- **Vendor:** Microsoft
- **Exam Code:** MS-500
- **Exam Name:** Microsoft 365 Security Administration
- **New Updated Questions from Braindump2go (Updated in May/2023)**

QUESTION 298
You've deployed AIP and need to choose the appropriate AIP client.
You have the following requirements, which AIP client will you choose?

```
- Your organization requires a HYOK deployment
- Your organization requires that you install the client on Windows and MacOS Label with
file explorer.
```

A. Classic
B. Unified
C. Office

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/information-protection/rms-client/use-client

QUESTION 299
You are implementing MCAS.
Which of the following data sources can be used for discovery of Shadow IT? (Choose three.)

A. Log collector
B. Data Gateway
C. Secure Web Gateway
D. Defender ATP
E. Azure Sentinel

Answer: ACD
Explanation:
MCAS integrates with Zscaler and iboss via secure web gateway
Data gateway is used by Azure data solutions like Power BI to get data from on-premises data sources
Azure Sentinel is Microsoft's SIEM/SOAR solution and not a data source for MCAS. MCAS is a data source for Sentinel, though.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery

QUESTION 300
What license level is needed for AAD Connect with password hash sync (PHS) and password write-back?

A. AAD P1
B. AAD P2
C. O365 Apps
D. AAD free

Answer: A
Explanation:
Reference:
https://azure.microsoft.com/en-us/pricing/details/active-directory/

QUESTION 301
You have implemented Azure AD Connect for your organization.
You have made some changes to user accounts in your local Active Directory and notice that these changes have not yet synchronized to Azure.
What is the PS command to force an Azure AD Connect sync?

A. Start-ADSyncSyncCycle -PolicyType Delta
B. Start-ADSyncSyncCycle -PolicyType Initial
C. Get-ADSyncScheduler
D. Set-MsolDirSyncFeature -Feature SynchronizeUpnForManagedUsers -Enable $true

Answer: A
Explanation:
Reference:
https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-how-to-force-azuread-connect-to-sync/ba-p/887043 https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-syncservice-features

QUESTION 302
Which of the following components are required for Azure AD Hybrid Identity with Passthrough Authentication? (Choose three.)

A. Azure AD Connect
B. Federation Proxy
C. Federation Server
D. Authentication Agent
E. Active Directory

Answer: ADE
Explanation:
You need the authentication agent which is a separate component from AD Connect. Although, AD Connect will install that component locally on the AD Connect server when you configure PTA.
Reference:
https://docs.microsoft.com/en-za/azure/security/fundamentals/choose-ad-authn

QUESTION 303
You want to detect and respond to possible attacks on the Kerberos protocol.
Which M365 security solution would you implement?

A. Network Security Group
B. Intrusion Detection System (IDS)
C. Microsoft Defender ATP
D. O365 ATP
E. Azure ATP
F. Microsoft Threat Prevention (MTP)

Answer: E
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/suspicious-activity-guide

QUESTION 304

You are implementing compliance management for your organization.
How do you enable O365 in-place archiving?

A. Admin.microsoft.com; Exchange; Compliance management; archive
B. Protection.office.com; information governance; archive
C. servicetrust.microsoft.com; Compliance manager, archiving
D. servicetrust.microsoft.com; Trust center; archiving

Answer: B
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-archive-mailboxes

QUESTION 305
You are adjusting data retention policies in O365. A colleague has set up a data retention policy that retains certain sensitive information types for 7 years. As part of your corporate data governance policies you are required to allow users to manually tag items for retention for up to 3 years. You open the SCC and create a data retention label with data retention of 3 years. A user creates an email that contains a GDPR-related sensitive information type. The user tags the item with the 3-year retention label.
How long will Exchange retain the email item for?

A. The item will be retained for 7 years
B. The item will be retained for 3 years
C. The item will be retained for 10 years
D. The item will be retained for 4 years

Answer: B
Explanation:
A retention label (however it was applied) provides explicit retention in comparison with retention policies, because the retention settings are applied to an individual item rather than implicitly assigned from a container. This means that a delete action from a retention label always takes precedence over a delete action from any retention policy.

QUESTION 306
You have a M365-E5 subscription. You have deployed Microsoft Defender ATP.
You want to run a phishing campaign in your organization using the Attack Simulator.
Which of the following options must you do?

A. Switch on Microsoft Cloud App Security in Defender ATP settings
B. Switch on Office 365 Threat Intelligence connection in Defender ATP settings
C. Enable your account for MFA
D. Deploy and configure Microsoft Cloud App Security
E. Create a user account from where attack simulator will send out the phishing emails

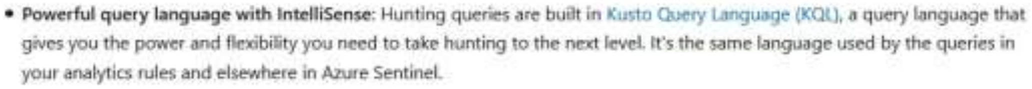
Answer: C
Explanation:
If you want to use the attach sim, you must have your account MFAed. All the other options are optional or not relevant.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide#what-do-you-need-to-know-before-you-begin

QUESTION 307
You have configured an Azure Sentinel solution and wish to proactively look for security threats using Hunting in the Sentinel Portal. Which query language must you use when searching for threats?

A. Transact-SQL
B. Gremlin query language
C. MySQL

D. Kusto query language

Answer: D
Explanation:
Hunting in Azure Sentinel is based on Kusto query language. This is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model designed to make the syntax easy to read, author, and automate. designed to make the syntax easy to read, author, and automate.



