



-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1

Topic 1

HOTSPOT

This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.

To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.

A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study

To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Existing Environment

Microsoft Entra configuration

Contoso has an Azure subscription.

Contoso has a Microsoft 365 E5 subscription.

Contoso has a Microsoft Entra tenant named contoso.com. The tenant has an administrative unit named AU1 that contains the following membership rule.

`(device.deviceTrustType -eq "Workplace") and (device.deviceOSType -in ["Windows", "Android"])`

The tenant contains the cloud-only users shown in the following table.

The tenant contains the groups shown in the following table.

The tenant contains the devices shown in the following table.

All the devices are managed by using Microsoft Intune.

Microsoft Entra authentication methods

Contoso contains an Authentication methods policy for Microsoft Authenticator that has the following settings:

Include: Group1

Exclude: Group3

Authentication mode: Passwordless

Privileged Identity Management (PIM) configuration

Privileged roles are managed by using Privileged Identity Management (PIM).

The PIM settings for the AI Administrator role are configured as shown in the following table.

Email configuration

Each user has a Microsoft Exchange mailbox.

Contoso contains an anti-spam outbound policy named Antispam1 that has the following configurations:

Included groups: Group4

Excluded users: User2

Set an external message limit: 3

Set an internal message limit: 5

Set a daily message limit: 13

Restriction placed on users who reach the message limit: Restrict the user from sending mail

Microsoft SharePoint configuration

Contoso has a Microsoft SharePoint site named Site1 that stores the following types of content and various other documents:

Project documents: All the documents have a project code that includes the letters PR, followed by a dash and nine digits (for example PR-123456789).

Proposal documents: All the documents have a customer ID that includes seven to 10 alphanumerical characters. All the customer IDs are recorded in a Microsoft Excel workbook.

Feedback forms: All the documents were created by using the same template.

Microsoft AI services

Contoso implements the following Microsoft AI services:

Microsoft 365 Copilot for selected users

Microsoft Foundry agents, including an agent named Agent1

Requirements

Planned changes

Contoso plans to implement the following changes:

Issue new Android devices to the Group1 users.

Assign Microsoft 365 Copilot licenses to the users in Group1.

Add an additional email address alias for the users in Group4.

Create a Conditional Access policy named CAPolicy1 for Group3.

Disable web search for Microsoft 365 Copilot and Microsoft 365 Copilot Chat.

Create classifiers to identify project documents and proposal documents stored on Site1.

Technical requirements

Contoso identifies the following technical requirements:

The users in Group3 that access Microsoft 365 resources from anonymous IP addresses must complete multifactor authentication (MFA).

Microsoft 365 Copilot responses must NOT use content from the project documents stored on Site1.

Microsoft 365 Copilot responses must use content from only Microsoft 365 locations.

The total costs of Agent1 must be monitored and evaluated monthly.

All the Android devices must be registered in Microsoft Entra.

Administrative effort must be minimized.

Administrative costs must be minimized.

You need to evaluate the configuration of AU1.

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

NOTE: Each correct selection is worth one point.

Name	Role	Department
Admin1	Global Administrator	Research
Admin2	AI Administrator	Research
Admin3	Privileged Role Administrator	IT
User1	- None - Eligible for AI Administrator	IT
User2	None	Development

Name	Type	Membership rule	Members
Group1	Security	<i>Not applicable</i>	User1, Group2, and Group3
Group2	Security	(user.displayName -endsWith "1") or (user.department -eq "IT")	<i>Not applicable</i>
Group3	Security	<i>Not applicable</i>	User2
Group4	Microsoft 365	<i>Not applicable</i>	User1 and User2

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra joined
Device2	Windows 11	Microsoft Entra registered
Device3	iOS	Microsoft Entra registered

Setting	Value
Activation maximum duration (hours)	24 hour(s)
Require approval to activate	Yes
Approvers	None
Expire eligible assignments after	1 month(s)
Expire active assignments after	15 day(s)

Answer Area

Statements	Yes	No
Admin1 can add Device1 to AU1 directly.	☐	☐
Device2 is member of AU1.	☐	☐
The devices issued to Group1 will be added to AU1 automatically.	☐	☐

Suggested Answer:

Answer Area

Statements	Yes	No
Admin1 can add Device1 to AU1 directly.	☐	☒
Device2 is member of AU1.	☒	☐
The devices issued to Group1 will be added to AU1 automatically.	☐	☒

Explanation: AU1 uses a dynamic device membership rule, so members are controlled by the rule and cannot be added manually while dynamic membership is enabled. Device2 is Microsoft Entra registered, which corresponds to deviceTrustType = "Workplace", and it runs Windows. Therefore, it satisfies the AU1 membership rule and is a member of AU1. Issuing devices to members of Group1 does not automatically make those devices members of AU1. Dynamic administrative unit membership is evaluated from the device attributes specified in the rule, not from the group membership of the device users. Reference: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-members-dynamic?tabs=admin-center> <https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership>

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

DRAG DROP

You have a Microsoft 365 subscription.

