# 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.pass2lead.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**

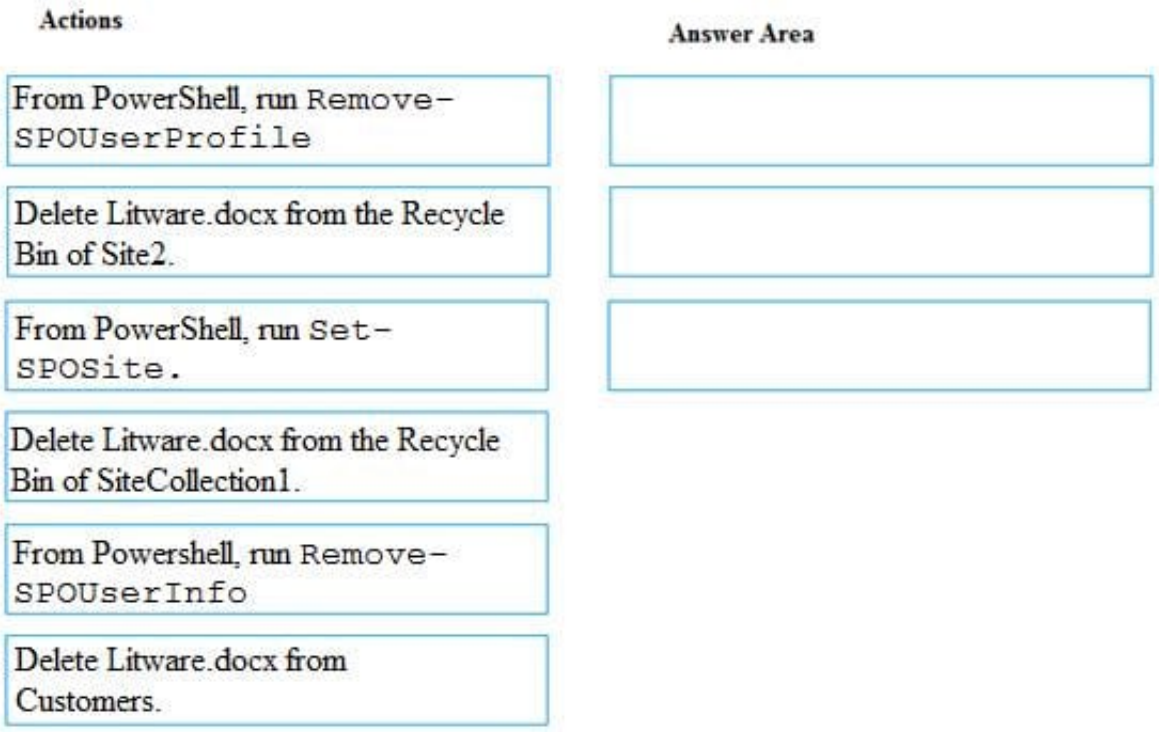
You have a Microsoft 365 subscription.

You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.

Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:




Correct Answer:

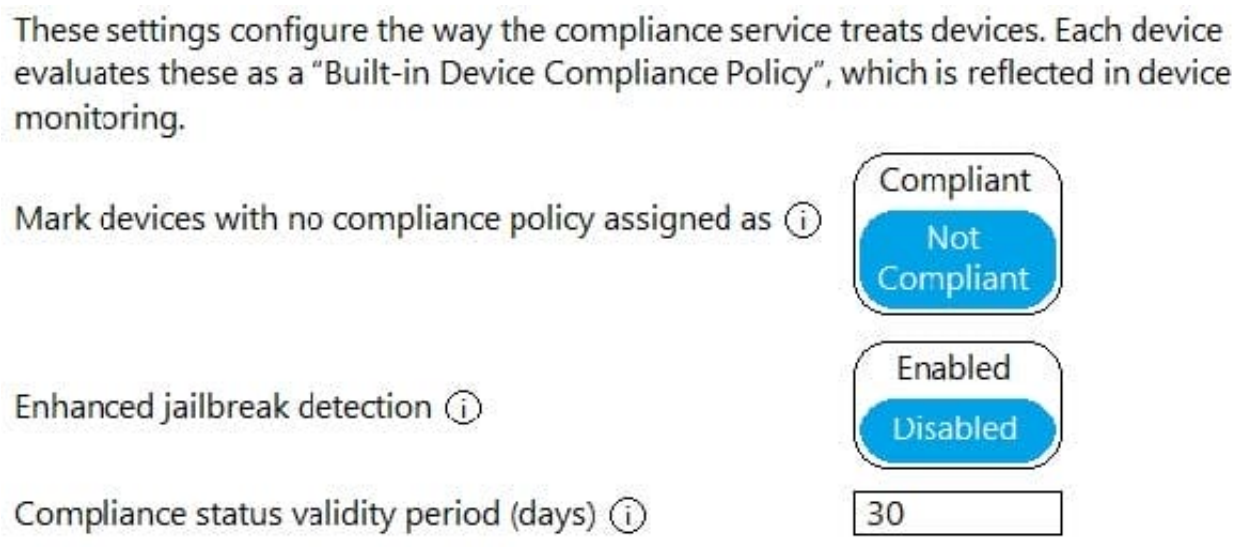
| Actions | Answer Area |
| --- | --- |
| From PowerShell, run `Remove-SPOUserProfile` | Delete Litware.docx from Customers. |
| | Delete Litware.docx from the Recycle Bin of Site2. |
| From PowerShell, run `Set-SPOSite.` | Delete Litware.docx from the Recycle Bin of SiteCollection1. |
| From Powershell, run `Remove-SPOUserInfo` | |

