MS-102 Microsoft 365 Administrator

Question #1 *Topic 1*

Overview -
Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.
Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -
The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.
All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.
Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.
You are evaluating the required processes for Project1.
You need to recommend which DNS record must be created while adding a domain name for the project.
Which DNS record should you recommend?

A. host (A)

B. host information (HINFO)

C. text (TXT)

D. pointer (PTR)

Correct Answer: *C*

Community vote distribution

C (100%)

Casticod 2 weeks, 5 days ago

Selected Answer: C

Its the first Step, C Correct

upvoted 2 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

Selected Answer: C

Before you start you have to verify your custom domain with a TXT record.

https://learn.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide

upvoted 3 times

Question #2 *Topic 1*

Overview -
Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.
Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -
The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.
All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.
Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.
You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication

B. pass-through authentication and seamless SSO

C. password hash synchronization and seamless SSO

D. password hash synchronization

Correct Answer: *C*

Community vote distribution

C (100%)

osxzvkwpfcfxobqjby Highly Voted 3 weeks, 4 days ago

Selected Answer: C

"Users must be able to authenticate to cloud services if Active Directory becomes unavailable." That would be hash sync. Pass-though with failback is also possible but more work to implement and maintain.

"After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically." that's the SSO.

upvoted 6 times

letters1234 Most Recent 6 days, 3 hours ago

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn

upvoted 1 times

Greatone1 1 week, 3 days ago

Selected Answer: C

C is the correct answer
https://www.examtopics.com/discussions/microsoft/view/11890-exam-ms-100-topic-15-question-3-discussion/

upvoted 1 times

Overview -
Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.
Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -
The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.
All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.
Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.

Requirements -

Planned Changes -
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.
Which role should you assign to User1?

A. Hygiene Management

B. Security Reader

C. Security Administrator

D. Records Management

Correct Answer: *B*

Community vote distribution

B (100%)

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

Selected Answer: B

https://learn.microsoft.com/en-us/purview/microsoft-365-compliance-center-permissions

upvoted 2 times

HOTSPOT -

Overview -
Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.
Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment -

Active Directory Environment -
The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.
All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.
Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.

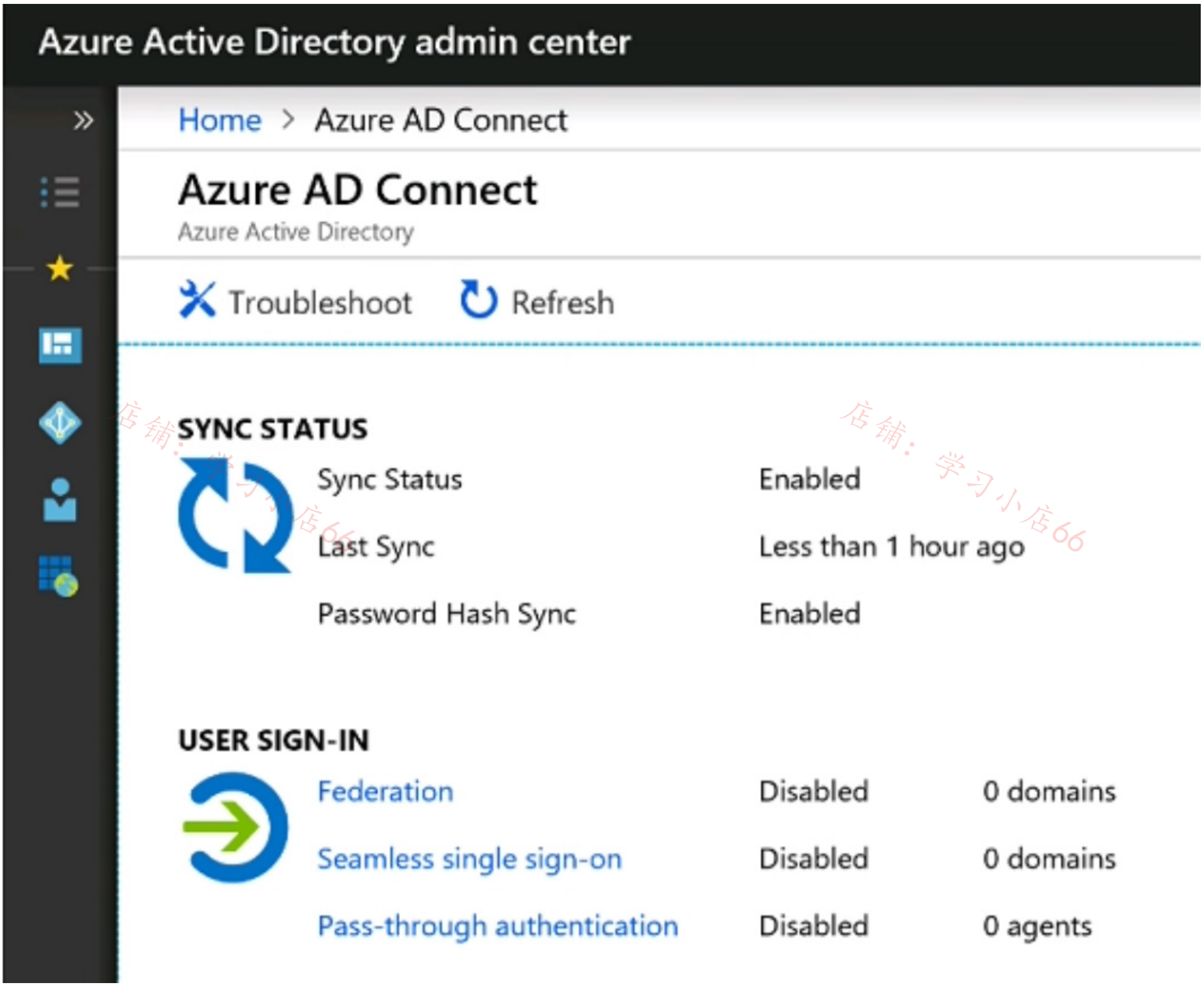
Requirements -

Planned Changes -
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

Technical Requirements -
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.

Application Requirements -
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.
You create the Microsoft 365 tenant.
You implement 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.

Answer Area

During Project1, sales department users can access **[answer choice]** applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources **[answer choice]**.

- both on-premises and in the cloud
- in the cloud only
- on-premises only

Answer Area

During Project1, sales department users can access **[answer choice]** applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

Correct Answer:

If Active Directory becomes unavailable during Project1, sales department users can access the resources **[answer choice]**.

- both on-premises and in the cloud
- in the cloud only
- on-premises only

gomezmax 6 days, 22 hours ago

Correct

upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

only on-prem: no sso configured in ADConnect

in the cloud only: AD is not available, assuming that the on-prem app use AD to authenticate users. Exchange online is still usable because of pass hash sync.

upvoted 4 times

Question #5 *Topic 1*

Your company has a Microsoft 365 subscription.

You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group used to assign the license.

What should you use?

A. Active users in the Microsoft 365 admin center

B. Reports in Microsoft Purview compliance portal

C. the Licenses blade in the Microsoft Entra admin center

D. Reports in the Microsoft 365 admin center

Correct Answer: *D*

Community vote distribution

C (100%)

osxzvkwpfcfxobqjby Highly Voted 3 weeks, 4 days ago

Selected Answer: C

There is no license report in "Reports in the Microsoft 365 admin center".

https://entra.microsoft.com > Billing > Licenses > All Products > Open License > Licensed groups

upvoted 7 times

ATHOOS Most Recent 2 days, 23 hours ago

Selected Answer: C

Correct Answer is C

upvoted 1 times

gomezmax 1 week, 3 days ago

D is wrong Answer, the Answer should be Is C

upvoted 2 times

Greatone1 1 week, 5 days ago

Selected Answer: C

C is correct

In the Azure AD Admin Center, select Azure Active Directory then select Licenses to open the Licenses blade. From there you need to click on the 'Managed your purchased licenses link'. Select a license you want to view,

upvoted 2 times

Dtriminio 3 weeks, 2 days ago

Selected Answer: C

C is correct

upvoted 2 times

Question #6 *Topic 1*

HOTSPOT -

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

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.

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

NOTE: Each correct selection is worth one point.

Answer Area

(user.userType [▼]) and (user.department [▼])

-eq "Guest"
-in "Guest"
-ne "Guest"
-notmatch "Member"

-contains "Support"
-in "Support"
-match "Support"
-startsWith "Sup"

Correct Answer:

Answer Area

(user.userType [-eq "Guest" ▼]) and (user.department [-contains "Support" ▼])

-eq "Guest"
-in "Guest"
-ne "Guest"
-notmatch "Member"

-contains "Support"
-in "Support"
-match "Support"
-startsWith "Sup"

nenge 4 days, 18 hours ago

This can be tricky if you're used to PowerShell syntax. In PS syntax, "-contains" would be incorrect as it checks for an item in a collection, not partial matches. In dynamic group syntax, it's the opposite. In dynamic group syntax, "-contains" matches partial strings, not items in collections.

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#supported-expression-operators

upvoted 1 times

Perycles 3 weeks, 3 days ago

Correct answers
(user.department -contains "Support") and (user.userType -eq "Guest")
Be carrefull : Case Sensitive

upvoted 2 times

HOTSPOT -

Your company uses a legacy on-premises LDAP directory that contains 100 users.

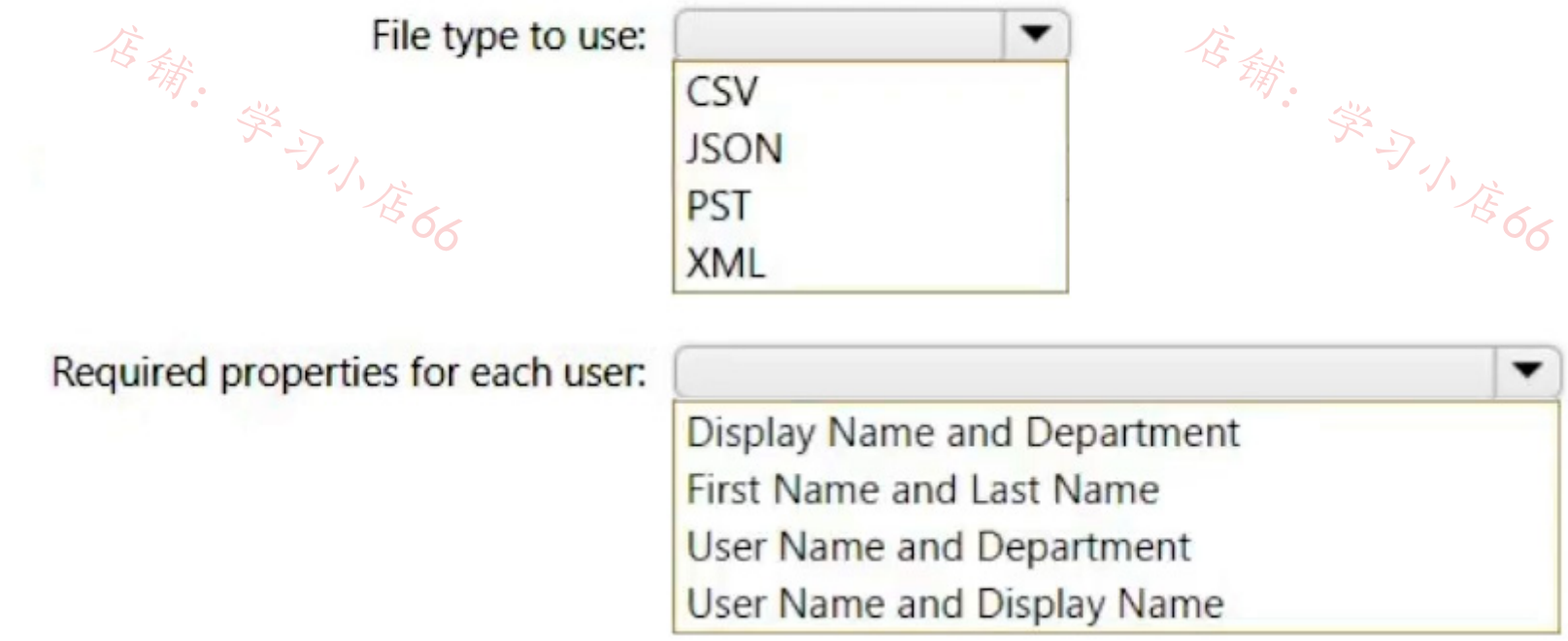
The company purchases a Microsoft 365 subscription.

You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.

Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.

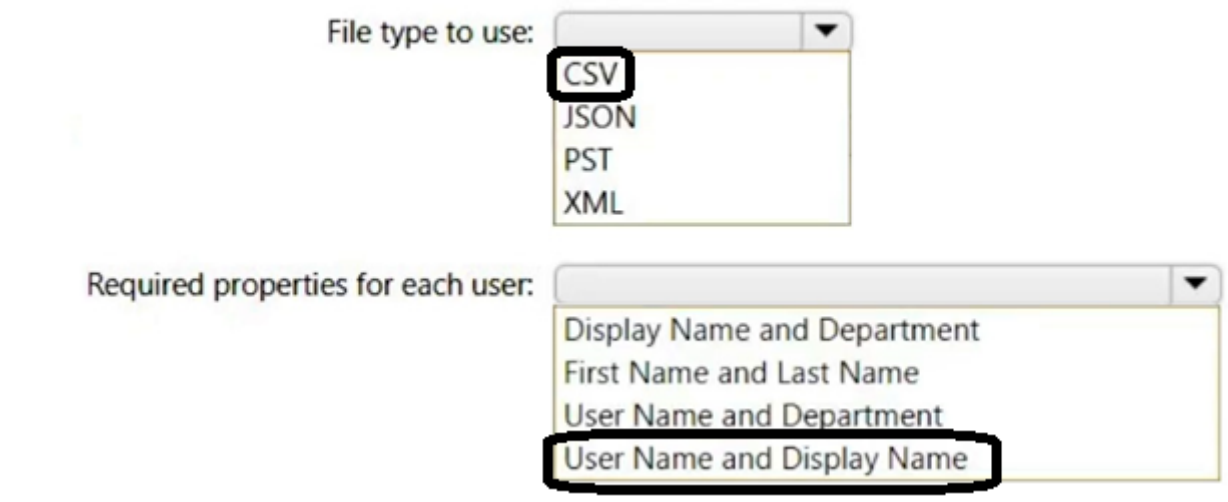
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Perycles Highly Voted 3 weeks, 4 days ago

CSV file type
"displayName" and "User Name" are mandatory

ref: https://learn.microsoft.com/fr-fr/training/modules/manage-accounts-licenses-microsoft-365/7-perform-bulk-user-maintenance

upvoted 5 times

Question #8 *Topic 1*

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

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:

To all users, deploy an Office 365 E3 license without the Power Automate license option.

To all users, deploy an Enterprise Mobility + Security E5 license.

To the users in the research department only, deploy a Power BI Pro license.

To the users in the marketing department only, deploy a Visio Plan 2 license.

What is the minimum number of deployment groups required?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: *C*

Community vote distribution

C (100%)

Perycles Highly Voted 3 weeks, 4 days ago

3 groups needed :

- Group 1 : Allusers (deploy EMS+S E5 licence and O365 E3 licence with "PowerAutomate for Office 365" disabled.

- group 2 : "Research group" : deploy Power Bi Pro Licence (not included in O365 E3 but in O365 E5).

- Group 3 : "Marketing group" deploy Visio plan 2 Licence.

upvoted 7 times

letters1234 Most Recent 6 days, 3 hours ago

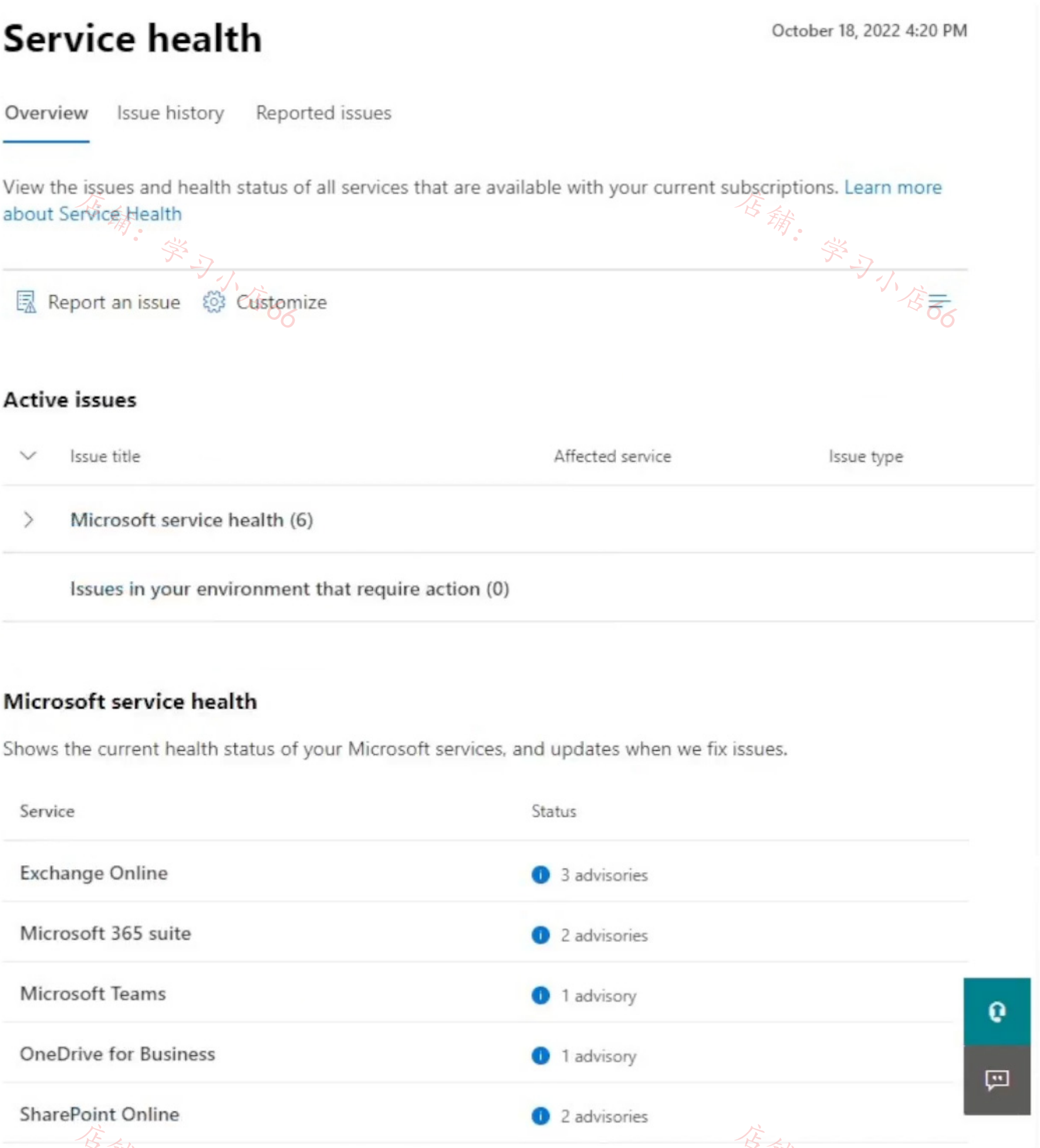
Selected Answer: C

All users and the two deparments, three groups

upvoted 1 times

You have a Microsoft 365 subscription.

You view the Service health Overview as shown in the following exhibit.



You need to ensure that a user named User1 can view the advisories to investigate service health issues.

Which role should you assign to User1?

A. Message Center Reader

B. Reports Reader

C. Service Support Administrator

D. Compliance Administrator

Correct Answer: *C*

Community vote distribution

C (100%)

rfree 2 days, 18 hours ago

https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide
People who are assigned the global admin or service support admin role can view service health.

upvoted 1 times

stai 5 days, 23 hours ago

Answer A is correct.
Message Center Reader
「Users in this role can monitor notifications and advisory health updates in Message center for their organization on configured services such as Exchange, Intune, and Microsoft Teams.」
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

upvoted 1 times

Casticod 5 days, 16 hours ago

Message center it´s not the same of service health

upvoted 1 times

letters1234 6 days, 2 hours ago

Selected Answer: C

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#commonly-used-microsoft-365-admin-center-roles

Service Support Admin - Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:
- Open and manage service requests
- View and share message center posts
- Monitor service health

upvoted 2 times

Casticod 2 weeks, 4 days ago

Selected Answer: C

In the link post by Venusasur, Search Service support administrator, and see the table

upvoted 2 times

Venusaur 3 weeks ago

Answer C is correct.

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide&redirectSourcePath=%252fen-us%252farticle%252fabout-office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d

upvoted 4 times

Question #10 *Topic 1*

HOTSPOT -

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

Scope type: Directory -

Selected members: Group1 -

Assignment type: Active -

Assignment starts: Mar 15, 2023 -

Assignment ends: Aug 15, 2023 -

You add the following assignment for the Exchange Administrator role:

Scope type: Directory -

Selected members: Group2 -

Assignment type: Eligible -

Assignment starts: Jun 15, 2023 -

Assignment ends: Oct 15, 2023 -

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
On July 15, 2023, Admin1 can reset the password of a user.	○	○
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	○	○
On May 1, 2023, Admin3 can reset the password of a user.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On July 15, 2023, Admin1 can reset the password of a user.	◉	○
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	○	◉
On May 1, 2023, Admin3 can reset the password of a user.	◉	○

Casticod Highly Voted 2 weeks, 5 days ago

Yes, Yes, Yes ??

upvoted 7 times

Tedd_TS Most Recent 2 weeks, 2 days ago

Yes, Yes, Yes i think too

upvoted 2 times

Venusaur 3 weeks ago

[ ] On May 1, 2023, Admin3 can reset the password of a user.
This should be YES right?
Admin3 is member of Group1 + Group2
Group1 assignment start from Mar 15 2023 to Aug 15 2023.
May 1 2023 should be within the range.

upvoted 3 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

- Y
Admin1 in Group1 has an active assignment for the User Administrator Role between mar 15 and aug 15.

- Y
This one is questionable. Admin2 in Group2 has an eligible assignment for the Exchange Administrator role from jun 15 til oct 15. It depends on the eligible assignment type. When MFA or justification is selected, the answer would be Y.
But if approved is selected, it depends on approval of the request if admin2 can manage Exchange.

- N
Not in the right date range

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user#assign-a-role

upvoted 4 times

cb0900 1 week, 6 days ago

Agree Admin2 is questionable. Does MS mark the answer where Admin2 manages to activate the Exchange Admin role (although this isn't mentioned in the question) then Y, or Admin2 doesn't take any action and as it's Eligible then answer is N.

upvoted 2 times

gbartumeu 2 weeks, 6 days ago

Admin3 is member of Group 1, and May 01, 2023 is in the date range (Mar 15, 2023 to Aug 15, 2023)

upvoted 7 times

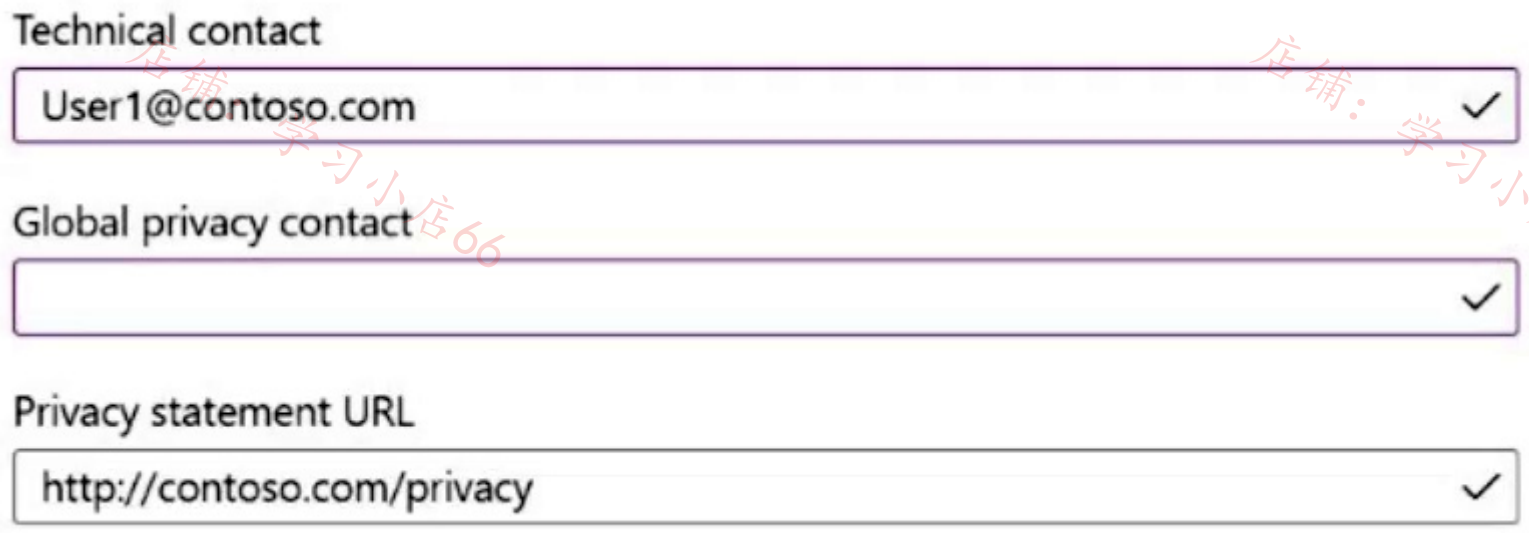
Question #11 *Topic 1*

You have a Microsoft 365 subscription.

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.



Which users will be contacted by Microsoft if the tenant experiences a data breach?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User2 only

E. User2 and User3 only

Correct Answer: *B*

Community vote distribution

D (63%) B (38%)

ae88d96 1 day, 19 hours ago

Selected Answer: D

Correct answer is D, see explanation below:

User1 is Security Administrator and Technical Contact hence he will receive a notification for being Technical Contact.
User2 is Global Administrator so he will received a notification as well.
User3 is Service Support Administrator so he won't received a notification.

Reference: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics#customer-notification

If warranted, one or more of the following roles may be notified via email of a security or privacy incident in conjunction with, or in lieu of, a service health notification:
Azure Subscription Administrators or Owners
Azure Active Directory Global Tenant Administrators
Azure Active Directory Tenant Technical Contacts

upvoted 1 times

letters1234 6 days ago

Selected Answer: D

"If the TENANT experiences data breach" which would be the Azure Tenant. It's not the Microsoft 365 notification policy as that would be for 365 services.

https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics#customer-notification
If warranted, one or more of the following roles may be notified via email of a security or privacy incident in conjunction with, or in lieu of, a service health notification:
-Azure Subscription Administrators or Owners
-Azure Active Directory Global Tenant Administrators
-Azure Active Directory Tenant Technical Contacts

upvoted 2 times

Greatone1 1 week, 1 day ago

Selected Answer: B

It should be B
If warranted, one or more of the following roles may be notified via email of a security or privacy incident in conjunction with, or in lieu of, a service health notification:

Azure Subscription Administrators or Owners
Azure Active Directory Global Tenant Administrators
Azure Active Directory Tenant Technical Contacts

upvoted 1 times

Casticod 2 weeks, 5 days ago

Selected Answer: D

The question says which roles can do it, therefore the usual condition of least privileges does not apply, have to mention all the ones that can, therefore Global and Security administrator can contact (D)

upvoted 2 times

Casticod 2 weeks, 4 days ago

Please admin delete my post, Rethinking de Answer The correct it´s B

upvoted 1 times

Dtriminio 3 weeks, 2 days ago

Selected Answer: B

As noted previously, Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.

https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

upvoted 2 times

Question #12 *Topic 1*

Your network contains an Active Directory forest named contoso.local.
You purchase a Microsoft 365 subscription.
You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.
You need to prepare for the planned move to Microsoft 365.
What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

A. Purchase a third-party X.509 certificate.

B. Create an external forest trust.

C. Rename the Active Directory forest.

D. Purchase a custom domain name.

Correct Answer: *D*

Community vote distribution

D (100%)

Greatone1 2 weeks ago

Selected Answer: D

Given answer is correct

upvoted 3 times

Question #13 *Topic 1*

You have a Microsoft 365 subscription.
You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.
Which type of group should you use to assign the Reports Reader role and to access App1?

A. a Microsoft 365 group that has assigned membership

B. a Microsoft 365 group that has dynamic user membership

C. a security group that has assigned membership

D. a security group that has dynamic user membership

Correct Answer: *C*

Community vote distribution

C (100%)

osxzvkwpfcfxobqjby Highly Voted 3 weeks, 4 days ago

Selected Answer: C

You can not assign Azure AD roles to dynamic groups. And you don't need a mailbox/sharepoint/etc, so it is not a 365 group.

upvoted 5 times

Question #14 *Topic 1*

You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?

A. Enable auditing.

B. Enable Microsoft 365 usage analytics.

C. Create an Insider risk management policy.

D. Create a communication compliance policy.

Correct Answer: *A*

Community vote distribution

A (100%)

anonavia 1 week, 6 days ago

Selected Answer: A

-A
When an elevation of Microsoft Exchange Online administrative privileges is detected in your Microsoft 365 E5 tenant, you should first enable auditing.

upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

- A
But, question makes no sense. Audit is enabled by default. All other options are less obvious.

https://learn.microsoft.com/en-us/purview/audit-solutions-overview#audit-standard

upvoted 1 times

Question #15 *Topic 1*

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.
You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.
You plan to onboard all the devices to Microsoft Defender for Endpoint.
You need to store the Microsoft Defender for Endpoint data in Europe.
What should you do first?

A. Delete the workspace.

B. Create a workspace.

C. Onboard a new device.

D. Offboard the test devices.

Correct Answer: *B*

Community vote distribution

D (75%) B (25%)

pantcm 1 day, 21 hours ago
D is the correct answer
upvoted 1 times

gomezmax 1 week, 5 days ago
(D) Offboard the test devices. from here to the Moon
upvoted 1 times

Greatone1 2 weeks ago
D is the correct answer from MS 101
upvoted 2 times

Dtriminio 3 weeks, 2 days ago
Selected Answer: D
i will go with D
upvoted 1 times

alecrobertburns 3 weeks, 2 days ago
Selected Answer: D
Answer is D
To onboard them all in Europe you first have to offboard the 10 that are onboarded in the US
upvoted 1 times

alecrobertburns 3 weeks, 2 days ago
Answer is D
To onboard them all in Europe you first have to offboard the 10 that are onboarded in the US
upvoted 1 times

nublit 3 weeks, 3 days ago
Selected Answer: D
Answer is D: First Offboard the test devices,
delete the workspace, create a workspace in Europe, onboard new devices. Reference:
https://www.examtopics.com/discussions/microsoft/view/68005-exam-ms-101-topic-2-question-29-discussion/
upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago
Selected Answer: B
Create a new workspace. After that you can connect existing and new clients to the new workspace.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/faq-data-collection-agents#how-can-i-use-my-existing-log-analytics-workspace-
upvoted 1 times

Question #16 *Topic 1*

You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list.
What should you use?

A. the Exchange admin center

B. the Microsoft Purview compliance portal

C. the Microsoft 365 admin center

D. the Microsoft 365 Defender portal

E. the Microsoft Entra admin center

Correct Answer: *D*

Community vote distribution

D (100%)

Dtriminio 3 weeks, 2 days ago

Selected Answer: D

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal
In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide

upvoted 4 times

RAG 3 weeks, 3 days ago

Selected Answer: D

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide

upvoted 3 times

Question #17 *Topic 1*

Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.
What should you do?

