Microsoft

MS-100 Exam

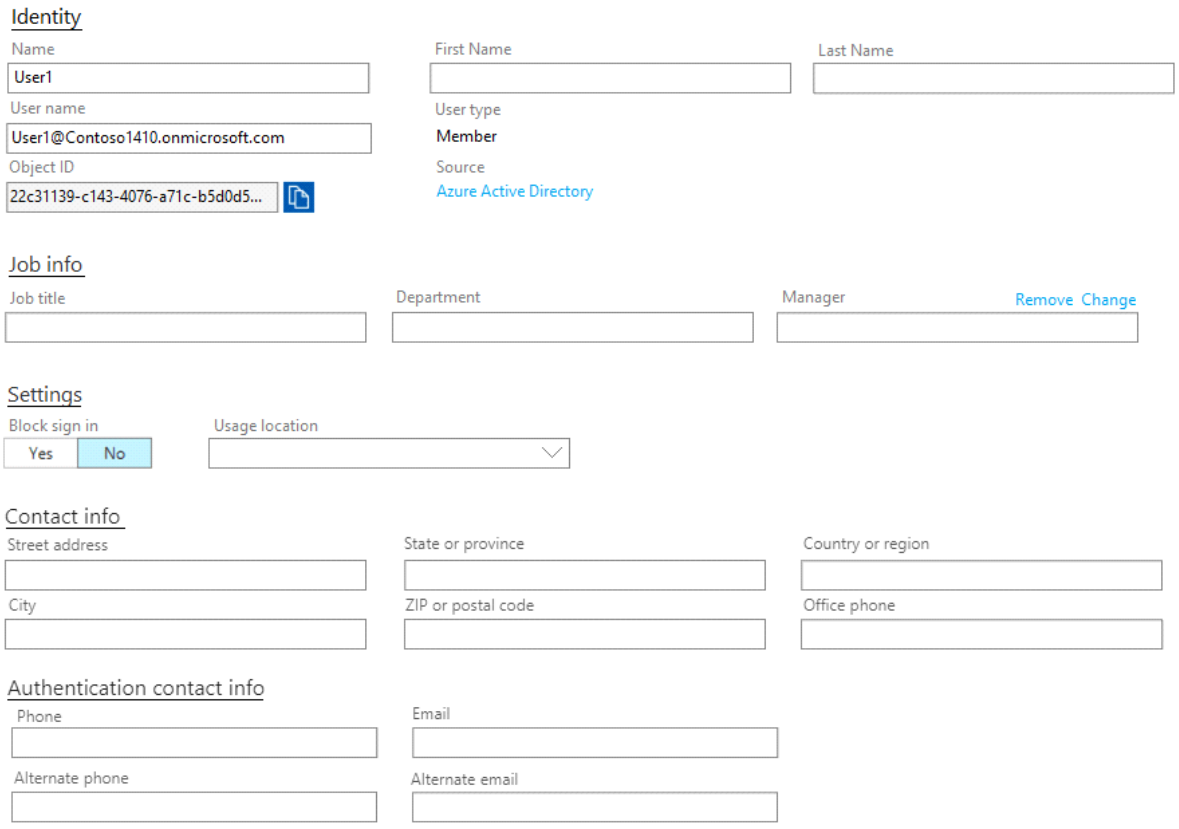
Microsoft 365 Identity and Services Exam

