MS-100$^{\text{Q\&As}}$

Microsoft 365 Identity and Services

QUESTION 1

You need to meet the security requirement for the vendors.

What should you do?

A. From Azure Cloud Shell, run the Set-MsolUserPrincipalName and specify the -tenantID parameter.

B. From Azure Cloud Shell, run the Set-AzureADUserExtension cmdlet.

C. Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the-UserPrincipalName parameter.

D. From Azure Cloud Shell, run the New-AzureADMSInvitation cmdlet and specify the -InvitedUserEmailAddress parameter.

Correct Answer: D

Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.

You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user\\'s account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest

user must then redeem their invitation to access resources. An invitation of a user does not expire.

The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question,the vendors already have Microsoft accounts so they can authenticate using them.

In this solution, we are creating guest account invitations by using the New-AzureADMSInvitation cmdlet and specifying the -InvitedUserEmailAddress parameter.

Note:

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

1.

From the Azure portal, create guest accounts.

2.

From Azure Cloud Shell, run the New-AzureADMSInvitation cmdlet and specify the ?€andquot;InvitedUserEmailAddress parameter.

Other incorrect answer options you may see on the exam include the following:

1.

From the Azure portal, modify the authentication methods.

2.

From the Azure portal, add an identity provider.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator https://docs.microsoft.com/enus/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

QUESTION 2

You have a Microsoft 365 subscription that contains Microsoft 365 Apps for enterprise.

Users report that they cannot install Microsoft Office 365 apps from the Office portal.

You need to ensure that the users can install Office 365 apps.

What should you do?

A. From the Microsoft 365 admin center, configure Office on the web.

B. From the Microsoft 365 admin center, configure Office installation options.

C. From the Microsoft 365 admin center, configure Office Scripts.

D. From the Microsoft 365 admin center, enable user consent to apps.

Correct Answer: B

Explanation:

Manage Microsoft 365 installation options in the Microsoft 365 admin center

As a Microsoft 365 admin, you can choose to do the following tasks on the Microsoft 365 installation options page in the Microsoft 365 admin center:

Choose how often to get feature updates for Office

Manage which version of Office is installed, including

Roll back to a previous version

Skip an upcoming version

Choose whether users can install Office on their own devices

Reference:

https://learn.microsoft.com/en-us/deployoffice/manage-software-download-settings-office-365

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 from the Security and Compliance admin center?

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

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

C. Modify the default safe links policy.

D. Create a new safe links policy.

Correct Answer: D

ATP Safe Links, a feature of Office 365 Advanced Threat Protection (ATP), can help protect your organization from malicious links used in phishing and other attacks. If you have the necessary permissions for the Office 365 Security and Compliance Center, you can set up ATP Safe Links policies to help ensure that when people click web addresses (URLs), your organization is protected. Your ATP Safe Links policies can be configured to scan URLs in email and URLs in Office documents.

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

QUESTION 4

Your network contains an Active Directory domain named contoso.com.

All users authenticate by using a third-party authentication solution.

You purchase Microsoft 365 and plan to implement several Microsoft 365 services.

You need to recommend an identity strategy that meets the following requirements:

1.

Provides seamless SSO

2.

Minimizes the number of additional servers required to support the solution

3.

Stores the passwords of all the users in Microsoft Azure Active Directory (Azure AD)

4.

Ensures that all the users authenticate to Microsoft 365 by using their on-premises user account

You are evaluating the implementation of federation.

Which two requirements are met by using federation? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. minimizes the number of additional servers required to support the solution

B. provides seamless SSO

C. stores the passwords of all the users in Azure AD

D. ensures that all the users authenticate to Microsoft 365 by using their on-premises user account

Correct Answer: BD

When you choose this federation as the authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user\\'s password. AD FS can use on-premise Active Directory as an authentication provider. AD FS can also provide SSO when using Active Directory as an authentication provider.

Incorrect Answers:

A: Additional servers are required to support the AD FS infrastructure.

C: The passwords are not synchronised to Azure AD.

Reference: https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

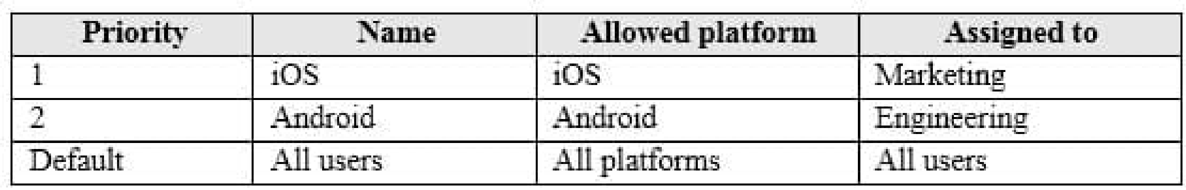
QUESTION 5

HOTSPOT

Your company has a Microsoft 365 tenant.