You need to meet the following requirements.

Report a Microsoft 365 service issue.

Request help on how to add a new user to a Microsoft Entra tenant.

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features	Answer Area
⋮ Message center	To report issues regarding a Microsoft 365 service: Feature
⋮ New service request	To request help on how to add a new user to the tenant: Feature
⋮ Product feedback	
⋮ Service health	

Suggested Answer:

Features	Answer Area
⋮ Message center	To report issues regarding a Microsoft 365 service: ⋮ Service health
⋮ New service request	To request help on how to add a new user to the tenant: ⋮ New service request
⋮ Product feedback	
⋮ Service health	

Explanation: Use Service health to review Microsoft 365 service status and report service problems to Microsoft. Use New service request to contact Microsoft support when administrative assistance is required, such as help adding a user to the Microsoft Entra tenant.

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

You have a Microsoft 365 E5 subscription and use Microsoft Intune for managing mobile devices.

You need to access service health alerts from a mobile phone.

What should you use?

- A. Intune Company Portal
- B. the Intune app
- C. the Microsoft 365 Admin mobile app
- D. the Microsoft Authenticator app

Suggested Answer: C

Explanation: The Microsoft 365 Admin mobile app provides administrators with access to Microsoft 365 service health information and alerts from a mobile device. This allows administrators to monitor incidents and advisories without using the full web-based admin center.

 **Ginnious** Most Recent 4 weeks ago

Selected Answer: C

C. the Microsoft 365 Admin mobile app
upvoted 2 times

HOTSPOT

Your company has a Microsoft 365 subscription that contains the domains 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.

Domains

+ Add domain Buy domain Refresh

Domain name ↑

Status

Choose columns

☐	contoso221018.onmicrosoft.com (Default)	✓ Healthy
☐	contoso.com	ⓘ Incomplete setup
☐	east.contoso221018.onmicrosoft.com	ⓘ No services selected

Answer Area

An administrator can create usernames that contain the [answer choice].

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Exchange Online can receive inbound email messages sent to the [answer choice].

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Suggested Answer:

Answer Area

An administrator can create usernames that contain the **[answer choice]**.

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Exchange Online can receive inbound email messages sent to the **[answer choice]**.

contoso221018.onmicrosoft.com domain only
contoso221018.onmicrosoft.com domain and all its subdomains only
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Explanation: All three domains are present in the Microsoft 365 tenant and can be used as sign-in/username suffixes. The Incomplete setup status for contoso.com indicates that required service DNS configuration is not complete, not that the domain is unavailable for user identities. For inbound Exchange Online email, the domain must be configured for the Exchange service with the required DNS records. The default contoso221018.onmicrosoft.com domain is healthy, while contoso.com has incomplete setup and the east.contoso221018.onmicrosoft.com domain has no services selected.

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

HOTSPOT

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

You need to perform the following actions:

Create a shared mailbox named Mbox1 in the subscription.

Grant User1 the Send As permission for Mbox1.

Which Microsoft 365 portals can you use to perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create Mbox1:

Exchange admin center only
Microsoft 365 admin center only
Exchange admin center and Microsoft 365 admin center only
Exchange admin center and Microsoft Entra admin center only
Microsoft 365 admin center and Microsoft Entra admin center only
Exchange admin center, Microsoft 365 admin center, and Microsoft Entra admin center

Grant User1 the Send As permission:

Exchange admin center only
Microsoft 365 admin center only
Exchange admin center and Microsoft 365 admin center only
Exchange admin center and Microsoft Entra admin center only
Microsoft 365 admin center and Microsoft Entra admin center only
Exchange admin center, Microsoft 365 admin center, and Microsoft Entra admin center

Suggested Answer:

Answer Area

Create Mbox1:

Exchange admin center only
Microsoft 365 admin center only
Exchange admin center and Microsoft 365 admin center only
Exchange admin center and Microsoft Entra admin center only
Microsoft 365 admin center and Microsoft Entra admin center only
Exchange admin center, Microsoft 365 admin center, and Microsoft Entra admin center

Grant User1 the Send As permission:

Exchange admin center only
Microsoft 365 admin center only
Exchange admin center and Microsoft 365 admin center only
Exchange admin center and Microsoft Entra admin center only
Microsoft 365 admin center and Microsoft Entra admin center only
Exchange admin center, Microsoft 365 admin center, and Microsoft Entra admin center

Explanation: A shared mailbox can be created from either the Exchange admin center or the Microsoft 365 admin center. The Send As permission can also be assigned from either of those portals. Microsoft Entra admin center manages identities and directory objects, but it does not provide Exchange mailbox delegation management. Reference: <https://learn.microsoft.com/en-us/exchange/collaboration/shared-mailboxes/create-shared-mailboxes> <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/give-mailbox-permissions-to-another-user?view=o365-worldwide>

You have a Microsoft 365 subscription.

