



MS-102^{Q&As}

Microsoft 365 Certified: Enterprise Administrator Expert

Pass Microsoft MS-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/ms-102.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

You have a Microsoft 365 E5 subscription that uses Microsoft intune.

in the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices,

You enable device clean-up rules

What can you configure as the minimum number of days before a device a removed automatically?

- A. 10
- B. 30
- C. 45
- D. 90

Correct Answer: D

QUESTION 2

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.

Hot Area:



Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Recent Microsoft service issues:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Correct Answer:

Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Recent Microsoft service issues:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

QUESTION 3

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

Use the Microsoft 365 Defender portal to create Safe Links policies In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email and Collaboration > Policies and Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use <https://security.microsoft.com/safelinksv2>.

1.

On the Safe Links page, select Create to start the new Safe Links policy wizard.

2.

On the Name your policy page, configure the following settings:

Name: Enter a unique, descriptive name for the policy. Description: Enter an optional description for the policy.

3.

When you're finished on the Name your policy page, select Next.

4.

On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):

Users: The specified mailboxes, mail users, or mail contacts.

*-> Groups:

Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).

The specified Microsoft 365 Groups.

Domains: All recipients in the specified accepted domains in your organization.

Etc.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure>



QUESTION 4

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

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	No ¹	No ¹	No ¹	No ¹
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

Reference: <https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports>

QUESTION 5

HOTSPOT

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



Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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

Hot Area:

Statements	Yes	No
User1 has their cache cleared on close.	<input type="radio"/>	<input type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>

Correct Answer:



Statements	Yes	No
User1 has their cache cleared on close.	<input type="radio"/>	<input checked="" type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 6

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

- A. Policy1 and Policy2 only
- B. Policy2 and Policy4 only
- C. Policy3 and Policy4 only
- D. Policy1 and Policy3only

Correct Answer: A

QUESTION 7

HOTSPOT

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:



Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations:

Name: Policy1

Assignments:

-Users and groups: Group1

-Cloud apps or actions: All cloud apps

Access controls:

Grant, require multi-factor authentication

Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to On .	<input type="radio"/>	<input type="radio"/>
Admin2 can set Enable policy for Policy1 to Off .	<input type="radio"/>	<input type="radio"/>
Admin3 can set Users and groups for Policy1 to All users .	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to On .	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can set Enable policy for Policy1 to Off .	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can set Users and groups for Policy1 to All users .	<input checked="" type="radio"/>	<input type="radio"/>



QUESTION 8

HOTSPOT

Your company has a Microsoft 365 tenant

You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)

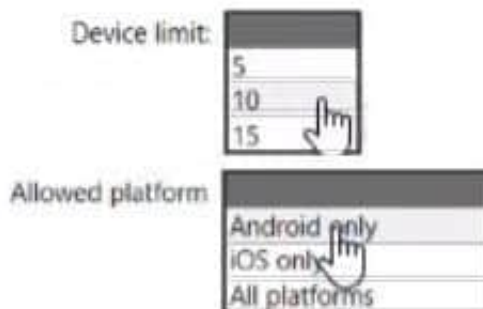
The device type restriction are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restriction are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

Hot Area:



Correct Answer:



QUESTION 9

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



Configure

Microsoft Intune

Save Discard Delete

MDM user scope ⓘ

None **Some** All

Groups

Select groups

Group1

MDM terms of use URL ⓘ

<https://portal.manage.microsoft.com/TermsOfUse.aspx>

MDM discovery URL ⓘ

<https://enrollment.manage.microsoft.com/enrollmentserver/discovery>

MDM compliance URL ⓘ

<https://portal.manage.microsoft.com/?portalAction=Compliance>

Restore default MDM URLs

MAM User scope ⓘ

None **Some** All

Groups

Select groups

Group2

MAM Terms of use URL ⓘ

MAM Discovery URL ⓘ

<https://wip.mam.manage.microsoft.com/Enroll>

MAM Compliance URI ⓘ

Restore default MAM URLs

You purchase a Windows 10 device named Device1.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 10

You have a Microsoft 365 subscription.