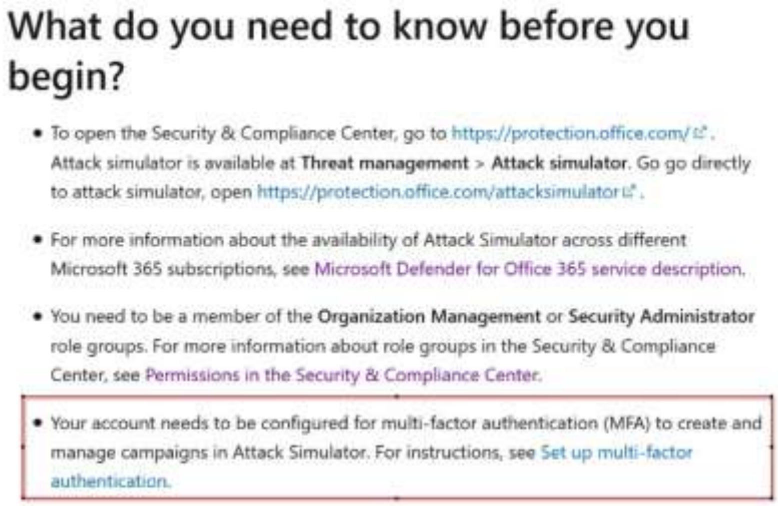
- **Powerful query language with IntelliSense:** Hunting queries are built in Kusto Query Language (KQL), a query language that gives you the power and flexibility you need to take hunting to the next level. It's the same language used by the queries in your analytics rules and elsewhere in Azure Sentinel.

Option A is incorrect. T-SQL (Transact-SQL) is a set of programming extensions from Sybase and Microsoft that add several features to the Structured Query Language. Some of the tools that use T-SQL are SQL Server Management Studio, Azure Data Studio, SQL Server Data Tools and sqlcmd.
Option B is incorrect. Gremlin is a query language used to retrieve data from and modify data in the applications graph. Azure Cosmos DB supports Gremlin.
Option C is incorrect. MySQL is an open source relational database management system with a client-server model. Azure Database for MySQL supports MySQL.
Reference:
https://docs.microsoft.com/nb-no/azure/sentinel/hunting

QUESTION 308
As a step to harden your Office 365 security you wish to run Microsoft Office 365 Attack simulator.
You configure Microsoft Defender Advanced Threat Protection and assign your users Microsoft 365 Enterprise E5 licenses.
What must be configured to run the attack simulator?

A. Create Conditional Access session control scoped at Office 365
B. Assign your users Defender plan 2-licenses
C. Configure an identity protection user risk-policy
D. Enable multi-factor authentication

Answer: D
Explanation:
Enabling MFA is a prerequisite for running Microsoft Attack Simulator.



What do you need to know before you begin?

- To open the Security & Compliance Center, go to https://protection.office.com/. Attack simulator is available at **Threat management** > **Attack simulator**. Go go directly to attack simulator, open https://protection.office.com/attacksimulator.
- For more information about the availability of Attack Simulator across different Microsoft 365 subscriptions, see Microsoft Defender for Office 365 service description.
- You need to be a member of the **Organization Management** or **Security Administrator** role groups. For more information about role groups in the Security & Compliance Center, see Permissions in the Security & Compliance Center.
- Your account needs to be configured for multi-factor authentication (MFA) to create and manage campaigns in Attack Simulator. For instructions, see Set up multi-factor authentication.

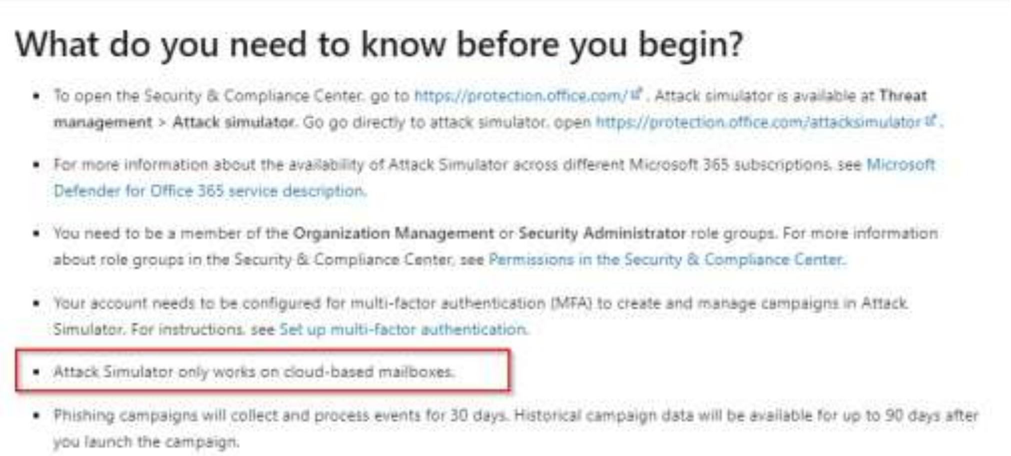
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide

QUESTION 309
You are an IT administrator in a hybrid environment consisting of Windows 10 devices. Most of your users have migrated their mailboxes to Exchange online, but Sales and Marketing still have their mailboxes on premise. All users

are assigned Microsoft 365 Enterprise E5 licenses. You wish to take advantage of the security capabilities in Microsoft Defender Advanced Threat Protection, and plan to run the Microsoft Office 365 Attack simulator on users in the Marketing-department. You have enabled MFA for all users. What must you do?

A. Migrate the Marketing group members to Exchange Online
B. Set AD Connect in staging mode
C. Create a mail-enabled security-group and add the Marketing group members
D. Configure the on-premise public IP in the MFA “trusted IP” settings

Answer: A
Explanation:
Attack Simulator only works on cloud-based mailboxes.



What do you need to know before you begin?