**QUESTION 2**

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager.

The Compliance policy settings are configured as shown in the following exhibit.




On February 25, 2020, you create the device compliance policies shown in the following table.

| Name | Require BitLocker Drive Encryption (BitLocker) | Require Secure Boot | Mark device as not compliant | Assigned to |
|---|---|---|---|---|
| Policy1 | Yes | No | 5 days after noncompliance | Group1 |
| Policy2 | No | Yes | 10 days after noncompliance | Group1, Group2 |

On March 1. 2020, users enroll Windows 10 devices in Microsoft Endpoint Manager as shown in the following table

| Name | BitLocker enabled | Secure Boot enabled | Member of |
|---|---|---|---|
| Device1 | Yes | No | Group1 |
| Device2 | No | No | Group2 |

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| On March 2, 2020, Device2 is marked as compliant. | ○ | ○ |
| On March 6, 2020, Device1 is marked as compliant. | ○ | ○ |
| On March 12, 2020, Device1 is marked as compliant. | ○ | ○ |

Correct Answer:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| On March 2, 2020, Device2 is marked as compliant. | ○ | ○ |
| On March 6, 2020, Device1 is marked as compliant. | ○ | ○ |
| On March 12, 2020, Device1 is marked as compliant. | ○ | ○ |

Box 1: Yes

Device2 is in Group2 so Policy2 applies.

Device2 is not compliant with Policy2. However, the device won\\'t be marked as non-compliant until 10 days after the device was enrolled.

Box 2: Yes

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2. However, the device won\\'t be marked as non-compliant until 10 days after the device was enrolled.

Box 3: No

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2.

March 12th is more than 10 days after the device was enrolled so it will now be marked as non-compliant by Policy2.

---

**QUESTION 3**

HOTSPOT

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

| Name | Type | Email address |
|---|---|---|
| Group1 | Security Group – Domain Local | Group1@contoso.com |
| Group2 | Security Group – Universal | None |
| Group3 | Distribution Group – Global | None |
| Group4 | Distribution Group – Universal | Group4@contoso.com |

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

| Name | Type | Membership type |
|---|---|---|
| Group11 | Security group | Assigned |
| Group12 | Security group | Dynamic |
| Group13 | Office 365 | Assigned |
| Group14 | Mail-enabled security group | Assigned |

You create a sensitivity label named Label1.

You need to publish Label1.

To which groups can you publish Label1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