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



Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

Report an issue Customize

Active issues

Issue title	Affected service	Issue type
> Microsoft service health (6)		
Issues in your environment that require action (0)		

Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

Service	Status
Exchange Online	3 advisories
Microsoft 365 suite	2 advisories
Microsoft Teams	1 advisory
OneDrive for Business	1 advisory
SharePoint Online	2 advisories



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

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

Incorrect:

* Message center reader

Assign the Message center reader role to users who need to do the following:

- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups

* Reports reader

Assign the Reports reader role to users who need to do the following:

- View usage data and the activity reports in the Microsoft 365 admin center

-

Get access to the Power BI adoption content pack

-

Get access to sign-in reports and activity in Azure AD

- View data returned by Microsoft Graph reporting API

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

QUESTION 11

HOTSPOT

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



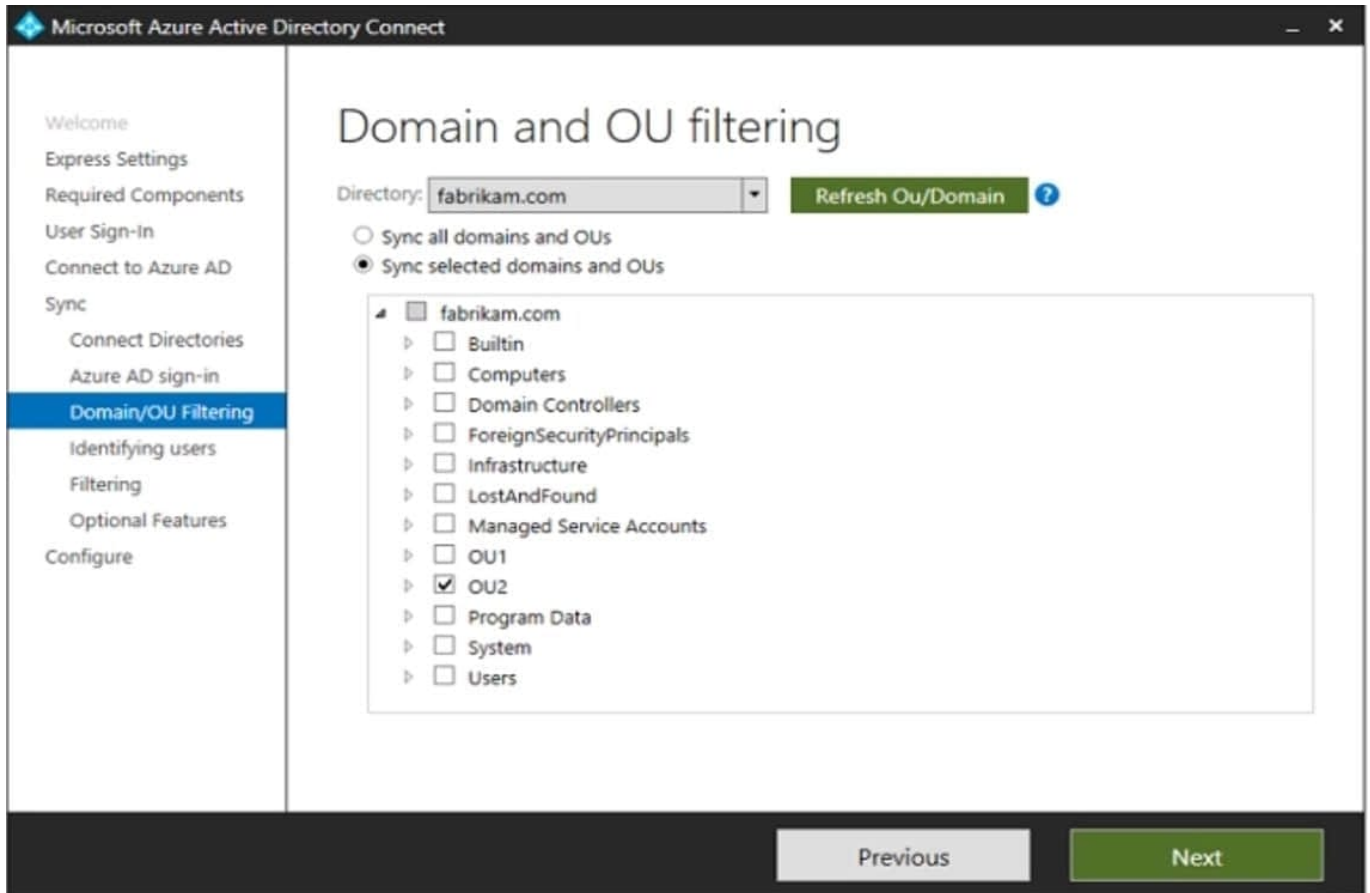
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