A. Create a data loss prevention (DLP) policy that has a Content is shared condition.

B. Modify the safe links policy Global settings.

C. Create a data loss prevention (DLP) policy that has a Content contains condition.

D. Create a new safe links policy.

Correct Answer: *D*

Greatone1 2 weeks ago

D is the correct answer

https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients

upvoted 2 times

HOTSPOT -

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

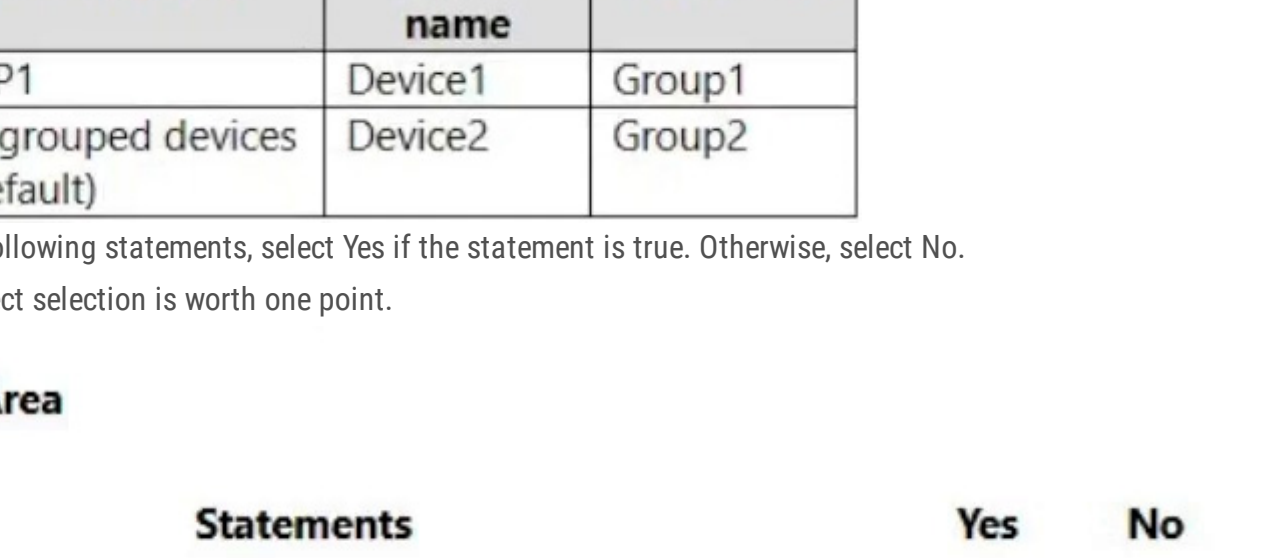
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

Correct Answer:



mhmyz 1 day, 4 hours ago

No,No,No
Box3: User3 can Remediation Action but, Group3 do not assinged ATP1.
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection

upvoted 1 times

hogehogehoge 5 days, 14 hours ago

Box3: No?
Because Defferent Group In User and Device.

upvoted 1 times

rinzler1 4 days, 3 hours ago

User3 is in default Admin group, has access to everything related to Endpoints

upvoted 1 times

Greatone1 1 week, 1 day ago

Answer is correct

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection

upvoted 1 times

Question #19 *Topic 1*

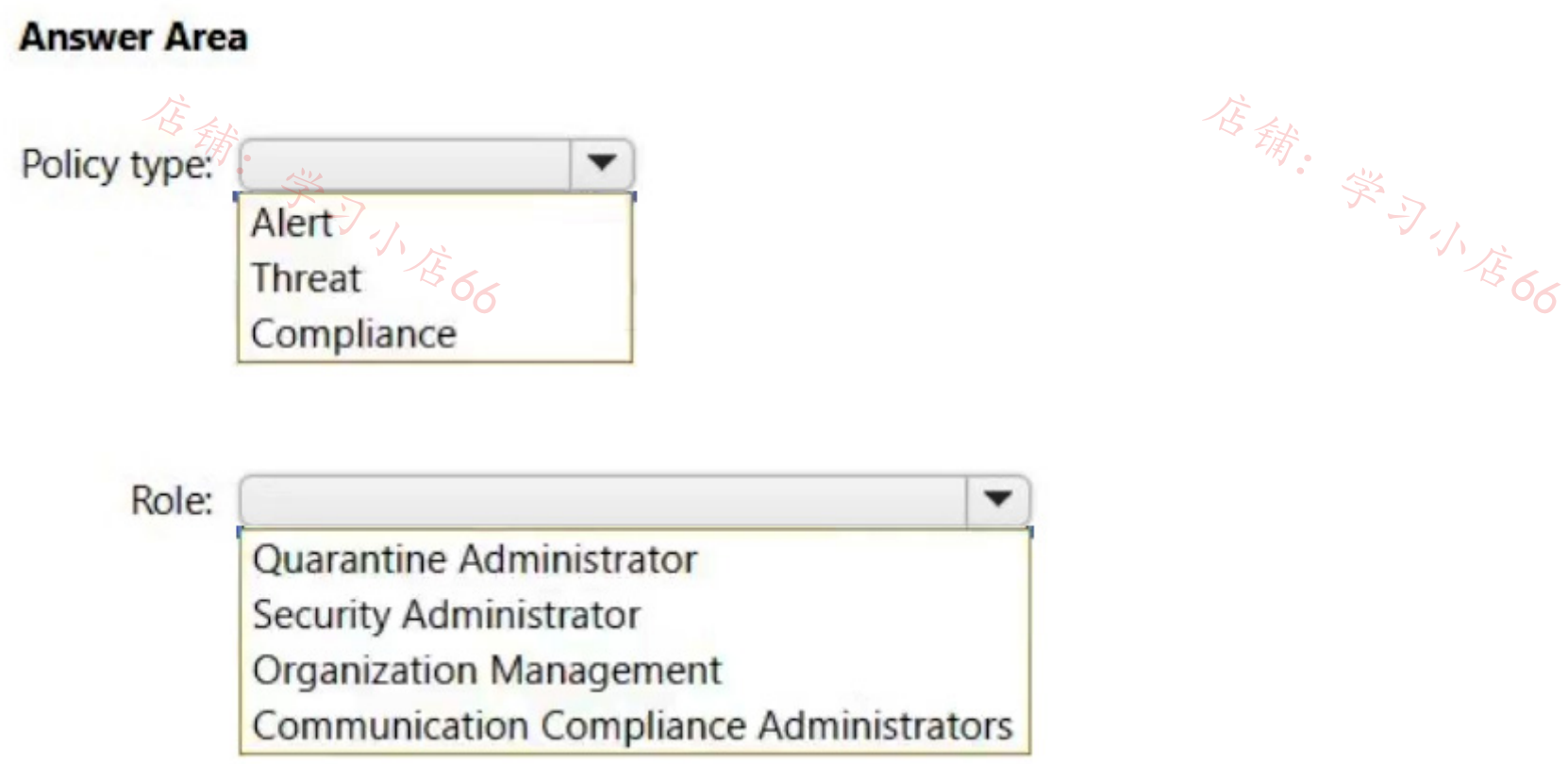
HOTSPOT -

You have a Microsoft 365 E5 tenant.

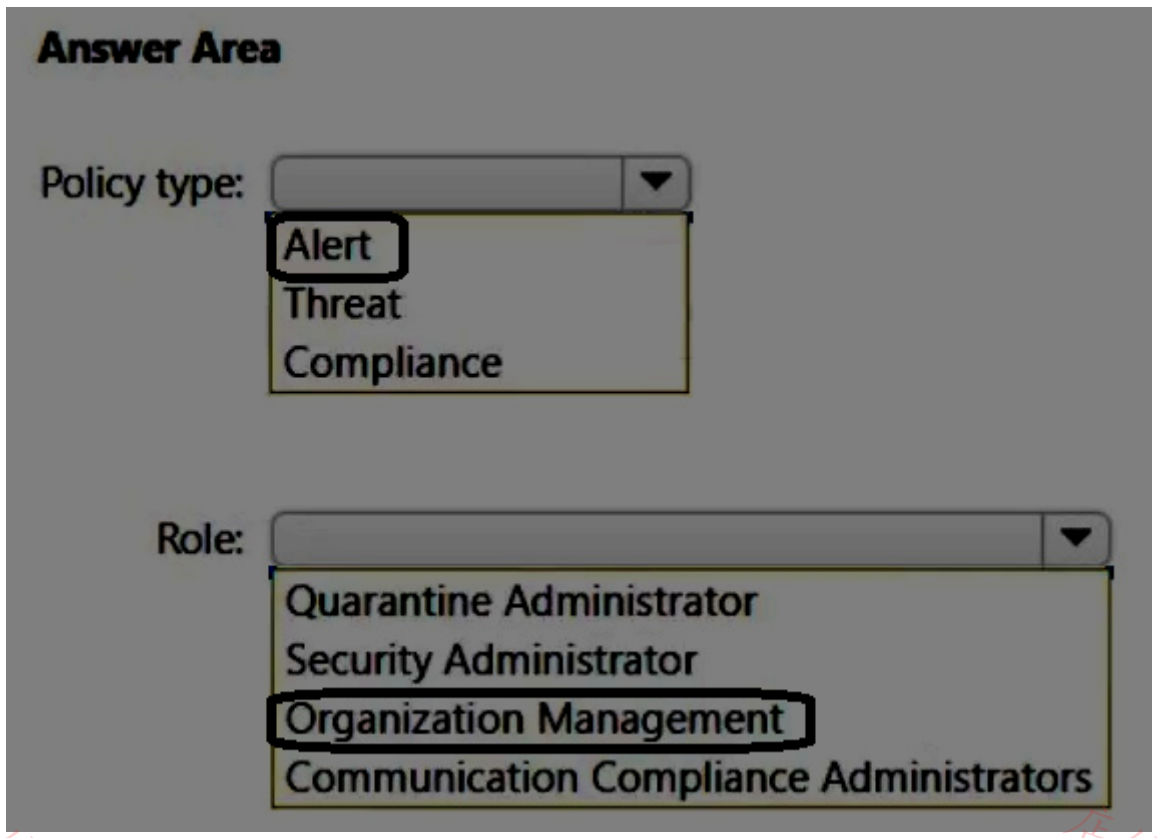
You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.

Which type of policy should you create, and which Microsoft Purview solutions role is required to create the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



letters1234 5 days, 4 hours ago

Security Administrator or Global Administrator are required to setup the alert notifications. Least privilege means SA instead of GA.
https://learn.microsoft.com/en-us/microsoft-365/security/defender/configure-email-notifications?view=o365-worldwide#create-rules-for-alert-notifications

upvoted 4 times

Casticod 5 days, 16 hours ago

I think security administrator.
Organization management, not Purview role, its a Echange Role. In the question need a Pureview role

upvoted 1 times

gomezmax 1 week, 3 days ago

Correct, Alert and Organization Management.

upvoted 1 times

Greatone1 1 week, 5 days ago

Should be Alert and Security Administrator

upvoted 2 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

- Alert
- Security administrator (principle of least privilege)

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide

upvoted 4 times

Question #20 *Topic 1*

You have a Microsoft 365 E5 subscription.
You need to compare the current Safe Links configuration to the Microsoft recommended configurations.
What should you use?

A. Microsoft Purview

B. Azure AD Identity Protection

C. Microsoft Secure Score

D. the configuration analyzer

Correct Answer: *C*

Community vote distribution

D (100%)

certma2023 Highly Voted 2 weeks, 5 days ago

Selected Answer: D

It should be answer D.

The goal of the configuration analyzer is to compare Exchange Online Protection policies (aka Threat Policies) currently configured with MS recommendations.

There is two tabs named "Standard recommendations" & "Strict recommendations" that give the gap between current configuration & MS recommendations.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configuration-analyzer-for-security-policies?view=o365-worldwide#use-the-configuration-analyzer-in-the-microsoft-365-defender-portal

upvoted 7 times

ae88d96 Most Recent 1 day, 17 hours ago

Selected Answer: D

Correct answer is D.

In the public documentation it is mentioned what's covered within the Configuration Analyzer.
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configuration-analyzer-for-security-policies?view=o365-worldwide#use-the-configuration-analyzer-in-the-microsoft-365-defender-portal

Microsoft Defender for Office 365 policies: Includes organizations with Microsoft 365 E5 or Defender for Office 365 add-on subscriptions:

Anti-phishing policies in Microsoft Defender for Office 365, which include:
The same spoof settings that are available in the EOP anti-phishing policies.
Impersonation settings
Advanced phishing thresholds
Safe Links policies.
Safe Attachments policies.

upvoted 2 times

gomezmax 3 days, 18 hours ago

It should be D

upvoted 1 times

Greatone1 1 week, 3 days ago

Selected Answer: D

Correct answer is D

upvoted 1 times

Takanami 1 week, 5 days ago

Configuration Analyzer is correct, direct link:

https://security.microsoft.com/configurationAnalyzer

upvoted 1 times

Question #21 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

You need to enable user access to the partner company's portal.

Which Microsoft Defender for Endpoint setting should you modify?

A. Alert notifications

B. Alert suppression

C. Custom detections

D. Advanced hunting

E. Indicators

Correct Answer: *E*

Community vote distribution

E (100%)

letters1234 5 days, 3 hours ago

Selected Answer: E

Answer lines up with image as well, Defender SmartScreen.

"To block malicious IPs/URLs (as determined by Microsoft), Defender for Endpoint can use:
- Windows Defender SmartScreen for Microsoft browsers
- Network Protection for non-Microsoft browsers, or calls made outside of a browser"
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide#overview

upvoted 1 times

Dtriminio 3 weeks, 2 days ago

Selected Answer: E

By creating indicators for IPs and URLs or domains, you can now allow or block IPs, URLs, or domains based on your own threat intelligence.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide

upvoted 3 times

RAG 3 weeks, 3 days ago

Selected Answer: E

Same question as listed on https://www.examtopics.com/discussions/microsoft/view/48796-exam-ms-101-topic-2-question-32-discussion/

upvoted 3 times

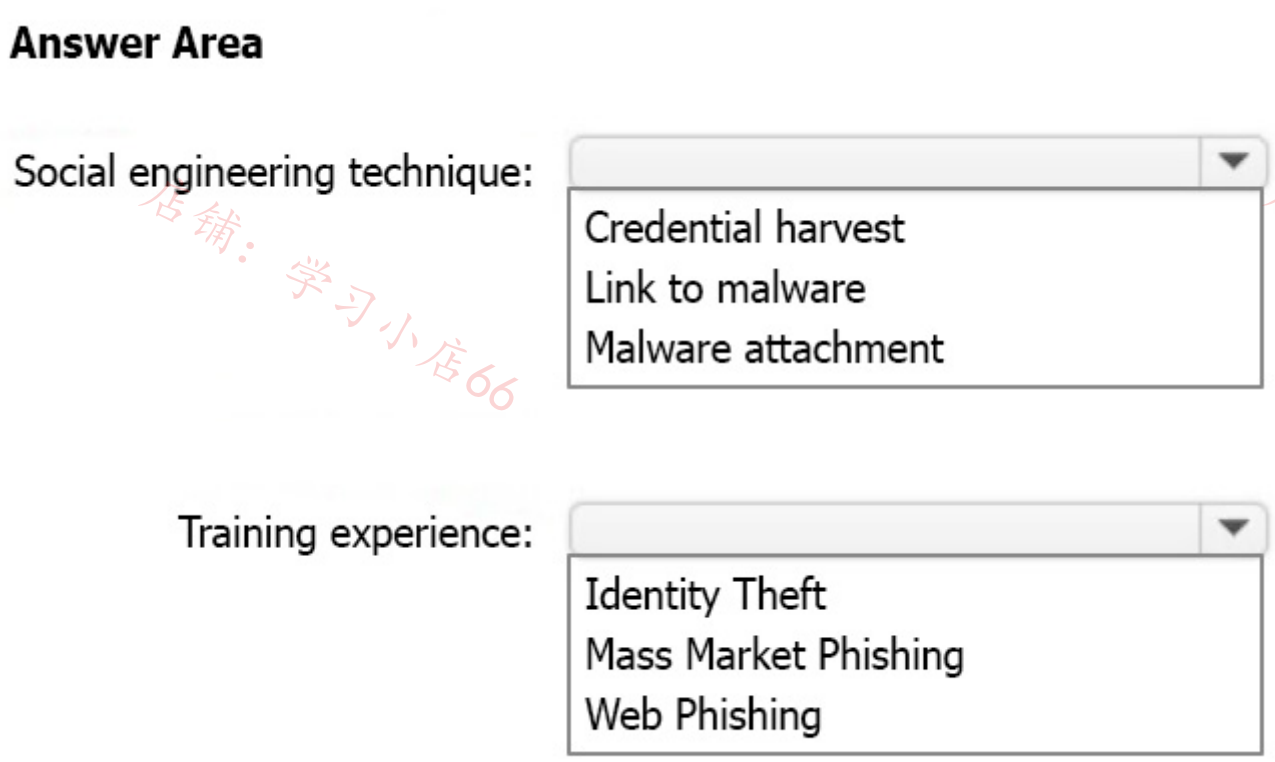
HOTSPOT -

You have a Microsoft 365 E3 subscription.

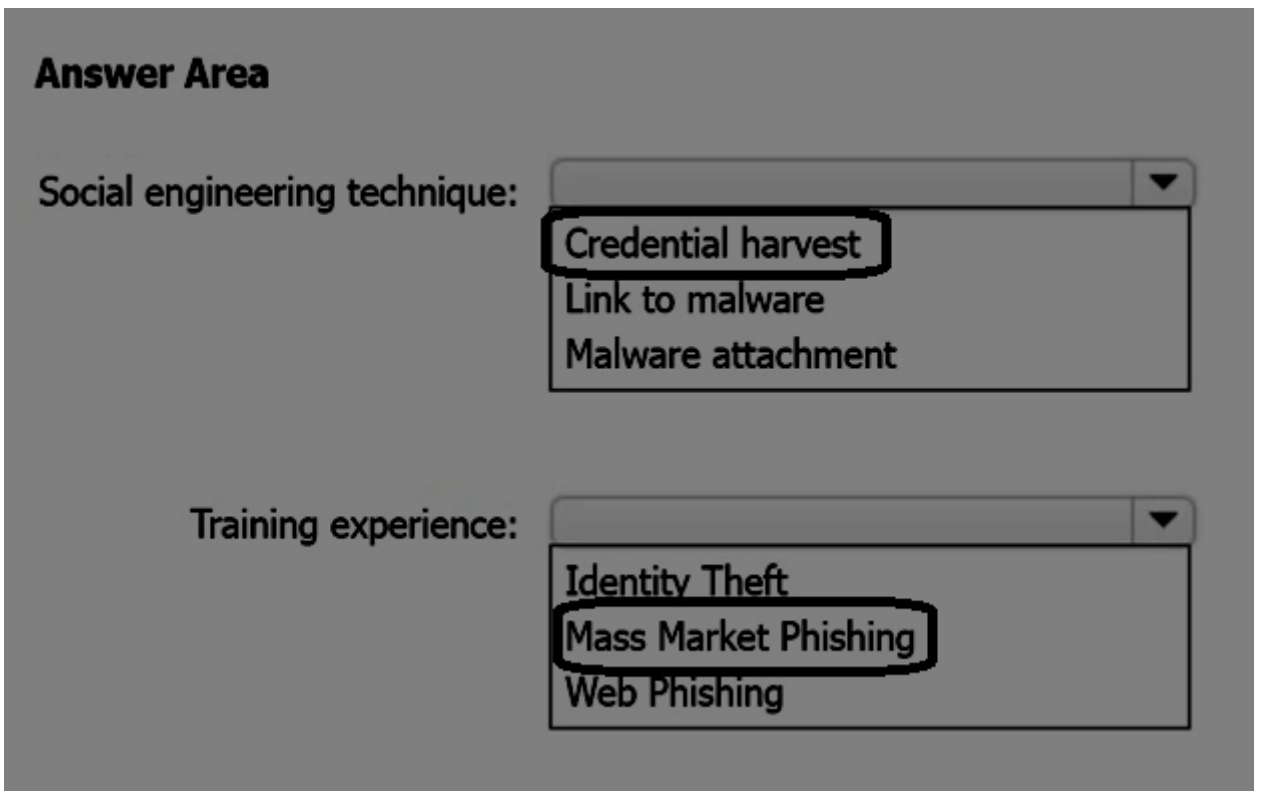
You plan to launch Attack simulation training for all users.

Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



letters1234 5 days, 3 hours ago

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide#what-do-you-need-to-know-before-you-begin

upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

- All are available
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide#simulations

- All are available
https://security.microsoft.com/attacksimulator?viewid=trainingcampaign

upvoted 1 times

RAG 3 weeks, 3 days ago

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.

upvoted 2 times

Question #23 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.
What should you do?

A. Create a new Anti-malware policy.

B. Configure the Safe Links global settings.

C. Create a new Anti-phishing policy.

D. Configure the Safe Attachments global settings.

Correct Answer: *D*

Community vote distribution

D (78%) B (22%)

mhmyz 9 hours, 12 minutes ago

Selected Answer: D

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about?view=o365-worldwide

upvoted 1 times

Greatone1 2 weeks ago

Selected Answer: D

D is the correct answer

upvoted 1 times

moshkoshbgosh 3 weeks ago

Selected Answer: D

Safe attachments supports Teams, SharePoint, OneDrive - https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about .
The following text is taken directly from Safe Attachments Global Settings in the Defender portal... "

Global settings
Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.
Protect files in SharePoint, OneDrive, and Microsoft Teams
If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, Safe Attachments will prevent users from opening and downloading the file. Learn more
Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams

upvoted 3 times

Dtriminio 3 weeks, 2 days ago

Selected Answer: B

In organizations with Microsoft Defender for Office 365, Safe Links scanning protects your organization from malicious links, including QR codes, that are used in phishing and other attacks. Specifically, Safe Links provides URL scanning and rewriting of inbound email messages during mail flow, and time-of-click verification of URLs and links in email messages, Teams, and supported Office 365 apps.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-about?view=o365-worldwide

upvoted 1 times

alecrobertburns 3 weeks, 2 days ago

Selected Answer: D

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/utilize-microsoft-defender-for-office-365-in-sharepoint-online?view=o365-worldwide#stop-infected-file-downloads-from-sharepoint-online

upvoted 1 times

RAG 3 weeks, 3 days ago

Selected Answer: D

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-configure?view=o365-worldwide

upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

Selected Answer: B

Safe attachments is only for mail so the answer is B

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure?view=o365-worldwide

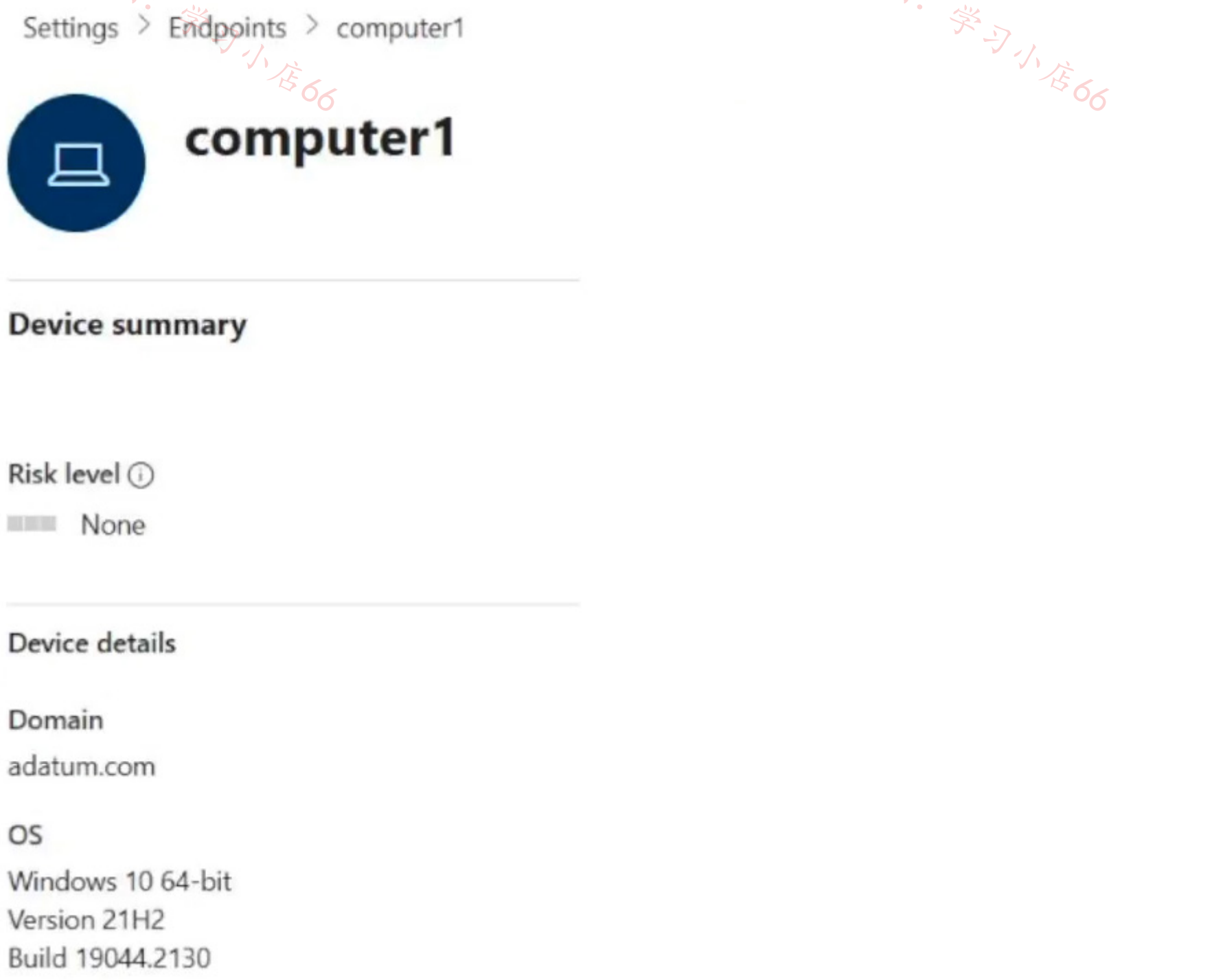
upvoted 1 times

HOTSPOT -

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	*Not applicable*

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

Answer Area

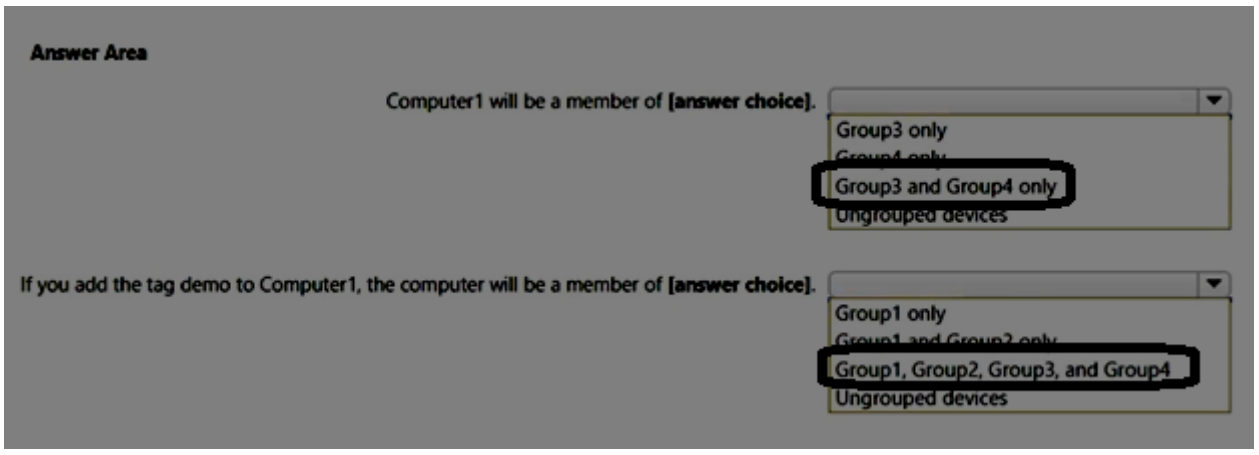
Computer1 will be a member of **[answer choice]**.

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

Correct Answer:



Nalle Highly Voted 3 weeks, 2 days ago

Group 3 only
Group 1 only

"If a device is also matched to other groups, it's added only to the highest ranked device group"

upvoted 8 times

jt2214 Most Recent 23 hours, 25 minutes ago

I didn't read the ranking at first. So it makes more sense, now.

upvoted 1 times

Greatone1 1 week, 5 days ago

Group 3 and Group 1
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 2 times

Casticod 2 weeks, 5 days ago

Group 3 only
Group 1 Only
https://www.examtopics.com/discussions/microsoft/view/48754-exam-ms-101-topic-2-question-15-discussion/

upvoted 3 times

Question #25 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.

The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.

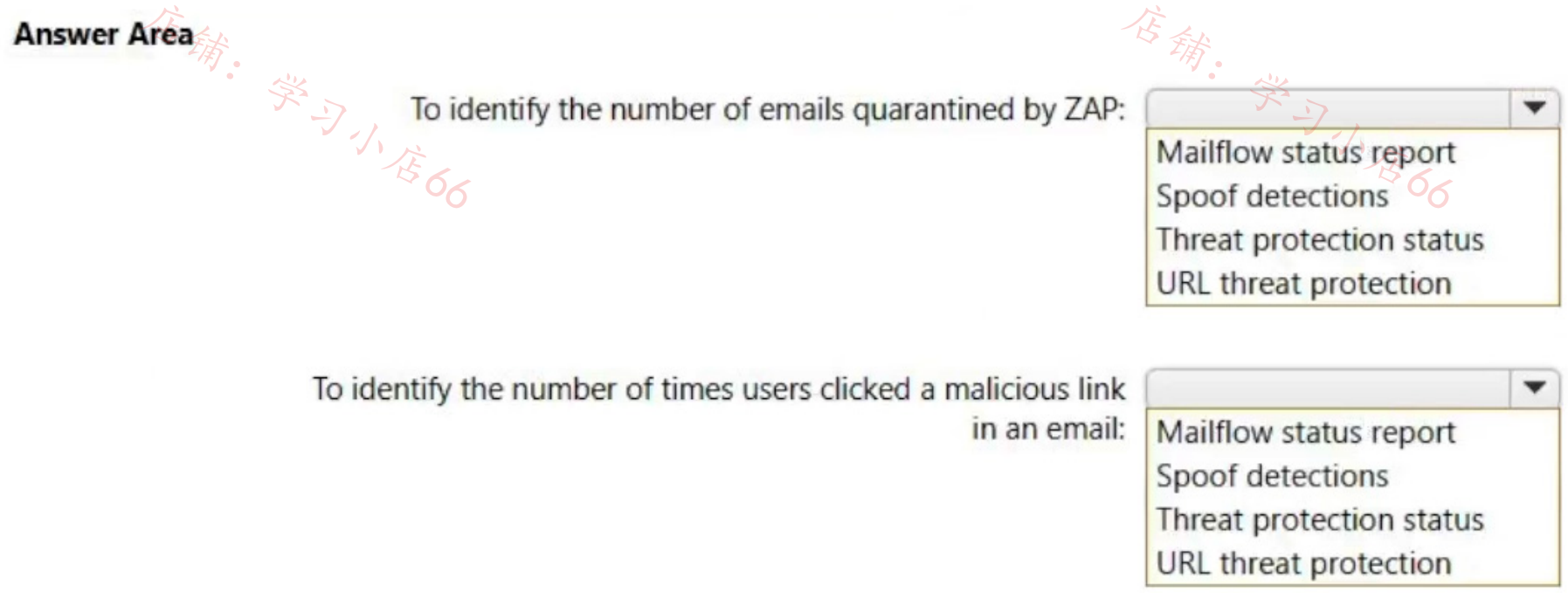
You need to identify the following information:

The number of email messages quarantined by zero-hour auto purge (ZAP)

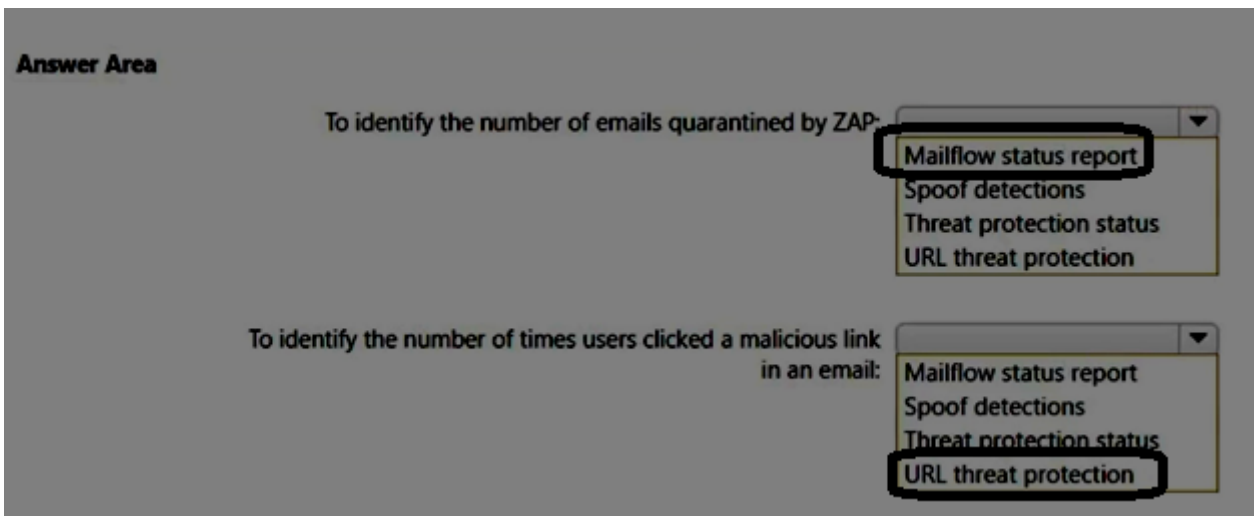
The number of times users clicked a malicious link in an email message

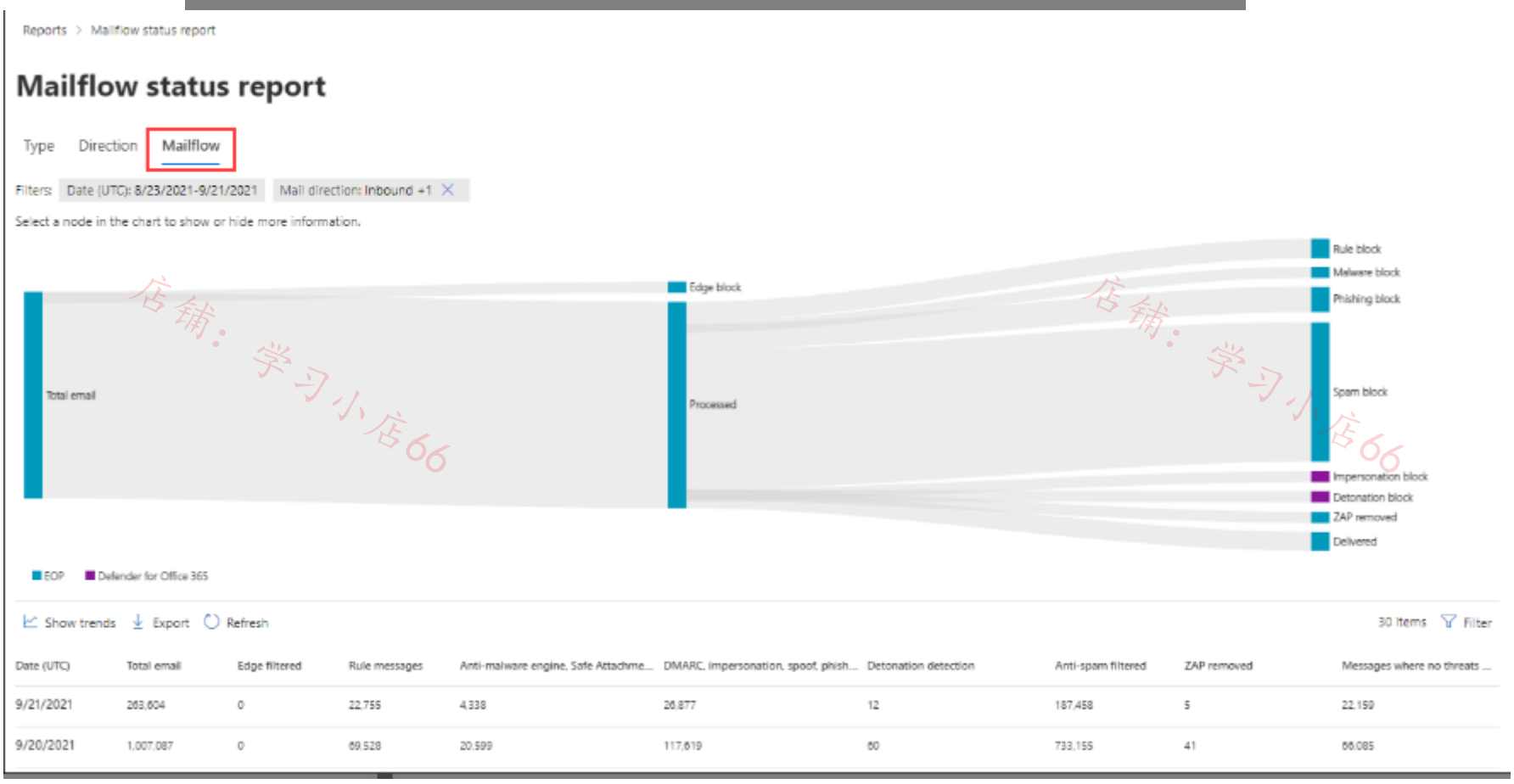
Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:





Greatone1 1 week, 5 days ago

Mailflow Status Report
2) URL Protection

upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 4 days ago

- Mailflow & URL

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#how-to-see-if-zap-moved-your-message

upvoted 2 times

Question #26 *Topic 1*

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 Defender.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender portal?