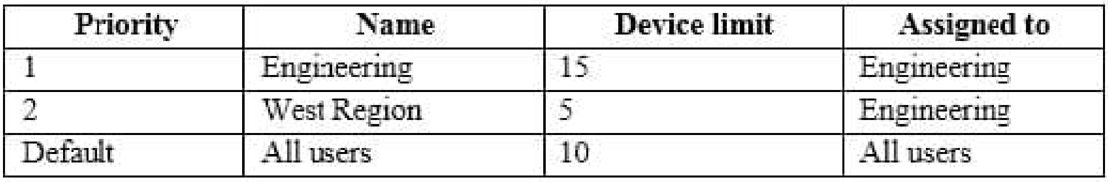
You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

The device type restrictions 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

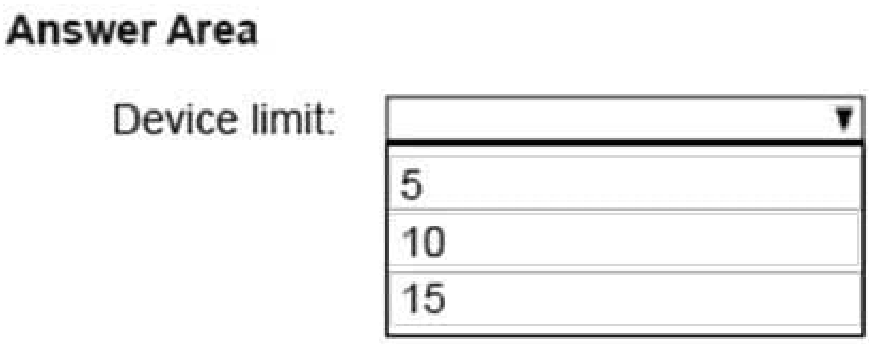
The device limit restrictions are configured as shown in the following table.



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

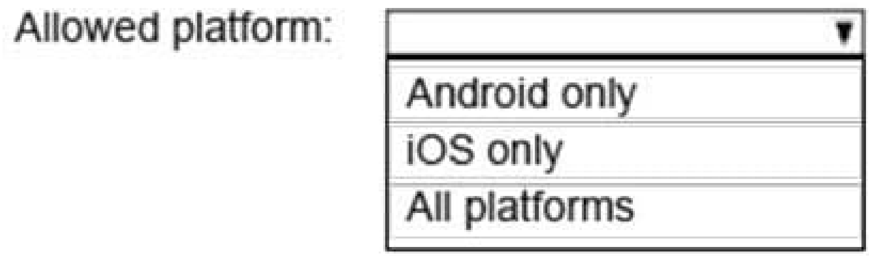
What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



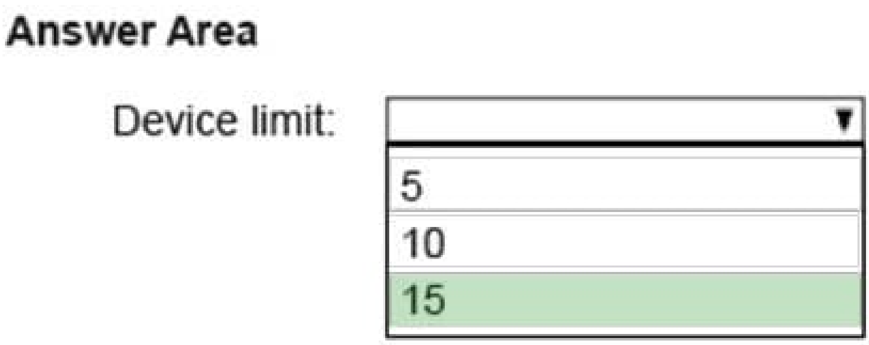
Answer Area

Device limit:
5
10
15



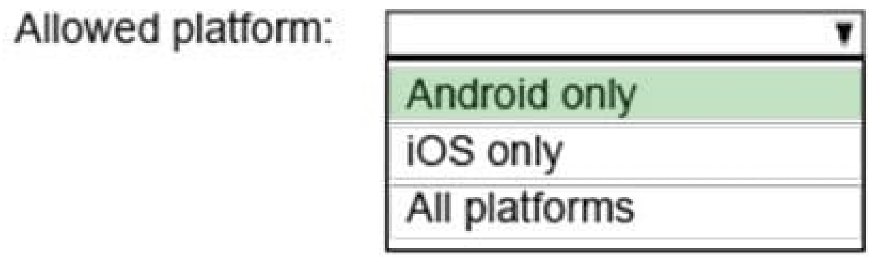
Allowed platform:
Android only
iOS only
All platforms

Correct Answer:



Answer Area

Device limit:
5
10
[✓ 15]



Allowed platform:
[✓ Android only]
iOS only
All platforms

When multiple policies are applied to groups that users are a member of, only the highest priority (lowest number) policy applies.

In this case, the Engineering users are assigned two device type policies (the default policy and the priority 2 policy). The priority 2 policy has a higher priority than the default policy so the Engineers' allowed platform is Android only.

The engineers have two device limit restrictions policies applied them. The priority1 policy is a higher priority than the priority2 policy so the priority1 policy device limit (15) applies.

Reference:

https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set