Vendor: Microsoft

Exam Code:MS-100

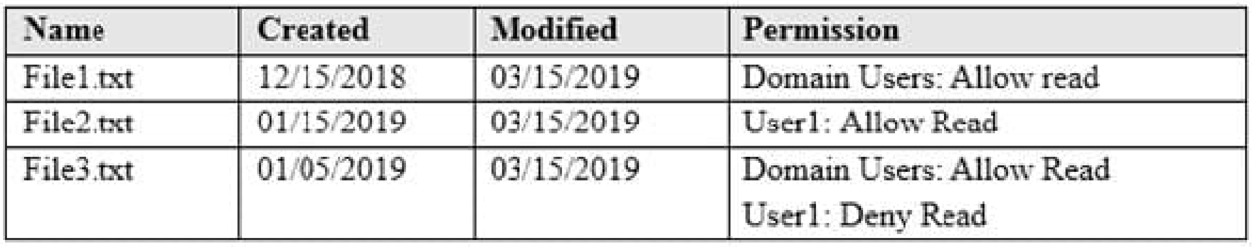
Exam Name: Microsoft 365 Identity and Services

Version: Demo

QUESTION 1

HOTSPOT

Your network contains an on-premises Active Directory domain. The domain contains a server named Server1. Server1 has a share named Share1 that contains the files shown in the following table.



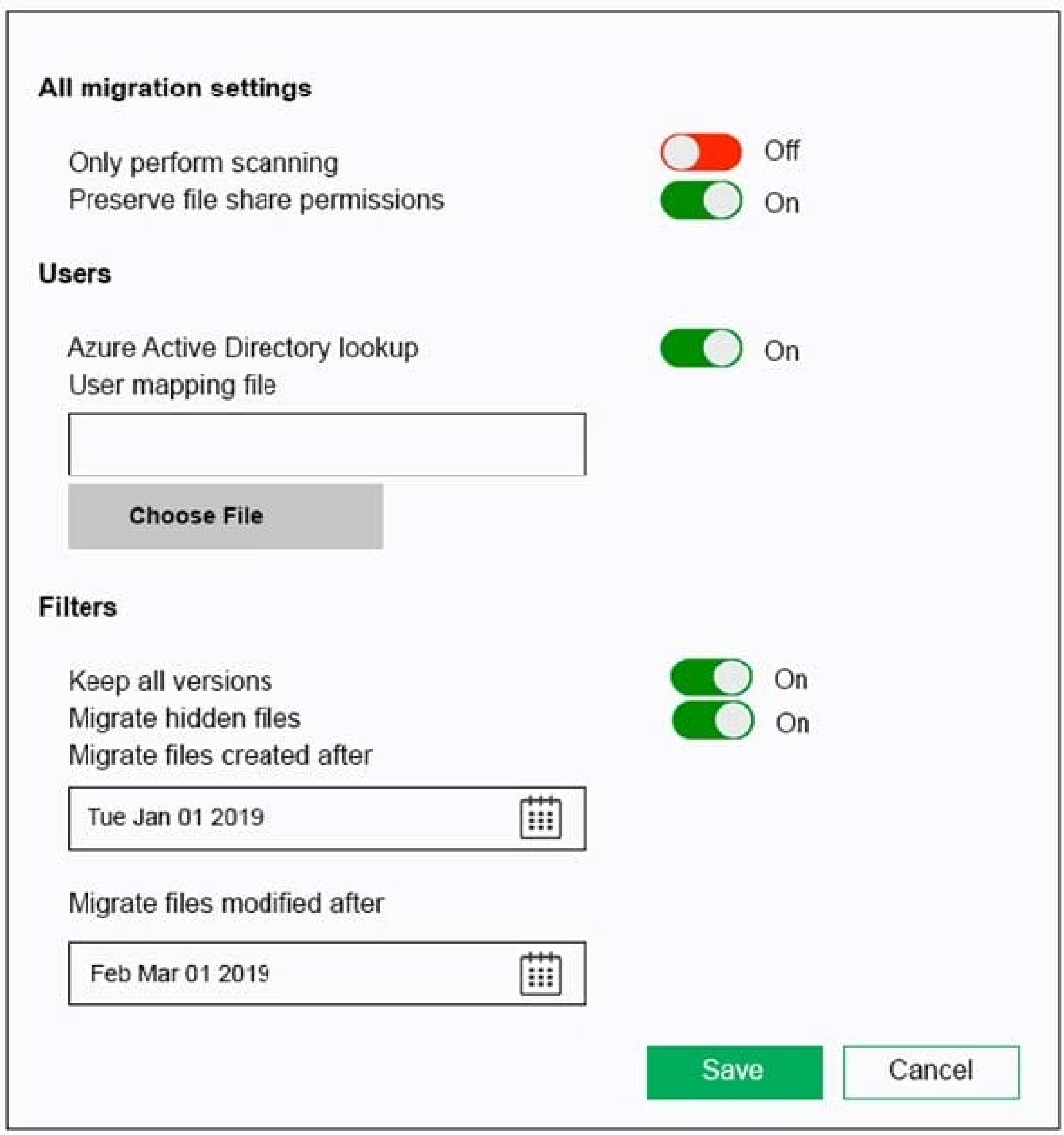
Name	Created	Modified	Permission
File1.txt	12/15/2018	03/15/2019	Domain Users: Allow read
File2.txt	01/15/2019	03/15/2019	User1: Allow Read
File3.txt	01/05/2019	03/15/2019	Domain Users: Allow Read User1: Deny Read

You have a hybrid deployment of Microsoft 365.