- To open the Security & Compliance Center, go to https://protection.office.com/. Attack simulator is available at **Threat management** > **Attack simulator**. Go go directly to attack simulator, open https://protection.office.com/attacksimulator.
- For more information about the availability of Attack Simulator across different Microsoft 365 subscriptions, see Microsoft Defender for Office 365 service description.
- You need to be a member of the **Organization Management** or **Security Administrator** role groups. For more information about role groups in the Security & Compliance Center, see Permissions in the Security & Compliance Center.
- Your account needs to be configured for multi-factor authentication (MFA) to create and manage campaigns in Attack Simulator. For instructions, see Set up multi-factor authentication.
- Attack Simulator only works on cloud-based mailboxes.
- Phishing campaigns will collect and process events for 30 days. Historical campaign data will be available for up to 90 days after you launch the campaign.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide

QUESTION 310
You are responsible for securing your organizations Exchange online environment. To help prevent impersonation attacks, you wish to enable artificial intelligence (AI) as a policy for all users. What should you configure?

A. Litigation Hold
B. Security defaults
C. Mailbox intelligence
D. Safe attachment policy

Answer: C
Explanation:
Mailbox intelligence uses the mailbox’s normal traffic patterns to better enable the impersonation detection to catch unusual messages. It is able to recognize if an email is coming from an impersonator and flag it. For example, if you usually receive emails from marketing@contoso.com and an email comes in from an impersonator with the address marketinn@contoso.com, the system will recognize that this is not the correct email address and flag the email.
Option A is incorrect. This is a notification sent from an organization’s legal team to employees instructing them not to delete electronically stored information that may be relevant to a legal case.
Option B is incorrect. This is a free security baseline offered by Microsoft.
Option D is incorrect. This is a policy to protect against malicious attachments.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide

QUESTION 311
You have a Microsoft 365 subscription and have assigned Microsoft 365 E5 licenses to your users. Some of your users have issues with their exchange online mailboxes, so you submit a support ticket to Microsoft. You want to ensure that Microsoft cannot access your content to perform service operations without your approval. The solution should allow Microsoft Engineers to make a data access request for a limited amount of time. From the Microsoft 365 admin center,

what should you enable?

A. Customer Lockbox
B. Whiteboard
C. Privacy profile
D. Bing data collection

Answer: A

Explanation:

Office 365 Customer Lockbox is a feature which enables customers to control how a Microsoft support engineer is going to access customer data when investigating and troubleshooting some service issues related to customers Office 365 tenant. This is typically after the customer has raised a ticket with Office 365 Support.

Option B is incorrect. This service allows users in your organization to use Microsoft Whiteboard and collaborate on shared whiteboards.

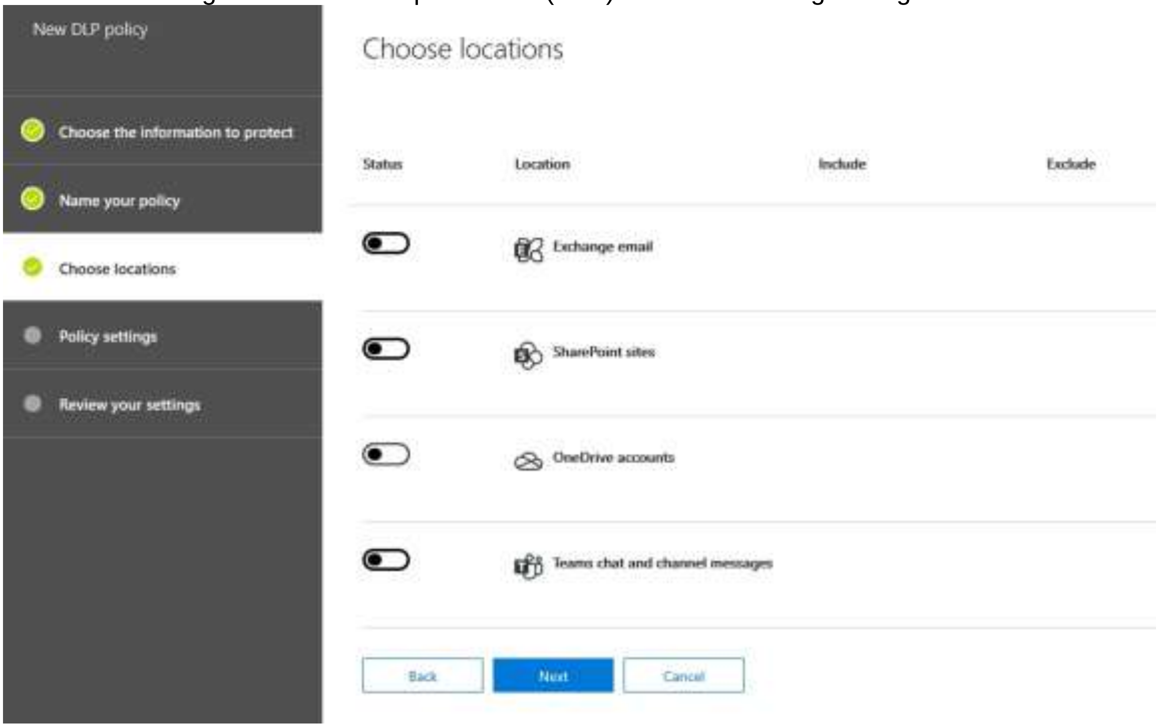
Option C is incorrect. This service lets you set the privacy statement of your organization.