Your company has multiple branch offices, including a branch office named Branch1. The users in Branch1 connect to Microsoft 365 by using a corporate web proxy.

On the Network connectivity page in the Microsoft 365 admin center, Branch1 displays the following network insight:

"We're detecting WebSocket (WSS) connection failures to the domain: *.cloud.microsoft, which causes Copilot to not work correctly for your users."

HTTPS access to Microsoft 365 apps from Branch1 succeeds.

You need to resolve the insight without changing connectivity for the other branch offices.

What should you configure?

- A. the Branch1 web proxy policy to allow required protocols for the hosts in *.cloud.microsoft
- B. the Branch1 DNS resolver policy to optimize regional name resolution for the hosts in *.cloud.microsoft
- C. the Branch1 web proxy policy to exempt hosts in *.cloud.microsoft from TLS inspection
- D. the Branch1 firewall policy to allow HTTPS connections for the hosts in *.cloud.microsoft

Suggested Answer: A

Explanation: The insight specifically identifies WebSocket (WSS) connection failures to *.cloud.microsoft. Configure the Branch1 web proxy policy to permit WebSocket protocol upgrades and WSS connections to hosts in that wildcard domain. HTTPS already works, so simply allowing HTTPS does not address the failed WebSocket connections. Reference: <https://learn.microsoft.com/en-us/microsoft-365/enterprise/office-365-network-mac-perf-insights?view=o365-worldwide> <https://learn.microsoft.com/en-us/microsoft-365/enterprise/office-365-network-mac-perf-connection-blockers?view=o365-worldwide>

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

You have a Microsoft 365 subscription that has an initial domain named contoso.onmicrosoft.com and two verified custom domains named contoso.com and fabrikam.com.

The contoso.com domain is NOT the default domain. No users, groups, or applications reference contoso.com.

The subscription contains the administrator accounts shown in the following table.

You need to delete contoso.com by using an account that is assigned the minimum required Microsoft Entra role.

Which account should you use?

Name	Role
admin1@contoso.onmicrosoft.com	Domain Name Administrator
admin2@fabrikam.com	Global Administrator
admin3@fabrikam.com	User Administrator
admin4@contoso.onmicrosoft.com	License Administrator

- A. admin4@contoso.onmicrosoft.com
- B. admin3@fabrikam.com
- C. admin2@fabrikam.com
- D. admin1@contoso.onmicrosoft.com

Suggested Answer: D

Explanation: The Domain Name Administrator role provides the least privilege required to manage verified custom domains in Microsoft Entra, including removing a custom domain when it is not the default domain and no users, groups, or applications reference it. Since contoso.com meets those removal prerequisites, the account assigned this role is sufficient.

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

HOTSPOT

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

You need to configure tenant notifications to meet the following requirements.

Group1: Receive email notifications when major service updates occur.

Group2: Receive email alerts when Microsoft 365 maintenance event occur.

Which type of notification should you configure for each group?

Answer Area

Group1:

	▼
Message Center Preferences	
Organization messages	
Service Health alerts	
Software updates	

Group2:

	▼
Message Center Preferences	
Organization messages	
Service Health alerts	
Software updates	

Suggested Answer:

Answer Area

Group1:

	▼
Message Center Preferences	
Organization messages	
Service Health alerts	
Software updates	

Group2:

	▼
Message Center Preferences	
Organization messages	
Service Health alerts	
Software updates	

Explanation: Use Message Center Preferences to configure email notifications for major Microsoft 365 service updates and changes announced through Message center. Use Service Health alerts to notify administrators about service incidents and planned maintenance events that can affect Microsoft 365 availability or performance.

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

You have a Microsoft 365 subscription that has an initial domain named contoso.onmicrosoft.com and two verified custom domains named contoso.com and fabrikam.com.

The fabrikam.com domain is the default domain.

The contoso.com domain uses managed authentication, and has 750 references across unused user accounts, application identifier URLs, and mail-enabled security groups.

You need to remove contoso.com from the subscription. The solution must minimize manual changes to Microsoft Entra objects.

What should you do?

- A. Rename all the user, group, and application references in the Microsoft Entra admin center, and then delete contoso.com.
- B. Use the `-ForceDelete` option for contoso.com without changing the mail-enabled security group references.
- C. Update or remove the mail-enabled security group references, and then use the `-ForceDelete` option for contoso.com.
- D. Make contoso.com the default domain, and then delete contoso.com.