You create a Microsoft SharePoint site collection named Collection1.

You plan to migrate Share1 to a document library in Collection1.

You configure the SharePoint Migration Tool as shown in the exhibit.



All migration settings

Only perform scanning Off

Preserve file share permissions On

Users

Azure Active Directory lookup On

User mapping file

Filters

Keep all versions On

Migrate hidden files On

Migrate files created after

Tue Jan 01 2019

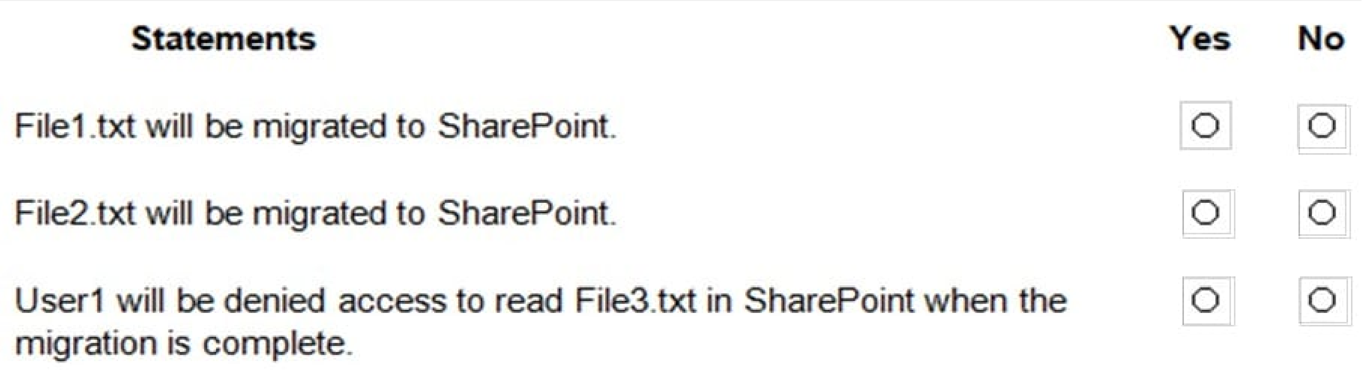
Migrate files modified after

Feb Mar 01 2019

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

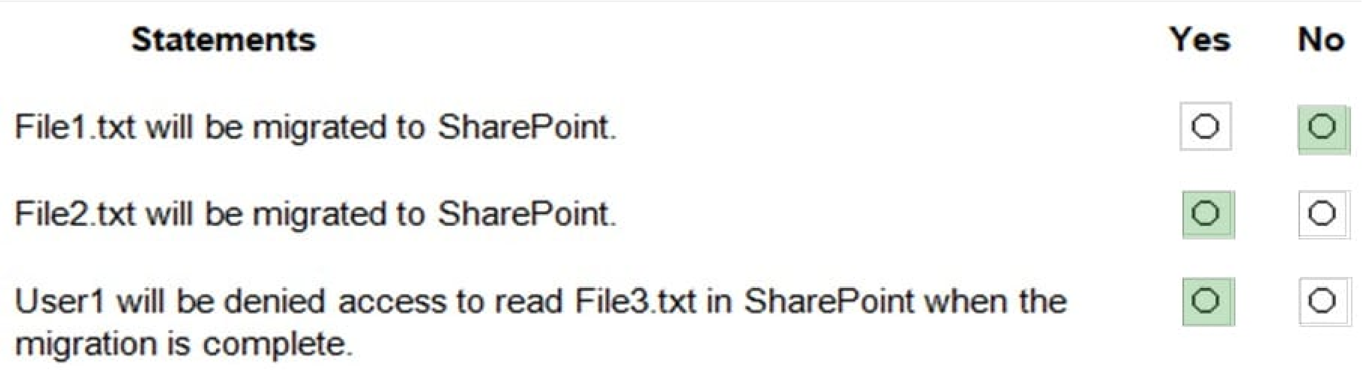
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
File1.txt will be migrated to SharePoint.	○	○
File2.txt will be migrated to SharePoint.	○	○
User1 will be denied access to read File3.txt in SharePoint when the migration is complete.	○	○

Correct Answer:



Statements	Yes	No
File1.txt will be migrated to SharePoint.	○	●
File2.txt will be migrated to SharePoint.	●	○
User1 will be denied access to read File3.txt in SharePoint when the migration is complete.	●	○

Box 1: No

File1.txt will not be migrated as it was created before Jan 1 2019

Box 2: Yes

File2.txt will be migrated as it was created after Jan 1 2019 and was modified after Mar 1 2019.

Box 3: Yes

File3.txt will be migrated as it was created after Jan 1 2019 and was modified after Mar 1 2019.