Option D is incorrect. This service lets you choose whether Bing can learn from your organization's search behavior to better its results.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide

QUESTION 312

You have a configured a data loss prevention (DLP) with the following settings:

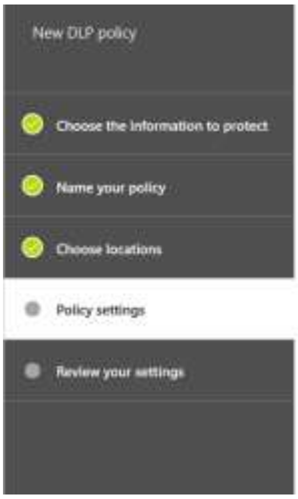


New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

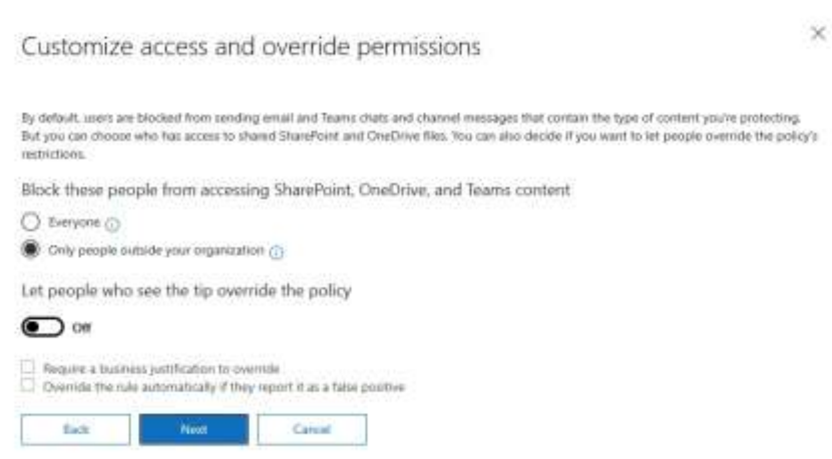
Choose locations

Status	Location	Include	Exclude
Off	Exchange email		
Off	SharePoint sites		
Off	OneDrive accounts		
Off	Teams chat and channel messages		



New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings



Customize access and override permissions

By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions.

Block these people from accessing SharePoint, OneDrive, and Teams content

○ Everyone

● Only people outside your organization

Let people who see the tip override the policy

Off

□ Require a business justification to override

□ Override the rule automatically if they report it as a false positive

After implementing the policy, your users are reporting that they can still send credit card number information out of the organization by mail. What must you change to ensure that the policy works as intended (stop information within the U.S. Patriot Act from being shared outside of the organization)?

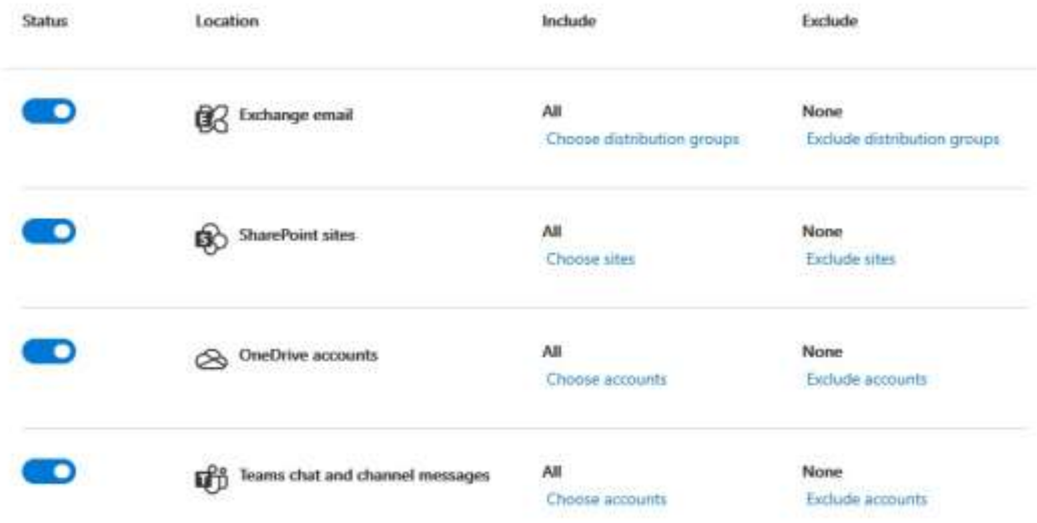
A. Encrypt email messages (applies only to content in Exchange)
B. Locations
C. Choose the information to protect
D. Let people who see the tip override the policy

Answer: B

Explanation:

In this policy all locations are disabled: Exchange email, SharePoint sites, OneDrive Accounts, Teams chat and channel messages.

You must enable the location of the service you want to impact:



Status	Location	Include	Exclude
On	Exchange email	All Choose distribution groups	None Exclude distribution groups
On	SharePoint sites	All Choose sites	None Exclude sites
On	OneDrive accounts	All Choose accounts	None Exclude accounts
On	Teams chat and channel messages	All Choose accounts	None Exclude accounts

QUESTION 313

You are a global administrator in an organization with a Microsoft 365 subscription. You want to protect the information that is being shared both inside and outside of your organization, so you decide to create Data Loss Prevention policies.

Your company has a big customer base in France, and you want to make sure email containing France National ID Card information cannot be sent out of your organization. Administrator and the user who is sending the email must be notified when rule match occurs.

For security reasons you would also like the administrator to be notified whenever someone emails Azure Storage Account Key information within your organization. The user sending the Storage Account Key information must also be

notified when rule match occurs.
You want to restrict users from sharing SWIFT Code from OneDrive outside of your organization, but also enable users to override the policy if needed. Users must state a business justification if they choose to override the policy.
Lastly you would like the administrator to be notified whenever someone is sharing a .exe file from OneDrive within your organization. The users sending and receiving the file must not be notified.
What is the minimum number of policies and rules needed to achieve this?