A. Microsoft Sentinel

B. Microsoft Defender for Cloud

C. Azure Arc

D. Microsoft Defender for Identity

Correct Answer: *D*

Community vote distribution

D (100%)

cb0900 1 week, 4 days ago

You can filter the alerts based on the Service Sources:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide#service-sources

upvoted 2 times

Greatone1 1 week, 5 days ago

Selected Answer: D

D is correct
https://www.examtopics.com/discussions/microsoft/view/56970-exam-ms-101-topic-2-question-70-discussion/

upvoted 1 times

Question #27 *Topic 1*

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.
Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com.
You plan to install Azure AD Connect on a member server and implement pass-through authentication.
You need to prepare the environment for the planned implementation of pass-through authentication.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From a domain controller, install an Authentication Agent.

B. From the Microsoft Entra admin center, configure an authentication method.

C. From Active Directory Domains and Trusts, add a UPN suffix.

D. Modify the email address attribute for each user account.

E. From the Microsoft Entra admin center, add a custom domain name.

F. Modify the User logon name for each user account.

Correct Answer: *ABE*

Community vote distribution

CEF (100%)

mccheesey 1 week, 2 days ago

CEF would be the logical answer in my mind... But in a roundabout way, I can see the justification behind ABE...

If they're just planning to not modify the UPNs at all from that .onmicrosoft.com domain, it makes sense to install the agent, enable an authentication method, and just modify the email address field without worrying about not having an actual domain attached to their UPNs. But of course, real world application vs. test questions are always different I suppose. :)

upvoted 1 times

certma2023 2 weeks, 4 days ago

Selected Answer: CEF

I Agree. As the local ADDS name is "contoso.local", we need to make some few steps/prerequisites before being able to set up account synchronization:

-> Add a custom domain name on the Azure AD / MS Entra portal (ex. contoso.com)
-> Add a local UPN suffix at the ADDS Forest level (contoso.com)
-> Modify all user account UPN from username@contoso.local to username@contoso.com

Then comes the Azure AD Connect deployment & the PTA configuration.

upvoted 4 times

Casticod 2 weeks, 4 days ago

Selected Answer: CEF

CDF I don´t Dude

upvoted 1 times

Casticod 2 weeks, 1 day ago

CEF, sorry

upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 3 days ago

Selected Answer: CEF

A. is required for HA, use it in real world, but it is not been asked for in this question.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start
https://learn.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide#what-if-i-only-have-a-local-on-premises-domain

upvoted 2 times

Question #28 *Topic 1*

HOTSPOT -

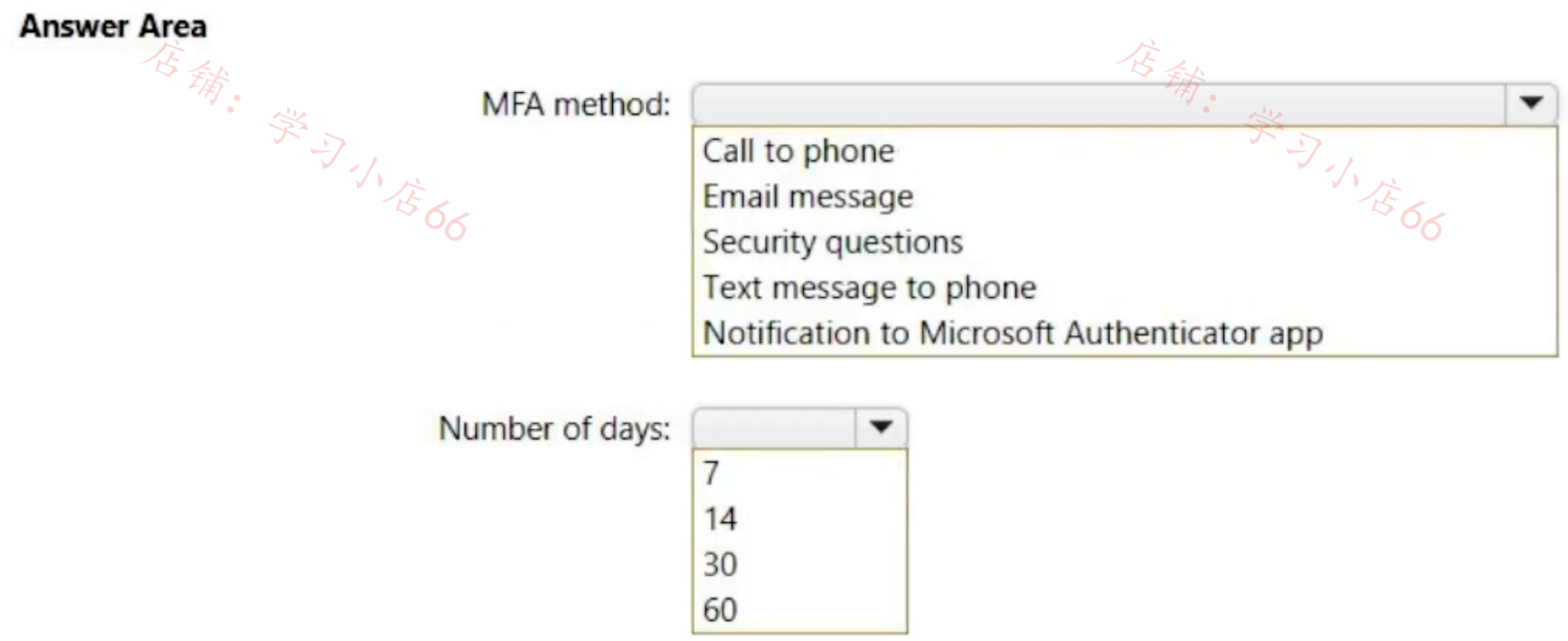
You have a new Microsoft 365 E5 tenant.

Enable Security defaults is set to Yes.

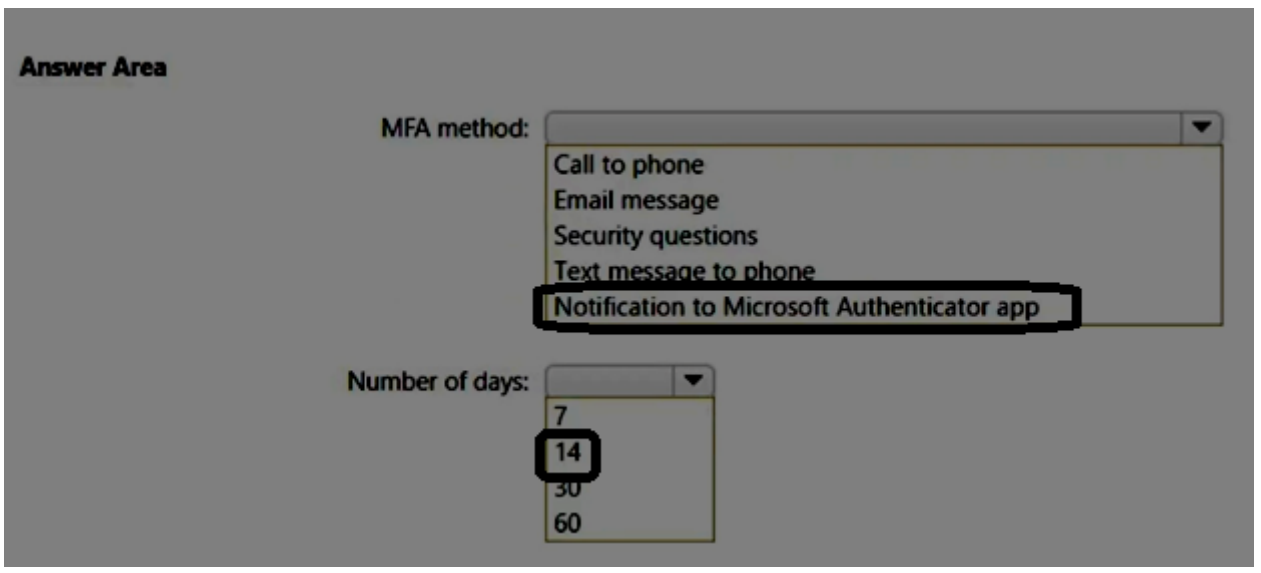
A user signs in to the tenant for the first time.

Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



osxzvkwpfcfxobqjby 3 weeks, 3 days ago

- Notification to Microsoft Authenticator app
- 14 days

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-defaults#authentication-methods

upvoted 3 times

Question #29 *Topic 1*

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.

Which objects will sync to Azure AD?

A. Group1 only

B. User1 and User2 only

C. Group1 and User1 only

D. Group1, User1, and User2

Correct Answer: *D*

Community vote distribution

D (62%) B (23%) C (15%)

Haso Highly Voted 2 weeks, 5 days ago

Selected Answer: D

It is D. Global security groups from your on-premises AD are synchronized to Azure AD, and they retain their membership and other attributes during the synchronization process. This means that if you have global security groups defined in your on-premises AD and these groups contain users or other groups, the membership information will be replicated to Azure AD.

Disabled user accounts are also synchronized: https://learn.microsoft.com/en-us/answers/questions/233667/will-azure-ad-connect-sync-disabled-user-accounts

upvoted 6 times

gomezmax Most Recent 1 week, 3 days ago

C. Group1 and User1 only User 2 is a disabled account

upvoted 1 times

Mr4D97 2 weeks, 3 days ago

Selected Answer: D

Builtin security groups are listed here (https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#default-active-directory-security-groups) and Global security group is not part of that list therefore it will be synchronised.

ANSWER IS D

upvoted 2 times

Casticod 2 weeks, 4 days ago

Selected Answer: B

In this conversation not much is clarified, for me the answer is B
https://www.examtopics.com/discussions/microsoft/view/48837-exam-ms-100-topic-3-question-77-discussion/

upvoted 1 times

moshkoshbgosh 3 weeks ago

Selected Answer: B

From https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts

Azure AD Connect excludes built-in security groups from directory synchronization.

Disabled accounts are synchronized as well to Azure AD

upvoted 2 times

moshkoshbgosh 2 weeks, 6 days ago

I'm starting to think this might be D... it's not specifically saying the global security group is a default global security group. Thoughts?

upvoted 3 times

certma2023 2 weeks, 4 days ago

You're right. Group1 is definitively a custom group not a built in securtity group like "domain admins" or "enterprise admins". Therefore it should synchronize to Azure AD without any issue.

upvoted 2 times

Mr4D97 2 weeks, 3 days ago

Yup, you're right. Builtin security groups are listed here (https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#default-active-directory-security-groups) and Global security group is not part of that list therefore it will be synchronised.

ANSWER IS D

upvoted 1 times

mrac 3 weeks ago

Selected Answer: C

C. Group1 and User1 only

Here's why:

Group1 is a global security group. By default, Azure AD Connect synchronizes security groups to Azure AD.

User1 is an enabled user. Enabled user accounts are synchronized to Azure AD by default.

User2 is a disabled user, and by default, disabled user accounts are not synchronized to Azure AD.

So, only Group1 and User1 will sync to Azure AD in this scenario.

upvoted 2 times

certma2023 2 weeks, 4 days ago

nope, It's answer D. By default disabled users are synced to Azure AD. If you want to change that, you need to implement a custom inbound synchronization rule.

"Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms."

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts#disabled-accounts

upvoted 2 times

Question #30 *Topic 1*

You have a Microsoft 365 E5 subscription.
You need to create Conditional Access policies to meet the following requirements:
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must be blocked from signing in from outside the United States and Canada.
Only users in the R&D department must be blocked from signing in from both Android and iOS devices.
Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.
What is the minimum number of Conditional Access policies you should create?

A. 3

B. 4

C. 5

D. 6

E. 7

F. 8

Correct Answer: *B*

Community vote distribution

B (100%)

nsotis28 1 week, 1 day ago

answer is correct
B

upvoted 1 times

certma2023 2 weeks, 4 days ago

Selected Answer: B

I would go for B answer.

4 rules configured like that :
-> One rule that target all users & all location except a custom trusted location (Public IP Ranges of the company). This rule grant access with MFA + Compliant device.
-> One rule that target all users & all location except US & Canada. This rule block access.
-> One rule that target R&D Users only & Android+IOS Devices. This rule block access.
-> One rule that target all users except Finance users. The rule target only App1. This rule block access.

For me, it should meet the goals.

upvoted 4 times

HOTSPOT -

Your network contains an on-premises Active Directory domain.

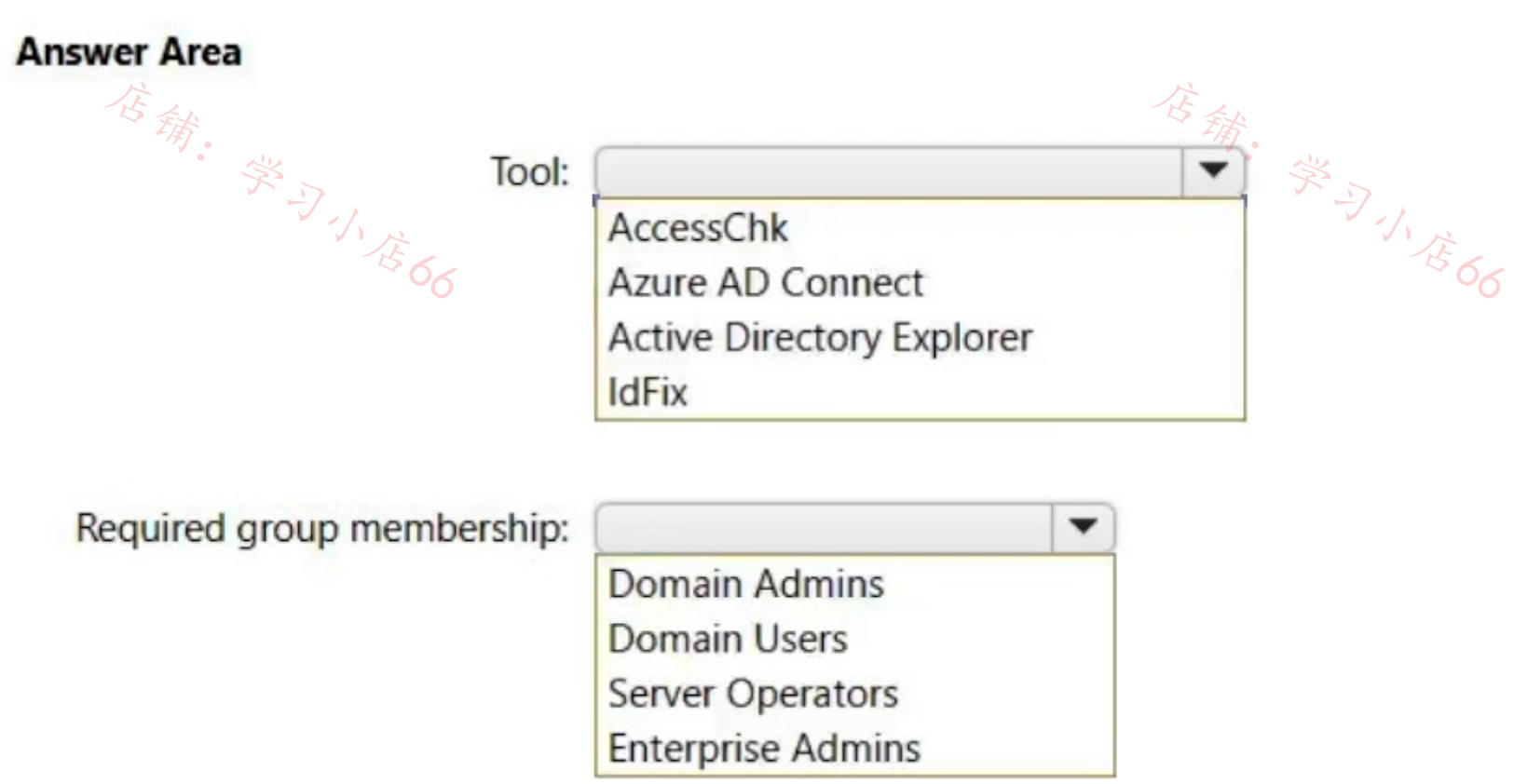
You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

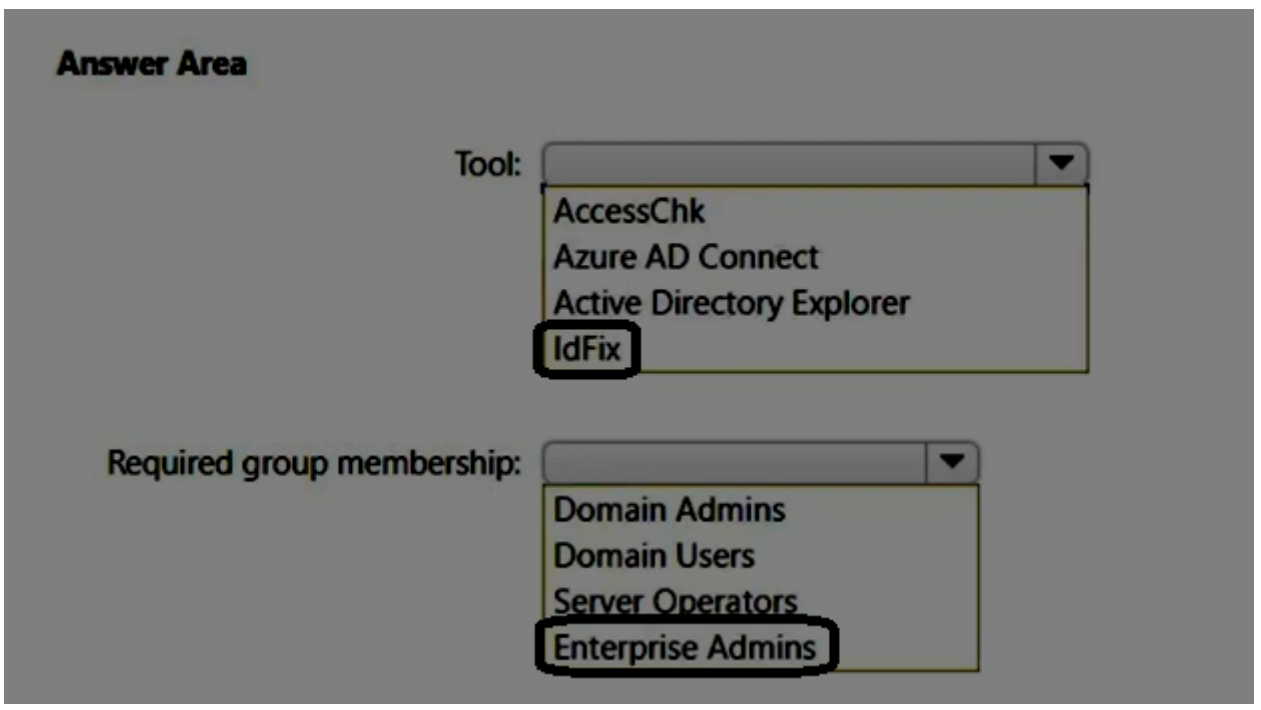
You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.



Correct Answer:



Casticod 2 weeks, 4 days ago

IdFix
Domain Users
The application runs in the context of the authenticated user, which means that it will query the authenticated forest and must have rights to read the directory.

upvoted 2 times

osxzvkwpfcfxobqjby 3 weeks, 3 days ago

IdFix & Domain Users

You only need to identify problems, so no rights needed to fix them.

https://microsoft.github.io/idfix/Step%201%20-%20Review%20the%20prerequisites/#permissions

upvoted 4 times

HOTSPOT -

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

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:

Users or workload identities assignments: All users

Cloud apps or actions assignment: App1

Conditions: Include all trusted locations

Grant access: Require multi-factor authentication

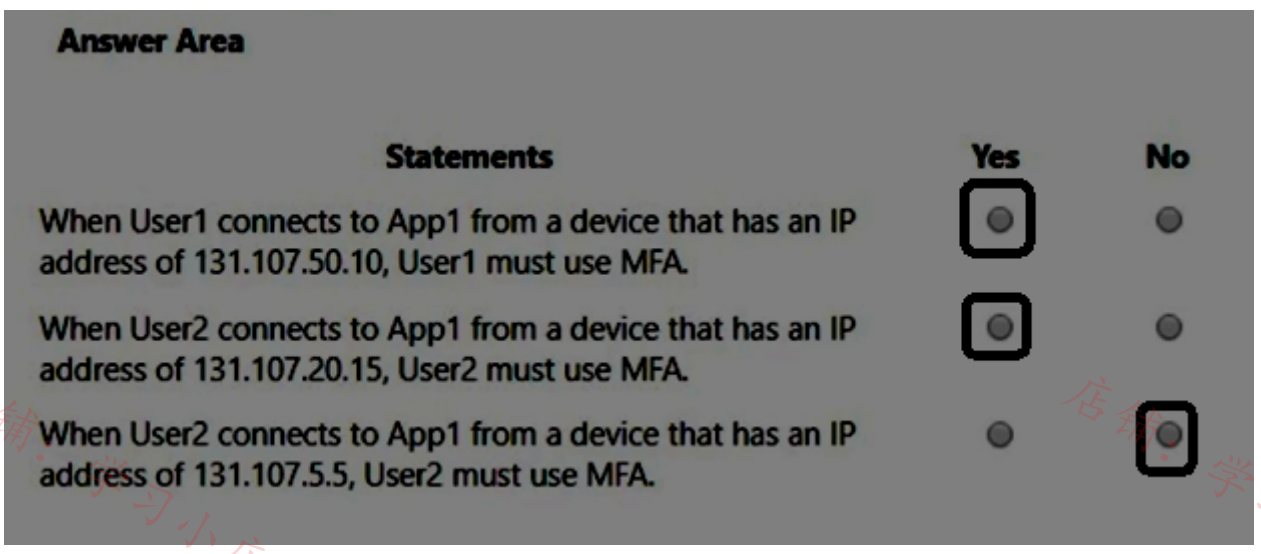
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	○	○

Correct Answer:



Haso Highly Voted 2 weeks, 5 days ago

Y: User is in trusted location from CA policy
Y: User is in trusted location from CA policy
N: Trusted IPs in the MFA settings containts a list of IPs that MFA can be skipped from.
https://c7solutions.com/2022/07/what-is-multifactor-authentication-trusted-ips

upvoted 5 times

osxzvkwpfcfxobqjby Most Recent 3 weeks, 3 days ago

Y: User is in trusted location from CA policy
Y: User is in trusted location from CA policy
Y: User is in trusted location set by MFA config

MFA per user setting is an old (but still existing) one.
AAD > All Users > Per-User MFA icon > Gray Service setting tab

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#view-the-status-for-a-user
upvoted 2 times

certma2023 2 weeks, 4 days ago

No it should be YYN.

The trusted IPs configured inside the legacy per-user MFA settings are IPs where MFA is bypassed. Therefore if the user connect from the "Trusted IPs" IP range he won't be prompt for MFA.
upvoted 2 times

Question #33 *Topic 1*

You have a Microsoft 365 subscription.
You register two applications named App1 and App2 to Azure AD.
You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

A. From the Microsoft Entra admin center, create a conditional access policy.

B. From the Microsoft 365 admin center, configure the Modem authentication settings.

C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.

D. From Multi-Factor Authentication, configure the service settings.

Correct Answer: *A*

Community vote distribution

A (100%)

GLL 5 days, 6 hours ago

Selected Answer: A

Conditional Access is found in the Microsoft Entra admin center under Protection > Conditional Access.
upvoted 1 times

Question #34 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

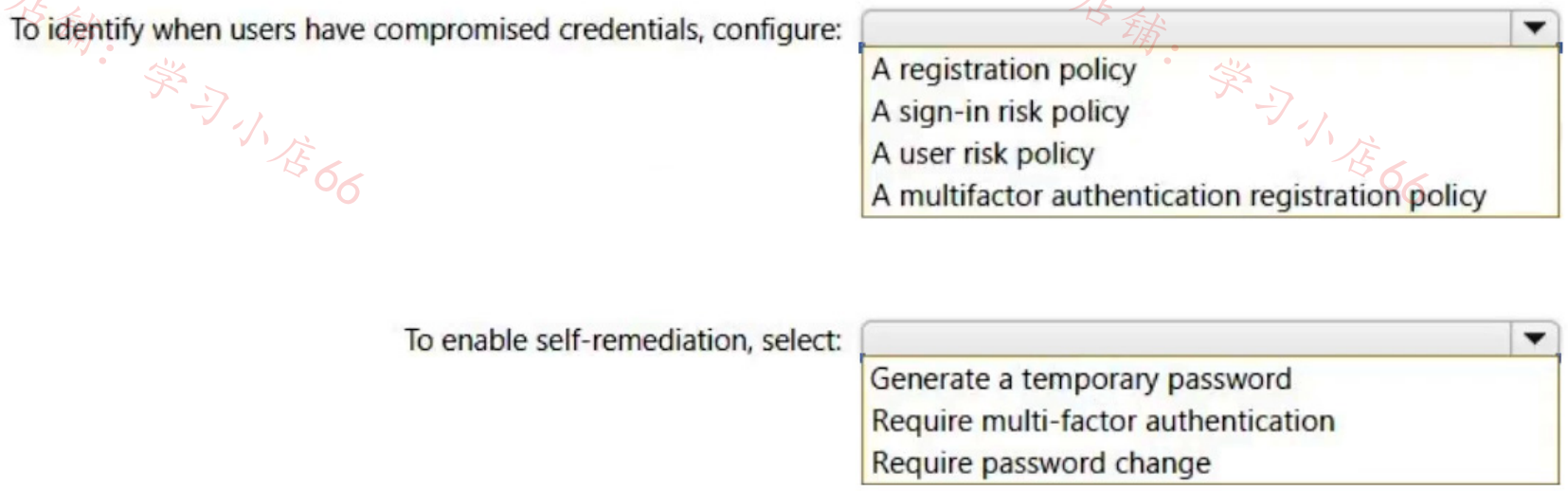
Identify when a user's credentials are compromised and shared on the dark web.

Provide users that have compromised credentials with the ability to self-remediate.

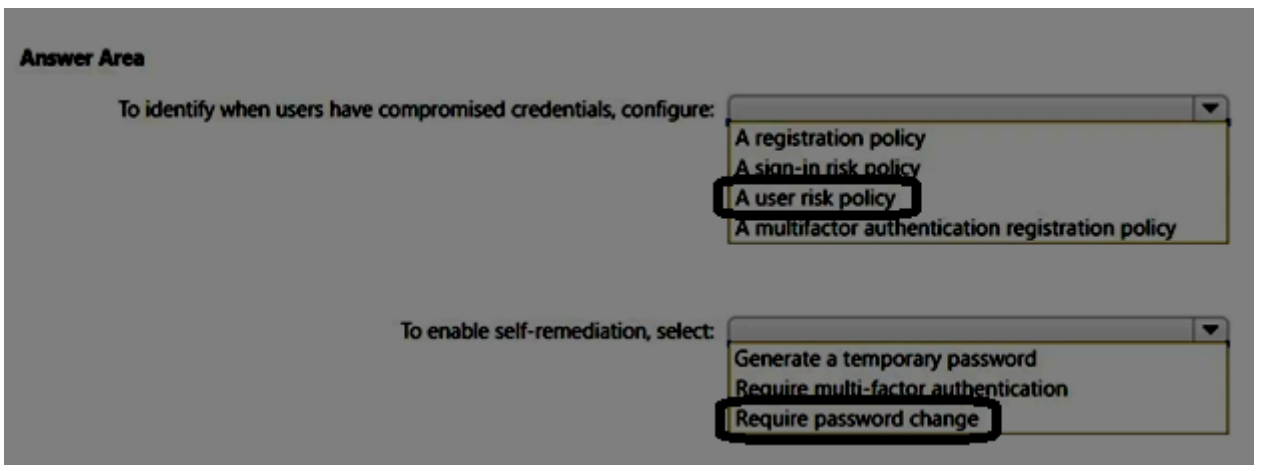
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:



RAG 3 weeks, 3 days ago

Looks correct - https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

upvoted 4 times

certma2023 2 weeks, 4 days ago

The second one is obviously correct. Require password change is the MS recommendation for a compromised account (user with a high risk or high sign-in risk).

For the first one the question is unclear. To identity a user with compromised credentials we would go the the "Risky Users" blade. But if the question is about configuring a rule that apply an action on account with credentials shared on the dark Web (or the regular Web like GitHub repos), we would create either a conditional access policy (new way with only an Azure AD P1 license) or either a risk user policy inside the Azure AD Identity Protection blade (legacy way that require an Azure AD P2 license).

Therefore the second one should be correct too, assuming that the question about configuring a rule that apply a specific action to compromised account (MS also say "leaked credentials" is some documentations).

upvoted 2 times

Nandokun01 1 week, 3 days ago

Correct (as expected :)) but since I dont see the CA policy option as an answer they must be looking for the old risk policy option to set these up. I didnt realize the P1 vs P2 difference until you mentioned it so thanks!

upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.

The domain contains the users shown in the following table.

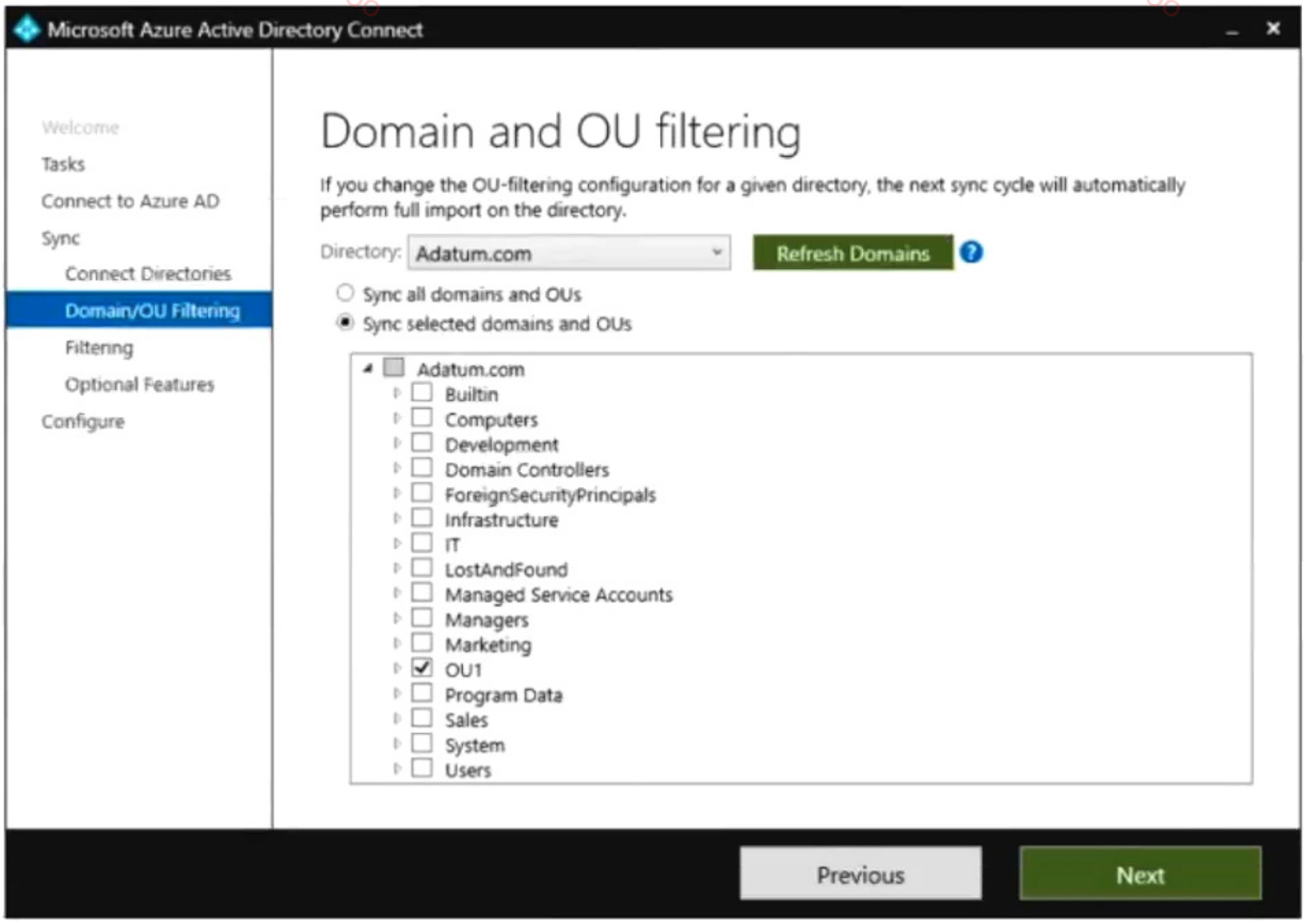
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

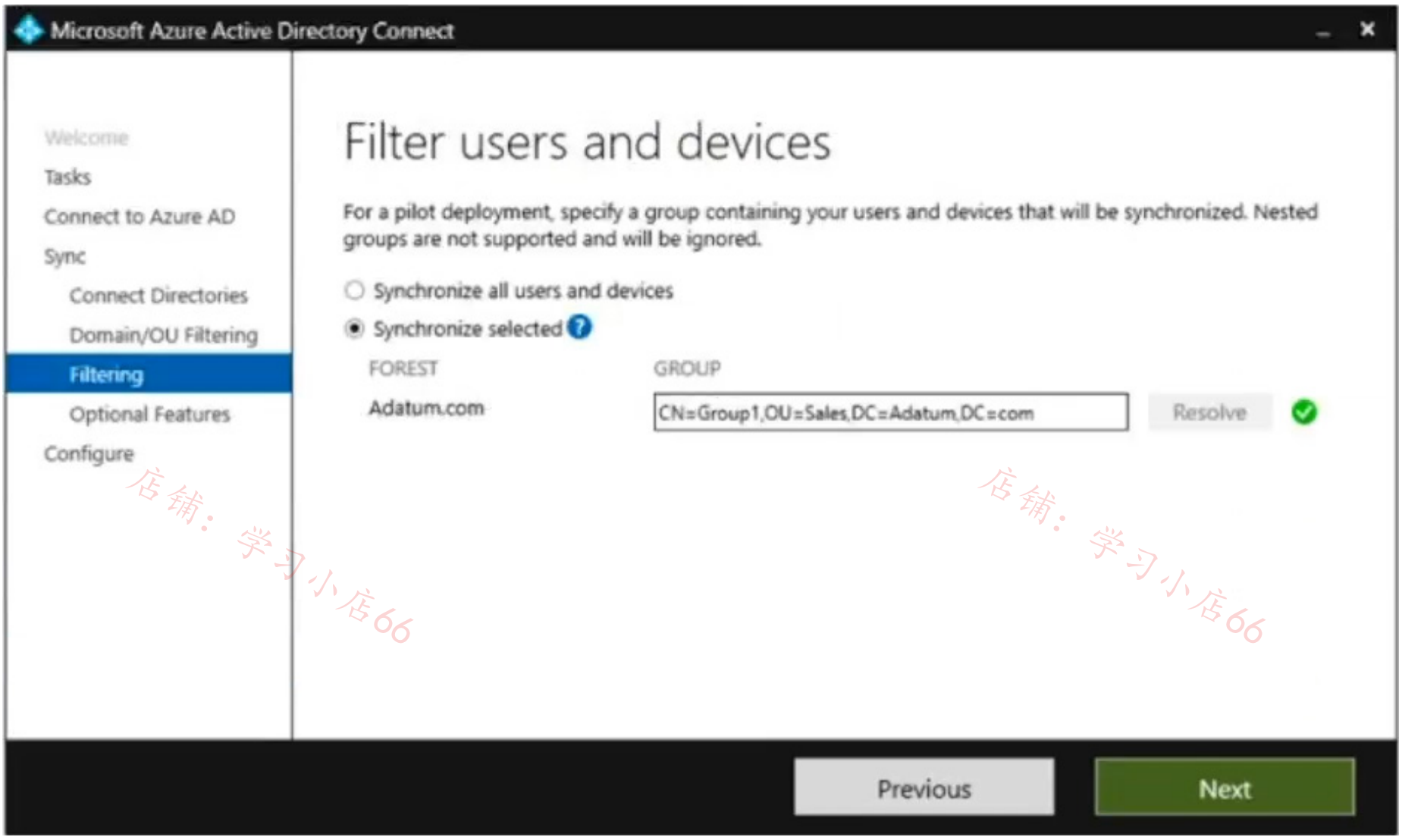
Name	Member of	In OU
Group1	*None*	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.