Reference:

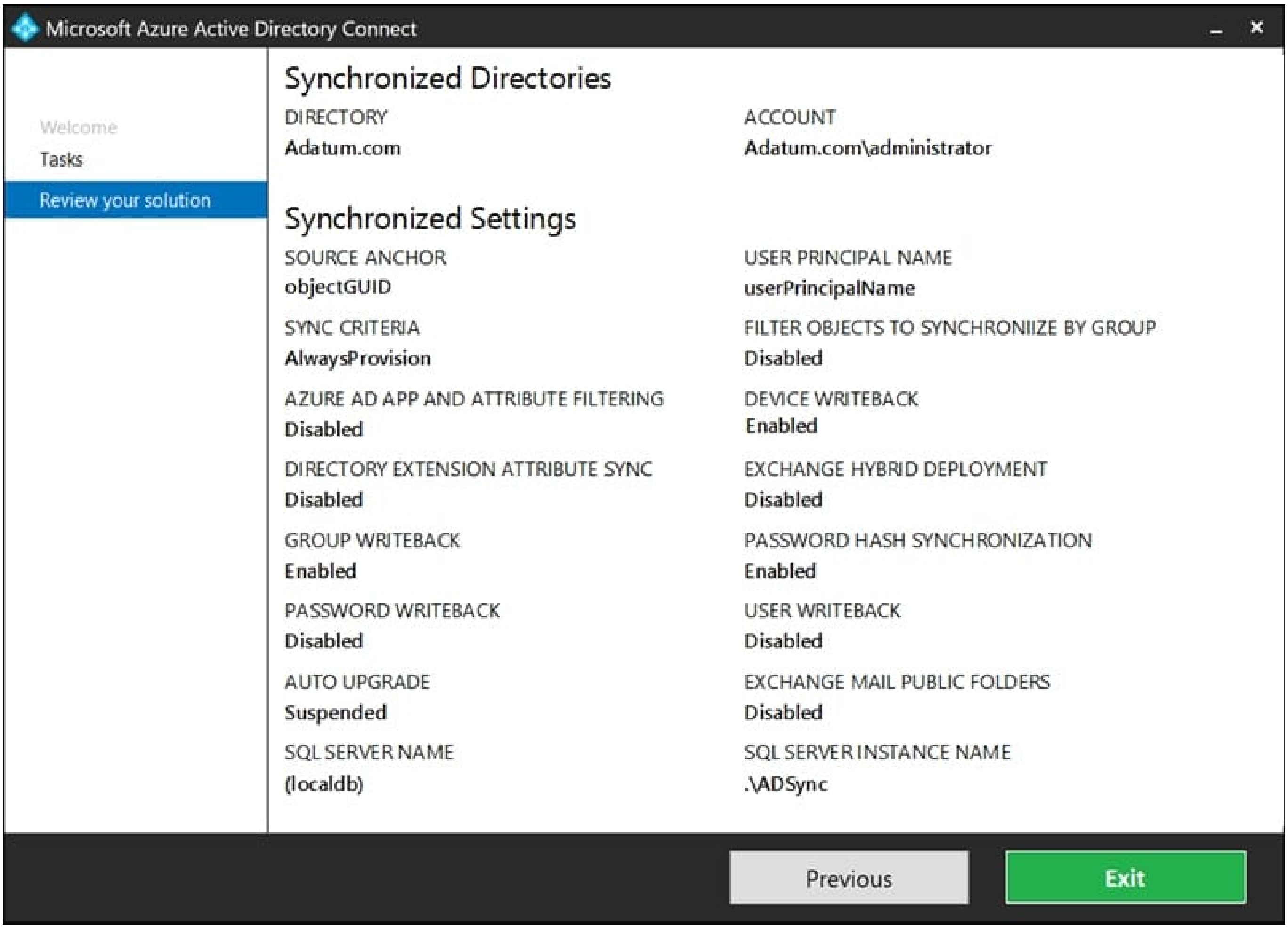
https://docs.microsoft.com/en-us/sharepointmigration/spmt-settings

---

QUESTION 2

HOTSPOT

You have an Active Directory domain named Adatum.com that is synchronized to Azure Active Directory as shown in the exhibit.



