTION 55
Case Study 1 - Contoso, Ltd
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

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

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



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

Existing Environment. Microsoft 365/Azure Environment

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

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

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

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

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

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

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

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

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

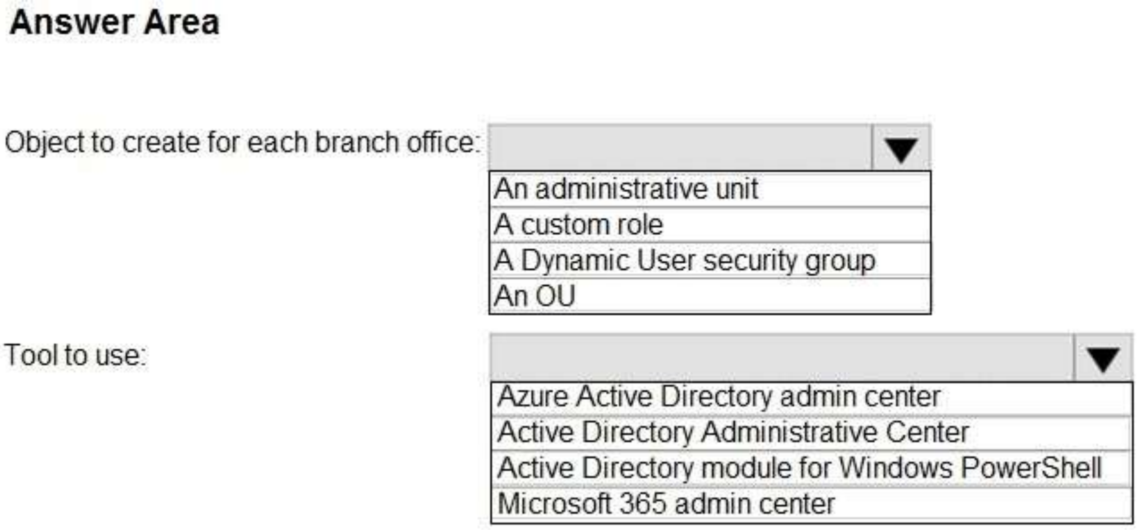
- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to https://contoso.com/auth- response.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department’s SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users’ identity was compromised.

Hotspot Question

You need to meet the technical requirements for license management by the helpdesk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

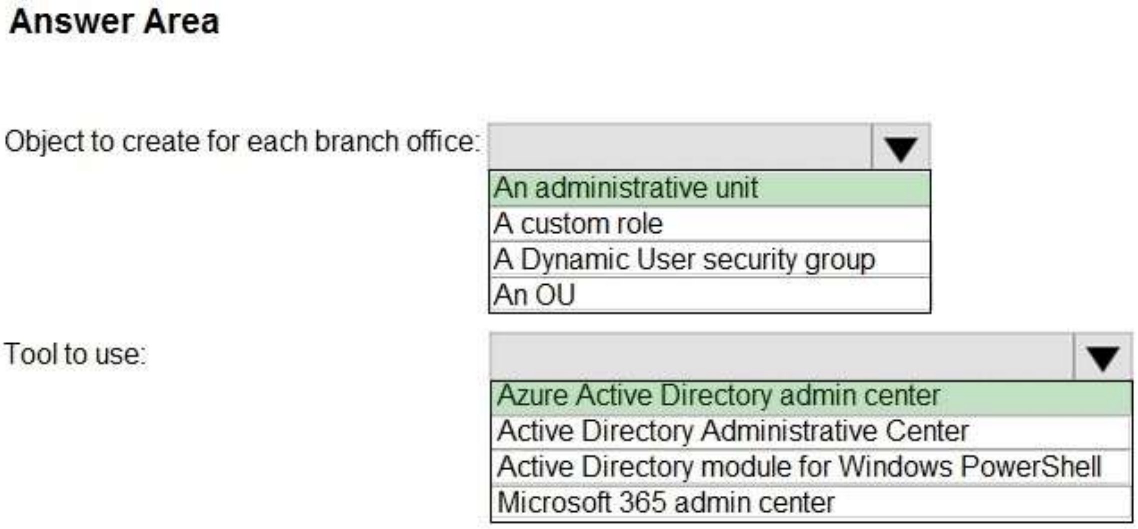


Answer Area

Object to create for each branch office: ▼
- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use: ▼
- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Answer:



Answer Area

Object to create for each branch office: ▼
- [✓ An administrative unit]
- A custom role
- A Dynamic User security group
- An OU

Tool to use: ▼
- [✓ Azure Active Directory admin center]
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units
https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-manage

QUESTION 56

Case Study 2 - Litware, Inc

Overview

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

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

Existing Environment. Identify Environment

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

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

Litware implements Azure AD Application Proxy.

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

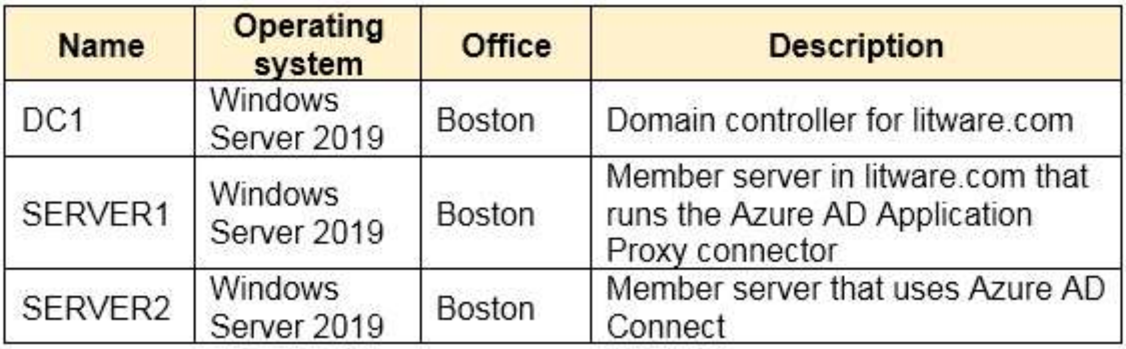
Existing Environment. Cloud Environment

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

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

Existing Environment. On-premises Environment

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



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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

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

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.

- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

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

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.

What should you include in the configuration?