You configure Domain and OU filtering as shown in the following exhibit.



You configure Filter users and devices as shown in the following exhibit.



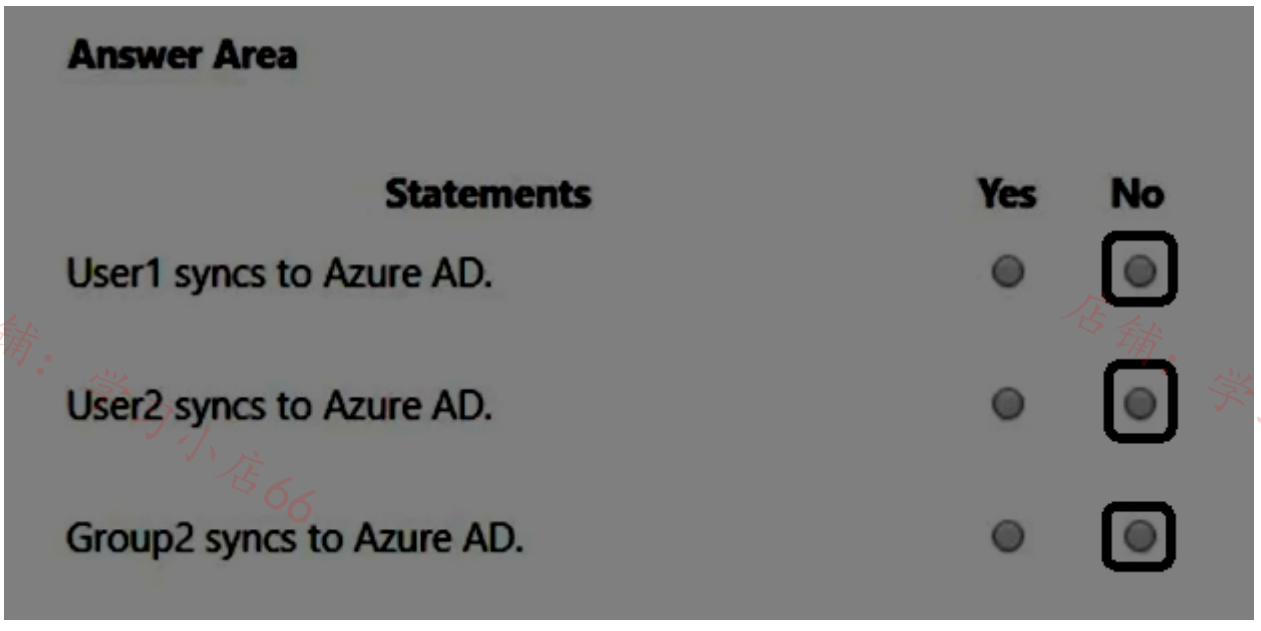
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Correct Answer:



letters1234 1 day, 12 hours ago

User 1 is member of Group 1 and in OU1, user/device filter applies for the user so allows sync
User 2 is member of group 2 and in OU1, user/device filter doesnt inlcude user so doesnt sync
Group 2 is in OU1, meaning it will sync, filter is for devices/users not groups.
Y,N,Y
The nesting comment is saying for the targeted group, if there are members of the group that are security groups, they will be ignored. The filter is for Users/Devices.

upvoted 1 times

Nandokun01 1 week, 3 days ago

OU filters define the connector scope and are an include/exclude conditional statement. Group-based filtering is an object-level condition which evaluates during each connector's sync cycle. If the OU is not in scope the object will never import via its connector so it will not be evaluated during the sync cycles. Casticod is correct

upvoted 1 times

Greatone1 1 week, 6 days ago

No sure answer from previous exam question
https://www.examtopics.com/discussions/microsoft/view/82530-exam-ms-100-topic-3-question-89-discussion/

upvoted 1 times

Casticod 2 weeks, 4 days ago

It should be No, No, No since group is Sales OU which does not synchronize

When using OU-based filtering in conjunction with group-based filtering, the OU(s) where the group and its members are located must be included. (https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-based-filtering)
https://www.examtopics.com/discussions/microsoft/view/82530-exam-ms-100-topic-3-question-89-discussion/

upvoted 3 times

Venusaur 2 weeks, 4 days ago

Filtering already show that OU=SALES will be synced only.
so all answers NO

upvoted 2 times

Mr4D97 2 weeks, 6 days ago

User 1 =Y
User 2 = N (Part of nested group 2 which is not in filter)
Group 2 = N (nested group not included)

upvoted 2 times

osxzvkwpfcfxobqjby 3 weeks, 3 days ago

User1: OU1+Group1 = Y
User2: Group2 not in filter = N
Group2: nested groups are not supported but group1 is in OU1 = Y

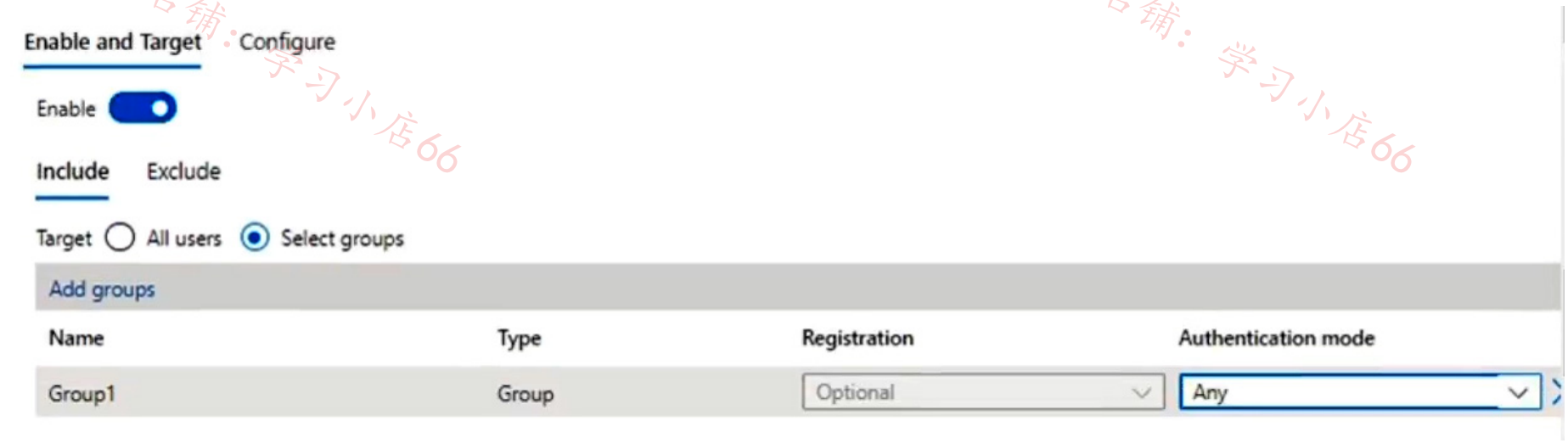
upvoted 1 times

HOTSPOT -

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

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	*None*

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.



Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.

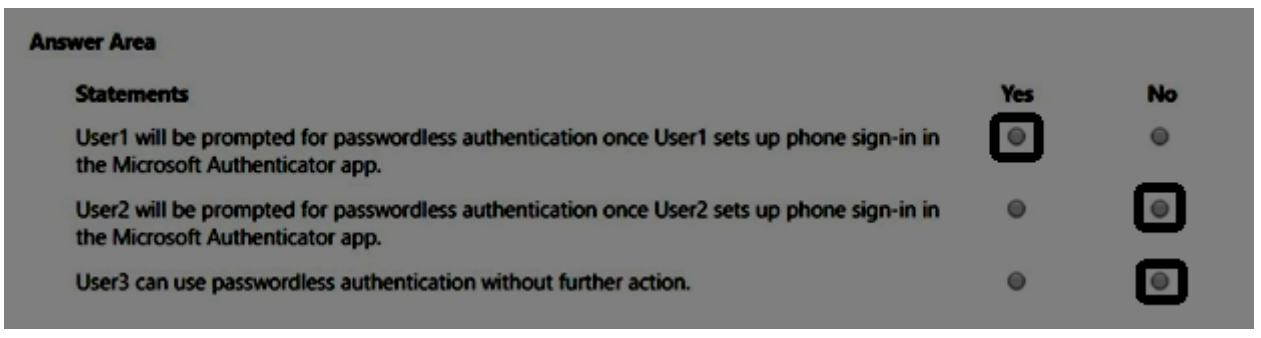
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User3 can use passwordless authentication without further action.	○	○

Correct Answer:



gomezmax 6 days, 20 hours ago

Yes Correct YNN

upvoted 1 times

certma2023 2 weeks, 4 days ago

Answer is correct. YNN.

User1 need to enable the phone sign-in option inside the Microsoft Authenticator app on his/her phone to be able to use passwordless (https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone#enable-phone-sign-in)

User2 is registred for MFA with the Authenticator App but is not targeted by the passwordless configuration (as he/she is not member of group1).

User3 has not registered yet for MFA.

upvoted 3 times

Question #37 *Topic 1*

You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview policies to meet the following requirements:
Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII).
Report on shared documents that contain PII.
What should you create?

A. a data loss prevention (DLP) policy

B. a retention policy

C. an alert policy

D. a Microsoft Defender for Cloud Apps policy

Correct Answer: *A*

Question #38 *Topic 1*

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

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1.
To which resource can you apply Label1?

A. Group1 only

B. Group2 only

C. Site1 only

D. Group1 and Group2 only

E. Group1, Group2, and Site1

Correct Answer: *E*

Dtriminio 3 weeks, 2 days ago

Selected Answer: E

https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites

upvoted 2 times

RAG 3 weeks, 2 days ago

Selected Answer: E

This is the correct see https://learn.microsoft.com/en-gb/purview/sensitivity-labels

upvoted 3 times

Question #39 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You need to meet the following requirements:

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

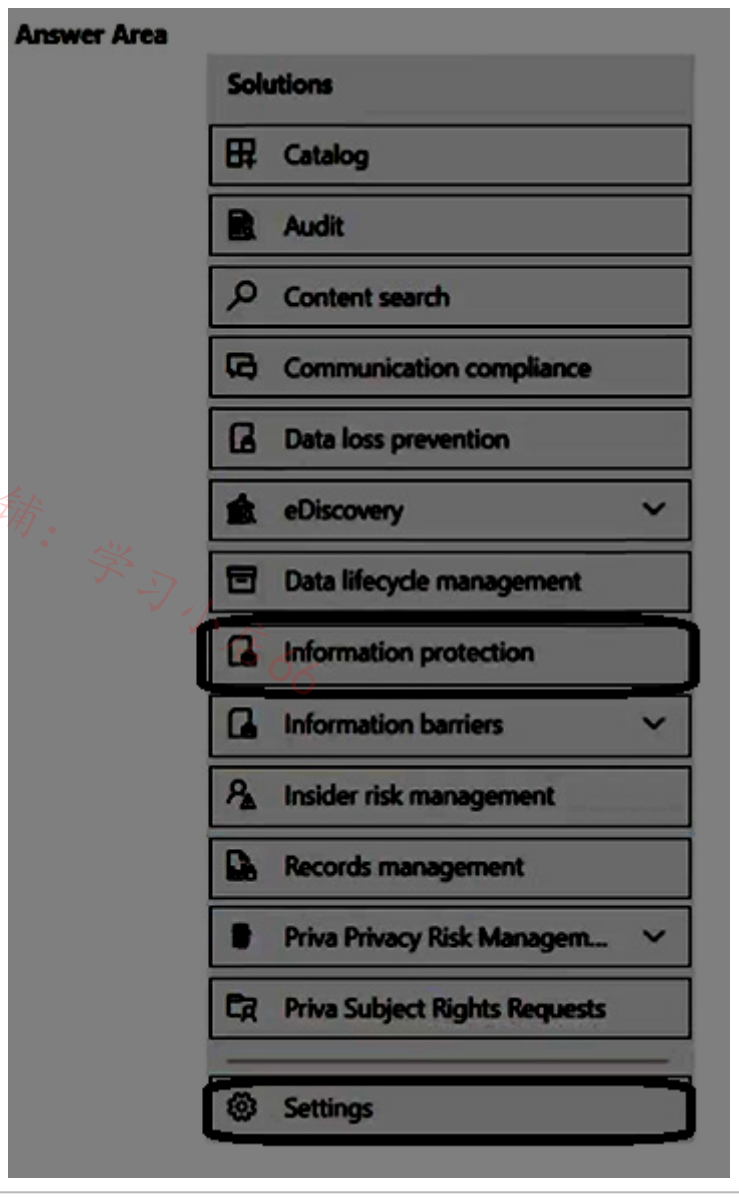
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Correct Answer:



Dtriminio 3 weeks, 2 days ago

Enable co-authoring for files with sensitivity labels

1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
Then select Turn on co-authoring for files with sensitivity labels, and Apply

upvoted 1 times

Question #40 *Topic 1*

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

Which conditions can you use in the DLP rules of the policy?

A. sensitive info types

B. content search queries

C. keywords

D. sensitivity labels

Correct Answer: *C*

SherylD 3 days, 20 hours ago

Selected Answer: A

Tested in Lab Environment, in create a new DLP policy, where locations are set to all, under customize advanced DLP rules > create rule > conditions > add a condition > content contains > add > then only option is "sensitive info types"

upvoted 1 times

gomezmax 1 week, 3 days ago

Should be A

upvoted 1 times

Greatone1 1 week, 6 days ago

Selected Answer: A

A should be the correct answer
https://www.examtopics.com/discussions/microsoft/view/94556-exam-ms-101-topic-3-question-154-discussion/

upvoted 1 times

moshkoshbgosh 3 weeks ago

Selected Answer: A

Sorry mods - can you delete the previous response I posted, the answer should be A, not D.

The reason I'm suggesting A is that this needs to apply to all locations, but sensitivity labels can't be applied to Teams Chat and Channel Messages. I know this is being fussy about the wording, but it would be a way to reduce the choice to one valid option. https://learn.microsoft.com/en-us/purview/dlp-policy-reference#location-support-for-how-content-can-be-defined

upvoted 2 times

certma2023 2 weeks, 4 days ago

I would go for anwser A too. When you select all locations inside the policy configuration (Exchange, Sharepoint, OneDrive, MS Defender for Cloud, Endpoint...), the only options you have on the custom rule is "sensitive info types".

upvoted 1 times

moshkoshbgosh 3 weeks ago

Selected Answer: D

The reason I'm suggesting D is that this needs to apply to all locations, but sensitivity labels can't be applied to Teams Chat and Channel Messages. I know this is being fussy about the wording, but it would be a way to reduce the choice to one valid option. https://learn.microsoft.com/en-us/purview/dlp-policy-reference#location-support-for-how-content-can-be-defined

upvoted 1 times

moshkoshbgosh 3 weeks ago

please delete, it should have said A as per the link.

upvoted 1 times

Dtriminio 3 weeks, 2 days ago

Selected Answer: D

A+D are correct

upvoted 2 times

osxzvkwpfcfxobqjby 3 weeks, 3 days ago

Selected Answer: A

Cannot select right answers: A+D

https://learn.microsoft.com/en-us/purview/dlp-policy-reference#content-contains

upvoted 2 times

Question #41 *Topic 1*

You have a Microsoft 365 E5 tenant.
Users store data in the following locations:

Microsoft Teams -

Microsoft OneDrive -

Microsoft Exchange Online -

Microsoft SharePoint -
You need to retain Microsoft 365 data for two years.
What is the minimum number of retention policies that you should create?

A. 1

B. 2

C. 3

D. 4

Correct Answer: *C*

moshkoshbgosh Highly Voted 3 weeks ago

Selected Answer: C

There's a trap with this one, you need two policies for Teams

1. Teams channel/chats
2. Teams private channel messages
3. OneDrive, SharePoint, Exchange

upvoted 5 times

Nandokun01 Most Recent 1 week, 3 days ago

Aside from adaptive policies you cannot create a policy with Teams channel messages and Teams private channel messages(https://go.microsoft.com/fwlink/?linkid=2220113). Thats 2 for teams and 1 for Exchange mailboxes, SharePoint, OneDrive = C:3

upvoted 2 times

Greatone1 1 week, 6 days ago

Selected Answer: C

3 is the correct answer from previous test

upvoted 1 times

nublit 2 weeks, 3 days ago

Selected Answer: B

In my opinion the correct answer is B.
1 Retention policy for Exchange, OneDrive and SharePoint
1 Retention policy for Teams cannels and chat.

upvoted 2 times

mrac 3 weeks ago

Selected Answer: B

To retain Microsoft 365 data for two years across all the mentioned locations (Microsoft Teams, OneDrive, Exchange Online, and SharePoint), you should create:

B. 2

One Retention Policy for Teams, OneDrive, and SharePoint:
Create a single retention policy that covers Microsoft Teams, OneDrive, and SharePoint. This policy will ensure that data stored in these locations is retained for the specified duration (two years).

Another Retention Policy for Exchange Online:
Create a separate retention policy for Microsoft Exchange Online. This policy will ensure that emails and related data stored in Exchange Online mailboxes are also retained for the same duration (two years).

So, the correct answer is B. 2 retention policies.

upvoted 1 times

osxzvkwpfcfxobqjby 3 weeks, 3 days ago

Selected Answer: B

Just checked.

Policy 1
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Exchange Online

Policy 1
- Microsoft Teams

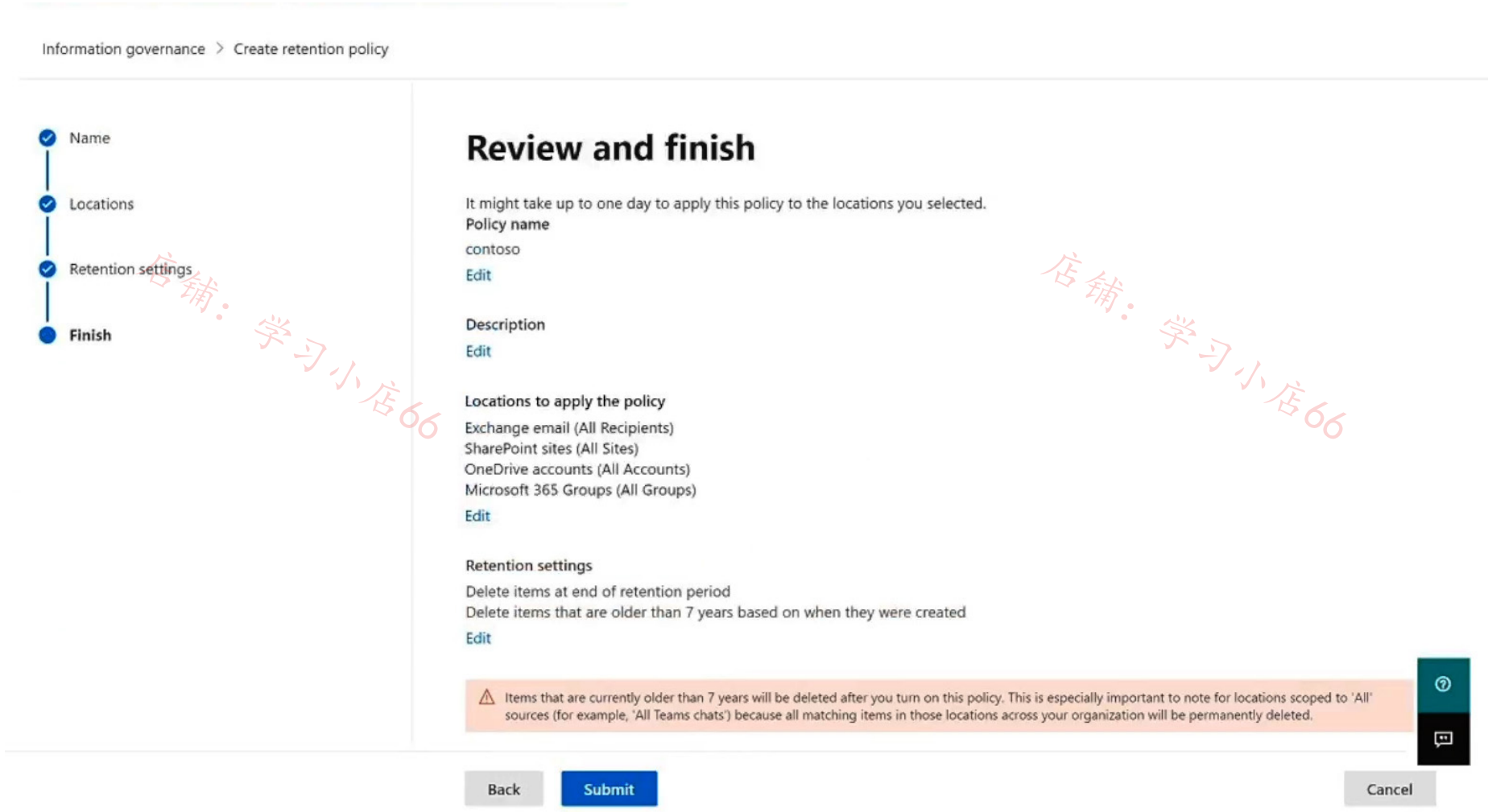
https://learn.microsoft.com/en-us/purview/create-retention-policies?tabs=other-retention
https://compliance.microsoft.com/informationgovernance?viewid=retention

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 tenant.

You plan to create a retention policy 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.

Answer Area

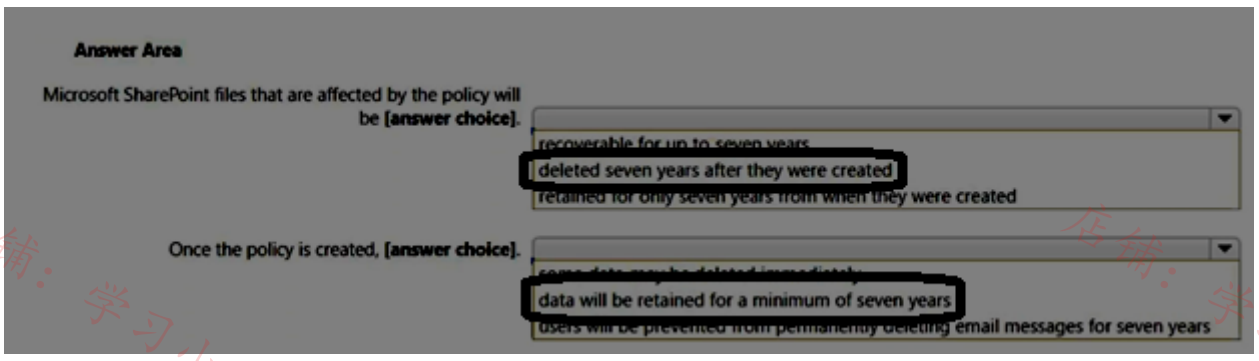
Microsoft SharePoint files that are affected by the policy will be **[answer choice]**.

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, **[answer choice]**.

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Correct Answer:



Mr4D97 Highly Voted 2 weeks, 6 days ago

Deleted 7 years after they were created = Correct
Data will be retained for a min of 7 years = incorrect, data will be stored for a MAX of 7 years
Should be: "Some data will be deleted immediately" (as it says data that is currently older than 7 years will be deleted once this policy is enabled)

upvoted 7 times

gomezmax Most Recent 6 days, 19 hours ago

First one is correct Deleted 7 years after they were created = Correct
but 2nd It's not correct should be some data may be deleted immediately

upvoted 3 times

Question #43 *Topic 1*

You have a Microsoft 365 subscription.
You need to configure a compliance solution that meets the following requirements:
Defines sensitive data based on existing data samples
Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages
Which two components should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a trainable classifier

B. a sensitive info type

C. an insider risk policy

D. an adaptive policy scope

E. a data loss prevention (DLP) policy

Correct Answer: *AE*

Hard1k 2 days, 3 hours ago

Selected Answer: AE

The correct answers are A and E.

A. A trainable classifier is used to define sensitive data based on existing data samples.
E. A data loss prevention (DLP) policy is used to automatically prevent data that matches the samples from being shared externally in Microsoft SharePoint or email messages.
The other options are not necessary for this solution.

B. A sensitive info type is a pre-defined category of sensitive data. This can be used to help you create a DLP policy, but it is not required.
C. An insider risk policy is used to detect and prevent malicious activity by internal users. This is not relevant to the requirement to prevent sensitive data from being shared externally.
D. An adaptive policy scope is used to define the scope of a DLP policy. This can be used to fine-tune the policy to apply to specific users, groups, or locations. However, it is not required for this solution.

upvoted 2 times

Nandokun01 1 week, 3 days ago

"Define from available sample data" means its looking for a trainable classifier as the SIT definition in the DLP policy. Answer is AE(https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide)

upvoted 2 times

gomezmax 1 week, 3 days ago

Agree Should be, BE

upvoted 1 times

Greatone1 1 week, 6 days ago

Selected Answer: BE

From MS 101 exam https://www.examtopics.com/discussions/microsoft/view/103044-exam-ms-101-topic-3-question-161-discussion/

upvoted 2 times

Nandokun01 1 week, 3 days ago

Previous test question most voted answer is insider risk policy which is wrong. "define from available sample data" means its looking for a trainable classifier as the SIT definition in the DLP policy. Answer is AE(https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide)

upvoted 4 times

HOTSPOT -

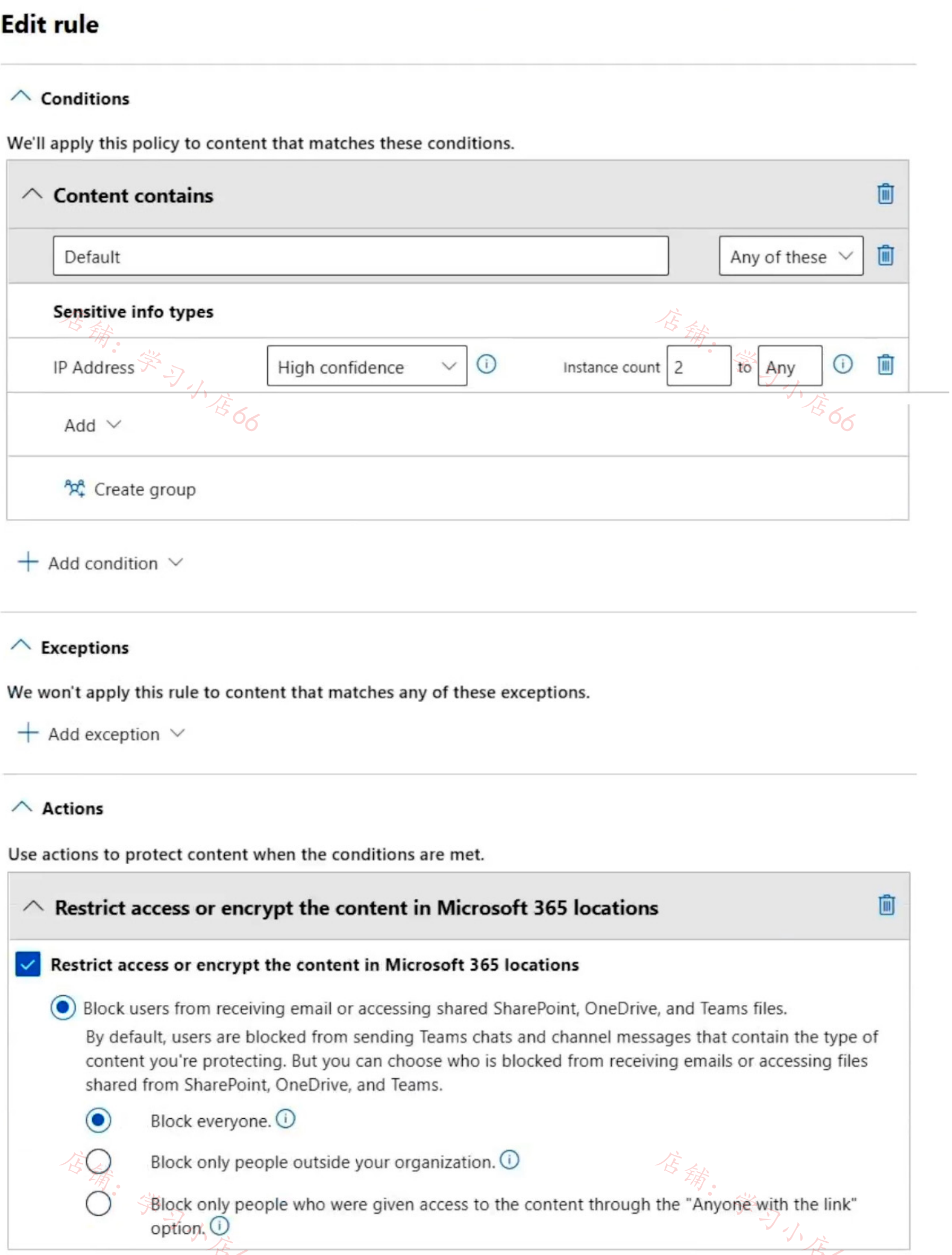
You have a Microsoft 365 subscription that contains a Microsoft SharePoint site named Site1. Site1 has the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.doc	5

For Site1, users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

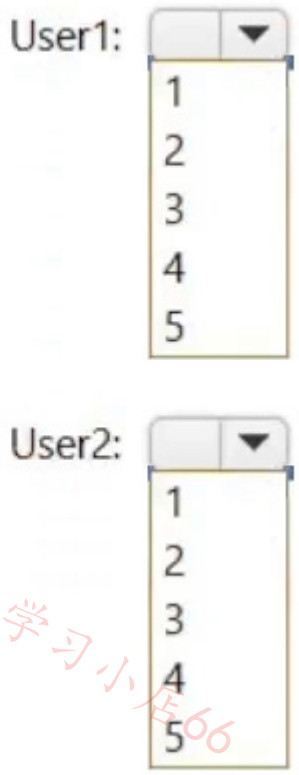
You create a data loss prevention (DLP) policy named Policy1 that contains a rule as shown in the following exhibit.