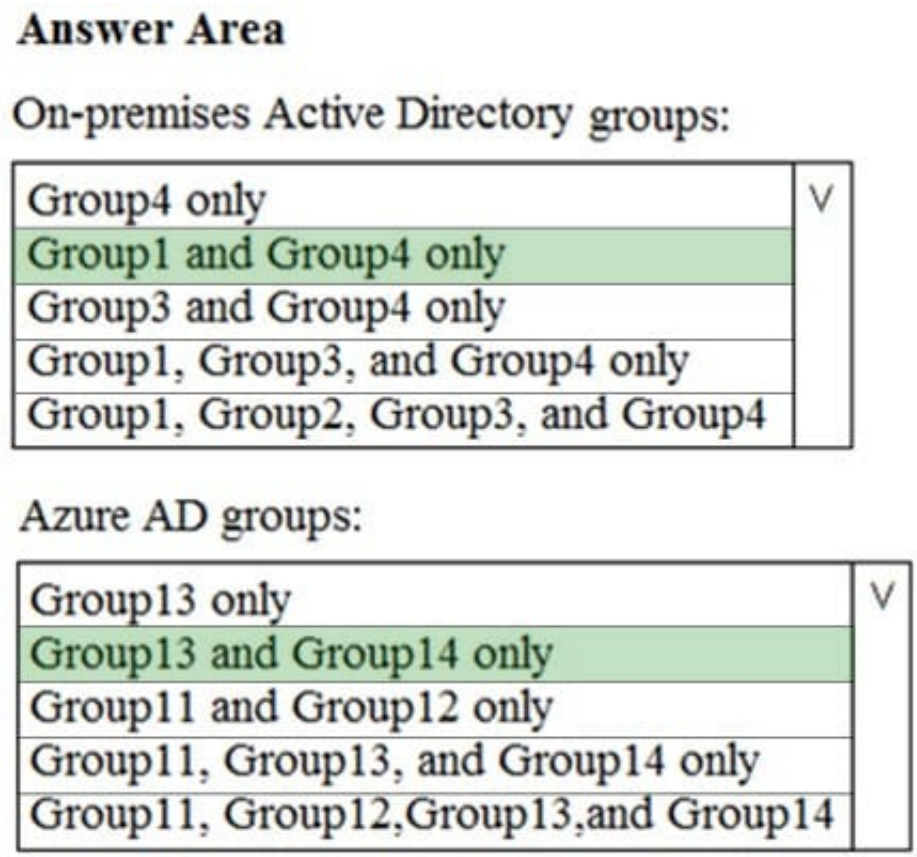
On-premises Active Directory groups:

| |
|---|
| Group4 only ∨ |
| Group1 and Group4 only |
| Group3 and Group4 only |
| Group1, Group3, and Group4 only |
| Group1, Group2, Group3, and Group4 |

Azure AD groups:

| |
|---|
| Group13 only ∨ |
| Group13 and Group14 only |
| Group11 and Group12 only |
| Group11, Group13, and Group14 only |
| Group11, Group12,Group13,and Group14 |

Correct Answer:




The groups must be mail-enabled.

Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.

Reference:

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

**QUESTION 4**

HOTSPOT

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

| Name | User principal name(UPN) | Member of |
|---|---|---|
| User1 | User1@contoso.com | Group1 |
| User2 | User2@contoso.com | Group2 |
| User3 | User3@contoso.com | Group2 |

Group1 is member of a group named Group3.

The Azure Active Directory (Azure AD) tenant contains the Windows 10 devices shown in the following table.

| Name | Join type | Owner | Mmeber of |
|---|---|---|---|
| Device1 | Azure AD-registered | User3 | Group4 |
| Device2 | Azure AD-joined | User2 | Group5 |

Microsoft Endpoint Manager has the devices shown in the following table.

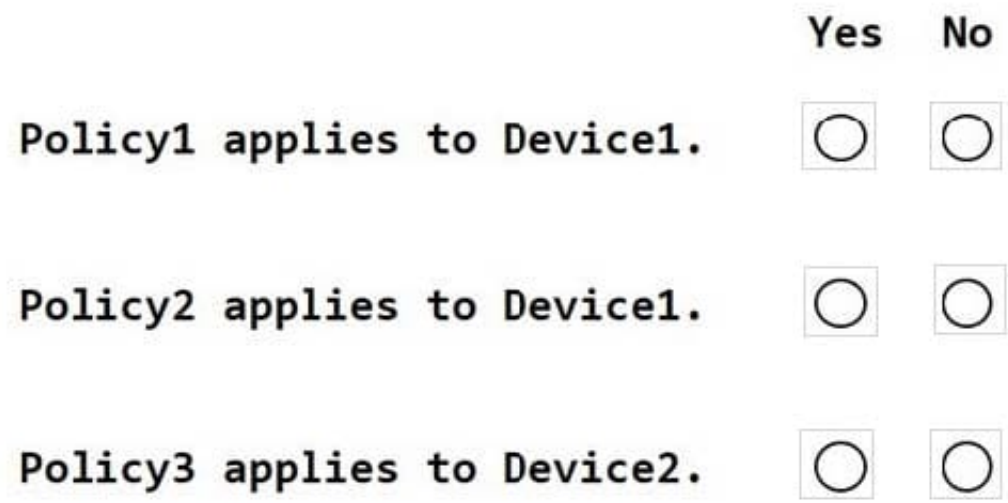
| Name | Enrolled by UPN |
|---|---|
| Device1 | User1@contoso.com |
| Device2 | User2@contoso.com |

Microsoft Endpoint Manager contains the compliance policies shown in the following table.