A. named locations that have a private IP address range
B. named locations that have a public IP address range
C. trusted IPs that have a public IP address range
D. trusted IPs that have a private IP address range

Answer: B

Explanation:

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

QUESTION 57

Case Study 2 - Litware, Inc

Overview

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

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

Existing Environment. Identify Environment

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

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

Litware implements Azure AD Application Proxy.

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

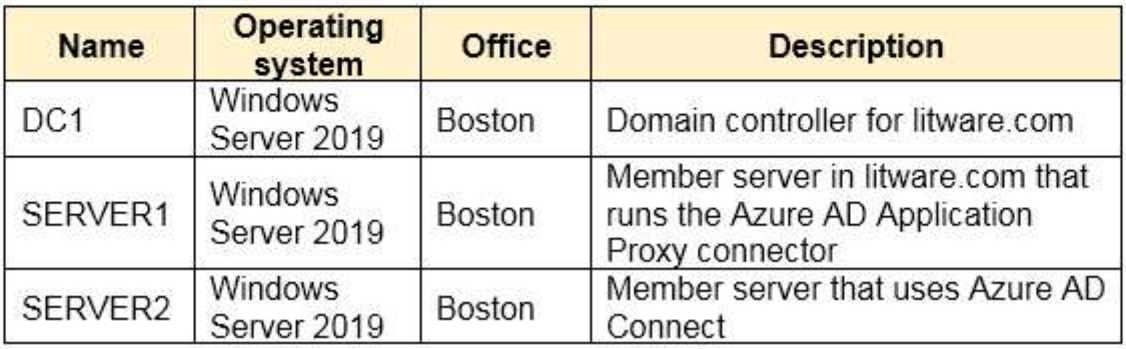
Existing Environment. Cloud Environment

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

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

Existing Environment. On-premises Environment

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



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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

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

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

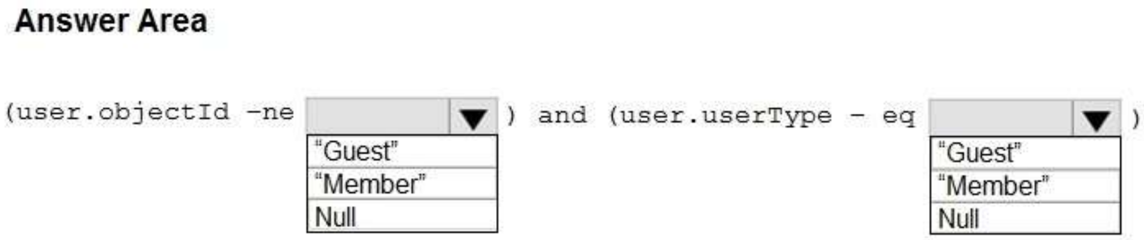
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Hotspot Question

You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

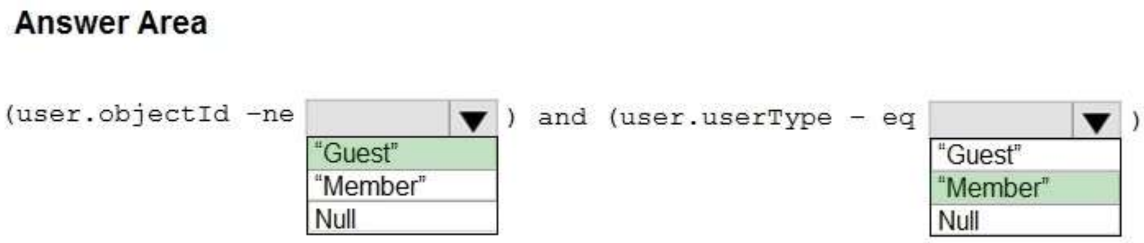
NOTE: Each correct selection is worth one point.



Answer Area

(user.objectId -ne [▼ "Guest" / "Member" / Null]) and (user.userType – eq [▼ "Guest" / "Member" / Null])

Answer:



Answer Area

(user.objectId -ne [✓ "Guest"] / "Member" / Null) and (user.userType – eq "Guest" / [✓ "Member"] / Null)

QUESTION 58

Case Study 2 - Litware, Inc

Overview

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

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

Existing Environment. Identify Environment

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

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

Litware implements Azure AD Application Proxy.

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

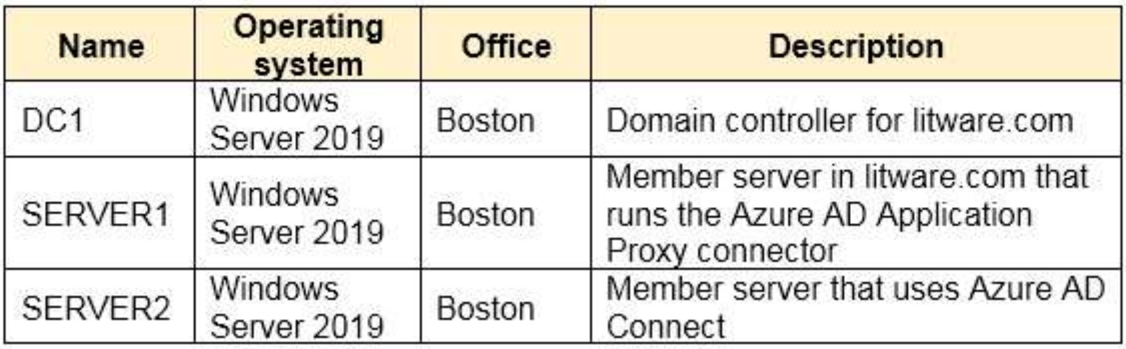
Existing Environment. Cloud Environment

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

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

Existing Environment. On-premises Environment

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



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

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

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

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

Requirements. Management Requirements

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

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

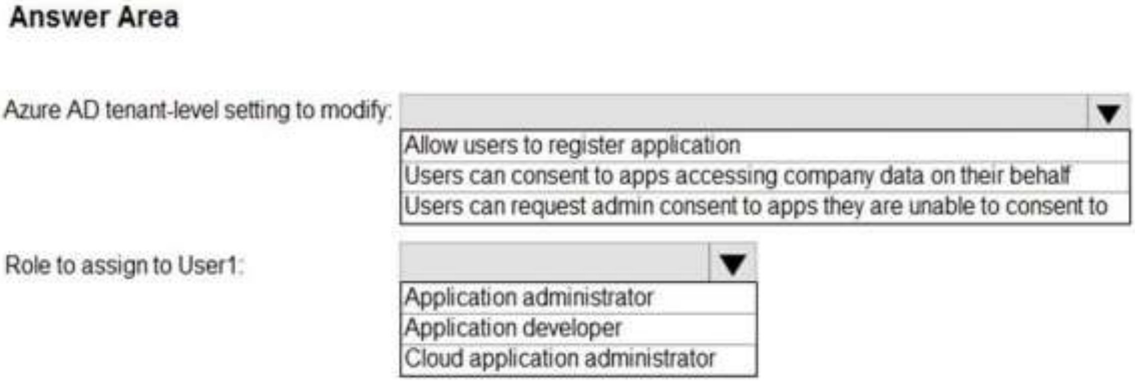
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Hotspot Question