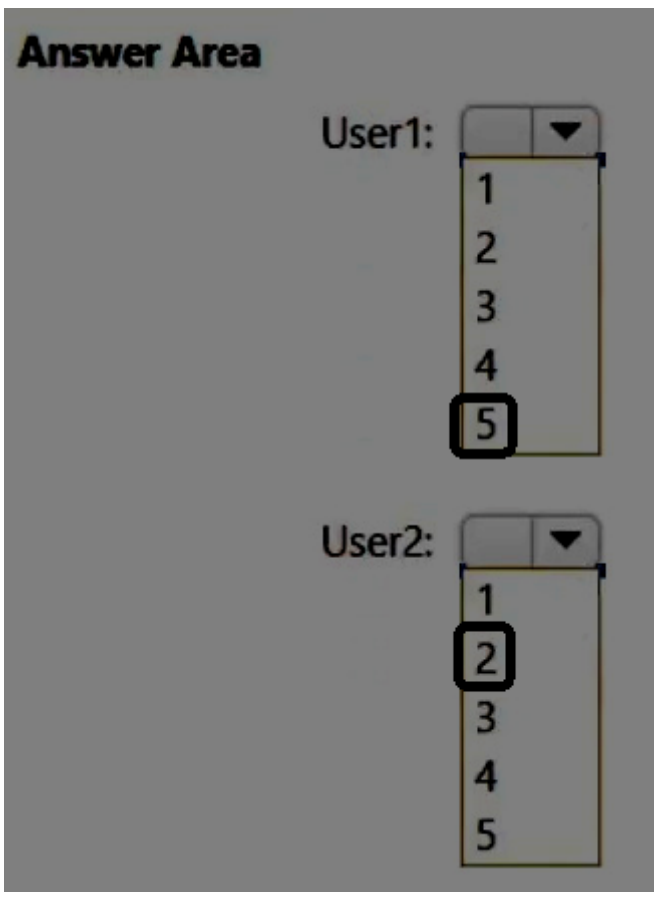
How many files will be visible to User1 and User2 after Policy1 is applied to Site1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:



hogehogehoge 1 week, 4 days ago

I think bmpfile is not target in this rule. So User2 can open file4.

upvoted 3 times

osxzvkwpfcfxobqjby 3 weeks, 3 days ago

Instances found in doc is 2 or more.

User1: can open all files because he is the owner: 5
User2: can open files with less than 2 IPs: 1

https://support.microsoft.com/en-us/office/overview-of-data-loss-prevention-in-sharepoint-server-2016-and-2019-80f907bb-b944-448d-b83d-8fec4abcc24c

upvoted 1 times

Nandokun01 1 week, 3 days ago

file type is .bmp = out of scope (unless OCR is enabled). Answer is 5/2

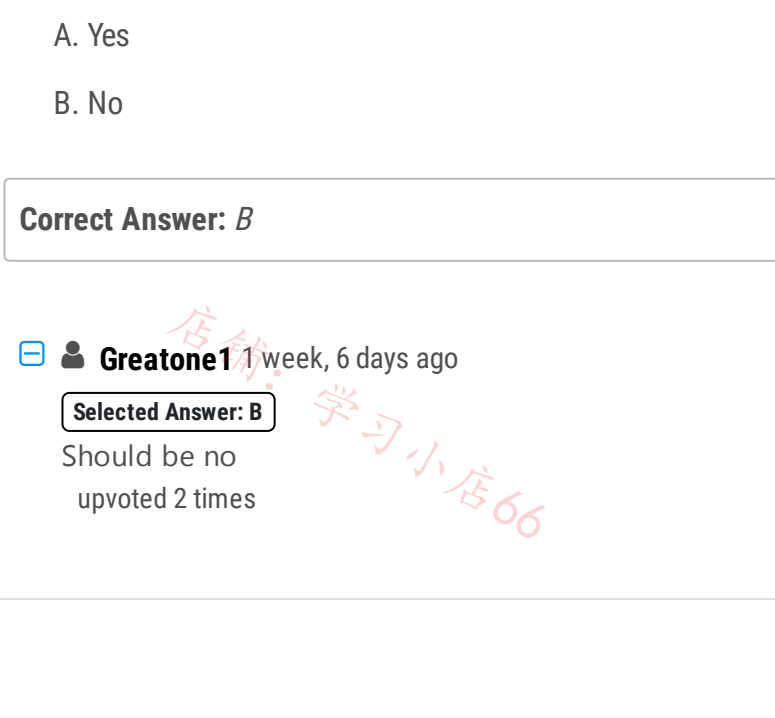
upvoted 2 times

Question #45 *Topic 1*

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.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Greatone1 1 week, 6 days ago

Selected Answer: B

Should be no

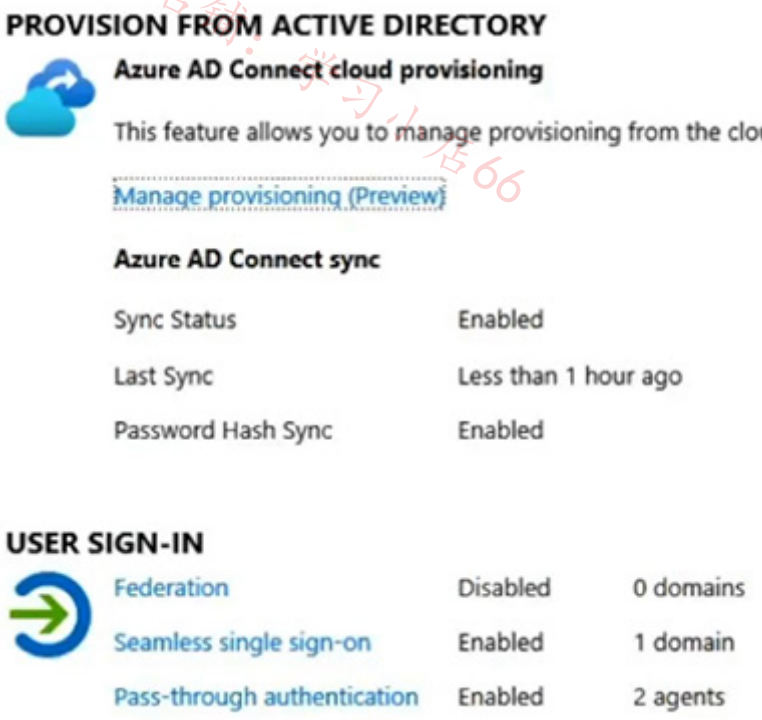
upvoted 2 times

Question #46 *Topic 1*

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. Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*

Greatone1 1 week, 6 days ago

Selected Answer: A

Correct answer is A

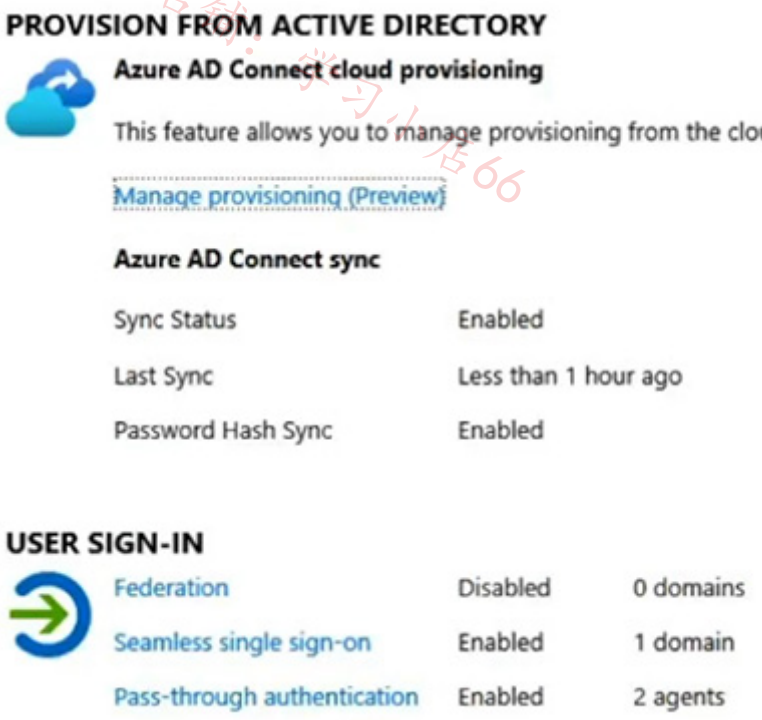
upvoted 2 times

Question #47 *Topic 1*

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. Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*

Greatone1 3 days, 11 hours ago

Looking at previous test no one has a real answer.
https://www.examtopics.com/discussions/microsoft/view/50100-exam-ms-100-topic-2-question-56-discussion/

upvoted 1 times

Greatone1 1 week, 4 days ago

Selected Answer: A

the answer is A.

upvoted 2 times

Question #48 *Topic 1*

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.
Your network contains an Active Directory domain.
You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: You run idfix.exe and export the 10 user accounts.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Takanami 1 week, 4 days ago

To give more context to why Answer is B:
You need to check if that OU containing those 10 users who are not syncronized is part of the OU Filtering option in Azure AD Connect.
Check the box for that OU and save, the sync will start immediately after saving changes in Azure AD Connect.

upvoted 1 times

Greatone1 1 week, 6 days ago

Selected Answer: B

Correct answer should be no

upvoted 1 times

Question #49 *Topic 1*

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.
Your network contains an Active Directory domain.
You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: From Azure AD Connect, you modify the Azure AD credentials.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Question #50 *Topic 1*

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.
Your network contains an Active Directory domain.
You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD.
Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

letters1234 1 day, 11 hours ago

Selected Answer: A

Other two answers for this group are definitely no, this one is yes as the OU may be excluded or not part of what was setup to sync.

upvoted 1 times

Greatone1 1 week, 2 days ago

Selected Answer: A

Correct answer should be yes

upvoted 2 times

osxzvkwpfcfxobqjby 3 weeks, 3 days ago

Selected Answer: A

The other administrator has forgotten/meshedup a rule so you have to create an extra one.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-create-custom-sync-rule

upvoted 1 times

Question #51 *Topic 1*

HOTSPOT -

You have a Microsoft 365 subscription.

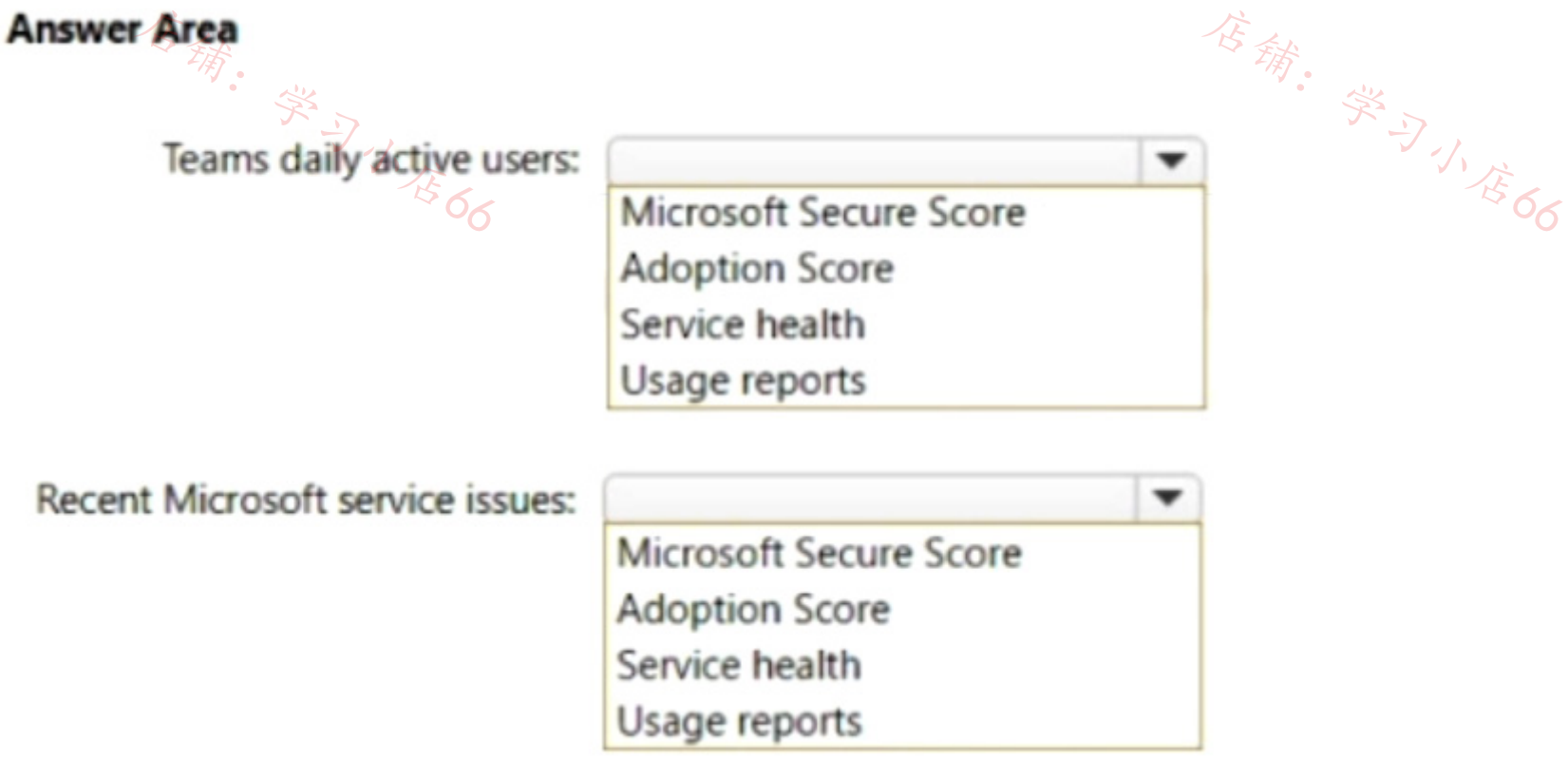
You need to review metrics for the following:

The daily active users in Microsoft Teams

Recent Microsoft service issues -

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

NOTE: Each correct selection is worth one point.



Correct Answer:

gomezmax 6 days, 19 hours ago

Correct

upvoted 2 times

Casticod 2 weeks, 1 day ago

The answer is correct if we take the values offered, but we must be attentive to whether in the exam they add the statistics section of the team administration portal, since (in a period of 7 days) but you can see the activity of one of them by hovering over the selected day or exporting the report to CSV

upvoted 3 times

Question #52 *Topic 1*

DRAG DROP -

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.

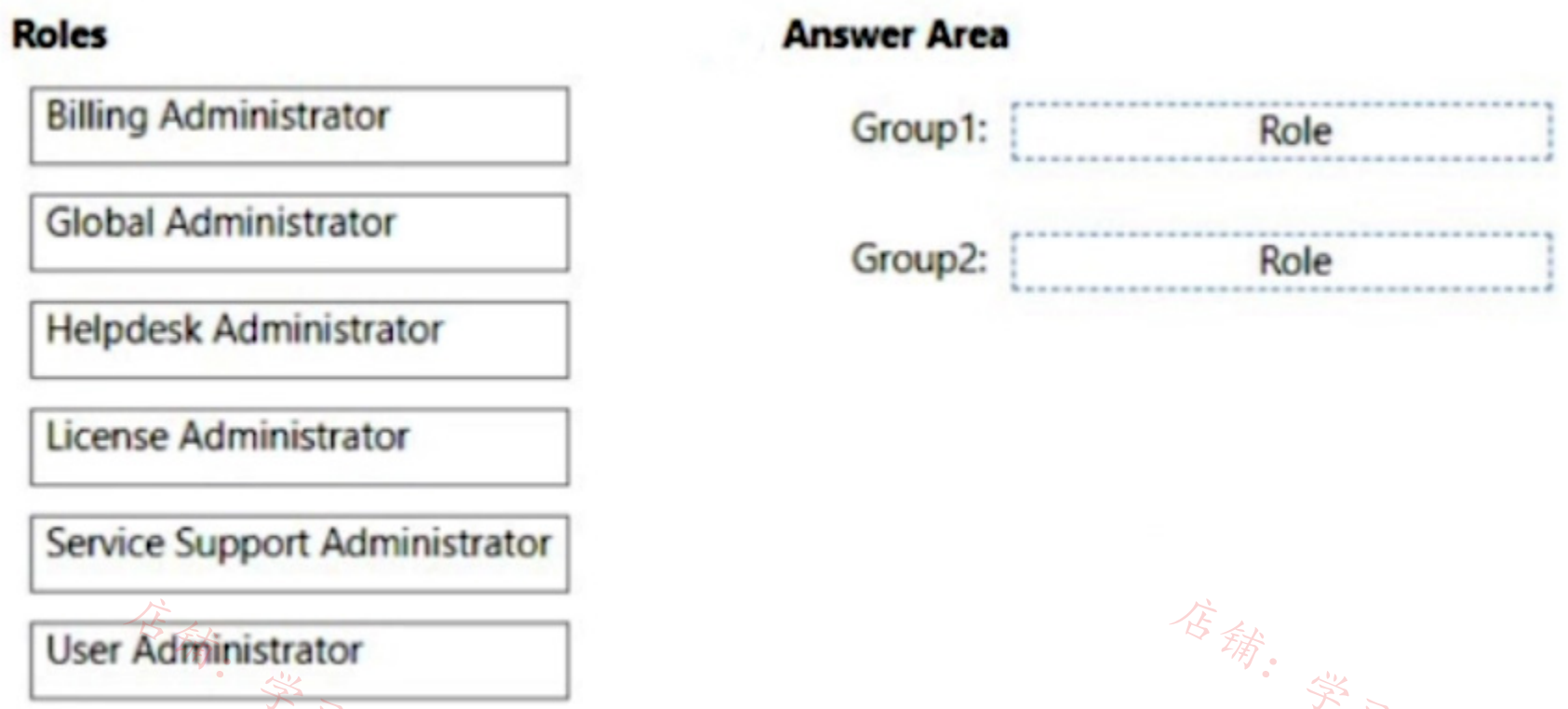
You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	• Manage service requests. • Purchase new services. • Manage subscriptions. • Monitor service health.
Group2	• Assign licenses. • Add users and groups. • Create and manage user views. • Update password expiration policies.

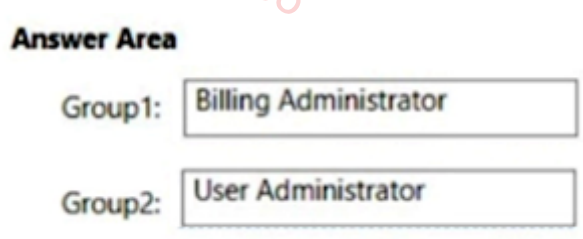
The solution must use the principle of least privilege.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role 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.



Correct Answer:



Casticod 2 weeks, 1 day ago

Correct: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#commonly-used-microsoft-365-admin-center-roles

upvoted 1 times

Question #53 *Topic 1*

You have a Microsoft 365 subscription.

You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

A. 1

B. 2

C. 5

D. 10

Correct Answer: *C*

nsotis28 1 week ago

i created 5 "onMicrosoft" domains and added all of them as additional email address. Also i received a test email on all of them so i'll select 5 Correct answer C

upvoted 2 times

Casticod 1 week, 5 days ago

Selected Answer: C

5 domains https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide#why-do-i-have-an--onmicrosoft-com--domain

upvoted 1 times

Casticod 2 weeks ago

I also don't understand the question, because it says to assign email addresses, that means that aliases count. I only hope that the question does not touch me, but if it does, I would put 5

upvoted 1 times

moshkoshbgosh 2 weeks, 6 days ago

Selected Answer: A

The wording here could be misleading... while 5 is the maximum number of onmicrosoft.com domains that can be added, the questions states "The additional domains must be assignable as email addresses for users" which means we can only have one active... so depending on how you interpret the question it could go either way...

upvoted 1 times

Question #54 *Topic 1*

HOTSPOT -

You have an Azure AD tenant that contains the administrative units shown in the following table.

Name	Members
AU1	User1, User2
AU2	User3

You have the following users:

- A user named User1 that is assigned the Password Administrator for AU1 and AU2.
- A user named User2 that is assigned the User Administrator for AU1.
- A user named User3 that is assigned the User Administrator for the tenant.

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 reset the password of User3.	○	○
User2 can update the display name of User1.	○	○
User1 can reset the password of User2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	◉
User2 can update the display name of User1.	◉	○
User1 can reset the password of User2.	○	◉

nsotis28 1 week ago

provided answer is correct

upvoted 1 times

Greatone1 1 week, 6 days ago

I think this one is correct as an Admin cannot reset another Admins password

upvoted 4 times

Question #55 *Topic 1*

Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.
The domain contains 100 user accounts.
The city attribute for all the users is set to the city where the user resides.
You need to modify the value of the city attribute to the three-letter airport code of each city.
What should you do?

A. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.

B. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.

C. From Windows PowerShell on a domain controller, run the Get-MgUser and Update-MgUser cmdlets.

D. From Azure Cloud Shell, run the Get-MgUser and Update-MgUser cmdlets.

Correct Answer: *A*

Greatone1 1 week, 6 days ago

Selected Answer: A

The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.

upvoted 2 times

HOTSPOT -

Your company has a Microsoft 365 E5 subscription.

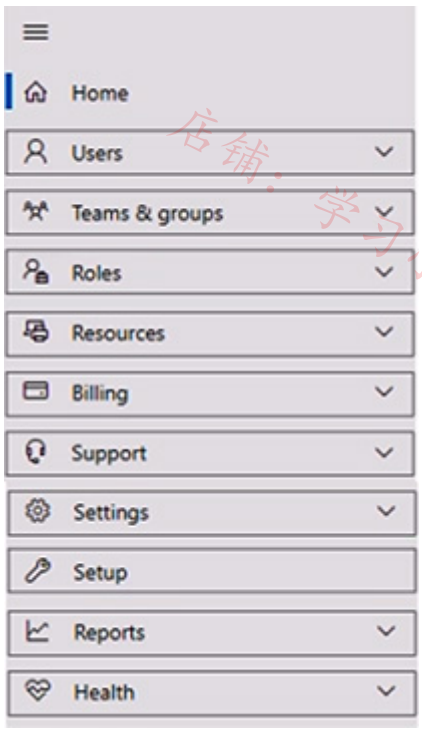
You need to perform the following tasks:

View the Adoption Score of the company.

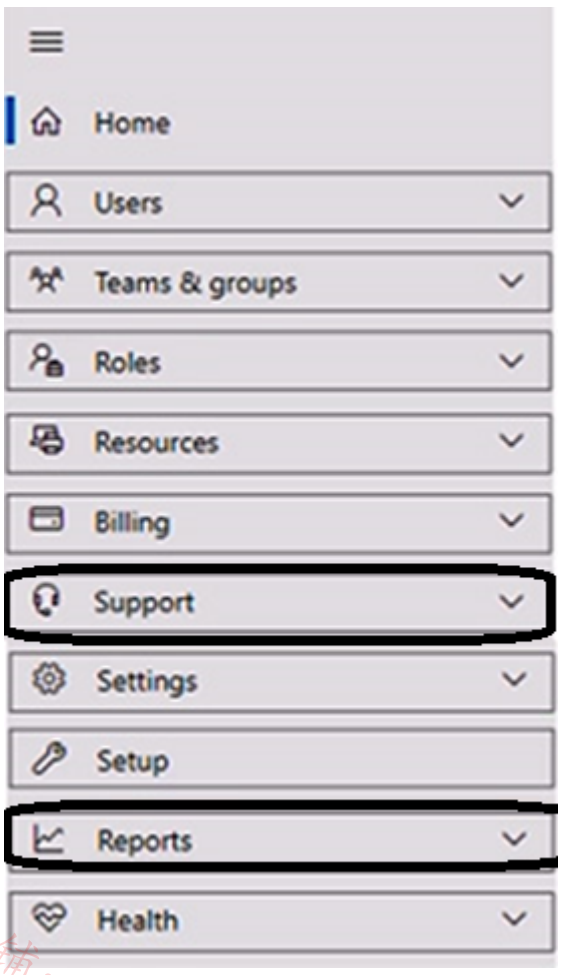
Create a new service request to Microsoft.

Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



gomezmax 1 week, 3 days ago

IT is Reports then Adoption Score

upvoted 2 times

Casticod 2 weeks ago

Correct.
Support to open case a MS
Report to access to the adoption Score

upvoted 2 times

Question #57 *Topic 1*

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

You add another user named User5 to the User Administrator role.

You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Delete User2 and User4 only.

B. Reset the password of User4 only.

C. Reset the password of any user in Azure AD.

D. Delete User1, User2, and User4 only.

E. Reset the password of User2 and User4 only.

F. Delete any user in Azure AD.

Correct Answer: *AE*

Casticod 2 weeks ago

Selected Answer: AE

A and E are correct.

upvoted 1 times

f7d3be6 2 weeks ago

https://www.examtopics.com/discussions/microsoft/view/98896-exam-ms-100-topic-3-question-21-discussion/

upvoted 1 times

Vaati 2 weeks, 3 days ago

Seems Wrong picture indeed

upvoted 2 times

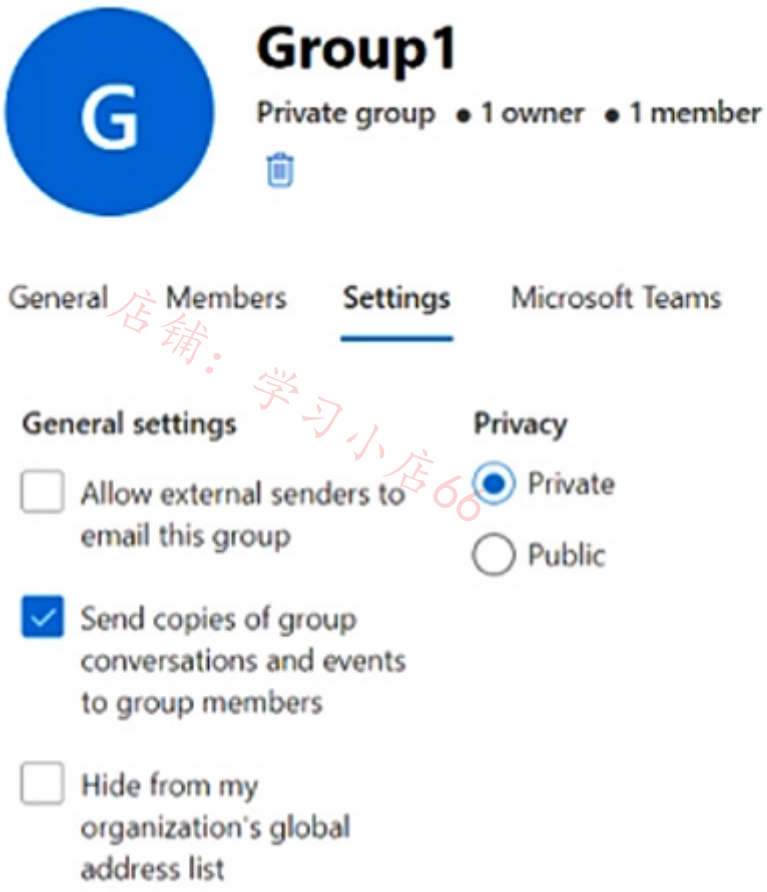
Mustardonk 2 weeks, 4 days ago

Wrong picture?

upvoted 3 times

HOTSPOT -

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



An external user named User1 has an email address of user1@outlook.com.

You need to add User1 to Group1.

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

NOTE: Each correct selection is worth one point.

Answer Area

Action: [ ]
- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal: [ ]
- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

Correct Answer:

Answer Area

Action: [Invite User1 to collaborate with your organization as a guest.]
- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal: [The Microsoft Entra admin center]
- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

Casticod 2 days ago

I just tested in my test tenant that from the Microsoft 365 portal you can create a guest user and add it to an existing group. Therefore in the second section there are 2 possible answers. Microsoft 365 admin center and Entra admin center... OMG I have always done it for Entra and I didn't know this

upvoted 1 times

hogehogehoge 1 week, 4 days ago

I think portal is The Microsoft 365 administrator. Because I test my lab. It is inpossible to change group type in Entra portal.

upvoted 1 times

hogehogehoge 5 days, 14 hours ago

Sorry. This answer is correct. Because Group type is not necessary to change.

upvoted 1 times

Greatone1 1 week, 6 days ago

Given answer is correct
https://www.examtopics.com/discussions/microsoft/view/94423-exam-ms-100-topic-3-question-94-discussion/

upvoted 2 times

Question #59 *Topic 1*

You have a Microsoft 365 subscription that contains a user named User1.
User1 requires admin access to perform the following tasks:
Manage Microsoft Exchange Online settings.
Create Microsoft 365 groups.
You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.
What should you use?

A. Azure AD Identity Protection

B. Microsoft Entra Verified ID

C. Conditional Access

D. Azure AD Privileged Identity Management (PIM)

Correct Answer: *D*

HOTSPOT -

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

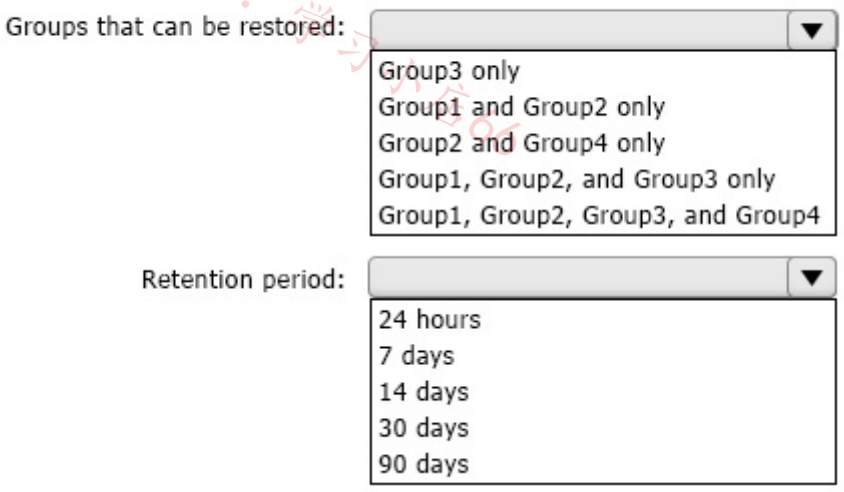
Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

All the groups are deleted.

Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.

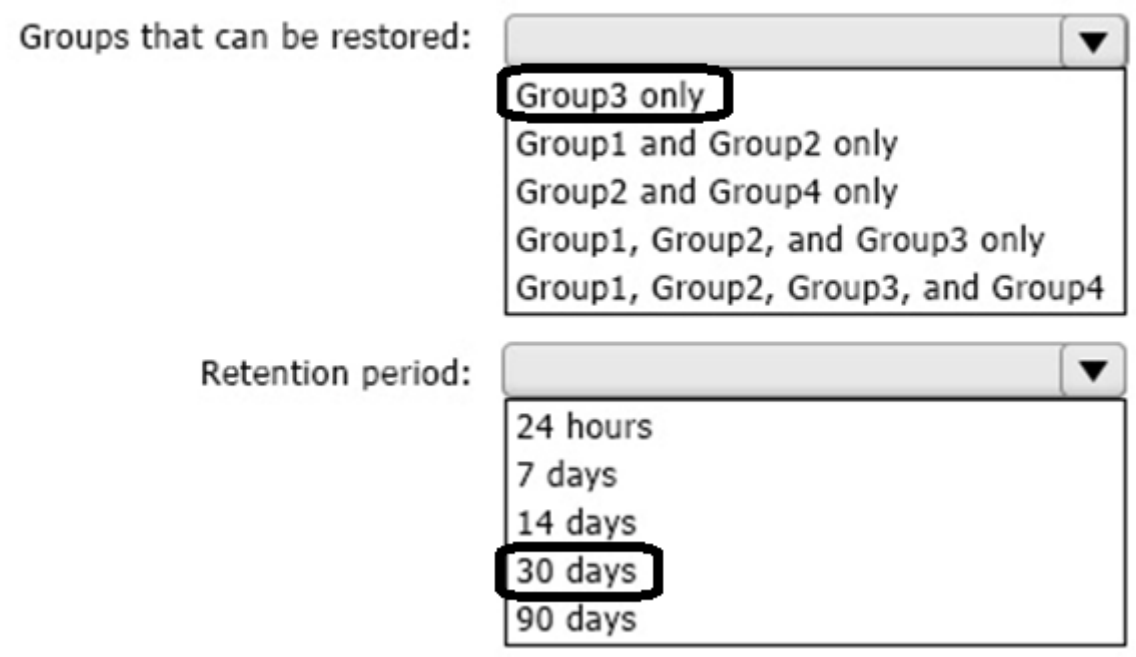
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Greatone1 1 day, 14 hours ago

Letters already provided the answer only m 365 groups can be restored not security or distribution groups
This functionality is restricted exclusively to Microsoft 365 groups in Azure AD. It isn't available for security groups and distribution groups. Please note that the 30-day group restoration period isn't customizable.

upvoted 1 times

letters1234 2 days, 12 hours ago

When you delete a Microsoft 365 group in Azure Active Directory (Azure AD), part of Microsoft Entra, the deleted group is retained but not visible for 30 days from the deletion date. This behavior is so that the group and its contents can be restored if needed. This functionality is restricted exclusively to Microsoft 365 groups in Azure AD. It isn't available for security groups and distribution groups.

Mail-enabled security group is still a security group

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-restore-deleted

upvoted 1 times

Greatone1 1 week ago

Should be group 3 and 30 days

upvoted 2 times

DiligentSam 1 week, 1 day ago

From ChatGPT， Mail-enabled security， Microsoft 365 and Distribution can be restored.
but i can't find this answer

Q2 30 days
upvoted 1 times

Greatone1 1 week, 6 days ago

Deleted users and deleted Office 365 groups are available for restore for 30 days. You cannot restore a deleted security group.
upvoted 2 times

HOTSPOT -

You have a Microsoft 365 E5 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

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

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

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

NOTE: Each correct selection is worth one point.