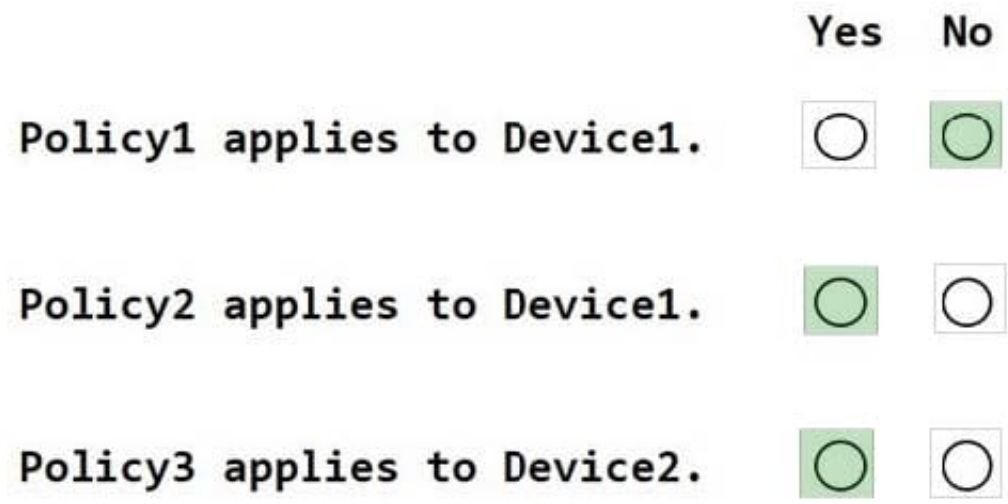
| Name | Assignment |
|---|---|
| Policy1 | Group3 |
| Policy2 | Group4 |
| Policy3 | Group2 |

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

Hot Area:




Correct Answer:




Deploy to users in user groups or devices in device groups. When a compliance policy is deployed to a user, all the user\\'s devices are checked for compliance. Using device groups in this scenario helps with compliance reporting.

**QUESTION 5**

HOTSPOT

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

You enroll devices in Microsoft Intune as shown in the following table.

| Name | Platform | Group |
|---|---|---|
| Device1 | Android | Group1, Group3 |
| Device2 | iOS | Group1, Group2 |
| Device1 | Android | Group3 |

Each device has two line-of-business apps named App1 and App2 installed.

You create application control policies targeted to all the app types in Microsoft Endpoint Manager as shown in the following table.

| Name | Platform | Deployed to | Protected apps |
|---|---|---|---|
| Policy1 | Android | Group3 | App2 |
| Policy2 | iOS | Group2 | App2 |
| Policy3 | Android | Group1 | App1 |

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 |
|---|---|---|
| Policy1 applies to Device1. | ○ | ○ |
| When User1 signs in to Device1, App1 is protected. | ○ | ○ |
| When User1 signs in to Device2, App1 is protected. | ○ | ○ |

Correct Answer:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Policy1 applies to Device1. | ○ | ○ |
| When User1 signs in to Device1, App1 is protected. | ○ | ○ |
| When User1 signs in to Device2, App1 is protected. | ○ | ○ |

Box 1: Yes

Device1 is an Android device in Group3 (and Group1). Policy1 applies to Android devices in Group3. Therefore, Policy1 does apply to Device1.

Box 2: Yes

Policy3 protects App1 for Android devices in Group1. Device1 is in Group1 (and Group3). Therefore, App1 is protected on Device1.

Box 3: No

Device2 is an iOS device in Group1 and Group2. Policy2 applies to iOS devices in Group2. However, Policy2 only protects App2. It does not protect App1.

Policy3 applies to Group1 and protects App1. However, Policy3 only applies to Android devices in Group1. It does not apply to iOS devices. Therefore, Policy3 does not apply to Device2 so App1 is not protected on Device2.