You need to configure app registration in Azure AD to meet the delegation requirements.

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

NOTE: Each correct selection is worth one point.

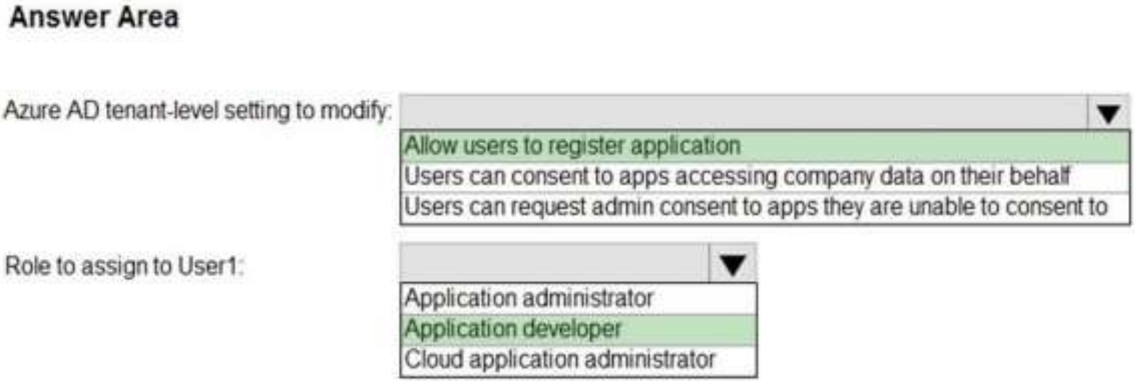


Answer Area

Azure AD tenant-level setting to modify:
- Allow users to register application
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:
- Application administrator
- Application developer
- Cloud application administrator

Answer:



Answer Area

Azure AD tenant-level setting to modify:
- [✓ Allow users to register application]
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:
- Application administrator
- [✓ Application developer]
- Cloud application administrator

Explanation:

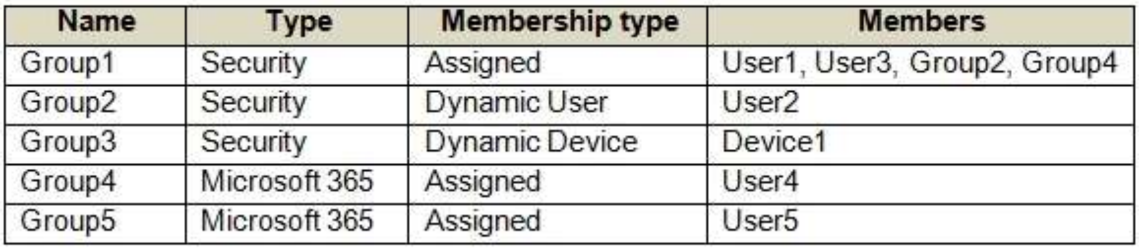
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

QUESTION 59

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

```
- A device named Devie1
- Users named User1, User2, User3, User4, and User5
- Five groups named Group1, Group2, Group3, Group4, and Group5
```

The groups are configured as shown in the following table.



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

How many licenses are used if you assign the Microsoft 365 Enterprise E5 license to Group1?

A. 0
B. 2
C. 3
D. 4

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

QUESTION 60
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.
A contractor uses the credentials of user1@outlook.com.
You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.
What should you do?

A. Run the New-AzADUser cmdlet.
B. Configure the External collaboration settings.
C. Add a WS-Fed identity provider.
D. Create a guest user account in contoso.com.

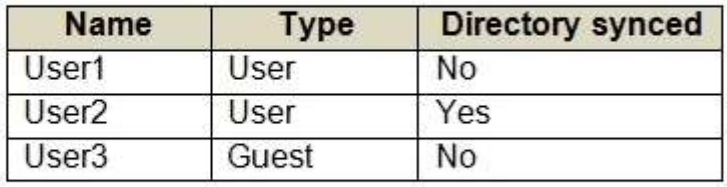
Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

QUESTION 61
Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.
You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync.
What should you do in Azure AD Connect?

A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
B. Configure a Full Import run profile.
C. Create an inbound synchronization rule for the Active Directory Domain Services connector.
D. Configure an Export run profile.