Answer Area

A user that is assigned the Global Administrator role as active **[answer choice]**. [ ]
- will lose the role after eight hours
- can reactivate the role every eight hours
- can reactivate the role every 15 days
- will lose the role after 15 days

You can make the Global Administrator role available to activation requests **[answer choice]**. [ ]
- for up to eight hours
- for up to three months
- for up to 15 days
- until the requests are revoked manually

Correct Answer:

Answer Area

A user that is assigned the Global Administrator role as active **[answer choice]**. [will lose the role after eight hours]
- will lose the role after eight hours
- can reactivate the role every eight hours
- can reactivate the role every 15 days
- will lose the role after 15 days

You can make the Global Administrator role available to activation requests **[answer choice]**. [for up to three months]
- for up to eight hours
- for up to three months
- for up to 15 days
- until the requests are revoked manually

spectre786 5 days, 4 hours ago

First one : will lose the role after 8 hours AND can reactivate every 8 hours
Right ?

upvoted 2 times

Casticod 6 days, 17 hours ago

First Option Correct 8 Hours
The second options are 15 Days... https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-renew-extend

upvoted 3 times

nsotis28 1 week ago

first is correct - will lose the role after 8 hours
second is questionable -- why not 15 days ?

upvoted 3 times

cb0900 4 days, 1 hour ago

Re: the second question, agree it would be 15 days in this case.
The first question states "A user that is assigned the the Global Administrator role as active" and the active assignment is set to expire after 15 days.

upvoted 2 times

Question #62 *Topic 1*

HOTSPOT -

You have a Microsoft 365 subscription.

A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
[ ▼ ] -Scopes User.ReadWrite.All, Organization.Read.All
      Connect-AzureAD
      Connect-MgGraph
      Connect-MSOLService

$E3 = [ ▼ ] | Where SkuPartNumber -eq 'EnterprisePack'
      Get-AzureADUser
      Get-MgSubscribedSku
      Get-MSOLAccountSKU

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)

[ ▼ ] -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
      Set-AzureADUser
      Set-MgUserLicense
      Set-MSOLUser
```

Correct Answer:

Answer Area

```
[ ▼ ] -Scopes User.ReadWrite.All, Organization.Read.All
      Connect-AzureAD
      Connect-MgGraph
      Connect-MSOLService

$E3 = [ ▼ ] | Where SkuPartNumber -eq 'EnterprisePack'
      Get-AzureADUser
      Get-MgSubscribedSku
      Get-MSOLAccountSKU

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)