Questions & Answers
Demo

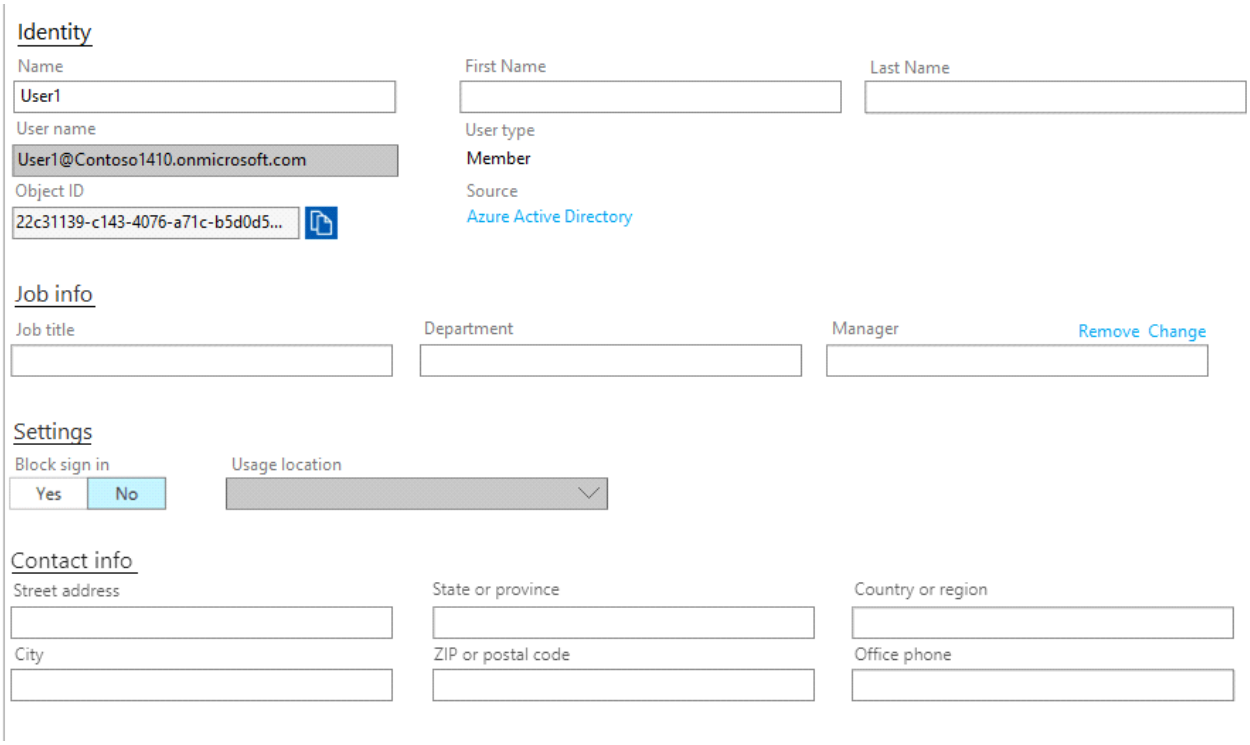
Version: 19.0

Question: 1

HOTSPOT
You need to meet the technical requirements for the user licenses.
Which two properties should you configure for each user? To answer, select the appropriate properties in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
All new users must be assigned Office 365 licenses automatically.
To enable Microsoft 365 license assignment, the users must have a username. This is also the UPN.
The users must also have a Usage Location.

Question: 2

You need to meet the security requirement for Group1.
What should you do?

A. Configure all users to sign in by using multi-factor authentication.
B. Modify the properties of Group1.
C. Assign Group1 a management role.
D. Modify the Password reset properties of the Azure AD tenant.

Answer: D

Explanation:
References:
• The members of Group1 must be required to answer a security question before changing their password.
If SSPR (Self Service Password Reset) is enabled, you must select at least one of the following options for the authentication methods. Sometimes you hear these options referred to as "gates."
Mobile app notification
Mobile app code
Email
Mobile phone

Office phone
Security questions
You can specify the required authentication methods in the Password reset properties of the Azure AD tenant. In this case, you should set the required authentication method to be 'Security questions'.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

Question: 3

To which Azure AD role should you add User4 to meet the security requirement?