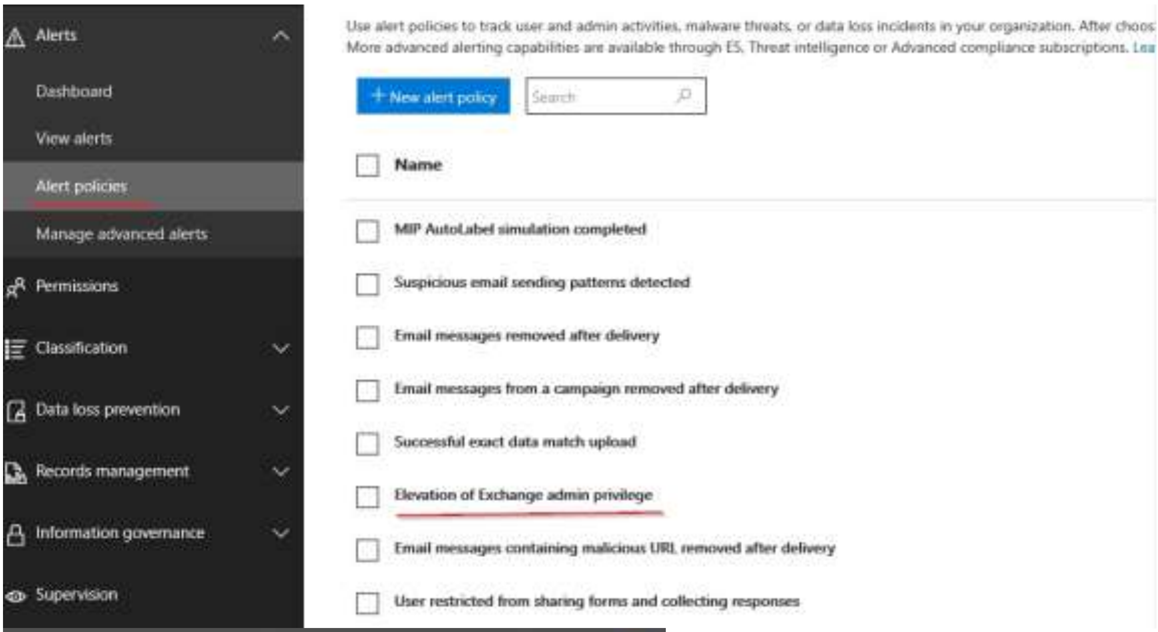
A. 1 policy, 2 rules
B. 2 policy, 2 rules
C. 2 policy, 3 rules
D. 2 policies, 4 rules
E. 3 policies, 2 rules
F. 3 policies, 3 rules

Answer: D
Explanation:
You need to create two DLP policies; one for Exchange (Policy 1) and one for OneDrive (Policy 2).
Within Policy 1 you must create two rules;
First one for stopping mail containing France National ID Card information from being sent outside the organization.
Second one for notifying the administrator and end user when they send mail containing Azure Storage Account Key information.
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

QUESTION 314
You are the IT administrator of an organization with a Microsoft 365 subscription. You need to be notified by email whenever someone is assigned administrative permissions in your Exchange Online organization. How would you configure this from the Security & Compliance admin center?

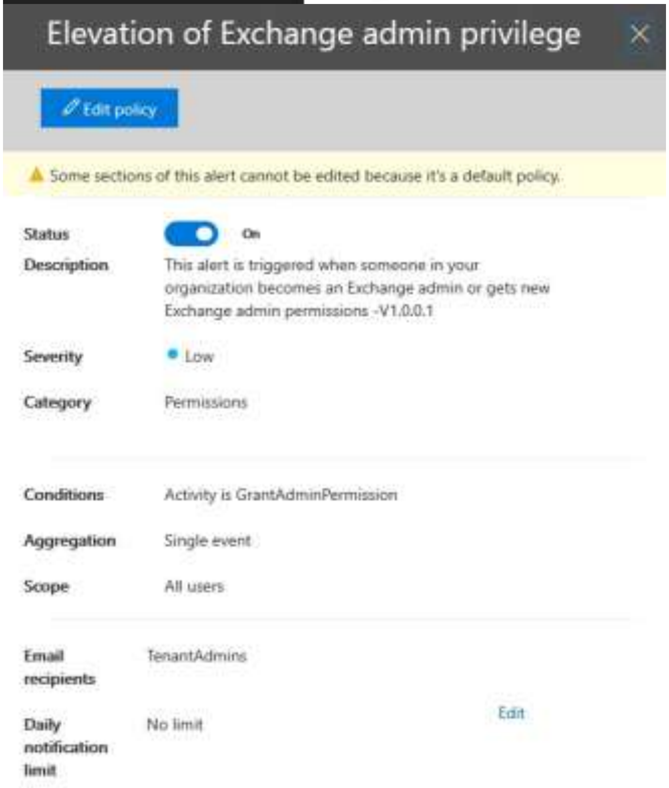
A. From Search & investigation, create an eDiscovery case
B. From Data privacy, create a Data subject request
C. From Records management, create an Event
D. From Alerts, create an alert policy

Answer: D
Explanation:
You need to create an alert policy for Elevation of Exchange admin privilege.
When enabled the policy generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.



Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choos
More advanced alerting capabilities are available through E5, Threat intelligence or Advanced compliance subscriptions. Lea

- □ Name
- □ MIP AutoLabel simulation completed
- □ Suspicious email sending patterns detected
- □ Email messages removed after delivery
- □ Email messages from a campaign removed after delivery
- □ Successful exact data match upload
- □ Elevation of Exchange admin privilege
- □ Email messages containing malicious URL removed after delivery
- □ User restricted from sharing forms and collecting responses



Elevation of Exchange admin privilege

Some sections of this alert cannot be edited because it's a default policy.

Status	On
Description	This alert is triggered when someone in your organization becomes an Exchange admin or gets new Exchange admin permissions -V1.0.0.1
Severity	● Low
Category	Permissions
Conditions	Activity is GrantAdminPermission
Aggregation	Single event
Scope	All users
Email recipients	TenantAdmins
Daily notification limit	No limit

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

QUESTION 315

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.

You have a Microsoft 365 subscription and are planning to install AD Connect to support an Active Directory hybrid identity solution. Your company is using a 3rd party authentication solution that requires smartcards. You need to choose an authentication method for the Azure AD hybrid identity solution. What do you do?
Solution: You configure Pass-through authentication.