[ ▼ ] -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
      Set-AzureADUser
      Set-MgUserLicense
      Set-MSOLUser
```

929826d 1 week, 6 days ago

Correct

https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide

upvoted 1 times

Question #63 *Topic 1*

You have a Microsoft E5 subscription.
You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time.
What should you implement?

A. Azure AD Privileged Identity Management (PIM)

B. a conditional access policy

C. a communication compliance policy

D. Azure AD Identity Protection

E. groups that have dynamic membership

Correct Answer: *A*

Question #64 *Topic 1*

You have a Microsoft 365 subscription.
You suspect that several Microsoft Office 365 applications or services were recently updated.
You need to identify which applications or services were recently updated.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. From the Microsoft 365 admin center, review the Service health blade.

B. From the Microsoft 365 admin center, review the Message center blade.

C. From the Microsoft 365 admin center, review the Products blade.

D. From the Microsoft 365 Admin mobile app, review the messages.

Correct Answer: *BD*

Hard1k 13 hours ago

Selected Answer: AB

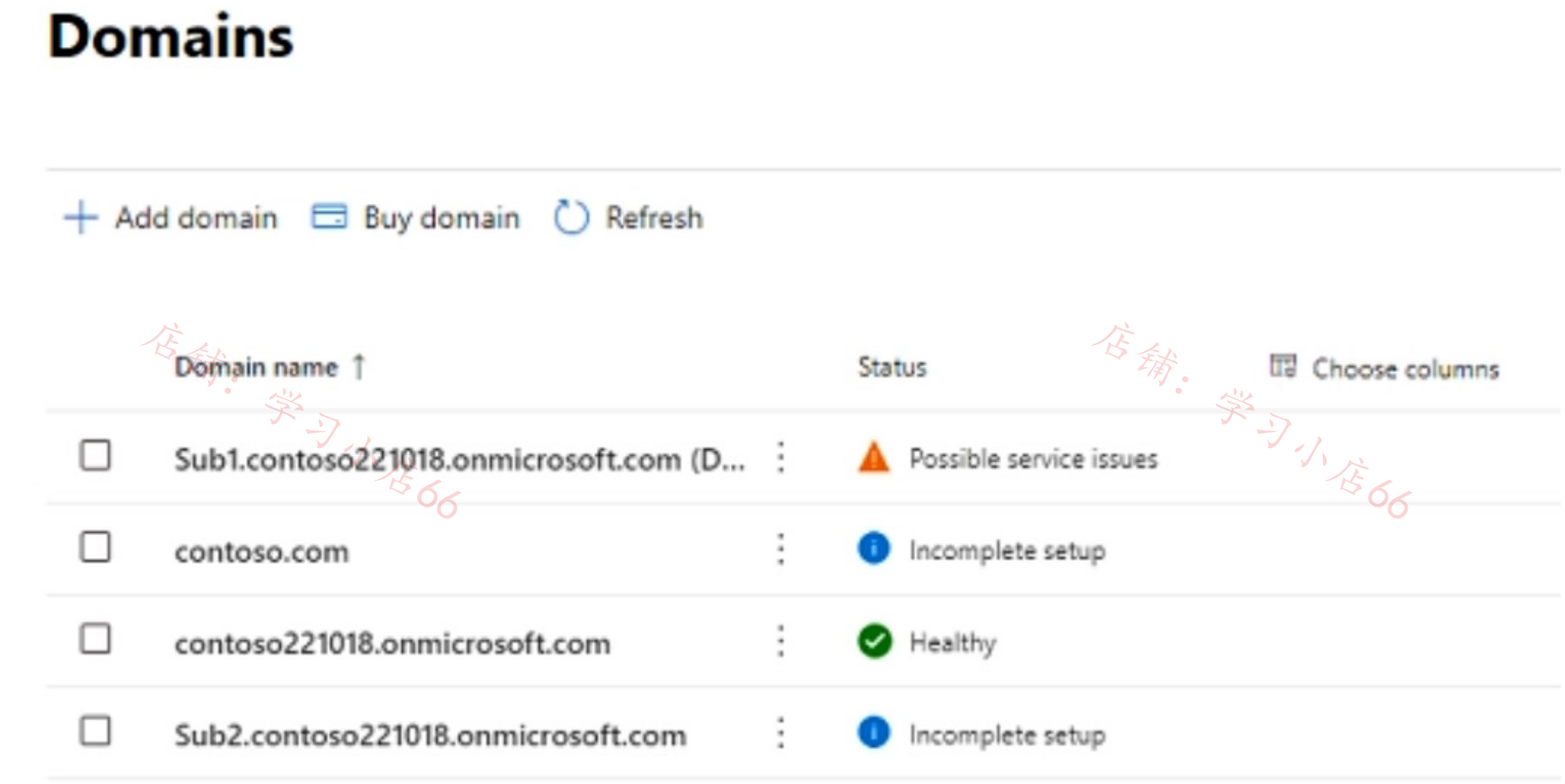
A. From the Microsoft 365 admin center, review the Service health blade. The Service health blade in the Microsoft 365 admin center provides information about the status of Microsoft 365 services. If a service has been recently updated, it will be listed on the Service health blade.

B. From the Microsoft 365 admin center, review the Message center blade. The Message center blade in the Microsoft 365 admin center provides information about important messages from Microsoft. If there have been any recent updates to Microsoft Office 365 applications or services, a message will be posted in the Message center.

The other options are not correct. Option C, reviewing the Products blade in the Microsoft 365 admin center, will not show you which applications or services have been recently updated. Option D, reviewing the messages in the Microsoft 365 Admin mobile app, will only show you messages that have been sent to you personally.

upvoted 1 times

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.



Which domain name suffixes can you use when you create users?

A. only Sub1.contoso221018.onmicrosoft.com

B. onlycontoso221018.onmicrosoft.com and Sub2.contoso221018.onmicrosoft.com

C. only contoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com

D. all the domains in the subscription

Correct Answer: *B*

DiligentSam 1 week, 1 day ago

my answer
Sub1.contoso221018.onmicrosoft.com - Possible service issues
contoso221018.onmicrosoft.com - healthy

upvoted 2 times

nsotis28 1 week, 2 days ago

Domains with status "incomplete setup" can not be used

upvoted 2 times

Casticod 1 week, 6 days ago

anything it's correct think that onlycontoso221018.onmicrosoft.com and Sub1.contoso221018.onmicrosoft.com
until the domain is finished configuring the domain, accounts cannot be assigned to users, in a healthy state or with possible malfunctions if it can be

upvoted 1 times

Casticod 1 week, 5 days ago

In the exam Ms-100 exist a similar question, and the comments content excelent explaineds
https://www.examtopics.com/discussions/microsoft/view/49388-exam-ms-100-topic-3-question-75-discussion/

upvoted 2 times

Vaati 2 weeks, 3 days ago

Why B?

upvoted 2 times

Question #66 *Topic 1*

You have a Microsoft 365 subscription.
You plan to implement Microsoft Purview Privileged Access Management.
Which Microsoft Office 365 workloads support privileged access?

A. Microsoft Exchange Online only

B. Microsoft Teams only

C. Microsoft Exchange Online and SharePoint Online only

D. Microsoft Teams and SharePoint Online only

E. Microsoft Teams, Exchange Online, and SharePoint Online

Correct Answer: *A*

DiligentSam 1 week, 1 day ago

From ChatGPT， answser is E
The documentation also says:

"When will privileged access support Office 365 workloads beyond Exchange?
Privileged access management will be available in other Office 365 workloads soon. Visit the Microsoft 365 Roadmap for more details."
upvoted 1 times

Greatone1 1 week, 6 days ago

Selected Answer: A
A is the correct answer
Source: https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management?view=o365-worldwide
upvoted 2 times

certma2023 2 weeks, 3 days ago

Selected Answer: A
Answer A.

PAM only works with Exchange Online at that time. Based on my test you see only Exchange roles inside the O365 Admin Portal (Settings -> Org Settings -> Security & Privacy -> Privileged Access)

The documentation also says:

"When will privileged access support Office 365 workloads beyond Exchange?
Privileged access management will be available in other Office 365 workloads soon. Visit the Microsoft 365 Roadmap for more details."

https://learn.microsoft.com/en-us/purview/privileged-access-management
upvoted 3 times

mrac 2 weeks, 6 days ago

Selected Answer: E
Microsoft Purview Privileged Access Management (PAM) helps you manage, control, and monitor access within Microsoft 365. It's designed to manage privileged access for various Microsoft Office 365 workloads, including Microsoft Teams, Exchange Online, and SharePoint Online.

So, the correct answer is E. Microsoft Teams, Exchange Online, and SharePoint Online.
upvoted 3 times

Question #67 *Topic 1*

HOTSPOT -

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

Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	*None*

You plan to provide User4 with early access to Microsoft 365 feature and service updates.

You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

Correct Answer:

Answer Area

Microsoft 365 setting:
- Office installation options
- **Privileged access**
- Release preferences

User:
- User1 only
- User2 only
- **User3 only**
- User1 and User2 only
- User1 and User3 only

certma2023 Highly Voted 2 weeks, 3 days ago

Answer is wrong.

To have new features & updates on all users or some/targeted users you need to configure "release preference" for the entire organization/tenant. Only the Global Admins can change this.

https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide#set-up-the-release-option-in-the-admin-center

upvoted 6 times

nsotis28 Most Recent 1 week, 2 days ago

release preferences
user1

upvoted 3 times

Casticod 6 days, 16 hours ago

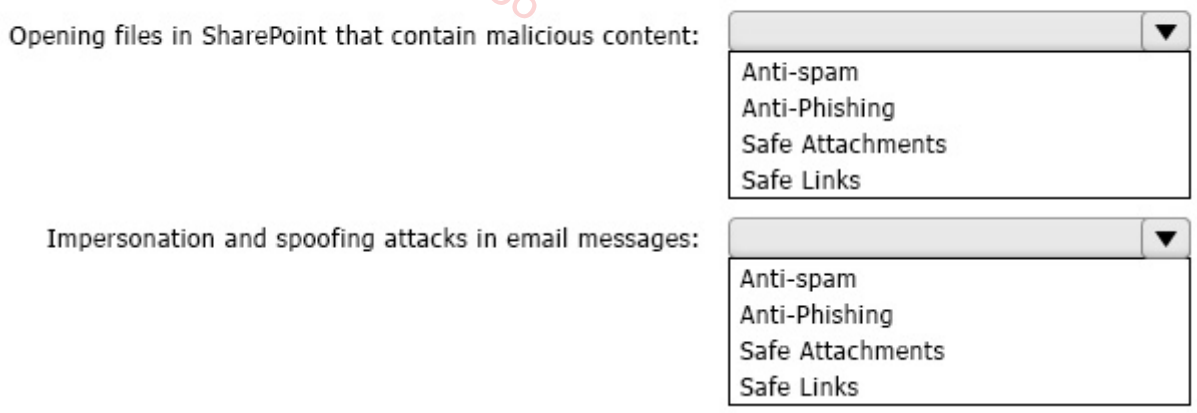
Me too
https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide

upvoted 2 times

Question #68 *Topic 1*

HOTSPOT -
You have a Microsoft 365 subscription.
You are planning a threat management solution for your organization.
You need to minimize the likelihood that users will be affected by the following threats:
Opening files in Microsoft SharePoint that contain malicious content
Impersonation and spoofing attacks in email messages
Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

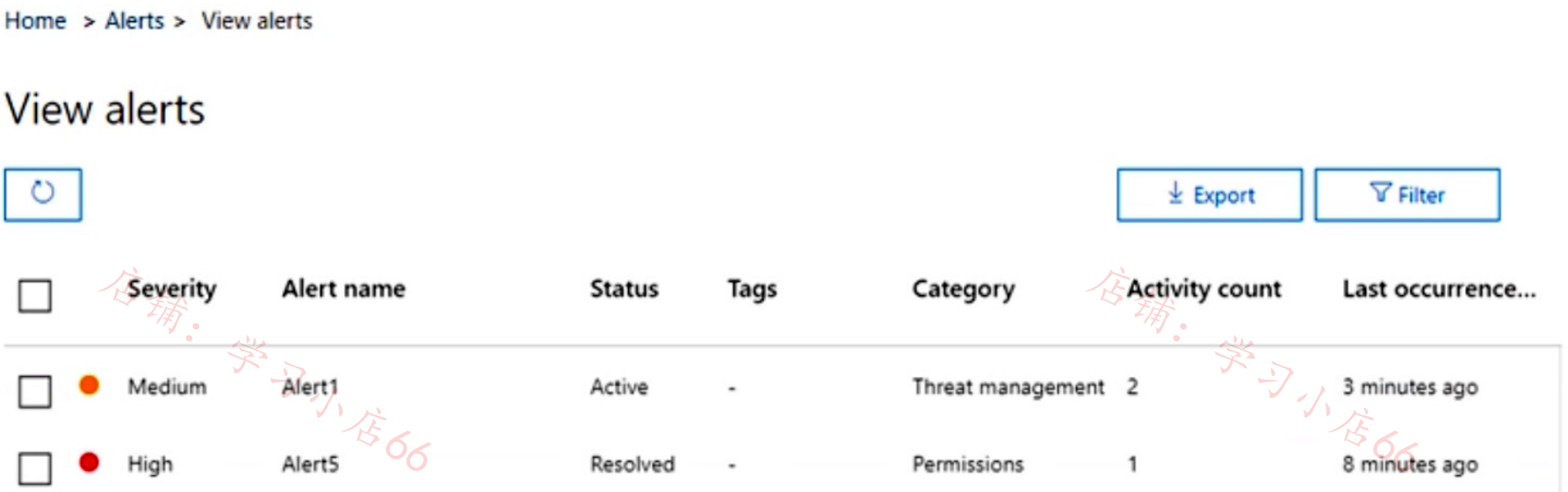
Answer Area

Greatone1 1 week, 6 days ago
Yes correct
safe attachments
anti-phishing
upvoted 2 times

HOTSPOT -

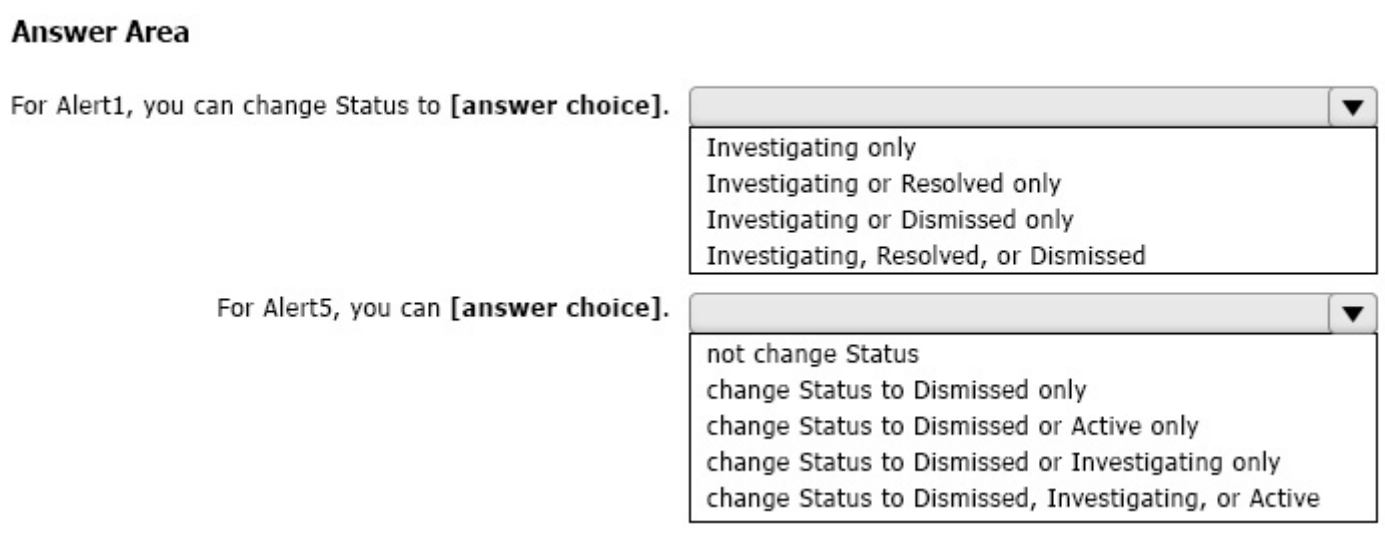
You have a Microsoft 365 E5 tenant.

You have the alerts shown in the following exhibit.

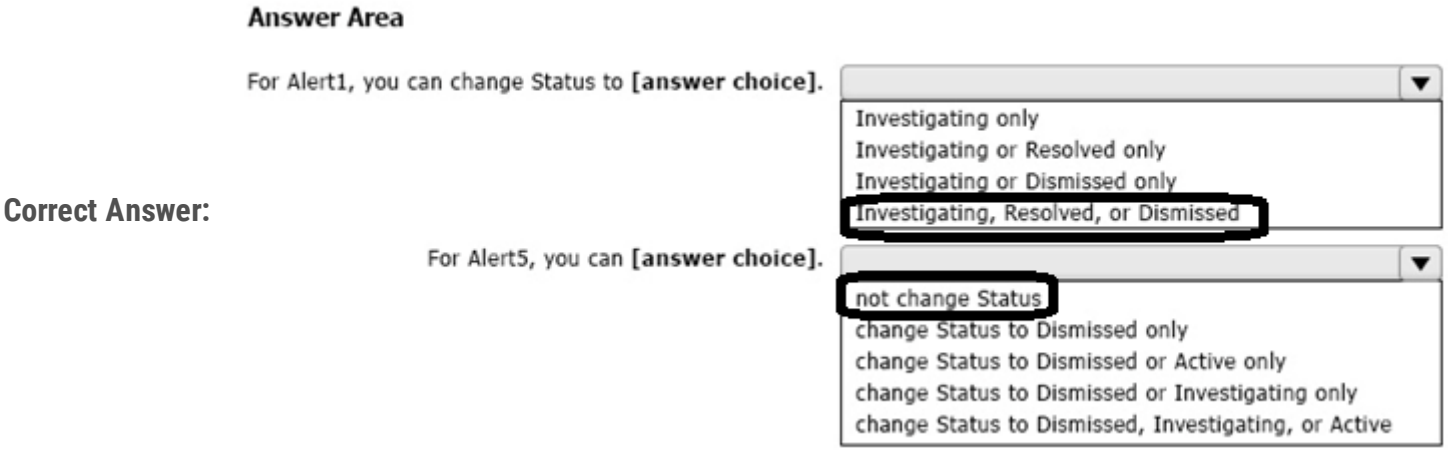


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Correct Answer:



Question #70 *Topic 1*

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.
Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. advanced hunting

B. security reports

C. digital certificate assessment

D. device discovery

E. attack surface reduction (ASR)

Correct Answer: *BE*

Hard1k 12 hours, 41 minutes ago

Selected Answer: BE

Correct answers

upvoted 1 times

letters1234 2 days, 7 hours ago

Can only see ASR and reports on the features for Defender P1
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

upvoted 1 times

Greatone1 1 week, 6 days ago

Selected Answer: BE

Answer is correct
https://www.examtopics.com/discussions/microsoft/view/94078-exam-ms-101-topic-2-question-123-discussion/

upvoted 2 times

Question #71 *Topic 1*

You are reviewing alerts in the Microsoft 365 Defender portal.
How long are the alerts retained in the portal?

A. 30 days

B. 60 days

C. 3 months

D. 6 months

E. 12 months

Correct Answer: *C*

Casticod 4 days, 16 hours ago

Selected Answer: C

Correct https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention?view=o365-worldwide

upvoted 1 times

Question #72 *Topic 1*

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.

What is the longest time range that can be included in the report?

A. 1 day

B. 7 days

C. 30 days

D. 90 days

Correct Answer: *C*

Casticod 4 days, 16 hours ago

Selected Answer: C

Correct https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-users?view=o365-worldwide#timeline

upvoted 1 times

Question #73 *Topic 1*

HOTSPOT -

You have a Microsoft 365 subscription.

You deploy the anti-phishing policy shown in the following exhibit.

Phishing threshold and protections

Phishing threshold
1 - Standard

User impersonation protection
- On for 0 user(s)

Domain impersonation protection
- Off for owned domains
- Off - 0 domain(s) specified

Trusted impersonated senders and domains
- Off

Mailbox intelligence
- On

Mailbox intelligence for impersonations
- Off (Mailbox intelligence must be turned on to access this)

Spoof intelligence
- Off

Edit protection settings

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

NOTE: Each correct selection is worth one point.

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the **[answer choice]** setting.

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the **[answer choice]** setting.

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence

Correct Answer:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the **[answer choice]** setting.

- Add trusted senders and domains
- Enable domains to protect
- **Enable users to protect**
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the **[answer choice]** setting.

- **Add trusted senders and domains**
- Enable intelligence for impersonation protection
- Enable spoof intelligence

letters1234 2 days, 6 hours ago

Would probably go for Phishing threshold as looking at the policy in security.microsoft.com / policies & rules / threat policies:

Phishing threshold & protection
-Phishing threshold
1 - Standard
-User impersonation protection
Off - 0 sender(s) specified
-Domain impersonation protection
Off for owned domains
Off - 0 domain(s) specified

Would most likely want to set Domain Impersonation Protection to On for owned domains and configure that.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about?view=o365-worldwide#domain-impersonation-protection

upvoted 1 times

Question #74 *Topic 1*

HOTSPOT -

You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint device groups shown in the following table.

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped devices (default)	Last	*Not applicable*

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

To which device group will each computer be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Computer1-London: [▼]
- Group1
- Group2
- Group3
- Ungrouped devices

Server1-London: [▼]
- Group1
- Group2
- Group3
- Ungrouped devices

Correct Answer:

Answer Area

Computer1-London: [▼]
- Group1
- Group2
- Group3
- Ungrouped devices

Server1-London: [▼]
- Group1
- Group2
- Group3
- Ungrouped devices

Greatone1 1 week, 6 days ago

Answer is correct. Devices can only be added to one group. They get added to the highest rank lowest number if they match multiple groups.

upvoted 1 times

Question #75 *Topic 1*

DRAG DROP -

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

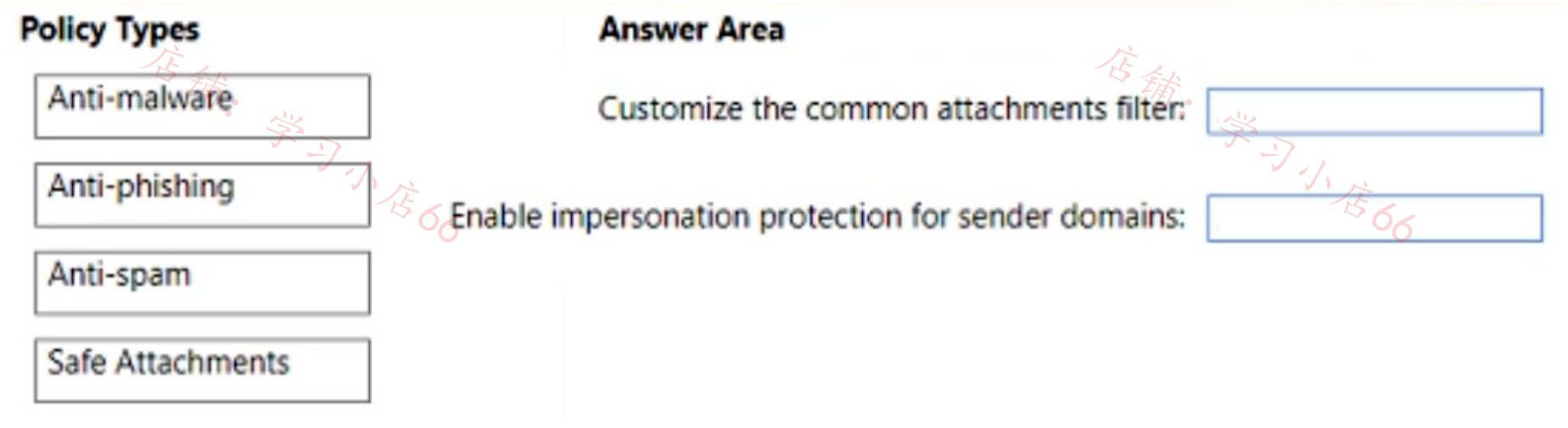
You need to configure policies to meet the following requirements:

Customize the common attachments filter.

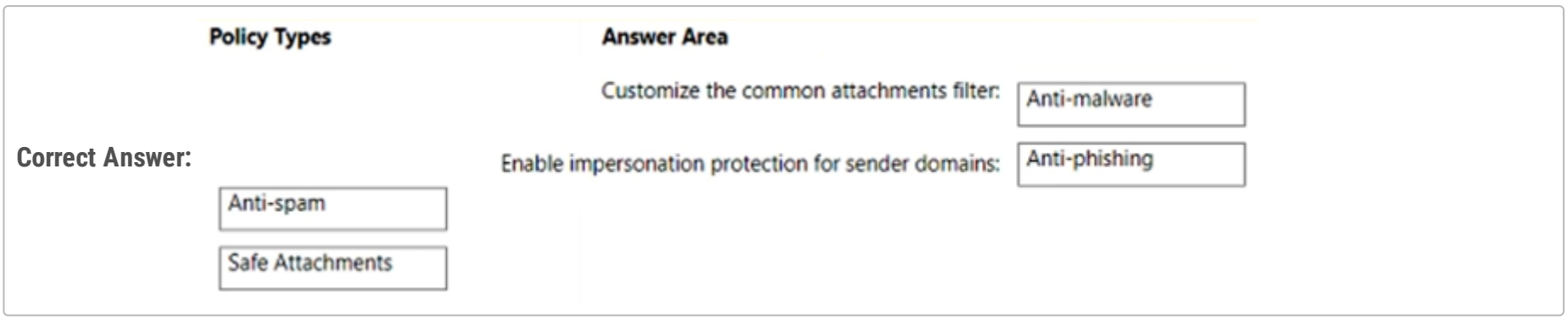
Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type 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.



Correct Answer:



f7d3be6 2 weeks ago

Correct Antimalware ,anti-phishing https://answers.microsoft.com/en-us/msoffice/forum/all/impersonation-protection/97b82164-5331-4ee6-97e0-423f17c55399

upvoted 2 times

Question #76 *Topic 1*

You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?

A. User1

B. User2

C. User3

D. User4

Correct Answer: *A*

letters1234 2 days, 6 hours ago

Selected Answer: C

Security reader Security readers can perform the following tasks:
- View a list of onboarded devices
- View security policies
- View alerts and detected threats
- View security information and reports

Security readers can't add or edit security policies, nor can they onboard devices.

upvoted 1 times

mccheesey 1 week, 3 days ago

Selected Answer: C

This should be C I think...

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide

"Security Reader - Members have read-only access to many security features of Identity Protection Center, Privileged Identity Management, Monitor Microsoft 365 Service Health, and the Defender and compliance portals. "

I see nothing in this statement or anywhere around the Security Reader role in this article indicating they wouldn't be able to view incidents within that portal.

upvoted 1 times

Greatone1 1 week, 4 days ago

https://www.examtopics.com/discussions/microsoft/view/49358-exam-ms-101-topic-2-question-27-discussion/

upvoted 2 times

Greatone1 1 week, 6 days ago

Selected Answer: A

A is correct
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

upvoted 1 times

Casticod 1 week, 6 days ago

Selected Answer: C

Only view security incident... Security reader.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-roles-permissions?view=o365-worldwide&tabs=M365Admin

upvoted 1 times

Question #77 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

Block a vulnerable app until the app is updated.

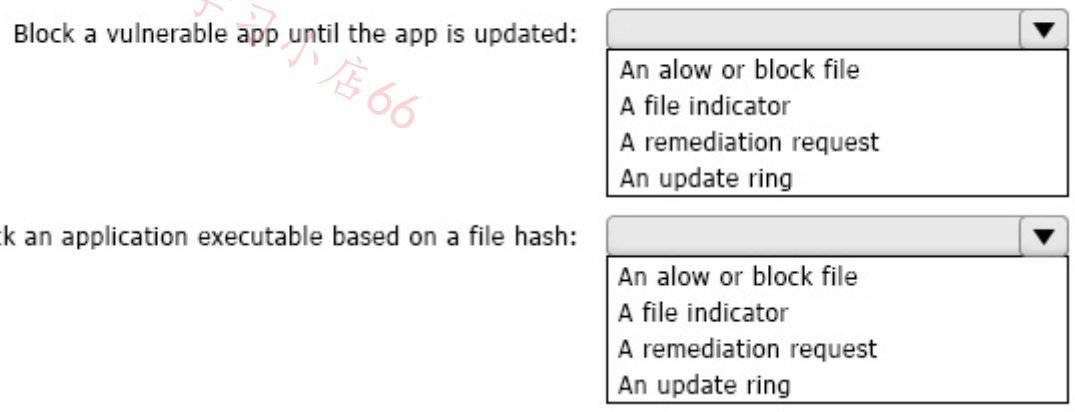
Block an application executable based on a file hash.

The solution must minimize administrative effort.

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

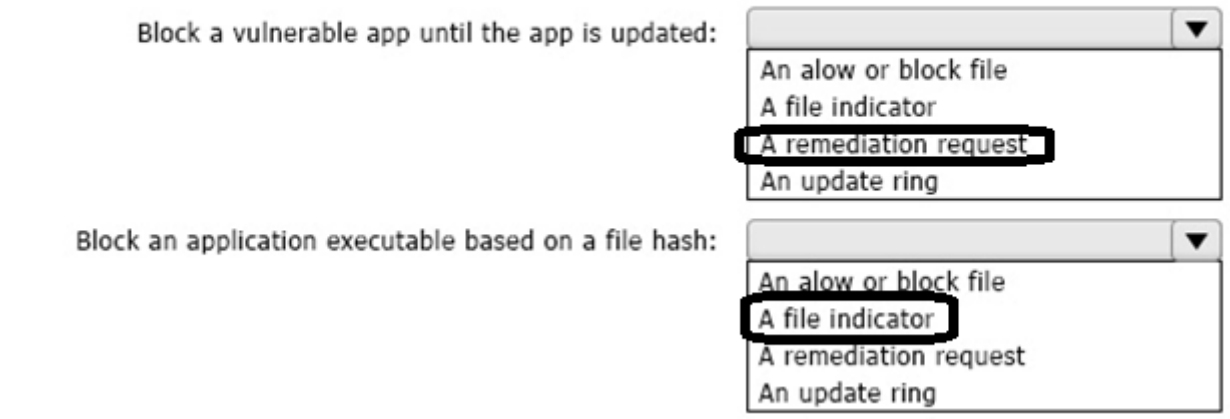
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	*Not applicable*

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@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.

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	●
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	●
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	●	○

nsotis28 1 week, 2 days ago

correct answer

upvoted 1 times

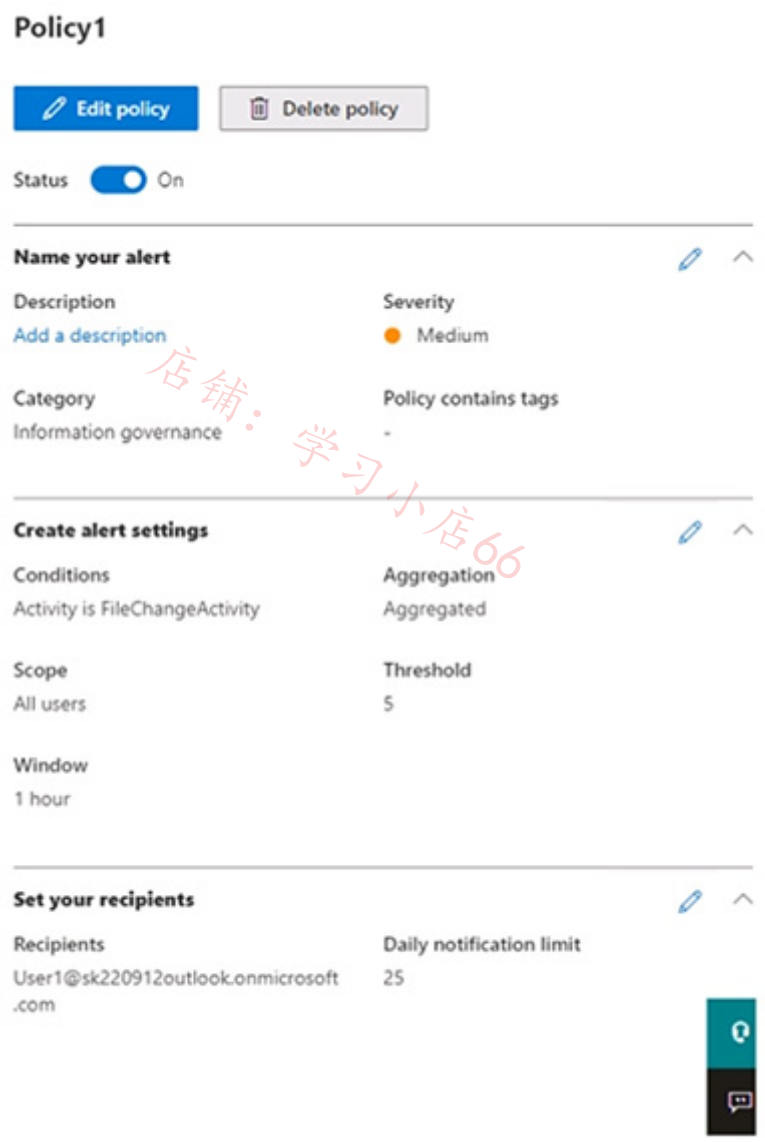
Greatone1 1 week, 6 days ago

No - High severity Alert.
No - Doesn't have 'Device' in name
Yes - Has OS name Andriod and Tag contains 'Inventory

upvoted 1 times

You have a Microsoft 365 tenant that contains two users named User1 and User2.

You create the alert policy shown in the following exhibit.



User2 runs a script that modifies a file in a Microsoft SharePoint library once every four minutes and runs for a period of two hours.

How many alerts will User1 receive?

A. 2

B. 5

C. 10

D. 25

E. 30

Correct Answer: *D*

nsotis28 1 week, 2 days ago

picture is wrong
In any case key here is "aggregation"
https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide

upvoted 1 times

gomezmax 1 week, 2 days ago

D Good 25

upvoted 1 times

Question #80 *Topic 1*

Your company has 10,000 users who access all applications from an on-premises data center.
You plan to create a Microsoft 365 subscription and to migrate data to the cloud.
You plan to implement directory synchronization.
User accounts and group accounts must sync to Azure AD successfully.
You discover that several user accounts fail to sync to Azure AD.
You need to resolve the issue as quickly as possible.
What should you do?

A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.

B. Run idfix.exe, and then click Edit.

C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.

D. Run idfix.exe, and then click Complete.

Correct Answer: *B*

Greatone1 1 week, 6 days ago

Selected Answer: B

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix

upvoted 1 times

Casticod 1 week, 6 days ago

Selected Answer: B

Correct It is necessary to modify the maximum threshold of modifications in each synchronization.

upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

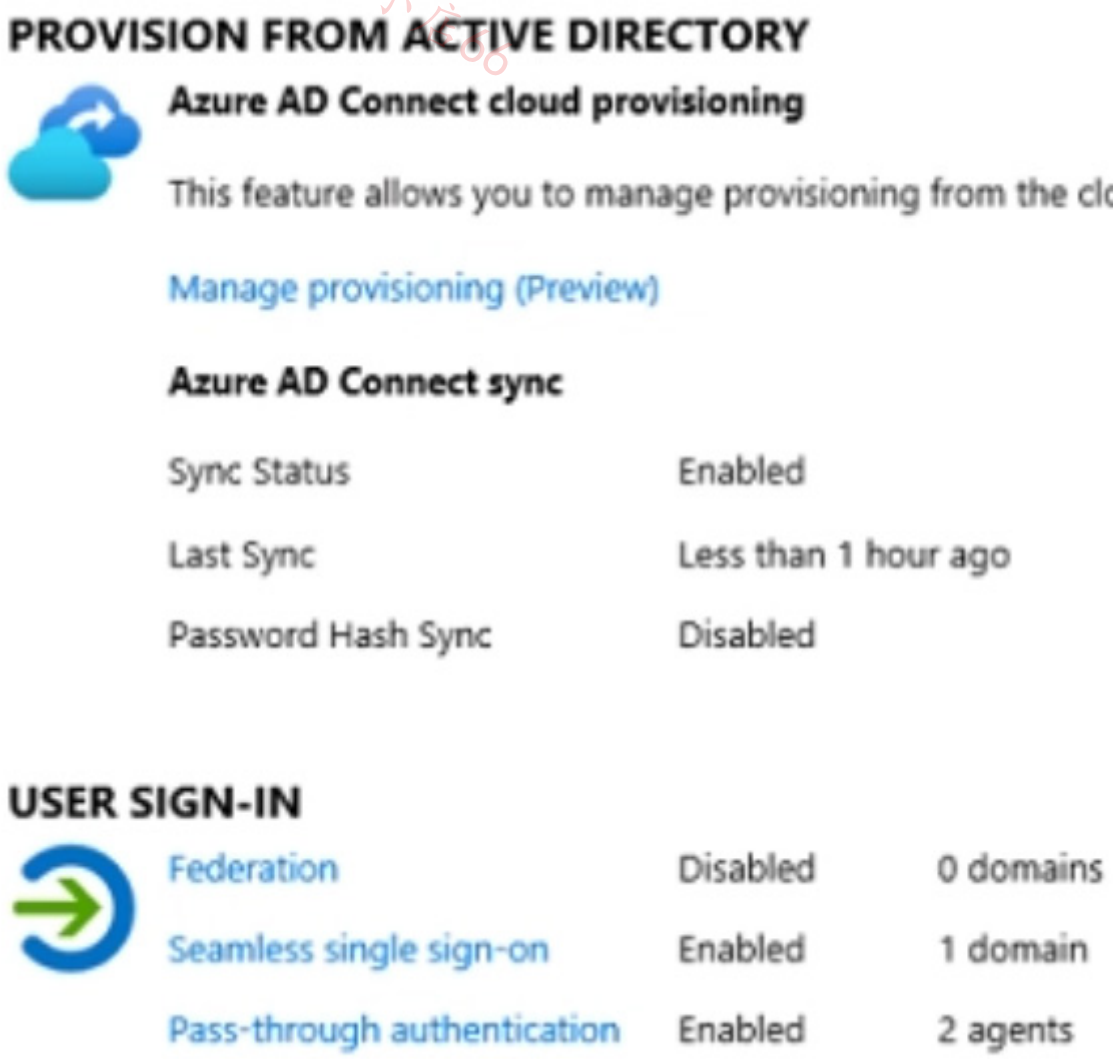
Contoso.com -

East.contoso.com -

The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit 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.

Answer Area

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	○	○
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	○	○
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	○	○
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	○	○
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	○	○

Greatone1 1 week, 6 days ago

Box 1: Yes -
The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.

Box 2: No -
The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.

Box 3: No -
The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

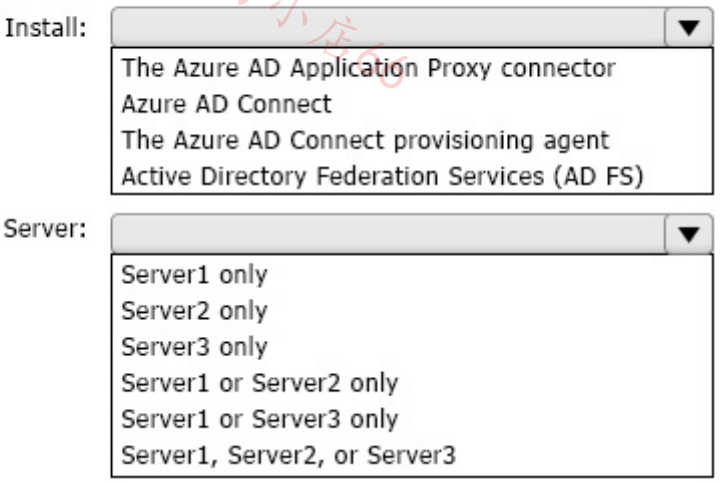
You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

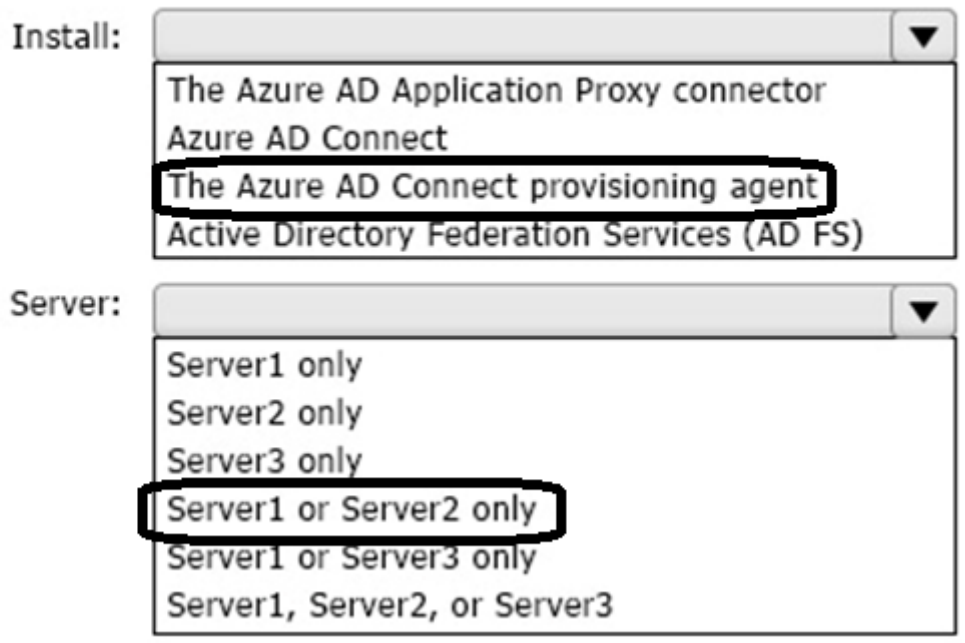
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



letters1234 2 days, 4 hours ago

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-prerequisites?tabs=public-cloud#in-your-on-premises-environment
2016+ domain member server, server core not supported.

upvoted 1 times

certma2023 2 weeks, 3 days ago

Answer is correct.

You need to install a small agent on an On-Premises server. This server must run Windows Server 2016 ou later. Agent installation on DC is supporter. Agent installation on Windows Server Core is not supported.

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	*None*
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings:

Assignments -

Users or workload identities: Group1

Cloud apps or actions: Office 365 SharePoint Online

Conditions -

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -startsWith "Device"

Access controls -

Grant -

Grant: Block access -

Session: 0 controls selected -

Enable policy: On -

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 access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User2 can access Site1 from Device3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	○	◉
User2 can access Site1 from Device2.	◉	○
User2 can access Site1 from Device3.	◉	○

hogehogehoge 1 week, 3 days ago

This answer is correct. Device1 is not registerd in Azure AD. In this case, Device filter is not enable. So Device1 is blocked.

upvoted 1 times

Question #84 *Topic 1*

You have a Microsoft 365 E5 subscription.

Conditional Access is configured to block high-risk sign-ins for all users.

All users are in France and are registered for multi-factor authentication (MFA).

Users in the media department will travel to various countries during the next month.

You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.

What should you configure?

A. an exclusion group

B. the MFA registration policy

C. named locations

D. self-service password reset (SSPR)

Correct Answer: *D*

letters1234 2 days, 3 hours ago

Selected Answer: D

A & B - Are excluding users from MFA, which is not a secure method of managing users and the risk to their accounts.
C - Named locations requires IP ranges, how do you know each Wi-Fi/network range the reps will visit? Wouldn't trust ChatGPT as far as I could throw it.
D - You can allow users to self-remediate their sign-in risks and user risks by setting up risk-based policies. If users pass the required access control, such as Azure AD Multifactor Authentication or secure password change, then their risks are automatically remediated.
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#self-remediation-with-risk-based-policy

upvoted 1 times

gomezmax 3 days, 16 hours ago

The Answer Is C

upvoted 1 times

DiligentSam 5 days, 21 hours ago

C.named locations. This answer from ChatGPT
By configuring named locations in Conditional Access, you can define trusted locations where users can sign in without being subject to the same level of risk assessment as other locations. This will allow the media department users to sign in from their travel locations without being blocked, as long as they are still using MFA. Additionally, if they are blocked, they can remediate the issue themselves by verifying their identity through MFA. This can be done without administrator intervention, using self-service password reset (SSPR) or other MFA verification methods.

upvoted 1 times

Ranger_DanMT 6 days, 19 hours ago

nevermind answer is correct https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#:~:text=If%20a%20user%20has%20registered,a%20self%2Dservice%20password%20reset.

upvoted 2 times

Ranger_DanMT 1 week ago

Pretty sure the answer to this would be B?

upvoted 1 times

Question #85 *Topic 1*

You have a Microsoft 365 E5 subscription that contains the following user:

Name: User1 -

UPN: user1@contoso.com -
Email address: user1@marketmg.contoso.com

MFA enrollment status: Disabled -
When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.
You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.
What should you do?