Synchronized Directories

DIRECTORY	ACCOUNT
Adatum.com	Adatum.com\administrator

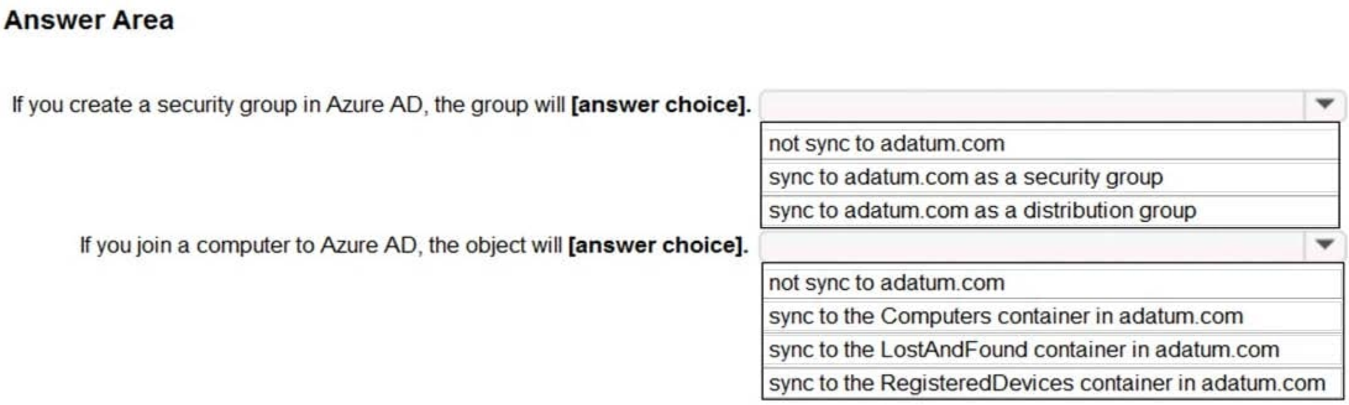
Synchronized Settings

SOURCE ANCHOR objectGUID	USER PRINCIPAL NAME userPrincipalName
SYNC CRITERIA AlwaysProvision	FILTER OBJECTS TO SYNCHRONIIZE BY GROUP Disabled
AZURE AD APP AND ATTRIBUTE FILTERING Disabled	DEVICE WRITEBACK Enabled
DIRECTORY EXTENSION ATTRIBUTE SYNC Disabled	EXCHANGE HYBRID DEPLOYMENT Disabled
GROUP WRITEBACK Enabled	PASSWORD HASH SYNCHRONIZATION Enabled
PASSWORD WRITEBACK Disabled	USER WRITEBACK Disabled
AUTO UPGRADE Suspended	EXCHANGE MAIL PUBLIC FOLDERS Disabled
SQL SERVER NAME (localdb)	SQL SERVER INSTANCE NAME .\ADSync

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:



Answer Area

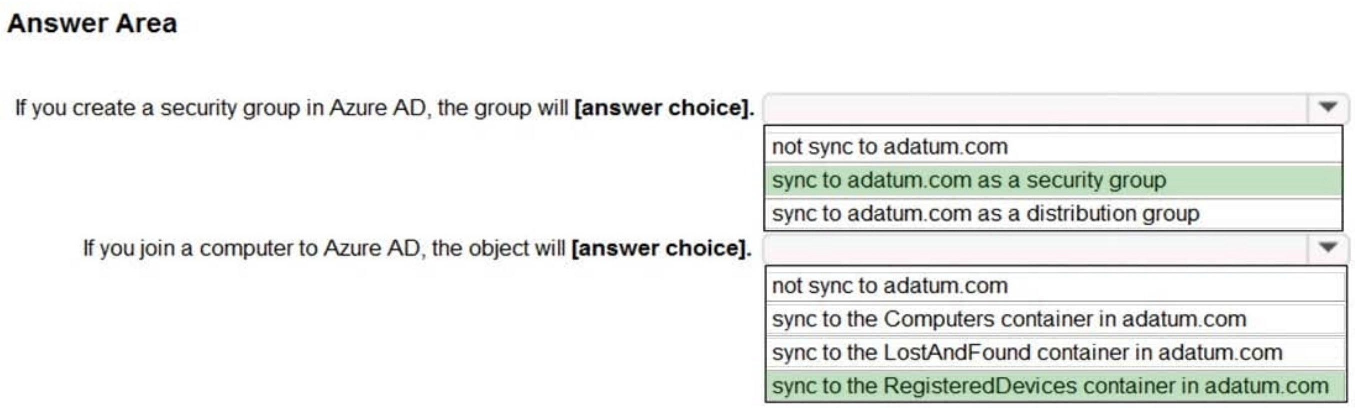
If you create a security group in Azure AD, the group will **[answer choice].**

- not sync to adatum.com
- sync to adatum.com as a security group
- sync to adatum.com as a distribution group

If you join a computer to Azure AD, the object will **[answer choice].**

- not sync to adatum.com
- sync to the Computers container in adatum.com
- sync to the LostAndFound container in adatum.com
- sync to the RegisteredDevices container in adatum.com

Correct Answer:



Answer Area

If you create a security group in Azure AD, the group will **[answer choice].**

- not sync to adatum.com
- [✓ sync to adatum.com as a security group]
- sync to adatum.com as a distribution group

If you join a computer to Azure AD, the object will **[answer choice].**

- not sync to adatum.com
- sync to the Computers container in adatum.com
- sync to the LostAndFound container in adatum.com
- [✓ sync to the RegisteredDevices container in adatum.com]

Group Writeback is enabled in the Azure AD Connect configuration so groups created in Azure Active Directory will be synchronized to the on-premise Active Directory. A security group created in Azure Active Directory will be synchronized to the on-premise Active Directory as a security group. Device Writeback is enabled in the Azure AD Connect configuration so computers joined to the Azure Active Directory will be synchronized to the on-premise Active Directory. They will sync to the RegisteredDevices container in the onpremise Active Directory.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

---

QUESTION 3

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 Azure Active Directory admin center, configure the Software download settings.

Correct Answer: ABC

An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.

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).

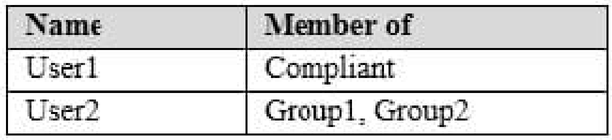
References:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy#how-application-proxy-works

QUESTION 4

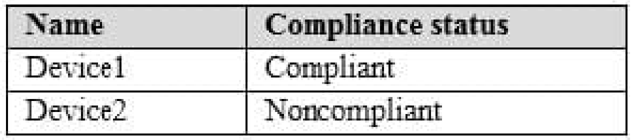
HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.



