



MS-500^{Q&As}

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

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

<https://www.geekcert.com/ms-500.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

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a published sensitivity label named Sensitivity1.

You plan to create an Azure Active Directory group named Group1 and assign Sensitivity1 to Group1.

How should you configure Group1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Setting:	<div><div></div><div>▼</div><div>ClassificationDescriptions</div><div>ClassificationList</div><div>DefaultClassification</div><div>EnableMIPLabels</div></div>
Type:	<div><div></div><div>▼</div><div>Distribution</div><div>Mail-enabled security</div><div>Microsoft 365</div><div>Security</div></div>

Correct Answer:



Answer Area

Setting:

	▼
ClassificationDescriptions	
ClassificationList	
DefaultClassification	
EnableMIPLabels	

Type:

	▼
Distribution	
Mail-enabled security	
Microsoft 365	
Security	

Box 1: EnableMIPLabels

The sensitivity label option is only displayed for groups when all the following conditions are met:

1.

The feature is enabled, EnableMIPLabels is set to True in from the Azure AD PowerShell module.

2.

The group is a Microsoft 365 group.

3.

Etc.

Box 2: Microsoft 365 Incorrect:

* Not ClassificationList:

Classic classifications are the old classifications you set up by defining values for the ClassificationList setting in Azure AD PowerShell. When this feature is enabled, those classifications will not be applied to groups.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels>



QUESTION 2

Your company has a Microsoft 365 subscription that includes a user named User1.

You suspect that User1 sent email messages to a competitor detailing company secrets.

You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.

What should you include in the recommendation?

- A. Enable In-Place Archiving for the mailbox of User1
- B. From the Security and Compliance, perform a content search of the mailbox of User1
- C. Place a Litigation Hold on the mailbox of User1
- D. Configure message delivery restrictions for the mailbox of User1

Correct Answer: C

A Litigation Hold is a feature that allows you to preserve all mailbox data, including deleted items, for a specified period of time. This means that if User1 deleted any email messages sent to the competitor, they will still be preserved and available for review.

QUESTION 3

HOTSPOT

You have a Microsoft 365 subscription that uses a default name of litwareinc.com.

You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.



Links

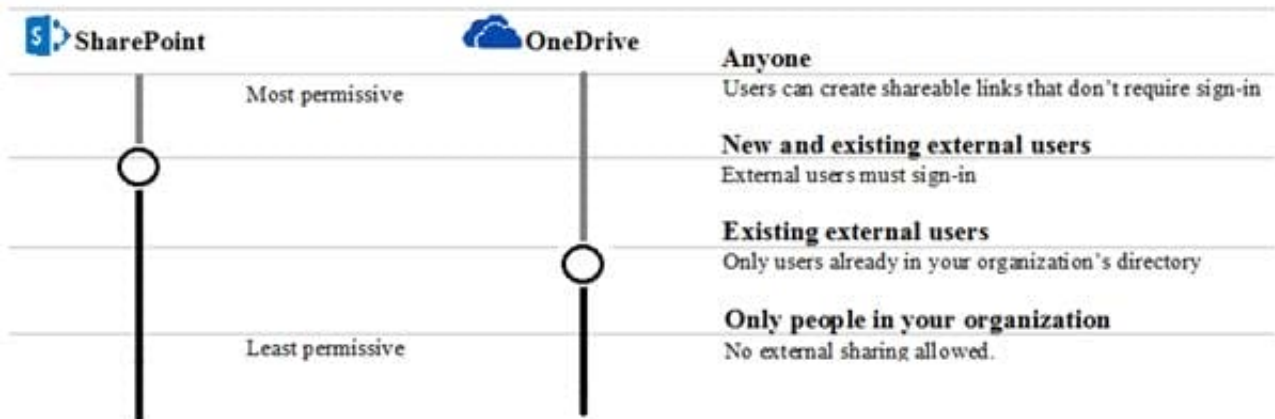
Choose the kind of link that's selected by default when users share items.