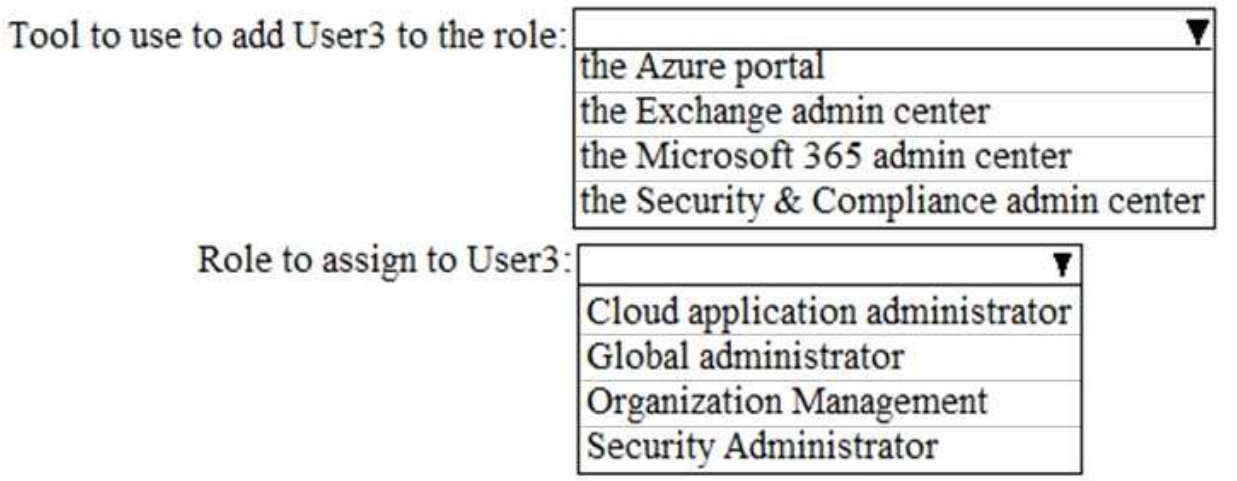
A. Password administrator
B. Global administrator
C. Security administrator
D. Privileged role administrator

Answer: B

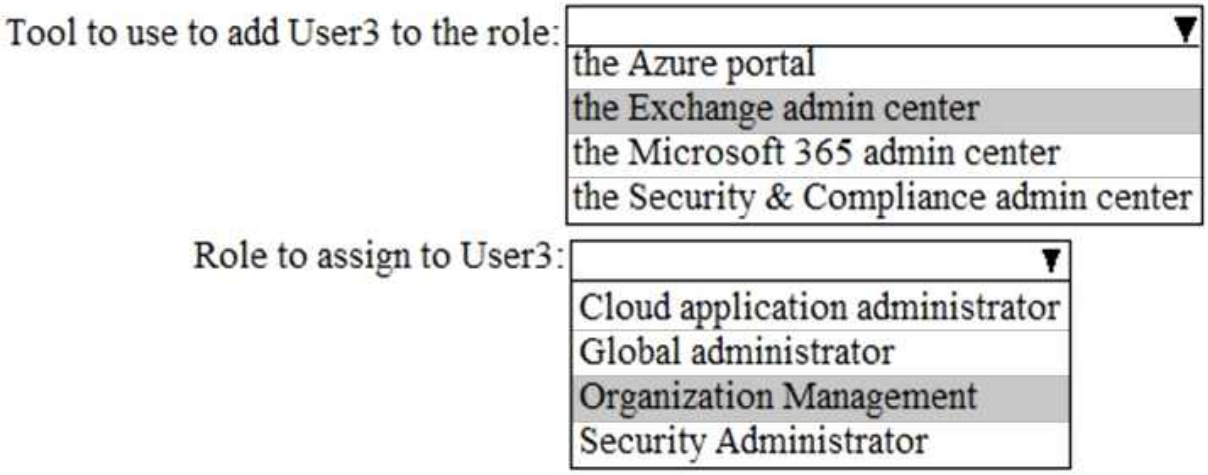
Explanation:
• User4 must be able to reset User3 password.
User3 is assigned the Customer Lockbox Access Approver role. Only global admins can reset the passwords of people assigned to this role as it's considered a privileged role.
Reference:
https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Customer-Lockbox-Approver-Role-Now-Available/ba-p/223393

Question: 4

HOTSPOT
You need to meet the security requirements for User3. The solution must meet the technical requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
• User3 must be able to manage Office 365 connectors.
• The principle of least privilege must be used whenever possible.
Office 365 connectors are configured in the Exchange Admin Center.
You need to assign User3 the Organization Management role to enable User3 to manage Office 365 connectors.
A Global Admin could manage Office 365 connectors but the Organization Management role has less privilege.
Reference:
https://docs.microsoft.com/en-us/office365/SecurityCompliance/eop/feature-permissions-in-eop

Question: 5

You need to meet the security requirement for the vendors.
What should you do?