A. Assign an MFA registration policy to User1.

B. Reset the password of User1.

C. Add an alternate email address for User1.

D. Modify the UPN of User1.

Correct Answer: *D*

HOTSPOT -

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

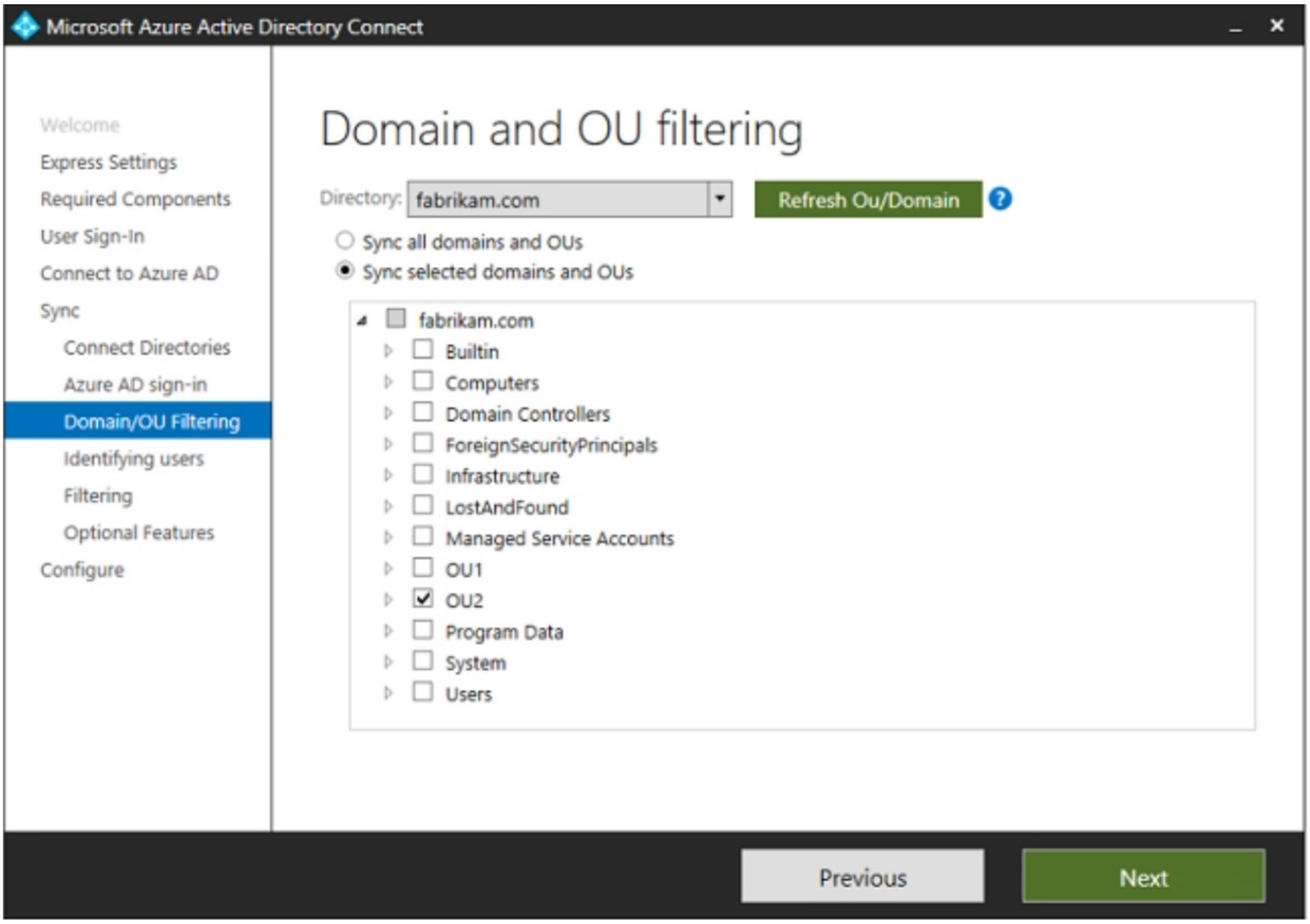
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

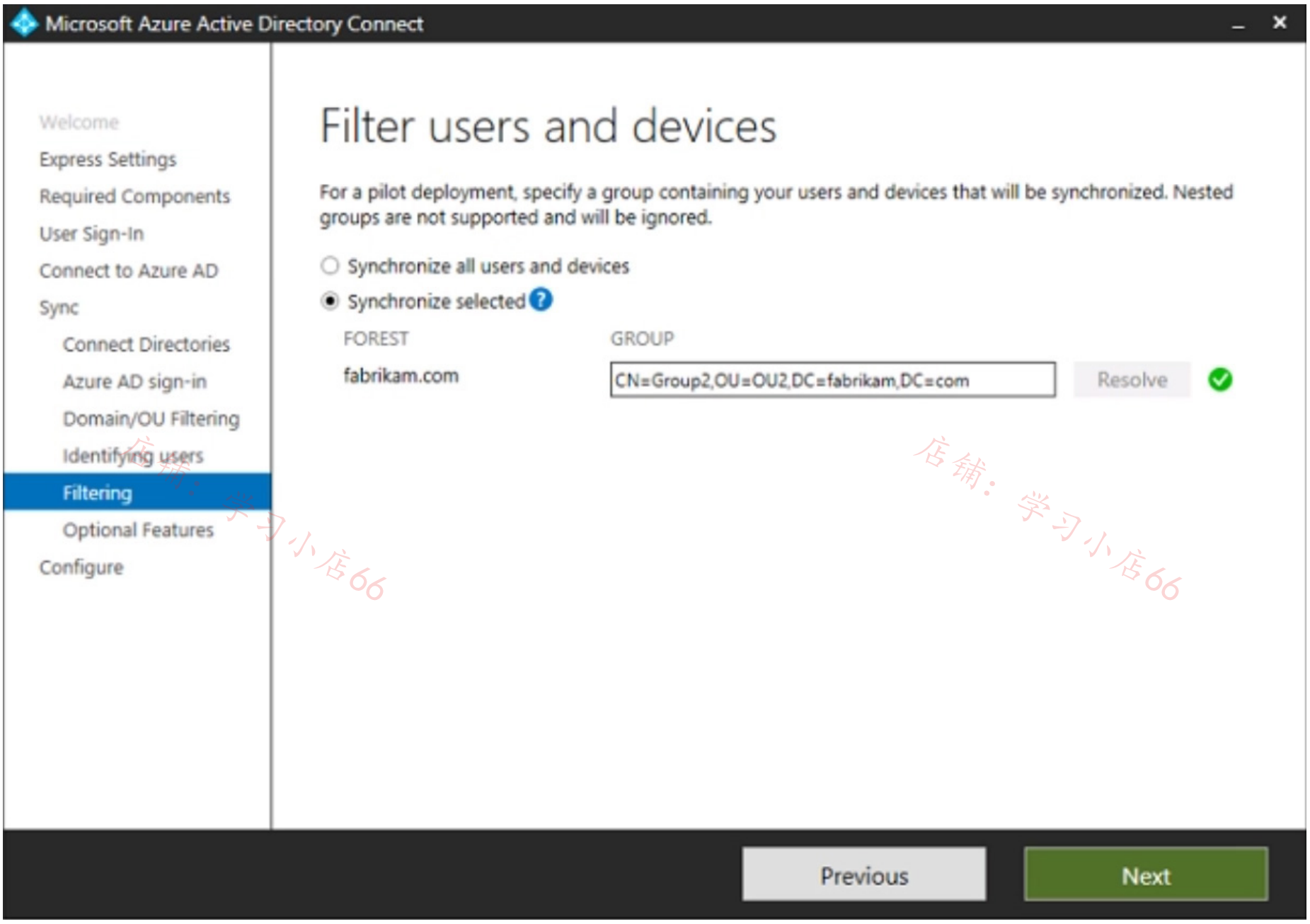
Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering 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.

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	○	○
Group2 will synchronize to Azure AD.	○	○
User3 will synchronize to Azure AD.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	○	◉
Group2 will synchronize to Azure AD.	◉	○
User3 will synchronize to Azure AD.	◉	○

nsotis28 1 week, 2 days ago

Answers are correct

upvoted 1 times

Greatone1 1 week, 4 days ago

Answers are correct
User 2 is not synced because it's not in an OU that is synced.
User 3 is synced because it is in both a synced OU and Group.

upvoted 1 times

Question #87 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

Assignments: All users -

Controls: Require Azure AD multifactor authentication registration

Enforce Policy: On -

On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:
- August 6
- August 17
- August 19
- September 3
- September 5

User2:
- August 8
- August 17
- August 19
- August 21
- September 7

Correct Answer:

Answer Area

User1:
- August 6
- August 17
- **August 19**
- September 3
- September 5

User2:
- August 8
- August 17
- August 19
- **August 21**
- September 7

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 1*

Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:
On-premises Active Directory password complexity policies must be enforced.
Users must be able to use self-service password reset (SSPR) in Azure AD.
What should you use?

A. password hash synchronization

B. Azure AD Identity Protection

C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)

D. pass-through authentication

Correct Answer: *D*

letters1234 2 days, 2 hours ago

Selected Answer: D

Password hash sync just does comparison of password hash. Passthrough respects the DC and doesnt approve the ticket itself.
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

upvoted 1 times

Casticod 6 days, 16 hours ago

Selected Answer: D

Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

upvoted 1 times

Casticod 6 days, 16 hours ago

Password writeback is supported in environments that use the following hybrid identity models:
Password hash synchronization
Pass-through authentication
Active Directory Federation Services
D or A??

upvoted 1 times

Ranger_DanMT 6 days, 19 hours ago

answer is correct, SSPR works for both Pass- thru and hash sync. The key here is that on-prem password policies need enforced.
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta

upvoted 1 times

Greatone1 1 week, 1 day ago

Selected Answer: D

Correct answer should be D
Source : https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#:~:text=is%20using%20federated%2C-,pass,-%2Dthrough%20authentication%2C%20or

upvoted 1 times

hogehogehoge 1 week, 3 days ago

I think A is correct. Because Users must use SSPR in AzureAD.

upvoted 1 times

Question #89 *Topic 1*

You have a Microsoft 365 E5 subscription.
Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.
From Azure AD Identity Protection, you enable a sign-in risk policy.
Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.
What should you configure?

A. the Tenant restrictions settings in Azure AD

B. a trusted location

C. a Conditional Access policy exclusion

D. the Microsoft 365 network connectivity settings

Correct Answer: *B*

certma2023 2 weeks, 3 days ago

Selected Answer: B

Answer B.

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

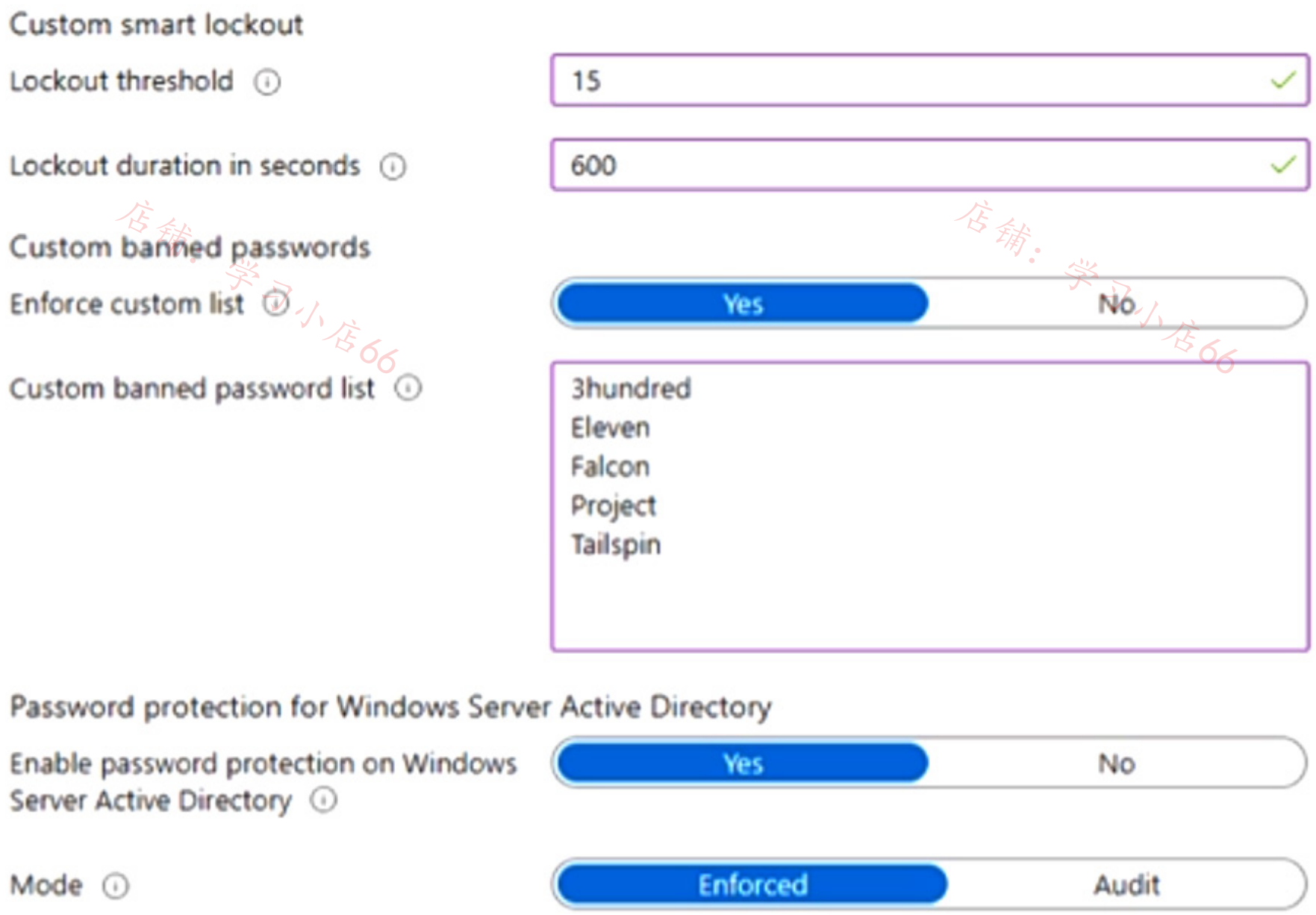
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains a user named User1.

Azure AD Password Protection is configured as shown in the following exhibit.



User1 attempts to update their password to the following passwords:

F@lcon -

Project22 -

T4il$pin45dg4 -

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

NOTE: Each correct selection is worth one point.

Answer Area

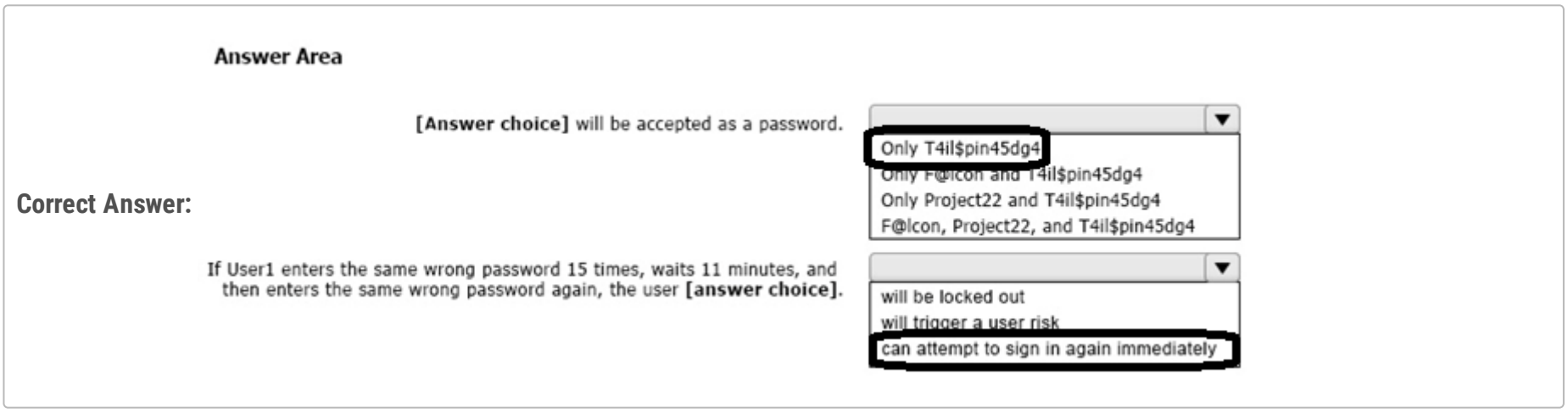
[Answer choice] will be accepted as a password.

- Only T4il$pin45dg4
- Only F@lcon and T4il$pin45dg4
- Only Project22 and T4il$pin45dg4
- F@lcon, Project22, and T4il$pin45dg4

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user **[answer choice]**.

- will be locked out
- will trigger a user risk
- can attempt to sign in again immediately

Correct Answer:



letters1234 2 days, 2 hours ago

Answers are correct

Only T4il$pin45dg4 will be allowed to change, the other two have an exact or within 1 character match to the banned passwords:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#fuzzy-matching-behavior

Lockout period is 10 minutes (600 seconds) meaning on the 11th minute, the count starts again from 1 and would need another 15 bad passwords within the next 9 minutes to lock the user out.

upvoted 1 times

nsotis28 1 week ago

Box 1 - only T4il$pin45dg4
Box 2 - will be locked

upvoted 1 times

hogehogehoge 1 week, 3 days ago

Box1:Only F@lcon and T4il$pin45dg4.
Because "a" is replaced "@", and match this policy.

upvoted 1 times

Vaati 2 weeks, 3 days ago

If you fail again after a lockout periode, you are locked again no?

upvoted 2 times

Question #91 *Topic 1*

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:

Password Hash Sync: Enabled -
Pass-through authentication: Enabled
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.
Which users should you identify?

A. none

B. User1 only

C. User1 and User2 only

D. User1, User2, and User3

Correct Answer: *D*

gomezmax 1 week, 2 days ago
it Should be A
upvoted 1 times

Greatone1 1 week, 3 days ago
Selected Answer: A
A is correct answer
Fail over to password hash synchronization doesn't happen automatically and you must use Azure AD Connect to switch the sign-on method manually.
upvoted 1 times

nsotis28 1 week, 4 days ago
For sure A
certman2023 has shared explanation
upvoted 1 times

certma2023 2 weeks, 3 days ago
Selected Answer: A
I would choose A.

According to the MS documentation:

"Does password hash synchronization act as a fallback to Pass-through Authentication?
No. Pass-through Authentication does not automatically failover to password hash synchronization. To avoid user sign-in failures, you should configure Pass-through Authentication for high availability."
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-faq#does-password-hash-synchronization-act-as-a-fallback-to-pass-through-authentication-

Therefore, without any admin actions, authentication won't be possible for any user until the admin make some changes on the tenant.
upvoted 2 times

Question #92 *Topic 1*

Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.
You plan to sync contoso.com to an Azure AD tenant
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?

A. pass-through authentication

B. conditional access policies

C. password synchronization

D. Azure AD Identity Protection policies

Correct Answer: *A*

DiligentSam 5 days, 5 hours ago
Conditional access policies. From ChatGPT
You should recommend using conditional access policies in Azure AD to enforce logon hour restrictions for synced users. Conditional access policies allow you to define access rules based on various conditions, including time of day. By creating a conditional access policy that requires users to sign in during business hours, you can ensure that logon hour restrictions are enforced for synced users in Azure AD.
upvoted 1 times

Casticod 1 week, 5 days ago
Selected Answer: A
This requirement can be achieved only if you have Pass through Authentication configured as a sign in option with Azure AD and with Logon hours setting configured in on-premise AD.
Other solution it´s PIM but not valid in that question
upvoted 1 times

Greatone1 2 weeks ago
I was wrong given answer is correct
upvoted 1 times

Greatone1 2 weeks ago
I believe answer is b conditional access
upvoted 1 times

Question #93 *Topic 1*

Your network contains three Active Directory forests. There are forests trust relationships between the forests.
You create an Azure AD tenant.
You plan to sync the on-premises Active Directory to Azure AD.
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.
What should you include in the recommendation?

A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode

B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode

C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Correct Answer: *A*

nsotis28 1 week, 4 days ago

A
AD connect supports only one instance of Azure AD Connect syncing to Azure AD. You can add directories during configuration
https://learn.microsoft.com/en-us/skypeforbusiness/hybrid/cloud-consolidation-aad-connect

upvoted 1 times

Question #94 *Topic 1*

You have a Microsoft 365 subscription.

You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx.

File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.

When will File1.docx be deleted automatically?

A. January 1, 2023

B. January 1, 2024

C. January 31, 2023

D. January 31, 2024

E. never

Correct Answer: *D*

letters1234 2 days, 2 hours ago

Selected Answer: E

https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden#the-principles-of-retention-or-what-takes-precedence
"At a high level, you can be assured that retention always takes precedence over permanent deletion, and the longest retention period wins. These two simple rules always decide how long an item will be retained."
Possibly E due to the "at end of retention" setting being no action, i.e., retain. Unless the polices change, it would not be deleted.

upvoted 1 times

hogehogehoge 1 week, 6 days ago

Selected Answer: D

I think D is correct. Please check this URL. https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden

upvoted 1 times

Vaati 2 weeks, 3 days ago

Could someone explain? im thinking E

upvoted 1 times

Question #95 *Topic 1*

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

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to publish a sensitivity label named Label1.

To which groups can you publish Label1?

A. Group1 only

B. Group1 and Group2 only

C. Group1 and Group4 only

D. Group1, Group2, and Group3 only

E. Group1, Group2, Group3, and Group4

Correct Answer: *A*

spectre786 3 days, 3 hours ago

Correct : D
You can publish labels to users but only to groups that have email addresses (Distribution groups, Microsoft 365 groups, and mail-enabled security groups). You can't publish a label to a security group. The group can have assigned or dynamic membership.

upvoted 1 times

gomezmax 5 days, 15 hours ago

(A) it is Correct only applied into the Email

upvoted 1 times

gomezmax 5 days, 15 hours ago

Correct

upvoted 1 times

Greatone1 2 weeks ago

Correct answer is D

upvoted 1 times

certma2023 2 weeks, 3 days ago

Answer D.
According to the documentation:

"Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD."
https://learn.microsoft.com/en-us/purview/sensitivity-labels

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:
- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:
- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

Correct Answer:

Answer Area

File1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

letters1234 2 days, 1 hour ago

Agree with Hoge, specific reference in the doc:
https://learn.microsoft.com/en-us/purview/dlp-policy-reference#the-priority-by-which-rules-are-evaluated-and-applied

upvoted 1 times

hogehogehoge 1 week, 6 days ago

File1.docx:rule2 only. And File2.docx:rule4 only.

When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the first rule evaluated that has the most restrictive action is enforced. For example, if content matches all of the following rules, Rule 3 is enforced because it's the highest priority, most restrictive rule:

https://learn.microsoft.com/en-us/purview/dlp-policy-reference

Question #97 *Topic 1*

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

A. actions

B. incident reports

C. exceptions

D. user overrides

Correct Answer: *D*

Greatone1 1 week, 5 days ago

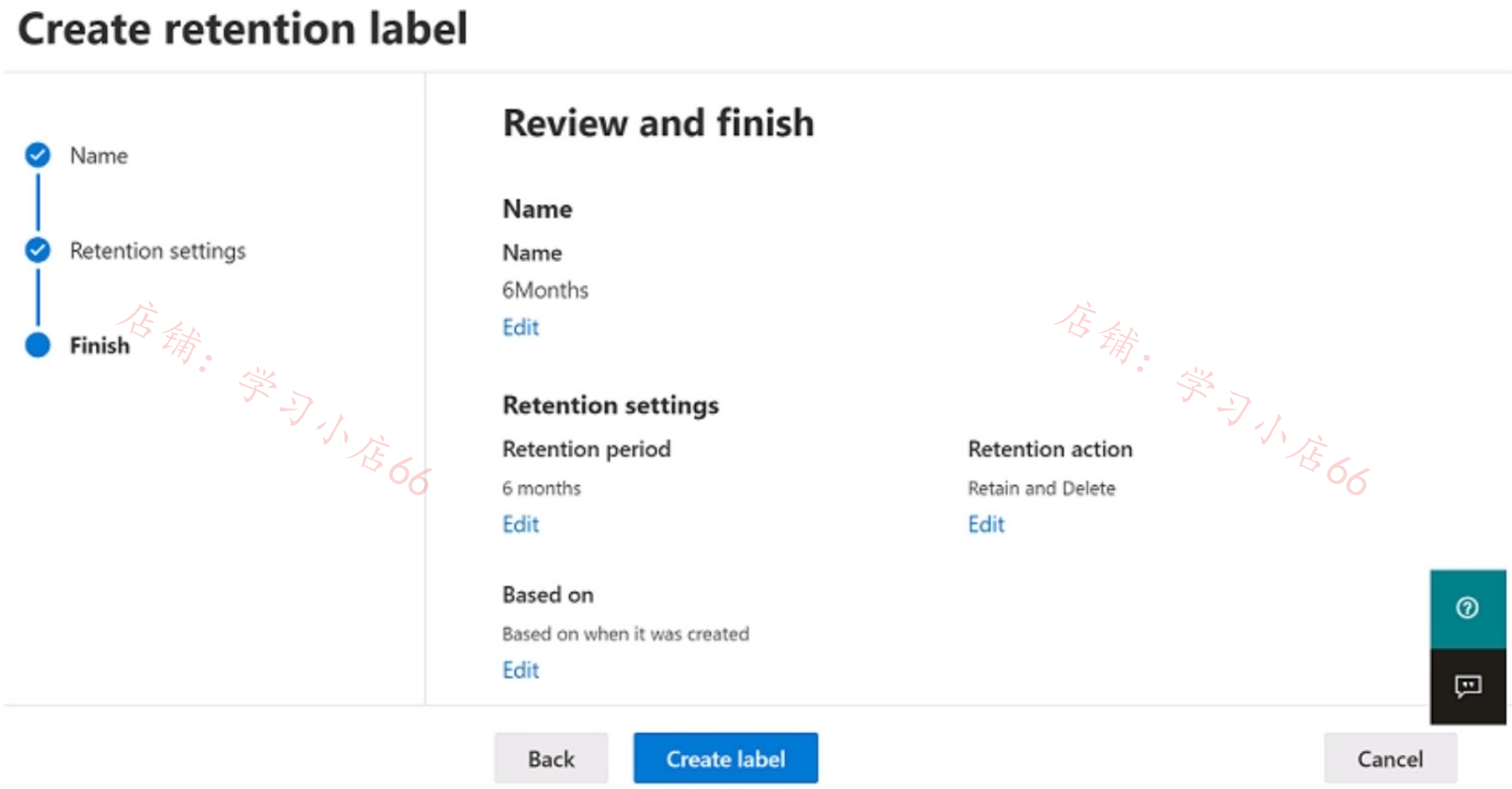
Selected Answer: D

Explanation:
A DLP policy can be configured to allow users to override a policy tip and report a false positive.

upvoted 1 times

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.



When users attempt to apply Retention1, the label is unavailable.

You need to ensure that Retention1 is available to all the users.

What should you do?

A. Create a new label policy.

B. Modify the Authority type setting for Retention1.

C. Modify the Business function/department setting for Retention1.

D. Use a file plan CSV template to import Retention1.

Correct Answer: *A*

letters1234 2 days, 1 hour ago

From Greatone1's link:
Making retention labels available to people in your organization so that they can classify content is a two-step process:
-Create the retention labels.
-Publish the retention labels by using a retention label policy.

upvoted 1 times

Greatone1 1 week, 5 days ago

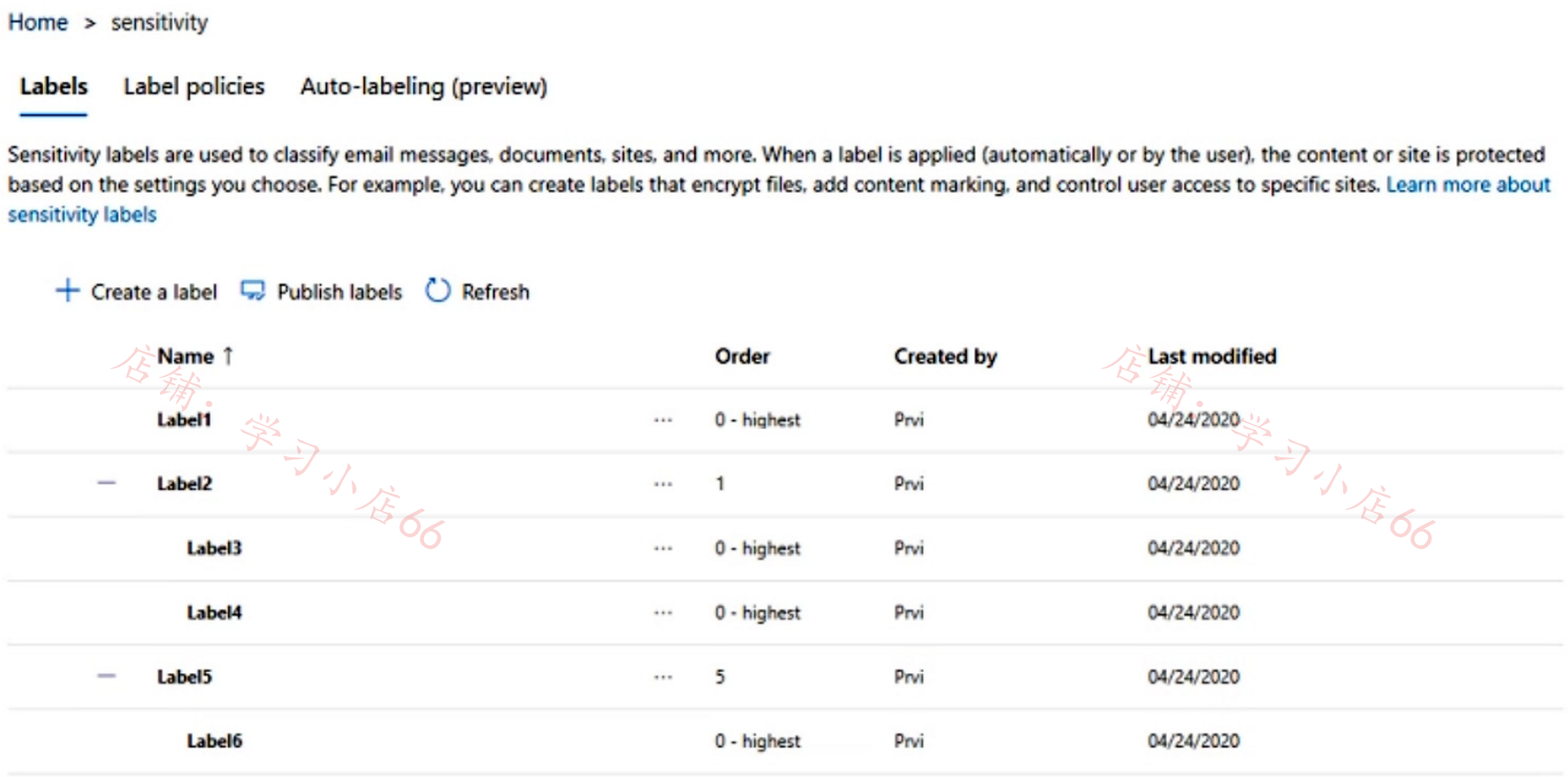
Selected Answer: A

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

upvoted 1 times

Question #99 *Topic 1*

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.



Which labels can users apply to content?

A. Label1, Label2, and Label5 only

B. Label3, Label4, and Label6 only

C. Label1, Label3, Label4, and Label6 only

D. Label1, Label2, Label3, Label4, Label5, and Label6

Correct Answer: *D*

letters1234 2 days, 1 hour ago

Selected Answer: C

https://learn.microsoft.com/en-us/purview/sensitivity-labels#sublabels-grouping-labels

upvoted 1 times

gomezmax 1 week, 2 days ago

Should be C. Label1, Label3, Label4, and Label6 only

upvoted 1 times

f7d3be6 1 week, 4 days ago

Respuesta C Por ejemplo, en Confidencial, su organización puede usar varias etiquetas diferentes para tipos específicos de esa sensibilidad. En este ejemplo, la etiqueta principal Confidencial es simplemente una etiqueta de texto sin configuración de protección y, dado que tiene subetiquetas, no se puede aplicar al contenido. En su lugar, los usuarios deben elegir Confidencial para ver las subetiquetas y, a continuación, pueden elegir una subetiqueta para aplicar al contenido.

upvoted 1 times

Greatone1 1 week, 5 days ago

Selected Answer: C

C is the correct answer

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

upvoted 1 times

hogehogehoge 1 week, 6 days ago

Selected Answer: C

C is correct. Because user can then apply that sublabel to content and containers, but can't apply just the parent label.
https://learn.microsoft.com/en-us/purview/sensitivity-labels

upvoted 1 times

Question #100 *Topic 1*

HOTSPOT -
Your company has a Microsoft 365 E5 tenant
Users at the company use the following versions of Microsoft Office:
Microsoft 365 Apps for enterprise

Office for the web -

Office 2016 -

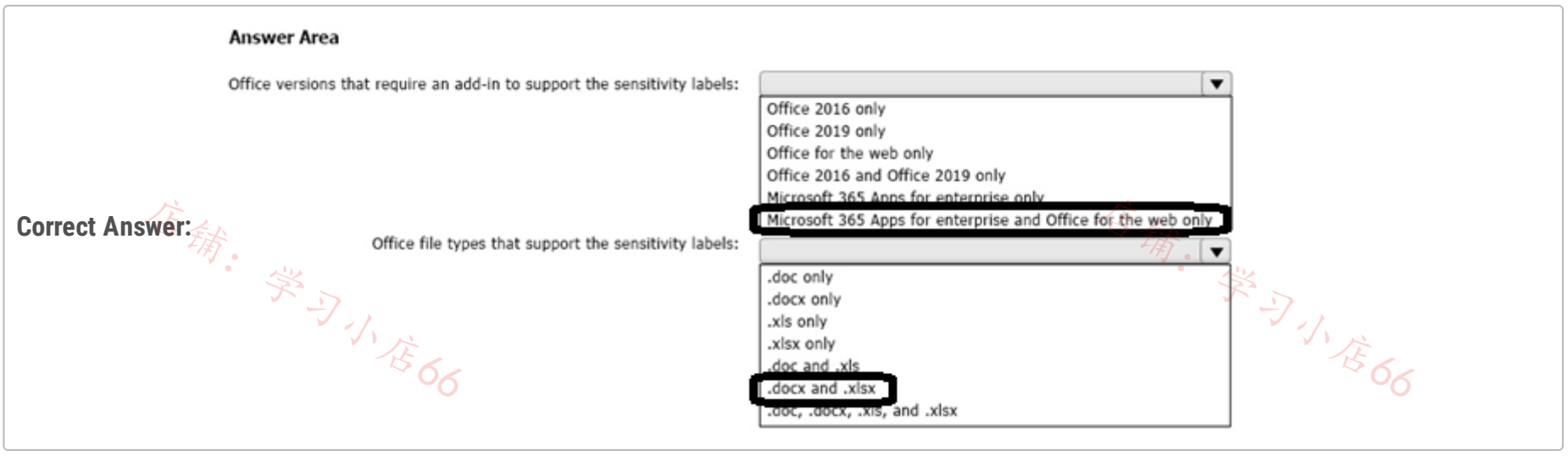
Office 2019 -
The company currently uses the following Office file types:
.docx
.xlsx
.doc
.xls
You plan to use sensitivity labels.
You need to identify the following:
Which versions of Office require an add-in to support the sensitivity labels.
Which file types support the sensitivity labels.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Office versions that require an add-in to support the sensitivity labels:
- Office 2016 only
- Office 2019 only
- Office for the web only
- Office 2016 and Office 2019 only
- Microsoft 365 Apps for enterprise only
- Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels:
- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx
- .doc, .docx, .xls, and .xlsx

Correct Answer:



letters1234 2 days, 1 hour ago

365 versions of Office (365 Apps) have it built in. Meaning only the 2016/2019 currently require the AIP UL add-in (which is being deprecated soon).
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sensitivity-labeling-now-built-into-office-apps-for-windows-to/ba-p/844506
https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#labeling-client-for-desktop-apps

Office 2016 is out of mainstream support (meaning no new features/functions added) and wouldn't expect them to develop the integrated label handling since it's in security patching only mode.
https://learn.microsoft.com/en-us/lifecycle/products/microsoft-office-2016

Would go with 2016 & 2019, however not sure how much longer this question will be around considering the add-in is being deprecated.

upvoted 1 times

Greatone1 2 weeks ago

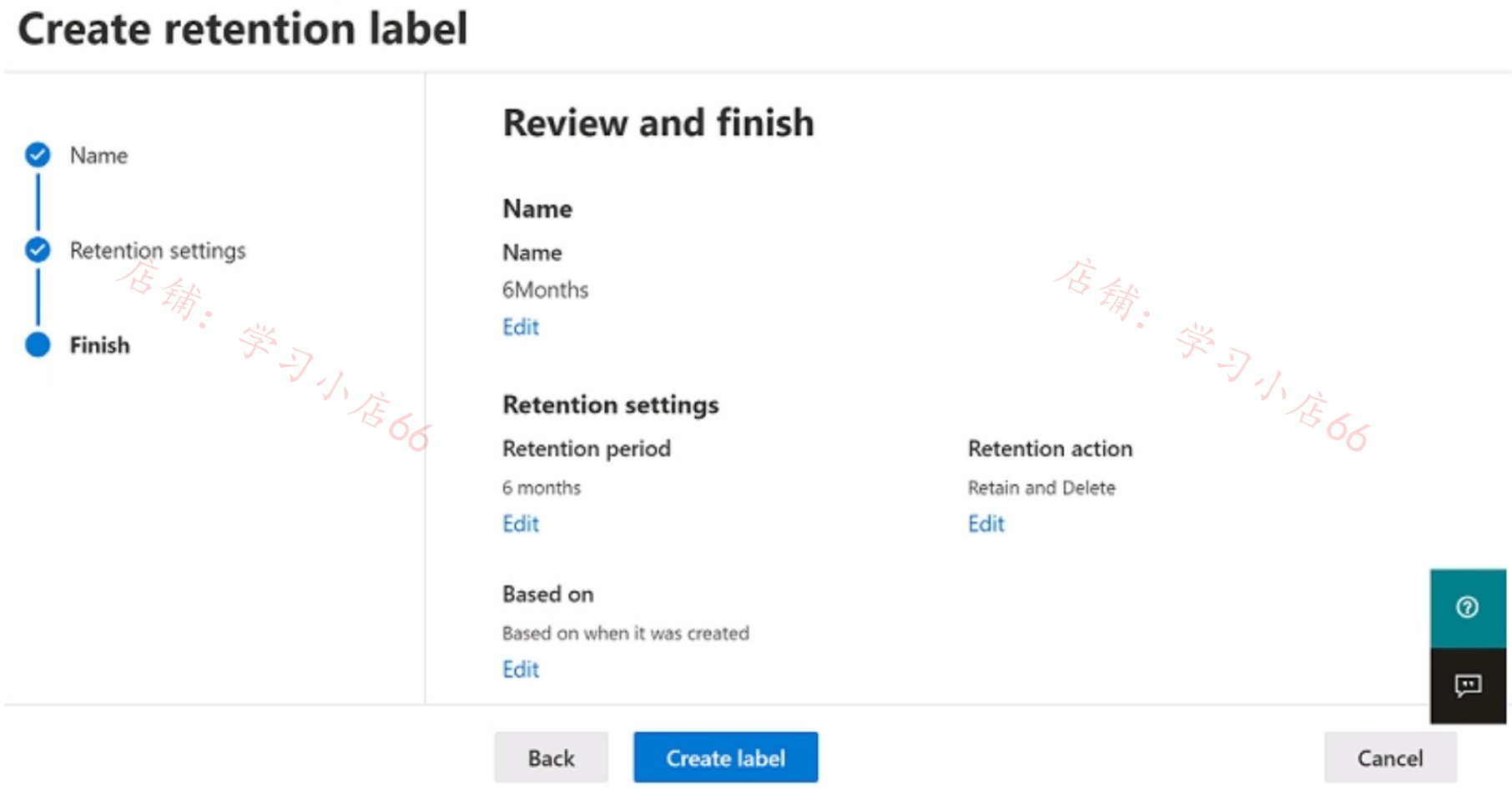
Given answer is correct.

upvoted 1 times

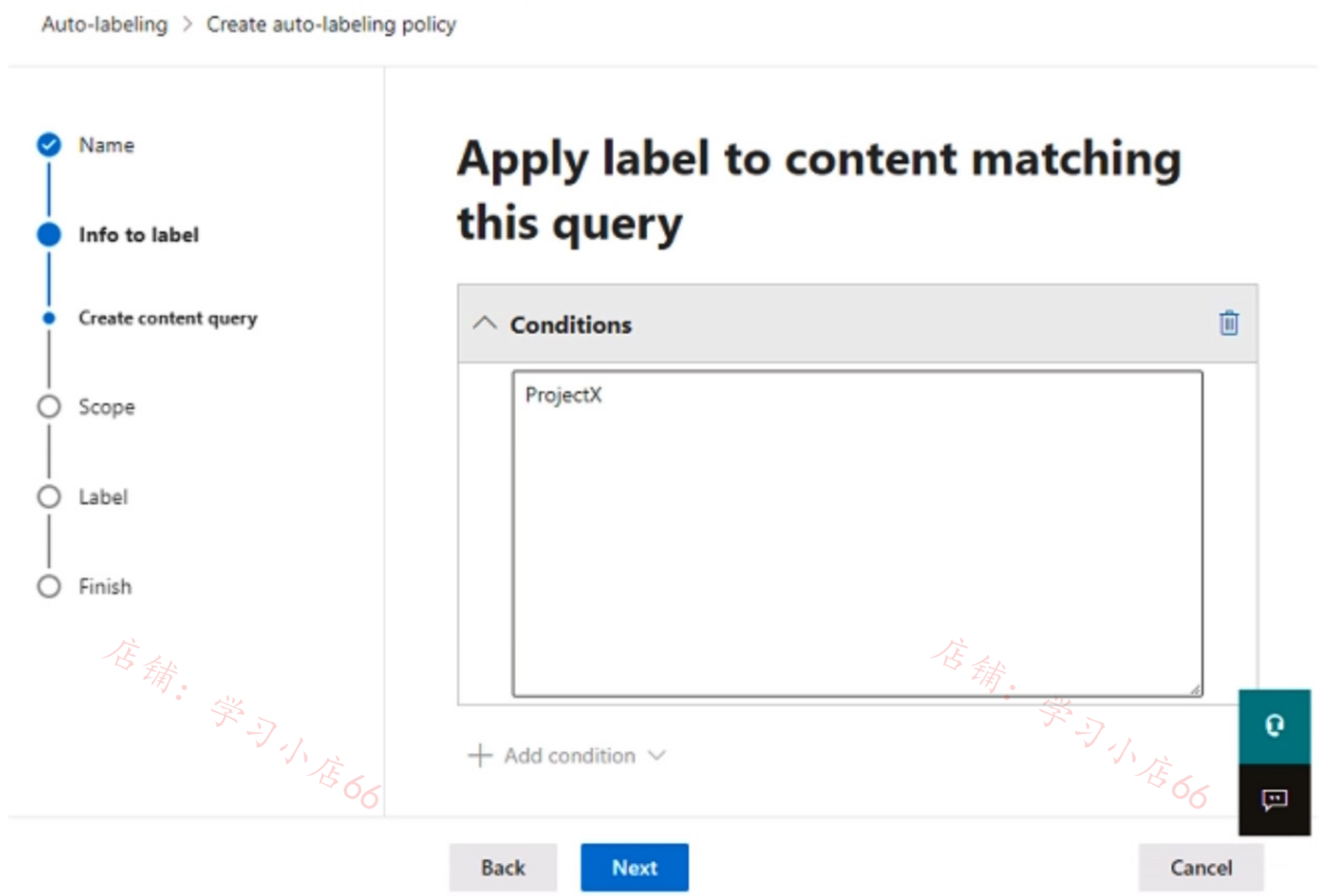
HOTSPOT -

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)



You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)



The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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
Any sent email message that contains the word ProjectX will be deleted immediately.	○	○
Any sent email message that contains the word ProjectX will be retained for six months.	○	○
Users are required to manually apply a label to email messages that contain the word ProjectX.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	○	●
Any sent email message that contains the word ProjectX will be retained for six months.	●	○
Users are required to manually apply a label to email messages that contain the word ProjectX.	○	●

Question #102 *Topic 1*

You have a Microsoft 365 subscription.
Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.
You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.
What should you create to ensure that the DLP policy can detect the customer IDs?

A. a PowerShell script

B. a sensitivity label

C. a sensitive information type

D. a retention label

Correct Answer: *C*

Greatone1 2 weeks ago
Answer is correct
https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide
upvoted 1 times

Question #103 *Topic 1*

You have a Microsoft 365 E5 subscription.
You define a retention label that has the following settings:

Retention period: 7 years -
Start the retention period based on: When items were created
You need to prevent the removal of the label once the label is applied to a file.
What should you select in the retention label settings?

A. Retain items forever or for a specific period

B. Mark items as a regulatory record

C. Mark items as a record

D. Retain items even if users delete

Correct Answer: *A*

letters1234 2 days, 1 hour ago

Selected Answer: B

Regulatory Record Labels can be used in situations where you absolutely need to ensure that the record isn't altered. They really aren't for the faint-hearted – once you apply one there is no going back – the record and its metadata are permanently locked.

upvoted 1 times

Greatone1 1 week, 3 days ago

Selected Answer: B

Sorry I meant B

upvoted 3 times

Greatone1 1 week, 3 days ago

Selected Answer: A

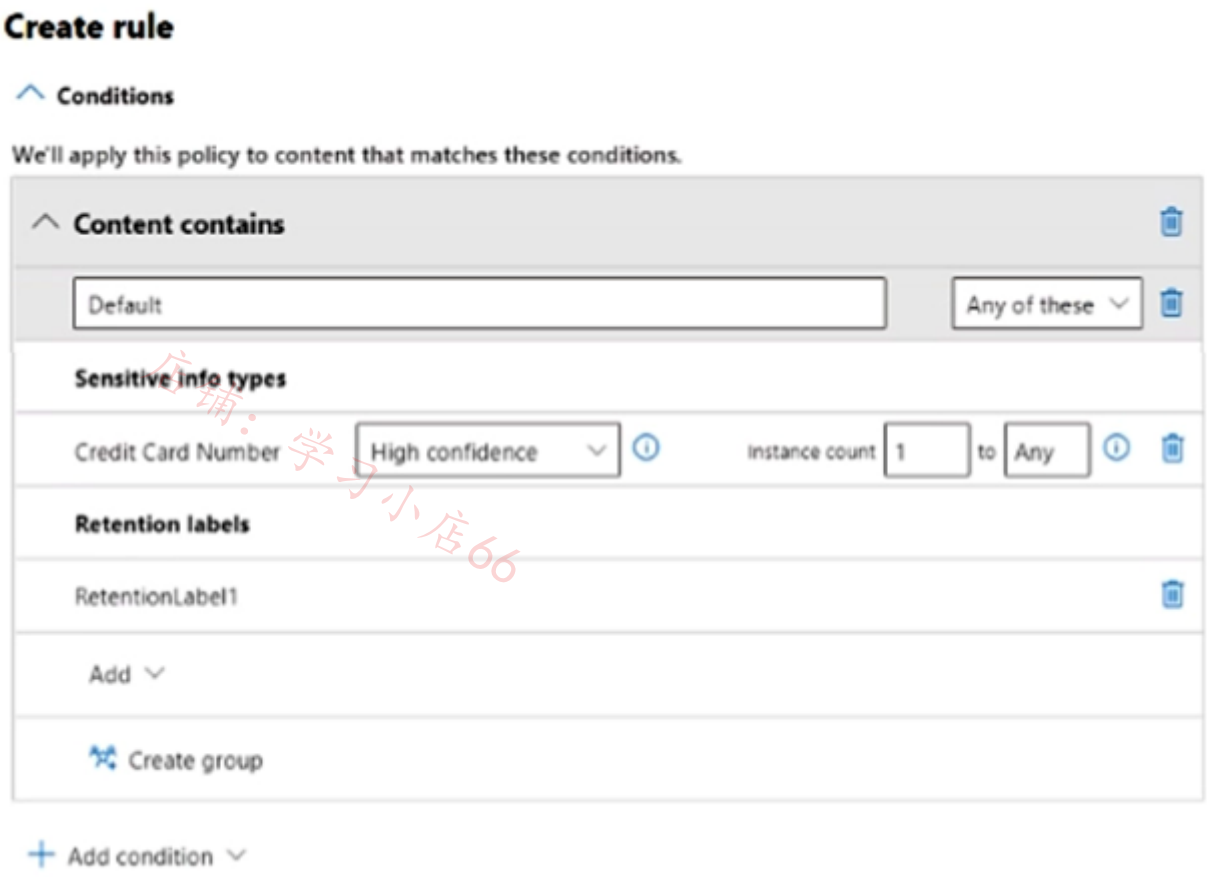
Correct answer is A
https://www.examtopics.com/discussions/microsoft/view/80391-exam-ms-101-topic-3-question-121-discussion/

upvoted 1 times

Question #104 *Topic 1*

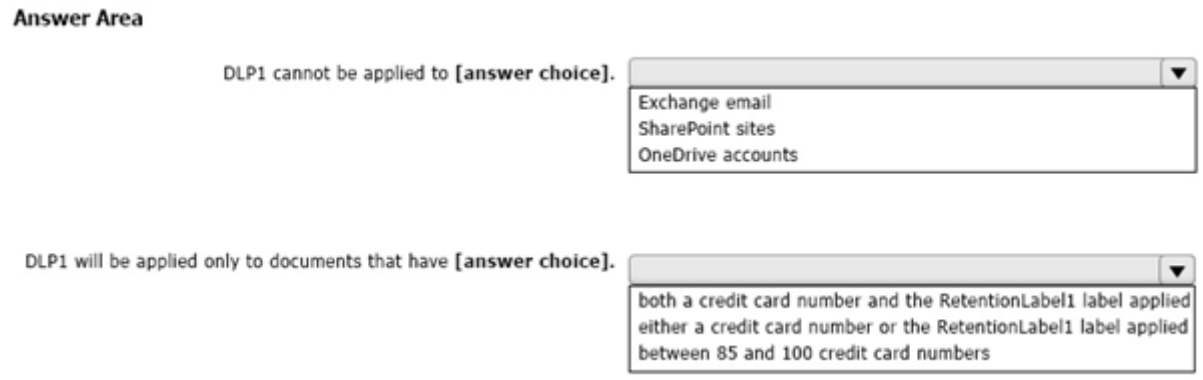
HOTSPOT -

You configure a data loss prevention (DLP) policy named DLP1 with a rule configured as shown in the following exhibit.

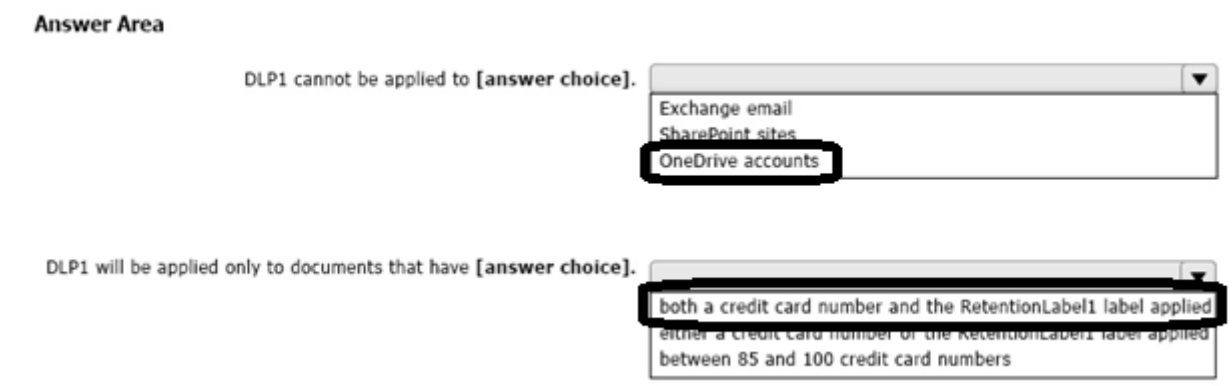


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Correct Answer:



letters1234 2 days, 1 hour ago

"Suppose you need to act on credit card information in messages. The actions you take once it's found aren't the subject of this article, but you can learn more about that in -**-Mail flow rule actions in Exchange Online.-**-"
https://learn.microsoft.com/en-us/exchange/security-and-compliance/data-loss-prevention/dlp-rule-application

upvoted 1 times

Greatone1 6 days, 13 hours ago

Box1: Correct the policy cannot be applied to Exchange
Box2: either a credit card number or the Retention label1 label will be applied

upvoted 2 times

hogehogehoge 1 week, 5 days ago

Box1:Exchange email. I tested this configuration in my lab.
Box2:ether a credit card number or the Retention label1 label applied.

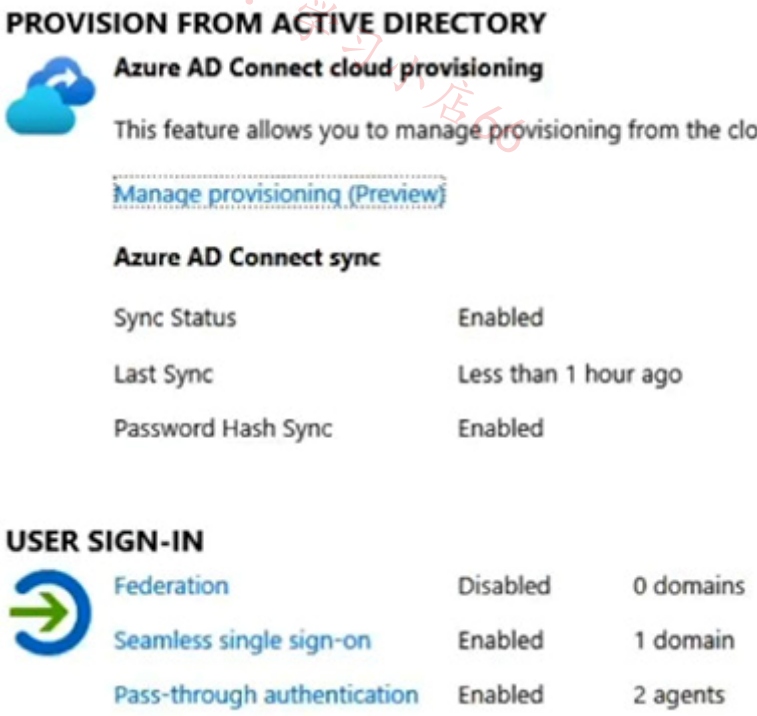
upvoted 2 times

Question #105 *Topic 1*

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.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.
You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Greatone1 1 day, 4 hours ago

This is not a permissions issue.
The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

upvoted 1 times

Greatone1 1 week, 5 days ago

Selected Answer: B

Correct answer should be no

upvoted 1 times

Question #106 *Topic 1*

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.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint Administrator role.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Question #107 *Topic 1*

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.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*

Greatone1 1 day, 4 hours ago

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

upvoted 1 times

Question #108 *Topic 1*

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.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*