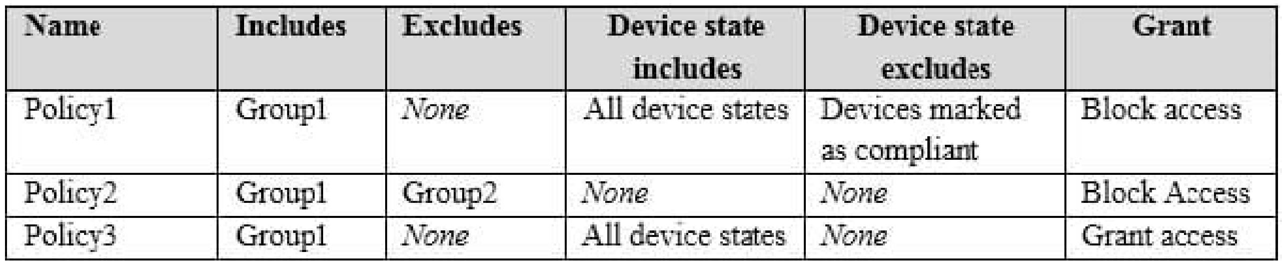
Name	Member of
User1	Compliant
User2	Group1, Group2

The domain contains the devices shown in the following table.



Name	Compliance status
Device1	Compliant
Device2	Noncompliant

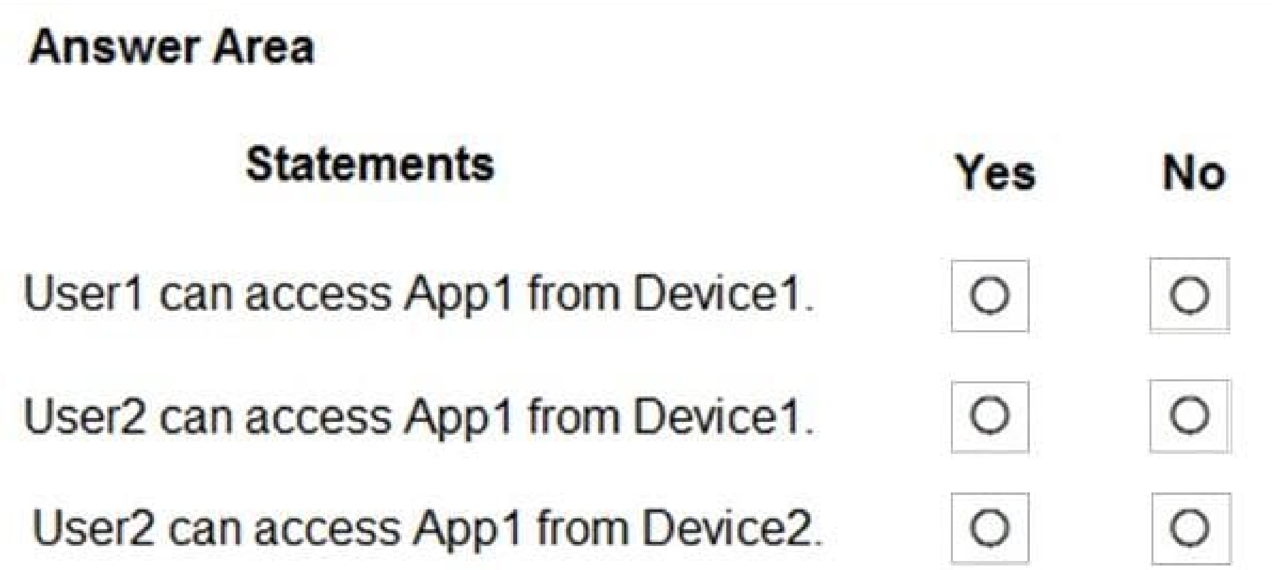
The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.



Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	*None*	All device states	Devices marked as compliant	Block access
Policy2	Group1	Group2	*None*	*None*	Block Access
Policy3	Group1	*None*	All device states	*None*	Grant access

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

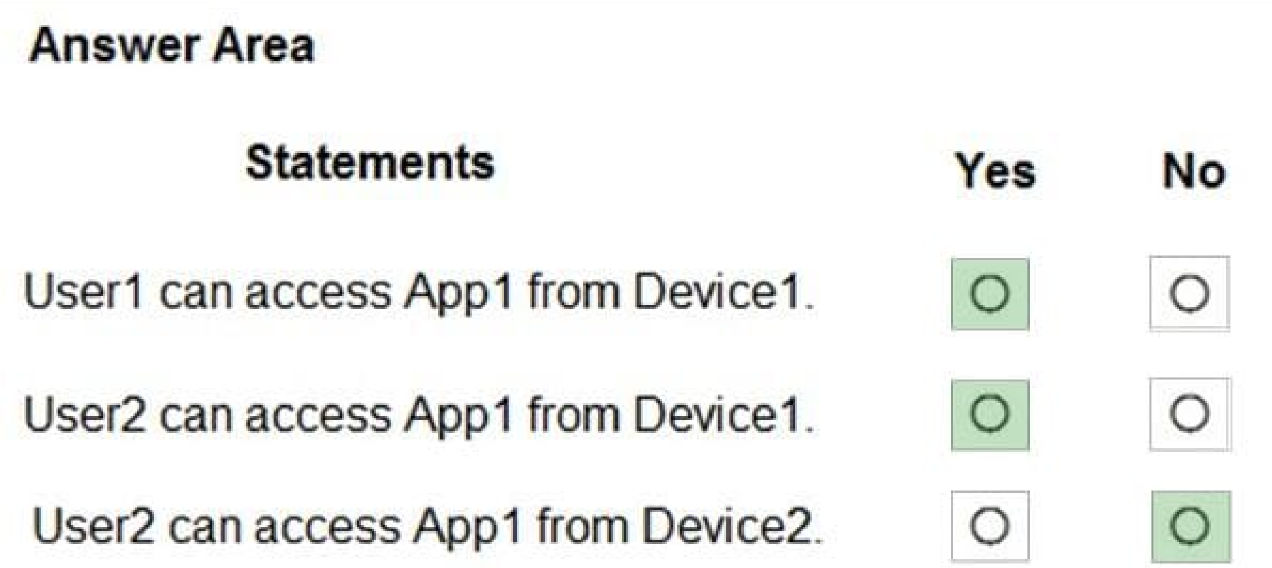
Hot Area:



Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	○	○
User2 can access App1 from Device1.	○	○
User2 can access App1 from Device2.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	[✓ ○]	○
User2 can access App1 from Device1.	[✓ ○]	○
User2 can access App1 from Device2.	○	[✓ ○]

Box 1: Yes.

User1 is in a group named Compliant. All the conditional access policies apply to Group1 so they don\\'t apply to User1.

As there is no conditional access policy blocking access for the group named Compliant, User1 is able to access App1 using any device.

Box 2: Yes.

User2 is in Group1 so Policy1 applies first. Policy1 excludes compliant devices and Device1 is compliant. Therefore, Policy1 does not apply so we move on to Policy2.

User2 is also in Group2. Policy2 excludes Group2. Therefore, Policy2 does not apply so we move on to Policy3.

Policy3 applies to Group1 so Policy3 applies to User2. Policy3 applies to ‘All device states’ so Policy3 applies to Device1. Policy3 grants access. Therefore, User2 can access App1 using Device1.

Box 3: No.

User2 is in Group1 so Policy1 applies. Policy1 excludes compliant devices but Devices is non-compliant. Therefore, User2 cannot access App1 from Device2.

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

---

QUESTION 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has 3,000 users. All the users are assigned Microsoft 365 E3 licenses.

Some users are assigned licenses for all Microsoft 365 services. Other users are assigned licenses for only certain Microsoft 365 services.

You need to determine whether a user named User1 is licensed for Exchange Online only.

Solution: You run the Get-MsolUser cmdlet.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

The Get-MsolUser cmdlet will tell you if a user is licensed for Microsoft 365 but it does not tell you which licenses are assigned.

Reference: https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0

QUESTION 6

SIMULATION

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn\\'t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are

able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

You may now click next to proceed to the lab.

Lab information

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@M365x981607.onmicrosoft.com

Microsoft 365 Password: *yfLo7Ir2andy-

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 10811525

You plan to invite several guest users to access the resources in your organization.

You need to ensure that only guests who have an email address that uses the @contoso.com suffix can connect to the resources in your Microsoft 365 tenant.

A. See explanation below.

Correct Answer: A

You need to add contoso.com as an allowed domain in the ‘External collaboration settings’.

1.

Go to the Azure Active Directory admin center.

2.

Select Users then select ‘User settings’.

3.

Under External Users, select the ‘Manage external collaboration settings’.

4.

Under ‘Collaboration restrictions’, select the ‘Allow invitations only to the specified domains (most restrictive)’ option.

5.

Under, Target Domains, type in the domain name ‘contoso.com’

6.

Click the Save button at the top of the screen to save your changes.

References: https://docs.microsoft.com/en-us/azure/active-directory/b2b/allow-deny-list

---

QUESTION 7

You have been tasked with enable Microsoft Azure Information Protection for your company Microsoft 365 subscription.

You are informed that only the members of a group, named Group1, are able to protect content. To achieve your goal, you plan to run a PowerShell cmdlet.

Which of the following is the cmdlet you should run?

A. The Add-AadrmRoleBaseAdministrator cmdlet.

B. The Set-AadrmDoNotTrackUserGroup cmdlet.

C. The Clear-AadrmSuperUserGroup cmdlet.

D. The Set-AadrmOnboardingControlPolicy cmdlet.

Correct Answer: D

If you don want all users to be able to protect documents and emails immediately by using Azure Rights Management, you can configure user onboarding controls by using the Set-AadrmOnboardingControlPolicy

References: https://docs.microsoft.com/en-us/azure/information-protection/activate-service

---

QUESTION 8

You have a Microsoft 365 E5 subscription. You plan to use supervised chat in Microsoft Teams. You need to configure chat permission roles. Which policy type should you use?

A. teams

B. messaging

C. setup

D. permission

Correct Answer: A

QUESTION 9

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP-related data to be stored in the United

States.

You plan to onboard all the devices to Windows Defender ATP data in Europe.

What should you do first?

A. Create a workspace

B. Offboard the test devices

C. Delete the workspace

D. Onboard a new device

Correct Answer: B

When onboarding Windows Defender ATP for the first time, you can choose to store your data in Microsoft Azure datacenters in the European Union, the United Kingdom, or the United States. Once configured, you cannot change the location

where your data is stored.

The only way to change the location is to offboard the test devices then onboard them again with the new location.

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/data-storage-privacy#do-i-have-the-flexibility-to-select-where-to-store-my-data

---

QUESTION 10

You need to ensure that Litware has the appropriate license to support the planned changes. The solution must minimize costs. Which license type should you use?