A. From the Azure portal, add an identity provider.
B. From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the –UserPrincipalName parameter.
C. From the Azure portal, create guest accounts.
D. From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the –UserType parameter.

Answer: C

Explanation:
• 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.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator

Question: 6

You need to assign User2 the required roles to meet the security requirements and the technical requirements.
To which two roles should you assign User2? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Exchange View-only Organization Management role
B. the Microsoft 365 Records Management role
C. the Exchange Online Help Desk role
D. the Microsoft 365 Security Reader role
E. the Exchange Online Compliance Management role

Answer: DE

Explanation:
• User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The Security Reader role can view reports but not schedule the email delivery of security and compliance reports.
The Exchange Online Compliance Management role can schedule the email delivery of security and compliance reports.
Reference:
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

Question: 7

You need to meet the security requirement for the vendors.
What should you do?

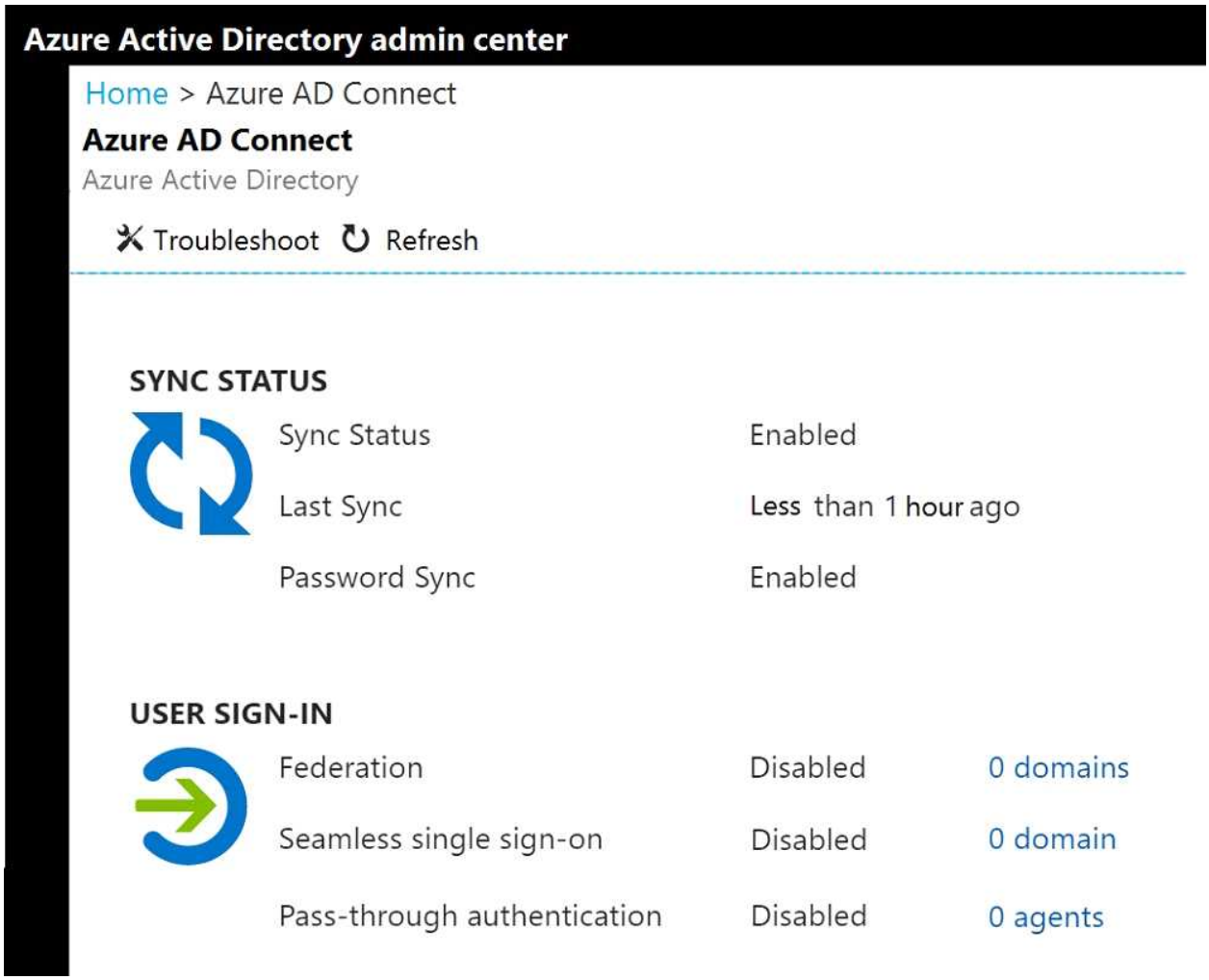
A. From the Azure portal, modify the authentication methods.
B. From Azure Cloud Shell, run the New-AzureADMSInvitation and specify the –InvitedIserEmailAddress cmdlet.
C. From Azure Cloud Shell, run the Set-MsolUserPrincipalName and specify the –tenantID parameter.
D. From the Azure portal, add an identity provider.