Does that meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Pass-through authentication is not compatible with 3rd MFA solutions or smartcards.
Pass-through authentication should be used when the password validation must be on-premise, as it relies on local Active Directory for authentication. It is set up by installing an agent on an on-premise server that allows Azure AD to validate local AD passwords and usernames.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION 316
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.
You have a Microsoft 365 subscription and are planning to install AD Connect to support an Active Directory hybrid identity solution. Your company are using a 3rd party authentication solution that requires smartcards. You need to choose an authentication method for the Azure AD hybrid identity solution. What do you do?
Solution: You configure Password hash synchronization.
Does that meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Password hash synchronization is not compatible with 3rd MFA solutions or smartcards.
Password hash synchronization synchronizes your AD DS user accounts with Microsoft 365 and manages your users on-premises. Hashes of user passwords are synchronized from your AD DS to Azure AD so that the users have the same password on-premises and in the cloud.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs

QUESTION 317
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.
You have a Microsoft 365 subscription and are planning to install AD Connect to support an Active Directory hybrid identity solution. Your company are using a 3rd party authentication solution that requires smartcards. You need to choose an authentication method for the Azure AD hybrid identity solution. What do you do?
Solution: You configure Federated authentication.
Does that meet the goal?

A. Yes
B. No

Answer: A
Explanation:
Federated authentication can support additional authentication requirements, such as smartcard-based authentication or a third-party multi-factor authentication.
Federated authentication is most common for large organizations with complex authentication requirements. Users

have the same password on-premise and in the cloud.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

QUESTION 318
You have a Microsoft 365 subscription with 30 E5 and 30 E3 available licenses. Your company has 3 departments: IT, Sales and Management. You need to make sure all users in the Management department will be assigned the E5 license automatically with the least amount of management on your end. What should you do?

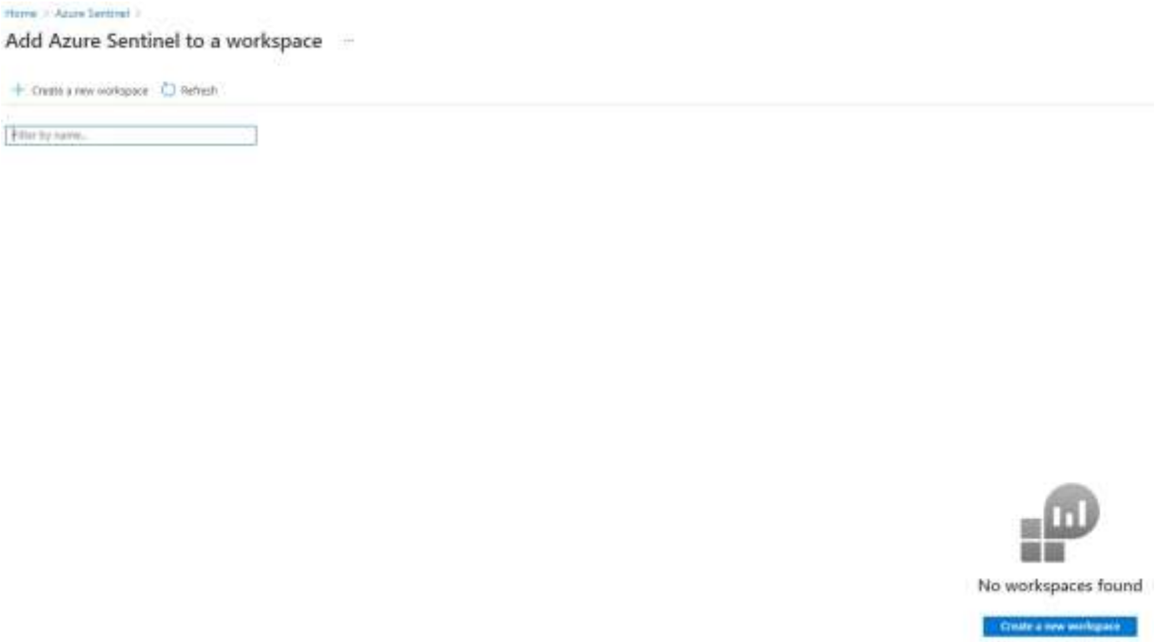
A. In Azure Active Directory, create a security group with dynamic membership rules. Set the rule property to department and value to "Management", and then assign the E5 license to the security group
B. Assign the license manually when creating the new users
C. Create an access review
D. Create a powershell script that assigns E5 license to Management-users and run it weekly

Answer: A
Explanation:
Best approach here is to create a dynamic membership security rule that will automatically include all users in the Management-department.
By assigning the license to the security group, all users within the group will be licensed.
Option B is incorrect. This will not assign the licenses automatically and would be time-consuming.
Option C is incorrect. Access reviews are typically used to scope out user access and assignments. Not the way to go here.
Option D is incorrect. This will not assign the licenses automatically and is time-consuming.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule

QUESTION 319
You are a global administrator in a company with Microsoft 365 E5 licenses assigned to your users. The company is planning onboarding to Azure Sentinel as a solution to proactively detect and stop threats. You will be deploying the solution. What is the first thing you must do?