Default link type

- ☒ Shareable: Anyone with the link
- ☐ Internal: Only people in your organization
- ☐ Direct: Specific people

External sharing

Users can share with:



Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

- ☒ Allow or block sharing with people on specific domains
- Allow only these domains: Contoso.com, Adatum.com

[Add domains](#)

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

NOTE: Each correct selection is worth one point.

Hot Area:



A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

Correct Answer:

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

References: <https://docs.microsoft.com/en-us/onedrive/manage-sharing>



QUESTION 4

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

You plan to use Compliance Manager.

You need to ensure that User1 can assign Compliance Manager roles to users. The solution must use the principle of least privilege.

Which role should you assign to User1?

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

Correct Answer: C

Reference:

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

QUESTION 5

You have a Microsoft 165 E5 subscription.

You need to enable support for sensitivity labels in Microsoft SharePoint Online.

What should you use?

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

Correct Answer: C

Use the Microsoft Purview compliance portal to enable support for sensitivity labels

This option is the easiest way to enable sensitivity labels for SharePoint and OneDrive, but you must sign in as a global administrator for your tenant.

1.

Sign in to the Microsoft Purview compliance portal as a global administrator, and navigate to Solutions > Information protection > Labels

2.



If you see a message to turn on the ability to process content in Office online files, select Turn on now:

Information protection

[Labels](#) [Label policies](#) [Auto-labeling](#)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

① Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn on here, but note that additional configuration is required for Multi-Geo environments. [Learn more](#)

Turn on now

[+ Create a label](#) [Publish labels](#) [Refresh](#)

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

QUESTION 6

You need to ensure that SharepointAdmins@contoso.com receives an alert when a user establishes a sync relationship to a document library from a computer that is a member of an Active Directory (AD) domain.

To complete this task, sign in to the Microsoft Office 365 admin center.

Correct Answer: See explanation below.

1.

Navigate to Manage Alerts in the Security and Compliance Center.

2.


On the Activity alerts page, click + New.


3.

Complete the following fields to create an activity alert:

The flyout page to create an activity alert is displayed.






Name * 

Description 

Alert type

Custom ▾





Send this alert when... *  

Activities *

Choose activities for alert ▾

Users:

Show results for all users

Send this alert to... *  

Recipients *

Show results for all users

a.

Name - Type a name for the alert. Alert names must be unique within your organization.

b.

Description (Optional) - Describe the alert, such as the activities and users being tracked, and the users that email notifications are sent to. Descriptions provide a quick and easy way to describe the purpose of the alert to other admins.

c.

Alert type - Make sure the Custom option is selected.



d.

Send this alert when - Click Send this alert when and then configure these two fields:

Activities - Click the drop-down list to display the activities that you can create an alert for. This is the same activities list that's displayed when you search the Office 365 audit log. You can select one or more specific activities or you can click

the activity group name to select all activities in the group. For a description of these activities, see the "Audited activities" section in Search the audit log. When a user performs any of the activities that you've added to the alert, an email

notification is sent.

Users - Click this box and then select one or more users. If the users in this box perform the activities that you added to the Activities box, an alert will be sent. Leave the Users box blank to send an alert when any user in your organization

performs the activities specified by the alert.

e.

Send this alert to - Click Send this alert, and then click in the Recipients box and type a name to add a user's who will receive an email notification when a user (specified in the Users box) performs an activity (specified in the Activities

box). Note that you are added to the list of recipients by default. You can remove your name from this list.

4. Click Save to create the alert.

The new alert is displayed in the list on the Activity alerts page.

Activity alerts			
Name	Recipients	Status ▲	Date modified
Executive mailbox alert	compliance@contoso.com	On	2016-06-08 14:42:02
SharePoint upload alert	admin@contoso.com	Off	2016-06-08 14:23:39
External sharing alert	admin@contoso.com	Off	2016-06-08 14:24:08

The status of the alert is set to On. Note that the recipients who will receive an email notification when an alert is sent are also listed.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/create-activity-alerts?view=o365-worldwide>

QUESTION 7

HOTSPOT

You have a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.



From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security play.