Suggested Answer: C

Explanation: The domain has fewer than 1,000 references and uses managed authentication, so ForceDelete can automatically update supported user, group, and application references to the initial onmicrosoft.com domain. However, Exchange-provisioned references, including mail-enabled security groups, must be updated or removed first. After those references are cleaned up, ForceDelete minimizes the remaining manual changes. Reference: <https://learn.microsoft.com/en-us/entra/identity/users/domains-manage> <https://learn.microsoft.com/en-us/graph/api/domain-forcedelete?view=graph-rest-1.0&tabs=http>

 **Skri113xX** Most Recent 1 week ago

Selected Answer: A

A maybe

upvoted 1 times

HOTSPOT

You have a Microsoft 365 subscription that contains a security group named Group1. The object ID of Group1 is stored in a PowerShell variable named \$groupId.

You have a CSV file named C:\Temp\members.csv that contains a column named memberObjectId. The column stores the directory object ID of each user that will be added to Group1.

You need to perform a bulk membership update for Group1 by using Microsoft Graph PowerShell.

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

NOTE: Each correct selection is worth one point.

Answer Area

▼	-Scopes "GroupMember.ReadWrite.All"
Connect-MgGraph Find-MgGraphCommand Get-MgContext Import-Module	

```
$members = Import-Csv -Path "C:\Temp\members.csv"
foreach ($member in $members) {
```

▼	-GroupId \$groupId -OdataId "https://graph.microsoft.com/v1.0/directoryObjects/\$(\$member.ObjectId) "
Get-MgGroupMember New-MgGroupMemberByRef New-MgGroupOwnerByRef Update-MgGroup	

```
}
Disconnect-MgGraph
```

Suggested Answer:

Answer Area

▼	-Scopes "GroupMember.ReadWrite.All"
Connect-MgGraph Find-MgGraphCommand Get-MgContext Import-Module	

```
$members = Import-Csv -Path "C:\Temp\members.csv"
foreach ($member in $members) {
```

▼	-GroupId \$groupId -OdataId "https://graph.microsoft.com/v1.0/directoryObjects/\$(\$member.ObjectId) "
Get-MgGroupMember New-MgGroupMemberByRef New-MgGroupOwnerByRef Update-MgGroup	

```
}
Disconnect-MgGraph
```

Explanation: Connect-MgGraph establishes a Microsoft Graph PowerShell session with the required GroupMember.ReadWrite.All permission. New-MgGroupMemberByRef adds each referenced directory object as a member of Group1 by using the group ID and the user's directory object ID.

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

You have a Microsoft 365 subscription that contains a distribution list named Group1.

Group1 does NOT have nested groups and is used by project members to send emails.

You need to provide the project members with group-based collaboration resources. The solution must meet the following requirements:

- Enable group owners to manage the membership of Group1
- Provide a shared calendar and shared files
- Support Microsoft Teams integration
- Minimize administrative effort

What should you do?

- A. Create a Microsoft SharePoint team site
- B. Create a dynamic security group
- C. Upgrade Group1 to a Microsoft 365 group
- D. Create a mail-enabled security group

Suggested Answer: C

Explanation: Upgrade Group1 to a Microsoft 365 group. This preserves the existing group-based membership model while adding collaboration resources such as a shared mailbox, shared calendar, SharePoint-based shared files, and Microsoft Teams integration. Group owners can manage membership directly, which minimizes administrative effort.

 **lightthetorch** Most Recent 2 weeks ago

Selected Answer: C

Upgrading Group1 to a Microsoft 365 group would be the only option to satisfy all 4 of these requirements at once.

upvoted 1 times

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Portal:

	▼
The Microsoft 365 admin center	
The Microsoft Defender portal	
The Microsoft Entra admin center	
The Microsoft Purview portal	

Group types:

	▼
Microsoft 365 only	
Security only	
Security and mail-enabled security only	
Microsoft 365 and distribution only	
Microsoft 365, mail-enabled security, and distribution only	
Security, Microsoft 365, mail-enabled security, and distribution	

Suggested Answer:

Answer Area

Portal:

	▼
The Microsoft 365 admin center	
The Microsoft Defender portal	
The Microsoft Entra admin center	
The Microsoft Purview portal	

Group types:

	▼
Microsoft 365 only	
Security only	
Security and mail-enabled security only	
Microsoft 365 and distribution only	
Microsoft 365, mail-enabled security, and distribution only	
Security, Microsoft 365, mail-enabled security, and distribution	

Explanation: A Microsoft 365 group naming policy is configured in the Microsoft Entra admin center. The policy applies to Microsoft 365 groups, including groups created through services such as Outlook and Teams, but it does not apply to security groups, mail-enabled security groups, or distribution groups.

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

HOTSPOT

This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.

To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.

A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study

To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Existing Environment

Microsoft Entra configuration

Contoso has an Azure subscription.

Contoso has a Microsoft 365 E5 subscription.

Contoso has a Microsoft Entra tenant named contoso.com. The tenant has an administrative unit named AU1 that contains the following membership rule.

`(device.deviceTrustType -eq "Workplace") and (device.deviceOSType -in ["Windows", "Android"])`

The tenant contains the cloud-only users shown in the following table.

The tenant contains the groups shown in the following table.