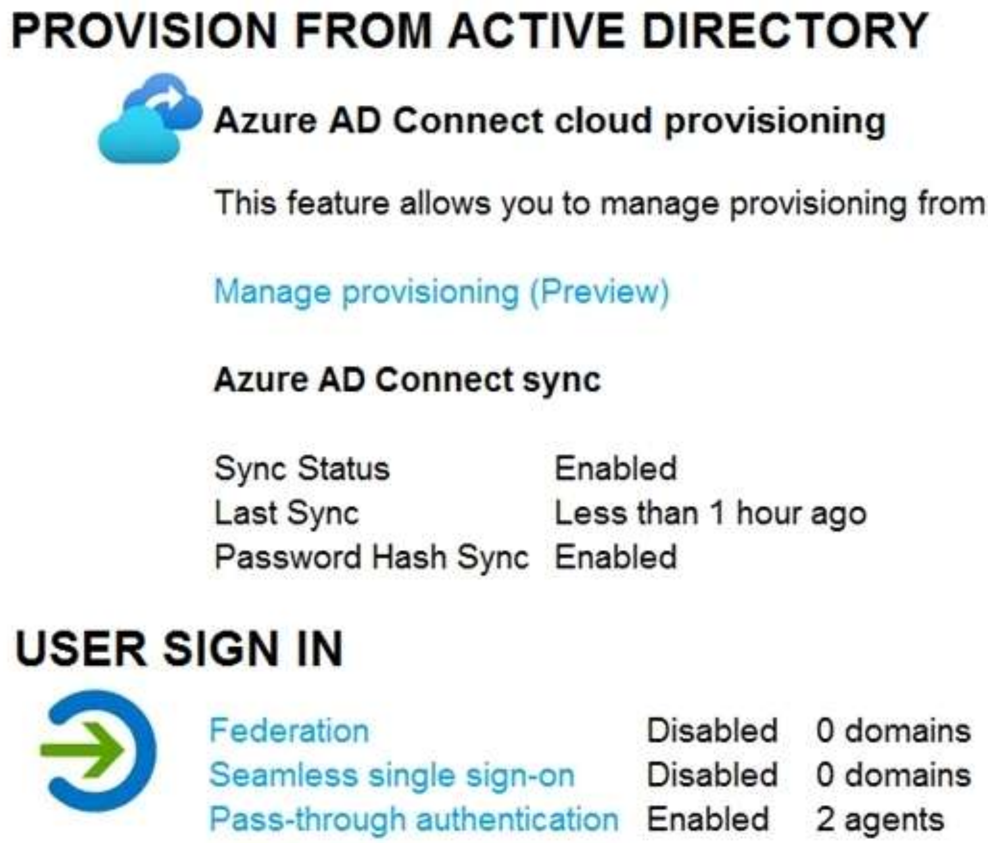
Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

QUESTION 62
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.
Azure AD Connect is configured in Azure AD as shown in the following exhibit.



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

Connectivity from the on-premises domain to the internet is lost.
Which users can sign in to Azure AD?

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

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations

QUESTION 63
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 Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.
You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.
You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.
Solution: You configure Azure AD Password Protection.
Does this meet the goal?

A. Yes
B. No

Answer: B

QUESTION 64
You have an Azure Active Directory (Azure AD) tenant.
For the tenant, Users can register applications is set to No.
A user named Admin1 must deploy a new cloud app named App1.
You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role should you assign to Admin1?

A. Managed Application Contributor for Subscription1.
B. Application developer in Azure AD.
C. Cloud application administrator in Azure AD.
D. App Configuration Data Owner for Subscription1.

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

QUESTION 65
You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection enabled.
You need to implement a sign-in risk remediation policy without blocking user access.
What should you do first?

A. Configure access reviews in Azure AD.
B. Enforce Azure AD Password Protection.
C. Configure self-service password reset (SSPR) for all users.
D. Implement multi-factor authentication (MFA) for all users.

Answer: D
Explanation:
MFA and SSPR are both required. However, MFA is required first.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

QUESTION 66
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc. Fabrikam uses a domain named fabrikam.com.
Fabrikam users must be removed automatically from the tenant when access is no longer required.
You need to configure the following settings:

```
- Block external user from signing in to this directory: No
- Remove external user: Yes
- Number of days before removing external user from this directory: 90
```

What should you configure on the Identity Governance blade?

A. Access packages
B. Settings
C. Terms of use
D. Access reviews

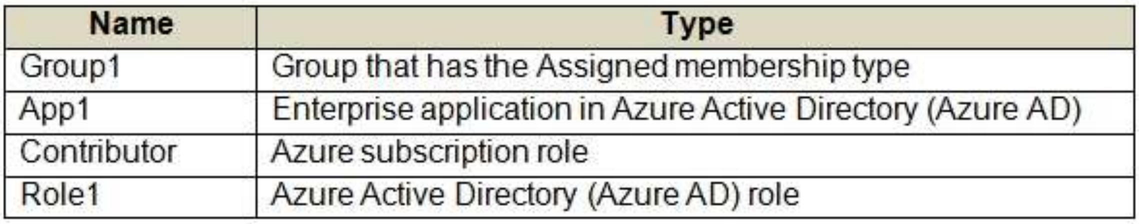
Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

QUESTION 67
You have an Azure Active Directory (Azure AD) tenant.
You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the past.
For how long does Azure AD store events in the sign-in logs?

A. 14 days
B. 30 days
C. 90 days
D. 365 days

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention#how-long-does-azure-ad-store-the-data

QUESTION 68
You have an Azure subscription that contains the resources shown in the following table.



Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

For which resources can you create an access review?

A. Group1, Role1, and Contributor only
B. Group1 only
C. Group1, App1, Contributor, and Role1
D. Role1 and Contributor only

Answer: C
Explanation:
Access reviews require an Azure AD Premium P2 license.
Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.
Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/toc.json
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