Answer: B

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

Question: 8

HOTSPOT
You create the Microsoft 365 tenant.
You implement Azure AD Connect as 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.

Answer Area

Sales department users can access [**answer choice**] applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable, users can access the resource [**answer choice**].

- both on-premises and in the cloud
- in the cloud only
- on-premises only

Answer:

Answer Area

Sales department users can access [**answer choice**] applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable, users can access the resource [**answer choice**].

- both on-premises and in the cloud
- in the cloud only
- on-premises only

Explanation:
In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.
In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Azure Active Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active Directory. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.

Question: 9

DRAG DROP
You need to prepare the environment for Project1.
You create the Microsoft 365 tenant.
Which three actions should you perform in sequence next? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Configure the required DNS records and verify fabrikam.com as a custom domain.
- Implement directory synchronization.
- Create a Microsoft Azure Active Directory (Azure AD) tenant.
- Modify the Exchange ActiveSync Access Settings.
- Run the Hybrid Configuration wizard.

Answer Area

Answer:

Answer Area

Create a Microsoft Azure Active Directory (Azure AD) tenant.
Configure the required DNS records and verify fabrikam.com as a custom domain.
Implement directory synchronization.

Explanation:
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
All users must be able to exchange email messages successfully during Project1 by using their current email address.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
This configuration requires a hybrid Exchange configuration during the pilot phase. This means that you will have mailboxes hosted in Exchange Online and mailboxes hosted in Exchange on-premise.
The first steps to configure Exchange hybrid are to Create the Azure AD tenant, add the Fabrikam.com domain as a custom domain, then configure directory synchronization to replicate the on-prem Active Directory user accounts to Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/exchange/exchange-hybrid

Question: 10

You need to meet the application requirement for App1.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From the Azure Active Directory admin center, configure the application URL settings.
B. From the Azure Active Directory admin center, add an enterprise application.
C. On an on-premises server, download and install the Microsoft AAD Application Proxy connector.
D. On an on-premises server, install the Hybrid Configuration wizard.
E. From the Microsoft 365 admin center, configure the Software download settings.

Answer: ABC

Explanation:
An on-premises web application named App1 must allow users to complete their expense reports online.
Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. Azure AD, the

Application Proxy service, and the Application Proxy connector work together to securely pass the user sign-on token from Azure AD to the web application.
In this question, we need to add an enterprise application in Azure and configure a Microsoft AAD Application Proxy connector to connect to the on-premises web application (App1).
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy#how-application-proxy-works