You need to ensure that you can add the security playbook and the custom query to the rule.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Set the template type of the analytics rule to: ▼
Fusion
Scheduled
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
A trigger
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Correct Answer:



Set the template type of the analytics rule to: ▼
Fusion
Scheduled
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
A trigger
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Box 1: Scheduled Create a custom analytics rule with a scheduled query

1.
From the Microsoft Sentinel navigation menu, select Analytics.
2.
In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.
3.
Etc.

Box 2: A trigger

Use triggers and actions in Microsoft Sentinel playbooks.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom> <https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions#microsoft-sentinel-triggers-summary>

QUESTION 8



You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You have a Data Subject Request (DSR) case named Case1.

You need to allow User1 to export the results of Case1. The solution must use the principle of least privilege.

Which role should you assign to User1 for Case1?

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

Correct Answer: A

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

QUESTION 9

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and a sensitivity label named Label1.

The external sharing settings for Site1 are configured as shown in the Site1 exhibit. (Click the Site1 tab.)



Sharing

The sharing settings available for this site depend on your organization-level settings. [Learn more about the external sharing settings](#)

External sharing

Site content can be shared with:

- ☐ Anyone
Users can share files and folders using links that don't require sign-in.
- ☐ New and existing guests
Guests must sign in or provide a verification code.
- ☐ Existing guests only
Only guests already in your organization's directory.
- ☒ Only people in your organization
No external sharing allowed.

The external sharing settings for Label1 are configured as shown in the Label1 exhibit. (Click the Label1 tab.)



Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

☒ Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

☒ Anyone ⓘ

Users can share files and folders using links that don't require sign-in.

☐ New and existing guests ⓘ

Guests must sign in or provide a verification code.

☐ Existing guests ⓘ

Only guests in your organization's directory.

☐ Only people in your organization

No external sharing allowed.

☐ Use Azure AD Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

Label 1 is applied to Site1.

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
Internal users can share documents on Site1 with external users.	<input type="radio"/>	<input type="radio"/>
External users require an invitation to access Site1.	<input type="radio"/>	<input type="radio"/>
Only users on managed devices can access Site1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

**Statements****Yes****No**

Internal users can share documents on Site1 with external users.

☒☐

External users require an invitation to access Site1.

☐☒

Only users on managed devices can access Site1.

☐☒

Box 1: Yes

The Sensitive label setting of Label1 in the second exhibit 2overrides the setting in exhibit 1.

Box 2: No Box 3: No

QUESTION 10

Several users in your Microsoft 365 subscription report that they received an email message without attachment.

You need to review the attachments that were removed from the messages.

Which two tools can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. the Exchange admin center
- B. the Azure ATP admin center
- C. Outlook on the web
- D. the Security and Compliance admin center
- E. Microsoft Azure Security Center

Correct Answer: AD

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files>

QUESTION 11

You have a Microsoft 365 E5 subscription.

Some users are required to use an authenticator app to access Microsoft SharePoint Online.

You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.



What should you do?

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

Correct Answer: A

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

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1.

From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

2.

From the Azure Active Directory admin center, view the sign-ins. Other incorrect answer options you may see on the exam include the following:

1.

From Azure Log Analytics, query the logs.

2.

From the Microsoft 365 Compliance center, perform an audit log search.

3.

From the Microsoft 365 Defender portal, download a report.

Reference:

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

QUESTION 12

HOTSPOT

You have a Microsoft 365 subscription. From the Security and Compliance admin center, you create the retention policies shown in the following table.



Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 is configured as shown in the following exhibit.

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 1 years ▾

☐ No, just delete content that's older than ⓘ

1 years ▾

Delete the content based on when it was created ▾ ⓘ

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

Policy2 is configured as shown in the following exhibit.



Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 3 years ▾

Retain the content based on when it was created ▾ ⓘ

Do you want us to delete it after this time?

☐ Yes ☒ No

☐ No, just delete content that's older than ⓘ

1 years ▾

Need more options?