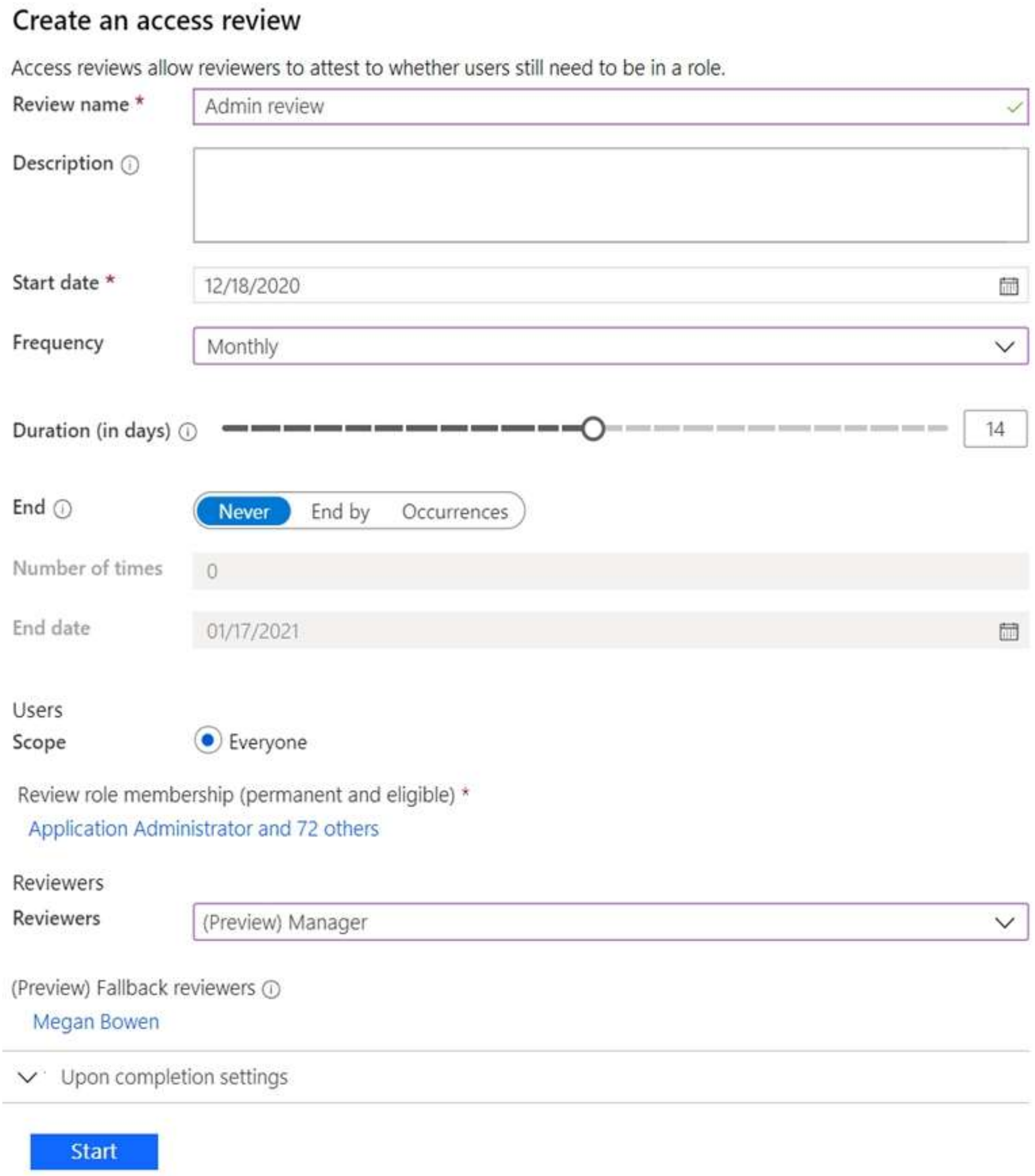
QUESTION 69
You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.
You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.
You need to download the Azure AD log by using the administrative portal. The log file must contain changes to conditional access policies.
What should you export from Azure AD?

A. audit logs in CSV format
B. sign-ins in CSV format
C. audit logs in JSON format
D. sign-ins in JSON format

Answer: C
Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

QUESTION 70
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
You have 100 IT administrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click the Exhibit tab.)



Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Admin review

Description

Start date * 12/18/2020

Frequency Monthly

Duration (in days) 14

End ● Never ○ End by ○ Occurrences

Number of times 0

End date 01/17/2021

Users

Scope ● Everyone

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

Reviewers

Reviewers (Preview) Manager

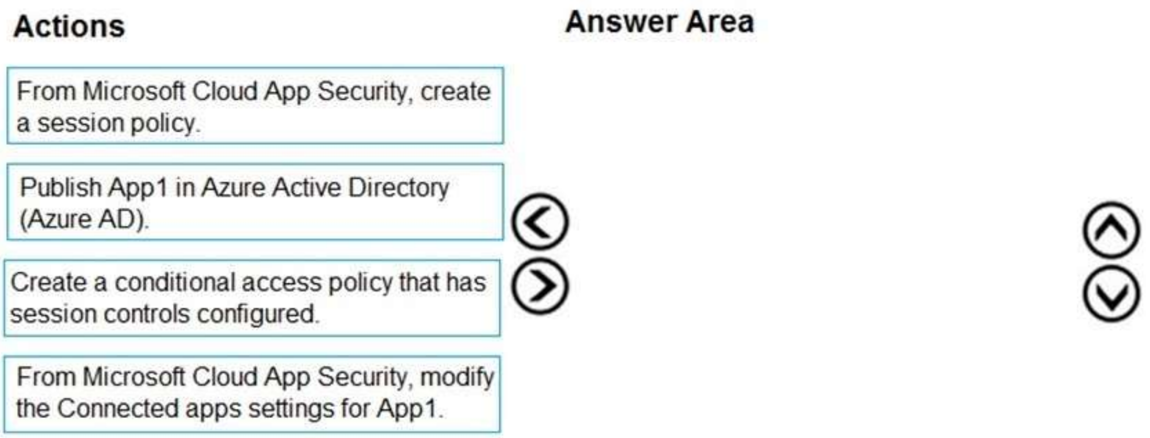
(Preview) Fallback reviewers
Megan Bowen

You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You add each manager as a fallback reviewer.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

QUESTION 71
Drag and Drop Question
You have a Microsoft 365 E5 tenant.
You purchase a cloud app named App1.
You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud App Security.
In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

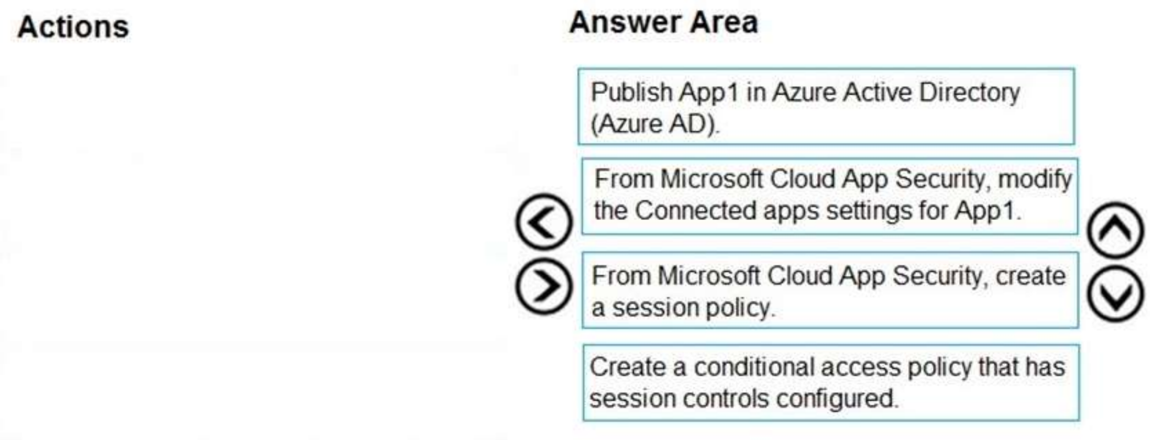


Actions

- From Microsoft Cloud App Security, create a session policy.
- Publish App1 in Azure Active Directory (Azure AD).
- Create a conditional access policy that has session controls configured.
- From Microsoft Cloud App Security, modify the Connected apps settings for App1.