A. Microsoft 365 Enterprise E5

B. Office 365 Enterprise F3

C. Microsoft 365 Enterprise E3

D. Office 365 Enterprise E5

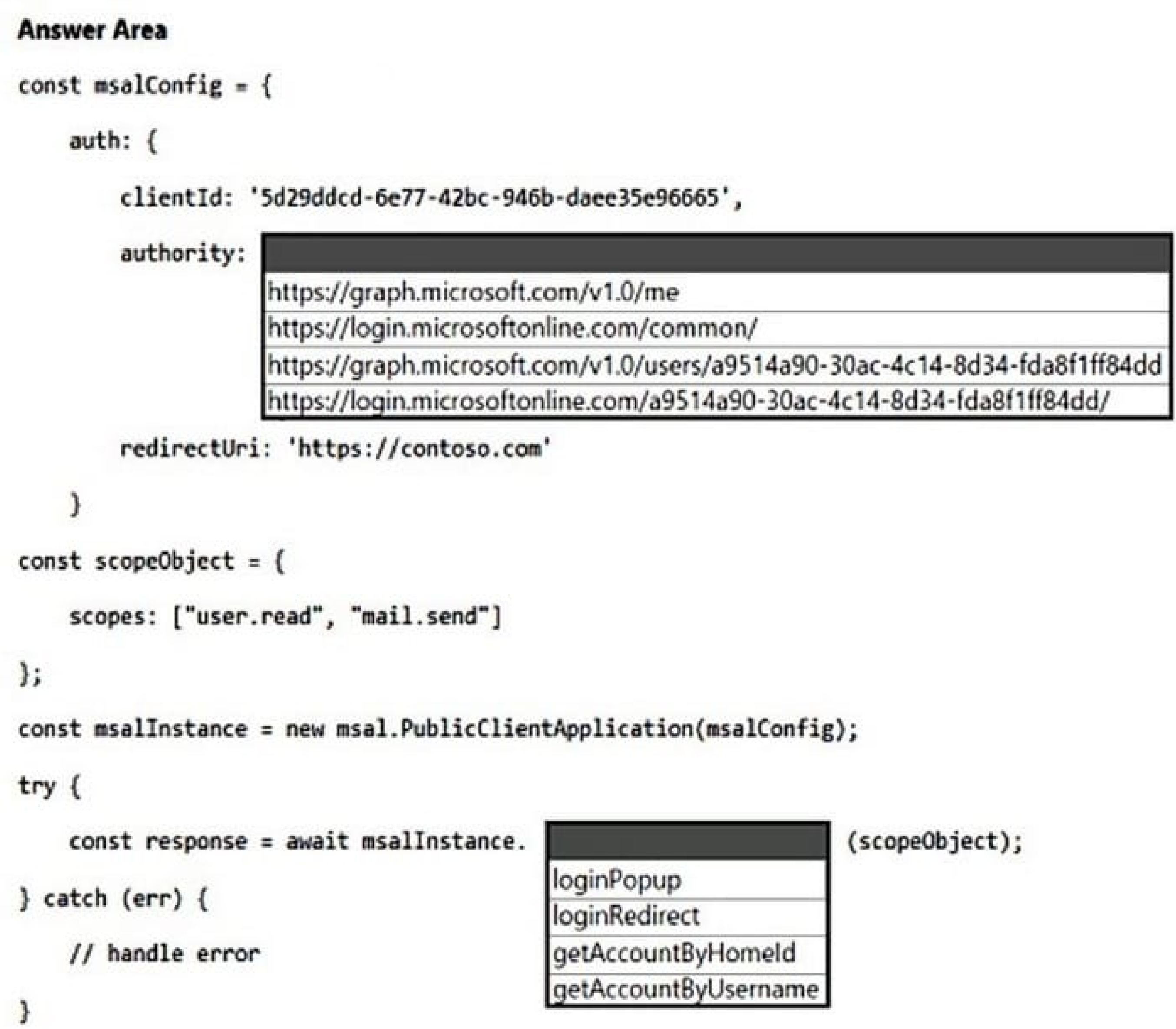
Correct Answer: A

QUESTION 11

HOTSPOT You have a multitenant app named App1. You need to ensure that App1 supports token acquisition when a user accesses the app by using a web browser that has a popup blocker extension enabled. How should you complete the Microsoft Authentication Library (MSAL) for

JavaScript v2.0 code? To answer, select the appropriate options m the answer area. NOTE: Each correct selection is worth one point.