A. Create a new Log Analytics Workspace
B. Upgrade your license to Microsoft Defender for Office 365 plan 2
C. Create a conditional access policy
D. Within Azure Sentinel, connect a data source

Answer: A
Explanation:
To enable Azure Sentinel, you must first create a Log Analytics Workspace. After it is created you will add Azure Sentinel to the new workspace:



Home > Azure Sentinel >

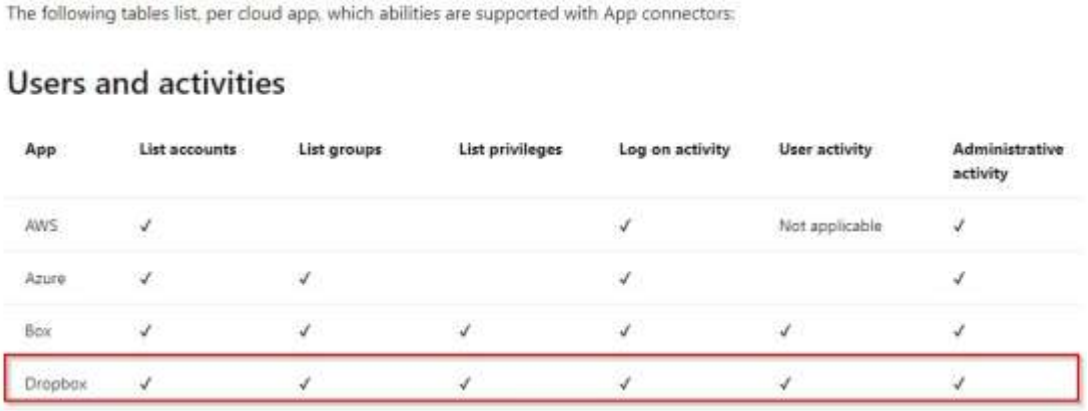
Add Azure Sentinel to a workspace ···

After these steps are completed you can start configuring your Sentinel solution by adding data sources.
Option B is incorrect. This is not a requirement to deploy Azure Sentinel.
Option C is incorrect. Creating a conditional access policy is not relevant in this scenario.
Option D is incorrect. You must first create a Log Analytics Workspace and the add Sentinel to the workspace.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

QUESTION 320
You are the IT administrator in a company with a Microsoft 365 E5 subscription. Your users are using Dropbox daily, and you want to be able to view the user activity from your organization in Dropbox. What should you configure?

A. In Cloud App Security - App connectors - Add an app
B. In Azure AD - register an app
C. In Cloud App Security - Control - Templates - Create a policy
D. In Azure AD - Create an access package

Answer: A
Explanation:
You can get visibility over the apps your users connect to by using Microsoft Cloud App Security.
You add an app by navigating to App connectors within Cloud App Security, and configuring steps to connect to the app. When the app is connected to gain visibility into the usage.



The following tables list, per cloud app, which abilities are supported with App connectors:

Users and activities

App	List accounts	List groups	List privileges	Log on activity	User activity	Administrative activity
AWS	✓			✓	Not applicable	✓
Azure	✓	✓		✓		✓
Box	✓	✓	✓	✓	✓	✓
Dropbox	✓	✓	✓	✓	✓	✓

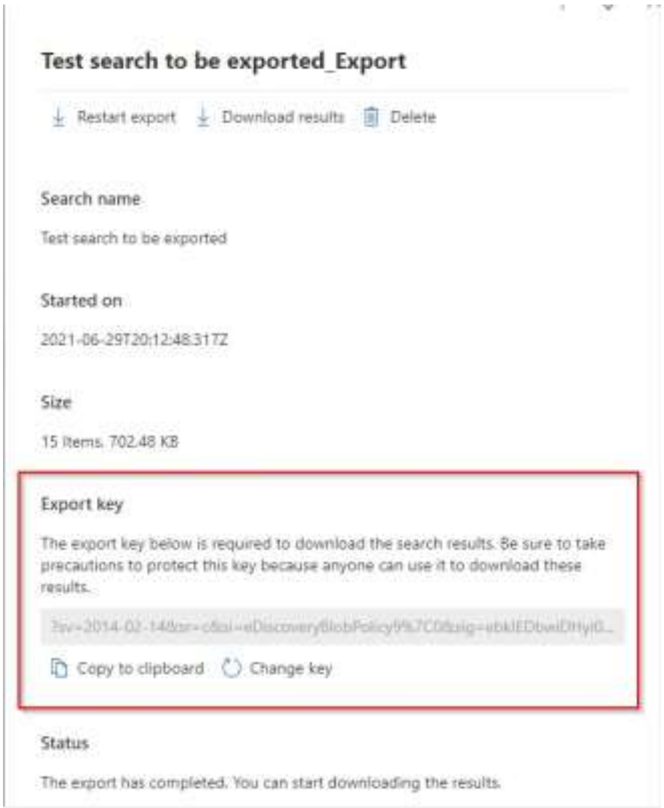
Option B is incorrect. Registering an app in Azure AD is not relevant in this scenario.
Option C is incorrect. Creating policies within cloud app security allows you to create governance actions and set data loss prevention and file-sharing controls.

Option D is incorrect. Creating an access package in Azure AD is not relevant in this scenario.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security

QUESTION 321
You are a global admin in a company with a Microsoft 365 subscription. In Microsoft 365 Compliance Center you have created a new Content Search, and now wish to export the result. What do you need first to export the findings?

A. a certificate
B. a shared access key
C. an export key
D. a password

Answer: C
Explanation:
After you have created a content search and waited for it to finish, you can export the results (given you have the appropriate role permissions). However, you must first obtain the Export key which will be needed when you download the results:



Test search to be exported_Export

Restart export | Download results | Delete

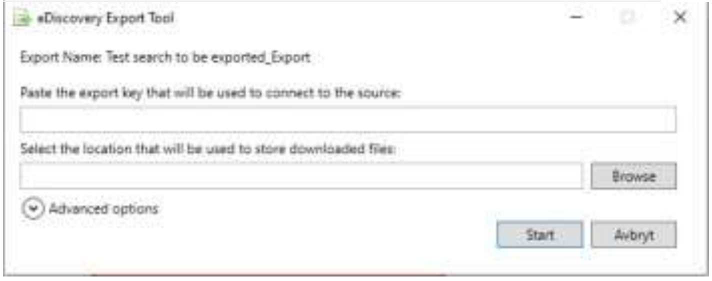
Search name
Test search to be exported

Started on
2021-06-29T20:12:48.317Z

Size
15 Items. 702.48 KB

Export key
The export key below is required to download the search results. Be sure to take precautions to protect this key because anyone can use it to download these results.
?sv=2014-02-14&sr=c&si=eDiscoveryBlobPolicy9%7C0&sig=ebklEDbwiDHyi0...
Copy to clipboard | Change key