Answer Area

Answer:



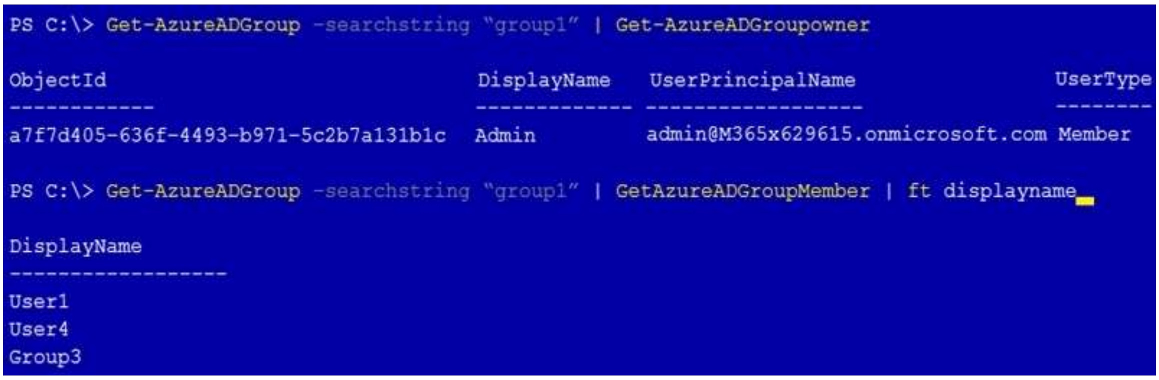
Actions

Answer Area

- Publish App1 in Azure Active Directory (Azure AD).
- From Microsoft Cloud App Security, modify the Connected apps settings for App1.
- From Microsoft Cloud App Security, create a session policy.
- Create a conditional access policy that has session controls configured.

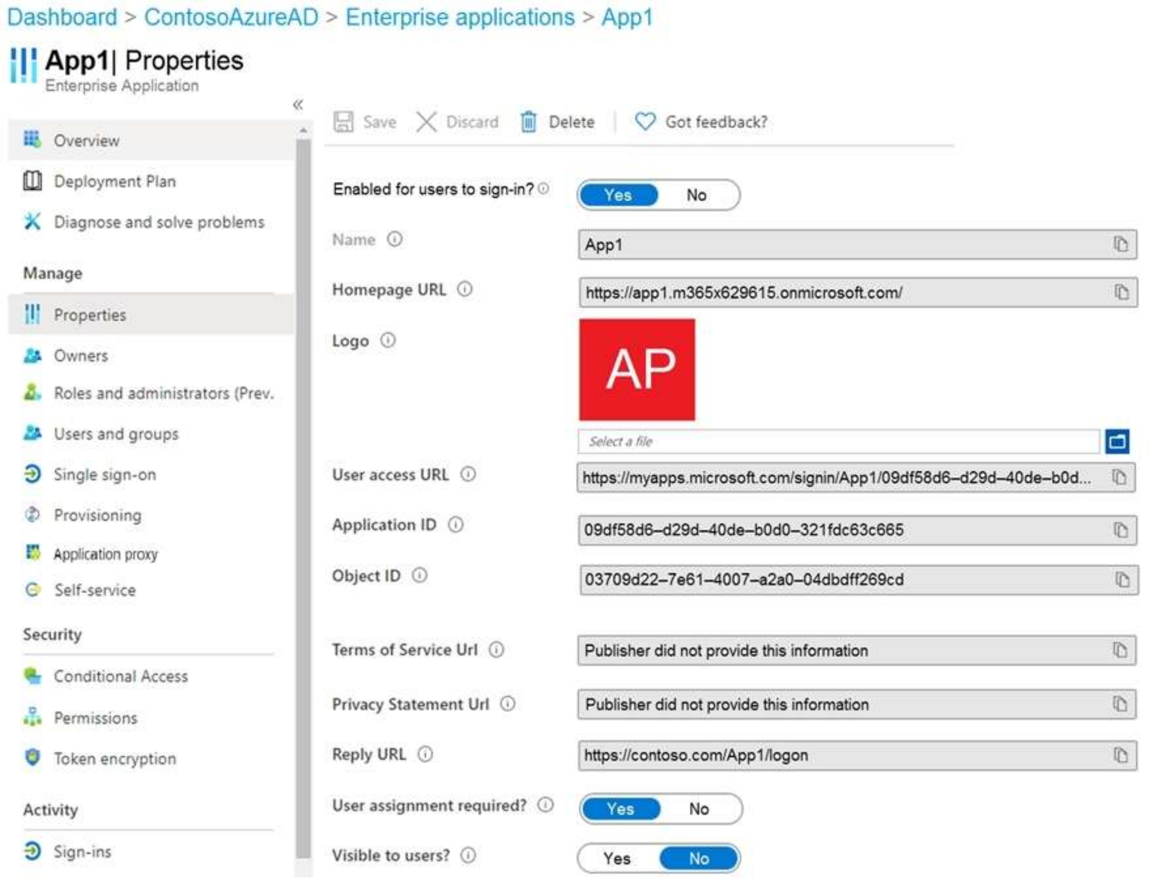
Explanation:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app
https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

QUESTION 72
Hotspot Question
You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit.
(Click the Group1 tab.)