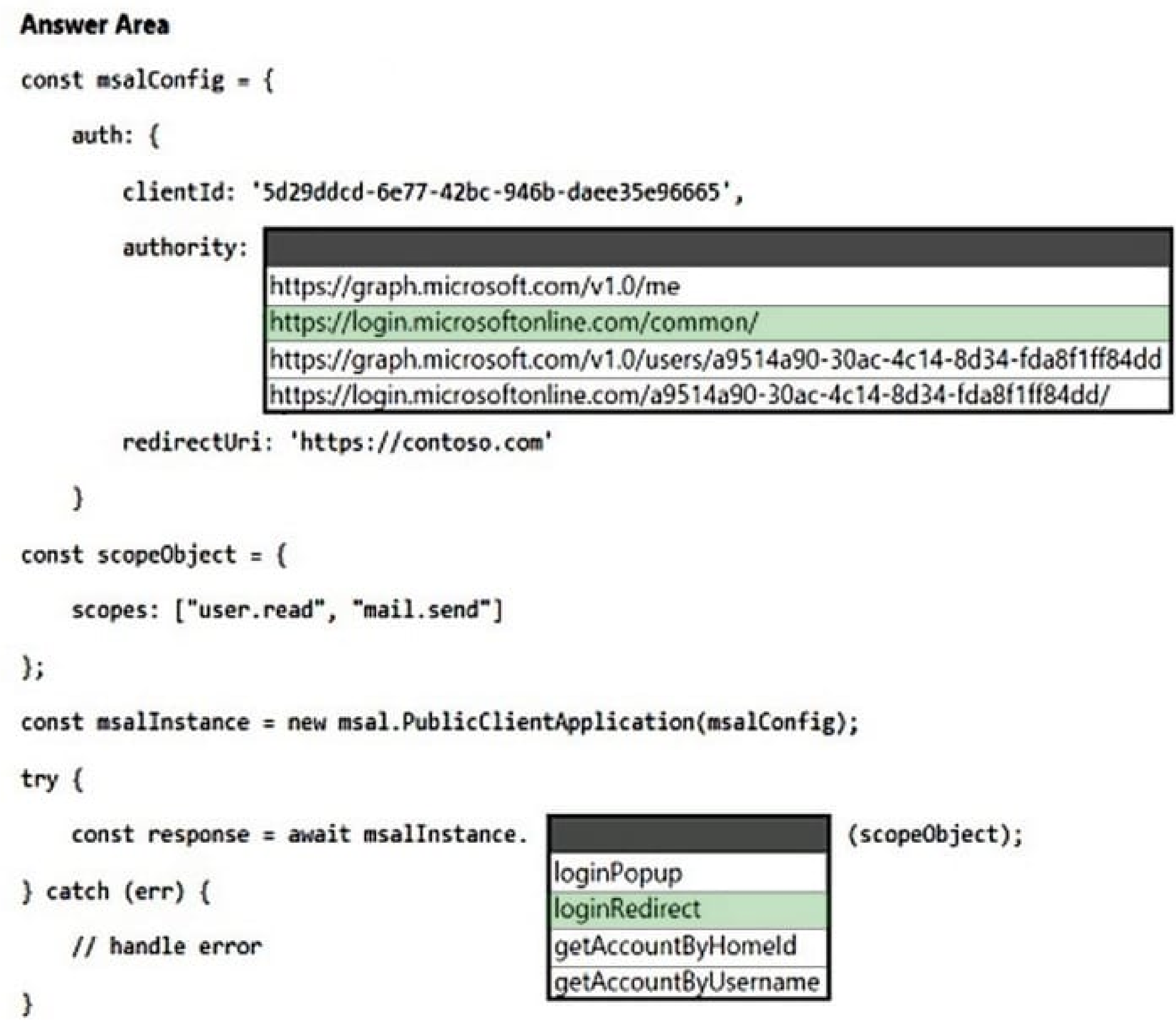
Hot Area:



Answer Area

```
const msalConfig = {
    auth: {
        clientId: '5d29ddcd-6e77-42bc-946b-daee35e96665',
        authority: https://graph.microsoft.com/v1.0/me
                   https://login.microsoftonline.com/common/
                   https://graph.microsoft.com/v1.0/users/a9514a90-30ac-4c14-8d34-fda8f1ff84dd
                   https://login.microsoftonline.com/a9514a90-30ac-4c14-8d34-fda8f1ff84dd/
        redirectUri: 'https://contoso.com'
    }
const scopeObject = {
    scopes: ["user.read", "mail.send"]
};
const msalInstance = new msal.PublicClientApplication(msalConfig);
try {
    const response = await msalInstance. loginPopup              (scopeObject);
} catch (err) {                         loginRedirect
    // handle error                     getAccountByHomeId
}                                       getAccountByUsername
```

Correct Answer:



Answer Area
https://graph.microsoft.com/v1.0/me
https://login.microsoftonline.com/common/
https://graph.microsoft.com/v1.0/users/a9514a90-30ac-4c14-8d34-fda8f1ff84dd
https://login.microsoftonline.com/a9514a90-30ac-4c14-8d34-fda8f1ff84dd/
loginPopup
loginRedirect
getAccountByHomeId
getAccountByUsername

```
const msalConfig = {
    auth: {
        clientId: '5d29ddcd-6e77-42bc-946b-daee35e96665',
        authority:
        redirectUri: 'https://contoso.com'
    }
const scopeObject = {
    scopes: ["user.read", "mail.send"]
};
const msalInstance = new msal.PublicClientApplication(msalConfig);
try {
    const response = await msalInstance.              (scopeObject);
} catch (err) {
    // handle error
}
```

Box 1: https://login.microsoftonline.com/common/

The authority is a URL that indicates a directory that MSAL can request tokens from.

* https://login.microsoftonline.com/common/

Sign in users with work and school accounts or personal Microsoft accounts.

QUESTION 12

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has a Microsoft Office 365 tenant.

You suspect that several Office 365 features were recently updated.

You need to view a list of the features that were recently updated in the tenant.

Solution: You review the Security and Compliance report in the Microsoft 365 admin center.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

The Security and Compliance reports in the Microsoft 365 admin center are reports regarding security and compliance for your Office 365 Services. For example, email usage reports, Data Loss Prevention reports etc. They do not display a list of the features that were recently updated in the tenant so this solution does not meet the goal.

To meet the goal, you need to use Message center in the Microsoft 365 admin center.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/download-existing-reports