Status
The export has completed. You can start downloading the results.



eDiscovery Export Tool

Export Name: Test search to be exported_Export

Paste the export key that will be used to connect to the source:

Select the location that will be used to store downloaded files:

Browse

Advanced options

Start | Avbryt

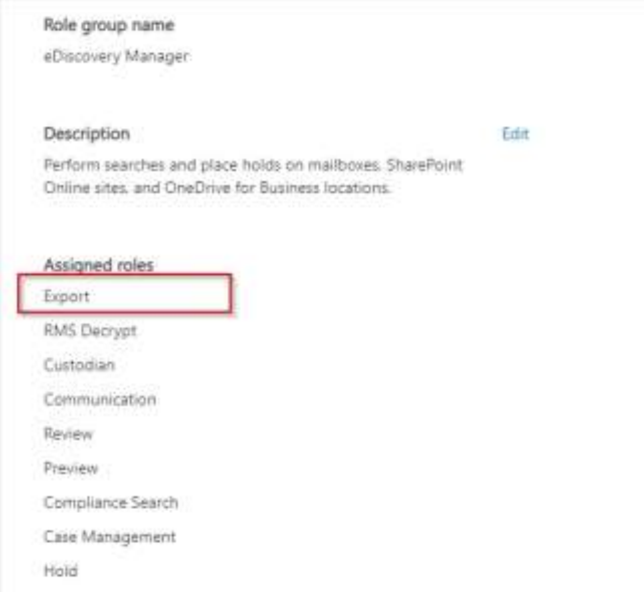
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide

QUESTION 322
You are a global admin in a company with a Microsoft 365 subscription. In Microsoft 365 Compliance Center you have created a new Content Search, and you want your helpdesk to be able to export the result. How should you enable

them to do this? You must use the principle of least privilege.

A. In Security & Compliance Center, add the users to the eDiscovery Manager role
B. In Office 365 admin center, add the users to the Helpdesk Administrator role
C. In Security & Compliance Center, add the users to the eDiscovery Administrator role
D. In Security & Compliance Center, add the users to the Compliance Administrator role

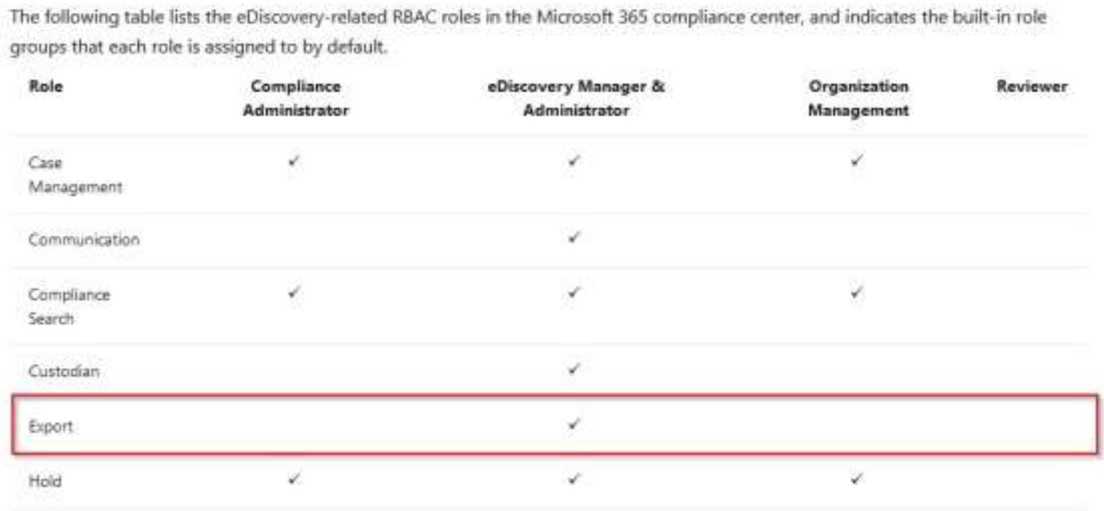
Answer: A
Explanation:
The least privileged role with permission to export content search results are the eDiscovery Manager role.



Role group name
eDiscovery Manager

Description
Perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations.

Assigned roles
Export
RMS Decrypt
Custodian
Communication
Review
Preview
Compliance Search
Case Management
Hold



The following table lists the eDiscovery-related RBAC roles in the Microsoft 365 compliance center, and indicates the built-in role groups that each role is assigned to by default.

Role	Compliance Administrator	eDiscovery Manager & Administrator	Organization Management	Reviewer
Case Management	✓	✓	✓	
Communication		✓		
Compliance Search	✓	✓	✓	
Custodian		✓		
Export		✓		
Hold	✓	✓	✓	

Option B is incorrect. This role will not permit you to export content search results.
Option C is incorrect. This role will allow you to export content search results, but it is not the least privileged alternative.
Option D is incorrect. This role will not permit you to export content search results.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide

QUESTION 323
You have several Conditional Access policies that block noncompliant devices from connecting to services.
You need to identify which devices are blocked by which policies.
What should you use?

A. the Setting compliance report in the Microsoft Endpoint Manager admin center
B. Sign-ins in the Azure Active Directory admin center
C. Activity log in the Cloud App Security portal
D. Audit logs in the Azure Active Directory admin center

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access

QUESTION 324
You have a Microsoft 365 tenant.
You need to implement a policy to enforce the following requirements:
- If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint Online only from a web browser. The user must be prevented from downloading files or syncing files from SharePoint Online.
- If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files.
What should you create?

A. a conditional access policy in Azure AD that has Client apps conditions configured
B. a conditional access policy in Azure AD that has Session controls configured
C. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured
D. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session