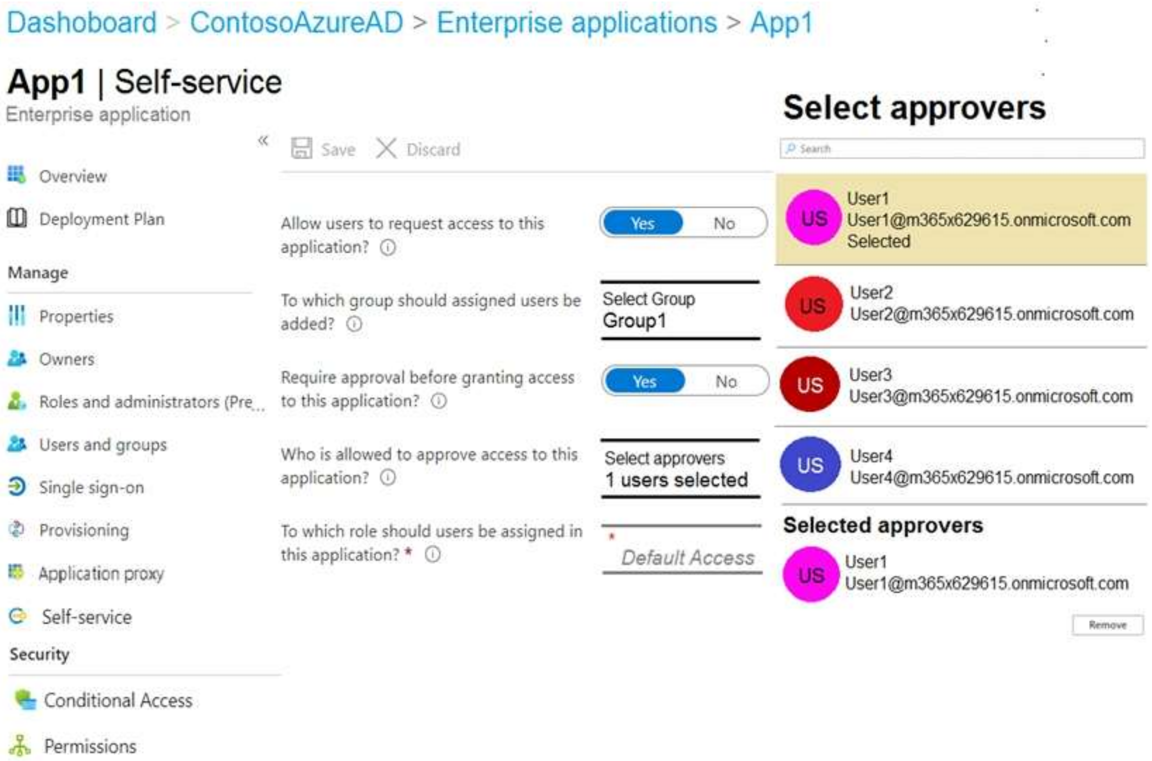
```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

ObjectId                             DisplayName  UserPrincipalName              UserType
------------                         ------------ ------------------             --------
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin        admin@M365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -searchstring "group1" | GetAzureADGroupMember | ft displayname_

DisplayName
-----------------
User1
User4
Group3
```

You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click the App1 Properties tab.)



Enabled for users to sign-in?	[✓ Yes] No
Name	App1
Homepage URL	https://app1.m365x629615.onmicrosoft.com/
Logo	AP
User access URL	https://myapps.microsoft.com/signin/App1/09df58d6–d29d–40de–b0d...
Application ID	09df58d6–d29d–40de–b0d0–321fdc63c665
Object ID	03709d22–7e61–4007–a2a0–04dbdff269cd
Terms of Service Url	Publisher did not provide this information
Privacy Statement Url	Publisher did not provide this information
Reply URL	https://contoso.com/App1/logon
User assignment required?	[✓ Yes] No
Visible to users?	Yes [✓ No]

You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click the App1 Self-service tab.)



Dashoboard > ContosoAzureAD > Enterprise applications > App1

App1 | Self-service
Enterprise application

Allow users to request access to this application? ⓘ — Yes ● No

To which group should assigned users be added? ⓘ — Select Group: Group1

Require approval before granting access to this application? ⓘ — Yes ● No

Who is allowed to approve access to this application? ⓘ — Select approvers: 1 users selected

To which role should users be assigned in this application? * ⓘ — * Default Access

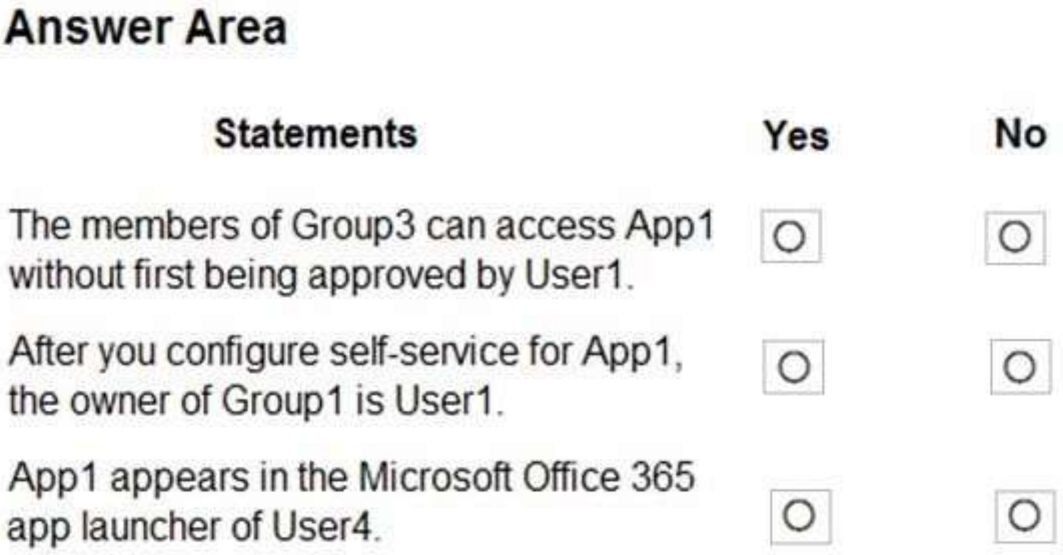
Select approvers

US	User1 User1@m365x629615.onmicrosoft.com Selected
US	User2 User2@m365x629615.onmicrosoft.com
US	User3 User3@m365x629615.onmicrosoft.com
US	User4 User4@m365x629615.onmicrosoft.com