The tenant contains the devices shown in the following table.

All the devices are managed by using Microsoft Intune.

Microsoft Entra authentication methods

Contoso contains an Authentication methods policy for Microsoft Authenticator that has the following settings:

- Include: Group1
- Exclude: Group3
- Authentication mode: Passwordless

Privileged Identity Management (PIM) configuration

Privileged roles are managed by using Privileged Identity Management (PIM).

The PIM settings for the AI Administrator role are configured as shown in the following table.

Email configuration

Each user has a Microsoft Exchange mailbox.

Contoso contains an anti-spam outbound policy named Antispam1 that has the following configurations:

- Included groups: Group4
- Excluded users: User2
- Set an external message limit: 3
- Set an internal message limit: 5
- Set a daily message limit: 13
- Restriction placed on users who reach the message limit: Restrict the user from sending mail

Microsoft SharePoint configuration

Contoso has a Microsoft SharePoint site named Site1 that stores the following types of content and various other documents:

- Project documents: All the documents have a project code that includes the letters PR, followed by a dash and nine digits (for example PR-123456789).
- Proposal documents: All the documents have a customer ID that includes seven to 10 alphanumeric characters. All the customer IDs are recorded in a Microsoft Excel workbook.
- Feedback forms: All the documents were created by using the same template.

Microsoft AI services

Contoso implements the following Microsoft AI services:

- Microsoft 365 Copilot for selected users
- Microsoft Foundry agents, including an agent named Agent1

Requirements

Planned changes

Contoso plans to implement the following changes:

- Issue new Android devices to the Group1 users.
- Assign Microsoft 365 Copilot licenses to the users in Group1.
- Add an additional email address alias for the users in Group4.
- Create a Conditional Access policy named CAPolicy1 for Group3.
- Disable web search for Microsoft 365 Copilot and Microsoft 365 Copilot Chat.
- Create classifiers to identify project documents and proposal documents stored on Site1.

Technical requirements

Contoso identifies the following technical requirements:

- The users in Group3 that access Microsoft 365 resources from anonymous IP addresses must complete multifactor authentication (MFA).
- Microsoft 365 Copilot responses must NOT use content from the project documents stored on Site1.
- Microsoft 365 Copilot responses must use content from only Microsoft 365 locations.
- The total costs of Agent1 must be monitored and evaluated monthly.
- All the Android devices must be registered in Microsoft Entra.
- Administrative effort must be minimized.
- Administrative costs must be minimized.

You need to implement CAPolicy1. The solution must meet the technical requirements.

Which two Conditional Access settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Name	Role	Department
Admin1	Global Administrator	Research
Admin2	AI Administrator	Research
Admin3	Privileged Role Administrator	IT
User1	- None - Eligible for AI Administrator	IT
User2	None	Development

Name	Type	Membership rule	Members
Group1	Security	<i>Not applicable</i>	User1, Group2, and Group3
Group2	Security	(user.displayName -endsWith "1") or (user.department -eq "IT")	<i>Not applicable</i>
Group3	Security	<i>Not applicable</i>	User2
Group4	Microsoft 365	<i>Not applicable</i>	User1 and User2

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra joined
Device2	Windows 11	Microsoft Entra registered
Device3	iOS	Microsoft Entra registered

Setting	Value
Activation maximum duration (hours)	24 hour(s)
Require approval to activate	Yes
Approvers	None
Expire eligible assignments after	1 month(s)
Expire active assignments after	15 day(s)

New ...

Conditional Access policy

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

Name *

CAPolicy1 ✓

Assignments

Users or agents (Preview) ⓘ

[Specific users included](#)

Target resources ⓘ

[All resources \(formerly 'All cloud apps'\)](#)

Network ⓘ

[Not configured](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant * ⓘ

0 controls selected

Session * ⓘ

[0 controls selected](#)

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ
User risk level is the likelihood that the user account is compromised.
[Not configured](#)

Sign-in risk ⓘ
Sign-in risk level is the likelihood that the sign-in session is compromised.
[Not configured](#)

Insider risk ⓘ
Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.
[Not configured](#)

Device platforms ⓘ
[Not configured](#)

Locations ⓘ
[Not configured](#)

Client apps ⓘ
[Not configured](#)

Filter for devices ⓘ
[Not configured](#)

Authentication flows ⓘ
[Not configured](#)

Suggested Answer:

Answer Area

New

Conditional Access policy

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

Name *

CAPolicy1

Assignments

Users or agents (Preview)

[Specific users included](#)

Target resources

[All resources \(formerly 'All cloud apps'\)](#)

Network

[Not configured](#)

Conditions

[0 conditions selected](#)

Access controls

Grant *

[0 controls selected](#)

Session *

[0 controls selected](#)

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk

User risk level is the likelihood that the user account is compromised.

[Not configured](#)

Sign-in risk

Sign-in risk level is the likelihood that the sign-in session is compromised.

[Not configured](#)

Insider risk

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

[Not configured](#)

Device platforms

[Not configured](#)

Locations

[Not configured](#)

Client apps

[Not configured](#)

Filter for devices

[Not configured](#)

Authentication flows

[Not configured](#)

Explanation: Configure the Sign-in risk condition to target risky sign-ins associated with anonymous IP addresses. Microsoft Entra ID Protection recognizes activity from anonymous IP addresses as a sign-in risk signal. Configure the Grant access control to Require multifactor authentication, ensuring that affected Group3 users must complete MFA before accessing Microsoft 365 resources.

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

You have a Microsoft 365 subscription that contains a Microsoft SharePoint communication site named Site1 and a security group named Group1.

Some users that are outside of Group1 have direct permissions or sharing links to the content in Site1.

You need to ensure that users can access Site1 and its content only when they meet both of the following conditions.

- The user is a member of Group1.
- The user has SharePoint permissions to the content.

The solution must meet the following requirements:

- Apply only to Site1.
- Preserve the existing SharePoint permissions.
- Minimize administrative effort.

What should you do?

- A. Configure sharing restrictions outside of Restricted Access Control groups
- B. Configure Restricted Content Discovery for Site1
- C. Configure Restricted Access Control for Site1
- D. Configure site permissions for Site1

Suggested Answer: C

Explanation: Configure Restricted Access Control for Site1 and specify Group1. Restricted Access Control adds an additional authorization requirement: users must both belong to an allowed group and already have the required SharePoint permissions. It applies at the site level, preserves existing permissions and sharing configuration, and avoids manually restructuring Site1 permissions.

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

You have a Microsoft 365 subscription.

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

You apply Retention1 to all the Microsoft OneDrive content.

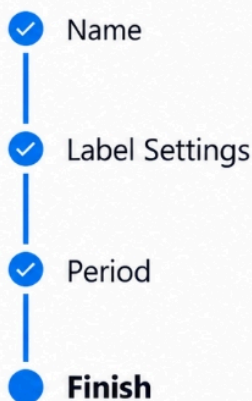
On January 1, 2025, a user stores a file named File1 in OneDrive.

On January 10, 2025, the user modifies File1.

On February 1, 2025, the user deletes File1.

When will File1 be removed permanently and unrecoverable from OneDrive?

Create retention label



Review and finish

Name

Name
Retention1
[Edit](#)

Retention settings

Retention period
6 months
[Edit](#)

Retention action
Retain and Delete
[Edit](#)

- A. February 1, 2025
- B. July, 2025
- C. July 10, 2025
- D. August 1, 2025

Suggested Answer: B

Explanation: Retention1 retains the file for six months based on when the item was created and then deletes it. File1 was created on January 1, 2025, so its retention period ends on July 1, 2025. The later modification and user deletion do not reset this creation-based retention period.

Reference: <https://learn.microsoft.com/en-us/purview/retention?tabs=table-override> <https://learn.microsoft.com/en-us/purview/retention-settings>

  **saidkha** Most Recent 2 weeks ago

Selected Answer: C

I think it should be from the date it has been modified + 93 days
upvoted 1 times

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

- A. the user overrides of the DLP policy rule
- B. the locations of the DLP policy
- C. the status of the DLP policy
- D. the conditions of the DLP policy rule

Suggested Answer: B

Explanation: Configure the locations of the DLP policy so that it applies to both Exchange email and SharePoint sites. The existing behavior shows that SharePoint is already covered, while email is not being evaluated by the policy. Adding the Exchange location ensures credit card information is protected from external sharing through email as well.

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

HOTSPOT

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

The Global Administrator role has the Privileged Identity Management (PIM) settings shown in the following table.

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

NOTE: Each correct selection is worth one point.

Name	Role	Role assignment type
User1	Global Administrator	Eligible
User2	Global Administrator	Assigned
User3	Global Administrator	Eligible

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
Expire eligible assignments after	15 Days

Answer Area**Statements****Yes****No**

User1 must provide justification to activate the Global Administrator role.

☐☐

User2 must perform multifactor authentication (MFA) to activate the Global Administrator role.

☐☐

After eight hours, User3 will no longer be able to activate the Global Administrator role.

☐☐

Suggested Answer:

Answer Area

Statements	Yes	No
User1 must provide justification to activate the Global Administrator role.	☒	☐
User2 must perform multifactor authentication (MFA) to activate the Global Administrator role.	☐	☒
After eight hours, User3 will no longer be able to activate the Global Administrator role.	☐	☒

Explanation: User1 has an eligible Global Administrator assignment, so activating the role requires the configured PIM activation controls, including justification. User2 has the role assigned rather than eligible, so the role is already active and does not require PIM activation or activation-time MFA. The eight-hour setting is the maximum duration of an activated role session. It does not limit how long User3 remains eligible to activate the role. User3's eligibility expires after 15 days.

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

You have a Microsoft 365 subscription.

You need to create a Conditional Access policy that blocks sign-ins for the following scenarios:

- Activity from anonymous IP address.
- Impossible travel between two geographical locations.

Which condition should you configure for the policy?

- A. Locations
- B. Insider risk
- C. User risk
- D. Sign-in risk

Suggested Answer: *D*

Explanation: Configure the Sign-in risk condition. Microsoft Entra ID Protection evaluates risk signals associated with a specific authentication attempt, including sign-ins from anonymous IP addresses and impossible travel between geographically distant locations.

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

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. Strict protection is enabled for all recipients.

The subscription contains a group named Group1 that contains all the mailboxes for your company's marketing department.

Several marketing department mailboxes recently sent high volumes of external email after a credential was compromised.

You need to enforce a lower external message limit for Group1. The solution must automatically restrict senders that reach the limit.

What should you do?

- A. Create a custom anti-spam outbound policy.
- B. Modify the default anti-spam outbound policy.
- C. Modify the Strict protection settings.
- D. Configure the Standard preset security policy.
- E. Create a custom anti-spam inbound policy.

Suggested Answer: A

Explanation: Create a custom anti-spam outbound policy and scope it to Group1. Outbound spam policies let you configure lower external message limits for selected users or groups and specify that users who reach the limit are automatically restricted from sending additional email.

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

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to enable passwordless authentication for all users.

Which authentication method and portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Authentication method:

	▼
Email OTP	
Microsoft Authenticator	
SMS	
Voice call	

Portal:

	▼
Microsoft 365 admin center	
Microsoft Defender portal	
Microsoft Entra admin center	

Suggested Answer:

Answer Area

Authentication method:

	▼
Email OTP	
Microsoft Authenticator	
SMS	
Voice call	

Portal:

	▼
Microsoft 365 admin center	
Microsoft Defender portal	
Microsoft Entra admin center	

Explanation: Microsoft Authenticator supports passwordless phone sign-in for Microsoft Entra users. The authentication method policy is configured in the Microsoft Entra admin center, where passwordless Microsoft Authenticator can be enabled for the required users or groups.

You have a Microsoft 365 subscription.

Several support engineers at your company require temporary access to Microsoft Entra administrator roles.

You need to configure role access for the engineers. The solution must meet the following requirements:

- The engineers must activate role access before role use.
- Role access must expire automatically after activation.

What should you do?

- A. Create an administrative unit and assign the required roles to the engineers at the scope of the administrative unit.
- B. Assign the engineers as active members of a role-assignable group that has the required role assignments.
- C. Create an access package that includes the required administrative resources and assign the package to the engineers.
- D. Assign the engineers as eligible for the required roles by using Privileged Identity Management (PIM).

Suggested Answer: D

Explanation: Assign the engineers as eligible for the required Microsoft Entra roles through Privileged Identity Management (PIM). Eligible assignments require users to activate the role before use, and PIM can enforce a limited activation duration so the elevated access expires automatically after the configured period.

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

HOTSPOT

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

Users collaborate on files in Microsoft Teams. Files that are identified as malicious cannot be opened, moved, copied, and shared, but users can still save local copies.

You need to configure file-based protection for the collaboration workloads. The solution must meet the following requirements:

- Apply malware protection to the files stored in Teams.
- Prevent users from retaining local copies of files identified as malicious.

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

NOTE: Each correct selection is worth one point.

Answer Area

To apply malware protection:

Create a Teams policy
Configure Safe Links for Teams
Run the Set-CsTeamsFilesPolicy cmdlet
Configure Safe Attachments for Microsoft SharePoint, OneDrive, and Teams

To prevent local copies:

Configure external sharing in SharePoint
Configure a site-level access restriction
Set Default sharing link type to Only people in your organization
Run the Set-SPOTenant cmdlet to prevent users from downloading infected files

Suggested Answer:

Answer Area

To apply malware protection:

Create a Teams policy
Configure Safe Links for Teams
Run the Set-CsTeamsFilesPolicy cmdlet
Configure Safe Attachments for Microsoft SharePoint, OneDrive, and Teams

To prevent local copies:

Configure external sharing in SharePoint
Configure a site-level access restriction
Set Default sharing link type to Only people in your organization
Run the Set-SPOTenant cmdlet to prevent users from downloading infected files

Explanation: Safe Attachments for SharePoint, OneDrive, and Teams scans files stored in collaboration workloads and blocks access to files identified as malicious. Use Set-SPOTenant with the infected-file download restriction enabled to prevent users from downloading malicious files locally, closing the remaining path for retaining copies of files that Defender has identified as infected.

HOTSPOT

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

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
- Priority: 0
- Include these users, groups and domains
 - Users: User3
 - Groups: Group1
- Exclude these users, groups and domains
 - Groups: Group2
- Message limits
 - Set a daily message limit: 100

- Name: AntiSpam2
- Priority: 1
- Include these users, groups and domains
 - Users: User1
 - Groups: Group2
- Exclude these users, groups and domains
 - Users: User3
- Message limits
 - Set a daily message limit: 50

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

NOTE: Each correct selection is worth one point.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

Answer Area**Statements**

User1 can send a maximum of 150 email messages per day.

Yes☐**No**☐

User2 can send a maximum of 50 email messages per day.

☐☐

User3 can send a maximum of 100 email messages per day.

☐☐

Suggested Answer:

Answer Area

Statements

User1 can send a maximum of 150 email messages per day.

Yes

☐

No

☒

User2 can send a maximum of 50 email messages per day.

☒☐

User3 can send a maximum of 100 email messages per day.

☐☒

Explanation: User1 matches AntiSpam1 through Group1 and also matches AntiSpam2 directly. Because AntiSpam1 has the higher priority, only its 100-message daily limit applies; policy limits aren't added together. User2 is excluded from AntiSpam1 because the user belongs to Group2. AntiSpam2 therefore applies through Group2 and enforces the 50-message daily limit. User3 is excluded from both custom policies: Group2 excludes the user from AntiSpam1, and User3 is explicitly excluded from AntiSpam2. Therefore, neither custom policy's 100-message limit applies. Reference: <https://learn.microsoft.com/en-us/defender-office-365/outbound-spam-policies-configure> <https://learn.microsoft.com/en-us/defender-office-365/anti-spam-policies-troubleshooting>

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

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named Admin1.

Your company deploys a new branch office named Branch1.

You need to provide Admin1 with the ability to manage Branch1. The solution must meet the following requirements:

- Admin1 must only be able to manage users that have Office location set to Branch1.
- Admin1 must be able to reset passwords, manage user licenses, and modify user attributes only for the users in Branch1.

What should you use to organize the Branch1 users, and which role should you assign to Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use:

	▼
An administrator unit	
A Microsoft 365 group	
A security group	

Role:

	▼
Help Desk Administrator	
Password Administrator	
User Administrator	

Suggested Answer:

Answer Area

Use:

	▼
An administrator unit	
A Microsoft 365 group	
A security group	

Role:

	▼
Help Desk Administrator	
Password Administrator	
User Administrator	

Explanation: An administrative unit can scope administrative permissions to only the Branch1 users, and it can use dynamic membership based on user attributes such as Office location. A scoped User Administrator can manage user properties, reset passwords, and manage licenses for users within that administrative unit. Reference: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units> <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/manage-roles-portal?tabs=admin-center>

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

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint site named Site1. Site1 contains the files shown in the following table.

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:

- Name: AutoLabel1
- Label to auto-apply: Sensitivity1
- Choose locations where you want to apply the label: Site1

The Define content that contains sensitive info settings for AutoLabel1 is 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.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

Define content that contains sensitive info

Choose a category of industry regulations to see the classification groups you can use to classify that information or create a custom group.

 **Content contains** 



Sensitive info types

IP Address

High confidence  

Instance count to  

Add 

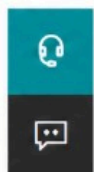
 Create group

 Add condition 

Back

Next

Cancel



Answer Area

Statements	Yes	No
Sensitivity1 is applied to File1.docx	☐	☐
Sensitivity1 is applied to File2.txt	☐	☐
Sensitivity1 is applied to File3.xlsx	☐	☐

Suggested Answer:

Answer Area

Statements	Yes	No
Sensitivity1 is applied to File1.docx	☐	☒
Sensitivity1 is applied to File2.txt	☒	☐
Sensitivity1 is applied to File3.xlsx	☒	☐

Explanation: The auto-labeling condition requires the IP Address sensitive information type at High confidence with an instance count of 2 or more. File1.docx contains only one matching instance, so the label is not applied. File2.txt contains two matching instances and File3.xlsx contains five, so both meet the configured threshold and receive the Sensitivity1 label.

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

HOTSPOT

You have a Microsoft Entra tenant that contains a cloud app named Payroll and three groups named Group1, Group2, and Group3.

Group2 is a member of Group1.

The subscription contains the users shown in the following table.

The subscription has the Conditional Access policies shown in the following table.

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

NOTE: Each correct selection is worth one point.

Name	Description
User1	User in Group2
User2	B2B collaboration guest user that is NOT in any groups
User3	User in Group1 and Group3

Name	Users and groups	Target resources	Access controls
CA1	Include: Group1 Exclude: Group3	Payroll	Grant access: Require multifactor authentication
CA2	Include all users Exclude: Group1 and Group3	Payroll	Block access

Answer Area**Statements****Yes****No**

User2 is prevented from accessing Payroll

☐☐

User1 must complete multifactor authentication (MFA) before accessing Payroll

☐☐

User3 must complete multifactor authentication (MFA) before accessing Payroll

☐☐