☐ Use advanced retention settings ⓘ

Back Next Cancel

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

Hot Area:

Answer Area

	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

Correct Answer:



Answer Area

Yes

No

If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019

☒☐

If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019

☒☐

If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022

☐☒

Principles of retention:

- Retention wins over deletion
- Longest retention period wins
- Explicit inclusion wins over implicit inclusion
- Shortest deletion period wins

Source: <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence>

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-orwhat-takes-precedence>

QUESTION 13

You need to ensure that a user named Allan Deyoung uses multi-factor authentication (MFA) for all authentication requests.

To complete this task, sign in to the Microsoft 365 admin center.

Correct Answer: See explanation below.

1.

Open the Admin Center and go to Users > Active Users

2.

Open Multi-factor authentication

Don't select any user yet, just open the Multi-factor authentication screen. You will find the button in the toolbar.



LazyAdmin.nl

Active users

Add a user	Add multiple users	Multi-factor authentication	Refresh	Export Users	...
Display name ↑		Username			Licenses
Elise Mens					Office 365 E3
info					Office 365 F1
Rudy Mens					Microsoft Flow Free, Off

3. Open the Service settings

Before we start enabling MFA for the users, we first go through the service settings. The button to the settings screen doesn't stand out, but it's just below the title

multi-factor authentication users **service settings**

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to](#) Before you begin, take a look at the [multi-factor auth deployment guide](#).

bulk update

View: Sign-in allowed users



Multi-Factor Auth status: Any

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Elise Mens		Disabled
<input type="checkbox"/>	info		Disabled
<input type="checkbox"/>	Rudy Mens		Disabled



4. Setup MFA Office 365

A few settings are important here:

1.

Make sure you check the App password. Otherwise, users can't authenticate in some applications (like the default mail app in Android).

2.

Also, take a look at the remember function. By default, it is set to 14 days.

multi-factor authentication

users service settings

app passwords

- ☒ Allow users to create app passwords to sign in to non-browser apps
- ☐ Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

- ☒ Call to phone
- ☒ Text message to phone
- ☒ Notification through mobile app
- ☒ Verification code from mobile app or hardware token

remember multi-factor authentication

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

save

5. Enable MFA for Office 365 users

After you have set the settings to your liking click on save and then on users (just below the title Multi-factor authentication).

You see the list of your users again. Here you can select single or multiple users to enable MFA.



At the moment you enable Office 365 MFA for a user it can get the setup screen as soon as the users browse to one of the Office 365 products.

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

View: Multi-Factor Auth status:

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Elise Mens		Disabled
<input type="checkbox"/>	info		Disabled
<input checked="" type="checkbox"/>	Rudy Mens		Disabled

Rudy Mens

quick steps

Enable

Manage user settings

Reference: <https://lazyadmin.nl/office-365/how-to-setup-mfa-in-office-365/>

QUESTION 14

You have a Microsoft 365 E5 subscription.

You need to use Attack simulation training to launch a credential harvest simulation.

For which Microsoft 365 workloads can you create a payload?

- A. Microsoft Exchange Online only
- B. Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive
- C. Microsoft Teams and Exchange Online only
- D. Microsoft SharePoint Online and OneDrive only

Correct Answer: A

Create a payload, select a payload type.

On the Select type page, the only value that you can currently select is Email.

Incorrect:



Not A, Not B, Not C: Payloads cannot be created for Microsoft Exchange Online.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-payloads>

QUESTION 15

HOTSPOT

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

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

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

1.

Assignments: Include Group1, Exclude Group2

2.

Conditions: Sign in risk of Low and above

3.

Access: Allow access, Require password change

You need to identify how the policy affects User1 and User2.

What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Must change their password:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 nor User2	

Prompted for MFA:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 nor User2	

Correct Answer:

Must change their password:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 nor User2	

Prompted for MFA:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 nor User2	

Box 1: User1 only



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

User 1 needs to change the Password.

Box 2: User2 only

MFA will be triggered for User 2.

Reference:

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

[MS-500 PDF Dumps](#)

[MS-500 Practice Test](#)

[MS-500 Braindumps](#)