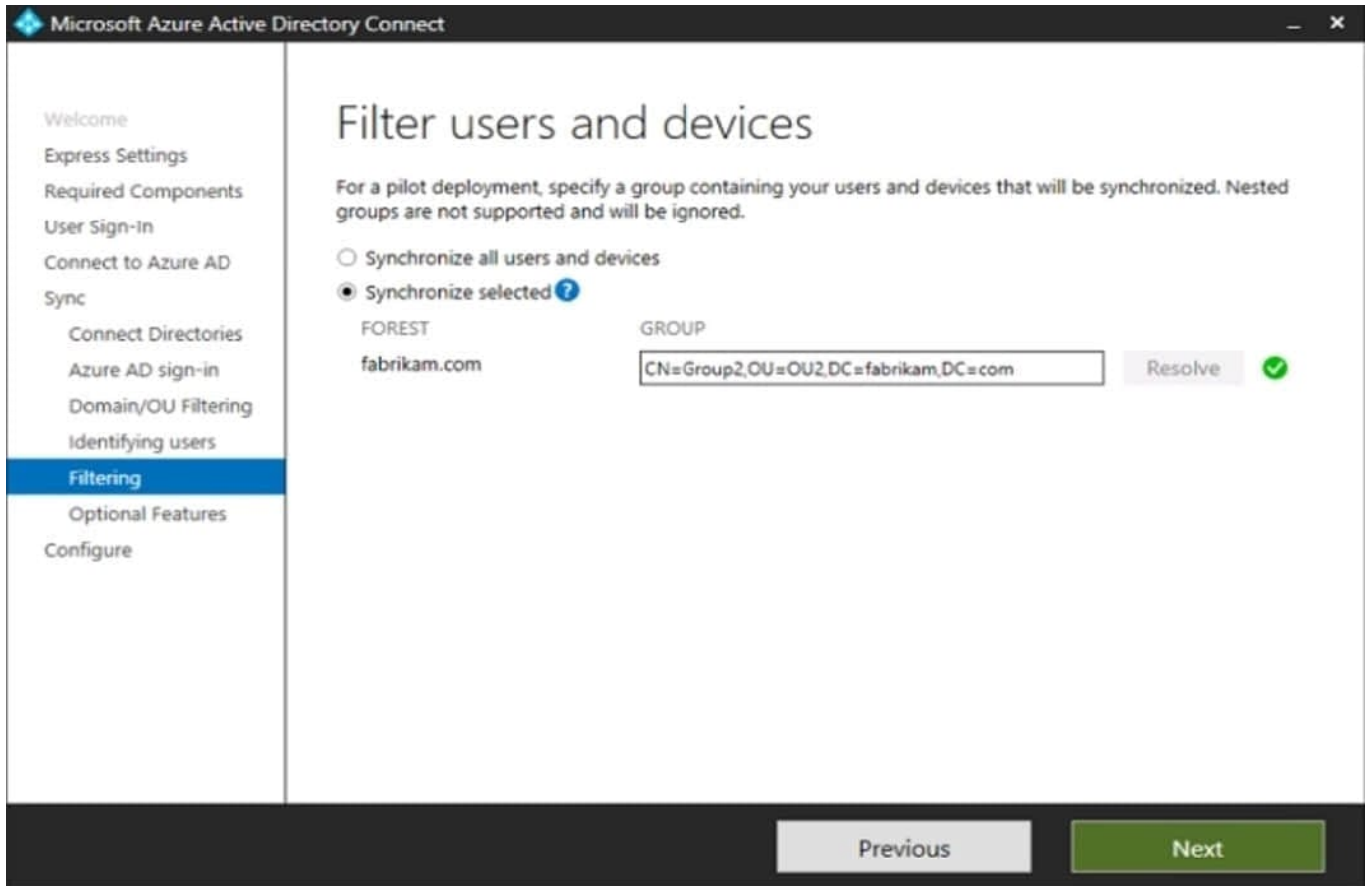
Group	Members
Group1	User1
Group2	User2, User3, Group1

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.

Hot Area:

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:

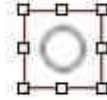
Answer Area

Statements

Yes

No

User2 will synchronize to Azure AD.



Group2 will synchronize to Azure AD.



User3 will synchronize to Azure AD.



QUESTION 12

HOTSPOT

You have a Microsoft 365 tenant that contains the compliance policies shown in the following table.

Name	Require BitLocker	Require the device to be at or under the machine risk score
Policy1	Required	High
Policy2	Not configured	Medium
Policy3	Required	Low

The tenant contains the devices shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Device1	Configured	High	Policy1, Policy3
Device2	Not configured	Medium	Policy2, Policy3
Device3	Not configured	Low	Policy1, Policy2



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

Hot Area:

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Device1 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 13

HOTSPOT

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

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.



Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress.	<input checked="" type="radio"/> Yes <input type="radio"/> No
Show time limit error when installation takes longer than specified number of minutes.	<input type="text" value="60"/>
Show custom message when time limit error occurs.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow users to collect logs about installation errors.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Only show page to devices provisioned by out-of-box experience (OOBE)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Block device use until all apps and profiles are installed	<input type="radio"/> Yes <input checked="" type="radio"/> No

You assign the policy to Group1.

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

Hot Area:



Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 14

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.



This website is blocked by your organization. Contact your administrator for more information.

Hosted by www.contoso.com

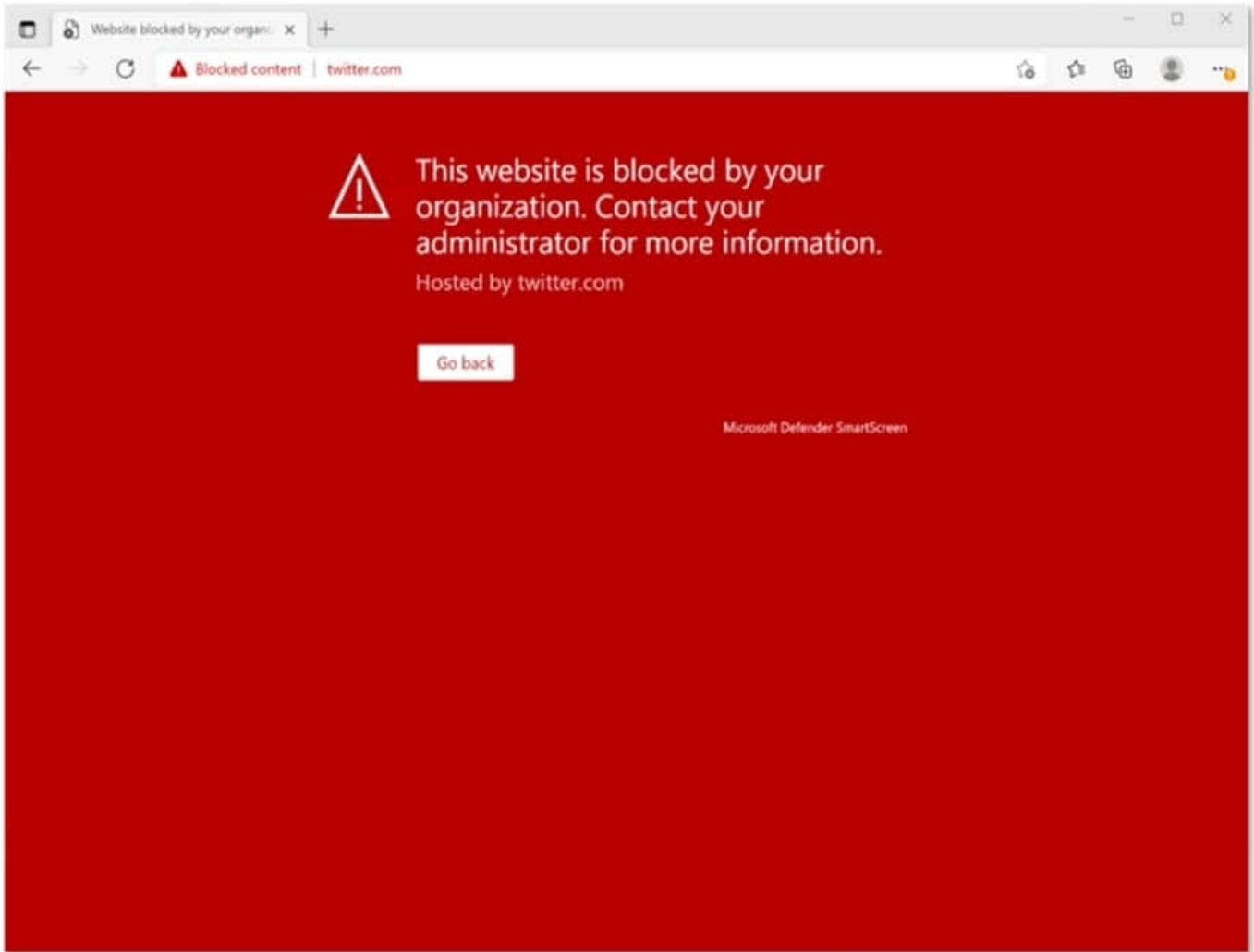
Go back

Microsoft Defender SmartScreen

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



This Website Is Blocked By Your Organization

Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.

Reference:

<https://jadexstrategic.com/web-protection/>

QUESTION 15

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

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?



A. Yes

B. No

Correct Answer: A

[Latest MS-102 Dumps](#)

[MS-102 PDF Dumps](#)

[MS-102 Exam Questions](#)