Selected approvers

US User1
User1@m365x629615.onmicrosoft.com

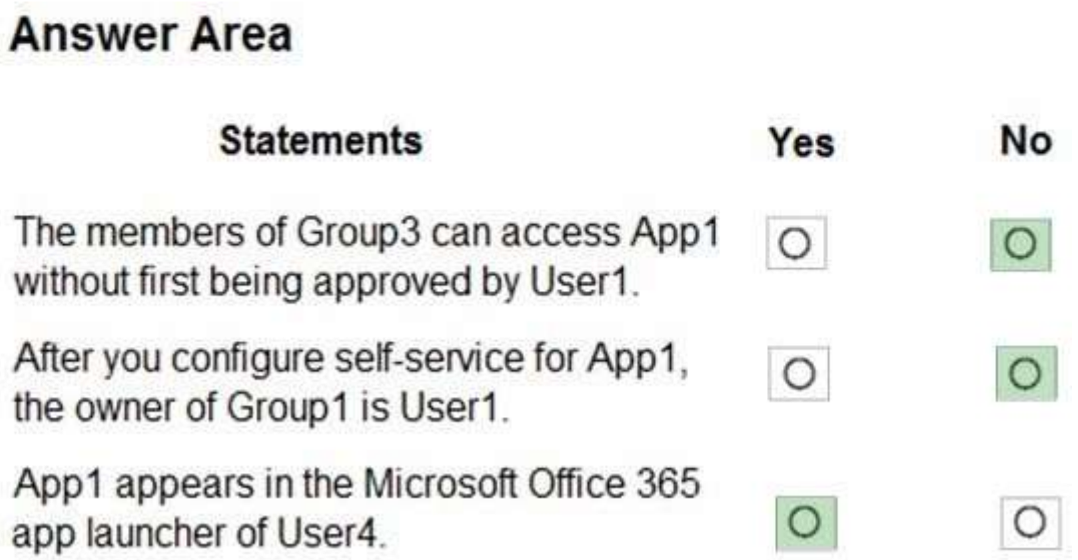
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Answer:



Answer Area

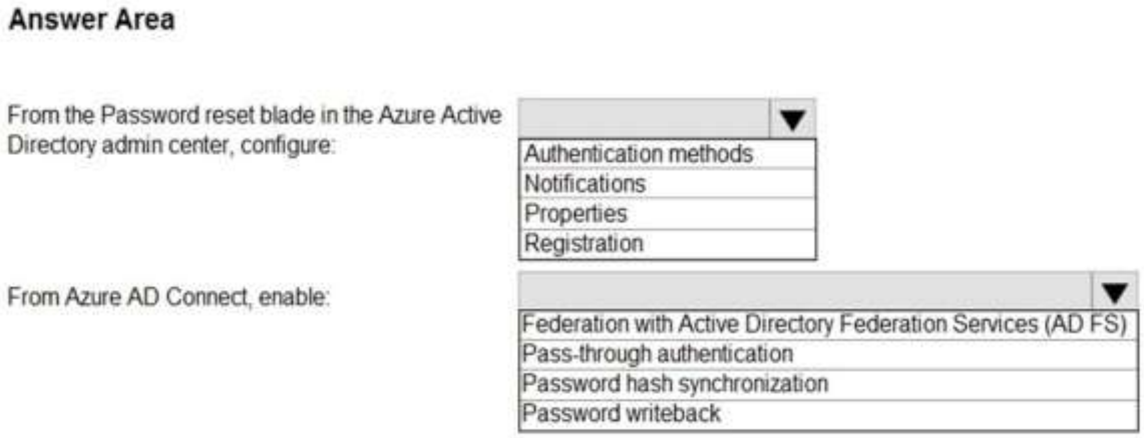
Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	●
After you configure self-service for App1, the owner of Group1 is User1.	○	●
App1 appears in the Microsoft Office 365 app launcher of User4.	●	○

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users

QUESTION 73
Hotspot Question
You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.
You deploy Azure AD Connect by using the Express Settings.
You need to configure self-service password reset (SSPR) to meet the following requirements:

```
- When users reset their password, they must be prompted to respond to a mobile app
notification or answer three predefined security questions.
- Passwords must be synced between the tenant and the domain regardless of where the
password was reset.
```

What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

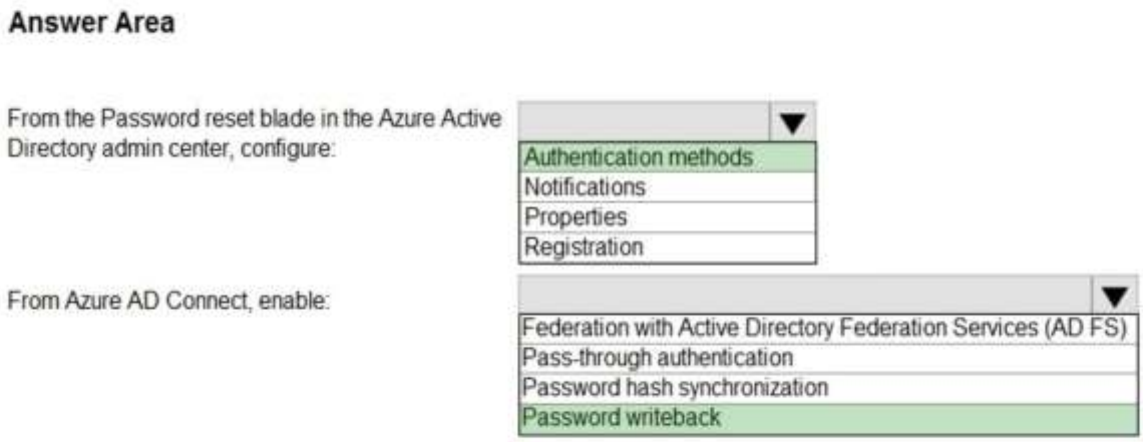
From the Password reset blade in the Azure Active Directory admin center, configure:

- Authentication methods
- Notifications
- Properties
- Registration

From Azure AD Connect, enable:

- Federation with Active Directory Federation Services (AD FS)
- Pass-through authentication
- Password hash synchronization
- Password writeback

Answer:



Answer Area

From the Password reset blade in the Azure Active Directory admin center, configure:

- [✓ Authentication methods]
- Notifications
- Properties
- Registration

From Azure AD Connect, enable:

- Federation with Active Directory Federation Services (AD FS)
- Pass-through authentication
- Password hash synchronization
- [✓ Password writeback]

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions